ON GALOIS FIELDS OF CERTAIN TYPES*

BY

LEONARD CARLITZ

1. Introduction

Several writers have considered the relations between the ζ-functions of an algebraic field and some of its subfields. Thus Artin† has, in a particular case, considered the question of the divisibility of the ζ-function of a field by that of a subfield. In another paper‡ he has shown how all possible ζ-relations can be found. Explicit results of a general nature are however not arrived at. Herglotz§ has investigated fields formed by the composition of several quadratic fields, thus generalizing a well known result of Dirichlet's.¶ Pollaczek|| has obtained results of a similar kind for Abelian fields with group of type (1, 1).

In all the cases cited, use is made of Hecke's** functional equation for the ζ-function in an arbitrary field. Thus, for example, in Artin's first paper, a ζ-relation is proved, except for a finite number of factors, by quite elementary methods; employing the functional equation, it is seen to hold in its entirety. Again, Herglotz and Pollaczek deduce discriminantal relationships by means of the functional equation.

In the following an explicit relation between ζ-functions is deduced. The fields considered include as special cases those of Artin (first paper), Herglotz, and Pollaczek. No use is made of the Hecke functional equation; instead a method of an elementary nature is employed. Relations between discriminants also are easily proved by direct means. The first result of interest may be formulated thus:

Let K be an (absolute) Galois field of degree m and group G_m.†† We make

* Presented to the Society, April 18, 1930; received by the editors in March, 1930.

† *Ueber die Zetafunktionen gewisser algebraischer Zahlkörper*, Mathematische Annalen, vol. 89 (1923), p. 147.

‡ *Ueber eine neue Art von L-Reihen*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 3 (1924), p. 88.

§ *Ueber einen Dirichletschen Satz*, Mathematische Zeitschrift, vol. 12 (1922), p. 255.

¶ Werke, vol. 1, p. 533.

|| *Ueber die Einheiten relativ-abelscher Zahlkörper*, Mathematische Zeitschrift, vol. 30 (1929), p. 520.

** *Ueber eine neue Anwendung der Zetafunktionen auf die Arithmetik der Zahlkörper*, Göttinger Nachrichten, 1917, p. 90.

†† Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), p. 248.

the following assumptions concerning G_m: G_l is an invariant subgroup of index a, $m=la$. The complex $(G_m-G_l+l\cdot I)$, I representing the identity, may be exhibited as the sum of l non-overlapping conjugate groups. Further let k_a be the Galois field corresponding* to G_l. To the l groups of order a mentioned above, let there correspond the l conjugate fields of degree l, $k_l, k_l', \cdots, k_l^{(l-1)}$. With the above definitions and assumptions we shall prove (§3)

$$\zeta^a\zeta_K = \zeta_{k_a}\zeta_{k_l}{}^a. \tag{1}$$

If we next suppose that K is a *relative* Galois field, the base field being some F, while all the remaining assumptions on K are taken over for K/F, then (1) becomes

$$\zeta_F{}^a\zeta_K = \zeta_{k_a}\zeta_{k_l}{}^a. \tag{1a}$$

(It should be noted that all our ζ-relations are proved only for a half-plane.)

The second general result concerns the discriminants of the fields defined. If by $d(k)$ we denote the discriminant of any field k, we find (§4)

$$d(K) = \pm\, d(k_a)d^a(k_l), \tag{2}$$

when K is absolute Galoisian. In the more general case, we may suppose that each d in (2) is a relative with respect to the field F. We then readily derive

$$d^a(F)d(K) = \pm\, d(k_a)d^a(k_l), \tag{2a}$$

where each d is now an absolute discriminant.

In §5 are sketched the proof of formulas like (1) and (2) for the case of Abelian fields of type $(1, 1, \cdots, 1)$; in particular might be mentioned (18) and (19).

In §§6, 7, (1) and (2) and their analogs of §5 are applied to prove results that appear new. The results of the first section are contained in (30) and (31). A typical though particular result of §7 follows:

Let $k_4^1=k([a+b^{1/2}]^{1/2})$, $k_4^2=k([2a+2(a^2-b^2)^{1/2}]^{1/2})$, $k_2=k([(a^2-b)b]^{1/2})$, where neither a^2-b nor $(a^2-b)b$ is a square. Then K, the field compounded of k_4^1, k_4^2, k_2 is readily seen to be Galoisian of degree eight,† and we shall prove

$$\zeta^2\zeta_K = \zeta_{k_2}\zeta_{k_4^1}\zeta_{k_4^2}$$

and

$$d(K) = \pm\, d(k_2)d(k_4^1)d(k_4^2).$$

---

* Hilbert, loc. cit., p. 250.

† Seidelmann, *Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich*, Mathematische Annalen, vol. 78 (1918), p. 232.

By means of (1) and (2) a ratio of class numbers is transformed into a corresponding ratio of regulators. In §8 this ratio of regulators is considered and, in a particular case, an upper and a lower bound of a simple sort are determined.

I wish to take this opportunity to acknowledge my indebtedness to Professor H. H. Mitchell for his valuable suggestions and his very helpful criticism.

2. Properties of G_m

Let G_a be one of the l subgroups of G_m contained in $(G_m - G_l + l\cdot I)$. Its operators will be denoted by $T_1, \cdots, T_a$. The operators of G_l will be taken as $S_1, \cdots, S_l$. We may suppose $S_1 = T_1 = I$.

Lemma 1.

$$G_m = G_l\cdot T_1 + \cdots + G_l\cdot T_a = G_l\cdot G_a, \tag{3}$$

and the factor group $G_m/G_l = G_a$.

To prove this, we observe first that the number of elements in $G_l\cdot T_1 + \cdots + G_l\cdot T_a$ is $la = m$. Further, no two complexes G_lT_α, G_lT_β have an element in common. For suppose

$$S_iT_\alpha = S_jT_\beta \quad (S_i, S_j \text{ in } G_l);$$

then

$$S_j^{-1}S_i = T_\beta T_\alpha^{-1}.$$

But G_l and G_a have only I in common; accordingly

$$S_i = S_j \quad\text{and}\quad T_\alpha = T_\beta,$$

which shows that all the elements in the sum are distinct.

Lemma 2.

$$l \equiv 1 \pmod{a}. \tag{4}$$

1. Let $S_i (2 \leqq i \leqq l)$ be any element of $(G_l - I)$. Then the set $T_\alpha S_i T_\alpha^{-1}$ $(\alpha = 1, \cdots, a)$ consists of a distinct elements of G. For from $T_\alpha S_i T_\alpha^{-1} = T_\beta S_i T_\beta^{-1}$ we have $S_i T_\alpha^{-1} T_\beta S_i^{-1} = T_\alpha^{-1} T_\beta$. But this implies $T_\alpha = T_\beta$.

2. Let now S_j be any element of $(G_l - I)$ not in the set $T_\alpha S_i T_\alpha^{-1}$. Then the sets $T_\alpha S_i T_\alpha^{-1}$ and $T_\alpha S_j T_\alpha^{-1}$ have no element in common. For from $T_\alpha S_i T_\alpha^{-1} = T_\beta S_j T_\beta^{-1}$ we should have $S_j = T_\beta^{-1} T_\alpha S_i T_\alpha^{-1} T_\beta$, which would mean that S_j belongs to the set $T_\alpha S_i T_\alpha^{-1}$.

We see then that the $l-1$ elements $S_i (i = 2, \cdots, l)$ fall into sets each containing a elements, and that no two of these sets have an element in common. Hence the truth of (4).

Suppose now that G_M is any subgroup of G_m. Let

$$G_L = D(G_M, G_l),$$

that is, the group common to G_M and G_l. We easily recognize that G_L is invariant under G_M. The nature of the factor group G_M/G_L is described by Lemmas 3 and 4.

LEMMA 3. *The factor group G_M/G_L is isomorphic with a subgroup of G_a.*

The lemma follows immediately from a known theorem.*

LEMMA 4. *The factor group G_M/G_L is isomorphic with G_A, a subgroup of G_M having only the identity in common with G_L.*

If G_L does not exhaust G_M let us take as G_a one of the l isomorphic subgroups that has in common with G_M at least one element other than the identity.

By (3), $G_m = G_l \cdot T_1 + \cdots + G_l \cdot T_a$; $G_a = (T_1 \cdots T_a)$. Let us suppose that G_M is contained in the first A complexes $G_l \cdot T_1 + \cdots + G_l \cdot T_A$ and that the T's are so numbered that each complex actually contains at least one element of G_M. Comparison with the proof of Lemma 3 shows that the complex $(T_1 \cdots T_A)$ forms a subgroup G_A of G_M isomorphic with G_M/G_L, thus establishing the lemma.

From Lemma 4 follows without difficulty

LEMMA 5. *The complex $(G_M - G_L + L \cdot I)$ may be exhibited as the sum of L non-overlapping conjugate groups each isomorphic with G_M/G_L.*

LEMMA 6. *Let G_M be an invariant subgroup of G_m, such that G_m/G_M is cyclic of order μ. Then, either*

$$(5)\quad \begin{array}{ll} \text{(I)} & l = L \text{ and } a = \mu A;\ \text{or} \\ \text{(II)} & l = \mu L \text{ and } a = A = 1. \end{array}$$

1. Assume (I) does not hold, and that $A > 1$.

Now the L subgroups G_A of G_M are contained in L of the l subgroups G_a. Let S (of G_l) transform one of these last groups into a G_a having only the identity in common with the set of L groups. Then the G_A it contains is transformed into a group necessarily different from any of the L subgroups G_A contained in G_M. Hence, when $l > L$ and $A > 1$, G_M cannot be invariant under G_m.

2. Suppose then that $l > L$, $A = 1$, but $a > A$.

Then

* Cf. Fricke, *Algebra*, 1924, vol. 1, p. 277.

$$
\begin{aligned}
G_m = G_l G_a &= \sum_{i=1}^{1/L} \sum_{j=1}^{a} S_i G_L T_j \\
&= \sum \sum S_j G_M T_j = \sum \sum G_M S_i T_j \\
&= \sum_{i=0}^{\mu-1} G_M V^2 .
\end{aligned} \tag{6}
$$

But $V = ST(T \neq I)$ is an element of $(G_m - G_l)$ and therefore of order $\leqq a$. But $\mu = la/L > a$; (6) is then impossible.

3. Derivation of the ζ-relation

Dedekind* has shown how to derive the decomposition of a rational prime in a subfield of a Galois field when its decomposition in the larger field is assumed:

Let K be a Galois field of degree m and group H_m. Let k be a subfield of K of degree μ corresponding to a subgroup H_ν of order ν, $m = \mu\nu$. Suppose that in K

$$p = (\mathfrak{P}_1 \cdots \mathfrak{P}_e)^\lambda ; \ \mathfrak{P}_i \text{ of degree } g. \tag{7}$$

Then in k,

$$p = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_\tau^{a_\tau} ; \ \mathfrak{p}_i \text{ of degree } g_i' ;$$

and

$$\mathfrak{p}_i = (\mathfrak{P}_{i1} \cdots \mathfrak{P}_{i\rho_i})^{\lambda_i} ; \ \mathfrak{P}_{ij} \text{ of relative degree } g_i .$$

The quantities τ, a_i, ρ_i, g_i, g_i', λ_i must now be determined.

Let H_κ be the "Zerlegungsgruppe"† of any prime ideal $\mathfrak{P}$ in the right member of (7). Let H_m be decomposed with respect to the two subgroups H_ν, H_κ:

$$H_m = H_\nu \cdot V_1 \cdot H_\kappa + \cdots + H_\nu \cdot V_\tau \cdot H_\kappa ;$$

the number of complexes is precisely τ; no two complexes have an element in common; the number of elements in the ith complex is $\kappa\rho_i$, where $\sigma_i \rho_i = \nu$ and

$$H_{\sigma_i} = D(V_i \cdot H_\kappa \cdot V_i^{-1}, H_\nu) .$$

If H_λ denote the "Trägheitsgruppe"‡ of the ideal $\mathfrak{P}$, then λ_i is the order of the group

---

* *Zur Theorie der Ideale*, Göttinger Nachrichten, 1894, p. 272; or Fricke, *Algebra*, 1928, vol. 3, p. 186.

† Cf. Fricke, loc. cit., p. 171.

‡ Fricke, loc. cit.

$$H_{\lambda_i} = D(V_i \cdot H_\lambda \cdot V_i^{-1}, H_\nu).$$

Other relationships to be noted are

$$\kappa = g\lambda, \quad g = g_i g_i', \quad g_i\lambda_i = \sigma_i, \quad a_i\lambda_i = \lambda, \quad \sum \rho_i = e.$$

To apply the Dedekind theory, suppose $H_m \equiv G_m$ as defined above.

1. Let $H_\nu = G_l$:

$$G_m = G_l \cdot V_1 \cdot H_\kappa + \cdots + G_l \cdot V_\tau \cdot H_\kappa.$$

By Lemma 5, $H_\kappa = G_L\ G_A$, $G_L = D(H_\kappa, G_l)$; and since H_κ satisfies all the assumptions made on G_m, we have $H_\lambda = G_{L'} \cdot G_{A'}$, where

$$G_{L'} = D(G_L, H_\lambda), \quad H_\lambda / G_{L'} = G_{A'}.$$

We have then

$$D(V_i \cdot H_\kappa \cdot V_i^{-1}, G_l) = V_i \cdot G_L \cdot V_i^{-1},$$

and

$$D(V_i \cdot H_\lambda \cdot V_i^{-1}, G_l) = V_i \cdot G_{L'} \cdot V_i^{-1}.$$

Therefore,

$$\begin{aligned} &\sigma_i = L, \quad &&\rho_i = l/L, \quad &&\tau\rho_i = e, \quad &&\tau = eL/l; \\ &\lambda_i = L', \quad &&g_i = L/L', \quad &&g_i' = gL'/L, \quad &&a_i = \lambda/L'. \end{aligned} \tag{8}$$

2. Let $H_\nu = G_a$:

$$G_m = G_a \cdot V_1 \cdot H_\kappa + \cdots + G_a \cdot V_\tau \cdot H_\kappa.$$

We may suppose G_a is that one of the l conjugates that contains $G_A (A > 1$; when $A = 1$, any G_a will serve the purpose). Evidently

$$D(V_i \cdot H_\kappa \cdot V_i^{-1}, G_a) = \begin{cases} G_{A'} & \text{for } i = 1, \\ G_1 & \text{for } i > 1; \end{cases}$$

whence

$$\sigma_1 = A, \quad \sigma_2 = \cdots = \sigma_\tau = 1;$$

$$\rho_1 = \frac{a}{A}, \quad \rho_2 = \cdots = \rho_\tau = a;$$

$$D(V_i \cdot H_\lambda \cdot V_i^{-1}, G_a) = \begin{cases} G_A & \text{for } i = 1, \\ G_1 & \text{for } i > 1; \end{cases} \tag{9}$$

$$\lambda_1 = A', \quad \lambda_2 = \cdots = \lambda_\tau = 1; \quad g_1 = \frac{A}{A'}, \quad g_2 = \cdots = g_\tau = 1;$$

$$g_1' = \frac{gA'}{A}, \quad g_2' = \cdots = g_\tau' = g; \quad a_1 = \frac{\lambda}{A'}, \quad a_2 = \cdots = a_\tau = \lambda;$$

$$\frac{a}{A} + (\tau - 1)a = e; \quad \tau - 1 = \frac{e}{a} - \frac{1}{A}\cdot$$

Now in K we clearly have, using (7),

$$\zeta_K(s) = \prod_p \frac{1}{\left(1 - \frac{1}{p^{gs}}\right)^e}\cdot \tag{10}$$

Let us fix our attention on a particular G_κ, and suppose it the Zerlegungsgruppe for some $\mathfrak{P}$, $\mathfrak{P}/p$. We then seek that factor of $\zeta_{k_a}(s)$ corresponding to p. By (8), the decomposition of p in k_a is

$$p = (\mathfrak{p}_1 \cdots \mathfrak{p}_\tau)^{\lambda/L'}, \ \tau = \frac{eL}{l};$$

each $\mathfrak{p}$ of degree gL'/L. Therefore the factor in question is

$$\frac{1}{\left(1 - \frac{1}{p^{gL's/L}}\right)^{eL/l}}\cdot \tag{11}$$

As for the factor in k_l, we have, by (9), that p decomposes in k_l thus:

$$p = \mathfrak{p}_1^{\lambda/A'}(\mathfrak{p}_2 \cdots \mathfrak{p}_\tau)^\lambda, \ \tau = 1 + \frac{e}{a} - \frac{1}{A};$$

degree of $\mathfrak{p}_1 = gA'/A$; degree of $\mathfrak{p}_i (i = 2, \cdots, \tau) = g$. We find then

$$\frac{1}{\left(1 - \frac{1}{p^{gA's/A}}\right)\left(1 - \frac{1}{p^{gs}}\right)^{e/a-1/A}}\cdot \tag{12}$$

To prove (1) we must then verify that the product of the expression (11) by the ath power of (12) is (using (10))

$$\frac{1}{\left(1 - \frac{1}{p^{gs}}\right)^e} \frac{1}{\left(1 - \frac{1}{p^{s}}\right)^a}\cdot$$

We notice first that G_κ, necessarily a subgroup of G_m, has the same properties as G_m (Lemma 5). Further it is known that G_λ is invariant under G_κ and that the factor group G_κ/G_λ is cyclic.* Lemma 6 may then be applied,

* Fricke, loc. cit., p. 175.

and we find that either

$$\text{(I)} \qquad L = L' \text{ and } A = gA'; \text{ or}$$

$$\text{(II)} \qquad L = gL \text{ and } A = A' = 1.$$

(I) We must show that

$$\left(1 - \frac{1}{p^{gs}}\right)^{-eL/l}\left[\left(1 - \frac{1}{p^{s}}\right)\left(1 - \frac{1}{p^{gs}}\right)^{e/a-1/A}\right]^{-a} = \left(1 - \frac{1}{p^{gs}}\right)^{-e}\left(1 - \frac{1}{p^{s}}\right)^{-a};$$

which is correct, since

$$\frac{eL}{l} + e - \frac{a}{A} = e + \frac{eLA - la}{lA} = e + \frac{e\kappa - m}{lA} = e.$$

(II) Here we are to prove

$$\left(1 - \frac{1}{p^{s}}\right)^{-eL/l}\left[\left(1 - \frac{1}{p^{gs}}\right)^{e/a}\right]^{-a} = \left(1 - \frac{1}{p^{gs}}\right)^{-e}\left(1 - \frac{1}{p^{s}}\right)^{-a}.$$

This follows immediately from

$$\frac{eL}{l} = \frac{eLA}{la}\cdot a = \frac{e\kappa}{m}\cdot a = a.$$

The proof of (1) is then complete.

It is unnecessary to give the proof of (1a) since the Dedekind theory holds (with one obvious modification) for relative Galois fields.*

4. Proof of (2)

Let Ω be the fundamental form† of K, and let $\mathfrak{d}$ be the "differente" of K. Evidently

$$\text{(13)} \qquad \mathfrak{d} = \prod_{\substack{U \text{ in } G_m \\ U \neq I}} (\Omega - U\Omega).$$

If k be any subfield of K, we shall let $\mathfrak{d}(k)$ and $\mathfrak{D}(k)$ denote respectively the differente of k and the differente of K relative to k. As is well known‡

$$\text{(14)} \qquad \mathfrak{d} = \mathfrak{d}(k)\mathfrak{D}(k).$$

If we suppose that k corresponds to the subgroup G_M of G_m, then

$$\text{(15)} \qquad \mathfrak{D}(k) = \prod_{\substack{U \text{ in } G_M \\ U \neq I}} (\Omega - U\Omega).$$

* See, for example, Weber, *Algebra*, 1899, vol. 2, p. 657.

† Cf. Hilbert, loc. cit., p. 195.

‡ Hilbert, loc. cit., Satz 41.

Applying (15) we find that

$$\mathfrak{D}(k_a) = \prod(\Omega - U\Omega),\ U \text{ in } (G_l - I),$$
$$\mathfrak{D}(k_l) = \prod(\Omega - U\Omega),\ U \text{ in } (G_a - I),$$
$$\mathfrak{D}(S_2k_l) = \prod(\Omega - U\Omega),\ U \text{ in } (S_2G_aS_2^{-1} - I),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{D}(S_lk_l) = \prod(\Omega - U\Omega),\ U \text{ in } (S_lG_aS_l^{-1} - I).$$

Multiplying together the corresponding members of these $l+1$ equations we get (using (13))

(16) $$\mathfrak{d} = \mathfrak{D}(k_a)\mathfrak{D}(k_l)\mathfrak{D}(S_2k_l)\cdots\mathfrak{D}(S_lk_l);$$

or, by (14),

$$\mathfrak{d}^l = \mathfrak{d}(k_a)\mathfrak{d}(k_l)\mathfrak{d}(S_2k_l)\cdots\mathfrak{d}(S_lk_l).$$

But

$$d(k_l) = \mathfrak{d}(k_l)\mathfrak{d}(S_2k_l)\cdots\mathfrak{d}(S_lk_l),*$$

so that (16) may be written

(17) $$\mathfrak{d}^l = \mathfrak{d}(k_a)d(k_l).$$

Now in a Galois field (of degree m) the discriminant is the mth power of the differente.† Hence, from (17) we infer

(2) $$d = d(k_a)d^a(k_l).$$

It seems scarcely necessary to go into the proof of (2a); the remark made in the Introduction indicates how it may be readily derived from (2).

5. Abelian fields of type (1, 1, · · · , 1)

We shall now briefly consider Abelian fields that are compounded of cyclic fields of equal prime degree. Assume then K an Abelian field with group G_{q^f} of type (1, 1, · · · , to f units), q a prime. G_{q^f} contains $(q^f-1)/(q-1)$ subgroups of order q^{f-1};‡ hence K contains $(q^f-1)/(q-1)$ cyclic fields. If these fields be denoted by $k^1, \cdots, k^{r_f}$, where $r_f=(q^f-1)/(q-1)$, then we shall prove

(18) $$\zeta^{r_f-1}\zeta_K = \zeta_{K^1}\cdots\zeta_{K^r};$$

(19) $$d(K) = d(k^1)\cdots d(k^{r_f}).\S$$

---

* Hilbert, loc. cit., Satz 37.

† Hilbert, loc. cit., Satz 68.

‡ Cf. Burnside, *Theory of Groups*, 1912, p. 60.

§ Cf. Pollaczek, loc. cit., p. 534.

(I) **Proof of (18).** Assume that in K, $p=(\mathfrak{P}_1 \cdots \mathfrak{P}_e)^\lambda$, each $\mathfrak{P}$ of degree g. We employ Dedekind's method (§3). Let G_κ be the Zerlegungsgruppe of $\mathfrak{P}_1$ (and therefore of each of the remaining $\mathfrak{P}$'s). Since G_κ/G_λ is cyclic, there are but two cases to consider: (1) $\kappa=\lambda$; (2) $\kappa=q\lambda$.

(1) $\kappa=\lambda=q^t$. Put $G_{q^f}=G_\nu\cdot V_1\cdot G_\kappa+\cdots+G_\nu\cdot V_\tau\cdot G_\kappa$, where G_ν is one of the r_f subgroups of G_{q^f} of order q. (Corresponding to G_ν is then a field of degree q^{f-1}.)

Now

$$D(G_\kappa,G_\nu) = \begin{cases} G_q & \text{for } r_t \text{ choices of } G_\nu, \\ G_1 & \text{for } (r_f - r_t) \text{ choices of } G_\nu; \end{cases}$$

$$D(G_\lambda,\ G_\nu) = D(G_\kappa,\ G_\nu).$$

For r_t choices of G_ν, then, $\tau=e$, $g_i'=1$; for the remaining (r_f-r_t) choices, $\tau=e/q$, $g_i'=1$. Typical factors of the associated ζ-functions are then

$$\frac{1}{\left(1-\dfrac{1}{p^s}\right)^e} \text{ and } \frac{1}{\left(1-\dfrac{1}{p^s}\right)^{e/p}}, \text{ respectively.}$$

Since

$$er_t + e(r_f - r_t)/q = er_{f-1} + q^{f-1},$$

we may conclude that in this case ($\kappa=\lambda$)

$$\left(\prod\frac{1}{\left(1-\dfrac{1}{p^s}\right)^e}\right)^{r_t}\left(\prod\frac{1}{\left(1-\dfrac{1}{p^s}\right)^{e/q}}\right)^{r_f-r_t}$$

$$(20)\qquad =\left(\prod\frac{1}{\left(1-\dfrac{1}{p^s}\right)^e}\right)^{r_{f-1}}\left(\prod\frac{1}{1-\dfrac{1}{p^s}}\right)^{q^{f-1}},$$

the products extending only to primes p for which $\kappa=\lambda$.

(2) $\kappa=q^t$, $\lambda=q^{t-1}$. Again put $G_{q^f}=G_\nu\cdot V_1\cdot G_\kappa+\cdots+G_\nu\cdot V_1\cdot G_\kappa$. Then $D(G_\kappa,\ G_\nu)=G_q$ for r_t choices of G_ν; and for these choices of G_ν,

$$D(G_\lambda,G_\nu) = \begin{cases} G_q & r_{t-1} \text{ times;} \\ G_1 & \text{the remaining } q^{t-1} \text{ times.} \end{cases}$$

$D(G_\kappa,\ G_\nu)=G_1$ for (r_f-r_t) choices of G_ν; and for each such choice $D(G_\lambda,\ G_\nu)=G_1$.

Therefore,

for r_{t-1} choices of G_ν, $\tau = e$, $g_i' = q$;

for q^{t-1} choices of G_ν, $\tau = e$, $g_i' = 1$;

$$\text{for } (r_f - r_t) \text{ choices of } G_\nu,\ \tau = e/q,\ g_i' = q.$$

Factors of the corresponding ζ's are then

$$\frac{1}{\left(1-\frac{1}{p^{qs}}\right)^{e}},\quad \frac{1}{\left(1-\frac{1}{p^{s}}\right)^{e}} \text{ and } \frac{1}{\left(1-\frac{1}{p^{qs}}\right)^{e/q}}, \text{ respectively.}$$

From this we may write, since $e \cdot q^{t-1} = q^{f-1}$, and

$$er_{t-1} + (r_f - r_t)e/q = er^{f-1},$$

$$\left(\prod\left(1-\frac{1}{p^{qs}}\right)^{-e}\right)^{r_{t-1}}\left(\prod\left(1-\frac{1}{p^{qs}}\right)^{-e/q}\right)^{r_f - r_t}\left(\prod\left(1-\frac{1}{p^{s}}\right)^{-e}\right)^{q^{t-1}}$$

$$(21)\qquad = \left(\prod\left(1-\frac{1}{p^{qs}}\right)^{-e}\right)^{r_{f-1}}\left(\prod\left(1-\frac{1}{p^{s}}\right)^{-1}\right)^{q^{f-1}},$$

the products extending only to primes p for which $\kappa = q\lambda$.

From (20) and (21) follows immediately

$$(22)\qquad \zeta^{q^{f-1}}\zeta_K = \prod_k \zeta_k,$$

the product extending over the r_f fields of degree q^{f-1}. Making use of (22), (18) follows easily by induction on f.

(II) **Proof of (19).** We notice, to begin with, that

$$(G_{q^f} - I) = \sum (G_q - I),$$

the sum extending over the r_f subgroups G_q of G_{q^f}.

Then, if $\mathfrak{d}(k)$ and $\mathfrak{D}(k)$ have the same significance as in §4,

$$(23)\qquad \mathfrak{d} = \mathfrak{d}(K) = \prod_k \mathfrak{D}(k),$$

the product extending over the r_f subfields of K of degree q^{f-1}. Equations (23) together with $\mathfrak{d} = \mathfrak{d}(k)\mathfrak{D}(k)$ imply

$$\mathfrak{d}^{r_f - 1} = \prod_1^{r_f} \mathfrak{d}(k).$$

Raising both members of this equality to the q^{f-1}th power, we find

$$(24)\qquad d^{r_f - 1}(K) = \pm \prod_1^{r_f} d(k),\ k \text{ of degree } q^{f-1}.$$

Then, exactly as in proving (18), we may prove (19) by induction, making use of (24).

We may put (19) in a more general form that will be seen to include (24) as well. The proof consists of an easy induction so that we shall state the result only:

$$d^{r_{f-1,m-1}}(K) = \pm \prod_{1}^{r_{f,m}} d(k), \tag{25}$$

where the product extends over all the subfields of K of degree q^m, and $r_{f,m}$ is the number of subgroups of G_{q^f} of order q^m:

$$r_{f,m} = \frac{q^f - 1}{q - 1} \cdots \frac{q^{f-m+1} - 1}{q^m - 1}.$$

A similar generalization holds for (18):

$$\zeta^{r_{f,m}-r_{f-1,m-1}}\zeta_K^{r_{f-1,m-1}} = \prod_{1}^{r_{f,m}} \zeta_k, \tag{26}$$

the product being taken as in (25).

Finally, if we suppose K relative Abelian, the base field being some F, while everything else remains unchanged, then we may rewrite (25) and (26) thus:

$$d^{r_{f,m}-r_{f-1,m-1}}(F)d^{r_{f-1,m-1}}(K) = \pm \prod d(k), \tag{25a}$$

$$\zeta_F^{r_{f,m}-r_{f-1,m-1}}\zeta_K^{r_{f-1,m-1}} = \prod \zeta_k, \tag{26a}$$

the products being taken as in (25).

6. Several illustrations and an application

It may be of interest at this point to give several examples illustrating the group G_m defined in §1.

(I) We mention first the case treated by Artin.* The group G_m may be defined as a group of transformations

$$x' = \alpha x + \beta,$$

α and β being marks of a finite (Galois) field of degree $l = q^f$. The subgroup G_l consists of the transformations

$$x' = x + \beta;$$

a particular G_a is defined by $x' = \alpha x$, so that it is in this case cyclic.

(II) In this example, G_l and G_a are Abelian but l may be divisible by more than one prime.

* Mathematische Annalen, vol. 89 (1923), p. 147.

Let $l = p_1^{e_1} \cdots p_r^{e_r}$ $(e_i \geqq 1)$; let a be chosen so that $p_i \equiv 1$, mod a; let u_i appertain to a, mod $p_i^{e_i}$; choose u to satisfy $u \equiv u_i$, mod $p_i^{e_i}$; then we define G_m as the group generated by S and T, $S_i = I = T^a$, $TST^{-1} = S^u$. The group G_l is generated by S; and G_a may be taken as T and its powers.

(III) For the third instance,* we use a subgroup G_{72} of the Hessian group G_{216}.

The G_{72} is generated by S_1, S_2, T_1, T_2, where

$$S_1^3 = S_2^3 = I, \quad S_2S_1 = S_1S_2;$$
$$T_1^4 = T_2^4 = I, \quad T_1^2 = T_2^2 \neq I, \quad T_2T_1 \neq T_1^3T_2;$$
$$T_1S_1T_1^{-1} = S_1S_2, \quad T_1S_2T_1^{-1} = S_1S_2^2,$$
$$T_2S_1T_2^{-1} = S_1^2S_2, \quad T_2S_2T_2^{-1} = S_1S_2.$$

G_l consists of S_1, S_2, and products of powers of these elements; G_l is evidently Abelian of type (1,1).

For a particular G_a we take the group of order eight generated by T_1 and T_2. This group is not Abelian; it is indeed the quaternion group.

Returning to the first example, let K be a Galois field with group G_{la} as described $(l = q^f)$. Let k_a be the field corresponding to G_l; it is evidently Abelian. Let k_l be one of the l conjugate fields of degree l. Suppose it possible to choose m so that $0 < m < f$, $q^m \equiv 1$, mod a. Then it is easily seen that any subfield of K of degree $q^m a$ is Galoisian; furthermore its structure is exactly like that of K if we merely replace f by m.

To begin with, let us think of K as relative Galoisian to k_a; the relative group is Abelian of type $(1, 1, \cdots, 1)$. By (26a), if $F \equiv k_a$,

$$\zeta_{k_a}^{r_{f,m} - r_{f-1,m-1}} \zeta_K^{r_{f-1,m-1}} = \prod_1^{r_{f,m}} \zeta_k, \tag{27}$$

the product extending over all subfields of K that are of degree q^m relative to k_a (that is, to F). Now, by (1),

$$\zeta^a \zeta_K = \zeta_{k_a} \zeta_{k_l}^a; \tag{28}$$

and k_j' denoting one of the subfields of degree $j = q^m$ of some k (k as in (27)),

$$\zeta^a \zeta_k = \zeta_{k_a} \zeta_{k_j} \tag{29}$$

for each k. Substituting (28) and (29) in (27), we get

$$\zeta^{r_{f,m} - r_{f-1,m-1}} \zeta_{k_l}^{r_{f-1,m-1}} = \prod_1^{r_{f,m}} \zeta_{k_j}, \tag{30}$$

* This was suggested by Professor Mitchell.

the product on the right extending over all fields of degree $j=q^m$ (each set of j conjugate fields but one representative, namely, the one contained in k_l).

We may in exactly the same way derive a relation like (30) for discriminants:

$$d(k_l)^{r_{j-1,m-1}} = \pm \prod_{1}^{r_{j,m}} d(k_j). \tag{31}$$

7. A second application

We consider again the group G_m of §1, but we shall now make an additional restriction: a is some prime, q. Let us define a group G_{lq^2} of order lq^2 as the direct product of G_m and H_q, a group of order q. The group G_{lq^2} then contains q invariant subgroups isomorphic with G_m: If G_q be generated by T, i.e., $G_q=\{T\}$, and $H_q=\{U\}$, then the q subgroups are

$$G_l\cdot\{U^iT\} \qquad (i=1,\cdots,q).$$

Suppose now K is an absolute Galois field with group G_{lq^2} as defined above. To each $G_l\ \{U^iT\}$ corresponds a cyclic field k_q^i of degree q; K is a relative Galois field of relative degree m with respect to k_q^i; the relative group is $G_l\cdot\{U^iT\}$, i.e. G_m. Accordingly, if in (1a) we let $F\equiv k_q^i$,

$$\zeta_{k_q^i}^{q}\zeta_K = \zeta_{K_q^i}\zeta_{K_l^i}^{q} \qquad (i=1,\cdots,q), \tag{32}$$

where K_q^i is of relative degree q, and $K_l{}^i$ is of relative degree l. The field K_q^i is then of absolute degree q; if we think of K as an absolute Galois field, then, since G_{lq^2} has but one subgroup of order l, evidently all the symbols K_q^i denote the same field, K_q, say. Further G_l is invariant under G_{lq^2} and the factor group is Abelian of type (1, 1); therefore K_q is Abelian with group of the same type. The q fields k_q^i are of course subfields of K_q; it must contain one other; namely, the field corresponding to the subgroup $G_l\times H_q$ ($\times$ means direct product); this field will be called k_q. By (18),

$$\zeta^q\zeta_{K_q} = \zeta_{k_q}\prod_{i=1}^{q}\zeta_{k_q^i}. \tag{33}$$

Multiplying together the q equations (32), we find

$$\zeta_K\prod_{i=1}^{q}\zeta_{k_q^i} = \zeta_{K_q}\prod_{i=1}^{q}\zeta_{K_l^i}.$$

Applying (33), this may be written

$$\zeta^q\zeta_K = \zeta_{k_q}\prod_{i=1}^{q}\zeta_{K_l{}^i}. \tag{34}$$

For the discriminants we prove without any change in method

$$d^q(k_q^i)d(K) = \pm\, d(K_q)d^q(K_l^i), \tag{35}$$

and

$$d(K) = \pm\, d(k_q) \prod d(K_l^i), \tag{36}$$

corresponding to (32) and (34) respectively.

The special case mentioned in the Introduction does not fall under the above, but may be handled in much the same way. The group of K (using the notation of §1) is G_8:

$$G_8 = \{S, T\}, \quad S^4 = I = T^2, \quad TST = S^{-1}.$$

To $\{T\}$ corresponds k_4^1; to $\{ST\}$, k_4^2; to $\{S\}$, k_2. Let k_2^1, k_2^2 correspond to $\{S^2, T\}$, $\{S^2, ST\}$, respectively. To the invariant subgroup $\{S^2\}$ corresponds an Abelian A_4, of type (1, 1), containing k_2, k_2^1, k_2^2. Now with respect to k_2^i $(i=1, 2)$, K is relative Abelian of type (1, 1): The three relative fields are k_4^i (counted twice) and A_4. Then, by (26a), if $F \equiv k_2^i$, and $m=1$, $f=2$,

$$\zeta_{k_2^i}^2 \zeta_K = \zeta_{k_4^i} \zeta_{A_4},$$

whence

$$\zeta_{k_2^1} \zeta_{k_2^2} \zeta_K = \zeta_{A_4} \zeta_{k_4^1} \zeta_{k_4^2}.$$

But

$$\zeta^2 \zeta_{A_4} = \zeta_{k_2} \zeta_{k_2^1} \zeta_{k_2^2};$$

therefore, finally,

$$\zeta^2 \zeta_K = \zeta_{k_2} \zeta_{k_4^1} \zeta_{k_4^2}.$$

8. Comparison of regulators

After the fundamental Dirichlet-Dedekind expression, h, the class number of a field k, may be evaluated thus:

$$h\mu = \lim_{s=1} (s-1)\zeta_k(s), \tag{37}$$

$$\mu = \frac{2^{r_1+r_2}\pi^{r_2}R}{w|d^{1/2}|},$$

where

r_1 = number of real fields conjugate to k,
r_2 = number of pairs of imaginary fields conjugate to k,
w = number of roots of unity in k,
R = regulator in k.*

Let us return to the (absolute) Galois field K with group G_m as defined in §1. We shall assume in what follows that K is real; we see then that

* See, for example, Hecke, *Die Theorie der Algebraischen Zahlen*, p. 156.

$$\mu(K) = \frac{2^{m-1}R(K)}{[d(K)]^{1/2}}, \quad \mu(k_l) = \frac{2^{l-1}R(k_l)}{[d(k_l)]^{1/2}}, \quad \mu(k_a) = \frac{2^{a-1}R(k_a)}{[d(k_a)]^{1/2}}.$$

Hence, by (1), (2), and (37)

$$\frac{h(K)}{h^a(k_l)h(k_a)} = \frac{R^a(k_l)R(k_a)}{R(K)}. \tag{38}$$

We shall now consider the quotient of regulators in the right member of (38).

Let $\epsilon_1, \cdots, \epsilon_{a-1}$ be a set of fundamental units in k_a; $\eta_1, \cdots, \eta_{l-1}$ a set of fundamental units in k_l. It will be convenient to employ the following abbreviations:

$$T_iE_j = \log|T_i\epsilon_j| \qquad (i = 1, \cdots, a; j = 1, \cdots, a-1),$$
$$S_iH_j = \log|S_i\eta_j| \qquad (i = 1, \cdots, l; j = 1, \cdots, l-1),$$

where, as in §2, $G_l=(S_1, \cdots, S_l)$, $G_a=(T_1, \cdots, T_a)$, $S_1=T_1=I$. We construct the set of a distinct elements $T_iS_2T_i^{-1}(i=1, \cdots, a)$. It will be convenient to denote the members of this set by $U_1, \cdots, U_a$.

We now consider the set of $(m-1)$ units ϵ_i, $U_\alpha\eta_j$ $(i=1, \cdots, a-1$; $j=1, \cdots, l-1; \alpha=1, \cdots, a)$. Our object is to prove that *at least when l is a prime, they form a set of independent units in K.* Since much of the work goes through in the general case, we shall make no assumption about the nature of l until it is necessary. The regulator of the units in question will be called R_0; it will be formed thus:

1st row: $E_1 \cdots E_{a-1}\ U_1H_1 \cdots U_1H_{l-1} \cdots U_aH_{a-1}$		l rows;
2d row:	S_2(1st row)	
. . . .		
lth row:	S_l(1st row)	
$(l+1)$st row:	T_2(1st row)	l rows;
$(l+2)$d row:	$S_2((l+1)$st row)	
. . . .		
$(2l)$th row:	$S_l((l+1)$st row)	
. . . .		
$((a-1)l+1)$st row:	T_a(1st row)	$(l-1)$ rows.
. . . .		
$(al-1)$st row:	$S_{l-1}[(a-1)l+1]$st row	

A first simplification of this determinant can be effected by noticing that

(i) $SE_i = E_i$, (ii) $S_1H_j + \cdots + S_lH_j = 0$.

Let us add the 1st, 2d, $\cdots$, $(l-1)$st rows to the lth row; it will become

$$lE_1 \cdots lE_{a-1} 0\ 0 \cdots (al - a \text{ zeros}).$$

Similarly, if we add the $(l+1)$st, $\cdots$, $(2l-1)$st rows to the $(2l)$th row, it will become

$$lT_2E_1 \cdots lT_2E_{a-1} 0\ 0 \cdots (al - a \text{ zeros}).$$

And so on. It is clear that R_0 becomes

$$l^{a-1}\begin{vmatrix} E_1 & \cdots & E_{a-1} \\ T_2E_1 & \cdots & T_2E_{a-1} \\ \cdot & \cdots & \cdot \\ T_{a-1}E_1 & \cdots & T_{a-1}E_{a-1} \end{vmatrix} \cdot \Delta = \pm\, l^{a-1}R(k_a)\Delta, \tag{39}$$

where

$$\Delta = |\, M_{ij}\,|, \quad M_{ij} = \begin{Vmatrix} T_iU_jH_1 & \cdots & T_iU_jH_{l-1} \\ S_2T_iU_jH_1 & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ S_{l-1}T_iU_jH_1 & \cdots & \cdot \end{Vmatrix}.$$

Now from the definition of U_j it is clear that the set of matrices M_{ij} (i fixed; $j=1, \cdots, a$) is identical except for order with the set M_{1j}. Furthermore the set of permutations

$$\begin{pmatrix} M_{11} & M_{12} \cdots M_{1a} \\ M_{i1} & M_{i2} \cdots M_{ia} \end{pmatrix}$$

form a group isomorphic with G_a.

Let us write $M_{ij} = N_{ij}\overline{R}$,

$$\overline{R} = \| S_iH_j \| \qquad (i,j = 1, \cdots, l-1).$$

Then

$$\begin{aligned} \Delta &= |\, N_{ij}\,| \cdot |\, \overline{R}\,|^a \\ &= \pm\, |\, N_{ij}\,| \cdot R^a(k_l). \end{aligned} \tag{40}$$

The determinant $|N_{ij}|$ is a generalization of the class of determinants known as circulants. When G_a is Abelian the determinant may be transformed into a product of determinants of the $(l-1)$st order; this is a direct generalization of a known result.*

Assuming then that G_a is Abelian, let $\chi_\alpha(T)$ $(\alpha=1, \cdots, a)$ represent the

* Burnside, Messenger of Mathematics, vol. 23, p. 112.

a characters of the group.* Let

$$X_0 = |\chi_i(T_j)| \qquad (i,j = 1, \cdots, a);$$

then

$$|X_0|^2 = |\chi_i(T_j)| \cdot |\chi_i(T_j^{-1})| = |\sum_\alpha \chi_\alpha(T_i)\chi_\alpha(T_j^{-1})|$$
$$= |\sum_\alpha \chi_\alpha(T_i T_j^{-1})| = a^a.$$

Therefore

$$|X_0| = a^{a/2} \neq 0.$$

Let now $X = |\chi_i(T_j)E|$, where E is the $(l-1)$-rowed unit matrix; clearly, $X = X_0^{l-1}$. Therefore

$$X \neq 0. \tag{41}$$

Returning to $|N_{ij}|$, we have

$$|N_{ij}| \cdot X = |N_{ij}| \cdot |\chi_i(T_j)E| = |\sum_\alpha \chi_i(T_\alpha)N_{j\alpha}|$$
$$= |\sum_\alpha \chi_i(T_\alpha T_j^{-1})N_{1\alpha}| = |\chi_i(T_j^{-1}) \sum_\alpha \chi_i(T_\alpha)N_{1\alpha}|$$
$$= |\chi_i(T_j^{-1})E| \cdot \prod_i |\sum_\alpha \chi_i(T_\alpha)N_{1\alpha}|.$$

Therefore, by (41),

$$|N_{ij}| = \prod_i |\sum_\alpha \chi_i(T_\alpha)N_{1\alpha}|, \tag{42}$$

in absolute value.

Now exactly the same result obtains when $N_{1\alpha}$ is an ordinary (rather than a matric) quantity. We see then that a *determinant like $|N_{ij}|$ may be reduced to a product of determinants of order $l-1$ by treating its matric elements as if they were ordinary numbers.*

We suppose in the following that G_m is a "congruence group, modulo l," that is, a group that may be defined as the set of transformations†

$$x' \equiv \alpha x + \beta \qquad (\text{mod } l).$$

Let r appertain to the index a, mod l; then, if we define a matrix A of order $(l-1)$ by

$$A = \begin{Vmatrix} 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & 1 \\ -1 & -1 & -1 & \cdot & \cdot & -1 \end{Vmatrix}, \tag{43}$$

* Weber, loc. cit., p. 49.

† Fricke, loc. cit., vol. 1, p. 443 ff.

it is easily seen that the set of matrices $N_{1\alpha}$ is now replaced by A^{r^i} ($i=0, \cdots, a-1$). It should be noticed that

$$(44) \qquad A^l = E, \quad E + A + \cdots + A^{l-1} = 0.$$

Also, since G_α is now cyclic, its characters may be expressed in terms of ρ, a primitive root of unity of index a.

From the above it readily follows that (42) becomes

$$(45) \qquad |N_{ij}| = \prod_i \left| \sum_j \rho^{ij} A^{r^j} \right| .$$

The determinants in the right member may be evaluated by substituting for A a primitive lth root of unity, ζ. Now, $\sum_j \rho^{ij}\zeta^{r^j}$ is not zero; this follows from Kronecker's theorem on the irreducibility of the cyclotomic equation. We may then assert that $|N_{ij}| \neq 0$. Therefore, by (39) and (40), R_0 is not zero, so that the statement made at the beginning of this section is substantiated: *ϵ_i, $U_\alpha\eta_j$ form a set of independent units in K.*

Explicit results may be obtained very easily in two extreme cases: (I) $a=l-1$; (II) $a=2$.

(I) $a=l-1$. To evaluate the right member of (45) we note that $\sum_{j=0}^{a-1}\rho^{ij}\zeta^{r^j}$ is now the familiar Lagrange resolvent generally denoted by (ρ^i, ζ). For the resolvent we have

$$(\rho^0,\zeta) = -1 \text{ and } (\rho^i,\zeta)(\rho^{-i},\zeta) = (-1)^i l \qquad (i = 1, \cdots, l-2).$$

Hence, in this case,

$$|N_{ij}| = l^{(l-1)(l-2)/2} \text{ in absolute value.}$$

Therefore

$$(46) \qquad R_0 = l^{(l+1)(l-2)/2} R(k_a) R^a(k_l).$$

(II) $a=2$. $|N_{ij}|$ is here

$$\begin{vmatrix} A & A^{-1} \\ A^{-1} & A \end{vmatrix} = |A^2 - A^{-2}| = |A^{-2}| \cdot |A - E| \cdot |A + E| \cdot |A^2 + E| .$$

But, from (43), $|A| = 1$.

Secondly,

$$|A + E| \cdot |A^2 + E| \cdots |A^{l-1} + E| = 1,$$

whence $|A+E|=1$, $|A^2+E|=1$.

Thirdly,

$$|I - A| \cdot |I - A^2| \cdots |I - A^{l-1}| = |l| = l^{l-1};$$

therefore

$$|I - A| = l.$$

Finally, then,

$$R_0 = l^2 R(k_a) R^2(k_l).$$

Returning to (46), we shall now show that *the ratio of* R_0 *to* $R(K)$ *is a power* ($\geqq 0$) *of* l.

Assume $R_0 > R(K)$; then there exist a positive integer n, and a unit B of K, such that

$$\sum_1^{l-2} b_i E + \sum_1^{l-1} \sum_1^{l-1} b_{ij} S^i H_j = n \log |B|, \tag{47}$$

where

$$0 \leqq b_i < n, \quad 0 \leqq b_{ij} < n; \quad (b_1, \cdots, b_{l-2}, b_{11}, \cdots, b_{l-1,l-1}) = 1.$$

Putting (47) in exponential form, applying T^u, and reverting to the logarithmic form ($TST^{-1} = S^r$),

$$\sum b_i T^u E_i + \sum \sum b_{ij} S^{ir^u} H_j = n \log |T^u B| \qquad (u = 1, \cdots, l-2). \tag{48}$$

Adding (47) to the $(l-2)$ equations (48), we have

$$\sum_{i,j,u=1}^{l-1} b_{ij} S^{ir^u} H_j = n \log |B \cdot TB \cdots T^{l-2} B| = n \log |\alpha|, \tag{49}$$

α a unit in k_l.

Now

$$\begin{aligned} \sum_u S^{ir^u} H_j &= \sum_u S^{iu} H_j \\ &= \sum_u S^u H_j \text{ (since } 1 \leqq i \leqq l-1) \\ &= -H_{\cdot j}, \end{aligned}$$

so that (49) becomes

$$-\sum \sum b_{ij} H_j = n \log |\alpha|;$$

that is

$$-\sum_j \left(\sum b_{ij} \right) H_j = n \log |\alpha|.$$

But since the η_j form a fundamental set in k_l, this last equation implies

$$n \mid \sum_i b_{ij}. \tag{50}$$

We return again to (47) and begin by applying S^{-1}:

$$\sum b_i E_i + \sum\sum b_{ij} S^{i-1} H_j = n \log |S^{-1}B| . \tag{51}$$

The double summation can be transformed thus:

$$\begin{aligned}\sum_{i,j=1}^{l-1} b_{ij} S^{i-1} H_j &= \sum_j b_{1j} H_j + \sum_j \sum_{i=2}^{l-1} b_{ij} S^{i-1} H_j \\ &= -\sum_i \sum_j b_{1j} S^i H_j + \sum_j \sum_{i=1}^{l-2} b_{i+1,j} S^i H_j \\ &= \sum_i \sum_j \bar{b}_{ij} S^i H_j,\end{aligned}$$

where

$$\begin{aligned}\bar{b}_{ij} &= b_{i+1,j} - b_{1j} \quad \text{for } 1 \leqq i \leqq l-2, \\ \bar{b}_{ij} &= -b_{1j} \qquad\qquad \text{for } i = l-1.\end{aligned}$$

(51) may now be written as

$$\sum b_i E_i + \sum\sum \bar{b}_{ij} S^i H_j = n \log |\bar{B}| \qquad (\bar{B} = S^{-1}B). \tag{52}$$

But (52) is exactly like (47); therefore from (50)

$$n \mid \sum_i \bar{b}_{ij}.$$

(Note that in proving (50) no use is made of the auxiliary relations in (47).) This may be written, in terms of b_{ij}, in the following way:

$$n \mid \left(\sum_i b_{ij} - l b_{1j} \right). \tag{53}$$

In the same way, we may extend (53) to

$$n \mid \left(\sum_i b_{ij} - l b_{uj} \right) \qquad (u = 1, \cdots, l-1); \tag{54}$$

or, making use of (50),

$$n \mid l b_{ij} \qquad (i,j = 1, \cdots, l-1); \tag{55}$$

that is, $n \mid l \cdot (b_{11}, b_{12}, \cdots, b_{l-1,l-1})$.

Put $\sigma = (b_{11}, b_{12}, \cdots, b_{l-1,l-1})$, and assume

$$(n,\sigma) = \tau > 1.$$

Then (47) may be written

$$\sum b_i E_i = \tau \log | B_1 | ,$$

or

$$\epsilon = B_1^{\tau}, \quad \epsilon = \epsilon_1^{b_1} \cdots \epsilon_{l-2}^{b_{l-2}}.$$

By one of the conditions in (47), $(\tau, b_1, \cdots, b_{l-2})=1$, so that ϵ is not the τth power of a unit in k_a. It remains to show that $\epsilon=B_1^\tau$ is impossible for any B_1 of K. Since k_a is a maximal proper subfield of K, τ must be a multiple of l. Hence we need only consider the possibility of

$$\epsilon = B_1{}^l.$$

But as K does not (under our assumptions) contain the lth roots of unity, this equality cannot hold.

We see then that τ is unity, and therefore

$$n \mid l. \tag{56}$$

Taking this in conjunction with (47), we see that our assertion on the ratio of R_0 to $R(K)$ is proved.

It is natural to enquire as to the number of independent relations like (47) actually existing in a field K. An exact answer apparently entails great difficulties; however it is easy to determine the maximum number of such relations. Making use of (50), this number is seen to be $(l-1)$ $(l-2)$. Therefore, we have at once

$$\frac{R_0}{R(K)} \Bigg| \, l^{(l-2)(l-1)}.$$

(46) may then be written

$$l^\lambda R(K) = l^{(l+1)(l-2)/2} R(k_a) R^{l-1}(k_l) \qquad (0 \leqq \lambda \leqq (l-1)(l-2)). \tag{57}$$

If (57) be compared with (36), we obtain the following class-number relationship $(a=l-1)$:

$$h(K) = l^{(l+1)(l-2)/2-\lambda} h(k_a) h^{l-1}(k_l). \tag{58}$$

It is of course rather obvious that the methods of this section may be applied to the other types of fields considered above. It does not however seem possible (using only these methods) to go as far as (57). On the other hand, Pollaczek, in the paper referred to above, obtains interesting results in the Abelian case (§5).

University of Pennsylvania,
Philadelphia, Pa.