# NORMAL ALGEBRAIC NUMBER FIELDS

BY

SAUNDERS MAC LANE AND O. F. G. SCHILLING

**Introduction.** In this paper we present a detailed account of the results recently published in the Proceedings of the National Academy of Sciences [29](1). Our theory is an attempt to generalize the results of the classical class field theory to arbitrary normal fields. In the last analysis, the theory of cyclic extensions $Z$ of an algebraic number field $k$ can be described in terms of cyclic algebras $(Z/k, \lambda, a)$ and collections of local algebras $(Z_P/k_p, \delta, a_p)$, for all prime divisors $p$ of the base field. As a matter of fact, Chevalley's new approach [11] to the classical theory by means of ideal elements may be viewed in the light of our assertion (§8). It is a well-known fact that for arbitrary normal fields $K/k$ with the Galois group $\Gamma$, the crossed products $(K/k, \Gamma, F)$, where $F$ denotes a factor set for $\Gamma$ in $K$, are the strict analogues of the cyclic algebras. We use this feature of normal fields and their associated algebras to extend the classical (cyclic) theory. In this generalization ideal elements are replaced by "ideal algebras," where an ideal algebra is a collection of local algebras, one for each $p$-adic extension $K_P/k_p$ (§4).

It might be conjectured from this approach that most of the results of the classical theory may easily be generalized, but this is not the case(2). Entirely new problems, mostly group-theoretical ones, block the path which has been envisaged by various statements of E. Noether [32, 33] on noncommutative methods. One of our final theorems may suffice to illustrate the rather unexpected results of this paper. Our new "class group" of ideal algebras can be represented as $F\mathfrak{A}'/(F'')T\mathfrak{A}'$, where $F\mathfrak{A}'$ denotes the group of factor sets of ideals relatively prime to the different of $K/k$, where $T\mathfrak{A}'$ is the group of transformation sets of such ideals, and where $(F'')$ are principal ideals generated by "norm residues" (§26). For an abelian (non-cyclic) field this class group is not isomorphic to the Galois group, as in the ordinary theory; it is rather a cyclic group whose order is equal to the least common multiple of the orders of the elements in the Galois group. In other words, for arbitrary abelian fields our theory does not give the classical law of reciprocity. Only a composition which is extraneous to the theory of factor sets yields the usual theory for general abelian extensions.

In the first part of this paper we follow an unpublished investigation of E. Artin (§5). It deals with the theory of $p$-primary factor sets, that is, factor sets whose elements involve only the divisors of a fixed prime divisor $p$ of $k$.

---

Presented to the Society, April 27, 1940; received by the editors August 5, 1940.

(1) The numbers in square brackets refer to the papers in the bibliography.

(2) The first attempts in this direction are due to Tannaka [38].

The results culminate in the following theorem: The least common multiple $J$ of the orders of the elements in $\Gamma$ is equal to the index $[F\mathfrak{A}' : (F'')T\mathfrak{A}']$. The proof of this theorem is obtained by collecting the results on $p$-primary factor sets by means of the Tschebotareff density theorem (§§6, 7).

The final chapter of this paper treats of the realization of the above mentioned index relation by a generalized Artin symbol (§29). It is not difficult to generalize the theory of the norm residue symbol (§28). All the formal properties of the old symbol hold true for the new one, except for the usual statements on the values taken by the norm residue symbol for variable argument. The real reason for this discrepancy may be sought in our results on the relation between local algebras and algebras in the large. It is found that in general not every local algebra for $K_P/k_p$ is the $p$-component of a suitable crossed product in the large (§§13–16).

The main part of the group-theoretic investigation of the class group is centered around a series of theorems on unit groups (§§17–23). As in the proof of the classical inversion theorem we try to treat the fundamental index $[F\mathfrak{A}' : (F'')T\mathfrak{A}']$ by means of arithmetical reductions of a group-theoretic nature. The class numbers, which are easily canceled off in the old proof, confront us here with a rather involved situation. By means of a group-theoretic invariant, the deficiency index, we finally succeed in disposing of them (§§15, 16). This deficiency index together with the theory of group extensions over unit groups give rise to new invariants for the field $K/k$. The customary reduction to the Herbrand subgroup can be carried out to a certain extent. However, we find a totally unexpected deviation from the classical case. The principal genus theorem for units and unit groups connects our investigations with Schur's theory of the multiplicator, as was pointed out to us by A. H. Clifford. The group generated by one of the Herbrand units $H$ belonging to an unramified infinite prime divisor can be described in purely group-theoretic terms. If $\Gamma$ is abelian, the number of group extensions by $\Gamma$ of such an "abstract unit group" turns out to be exactly the order of the multiplicator of $\Gamma$ in an algebraically closed field (of characteristic $\infty$). We wish to emphasize that many of the arithmetic properties of $K/k$ are of strictly group-theoretic nature and can be formulated as such. There are a large number of new problems in group theory which originate in our analysis of normal fields(3). Finally, comparison of the two evaluations for the fundamental index leads to a very complicated relation between the invariants we introduced in the course of our investigation (§25). We discuss this rather mysterious equality in a number of special cases which indicate the relative contributions of the partial indices of $[F\mathfrak{A}' : (F'')T\mathfrak{A}']$. In conclusion we may say that we have explored the potentialities of the concept of factor sets and algebras for arbitrary normal fields.

(3) The statement of these problems in §§17, 21–23 may be read without detailed reference to the remaining sections.

## CHAPTER I. FACTOR SETS AND ALGEBRAS

1. **Preliminaries on factor sets.** Let $G$ be a group with an abelian normal subgroup $N$ and a corresponding factor group $\Gamma = G/N$. In each coset $\sigma$ of $G/N$ choose a representative $u_\sigma$, so that the coset $\sigma$ is $Nu_\sigma$. This element $u_\sigma$ induces in $N$ an automorphism

$$A \leftrightarrow A^\sigma = u_\sigma A u_\sigma^{-1} \qquad (A \text{ in } N). \tag{1}$$

Since $N$ is abelian, any other element $v_\sigma$ in the coset $Nu_\sigma$ will induce the same automorphism $A \leftrightarrow A^\sigma$. For $\sigma$ and $\tau$ in $\Gamma$, $(A^\tau)^\sigma = A^{\sigma\tau}$ (note the order!).

Conversely, let an abelian group $N$ and a group $\Gamma$ be given, and let each element $\sigma$ of $\Gamma$ be assigned to a definite automorphism $A \leftrightarrow A^\sigma$ of $N$. We assume that this assignment preserves the products, so that

$$A^{\sigma\tau} = (A^\tau)^\sigma \qquad (\text{all } \sigma, \tau \text{ in } \Gamma). \tag{2}$$

A *group extension* of $N$ by $\Gamma$, with the given assignment of automorphisms, is then any group $G$ with $N$ as normal subgroup, and $\Gamma = G/N$ as quotient group, in which each coset $\sigma$ of $\Gamma$ induces in $N$ the given automorphism[4] $A \leftrightarrow A^\sigma$.

To represent a group extension explicitly, use a fixed representative $u_\sigma$ in each coset $\sigma$ of $G/N$. The product of two representatives $u_\sigma$ and $u_\tau$ is in the coset of $\sigma\tau$, hence

$$u_\sigma u_\tau = F_{\sigma,\tau} u_{\sigma\tau} \qquad (\text{each } F_{\sigma,\tau} \text{ in } N). \tag{3}$$

The associative law $u_\sigma(u_\tau u_\rho) = (u_\sigma u_\tau)u_\rho$ implies that these constants $F_{\sigma,\tau}$ satisfy the *associativity conditions*

$$F_{\sigma,\tau} F_{\sigma\tau,\rho} = F_{\tau,\rho}^\sigma F_{\sigma,\tau\rho} \qquad (\text{all } \sigma, \tau, \rho \text{ in } \Gamma). \tag{4}$$

The equations (1), (3), and (4) determine the group extension $G$ in terms of the subgroup $N$, quotient group $\Gamma$, and constants $F_{\sigma,\tau}$. Any set $F$ of constants $F_{\sigma,\tau}$ in $N$ which satisfy the associativity conditions (4) is called a *factor set*. Every factor set for $\Gamma$ in $N$ determines a group extension $G$ which consists of elements $Au_\sigma$, for $A$ in $N$, $\sigma$ in $\Gamma$, which are to be multiplied by the rules (1) and (3), or

$$u_\sigma u_\tau = F_{\sigma,\tau} u_{\sigma\tau}, \qquad u_\sigma A = A^\sigma u_\sigma. \tag{5}$$

The *product* of two factor sets $F$ and $F'$ is a third factor set with components $F''_{\sigma,\tau} = F'_{\sigma,\tau} F_{\sigma,\tau}$, for this set $F''$ clearly satisfies (4). All factors sets $F$ form a group which we denote by $F_\Gamma N$, or simply by[5] $FN$.

[4] See discussion in Baer [6, 7]; Zassenhaus [43].

[5] We shall adopt this abbreviation if there is no ambiguity about the group $\Gamma$. Here and subsequently, starred definitions are given special numbers. They introduce notation important for later arguments.

(*1.1) $F_\Gamma N$ = the group of all factor sets $F$ with components $F_{\sigma,\tau}$ in $N$.

In a group extension the representatives $u_\sigma$ of the cosets may be replaced by new representatives $v_\sigma = N_\sigma u_\sigma$, with $N_\sigma$ in $N$. This replaces the factor set $F$ by a new set $F'$, given by $F'_{\sigma,\tau} = F_{\sigma,\tau}(N_\sigma N_\tau^\sigma N_{\sigma\tau}^{-1})$. These two factor sets $F$ and $F'$ are called *similar* (notation $F \sim F'$), so

(*1.2) $F \sim F'$ means $F'_{\sigma,\tau} = F_{\sigma,\tau}(N_\sigma N_\tau^\sigma N_{\sigma\tau}^{-1})$,

with suitable elements $N_\sigma$ of $N$. Two factor sets determine isomorphic group extensions (with $N$ and $\Gamma$ fixed) if and only if they are similar.

The added factors $N_\sigma N_\tau^\sigma N_{\sigma\tau}^{-1}$ of (*1.2) themselves form a special sort of factor set known as a *transformation set*. We write

(*1.3) $TN = TN_\sigma$ for a transformation set $N_\sigma N_\tau^\sigma N_{\sigma\tau}^{-1}$, $N_\sigma$ in $N$.

If $\Gamma$ is finite, each such set is derived from a vector

(*1.4) $N_\sigma = \{N_{\sigma_1}, N_{\sigma_2}, \cdots, N_{\sigma_n}\}$,

where each $N_{\sigma_i}$ is in $N$ and the subscripts $\sigma_i$ denote the $n$ distinct elements of $\Gamma$. The symbol $N_\sigma$ denotes ambiguously the whole vector or just one component.

LEMMA 1.1. *If $\Gamma$ has order $n$, the nth power $F^n$ of any factor set $F$ in $F_\Gamma N$ is a transformation set $TN$.*

**Proof**([6]). From the given factor set $F$ construct the products

$$C_\sigma = \prod_\tau F_{\sigma,\tau} \qquad \text{(over all } \tau \text{ in } \Gamma\text{)}. \tag{6}$$

The associativity relations (4), multiplied together over all $\rho$ in $\Gamma$, become

$$F_{\sigma,\tau}^n C_{\sigma\tau} = C_\tau^\sigma C_\sigma. \tag{7}$$

This states that $F^n$ is the transformation set $TC_\sigma$.

2. **Crossed products.** For the basic normal field $K$ of our investigation, we use throughout the following notation:

(*2.1) $K$, a fixed normal extension of an algebraic number field $k$,
(*2.2) $n = [K:k]$, the degree of $K$ over $k$,
(*2.3) $A$, a nonzero number of $K$, or ([7]) the group of all such numbers,
(*2.4) $\sigma$, $\tau$, $\rho$, automorphisms $A \leftrightarrow A^\sigma$ of $K/k$,
(*2.5) $\Gamma$, the Galois group of $K/k$, composed of all $\sigma$,
(*2.6) $F = F_\Gamma A$, a factor set of numbers $F_{\sigma,\tau}$ in $A$,
(*2.7) $(S)$, a class of normal simple algebras split by $K$ over $k$.

([6]) This proof is apparently originally due to Artin.

([7]) As in Hasse's group-stenographic method, a letter may denote ambiguously a group or an arbitrary element of that group.

In connection with this last definition, we recall the properties of algebra classes. Every normal simple algebra $B$ over $k$ has the form of a direct product $B=M\times D$, where $D$ is a division algebra, $M$ a total matric algebra. Two such algebras $B_1=M_1\times D_1$ and $B_2=M_2\times D_2$ are *similar* if and only if $D_1$ is equivalent to $D_2$ over $k$. The set of all algebras similar to $B$ is termed an algebra class $(B)$. The field $K$ is said to *split* an algebra $B$ over $k$ if the algebra $B_K$ formed by extending the coefficient field of $B$ to $K$ is a total matric algebra. If $K$ splits $B$, it splits every algebra of the class $B$. The direct *product* of two classes of algebras, taken term-by-term, is a third class $(B_1)\times(B_2)=(B_1\times B_2)$. If both $B_1$ and $B_2$ are split by $K$, so is their product. Therefore the algebra classes $(S)$ of (*2.7) form a group.

Every factor set $F$ in $K$ determines an algebra called a *crossed product* of $K$ by $F$. It consists of all sums $\sum_\sigma B_\sigma u_\sigma$ formed, with coefficients $B_\sigma$ in $K$, from $n$ linearly independent elements $u_\sigma$, one for each $\sigma$ in $\Gamma$. These sums are to be added term-by-term and multiplied by the distributive law and the rules (5) of §1 for multiplying the elements $u_\sigma$ in a group extension. With this convention, the sums $\sum_\sigma B_\sigma u_\sigma$ constitute a normal simple algebra $(K, \Gamma, F)=(K/k, \Gamma, F)$. It has order $n^2$ over $k$ and contains $K$ as a subfield. Conversely([8]), every normal simple algebra $S$ over $k$ of order $n^2$ with the subfield $K$ has a crossed product representation $(K, \Gamma, F)$ for some factor set $F$. Consequently every algebra class $(S)$ split by $K$ contains a crossed product $S=(K, \Gamma, F)$. Two crossed products belong to the same algebra class if and only if their factor sets are similar. The direct product of two crossed products ([2, pp. 67–73]) is given by the product of the factor sets,

$$(1)\qquad (K/k, \Gamma, F)\times(K/k, \Gamma, F')\sim(K/k, \Gamma, FF').$$

Hence the correspondence $F\rightarrow(K, \Gamma, F)$ maps the group $F$ of factor sets homomorphically on the group $(S)$ of algebra classes split by $K$.

The explicit theory of the algebras $S$ depends on the *valuations* of the base field $k$: the non-negative real-valued functions $\|a\|$ defined on $k$ with $\|ab\|=\|a\|\|b\|$, $\|a+b\|\leqq\|a\|+\|b\|$, $\|a\|=0$ if and only if $a=0$. Two valuations are equivalent if the convergent sequences which they determine are the same; they then determine the same minimal field $k_p\supset k$ *complete* in the convergent sequence topology. By a *prime divisor* (or prime spot) $p$ of $k$ we mean a class of equivalent valuations([9]) of $k$, so

(*2.8) $k_p=$the minimal complete field $k_p\supset k$ in the valuation at $p$.

There are two types of prime divisors. If $a\leftrightarrow a_i$ is an isomorphic mapping of $k$ on the field of complex numbers, so that $a_i$ is a conjugate of $a$, then the

([8]) See [2, chap. 5], or the parallel discussion in [13, chap. 5]. In our formula (3) of §1 the coefficients $F_{\sigma,\tau}$ appear on the left; in [2] and [13] the corresponding symbols are to the right of $u_\sigma$. This causes slight changes in the form of the associativity relations, etc.

([9]) Discussion in [1, pp. 251–305], [13, pp. 93–105], [42, 2d edition, vol. 1].

ordinary absolute value of $a_i$ gives a valuation $\|a\| = |a_i|$ of $k$. The corresponding prime divisor is called an *infinite* prime divisor $p = p_\infty$, and the associated complete field $k_p$ is either the field of complex numbers or that of real numbers (the latter if the conjugates $a_i$ of all $a$ are real). If $p$ is a prime ideal of the number field $k$, there is a valuation function $\|a\|_p = \exp[-V_p(a)]$, where

(*2.9) $V_p(a)$ = the exact power to which $p$ divides the ideal $(a)$.

The corresponding prime divisor $p$ is said to be *finite*, and the complete field $k_p$ $p$-adic. Every prime divisor of $k$ is either finite or infinite in this sense.

Each prime divisor $P$ of the extended field $K$ determines a valuation and hence a prime divisor $p$ of the subfield $k$; call $P$ a *divisor* of $p$. Every $p$ has at least one divisor $P$; the corresponding complete field $K_P$ may be considered as an extension of the original complete field $k_p$. This *local extension* $K_P/k_p$ is normal, and its Galois group $\Delta(P)$ is a subgroup of the original Galois group $\Gamma$ of $K/k$. If $P$ is finite and belongs to a prime ideal $P$, then $\Delta(P)$ is the Hilbert *decomposition group* of this $P$, so

(*2.10) $\Delta(P)$ = all $\delta$ in the Galois group $\Gamma$ with $P^\delta = P$.

Conjugate prime ideals $P$ have conjugate groups $\Delta(P)$, so the order of $\Delta(P)$ depends only on the original $p$,

(*2.11) $m_p = [K_P : k_p] = [\Delta(P) : 1]$.

If $P$ is infinite, $K_P$ is either the real or the complex field. If $K_P = k_p$, $\Delta(P) = 1$, and $P \mid p$ is said to be *unramified*. If $K_P$ is complex, $k_p$ real, $\Delta(P)$ is cyclic of order 2 with a generator $\delta = \delta_P$ and $P \mid p$ is *ramified*.

Consider the corresponding local algebras for any $p$,

(*2.12) $S_p$ = a normal simple algebra of degree $m$ over $k_p$, split by $K_P/k_p$.

A normal simple algebra of degree $m$ over $k_p$ contains an isomorphic map of every possible extension of degree $m$ over $k_p$ (see [9, Lemma 0]), hence $S_p$ contains an unramified cyclic extension $W$ of degree $m = m_p$. Therefore $S_p$ has a cyclic representation $(W/k_p, \sigma, a)$ where $\sigma$ generates the cyclic group of $W/k_p$, while $a$ is an element of $k_p$.

The symbol $(W/k_p, \sigma, a)$ represents the *cyclic algebra* which has over $W$ a basis of $m$ linearly independent elements $1, u_\sigma, u_\sigma^2, \cdots, u_\sigma^{m-1}$, connected by the multiplication table

$$u_\sigma A = A^\sigma u_\sigma, \qquad u_\sigma^m = a; \qquad m = [W : k_p]. \tag{2}$$

For such an algebra one may determine an integer which is invariant (independent of the particular cyclic representation) by the formula[10]

[10] In [22], Hasse uses as invariant the quantity $\rho_p = (1/n)\mu_p$, modulo 1, which is independent of our fixed degree $n$.

$$\mu(S_p) = \mu(W/k_p, \sigma, a) \equiv (n/m_p)V_p(a) \pmod{n}. \tag{3}$$

Two normal simple algebras over $k_p$ are similar if and only if they have the same invariant $\mu$ modulo $n$.

Another invariant is the index $i_p$ of $S_p/k_p$, defined as the degree of the division algebra (unique up to isomorphism) which is similar to $S_p$. This index is known [21, 22] to be the reduced denominator of $\mu_p/n$; that is, it is the smallest integer $i_p$ such that

$$i_p\mu_p \equiv 0 \pmod{n}, \qquad i_p = \text{the index of the algebra } S_p. \tag{4}$$

For an infinite prime divisor $p$, $k_p$ is either the real or complex field, and the only proper normal division algebra over $k_p$ the algebra of real quaternions $Q$. The invariant of a normal simple algebra $S_p/k_p$ may then be defined by

$$\begin{aligned} \mu(S_p) &= 0 \qquad \text{if } S_p \text{ is a total matric algebra,} \\ \mu(S_p) &= n/2 \qquad \text{if } S_p \text{ is similar to } Q. \end{aligned} \tag{5}$$

For the direct product $S_p^{(1)} \times S_p^{(2)}$ of two algebras over $k_p$ ($p$ finite or infinite) one always has the formulas

$$\mu(S_p^{(1)} \times S_p^{(2)}) \equiv \mu(S_p^{(1)}) + \mu(S_p^{(2)}) \pmod{n}. \tag{6}$$

An algebra $S$ over $k$ has for each prime divisor $p$ of $k$ a local component $(S)_p = S_p = S \times k_p$, obtained by extending the coefficient field to the complete field $k_p$. This algebra $S_p$ is normal simple over $k_p$. Hence $S$ has a set of invariants $\mu_p(S) = \mu(S_p)$, one for each $p$. Conversely, it is known that $S$ is determined up to similarity by the set of its invariants [2, 21, 22]. If $S_p$ is a total matric algebra, $S_p \sim k_p$, then $S$ is said to be unramified at $p$, otherwise ramified. It is known that $S$ is ramified at only a finite number of prime divisors ([2, pp. 148–149]).

For a crossed product the local algebras can be explicitly represented ([21, 22]) as

$$S_p = (K/k, \Gamma, F)_p \sim (K_P/k_p, \Delta(P), F \cap \Delta) \tag{7}$$

where $F \cap \Delta$ denotes the part of the factor set $F$ applying to the group $\Delta(P) = \Delta$; that is, $F \cap \Delta$ is the factor set with terms $F_{\zeta,\eta}$ for $\zeta$, $\eta$ in $\Delta$. Here $\Delta$ may be the decomposition group for any one of the prime divisors $P$ of $p$. If $P$ is finite and $P \mid p$ unramified, the invariant $\mu_p$ may be explicitly calculated from the factor set $F$. For, under these circumstances the local extension $K_P/k_p$ is cyclic, and its group $\Delta$ has as generator

(*2.13) $\delta = \delta_P =$ the Frobenius automorphism $[(K/k)/P]$ which is characterized by the property([11])

([11]) See [20, Part Ia, p. 71]; [23, pp. 36, 38].

(8) $$A^{\delta} \equiv A^{Np} \pmod{P},\ Np = \text{absolute norm of } p,\ V_P(A) \geqq 0.$$

Because $K_P/k_p$ is cyclic, the crossed product $(K_P/k_p, \Delta(P), F \cap \Delta)$ can be written as a cyclic algebra $(K_P/k_p, \delta_P, a)$, while the generator $u_\delta$ for this algebra may be chosen as the corresponding basis element $u_\delta$ of the given crossed product. By (2) the multiplication constant $a$ is then $u_\delta^m$, where $m$ is the $p$-degree $m = m_p$ of (*2.11). However

$$a = u_\delta^m = (u_\delta u_\delta)u_\delta^{m-2} = F_{\delta,\delta}(u_{\delta^2}u_\delta)u_\delta^{m-3} = \cdots = F_{\delta,\delta}F_{\delta^2,\delta}\cdots F_{\delta^{m-1},\delta}u_{\delta^m}.$$

But $u_{\delta^m} = u_1$, and $u_1 u_\delta = F_{1,\delta}u_\delta$, so $u_1 = F_{1,\delta}$. Consequently

(9) $$a = F_{1,\delta}F_{\delta,\delta}\cdots F_{\delta^{m-1},\delta} = \prod_{i=0}^{m-1} F_{\delta^i,\delta} \qquad (\delta = \delta_P).$$

According to the definition (3) of the invariant $\mu_p$, we have

(10) $$\mu_p(K, \Gamma, F) = (n/m)V_P\left[\prod_{i=0}^{m-1} F_{\delta^i,\delta}\right],$$

where $\delta = \delta_P$ is the Frobenius-Artin automorphism of order $m = m_p$.

3. **The module** $M$. As in the cyclic case, one must restrict the numbers under consideration to those relatively prime to some divisor

(1) $$M = P_1^{h_1}P_2^{h_2}\cdots P_s^{h_s},$$

where each $P_i$ denotes a finite or infinite prime divisor of $K$, while the $h_i$ are positive integers. The requirement "$A$ relatively prime to $M$" means that $A$ is relatively prime to each factor $P_i^{h_i}$ in $M$. If $P_i$ is a finite prime divisor, this statement has its customary meaning, while "$A$ is relatively prime to an infinite $P$" means simply "$A \neq 0$." It is convenient to say that a prime divisor $p$ of $k$ is *involved* in $M$ if some factor $P$ of $p$ is present in $M$ (with a positive exponent).

For $M$ in the subsequent developments we use any module which satisfies the conditions

(i) any $p$ ramified in $K/k$ is involved in $M$,
(ii) if $p$ is involved in $M$, every $P \mid p$ is present in $M$.

For example, $M$ might be the product of all $P$'s ramified in $K/k$. Alternatively, $M$ might be the factor-set conductor of $K/k$ which is defined in §26.

A prime "$'$" will be used to denote elements or groups of elements relatively prime to the module $M$.

(*3.1) $A'$ = the group of numbers $A \neq 0$ of $K$ relatively prime to $M$.

(*3.2) $F'$ = the group of all factor sets of numbers $F_{\sigma,\tau}$ relatively prime to $M$.

(*3.3) $S'=S'(K)=$the group of all normal simple algebras $S$ relatively prime to $M$.

Here we call an algebra $S$ "relatively prime to $M$" if none of the ramification divisors of $S$ are involved in $M$; that is, if $p$ involved in $M$ implies $S\times k_p\sim 1$ ([12]).

4. **Ideal algebras.** By an *ideal algebra* $\mathfrak{S}$ over the field $k$ we simply mean a specification of normal simple algebras $S_p$ over $k_p$, one for each prime divisor $p$ of $k$, such that $S_p\sim k_p$ except for a finite number of prime divisors. The algebra $S_p$ is the *component* $(\mathfrak{S})_p=\mathfrak{S}_p$ of $\mathfrak{S}$. We agree to call two such ideal algebras $\mathfrak{S}_1$ and $\mathfrak{S}_2$ equal if and only if their components $(\mathfrak{S}_1)_p\sim(\mathfrak{S}_2)_p$ are similar for every $p$. For each such $p$ we have the corresponding $p$-index $i_p(\mathfrak{S})=i(S_p)$ of the local algebra $S_p$. We say that $\mathfrak{S}$ is *split* by the given extension $K/k$ if, for each $p$, $i_p(\mathfrak{S})$ is a divisor of the $p$-degree $m_p$ of $K/k$. In case $\mathfrak{S}$ has the components $\mathfrak{S}_p=S_p$ of an actual algebra $S$, this condition is simply the usual condition that the algebra $S$ be split by $K$ [21, 22, 2]. Ideal algebras form an abelian group under the operation of the direct product

$$(\mathfrak{S}_1\times\mathfrak{S}_2)_p=S_{1p}\times S_{2p}. \tag{1}$$

Under this operation the set of all ideal algebras split by $K$ constitutes a subgroup

(*4.1) $\mathfrak{S}(K)=\mathfrak{S}=$the group of all $\mathfrak{S}$'s split by $K$,

(*4.2) $\mathfrak{S}'(K)=\mathfrak{S}'=$the group of all $\mathfrak{S}$'s relatively prime to $M$ and split by $K$.

Again, $\mathfrak{S}$ relatively prime to $M$ means $S_p\sim k_p$ for all $p$ involved in $M$. The group $S(K)=S$ of actual algebras forms, in natural fashion, a subgroup of $\mathfrak{S}$. We propose to compute the index

(*4.3) $J=[\mathfrak{S}':S']$.

An ideal algebra $\mathfrak{S}$ is determined uniquely by giving the set of its local invariants $\mu_p=\mu_p(\mathfrak{S})=\mu(S_p)$, for each prime divisor $p$. Thus an ideal algebra $\mathfrak{S}$ split by $K$ is completely specified by a list of integers $\mu_p$ subject to the conditions

$$m_p\mu_p\equiv 0 \pmod{n} \qquad \text{for all } p, \tag{2}$$

$$\mu_p\equiv 0 \pmod{n} \qquad \text{for all but a finite number of prime divisors } p. \tag{3}$$

THEOREM 4.1. *The index $J$ defined in* (*4.3) *is $J(\Gamma)$, the least common multiple of the orders of the elements of the Galois group $\Gamma$.*

**Proof.** The only relation between the invariants of a crossed product is $[2, 13, 22]\sum_p\rho_p(S)\equiv 0 \pmod 1$. In terms of the invariants $\mu_p$, this becomes

([12]) Remember that $(K/k, \Gamma, F')_p\sim 1$ need not hold for $p$ involved in $M$.

$\sum_p \mu_p(S) \equiv 0 \pmod{n}$. For a given ideal algebra the quantity

$$d(\mathfrak{S}) \equiv \sum_p \mu_p(\mathfrak{S}) \pmod{n} \tag{4}$$

measures the divergence of $\mathfrak{S}$ from "actuality." More explicitly, the map $\mathfrak{S} \to d(\mathfrak{S})$ carries the group $\mathfrak{S}$ homomorphically (see §2, (6)) into an additive group of integers $d$ mod $n$, in such a fashion that the subgroup carried into 0 mod $n$ is the group of actual algebras. By the restriction (2), each $d(\mathfrak{S}')$ satisfies the condition $J(\Gamma)d(\mathfrak{S}') \equiv 0 \pmod{n}$. Therefore $\mathfrak{S} \to d(\mathfrak{S})$ maps the quotient group $\mathfrak{S}'/S'$ isomorphically on the cyclic group of integers of order $J(\Gamma)$, generated by $n/J(\Gamma) \pmod{n}$, provided there exists an ideal algebra $\mathfrak{S}'$ with $d(\mathfrak{S}') = n/J(\Gamma)$. It remains to construct this $\mathfrak{S}$. Recall that $J(\Gamma)$ is the least common multiple of the orders $O_1, \cdots, O_t$ of certain elements $\sigma_1, \cdots, \sigma_t$ of the Galois group. By partial fractions, we may express $1/J(\Gamma)$ as

$$1/J(\Gamma) = a_1/O_1 + \cdots + a_t/O_t \qquad (a_i \text{ integers}).$$

The Tschebotareff density theorem (see [20, Part II, §24]) asserts that for a given $\sigma_i$ there are (infinitely many) sets of distinct prime divisors $p_i$ of $k$ with factors $P_i$ in $K$ such that the Frobenius automorphism of $P_i$ is $\sigma_i$. One may assume each $p_i$ to be relatively prime to $M$. By definition, the Frobenius automorphism generates the decomposition group $\Delta(P_i)$, so that the order $m_i$ of this group is the given order $O_i$ of $\sigma_i$. There is thus an ideal algebra $\mathfrak{S}$ relatively prime to $M$ and split by $K$, with invariants

$$\mu_{p_i} \equiv n a_i/O_i \pmod{n}, \qquad i = 1, 2, \cdots, t,$$
$$\mu_q \equiv 0 \pmod{n}, \qquad (q \neq p_1, p_2, \cdots, p_t).$$

For this algebra $\mathfrak{S}$ we get $d(\mathfrak{S}) = n/J(\Gamma)$, as desired for Theorem 4.1.

In this proof we may drop the requirement that the ideal algebras $\mathfrak{S}$ be relatively prime to $M$. The result is analogous.

THEOREM 4.2. *The index* $[\mathfrak{S}:S]$ *of the group of actual algebras in the group of ideal algebras split by* $K$ *equals* $J_0(\Gamma)$, *the least common multiple of the orders* $m_p$ *of the decomposition groups of the primes* $p$ *in* $K/k$.

5. **Artin's character method.** An ideal algebra can be given by a factor set of ideals in $K$, as we now show by computing the "*invariants*" $\mu_p$ of such a factor set. We use the following notation, in which each letter may also denote the group of all objects so labelled, while a prime "′" will denote the restriction "relatively prime to $M$":

(*5.1) $\mathfrak{A}$ = an ideal of $K$ (possibly a fractional ideal),
(*5.2) $\mathfrak{A}_\sigma$ = a vector of $n$ ideals, one for each $\sigma$ in $\Gamma$,
(*5.3) $T\mathfrak{A}$ = a transformation set $\mathfrak{A}_\sigma \mathfrak{A}_\tau^{\sigma} \mathfrak{A}_{\sigma\tau}^{-1}$ derived from $\mathfrak{A}_\sigma$,
(*5.4) $\mathfrak{F}$ = a factor set $\mathfrak{F}_{\sigma,\tau}$ of ideals of $K$, with $\sigma$, $\tau$ in $\Gamma$.

For each such set we introduce a function $h_P(\sigma)$, determined by $\sigma$ in $\Gamma$ and a prime divisor $P$ of $K$,

(*5.5) $h_P(\sigma)=h_P(\sigma, \mathfrak{F})\equiv\sum_\tau V_P(\mathfrak{F}_{\sigma,\tau}) \pmod n$,

where $V_P$ is the $P$-adic valuation (see (*2.9)). If $P$ is unramified in $K/k$, we propose as an invariant of $\mathfrak{F}$ the integer

(*5.6) $\mu_P=\mu_P(\mathfrak{F})\equiv h_P(\delta, \mathfrak{F}) \pmod n$,

where $\delta=\delta_P$ is the Frobenius automorphism (see (*2.13)).

If $p$ is the prime ideal of $k$ divisible by $P$, each ideal in a factor set $\mathfrak{F}$ may be factored as

$$\mathfrak{F}_{\sigma,\tau} = \mathfrak{F}^{(p)}_{\sigma,\tau}\cdot\mathfrak{B}_{\sigma,\tau}, \qquad (\mathfrak{B}_{\sigma,\tau}, p) = 1 \tag{1}$$

where the first factor $\mathfrak{F}^{(p)}_{\sigma,\tau}$ involves only the prime factors $P_1, P_2, \cdots$ of $p$. These ideals $\mathfrak{F}^{(p)}_{\sigma,\tau}$ constitute by themselves a factor set which is $p$-primary in the sense of the

DEFINITION. *An ideal factor set $\mathfrak{F}$ is called $p$-primary if all prime ideal factors of any ideal $\mathfrak{F}_{\sigma,\tau}$ of the set are prime ideal factors $P$ of the given $p$.*

The factor set $\mathfrak{F}$ and its $p$-primary component $\mathfrak{F}^{(p)}$ clearly determine the same function $h_p(\sigma)$[13].

LEMMA 1. *For factor sets of ideals $\mathfrak{F}_1$ and $\mathfrak{F}_2$, $\mathfrak{F}_1\sim\mathfrak{F}_2$ implies $h_P(\delta, \mathfrak{F}_1)\equiv h_P(\delta, \mathfrak{F}_2) \pmod n$ for all $\delta$ in $\Delta(P)$.*

**Proof.** Multiplication of factor sets is represented by addition of the corresponding functions $h$, for the definition shows that

$$h_P(\sigma, \mathfrak{F}_1\mathfrak{F}_2) \equiv h_P(\sigma, \mathfrak{F}_1) + h_P(\sigma, \mathfrak{F}_2) \pmod n. \tag{2}$$

But $\mathfrak{F}_1\sim\mathfrak{F}_2$ means that $\mathfrak{F}_1=\mathfrak{F}_2\mathfrak{F}$, where $\mathfrak{F}$ is a transformation set. Hence we need only prove $h_P(\delta, \mathfrak{F})\equiv 0 \pmod n$, whenever $\mathfrak{F}$ is a transformation set $T\mathfrak{A}$. But

$$\prod_\tau [\mathfrak{A}_\sigma\mathfrak{A}_\tau^\sigma\mathfrak{A}_{\sigma\tau}^{-1}] = \mathfrak{A}_\sigma^n\Big(\prod_\tau \mathfrak{A}_\tau\Big)^\sigma\cdot\Big(\prod_{\tau'}\mathfrak{A}_{\tau'}\Big)^{-1} = \mathfrak{A}_\sigma^n\Big(\prod_\tau \mathfrak{A}_\tau\Big)^{\sigma-1}. \tag{3}$$

For $\sigma$ in $\Delta(P)$, $V_P(\prod_\tau\mathfrak{A}_\tau)=V_P(\prod_\tau\mathfrak{A}_\tau)^\sigma$, since $\sigma$ leaves $P$ fixed. Hence

$$h_P(\delta, \mathfrak{A}_\sigma\mathfrak{A}_\tau^\sigma\mathfrak{A}_{\sigma\tau}^{-1}) = nV_P(\mathfrak{A}_\sigma) \equiv 0 \pmod n.$$

---

[13] The function $h$ and its properties are due to unpublished work of E. Artin. The method used will apply to factor sets $\mathfrak{F}$ in any $F_\Gamma(\mathfrak{A})$ for which the abstract group $\mathfrak{A}$ with operators has a suitable structure (generated by free generators $P, Q, \cdots$, suitably permuted by $\Gamma$); see the statement of Theorem 5 in [17].

LEMMA 2. *The function h corresponding to any factor set* $\mathfrak{F}$ *is a character of* $\Delta(P)$ mod $n$; *which is to say that*

$$h_P(\zeta) + h_P(\eta) \equiv h_P(\zeta\eta) \pmod{n} \qquad (\zeta, \eta \text{ in } \Delta(P)). \tag{4}$$

**Proof.** As in §1, (7) and (8), we introduce a vector $\mathfrak{C}_\sigma$ for each $\mathfrak{F}$, with

$$\mathfrak{C}_\sigma = \prod_\tau \mathfrak{F}_{\sigma,\tau}, \qquad \mathfrak{F}^n_{\sigma,\tau} = \mathfrak{C}_\sigma \mathfrak{C}_\tau^\sigma \mathfrak{C}_{\sigma\tau}^{-1}. \tag{5}$$

The function $h_P(\sigma)$ is then given by

$$h_P(\sigma) \equiv V_P(\mathfrak{C}_\sigma) \pmod{n}. \tag{6}$$

By (5), the transformation set $T\mathfrak{C}$ consists of $n$th powers, which means that

$$V_P(\mathfrak{C}_\sigma) + V_P(\mathfrak{C}_\tau^\sigma) \equiv V_P(\mathfrak{C}_{\sigma\tau}) \pmod{n}. \tag{7}$$

But $V_P(\mathfrak{C}_\tau^\sigma)$, the exponent to which the prime $P$ appears in $\mathfrak{C}_\tau^\sigma$, is simply the exponent of the prime $P^{\sigma^{-1}}$ in $\mathfrak{C}_\tau$. If we set $\sigma^{-1} = \rho$, (7) becomes

$$V_{P^\rho}(\mathfrak{C}_\tau) \equiv h_P(\rho^{-1}\tau) - h_P(\rho^{-1}) \pmod{n}. \tag{8}$$

If in (7) we let $\sigma$ be an element $\delta^{-1}$ in the decomposition group $\Delta(P)$, the result, expressed in terms of $h$, is

$$h_P(\delta) + h_P(\tau) \equiv h_P(\delta\tau) \pmod{n}, \qquad (\delta \text{ in } \Delta(P),\ \tau \text{ in } \Gamma). \tag{9}$$

This includes the desired conclusion (4) as a special case. By a similar device we may prove a partial converse to Lemma 1.

LEMMA 3. *If* $h_P(\delta, \mathfrak{F}^{(p)}) \equiv 0 \pmod{n}$, *for all* $\delta$ *in* $\Delta(P)$, *then the primary factor set* $\mathfrak{F}^{(p)}$ *is a transformation set.*

**Proof.** By (9), $h_P(\delta\tau) \equiv h_P(\tau) \pmod{n}$ then depends only on the coset of $\tau$ modulo $\Delta(P)$. There is therefore an ideal $\mathfrak{L}$ divisible by $P^\rho$ exactly to the power $h_P(\rho^{-1})$, for each factor $P^\rho$ of $p$, or

$$V_{P^\rho}(\mathfrak{L}) = h_P(\rho^{-1}, \mathfrak{F}).$$

Using (8), one may then show that $V_{P^\rho}(\mathfrak{L}^{1-\tau}\mathfrak{C}_\tau) \equiv 0 \pmod{n}$ for every $\rho$, which is to say that $\mathfrak{L}^{1-\tau}\mathfrak{C}_\tau$ is the $n$th power of some vector of ideals $\mathfrak{B}_\sigma$,

$$\mathfrak{L}^{1-\tau}\mathfrak{C}_\tau = \mathfrak{B}_\tau^n \qquad (\text{all } \tau \text{ in } \Gamma).$$

Substitution of this value of $\mathfrak{C}_\tau$ in the second equation of (5) yields $\mathfrak{F}^n = T\mathfrak{B}^n$. Since the $n$th roots can be extracted uniquely (if at all) in the group of ideals, the last equation means that $\mathfrak{F} = T\mathfrak{B} \sim 1$, as asserted.

LEMMA 4. *Every character* $h(\delta)$ *of the decomposition group* $\Delta(P)$ *is the character* $h(\delta) = h_P(\delta, \mathfrak{F})$ *of some p-primary factor set* $\mathfrak{F}$ *of ideals.*

**Proof.** In $\Gamma$ select for each coset $\sigma\Delta(P)$ a representative $\sigma^*$, taking care to select the identity as the representative of $\Delta(P)$ itself. A product $\sigma\sigma^{*-1}$ is then always in $\Delta(P)$. From the given character $h(\delta)$ of $\Delta(P)$ we define an extended function $h^*(\sigma)$ as

$$h^*(\sigma) = h(\sigma\sigma^{*-1}). \tag{10}$$

By the assumption (4) on $h$ one then computes that $h^*$ satisfies (9). This implies that the expression $h^*(\sigma\tau)-h^*(\tau)$ is unaltered, modulo $n$, by replacement of $\sigma$ by another element $\delta\sigma$ in the same coset. There must therefore be a vector of ideals $\mathfrak{C}_\tau$ with

$$\begin{aligned} V_P(\mathfrak{C}_\tau) &= h^*(\tau) - h^*(1), \\ V_{P^\rho}(\mathfrak{C}_\tau) &\equiv h^*(\rho^{-1}\tau) - h^*(\rho^{-1}) \pmod{n}, \end{aligned} \tag{11}$$

in analogy with (8). From this definition one computes that $V_{P^\rho}(\mathfrak{C}_\sigma\mathfrak{C}_\tau^\sigma\mathfrak{C}_{\sigma\tau}^{-1}) \equiv 0 \pmod{n}$, so that this transformation set must be an $n$th power $T\mathfrak{C} = \mathfrak{F}^n$. Here $\mathfrak{F}$ must be a factor set because it is the (unique) $n$th root of the known factor set $T\mathfrak{C}$. Furthermore this $p$-primary factor set $\mathfrak{F}$ has the given function $h(\delta)$ as character, for one computes by (11) that $h_P(\delta) = V_P(\mathfrak{C}_\delta) = h(\delta) - h(1) \equiv h(\delta) \pmod{n}$.

These results may be summarized by

THEOREM 5.1. *If the prime ideal factor $P$ of $p$ in $K/k$ has the decomposition group $\Delta(P)$ with the commutator subgroup $\Delta(P)'$, then the number of classes of $p$-primary factor sets of ideals in $K$ is equal to the index $[\Delta(P):\Delta(P)']$.*

**Proof.** The preceding lemmas show that the correspondence $\mathfrak{F} \to h_P(\delta, \mathfrak{F})$ maps the group of classes of $p$-primary factor sets isomorphically on the group of characters $h(\delta)$ mod $n$ of $\Delta(P)$. Hence we need only count the number of such characters. Each character maps the commutator subgroup $\Delta(P)'$ onto zero, mod $n$. Furthermore, each character of $\Delta(P)$ is induced by a character of the abelian quotient group $\Delta(P)/\Delta(P)'$. Conversely, this abelian group has a number of characters equal to its order, which is the index $[\Delta(P):\Delta(P)']$ of the conclusion.

COROLLARY. *If $P \mid p$ is unramified, the number of classes of $p$-primary factor sets is the $p$-degree $m_p$ of $K_P$ over $k_p$.*

**Proof.** $P \mid p$ unramified makes $\Delta(P)$ cyclic. The character $h_P(\delta)$ is essentially independent of the choice of the prime ideal factor $P$ of $p$. If $P^\rho$ is any other factor, the decomposition group $\Delta(P^\rho)$ of $P^\rho$ is obtained from $\Delta(P)$ by the isomorphism $\delta \to \rho\delta\rho^{-1}$. If $\delta$ is the Frobenius automorphism of $P$, then $\rho\delta\rho^{-1}$ is the Frobenius automorphism of $P^\rho$.

LEMMA 5. *For any prime factor $Q = P^\rho$, the corresponding character is*

$$h_Q(\rho\delta\rho^{-1}, \mathfrak{F}) = h_P(\delta) \qquad (\delta \text{ in } \Delta(P)). \tag{12}$$

*If $P \mid p$ is unramified, $P$ and $Q$ determine the same invariant $\mu_P(\mathfrak{F}) = \mu_Q(\mathfrak{F})$.*

For by (6), (8), and (9),

$$h_Q(\rho\delta\rho^{-1}) = V_Q(\mathfrak{C}_{\rho\delta\rho^{-1}}) = V_P(\mathfrak{C}_{\rho\delta\rho^{-1}}^{\rho^{-1}})$$
$$= V_P(\mathfrak{C}_{\delta\rho^{-1}}) - V_P(\mathfrak{C}_{\rho^{-1}}) \equiv h_P(\delta\rho^{-1}) - h_P(\rho^{-1}) \equiv h_P(\delta) \pmod{n}.$$

It is useful to express the character $h$ in several different forms.

LEMMA 6. *The character of any factor set $\mathfrak{F}$ is given by the expressions*

$$\begin{aligned} h_P(\delta, \mathfrak{F}) &\equiv (n/m) \sum_{\eta} V_P(\mathfrak{F}_{\delta,\eta}) && (\textit{summed over all } \eta \textit{ in } \Delta), \\ &\equiv (n/m) \sum_{\eta} V_P(\mathfrak{F}_{\eta,\delta}) && (\textit{summed over all } \eta \textit{ in } \Delta), \end{aligned} \tag{13}$$

*where $m = m_p$ is the order of the decomposition group $\Delta = \Delta(P)$. If $\zeta$ lies in a subgroup $\Lambda \subset \Delta$ of order $r$, then*

$$h_P(\zeta, \mathfrak{F}) \equiv (n/r) \sum_{\eta} V_P(\mathfrak{F}_{\eta,\zeta}) \qquad (\textit{summed over all } \eta \textit{ in } \Delta). \tag{14}$$

**Proof.** In the second half of (5), set $\sigma = \delta$, $\tau = \eta$, take the order $V_P$ and sum over $\eta$ (i.e., over $\delta\eta$). There results

$$n \sum_{\eta} V_P(\mathfrak{F}_{\delta,\eta}) = m V_P(\mathfrak{C}_\delta).$$

By (6), we have on the right $m h_P(\delta)$, hence the first result of (13). For convenience, we represent the exact exponent of $P$ in the decomposition of $\mathfrak{F}_{\zeta,\eta}$ by

$$e_{\zeta,\eta} = V_P(\mathfrak{F}_{\zeta,\eta}).$$

The second half of (13) reduces to proving that the "right" and "left" sum functions

$$R(\zeta) = \sum_{\eta} e_{\zeta,\eta}, \qquad L(\zeta) = \sum_{\eta} e_{\eta,\zeta}$$

are identical. But the associativity relations for $\mathfrak{F}$ yield for the exponents $e_{\zeta,\eta}$ the analogous relations

$$e_{\zeta,\eta} + e_{\zeta\eta,\xi} = e_{\eta,\xi} + e_{\zeta,\eta\xi} \qquad (\zeta, \eta, \xi \text{ in } \Delta(P)). \tag{15}$$

If this equation is added over $\zeta$ and then over $\xi$, one finds

$$L(\eta) + L(\xi) = m e_{\eta,\xi} + L(\eta\xi), \quad m e_{\zeta,\eta} + R(\zeta\eta) = R(\eta) + R(\zeta).$$

If we solve these equations for the common value $m e_{\zeta,\eta}$, we find

$$R(\zeta) + R(\eta) - R(\zeta\eta) = L(\zeta) + L(\eta) - L(\zeta\eta).$$

In this equation set $\eta=\delta^i$, $\zeta=\delta$, and add for $i=0, 1, \cdots, m-1$. The result is $mR(\delta)=mL(\delta)$, and hence $R(\delta)=L(\delta)$, as desired for (13).

The relation (14) describes in effect the behaviour of a character when applied to a subfield (corresponding to the subgroup $\Lambda$) of $K$. We set

$$L_\Lambda(\zeta) = \sum_\eta e_{\eta,\zeta} \qquad \text{(summed over all } \eta \text{ in } \Lambda).$$

The associativity relations (15), summed over all $\zeta$ in $\Lambda$, give

$$L_\Lambda(\eta) + L_\Lambda(\xi) = re_{\eta,\xi} + L_\Lambda(\eta\xi) \qquad (\eta, \xi \text{ in } \Lambda).$$

Combination with the similar equation for $L$ itself yields

$$(m/r)\left[L_\Lambda(\eta) + L_\Lambda(\xi) - L_\Lambda(\eta\xi)\right] = L(\eta) + L(\xi) - L(\eta\xi).$$

As in the previous case this entails $(m/r)L_\Lambda(\eta)=L(\eta)$. This gives (14), for the functions $L$ can be written as

$$L_\Lambda(\zeta) = \sum_\eta V_P(\mathfrak{F}_{\eta,\zeta}) \qquad (\eta \text{ in } \Lambda),$$

$$L(\zeta) = \sum_\eta V_P(\mathfrak{F}_{\eta,\zeta}) \qquad (\eta \text{ in } \Delta(P)).$$

The invariant $\mu_P(\mathfrak{F})$ as defined in (*5.2) is the same for all prime factors $Q$ of $p$ by Lemma 5, for it is known (see [20, Part II, p. 51]) that the Frobenius automorphism for $Q=P^\rho$ is obtained from that of $P$ as $\delta_Q=\rho\delta_P\rho^{-1}$. We write $\mu_p(\mathfrak{F})=\mu_P(\mathfrak{F})=\mu_Q(\mathfrak{F})$ for this common value. These invariants of $\mathfrak{F}$ form a complete set for ideals relatively prime to the module $M$.

THEOREM 5.2. *Two factor sets $\mathfrak{F}_1'$, $\mathfrak{F}_2'$ satisfy $\mathfrak{F}_1'\sim\mathfrak{F}_2'$ if and only if $\mu_p(\mathfrak{F}_1')\equiv\mu_p(\mathfrak{F}_2')$ (mod $n$) for every $p$ relatively prime to $M$.*

**Proof.** According to Lemma 1 we need only show that a factor set $\mathfrak{F}$ with its invariants all zero is a transformation set. As in (1), consider some $p$-primary component $\mathfrak{F}^{(p)}$ of the given factor set. Since the ideals are all relatively prime to the module $M$, we need consider here only prime divisors $p$ which are unramified in $K/k$. For such an unramified $p$ the decomposition group $\Delta(P)$ is cyclic with generator $\delta_P$, and the invariant $\mu_p=h_P(\delta_P)$ determines the whole character $h(\delta_P)$. Hence $\mu_p\equiv 0$ (mod $n$) implies $h_P(\delta_P)\equiv 0$ (mod $n$), which in turn makes $\mathfrak{F}^{(p)}\sim 1$, as in Lemma 3. Since this holds for any $p$-component, $\mathfrak{F}$ itself is $\sim 1$. In similar fashion we have

THEOREM 5.3. *Let integers $\mu_p$ be given for every $p$ relatively prime to $M$ such that, for every $p$,*

$$m_p\mu_p \equiv 0 \text{ (mod } n),$$

*and such that $\mu_p\equiv 0$ (mod $n$) except for a finite number of prime divisors $p$. Then there exists a factor set $\mathfrak{F}'$ of ideals relatively prime to $M$ with the invariants $\mu_p$.*

The computation of $\mu_p$ may be summarized (see [13, 14]) by

LEMMA 7. *If $\delta = \delta_P$ is the Frobenius automorphism of a factor $P$ of $p$, then*

$$\mu_p(\mathfrak{F}) = (n/m)V_P\left[\prod_{i=0}^{m-1} \mathfrak{F}_{\delta^i,\delta}\right], \qquad m = m_p. \tag{16}$$

*Furthermore, for the product of two factor sets*

$$\mu_p(\mathfrak{F}_1\mathfrak{F}_2) \equiv \mu_p(\mathfrak{F}_1) + \mu_p(\mathfrak{F}_2) \pmod{n}. \tag{17}$$

*If $\eta = \delta^t$ generates in $\Delta(P)$ a subgroup of order $r$, then*

$$t\mu_p(\mathfrak{F}) \equiv (n/r)V_P\left[\prod_{i=0}^{r-1} \mathfrak{F}_{\eta^i,\eta}\right] \pmod{n}. \tag{18}$$

Note that formula (16) is just like the formula (10) in §2 for the invariant $\mu_p$ of an actual algebra. Hence

THEOREM 5.4. *Any factor set $FA$ of numbers determines a factor set $\mathfrak{F} = (FA)$ of principal ideals, such that for unramified $p$ the invariants $\mu_p$ of the ideal factor set $\mathfrak{F}$ and the algebra $(K, \Gamma, FA)$ coincide:*

$$\mu_p((FA)) \equiv \mu_p(K, \Gamma, FA) \pmod{n}. \tag{19}$$

It is instructive to observe that the analysis of $p$-primary factor sets may be reduced to the factor sets $e_{\zeta,\eta}$ of integers with the associativity conditions (15). Such a factor set determines a group extension of the additive group $E$ of rational integers by the group $\Delta(P)$, under the assumption that each $\zeta$ in $\Delta(P)$ induces in $E$ the identity automorphism $e^\zeta = e$, $e$ in $E$. One may prove

THEOREM 5.5. *If $P$ is a prime ideal factor of $p$, and if $\mathfrak{F}_{\sigma,\tau} = P^{f\sigma,\tau}\mathfrak{B}_{\sigma,\tau}$, with $(\mathfrak{B}_{\sigma,\tau}, P) = 1$, is a $p$-primary factor set $\mathfrak{F}$ of ideals, then the exponents $f_{\zeta,\eta}$ for $\zeta$, $\eta$ in the decomposition group form an additive factor set $FE = f_{\zeta,\eta}$ of integers. The correspondence $\mathfrak{F} \to FE$ maps the classes of similar factor sets $\mathfrak{F}$ isomorphically on the classes of similar factor sets of integers.*

COROLLARY. *The number of group extensions of the group of $p$-primary ideals by the Galois group $\Gamma$ is the same as the number of group extensions of the additive group of integers by the decomposition group $\Delta(P)$.*

Here a "$p$-primary ideal" is one whose prime ideal factors are all factors of the given prime ideal $p$ of $k$.

6. **Factor sets for ideal algebras.** Following E. Noether, we consider the factor sets given by

(*6.1) $F'' =$ factor sets $FA$ composed of numbers $F_{\sigma,\tau}$ relatively prime to $M$, and such that the algebra $S = (K, \Gamma, FA)$ is relatively prime to $M$.

As before, "$S$ relatively prime to $M$" means $S_p \sim k_p$ for every $p$ involved in $M$.

Such factor sets $F''$ determine certain factor sets of principal ideals $(F_{\sigma,\tau})$ which are said to constitute the *principal class*(14) of ideal factor sets.

(*6.2) $(F'')$ = the group of factor sets $(F_{\sigma,\tau})$ of principal ideals generated by(15) factor sets $F_{\sigma,\tau}$ of type $F''$.

This group is contained in the group $\mathfrak{F}'$ of all factor sets of ideals relatively prime to(16) $M$.

The representation of an ideal algebra $\mathfrak{S}'$ by an ideal factor set in $\mathfrak{F}' = F\mathfrak{A}'$ may be stated as

THEOREM 6.1. *The index $J$ (the number of ideal algebras relatively prime to $M$ modulo the actual algebras relatively prime to $M$) is given by*

$$J = [\mathfrak{S}' : S'] = [F\mathfrak{A}' : T\mathfrak{A}' \cdot (F'')], \tag{1}$$

*where $T\mathfrak{A}' \cdot (F'')$ denotes the join of the subgroup $T\mathfrak{A}'$ of transformation sets and the subgroup $(F'')$ described above.*

**Proof.** Each factor set $\mathfrak{F}' = F\mathfrak{A}'$ of ideals determines a set of invariants $\mu_p(\mathfrak{F}')$ which are the invariants of some ideal algebra split by $K$. The correspondence

$$\mathfrak{F}' \to \mathfrak{S}' \quad \text{if, for all } p, \quad \mu_p(\mathfrak{F}') \equiv \mu_p(\mathfrak{S}') \pmod{n} \tag{2}$$

maps the group of factor sets $\mathfrak{F}'$ homomorphically into the group of ideal algebras $\mathfrak{S}'$ relatively prime to $M$, for multiplication of factor sets corresponds to multiplication of algebras (§5, (17), §2, (6)). For each $\mathfrak{S}'$ there is a corresponding set of invariants $\mu_p$, for which there must be, by Theorem 5.3, a corresponding ideal factor set $\mathfrak{F}'$. Hence (2) is a homomorphism. To prove the identity (1), it remains only to investigate the subgroup of $\mathfrak{F}$ carried by (2) into the group of actual algebras.

The subgroup $T\mathfrak{A}'$ of transformation sets is clearly carried by (2) into a certain group of actual algebras, for the invariants of a transformation set are all zero (mod $n$), as stated in Theorem 5.2, so the corresponding algebra is similar to $k$. On the other hand, the principal ideal factor set $(F'')$ is mapped by (1) on the actual algebra $(K, \Gamma, F'')$, according to Theorem 5.4. It remains to show that every factor set mapped into $S'$ lies in the product $T\mathfrak{A}' \cdot (F'')$. If $F \to S'$, then the algebra $S'$ has a crossed product representation $(K, \Gamma, F)$ in which the factor set $F$ may be so chosen that its components are relatively prime to(17) $M$. Thus $F$ is a factor set $F''$. According to the correspondence

(14) This principal class is narrower than that defined by Noether in [33], to the exact extent of the requirement that each $F_{\sigma,\tau}$ be relatively prime to $M$.

(15) In this definition, it is essential not only that $(F_{\sigma,\tau})$ be an ideal factor set, but also that the numbers $F_{\sigma,\tau}$ be themselves a factor set.

(16) Note that the infinite prime divisors in $M$ do not impose conditions on ideals.

(17) Proof is given below; see Theorem 6.2.

(2), $\mathfrak{F}$ and $S'$ have the same invariants. Hence, by Theorem 5.4, $\mathfrak{F}$ and $(F'')$ have the same invariants. Therefore their quotient is a transformation set (see Theorem 5.2). This proves (1) completely.

In the above proof we have assumed part of the following characterization of factor sets relatively prime to $M$.

THEOREM 6.2. *Let $S$ be a normal simple algebra over $k$ with maximal subfield $K$. Then $S$ has a crossed product representation $S=(K, \Gamma, F')$ with a factor set $F'$ of numbers relatively prime to the module $M$ if and only if, for every prime ideal $p$ involved in $M$, the $p$-adic component $S_p$ of $S$ has a representation*

$$S_p \sim (K_P/k_p, \Delta(P), FE_P) \tag{3}$$

*in which $FE_P$ is a factor set for the group $\Delta(P)$ in the group $E_P$ of units of the field $K_P$*[18].

**Proof.** If $S=(K, \Gamma, F')$, then each $F'_{\sigma,\tau}$ is a unit of each $K_P$, so we have the representation (3) by the usual formula of §2, (7) for the $p$-component of a crossed product. Conversely, assume (3) for every $p$ involved in $M$. The algebra $S$ has some crossed product representation $S=(K, \Gamma, \overline{F})$ with a factor set $\overline{F}$ not necessarily relatively prime to $M$. Then $S_p$ can be computed (by §2, (7)) as

$$S_p \sim (K_P/k_p, \Delta, \overline{F}_{\xi,\eta}) \sim (K_P/k_p, \Delta, E_{\xi,\eta})$$

where $E_{\xi,\eta}$ denotes the given factor set of $P$-adic units and $\Delta=\Delta(P)$. Since similar algebras arise only from similar factor sets, one has

$$\overline{F}_{\xi,\eta} \sim E_{\xi,\eta}, \quad \text{or} \quad \overline{F}_{\xi,\eta} = (A_\xi A_\eta^{\xi} A_{\xi\eta}^{-1}) E_{\xi,\eta},$$

from some vector $A_\xi$ of elements in $K_P$. One may then compute the character function $h$ associated with the factor set of principal ideals $(\overline{F})$. By Lemma 5.6, putting $m=m_p$,

$$\begin{aligned} h_P(\xi, (\overline{F})) &\equiv (n/m) \sum_\eta V_P(\overline{F}_{\xi,\eta}) \\ &\equiv (n/m) \sum_\eta V_P(A_\xi A_\eta^{\xi} A_{\xi\eta}^{-1}) \\ &\equiv (n/m)\left[ mV_P(A_\xi) + \sum_\eta V_P(A_\eta) - \sum_{\eta'} V_P(A_{\eta'}) \right] \equiv 0 \pmod{n}. \end{aligned}$$

Therefore the $p$-primary part of $(\overline{F})$ has character 0 and so is similar to 1,

[18] Note that in the theorem we consider only finite prime divisors. For infinite unramified prime divisors $p$ there are no proper local division algebras. If $p$ is ramified then there is the algebra of all real quaternions. The condition $F'$ relatively prime to $M$ admits in the latter case the real quaternions. One finds that $F'_{1,\delta} F'_{\delta,\delta} < 0$ ($\delta$ in the decomposition group of the ramified prime divisor) implies that $(K, \Gamma, F')_p$ is not similar to $k_p$.

which is to say that there are ($p$-primary) ideals $\mathfrak{B}_\sigma$ for which the similar factor set $(\overline{F})\cdot(T\mathfrak{B})$ is relatively prime to $p$. This can be done simultaneously for all the prime divisors $p$ involved in $M$. One may then select another vector of ideals $\mathfrak{C}_\sigma$ such that $\mathfrak{C}_\sigma$ is relatively prime to $M$ and $\mathfrak{B}_\sigma\mathfrak{C}_\sigma$ is a principal ideal $(D_\sigma)$. We obtain then by the transformation

$$(\overline{F}) \sim (\overline{F})(T\mathfrak{B})(T\mathfrak{C}) = (\overline{F})(T\mathfrak{B}\mathfrak{C}) = (\overline{F})(TD)$$

a new factor set which is relatively prime to $M$. Thus $F' = \overline{F}\cdot TD$ is a new factor set of numbers which is similar to $F$ and relatively prime to $M$. This gives the desired representation of $S$ as $S = (K, \Gamma, F')$.

7. **Crossed characters and principal genera.** In considering transformation sets $TA$ we shall repeatedly deal with the group of those vectors $A_\sigma$ for which the transformation set $TA$ is 1. Following a terminology suggested by A. H. Clifford, we call these vectors "*crossed characters*" of $\Gamma$. Specifically, let $H$ be any multiplicative abelian group with $\Gamma$ as a group of operators. Then a crossed character of $\Gamma$ in $H$ is any function $U(\sigma)$, with values $U(\sigma)$ in $H$ for each $\sigma$ in $\Gamma$, which satisfies the identity

(*7.1) $U(\sigma\tau) = U(\sigma)[U(\tau)]^\sigma$ ($U$ a crossed character).

The vector group of all such crossed characters we call $UH$. From a fixed element $H$ of the given group one may trivially obtain a crossed character $U(\sigma) = H^{1-\sigma}$. We call this a *unit character*, while two characters are *associates* if their quotient is a unit character. With the notation

(*7.2) $UH$ = the group of all crossed characters in $H$,

(*7.3) $H^{1-\sigma}$ = the group of unit characters = the group of vectors $\{H^{1-\sigma}$, all $\sigma$ in $\Gamma\}$,

the index $[UH: H^{1-\sigma}]$ will measure the number of classes of associated crossed characters of $\Gamma$ in $H$.

A "*principal genus theorem*" is an assertion that every crossed character, under certain conditions, is a unit character. The principal genus theorem for ideals [33] is

THEOREM 7.1. *Every crossed character of the Galois group $\Gamma$ in the group $\mathfrak{A}$ of all ideals of $K$ is a unit character. The same conclusion holds for crossed characters in the group $\mathfrak{A}'$ of all ideals relatively prime to $M$.*

**Proof.** If $\mathfrak{C}_\sigma$ is a vector of ideals, the theorem asserts that $T\mathfrak{C} = 1$ implies $\mathfrak{C}_\sigma = \mathfrak{B}^{1-\sigma}$ for some ideal $\mathfrak{B}$. Let $\mathfrak{B}$ denote the greatest common divisor $\sum\mathfrak{C}_\sigma$ of the given ideals. Then one computes that $\mathfrak{B}^\sigma\mathfrak{C}_\sigma = \mathfrak{B}$ ([13, p. 127]). One may write $\mathfrak{B} = \mathfrak{B}'\mathfrak{P}$, where $\mathfrak{B}'$ is relatively prime to $M$ and $\mathfrak{P}$ contains only prime factors of $M$. If each $\mathfrak{C}_\sigma$ is relatively prime to $M$, then

$$\mathfrak{P}^{1-\sigma} = \mathfrak{B}^{1-\sigma}/\mathfrak{B}'^{1-\sigma} = \mathfrak{C}_\sigma/\mathfrak{B}'^{1-\sigma}$$

is relatively prime to $M$ for every $\sigma$, so that $\mathfrak{P}^{1-\sigma}=1$. Then $\mathfrak{C}_\sigma=\mathfrak{B}^{1-\sigma}=\mathfrak{B}'^{1-\sigma}$, so $\mathfrak{B}'$ is the desired ideal in the group $\mathfrak{A}'$.

There is also a similar theorem for numbers (Noether's principal genus theorem([19])).

THEOREM 7.2. *Every crossed character of* $\Gamma$ *in the group of all nonzero numbers of* $K$ *is a unit character*([20]).

LEMMA 1. *Given a factor set* $F=TB$, *with* $F$ *but not necessarily* $B_\sigma$ *relatively prime to* $M$, *there exists a vector* $B'_\sigma$ *relatively prime to* $M$ *for which* $F=TB'$.

**Proof.** Write the principal ideals $(B_\sigma)$ as $(B_\sigma)=\mathfrak{A}_\sigma\mathfrak{C}_\sigma$, $\mathfrak{A}_\sigma$ relatively prime to $M$, where $\mathfrak{C}_\sigma$ involves only those prime ideals $\mathfrak{p}$ of $K$ which are involved in $M$. Then $(F)=T(B)=T\mathfrak{A}\cdot T\mathfrak{C}$. Since $(F)$ does not involve any $\mathfrak{p}$ of $M$, the transformation set $T\mathfrak{C}$ has no prime factors in common with either $(F)$ or $T\mathfrak{A}$. Hence $T\mathfrak{C}=1$, and $\mathfrak{C}_\sigma=\mathfrak{B}^{1-\sigma}$, by the principal genus theorem. Choose $\mathfrak{A}'$ such that $\mathfrak{B}\mathfrak{A}'$ is a principal ideal $(D)$. Then

$$(B_\sigma/D^{1-\sigma}) = (B_\sigma)/(D)^{1-\sigma} = \mathfrak{A}_\sigma\mathfrak{C}_\sigma/\mathfrak{B}^{1-\sigma}\mathfrak{A}'^{1-\sigma} = \mathfrak{A}_\sigma\mathfrak{A}'^{1-\sigma},$$

so that $B'_\sigma=B_\sigma/D^{1-\sigma}$ is, like $\mathfrak{A}_\sigma$, relatively prime to $M$. Furthermore,

$$TB' = TB/TD^{1-\sigma} = TB = F,$$

so the vector $B'_\sigma$ has the desired properties.

In order to clarify the meaning of the principal class $(F'')$ of ideal factor sets which appears in our basic index §6 (1), we now quote Noether's generalized principal genus theorem [33, 13]:

THEOREM 7.3. *If the vector* $\mathfrak{C}_\sigma$ *of ideals (not necessarily relatively prime to* $M$*) yields a transformation set* $T\mathfrak{C}$ *which lies in the principal class* $(F'')$ *of ideal factor sets, then there exists an ideal* $\mathfrak{B}$ *of* $K$, *such that* $\mathfrak{B}^{1-\sigma}$ *and* $\mathfrak{C}_\sigma$ *lie in the same ideal class, for every* $\sigma$ *in* $\Gamma$. *In other words, there exists a vector of principal ideals* $(B_\sigma)$ *such that*

$$\mathfrak{C}_\sigma = (B_\sigma)\mathfrak{B}^{1-\sigma} \qquad (\textit{all } \sigma \textit{ in } \Gamma). \tag{1}$$

*If* $\mathfrak{C}_\sigma$ *is relatively prime to* $M$, $\mathfrak{B}$ *and* $B_\sigma$ *may be chosen relatively prime to* $M$. *In other words, we have the implication*

$$T\mathfrak{C} = (F'') \rightarrow \mathfrak{C}_\sigma = (B_\sigma)\mathfrak{B}^{1-\sigma}. \tag{2}$$

**Proof**([21]). Let $T\mathfrak{C}=(F'')$. By definition (*6.2) of $F''$, the algebra $S$

([19]) Principal genus theorem "im Minimalen" [33].

([20]) The corresponding assertion for the group $A'$ of all numbers relatively prime to $M$ is false. If $\mathfrak{p}=(P_1\cdots P_g)^e$ is ramified in $K/k$, then there is an element $B$ with $(B)=P_1\cdots P_g\mathfrak{C}$, $\mathfrak{C}$ relatively prime to $M$. The vector $C_\sigma=B^{1-\sigma}$ is relatively prime to $M$, but $C_\sigma=B'^{1-\sigma}$ can be shown to be impossible.

([21]) We repeat a proof here to check the provisions "relatively prime to $M$" which are not present to Noether's original theorem.

$=(K, \Gamma, F'')$ has $S_p \sim 1$ for any $p$ involved in $M$. On the other hand, for a prime divisor $p$ not involved in $M$, we may compute the invariant

$$\mu_p(S) = \mu_p(F'') = \mu_p(T\mathfrak{C}) \equiv 0 \pmod{n},$$

according to Theorem 5.4 and Lemma 5.1. Hence $S_p \sim 1$ for all $p$. This means that $S \sim 1$, so the factor set for $S$ is $F'' = TB$, where the elements $B_\sigma$ may be chosen relatively prime to $M$, as in Lemma 7.1. Thus $T\mathfrak{C} = (F'') = (TB)$, $T[\mathfrak{C}_\sigma(B_\sigma^{-1})] = 1$, so $\mathfrak{C}_\sigma(B_\sigma^{-1}) = \mathfrak{B}^{1-\sigma}$, by the principal genus theorem for ideals. This gives the result (2).

8. **Cyclic analogues to factor sets.** It has long been recognized that properties of factor sets provide parallels to the properties of the numbers which appear in the usual class field theory for cyclic fields $Z/k$. The parallel is as follows (we denote by $\lambda$ a generator of the cyclic group of $Z/k$):

| CYCLIC $Z/k$ | ARBITRARY NORMAL $K/k$ |
|---|---|
| 1. A normal simple algebra $S/k$ with maximal subfield $Z$ (or $K$) may be represented as | |
| a cyclic algebra $S = (Z, \lambda, a)$, | a crossed product $S = (K, \Gamma, F)$. |
| 2. This algebra is then determined by | |
| $a$, a number, | $F$, a factor set. |
| 3. The associativity of the products in the algebra gives the condition | |
| $a$ in $k$, | $F$ satisfies the associativity conditions of §1, (4). |
| 4. The algebra $S$ is a total matric algebra if and only if | |
| $a$ is a relative norm in $Z/k$: $a = N_{Z/k}C$, | $F$ is a transformation set: $F = TA$. |
| 5. The algebra $S$ is a total matric algebra if and only if $S_p \sim k_p$ for all $p$; that is, if and only if, for each $p$, | |
| $a = N_p C_p$ where $N_p$ is the relative norm in $Z_P/k_p$, | $F \cap \Delta = T_\Delta A_P$ where $T_\Delta$ is a transformation set for $\Delta = \Delta(P)$, $A_P$ in $K_P$. |
| 6. If $B$ is a number of $Z$ ($B_\sigma$ a vector of $K$) then | |
| $N_{Z/k}B = 1$, | $TB_\sigma = 1$ |

holds if and only if, for some $C$ in $Z$ (or in $K$),

$$B = C^{1-\lambda} \qquad B_\sigma = C^{1-\sigma} \quad \text{(all } \sigma \text{ in } \Gamma\text{)}$$

(Hilbert's norm theorem), (minimal principal genus theorem).

7. A conductor

$$c(Z/k), \qquad C(K/k)$$

(see §26 below).

8. The principal genus consists of all ideals $\mathfrak{B}$ (ideal vectors $\mathfrak{B}_\sigma$) relatively prime to the conductor $c$ (to $M$) such that

$$N_{Z/k}\mathfrak{B} = (\nu), \qquad T\mathfrak{B} = (F''),$$

where the essential condition([22]) is that, for every $p$ in $C(Z/k)$ or $M$,

$$(Z, \lambda, \nu)_p \sim k_p, \qquad (K, \Gamma, F'')_p \sim k_p.$$

In the cyclic case the precise results of the class field theory depend on the computation that

$$[\mathfrak{a}' : (\nu)N\mathfrak{A}'] = n$$

where $\mathfrak{a}'$ denotes the group of all ideals in $k$ which are relatively prime to the conductor $c(Z/k)$. Since norms correspond to transformation sets, elements of $k$ to factor sets, ideals in $k$ to ideal factor sets, and norm residues to factor sets $F''$, one sees that the corresponding index in the general case will be the index

$$J = [F\mathfrak{A}' : T\mathfrak{A}'(F'')]$$

which has already appeared in Theorem 6.1 as our main index $J$.

Next we shall show briefly that the general index $J$ specializes to $[\mathfrak{a}' : (\nu)N\mathfrak{A}']$ in the cyclic case. So suppose that the cyclic Galois group is generated by $\lambda$. We can normalize the factor set in the usual manner([23])

$$u_\lambda^n = u_\lambda u_\lambda \cdots u_\lambda = \prod_{i=0}^{n-1} F_{\lambda^i,\lambda}.$$

We apply this process to the various groups involved in $J$, so

$$(1) \qquad F\mathfrak{A}' \to \prod_{i=0}^{n-1} \mathfrak{F}_{\lambda^i,\lambda} = \mathfrak{B},$$

$$(2) \qquad (F'') \to \prod_{i=0}^{n-1} (F''_{\lambda^i,\lambda}) = (B),$$

---

([22]) The condition on $\nu$ is equivalent to requiring that $\nu$ be a norm residue for $c(Z/k)$.

([23]) See, for example [13, pp. 64–65]; as well as §2, (9) above.

$$T\mathfrak{A}' \to \prod_{i=0}^{n-1} (\mathfrak{A}'_{\lambda^i} \mathfrak{A}'^{\lambda^i}_{\lambda} \mathfrak{A}'^{-1}_{\lambda^{i+1}}) = N_{Z/k}\mathfrak{A}'_{\lambda} \tag{3}$$

gives a homomorphism of the various groups involved in $J$ upon those of the classical class field theory. We first remark that $\mathfrak{B}$ is an ideal $\mathfrak{b}$ of $k$, for $\mathfrak{B}$ is relatively prime to $M$ and invariant under $\lambda$. Inversion of the normalization of factor sets proves that every ideal $\mathfrak{a}'$ in $k$ can be obtained as a $\mathfrak{B}$ from some $F\mathfrak{A}'$, and that every $N\mathfrak{A}'$ has the form $N\mathfrak{A}'_{\lambda}$ for some $T\mathfrak{A}'_{\lambda}$ of (3). It remains to prove only that the norm residues $\nu$ are the elements $B$ obtained from the principal class $(F'')$ in (2). Assume that the prime divisors $p$ involved in the module $M$ are precisely those which appear in the conductor $c(Z/k)$ (i.e., precisely those ramified in $Z/k$). Then $B$ of (2) is in $k$, is relatively prime to $c(Z/k)$, and is the normalized constant of the algebra $S=(Z,\lambda,B)=(K,\Gamma,F'')$. By definition of $F''$, $S_p=(Z,\lambda,B)_p \sim k_p$ for all $p$ in $c(Z/k)$. Therefore $B$ is a local norm for each such $p$, so is a norm residue for $c(Z/k)$. Conversely, any norm residue $\nu$ is relatively prime to $M$ and determines an algebra $(Z,\lambda,\nu)$ which is relatively prime to $M$ and so can be written, by the inverse of the normalization process, as $(Z,\Gamma,F'')$. This completes the proof of the assertion that $J$ specializes to the classical index in the cyclic case[24].

We propose to investigate how far the methods used for the cyclic case will carry in the calculation of $J=[F\mathfrak{A}' : T\mathfrak{A}'(F'')]$.

## CHAPTER II. INDICES FOR GROUPS OF ALGEBRAS

9. **Group-theoretic principles.** The usual computations for the group indices in the cyclic case involve a number of principles for transforming given group indices. These we now state for reference. It is customary to carry out these group reductions formally, without any indication of purpose. Rather than join in this type of obscurantism, we attempt to formulate some directions for such calculations. If $R$, $S$, $T$[25] are given abelian groups, the usual problem is to compute the index $[R:S]$ of some subgroup $S$ in $R$.

The objective can be attained if $R$ and $S$ are groups determined by simple and explicit generators, so that the quotient group $R/S$ can be described completely and its order $[R:S]$ computed. For example, the group $\mathfrak{A}$ of all ideals has a simple generation by prime ideals. In order that this *direct computation* be possible, it is necessary to change a given index to indices involving other, simpler groups.

The simplest case is the *introduction* of suitable *intermediate* groups. In the class field theory it is especially useful to introduce a subgroup from the

[24] For general abelian extensions $K/k$ the general index obviously does not specialize to $[\mathfrak{A}' : (\nu)N\mathfrak{A}']$. The fact that the latter factor group is isomorphic with $\Gamma$ cannot be explained by referring to general factor sets. It is a consequence of the special structure of $K$ over $k$.

[25] The letters $R$, $S$, $T$ are used in this section without reference to their previous and later meaning.

base field corresponding to a given group in the extension $K$. (Thus the group of numbers $\neq 0$ of $k$ is a subgroup of the group $A$ for $K$.) In general, if $[R:T]$ is finite,

$$(1) \qquad R \supset S \supset T \rightarrow [R:T] = [R:S]\cdot[S:T].$$

A *characterization* of a given group in different terms is often an essential preparatory step to a reduction. Thus the principal genus theorem for ideals characterizes the vectors $\mathfrak{B}^{1-\sigma}$ as those vectors $\mathfrak{C}_\sigma$ for which $T(\mathfrak{C}_\sigma)=1$.

A *reduction principle* may be applied if a given group is a composite of two groups $R$ and $S$. Since the groups are abelian, this composite is

(*9.1) $R\cdot S=$the set of all products $rs$, for $r$ in $R$, $s$ in $S$.

One has [23, p. 129],

$$(2) \qquad [RS:S] = [R:R\cap S],$$

where $R\cap S$ denotes the intersection. This equality may be proved on the assumption that either one of the two given indices is finite. If the composite occurs as a subgroup $ST\subset R$, one may introduce a smaller subgroup $S$ and write, using (1)

$$(3) \qquad [R:ST] = [R:S]\cdot[ST:S]^{-1} = [R:S]\cdot[T:S\cap T]^{-1}$$

on the assumption that $[R:S]$ is finite, or that $[R:ST]$ and $[T:S]$ are both finite.

The *isomorphism principle* is the well-known description of the effect of a homomorphism upon suitable subgroups. If $\phi$ is a homomorphic map of $R$ on $R'$, while $S'$ is a subgroup of $R'$, the set $\phi^{-1}(S')$ composed of all elements of $R$ mapped by $\phi$ into $S'$ is a subgroup of $R$, and the quotient groups $R/\phi^{-1}(S')$ and $R'/S'$ are isomorphic. Hence

$$(4) \qquad [R:\phi^{-1}(S')] = [R':S'],$$

provided either index is known to be finite.

The *homomorphism principle* describes the similar computation for any index $[R:S]$ under a homomorphism $\phi$ mapping $R$ into part of a group $T$. Let $\phi^{-1}(1)$ denote the set of all elements mapped by $\phi$ onto the identity 1 in $T$. Then

$$(5) \qquad \phi^{-1}(1)\cap S = \text{all elements of } S \text{ mapped onto 1 by } \phi.$$

One has

$$(6) \qquad [R:S] = [\phi(R):\phi(S)]\cdot[\phi^{-1}(1)\cap R:\phi^{-1}(1)\cap S],$$

provided $[R:S]$ is finite.

This principle will be applied to two homomorphisms occurring naturally in our theory. The first is the map

$$\mathfrak{A} \to \mathfrak{A}^{1-\sigma} = \mathfrak{A}/\mathfrak{A}^{\sigma} \tag{7}$$

carrying an ideal $\mathfrak{A}$ into the vector with components $\mathfrak{A}^{1-\sigma}$. The second is the map

$$\mathfrak{A}_\sigma \to T\mathfrak{A}_\sigma = T\mathfrak{A} = \mathfrak{A}_\sigma \mathfrak{A}_\tau^{\sigma}/\mathfrak{A}_{\sigma\tau} \tag{8}$$

under which a vector $\mathfrak{A}_\sigma$ determines its correspondent transformation set. The analogous homomorphisms in the cyclic theory are

$$\mathfrak{A} \to \mathfrak{A}^{1-\lambda}, \qquad \mathfrak{A} \to N_{Z/k}\mathfrak{A}.$$

These homomorphisms have the convenient property that they may be applied in either order, one after the other, with the result always the identity

$$N(\mathfrak{A}^{1-\lambda}) = (N\mathfrak{A})^{1-\lambda} = 1.$$

This situation is exploited in the famous Herbrand group reduction principle [23, pp. 130–131]. In the general case this cannot be done, for it is meaningless to apply (8) "followed by" (7). This is the root for some essential difficulties in our computations (see §§18–23).

Another important homomorphism is

$$A \to (A) \tag{9}$$

mapping the group of nonzero numbers on the group of principal ideals. This homomorphism is often applied backwards, to reduce an index on principal ideals to one on numbers. Under this homomorphism, the group mapped onto the identity is exactly the group of units. This is the point at which the units are inserted into the computations.

LEMMA 1. *Let $R \supset S$ be multiplicative groups of numbers in $K$, while $(R)$, $(S)$ are the corresponding groups of principal ideals, generated by these numbers. If $E$ is the group of units of $K$, then*

$$[(R):(S)] = [RE:SE], \tag{10}$$

*provided either of the indices concerned is finite. If $R \supset E$, one also has*

$$[(R):(S)] = [R:S][E:S \cap E]^{-1} \tag{11}$$

*provided the index $[R:S]$ is finite.*

The proof will illustrate the systematic application of the principles above. Apply the homomorphism $R \to (R)$ and observe that the subgroup carried into the identity is simply the group $E$. Hence by (6), one has

$$[R:S] = [(R):(S)][R \cap E:S \cap E],$$

which gives (11). On the other hand, the homomorphism $RE \to (RE) = (R)$ is

one in which all elements mapped on 1 lie in the subgroup $E$ of $SE$. Thus the isomorphism principle of (4) applies to give (10).

For direct products, one has

LEMMA 2. *Let $R_1 \subset R$ and $S_1 \subset S$ be subgroups of the respective factors of a direct product $R \times S$. Then*

$$[R \times S : R_1 \times S_1] = [R : R_1] \cdot [S : S_1], \tag{12}$$

*provided the indices on either side of this equation are known to be finite.*

As an application, suppose that $R \supset S$ are groups of numbers of $K$, while $R_\sigma$ ($S_\sigma$) is the group of vectors with components $R_\sigma$ ($S_\sigma$) in $R$ ($S$) for every $\sigma$ in $\Gamma$. The group $R_\sigma$ is thus the direct product of $n$ groups $R$, where $n$ is the order of $\Gamma$. Hence, if $[R:S]$ is finite,

$$[R_\sigma : S_\sigma] = [R:S]^n. \tag{13}$$

10. **Invariant ideal classes.** The basic index $J$ can be transformed into a form involving the number of ideal classes of $K$ invariant under the group $\Gamma$. The results are stated in Theorems 10.1 and 10.2, while the method is directed at successive applications of the basic homomorphisms $\mathfrak{A} \to \mathfrak{A}^{1-\sigma}$ and $\mathfrak{A}_\sigma \to T\mathfrak{A}$. We need the notation:

(*10.1) $\mathfrak{A}^{1-\sigma}$ = a vector $\{\mathfrak{A}^{1-\sigma}, \sigma$ all elements of $\Gamma\}$, for $\mathfrak{A}$ a fixed ideal,
(*10.2) $E$ = the group of all units in $K$,
(*10.3) $H = [\mathfrak{A} : (A)]$ = the class number of $K$,
(*10.4) $h = [\mathfrak{a} : (a)]$ = the class number of $k$.

Consider the index $J = [F\mathfrak{A}' : T\mathfrak{A}'(F'')]$. Since the second group is composite, one applies the appropriate reduction of §9, (3), to get

$$J = [F\mathfrak{A}' : (F'')][T\mathfrak{A}' : T\mathfrak{A}' \cap (F'')]^{-1}.$$

This is valid because the second index is finite, as will appear in the course of the subsequent computations of this section. The second member of $J$ arises from a homomorphic map $\mathfrak{A}_\sigma \to T\mathfrak{A}$, and the principal genus theorem states that the vectors carried into the subgroup $T\mathfrak{A}' \cap (F'')$ by this map are exactly the vectors of the form $\mathfrak{A}^{1-\sigma}(A_\sigma)$, with $\mathfrak{A}$ and $A_\sigma$ relatively prime to $M$. Hence the isomorphism principle yields

$$J = [F\mathfrak{A}' : (F'')][\mathfrak{A}'_\sigma : \mathfrak{A}'^{1-\sigma}(A')_\sigma]^{-1}. \tag{1}$$

Here the vector groups occurring on the right are (temporary notation):

$\mathfrak{A}'_\sigma$ = the group of all vectors $\mathfrak{A}_\sigma$ with components relatively prime to $M$,
$\mathfrak{A}'^{1-\sigma}$ = the group of all vectors of the form $\mathfrak{A}'^{1-\sigma}$, for an $\mathfrak{A}'$ relatively prime to $M$,
$(A')_\sigma$ = the group of all vectors of principal ideals generated by numbers $A'$ relatively prime to $M$.

The composite appearing in the second index again suggests a reduction by (3) in §9,

$$(2) \qquad [\mathfrak{A}'_\sigma : \mathfrak{A}'^{1-\sigma}(A')_\sigma] = [\mathfrak{A}'_\sigma : (A')_\sigma][\mathfrak{A}'^{1-\sigma} : \mathfrak{A}'^{1-\sigma} \cap (A')_\sigma]^{-1}.$$

This step (and the previous one) is valid if the index $[\mathfrak{A}'_\sigma : (A')_\sigma]$ on the right is finite. This it is, for such an index of two vector groups reduces, as in Lemma 2 of §9, to[26]

$$[\mathfrak{A}'_\sigma : (A')_\sigma] = [\mathfrak{A}' : (A')]^n = H^n.$$

But the second member of (2) suggests the homomorphism $\mathfrak{A} \to \mathfrak{A}^{1-\sigma}$. For the elements carried by this homomorphism into the subgroup $\mathfrak{A}^{1-\sigma} \cap (A)_\sigma$ we use the letter $\mathfrak{D}$:

(*10.5) $\mathfrak{D}$ = all ideals in $K$ with $\mathfrak{D}^{1-\sigma}$ principal for every $\sigma$ in $\Gamma$.

For the moment we also denote by $\mathfrak{D}'$ the ideals of $\mathfrak{D}$ relatively prime to $M$. These ideals $\mathfrak{D}$ might be called ideals in "invariant classes," for by definition $\mathfrak{D}^\sigma$ and $\mathfrak{D}$ lie in the same ideal class, for every $\sigma$. Under this homomorphism, (2) becomes

$$(3) \qquad [\mathfrak{A}'_\sigma : \mathfrak{A}'^{1-\sigma}(A')_\sigma] = H^n[\mathfrak{A}' : \mathfrak{D}']^{-1}.$$

The quotient $H[\mathfrak{A}' : \mathfrak{D}']^{-1}$ involved here suggests the elimination of the group $\mathfrak{A}'$,

$$(4) \qquad H[\mathfrak{A}' : \mathfrak{D}']^{-1} = [\mathfrak{A}' : (A')][\mathfrak{A}' : \mathfrak{D}']^{-1} = [\mathfrak{D}' : (A')].$$

In the latter index, one may drop the condition "relatively prime to $M$." Specifically, any ideal $\mathfrak{D}$ generates an ideal class which contains some ideal $\mathfrak{B}'$ relatively prime to $M$, so $\mathfrak{D} = \mathfrak{B}'(A)$. Here $\mathfrak{B}'^{1-\sigma}$, like $\mathfrak{D}^{1-\sigma}$, must be principal, so that $\mathfrak{B}'$ is in $\mathfrak{D}'$, and $\mathfrak{D}$ is the group join $\mathfrak{D}'(A)$. By the reduction principle

$$[\mathfrak{D} : (A)] = [\mathfrak{D}'(A) : (A)] = [\mathfrak{D}' : (A) \cap \mathfrak{D}'].$$

The intersection $(A) \cap \mathfrak{D}'$ is just the group of principal ideals $(A')$, so

$$(5) \qquad [\mathfrak{D} : (A)] = [\mathfrak{D}' : (A')].$$

A combination of the results of (1), (3), (4), and (5) yields

THEOREM 10.1. *If $H$ is the class number of $K$, while $[\mathfrak{D} : (A)]$ is the number of invariant ideal classes of $K$ (see* (*10.5)*), then the basic index is*

$$(6) \qquad J = [F\mathfrak{A}' : (F'')][\mathfrak{D} : (A)]^{-1} H^{1-n},$$

*where the first factor gives the number of ideal factor sets relatively prime to $M$ modulo the "principal class" $(F'')$ of* (*6.2).

[26] Note that the class number $H$ may be computed with a restriction to ideals relatively prime to $M$ (any ideal class contains an ideal relatively prime to any given module).

To study the index $[\mathfrak{D}:(A)]$ appearing above, we use the definition of $\mathfrak{D}$, which involves the mapping of $\mathfrak{D}$ on the vector $\mathfrak{D}^{1-\sigma}$ of principal ideals. The subgroup carried into the identity by this mapping is the *group of invariant ideals* $\mathfrak{J}$,

$$\mathfrak{J} = \text{all ideals of } K \text{ with } \mathfrak{J} = \mathfrak{J}^{\sigma}, \text{ for every } \sigma \text{ in } \Gamma.$$

The corresponding subgroup of invariant principal ideals is $(\Delta)$, where

(*10.6) $\Delta = \text{all numbers} \neq 0 \text{ of } K \text{ with } (\Delta^{1-\sigma}) = 1, \text{ for every } \sigma.$

According to the homomorphism principle we get,

$$[\mathfrak{D}:(A)] = [\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})][\mathfrak{J}:(\Delta)]. \tag{7}$$

The group of principal ideals $(\Delta)$ certainly includes all principal ideals $(a)$ of $k$. The introduction of this subgroup in the second factor of (7) yields

$$[\mathfrak{J}:(\Delta)] = [\mathfrak{J}:(a)][(\Delta):(a)]^{-1}, \tag{8}$$

provided the first index is finite. To see this, use the subgroup of ideals $\mathfrak{a}$ in $k$, for which

$$[\mathfrak{J}:(a)] = [\mathfrak{J}:\mathfrak{a}][\mathfrak{a}:(a)].$$

The second factor is the (finite) class number $h$, while the first measures the number of invariant ideals $\mathfrak{J}$ which are not extensions of ideals in $k$. But an invariant ideal $\mathfrak{J}$ involves with each prime factor $P$ every conjugate $P^{\sigma}$. If $P$ is unramified in $K/k$, the product $P_1P_2 \cdots P_g$ of all conjugates $P_i$ of $P$ is a prime ideal $p$ of $k$, consequently is in the group $\mathfrak{a}$. Hence any $\mathfrak{J}$ is congruent modulo $\mathfrak{a}$ to an invariant ideal $\mathfrak{J}$ involving only prime factors $P$ ramified in $K/k$. If $p$ is a ramified ideal in $K/k$, with

$$p = (P_1 \cdots P_g)^e, \qquad e = e_p, \tag{9}$$

then the invariant ideals involving only factors of $p$ must all be of the form $(P_1 \cdots P_g)^i$. For these ideals we get a complete set of representatives modulo $\mathfrak{a}$ if $i$ ranges from 0 to $e-1$, for $(P_1 \cdots P_g)^e = p$ is an ideal in $\mathfrak{a}$. Combining the effects due to the different ramified primes (according to the direct product of the partial groups $\mathfrak{J}$) one finds

$$[\mathfrak{J}:\mathfrak{a}] = \prod e_p \qquad \text{(over all finite } p \text{ of } k).$$

Therefore the first factor on the right of (8) is indeed finite, and the result is

$$[\mathfrak{J}:(\Delta)] = h(\prod e_p)[(\Delta):(a)]^{-1}. \tag{10}$$

The index $[(\Delta):(a)]$ may be shifted to one involving only numbers. Since every unit $E$ is by definition (*10.6) a number $\Delta$, one has, by equation (10) of §9,

$$[(\Delta):(a)] = [\Delta:aE].$$

To exploit the definition of $\Delta$ one clearly must use the homomorphism $\Delta \to \Delta^{1-\sigma}$. In this homomorphism the only elements mapped on the identity are in $a$, so the isomorphism principle yields

$$[(\Delta):(a)] = [\Delta^{1-\sigma}:E^{1-\sigma}].$$

The vector $\Delta^{1-\sigma}$ can be characterized as a vector of units $E_\sigma$ which can be obtained as $E_\sigma = A^{1-\sigma}$ for a number $A = \Delta$. By the principal genus theorem for numbers, the vector $E_\sigma$ has this form if and only if $TE_\sigma = TE = 1$, i.e., if and only if $E_\sigma$ is a crossed character $U(\sigma)$ (see §7).

(*10.7) $UE$ = the group of all crossed characters of $\Gamma$ in the group of units = all vectors of units $U(\sigma)$ with $U(\sigma)[U(\tau)]^\sigma = U(\sigma\tau)$.

Then

$$[(\Delta):(a)] = [UE:E^{1-\sigma}]. \tag{11}$$

THEOREM 10.2. *The number of invariant ideal classes of $K$ is*

$$[\mathfrak{D}:(A)] = [\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})][UE:E^{1-\sigma}]^{-1} h \prod e_p, \tag{12}$$

*where $[UE:E^{1-\sigma}]$ denotes the number of non-associated crossed characters in $E$, $h$ is the class number of the base field $k$, and the product $\prod e_p$, taken over all finite prime divisors $p$, uses*

(*10.8) *$e_p$ = the ramification order of the prime ideal $p$ in $K/k$.*

The crossed characters of units are closely related by (11) to the principal ideal theorem [30]. The group $(\Delta)$ of principal invariant ideals includes the group $\mathfrak{a}_K$ of those ideals in $k$ which become principal ideals in $K$, so that

$$[\mathfrak{a}_k:(a)] \leqq [UE:E^{1-\sigma}]. \tag{13}$$

In case $K/k$ is unramified, the above computation of $[\mathfrak{J}:\mathfrak{a}]$ shows that all $(\Delta)$ lie in $\mathfrak{a}_K$, so that this inequality becomes an equation. We state the result as

THEOREM 10.3. *The number $[\mathfrak{a}_K:(a)]$ of ideal classes of $k$ which become principal in $K$ is at most equal to the number of classes of associated crossed characters of $\Gamma$ in the group $E$ of units. If $K/k$ is unramified, these two numbers are equal.*

The equation (11) in reality involves an isomorphism $(\Delta)/(a) \simeq UE/E^{1-\sigma}$. As Moriya ([30]) has done in the cyclic case, one may call those crossed characters, which in this isomorphism correspond to elements in the subgroup $\mathfrak{a}_K/(a)$, crossed characters of the "first kind." This allows an obvious restatement of Theorem 10.3.

11. **Reduction to unit factor sets.** A further reduction leads now to the formula for $J$ given in Theorem 11.2 below. We use the notation

(*11.1) $FE$ = the group of factor sets of units,

(*11.2) $TE$ = the group of all transformation sets of units.

The index $[\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})]$ of Theorem 10.2 may be shifted from ideals to numbers if one observes that by definition (*10.5) each $\mathfrak{D}^{1-\sigma}$ is a principal ideal $(\theta_\sigma)$. Let $\theta_\sigma$ temporarily denote any vector of numbers so obtainable,

$$(\theta_\sigma) = \mathfrak{D}^{1-\sigma}, \qquad \text{for some } \mathfrak{D} \text{ and all } \sigma.$$

Surely a vector of units $E_\sigma$ is such a vector, for each $(E_\sigma)$ is 1. Therefore the principal ideal shift of §9, applied to these vector groups, yields

$$[\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})] = [(\theta_\sigma):(A^{1-\sigma})] = [\theta_\sigma:A^{1-\sigma}E_\sigma].$$

Now apply the homomorphism $\theta_\sigma \to T\theta_\sigma = T\theta$. The elements mapped on 1 by this homomorphism are all in the group of vectors $A^{1-\sigma}$, according to the minimal principal genus theorem (see §7). Hence the isomorphism principle yields

$$[\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})] = [\theta_\sigma:A^{1-\sigma}E_\sigma] = [T\theta:TE]. \tag{1}$$

We next investigate the group $T\theta$. By definition, $(\theta_\sigma)=\mathfrak{D}^{1-\sigma}$, so $T(\theta)=T\mathfrak{D}^{1-\sigma}=1$. Each element of the factor set $T\theta$ is thus a unit of $K$, so $T\theta$ is contained in the group $FE$ of factor sets of units. On the other hand, $T\theta$ is a transformation set of numbers, hence the corresponding crossed product algebra $S=(K, \Gamma, T\theta)$ is a total matric algebra. Since each $p$-adic component $S_p$ of this algebra is then similar to $k_p$, it follows that $T\theta$ is one of the factor sets $F''$ considered in our basic index.

We now assert that these two groups $FE$ and $F''$ not only both contain $T\theta$, but that their intersection is $T\theta$,

$$FE \cap F'' = T\theta. \tag{2}$$

For, let $F$ be a factor set in the intersection([27]), and consider the invariants of the crossed product $(K, \Gamma, F)=S$. If $p$ is ramified in $K/k$, the assumption $F$ in $F''$ means that $S_p \sim 1$, hence that the corresponding invariant $\mu_p \equiv 0 \pmod{n}$. If $p$ is finite and not ramified in $K/k$, the invariant $\mu_p(S)$ may be computed by the explicit formula of §2, (10). Since all the $F_{\sigma,\tau}$ of the factor sets are units in $K$, the invariant turns out to be $\equiv 0 \pmod{n}$. If $p$ is infinite and unramified the invariant is also $\equiv 0 \pmod{n}$. As the algebra $S$ is completely determined (up to similarity) by its invariants, this proves $S \sim 1$. Therefore the factor set $F$ is a transformation set $F=TA_\sigma=TA$. The principal ideals $T(A_\sigma)=(TA_\sigma)=(F_{\sigma,\tau})$ are then all equal to 1. The principal genus theorem for ideals then asserts that $(A_\sigma)=\mathfrak{D}^{1-\sigma}$ for some ideal $\mathfrak{D}$. Therefore the vector $A_\sigma$ is one of the vectors $\theta_\sigma$, $F=TA$ lies in the group $T\theta_\sigma$, and (2) is established.

Introducing this expression in the index (1), we have

THEOREM 11.1. *The first index of Theorem* 10.2 *is*

([27]) This proof is essentially due to E. Noether [33].

$$(3) \qquad [\mathfrak{D}^{1-\sigma}:(A^{1-\sigma})] = [FE \cap F'':TE].$$

The same intersection group may be extracted from the first factor of $J$, as found in Theorem 10.1. In $[F\mathfrak{A}':(F'')]$ insert the intermediate group $(F')$ of ideal factor sets (see (*3.2)):

$$[F\mathfrak{A}':(F'')] = [F\mathfrak{A}':(F')][(F'):(F'')].$$

Here the second index may be shifted to numbers, after the manner of §9, (11), with the results

$$(4) \qquad [F\mathfrak{A}':(F'')] = [F\mathfrak{A}':(F')][F':F''][FE:F'' \cap FE]^{-1}$$

which is valid provided $[F':F'']$ is finite.

When this result is inserted in the expression (6) for $J$ in Theorem 10.1 and combined with the results of Theorems 10.2 and 11.1, we find a formula for $J$, the denominator of which involves parts of (4), as

$$[FE:F'' \cap FE][FE \cap F'':TE] = [FE:TE].$$

All told, one has

THEOREM 11.2. *If the factor set index* $[F':F'']$ *is finite*[28] *(see* (*6.1)), *then*

$$(5) \qquad \begin{aligned} J &= [F\mathfrak{A}':(F')]H^{1-n}h^{-1}[F':F''](\prod e_p)^{-1}J(E), \\ J(E) &= [UE:E^{1-\sigma}][FE:TE]^{-1}, \end{aligned}$$

*where the product is taken over the ramification orders* $e_p$ *of all finite primes, where* $H$ *and* $h$ *are class numbers, and* $[F\mathfrak{A}':(F')]$ *is the number of ideal factor sets relatively prime to* $M$ *modulo the principal ideal factor sets.*

The group $E$ of units in $K$ appears in (5), as the quotient $J(E)$: the number of classes of crossed characters of $E$ divided by the number of group extensions of $E$. In the sequel we turn to the separate investigation of the terms in (5). We first compute $[F':F'']$, proving it finite, then reduce the index $[F\mathfrak{A}':(F')]$ in terms of a certain group-theoretic "deficiency" index, and finally devote a chapter to the index $J(E)$.

12. **Local algebras with factor sets of units.** The study of factor sets $F''$ for algebras unramified at the divisors of $M$ will subsequently be reduced to questions on local algebras $S_p$ with factor sets of $p$-adic units. For any local algebra $S_p$ split by $K_P/k_p$ we consider the possible crossed product representation

$$(1) \qquad S_p = (K_P/k_p, \Delta(P), F)$$

in which $F = F_{\zeta,\eta}$ denotes now a factor set defined for the elements $\zeta$, $\eta$ in the Galois group $\Delta(P) = \Delta$ of $K_P/k_p$. Since the invariant $\mu$ of this algebra is

[28] The finiteness $[F':F'']$ will be proved later, in Theorem 13.1.

an element of an additive cyclic group, the class group of these algebras is cyclic of order $m_p = m = [K_P : k_p]$. Consider now only those factor sets $F$ which consist of $P$-adic units.

THEOREM 12.1. *The p-adic algebra classes $S_p$ which have a crossed product representation* (1) *with a factor set $FE_P$ consisting of P-adic units $E_{\zeta,\eta}$ form a cyclic group of order $e_p$, where $e_p$ is the ramification order of $K_P/k_p$.*

**Proof.** If $K_p$ is unramified over $k_p$, $e = e_p = 1$, and the theorem follows readily. For $\Delta = \{\delta\}$ is then a cyclic group, so the invariant $\mu(S_p)$ can be computed as in (10) of §2. The result is a sum of terms $V_P[E_{\delta^i,\delta}]$ which are all zero because the $P$-adic order of a unit $E_{\delta^i,\delta}$ is zero. Since the invariant is zero, the algebra $S_p \sim k_p$, as asserted. In the general case the maximal unramified subfield $W$ of $K_P$ has over $k_p$ a degree $f = m/e$. Any algebra $S_p$ has as index a divisor of $m$, and the index is the same as the exponent of $S_p$ in the group of algebra classes. Hence the index of the power $S_p^e$ is a divisor of $m/e$. This means that $S_p^e$ has $W/k_p$ as splitting field, so that $S_p^e$ is similar to some crossed product of $W$. By a formula due to Witt [41], one can explicitly calculate this representation of $S_p^e$. If $\Omega$ is the subgroup of $\Delta$ corresponding to $W$ according to the Galois theory, the extension $W/k_p$ has the factor group $\Delta/\Omega$ as Galois group. If for each coset $\eta\Omega$ of this factor group a representative $\eta'$ in $\Delta$ is selected, Witt showed that

$$S_p^e = (K_P, \Delta, FE_P)^e \sim (W/k_p, \Delta/\Omega, B) \tag{2}$$

where the factor set $B$ consists of quantities given in terms of $FE_P = E_{\zeta,\eta}$ as

$$B_{\zeta\Omega,\eta\Omega} = \prod_{\omega}^{\omega} E_{\zeta',\eta'} E_{\omega,\zeta'\eta'} E_{\omega,(\zeta\eta)'}^{-1} \qquad \text{(over all } \omega \text{ in } \Omega\text{)}.$$

For our purpose we need only note that if the original factor set $FE_P$ consists of units, then this derived factor set will also consist of units. By the computation already made for the unramified case, the algebra $(W, \Delta/\Omega, B)$ of (2) is then similar to $k_p$, so that $S_p^e \sim k_p$. In the group of all algebras with factor sets of units any algebra thus has order at most $e$. This group must be cyclic by the remark at the beginning of this section. Consequently to complete the proof of the present theorem we need only show that some algebra with factor set of units has order at least $e$. In the whole (cyclic) group of all local algebras $S_p$ there is one algebra of order $m = ef$. Hence it will suffice to show that the $f$th power of this algebra has a factor set of units. This is indeed the case, as we shall prove in

THEOREM 12.2. *Any factor set $F$ for $K_P/k_p$ has its fth power $F^f$ similar to a factor set of units.*

**Proof.** The integer $f = m/e$ can be described as the inertial degree of $K_p$

over $k_p$. If the factor set $F$ does not already consist of $P$-adic units, denote by $e_{\zeta,\eta}$ the $P$-adic orders $V_P[F_{\zeta,\eta}]$ of its elements. The associativity relations

$$F_{\zeta,\eta}F_{\zeta\eta,\xi} = F_{\eta,\xi}^{\zeta}F_{\zeta,\eta\xi},$$

if multiplied over all values of $\zeta$ (in $\Delta$), yield for the $e$'s the relations

$$b_\eta + b_\xi = me_{\eta,\xi} + b_{\eta\xi}. \tag{3}$$

Here $b_\eta$ denotes the $P$-adic order $V_P(B_\eta)$ of a vector $B_\eta$, with

$$B_\eta = \prod_\zeta F_{\zeta,\eta}, \qquad C_\zeta = \prod_\eta F_{\zeta,\eta}.$$

For these two vectors the associativity relations, multiplied over all values of $\eta$, yield

$$C_\zeta B_\xi = B_\xi^\zeta C_\zeta,$$

which is to say that $B_\xi^\zeta = B_\xi$. The invariant element $B_\xi$ must therefore lie in the subfield $k_p$, which implies in turn that its $P$-adic order $b_\xi$ is a multiple of the ramification order $e$. Hence $b_\xi = ea_\xi$ for a suitable integer $a_\xi$, and (3) can be rewritten as

$$fe_{\eta,\xi} = a_\eta + a_\xi - a_{\eta\xi}.$$

If $A_\zeta$ is a vector of elements of the respective orders $-a_\zeta$, this means that

$$(F_{\eta,\xi})^f TA_\zeta$$

will be a factor set each of whose elements has $P$-adic order zero (i.e., is a $P$-adic unit). In other words $F^f$ is similar to a factor set of $P$-adic units, as asserted.

If $p$ is an infinite prime divisor, Theorem 12.1 still is valid, if we adopt the usual convention as to ramifications at infinity. If $K_P = k_p$, the extension $K_P/k_p$ is, of course, unramified, and $e_p = 1$. If $K_P$ is the field of complex numbers, $k_p$ is that of real numbers, then $K_P$ is ramified over $k_p$ with ramification order $e_p = 2$. Theorem 12.1 then holds because the group of algebras $S_p$ over $k_p$ is then generated by the algebra of real quaternions.

13. **Algebras with factor sets relatively prime to** $M$. One of the partial indices in the formulas (5) of §11 is $[F' : F'']$, for the group $F'$ of all factor sets of numbers relatively prime to $M$ and the subgroup $F''$ consisting of those factor sets $F'$ for which $(K, \Gamma, F'')_p \sim k_p$ whenever $p$ is involved in $M$. To reduce this index, we apply the natural homomorphism carrying $F$ into a crossed product

$$F \to S = (K, \Gamma, F). \tag{1}$$

According to Theorem 6.2 we map $F'$ on the group $S_e$, defined by

$S_e$=all normal simple algebras $S/k$ split by $K/k$ such that, whenever $p$ is involved in $M$, $S_p$ has a crossed product representation $(K_P/k_p, \Delta(P), FE_P)$, with a factor set $FE_P$ of $P$-adic units.

The subgroup $F''$ is, by its very definition, the group of those factor sets carried by the homomorphism (1) into algebras $S'$ relatively prime to $M$. Hence, by the isomorphism principle([29]),

$$[F':F''] = [S_e:S']. \tag{2}$$

The index on the right can be computed in terms of the behaviour of local algebras $S_p$ at the ramified prime divisors. Let us use the following notation:

(*13.1) $p_1, p_2, \cdots, p_t$ all (finite and infinite) prime divisors of $k$ which are ramified in $K$,

(*13.2) $e_i$=the ramification order of a divisor $P_i$ of $p_i$,

(*13.3) $m_i=[K_{P_i}:k_{p_i}]$=the local $p_i$-degree of $K/k$.

Then $e_i \mid m_i$ and $m_i \mid n$ ($n/m_i$ is the number of distinct prime factors of $p$).

THEOREM 13.1. *The index* $[F':F'']$ *may be computed in terms of invariants of* $K/k$ *as*

$$[F':F''] = n^{-1}(n, J(\Gamma)n/e_1, \cdots, J(\Gamma)n/e_t)\prod_p e_p, \tag{3}$$

*where the product is taken over all (finite and infinite) ramification divisors of* $K/k$, *while* $J(\Gamma)$ *is the least common multiple of the orders of the elements of the Galois group* $\Gamma$ *of* $K/k$.

For a proof we appeal to the local invariants of the algebras $S_e$. If $p_i$ is a ramified prime divisor, the component $S_p$ of an algebra in $S_e$ has by definition a factor set of $P_i$-adic units. In the group of all algebra classes split by $K_P/k_p$, $S_P$ consequently has an order which divides $e_i$ (Theorem 12.1). The integral invariant of $S$ at $p_i$ thus equals([30]) $\mu_i(S)=x_i(n/e_i)$, where $x_i$ is an integer which is uniquely determined mod $e_i$. We map the group $S_e$ on a vector group of these invariants,

$$X = (x_1, x_2, \cdots, x_t), \qquad nx_i = e_i\mu_i(S). \tag{4}$$

---

([29]) This equation may also be viewed as follows. The homomorphism which carries a factor set $F$ into an algebra $S$ is in effect the reduction of the group of factor sets modulo the transformation sets. The group of algebras $S_e$ obtainable from $F'$ is therefore isomorphic with $F'/(TA \cap F')$. Similarly, $S'$ is isomorphic with $F''/(TA \cap F'')$. But the intersections $TA \cap F'$ and $TA \cap F''$ are identical, for a transformation set $TA$ which is relatively prime to $M$ will necessarily determine a total matric algebra. Hence it will lie in $F''$. Consequently $[S_e:S'] = [F'/(TA \cap F'):F''/(TA \cap F')] = [F':F'']$.

([30]) For simplicity we write the local algebra $S$ and the invariant $\mu$ with $i$ instead of $p_i$ as subscript.

For all the unramified prime divisors $p$ which are involved in $M$ we have $S_p \sim k_p$. Hence an algebra $S$ of $S_e$ belongs to the subgroup $S'$ if and only if each $S_i \sim k_i$; that is, if and only if the vector $X$ of invariants corresponding to $S$ has the form

$$Y = (y_1 e_1, y_2 e_2, \cdots, y_t e_t),$$

with invariants $\mu_i(S) = y_i e_i (n/e_i) \equiv 0 \pmod{n}$. Therefore our index becomes

$$[F' : F''] = [S_e : S'] = [X : Y].$$

If we introduce the group of all vectors

$$Z = (z_1, z_2, \cdots, z_t) \quad \text{(each } z_i \text{ a rational integer)},$$

this index will become

$$[F' : F''] = [Z : Y]/[Z : X] = \prod_p e_p/[Z : X], \tag{5}$$

where the product is taken over all prime divisors of $k$.

It remains only to compute the index $[Z : X]$, which measures how many of the *a priori* conceivable sets of invariants $z_i$ are possible for an actual algebra $S$. The only condition on the invariants of an algebra $S$ is the sum relation (see [22]),

$$0 \equiv \sum_p \mu_p(S) \equiv \sum_{i=1}^{t} \mu_i(S) + \sum_q \mu_q(S) \equiv \sum_{i=1}^{t} x_i(n/e_i) + \sum_q \mu_q(S) \pmod{n}, \tag{6}$$

where $q$ runs over all prime divisors distinct from $p_1, \cdots, p_t$. The invariants $\mu_q(S) = \mu_q$ can be considered as the invariants of an ideal algebra $\mathfrak{S}$ which is unramified at every $p_i$ $(i = 1, 2, \cdots, t)$, but which otherwise has the same components as does $S$. We have

LEMMA 1. *An integer $r$ can be the sum $\sum_p \mu_p(\mathfrak{S}')$ of the invariants of an ideal algebra $\mathfrak{S}'$ if and only if $J(\Gamma) r \equiv 0 \pmod{n}$.*

**Proof.** In establishing Theorem 4.1 we showed that any $r$ satisfying the above condition is the invariant sum of a suitable ideal algebra $\mathfrak{S}'$. Conversely, an invariant $\mu_p(\mathfrak{S}')$ for an unramified $p$ has by definition (see §2, (3)) the form $sn/m_p$, where $s$ is an integer and $m_p$ is the order of a corresponding Frobenius automorphism. Since $m_p \mid J(\Gamma)$ we have $J(\Gamma)\mu_p(\mathfrak{S}') \equiv 0$, and $J(\Gamma)\sum_p \mu_p(\mathfrak{S}') \equiv 0 \pmod{n}$.

LEMMA 2. *A set of integers $x_i$ belongs to the group $X$ of* (4) *if and only if $\sum_{i=1}^{t} x_i (J(\Gamma) n/e_i) \equiv 0 \pmod{n}$.*

**Proof.** The relation (6) characterizes the integers $x_i$ by the condition that $-\sum_{i=1}^{t} x_i (n/e_i)$ be congruent, mod $n$, to the invariant sum of an ideal algebra $\mathfrak{S}'$. Lemma 1 now gives the result desired.

By the elementary theory of congruences it is now possible to find a basis for the group $X$. One need only select from those vectors in which the first $i-1$ components are zero a vector $(0, 0, \cdots, 0, x_{ii}, \cdots, x_{it})$ in $X$ with a minimal $i$th component $x_{ii}>0$. The index $[Z:X]$ of (5) is then $\prod_{i=1}^{t} x_{ii}$. This product can be computed as $n$ divided by the greatest common divisor

(*13.4) $n^* = (n, J(\Gamma)n/e_1, \cdots, J(\Gamma)n/e_t)$.

The formula (5) then becomes the assertion (3) of Theorem 13.1.

We pause to discuss the invariant $n^*$ of (*13.4), which appears in the formula (3). Clearly $J(\Gamma) \mid n^* \mid n$. In the definition (*13.4) one may omit any $e_i$ which divides $J(\Gamma)$. Suppose in particular that some $p_i$ has no higher ramification([31]). Then the ramification order $e_i$ is the order of the inertial group of $P_i \mid p_i$, which is cyclic, so certainly $e_i \mid J(\Gamma)$. The formula (*13.4) thus need include only the prime divisors $p_i$ with higher ramification.

THEOREM 13.2. *The invariant of* (*13.4) *satisfies* $n^*=n$ *if and only if the ramification order* $e$ *of every* $p$ *in* $K/k$ *is a divisor of* $J(\Gamma)$. *In particular,* $n^*=n$ *whenever* $J(\Gamma)=n$, *or whenever there is no prime ideal* $p$ *in* $k$ *with higher ramification in* $K$.

THEOREM 13.3. *Let* $l^r$ *be the exact power of a rational prime* $l$ *which divides the degree* $n=[K:k]$, *while* $l^s$ *is the largest power of* $l$ *which occurs as the order of an element in the Galois group* $\Gamma$. *Among the prime ideal divisors* $P$ *of* $l$ *in* $K$ *select one whose Hilbert ramification group* $V_1$ *has as large an order* $l^v$ *as possible. Then the exact power* $l^u$ *of* $l$ *dividing* $n^*$ *is given by*

$$u = r \qquad (\text{if } v < s),$$

$$u = r - (v - s) \qquad (\text{if } v \geqq s).$$

**Proof.** This theorem follows at once from (*13.4), for the ramification order $e$ of a prime ideal which divides the rational prime $l$ has the form $e=e_0 l^v$, where $(e_0, l)=1$, while $l^v$ is the order of the first Hilbert ramification group.

The inequality $n^*<n$ can actually arise, even though an earlier summary of these results ([29]) was based on the assumption $n^*=n$. For a simple explicit example, let $k$ be the field $R$ of all rational numbers, while $K=R(6^{1/2}, 7^{1/2})$ is a quartic field with the four group as Galois group. In each of the three quadratic subfields $R(6^{1/2})$, $R(7^{1/2})$, and $R(42^{1/2})$, the rational prime 2 is ramified, since each field has an even discriminant. It follows that the ideal (2) is totally ramified in $K/R$, for in any other event, $K$ would have a quadratic subfield which is an inertial or decomposition field for (2), counter to the observation above. Since (2) has ramification order 4, while $J(\Gamma)=2$, we conclude by Theorem 13.2 that $n^*=2$, $n=4$.

A more general construction is embodied in

([31]) Each prime factor $P_i$ of $p_i$ has its first ramification group $V_1=1$. See [20, Part Ia, p. 70].

THEOREM 13.4. *Let $l$ be a rational prime which is not totally decomposed in an algebraic number field $k$. Then $k$ has an abelian extension $K$ with a degree $n=l^l\geqq l^3$ such that the invariant $n^*$ is at most $l^2$.*

**Proof.** The local class field theory [9] may be used to construct an abelian extension of type $(l, l, \cdots, l)$ with sufficiently complicated ramifications. By hypothesis, $l$ has in $k$ some prime factor $p$ with a local degree $n_p=[k_p:R_l]\geqq 2$. Consider the corresponding group $k_p^*/k_p^{*l}$. This group can be explicitly expressed by using a basis of the units in $k_p$. In the regular case, when $k_p$ contains no primitive $l$th roots of unity, the group $k_p^*/k_p^{*l}$ is abelian of type $(l, l, \cdots, l)$, with $n_p+1$ generators. In the irregular case, when $k_p$ contains all $l$th roots of unity, the group $k_p^*/k_p^{*l}$ is abelian of type $(l, l, \cdots, l)$ with $n_p+2$ generators. (See [18] and [24].) In either event the existence theorem of local class field theory asserts that $k_p$ has an abelian extension $A_p$ with a Galois group isomorphic with $k_p^*/k_p^{*l}$. The degree of this extension is at least $l^{n_p+1}\geqq l^3$, since by hypothesis $n_p\geqq 2$. In $A_p/k_p$, the Galois group modulo the inertial group is cyclic, consequently it has order at most $l$. By Grunwald's existence theorem [16], the local extension $A_p/k_p$ can be obtained from infinitely many abelian extensions $A/k$ with the same Galois groups as $A_p/k_p$. The invariant $n^*$ of (7) is then $n^*\leqq(n, J(\Gamma)n/e)\leqq(n, ll)=l^2$, as asserted.

These examples may be combined to give the following conclusion:

THEOREM 13.5. *Over any algebraic number field $k$ there is a normal (abelian) extension $K$ with*[32] $n^*<n$.

14. **Algebras with given local components.** The questions raised in §13 as to the existence of local algebras with specified local components suggest an analogous inquiry: when is a given local algebra a component of an actual algebra? This leads to a certain index $[\mathfrak{S}^{(p)}:S^{(p)}]$, analogous to the main index $[\mathfrak{S}':S']$, where

(*14.1) $\mathfrak{S}^{(p)}$ = the group of classes of normal simple algebras $S^{(p)}$ split by $K_P/k_p$,

(*14.2) $S^{(p)}$ = the group of those algebras $\mathfrak{S}^{(p)}$ which are components of some $S$ split by $K/k$.

If $p$ is unramified, the invariant of $\mathfrak{S}^{(p)}$ has the form $\mu_p(\mathfrak{S}^{(p)})\equiv x(n/m_p) \pmod n$. By the Tschebotareff density theorem we know that $m_p=m_q$ for at least one other unramified prime ideal $q$ of $k$. There is thus a local algebra $S_q$ with an invariant $\mu_q(S_q)\equiv -x(n/m_q) \pmod n$. These two invariants add up to $\mu_q(S_q)+\mu_p(\mathfrak{S}^{(p)})\equiv 0 \pmod n$, so there is an actual algebra $S$ with $\mathfrak{S}^{(p)}$ and $\mathfrak{S}_q$ as its only non-trivial components. Therefore $S^{(p)}=\mathfrak{S}^{(p)}$ for any unramified $p$.

Consider next the $t$ ramified prime divisors $p_i$ with associated decomposi-

---

[32] For the existence of suitable primes $l$ consult the density theorems. See [20, Part II].

tion groups of order([33]) $m_i$. The invariants of an actual algebra $S$ must satisfy the relation

$$\mu_i(S) + \sum_{j\neq i,\, j=1}^{t} \mu_j(S) + \sum_{q} \mu_q(S) \equiv 0 \pmod{n} \qquad (q \neq p_1, \cdots, p_t).$$

The terms here can be arbitrary multiples of $n/m_i$, $n/m_j$, and $n/m_q$ respectively. The possible values for $\mu_i(S)$ are then found by elementary number theory.

THEOREM 14.1. *At an unramified prime divisor $p$ every local algebra $S_p$ split by $K_P/k_p$ is a component([34]) $(S)_p$ of an algebra $S$ split by $K/k$, while at a ramified prime divisor $p=p_i$ of $p$-degree $m_i$ $(i=1, \cdots, t)$ the index of the group $S^{(p)}$ in $\mathfrak{S}^{(p)}$ is*

$$(1) \qquad [\mathfrak{S}^{(p)}:S^{(p)}] = m_i[(m_i, \bar{n}_i)]^{-1},$$
$$\bar{n}_i = \text{l.c.m.}\ [m_1, \cdots, m_{i-1}, m_{i+1}, \cdots, m_t, J(\Gamma)].$$

*Specifically, a local algebra $S^{(p)}$ is a component $(S)_p$ of some $S$ if and only if its invariant satisfies the condition*

$$(m_i, \bar{n}_i)\mu(S^{(p)}) \equiv 0 \pmod{n}.$$

That the indices (1) are drastically limited is indicated by the following calculation. In $[\mathfrak{S}:S]$ introduce as an intermediate group the composite $S\mathfrak{S}'$ and apply the reduction principle (2) of §9. Then

$$(2) \qquad [\mathfrak{S}:S] = [\mathfrak{S}:\mathfrak{S}'S][\mathfrak{S}'S:S] = [\mathfrak{S}:\mathfrak{S}'S][\mathfrak{S}':S'].$$

The second index was computed in Theorem 4.1 to be $J(\Gamma)$. The first index may be transformed by the homomorphism which carries each ideal algebra $\mathfrak{S}$ into the vector $\{(\mathfrak{S})_1, \cdots, (\mathfrak{S})_t\}$ of its components $(\mathfrak{S})_i$ at the ramified prime divisors $p_i$. Under this homomorphism each algebra of the join $\mathfrak{S}'S$ goes into the vector of components $\{(S)_1, \cdots, (S)_t\}$ of the actual algebra $S$. Hence, by the isomorphism principle,

$$[\mathfrak{S}:\mathfrak{S}'S] = [\{(\mathfrak{S})_1, \cdots, (\mathfrak{S})_t\}:\{(S)_1, \cdots, (S)_t\}].$$

On the right we obtain a larger group if we allow distinct $(S)_i$'s to arise from different algebras $S$. The group index is then that for a direct product, so that

$$[\mathfrak{S}:\mathfrak{S}'S] \geqq \prod_{i=1}^{t} [\mathfrak{S}^{(p_i)}:S^{(p_i)}] = \prod_{i=1}^{t} m_i/(m_i, \bar{n}_i).$$

If in (2) $[\mathfrak{S}:S]=N$ and $[\mathfrak{S}':S']=J(\Gamma)$ are evaluated as in Theorems 4.2 and 4.1, we obtain

([33]) Notation as in (*13.1).

([34]) For the time being, we denote the $p$-component of an actual algebra $S$ by $(S)_p$.

THEOREM 14.2. *The local algebra indices of* (1) *are limited by*

$$\prod_{i=1}^{t} [\mathfrak{S}^{(p_i)}:S^{(p_i)}] \leqq N/J(\Gamma). \tag{3}$$

*However, these local indices are not necessarily all* 1.

THEOREM 14.3. *Over any algebraic number field $k$ there is an (abelian) normal extension $K$ for which $[\mathfrak{S}^{(p)}:S^{(p)}]>1$ for at least one prime divisor $p$.*

**Proof.** If $k$ is not the rational number field, there is at least one([35]) rational prime $l$ which has in $k$ a prime ideal divisor $p$ of absolute local degree greater than 1. We assert then that $[\mathfrak{S}^{(p)}:S^{(p)}]>1$. As in Theorem 13.4, the local class field theory gives an extension $A_P/k_p$ which is abelian of type $(l, l, \cdots, l)$ with at least three generators. According to the Grunwald existence theorem there is a field $A/k$ with the same Galois group as $A_P/k_p$ which has at $p$ the local component $A_P/k_p$ and which has at each other prime ideal divisor $q$ of $l$ some specified local component $A_Q/k_q$ of degree (say) $l^2$. Then in the index $[\mathfrak{S}^{(p)}:S^{(p)}]$ of (1), the $p$-degree $m_1$ corresponding to $p_1=p$ is at least $l^3$. If any $q=q_i$ is ramified, the corresponding degree $m_i$ is at most $l^2$, by construction. Finally, if there is a ramified $p_j$ not a divisor of $l$, this $p_j$ cannot have higher ramifications because the degree of the extension $A/k$ is a power of $l$. By the Hilbert theory, the $p_j$-degree $m_j$ can then be at most $l^2$. In (1), each degree $m_i$ (with $i\neq 1$) is at most $l^2$, while $J(\Gamma)$ is $l$. It follows that $[\mathfrak{S}^{(p)}:S^{(p)}]\geqq l$.

It remains to consider the case when $k=R$, the field of rational numbers. The extension $K=R(2^{1/2}, (-1)^{1/2}, 5^{1/2})$ is abelian of type (2, 2, 2). The prime ideal (2) of $R$ is ramified in six of the quadratic subfields of $K$, while in the seventh field $R(5^{1/2})$ it is inert. By the Hilbert theory it follows that $(2)=P^4$ in $K$. Therefore the degree $m_1$ corresponding to $p_1=(2)$ is $m_1=8$, any $q\neq 2$ in $R$ has no higher ramifications, hence has degree $m_q$ at most 4. By formula (1) it follows that([36]) $[\mathfrak{S}^{(p)}:S^{(p)}]\geqq 2$.

Certain properties of the norm residue symbol([37]) suggest also the consideration of algebras with unit factor sets

$\mathfrak{U}^{(p)}$ = the group of classes of algebras $\mathfrak{S}^{(p)}$ with factor sets of $P$-adic units.

By Theorem 12.1 the group $\mathfrak{U}^{(p)}$ has order $e_p$. As in Theorem 6.2 one may prove

THEOREM 14.4. *An algebra $S$ has its $p$-component in $\mathfrak{U}^{(p)}$ if and only if $S$ has a crossed product representation with a factor set $F$ of numbers relatively prime to $p$.*

([35]) For example, one might select any $l$ which is ramified in $k/R$.

([36]) The extension $K$ might also have been constructed by local class field theory. Indeed, 2, $-1$, and 5 are the generators of the factor group $R_2^*/R_2^{*2}$ in the dyadic field $R_2$.

([37]) See Chapter V, §27, Theorem 27.4.

The previous methods also enable us to determine when a local algebra $\mathfrak{U}^{(p)}$ with an invariant $x[n/e_p]$ (mod $n$) can be realized as the component of an actual algebra $S$.

THEOREM 14.5. *At a ramified prime divisor $p=p_i$ the number of algebras $\mathfrak{U}_i=\mathfrak{U}^{(p_i)}$ which cannot be realized as components $S_i=S^{(p_i)}$ of an actual algebra $S$ is given by*

$$[\mathfrak{U}_i:\mathfrak{U}_i \cap (S)_i] = e_i/(e_i, \bar{n}_i), \tag{4}$$

*where $\bar{n}_i$ is determined*(38) *as in* (1); $i=1, 2, \cdots, t$.

By the devices used in the proof of Theorem 14.3 one may demonstrate that this index necessarily exceeds 1 if $p$ is a prime divisor of $k$ of absolute degree at least 3, and if $K$ is suitably constructed.

15. **An invariant of a group pair.** For the convenient statement of subsequent results we need a certain "*deficiency*" invariant for homomorphisms of groups. Consider any abelian group $R$ for which $\Gamma$ is a group of operators, with a $\Gamma$-allowable subgroup $S$(39), and

(1) $\mathfrak{R} = R/S$, a group with operators in $\Gamma$,

(2) $\phi$, the natural homomorphism of $R$ on $R/S = R\phi$,

(3) $\mathfrak{E}(R) = G$, a group extension of $R$ by $\Gamma$.

Since $S$ is a $\Gamma$-allowable subgroup of $R$, it follows that $S$ is a normal subgroup of the extension $G$, so that the quotient group $G/S$ is a group extension of $R/S$ by $\Gamma$. The set of all such extensions $G\phi=G/S$ forms a subgroup of the group of all extensions of $\mathfrak{R}$ [6, 43]:

(4) $\mathfrak{E}(\mathfrak{R}) = \mathfrak{G}$, a group extension of $\mathfrak{R}$ by $\Gamma$.

The index of this subgroup in $G$ is our deficiency index.

DEFINITION. *If the homomorphism $\phi$ of $R$ has $S$ as the subgroup of elements mapped into* 1, *the deficiency of $R$ modulo $S$ is*

$$(*15.1)\quad \omega(R, S) = [\mathfrak{E}(R\phi): \{\mathfrak{E}(R)\}\phi].$$

The special extensions $G\phi$ may also be described in the following terms, due essentially to A. H. Clifford. Given an extension $G$ of $R$, an extension $\mathfrak{G}$ of $\mathfrak{R}$ by the same group $\Gamma$, and a homomorphism $\phi$ of $R$ to $\mathfrak{R}$, we say that $G$ is a $\phi$-prolongation of $\mathfrak{G}$ by $S$ if and only if the homomorphism $\phi$ can be so extended to a homomorphism of $G$ to $\mathfrak{G}$ that the subgroup of those elements of $G$ mapped into 1 is exactly the given subgroup $S$ of $R$. The extensions $G\phi$

(38) For the notation see the preceding developments.

(39) That is; $s^\sigma$ is in $S$ for every $s$ in $S$ and $\sigma$ in $\Gamma$.

of our definition can then be characterized as those extensions $\mathfrak{G}$ of $\mathfrak{R}$ which admit a $\phi$-prolongation by $S$. The problem of prolonging a given group $\mathfrak{G}$ by $S$ may also be described as the problem of superimposing two group pairs,

$$\mathfrak{G} \supset \mathfrak{R} \supset 1, \qquad R \supset S \supset 1, \qquad R/S = \mathfrak{R},$$

in such a fashion that they "overlap" properly in a combined group

$$G \supset R \supset S \supset 1, \qquad G/S = \mathfrak{G} \text{ extending } R/S = \mathfrak{R}.$$

This combined group may be viewed as a specially restricted extension of $S$ by $\mathfrak{G}$, where $S$ is considered as a group with operators in $\mathfrak{G}$ according to the natural rule $S^{u_\sigma} = S^\sigma$ for all elements $u_\sigma$ in a coset $\sigma$ of $\mathfrak{G}/\mathfrak{R}$.

In less invariant fashion, the same deficiency index may be described in terms of factor sets. If $R_{\sigma,\tau}$ is a factor set $FR$, then the elements $(R_{\sigma,\tau})\phi$ constitute a factor set for $R\phi = \mathfrak{R}$.

THEOREM 15.1. *The deficiency index, in terms of factor sets, is*

$$\omega(R, S) = [F(R\phi) : (FR)\phi], \tag{5}$$

*provided one of these indices is finite.*

**Proof.** Each factor set $F(R\phi)$ determines in the usual manner a group extension $\mathfrak{G} = (R\phi, \Gamma, F(R\phi))$, while a factor set $(FR)\phi$ yields under this map one of the "prolongable" extensions $G\phi = (R, \Gamma, FR)\phi$. We shall have proven (5) in accordance with the isomorphism principle of group theory, provided we show conversely that

$$(R\phi, \Gamma, F(R\phi)) = G\phi \quad \text{implies} \quad F(R\phi) = (FR)\phi.$$

Now $G$ is given by a factor set as $G = (R, \Gamma, FR)$, so $G\phi$ also has the factor set $(FR)\phi$. The sets $F(R\phi)$, $(FR)\phi$ thus determine the same extension of $\mathfrak{R}$, hence are similar,

$$F(R\phi) = (FR)\phi[\mathfrak{R}_\sigma \mathfrak{R}_\tau^\sigma \mathfrak{R}_{\sigma\tau}^{-1}].$$

The transformation set $T\mathfrak{R}_\sigma$ can clearly be written as the homomorphic image of a transformation set $TR_\sigma$, where $R_\sigma$ is chosen in the coset $\mathfrak{R}_\sigma$. Hence

$$F(R\phi) = \{(FR)[R_\sigma R_\tau^\sigma R_{\sigma\tau}^{-1}]\}\phi,$$

as required for our proof.

16. **Factor sets of principal ideals.** In the formulas of §11, there appears the index $[F\mathfrak{A}' : (F')]$, known to be finite. Between these two groups we may insert the group $F(A')$ of factor sets of principal ideals. This group need not be the same as the group $(F') = (FA')$ of principal ideals derived from factor sets of numbers. In fact, the index of $(F')$ in $F(A')$ is exactly a deficiency index, in the sense of §15, for the homomorphism $A' \to (A')$ belonging to the subgroup $E$ of units; or

$$[F(A'):(F')] = [F(A'):(FA')] = \omega(A', E), \tag{1}$$

$$[F\mathfrak{A}':(F')] = [F\mathfrak{A}':F(A')]\omega(A', E). \tag{2}$$

The first index here suggests the use of the group of ideal classes in $K$. Specifically, set

(*16.1) $\mathfrak{A}^\sharp$ = the ideal class determined by the ideal $\mathfrak{A}$.

Then $\mathfrak{A}^\sharp$ will also, as usual, denote the (finite) group of all ideal classes in $K$. Applying to part of (2) the homomorphism $\mathfrak{A}\to\mathfrak{A}^\sharp$, we have

$$[F\mathfrak{A}':F(A')] = [(F\mathfrak{A}')^\sharp:1] = [F\mathfrak{A}'^\sharp:1][F\mathfrak{A}'^\sharp:(F\mathfrak{A}')^\sharp]^{-1}. \tag{3}$$

The second index is by definition a deficiency index

$$\omega(\mathfrak{A}', (A')) = [F\mathfrak{A}'^\sharp:(F\mathfrak{A}')^\sharp] = [F\mathfrak{A}^\sharp:(F\mathfrak{A}')^\sharp], \tag{4}$$

for $\mathfrak{A}^\sharp = \mathfrak{A}'^\sharp$. The first index $[F\mathfrak{A}'^\sharp:1]$ may be reduced to group extensions,

$$[F\mathfrak{A}^\sharp:1] = [F\mathfrak{A}^\sharp:T\mathfrak{A}^\sharp][T\mathfrak{A}^\sharp:1]. \tag{5}$$

The homomorphism which carries a vector of classes $\mathfrak{A}_\sigma^\sharp$ into a transformation set $T\mathfrak{A}^\sharp$ will introduce the group of crossed characters $U\mathfrak{A}^\sharp$, as

$$\begin{aligned}[T\mathfrak{A}^\sharp:1] &= [\mathfrak{A}_\sigma^\sharp:1][U\mathfrak{A}^\sharp:1]^{-1} \\ &= [\mathfrak{A}^\sharp:1]^n[U\mathfrak{A}^\sharp:\mathfrak{A}^{\sharp 1-\sigma}]^{-1}[\mathfrak{A}^{\sharp 1-\sigma}:1]^{-1}.\end{aligned}$$

The index $[\mathfrak{A}^\sharp:1]$ is the class number $H$, while the homomorphism $\mathfrak{A}^\sharp\to\mathfrak{A}^{\sharp 1-\sigma}$ will give

$$[T\mathfrak{A}^\sharp:1] = H^{n-1}[U\mathfrak{A}^\sharp:\mathfrak{A}^{\sharp 1-\sigma}]h. \tag{6}$$

The results (2) through (6) may now be combined as

THEOREM 16.1. *In terms of the group $\mathfrak{A}^\sharp$ of ideal classes in $K$ and the deficiency index $\omega$ of* §15, *we may write*

$$\begin{aligned}[F\mathfrak{A}':(F')] &= H^{n-1}h\omega(A', E)[\omega(\mathfrak{A}', (A'))]^{-1}[J(\mathfrak{A}^\sharp)]^{-1}, \\ J(\mathfrak{A}^\sharp) &= [U\mathfrak{A}^\sharp:\mathfrak{A}^{\sharp 1-\sigma}][F\mathfrak{A}^\sharp:T\mathfrak{A}^\sharp]^{-1}.\end{aligned} \tag{7}$$

In this formula there appear two indices $\omega$ depending on the module $M$. We inquire now how each depends on the nature of $M$.

THEOREM 16.2. *The index $\omega(\mathfrak{A}', (A'))$ is independent of the choice of the module $M$, provided only that this module involves all ramified prime divisors for $K/k$.*

**Proof.** We may consider two such modules $M_1$ and $M$ with $M_1 | M$. The respective indices are (4) and

$$\omega(\mathfrak{A}_1', (A_1')) = [F\mathfrak{A}_1^{\sharp}:(F\mathfrak{A}_1')^{\sharp}],$$

where $\mathfrak{A}_1'$ $(A_1')$ are ideals (elements) relatively prime to $M_1$. Hence the conclusion of the theorem will follow if we prove $(F\mathfrak{A}_1')^{\sharp}=(F\mathfrak{A}')^{\sharp}$. This will be the case provided the factor set $F\mathfrak{A}_1'$ can be turned into a factor set relatively prime to $M$ by multiplication with a suitable factor set of principal ideals, as asserted in the following lemma:

LEMMA 1. *If $p$ is unramified in $K/k$ and $\mathfrak{F}$ is a $p$-primary factor set of ideals in $K$, there exists another factor set $\mathfrak{F}_1$ relatively prime to any specified module such that $\mathfrak{F}\mathfrak{F}_1$ is a factor set of principal ideals.*

**Proof.** Our chief concern is to show that $\mathfrak{F}_1$ can be chosen so as to be a factor set. Select $P$, a prime factor of $p$ with the decomposition group $\Delta(P)$, and let $L$ be the corresponding decomposition field in $K/k$. Since $P$ is unramified the ideal $P$ is present[40] in $L$. There is then in $L$ an ideal $\mathfrak{C}$ relatively prime to $M$ such that $P\mathfrak{C}$ is principal. Furthermore $\mathfrak{C}$, like all the elements of $L$, is invariant under all automorphisms $\delta$ of the group $\Delta(P)$. Because of this invariance, we can, in an unambiguous fashion, set up the following extension of the correspondence $\Psi(P)=\mathfrak{C}$ to all $p$-primary ideals (see §5). If $\mathfrak{A}=\prod_{\sigma}P^{a_\sigma\sigma}$, let

$$\Psi(\mathfrak{A}) = \prod_{\sigma} \mathfrak{C}^{a_\sigma\sigma}.$$

For arbitrary $p$-primary ideals $\mathfrak{A}$, $\mathfrak{B}$ this function has, according to its origin, the properties

(8) $\Psi(\mathfrak{A})$ is relatively prime to $M$, $\mathfrak{A}\Psi(\mathfrak{A})$ is principal,

(9) $$\Psi(\mathfrak{A}\mathfrak{B}) = \Psi(\mathfrak{A})\Psi(\mathfrak{B}), \qquad \Psi(\mathfrak{B}^{\tau}) = [\Psi(\mathfrak{B})]^{\tau},$$

for every $\tau$ in $\Gamma$. In other words, the mapping $\mathfrak{A}\to\Psi(\mathfrak{A})$ is an operator homomorphism of the group $\mathfrak{A}^{(p)}$ of $p$-primary ideals on a subgroup of the group $\mathfrak{A}'$. It follows that the map $\Psi(\mathfrak{F})$ of a $p$-primary factor set will be itself a factor set. Consequently, the product $\mathfrak{F}\Psi(\mathfrak{F})$ will be a factor set of principal ideals, as asserted in the lemma.

The dependence of the other deficiency index of (7) on $M$ is exhibited by

(10) $$M \mid M_1 \quad \text{implies} \quad \omega(A_1', E) \leqq \omega(A', E).$$

For, the index $\omega(A', E)$ of (1) involves the subgroup $(FA')$, which may be written as the intersection $(FA')=(FA)\cap F(A')$, since a factor set of principal ideals is relatively prime to $M$ if and only if the generators of the ideals are relatively prime to $M$. Hence

(40) Subject to the usual convention that an ideal in $L$ is to be identified with its extended ideal in $K$.

$$\omega(A', E) = [F(A') : (FA) \cap F(A')] = [(FA)F(A') : (FA)]. \tag{11}$$

In this form the conclusion (10) is immediate. It implies that $\omega(A', E)$ is eventually independent of the module $M$. In order to obtain a more precise result we must employ a roundabout method.

THEOREM 16.3. *The index $\omega(A', E)$ is independent of the module $M$, provided only that this module $M$ involves all ramified prime divisors of $K/k$.*

**Proof.** If the formula (11) is substituted in the final formula (5) of Theorem 11.2 for the basic index $J$, one obtains a relation (see (15) below) between various indices which are all independent of the module $M$, with the exception of the indices $\omega(A', E)$, $\omega(\mathfrak{A}', (A'))$, and $[F' : F'']$. The latter index was shown in Theorem 13.1 to be independent of $M$, while we have just shown that the index $\omega(\mathfrak{A}', (A'))$ is independent of a module $M$ of the type under consideration. This gives the result of Theorem 16.3.

THEOREM 16.4. *If $K/k$ is a normal extension such that $K$ and all subfields $L$ over which $K$ is cyclic have class number* 1, *then $\omega(A', E) = 1$.*

**Proof.** The proof of the theorem depends on a choice of special prime elements in $K$. Let $p$ be an unramified prime ideal for $K/k$, $\mathfrak{A}^{(p)}$ the group of $p$-primary ideals in $K$, $P$ a typical prime divisor of $p$ in $K$, $\Delta = \{\delta\}$ the associated decomposition group. Then $P$ is an ideal of the decomposition field $L_\Delta$, over which $K$ is a cyclic extension. By hypothesis $L_\Delta$ has class number 1, hence

$$P = (\pi), \qquad \text{with } \pi \text{ in } L_\Delta \text{ and } \pi^\delta = \pi. \tag{12}$$

Next write $\Gamma$ in terms of cosets

$$\Gamma = \sigma_1\Delta + \sigma_2\Delta + \cdots + \sigma_g\Delta, \qquad g = [\Gamma : \Delta].$$

The prime ideal factorization of $p$ in $K$ is given as

$$p = \prod_{i=1}^{g} P^{\sigma_i}, \qquad P^{\sigma_i\delta} = (P^\delta)^{\sigma_i} = P^{\sigma_i}. \tag{13}$$

Now select for each prime ideal $P^{\sigma_i} = P_i$ the prime element $\pi^{\sigma_i} = \pi_i$ as generator, $P_i = (\pi_i)$ in $K$. Let $\Pi^{(p)}$ be the group of power products of all the prime elements $\pi_i$. By construction $\mathfrak{A}^{(p)}$ and $\Pi^{(p)}$ are groups with $\Gamma$ as operator group. We assert that they are operator isomorphic with respect to $\Gamma$. For the proof we use the correspondence

$$\pi_1^{a_1} \cdots \pi_g^{a_g} \to (\pi_1^{a_1} \cdots \pi_g^{a_g}) = P^{a_1\sigma_1} \cdots P^{a_g\sigma_g}. \tag{14}$$

We have to investigate the effect of an element $\sigma$ in $\Gamma$. By the coset decomposition of $\Gamma$, we get $\sigma = \sigma_i\delta$, $\sigma\sigma_j = \sigma_{j'}\delta_j$, where $\delta_j$ in $\Delta$ and $j'$ in $\{1, \cdots, g\}$ are both determined by $j$. Consequently

$$\left(\prod_{j=1}^{g} \pi_j^{\sigma_j a_j}\right)^{\sigma} = \prod_{j=1}^{g} \pi^{\sigma\sigma_j a_j} = \prod_{j=1}^{g} \pi^{\sigma_{j'}\delta_j a_j} = \prod_{j=1}^{g} \pi^{\sigma_{j'} a_j}$$

is an element of $\Pi^{(p)}$. Similarly

$$\left(\prod_{j=1}^{g} P^{\sigma_j a_j}\right)^{\sigma} = \prod_{j=1}^{g} P^{\sigma\sigma_j a_j} = \prod_{j=1}^{g} P^{\sigma_{j'}\delta_j a_j} = \prod_{j=1}^{g} P^{\sigma_{j'} a_j}.$$

Thus the correspondence (14) is an operator isomorphism with $\Gamma$ as allowed set of operators.

Choose now for every $p$ relatively prime to $M$ such a group $\Pi^{(p)}$, and let $B'$ be the group of numbers generated by all groups $\Pi^{(p)}$. Then $\mathfrak{A}'$ is operator isomorphic with $B'$ under the natural extension of the mapping (14). For the proof remark that $\mathfrak{A}'$ is the direct product([41]) of the groups $\mathfrak{A}^{(p)}$. By the correspondence $B' \leftrightarrow (B')$ we map $B'$ in an operator isomorphic fashion in $\mathfrak{A}'$. This rule is, in fact, the rule (14). It is an isomorphism by the behaviour of the exponents. Finally, we remark that every element $A$ in $A'$ has a unique representation $A = EB$ where $E$ is a unit of $K$ and $B$ an element of $B'$. By the prime ideal decomposition of $(A)$ we first determine an element $B$ in $B'$ such that $(B) = (A)$. Then $(AB^{-1}) = 1$, whence $A = BE$ with a unit. This representation is unique, for $A = E_1B_1 = EB$ implies $(B) = (B_1)$ and therefore $B = B_1$ and $E = E_1$. Consequently, $A'$ is equal to the direct product $B' \times E$ with $\Gamma$ as operator group. Therefore by Lemma 2 of §9([42]), $\omega(A', E) = 1$.

To summarize the results thus far obtained, use the basic formula (5) of §11 with the value for $[F\mathfrak{A}' : (F')]$ obtained in Theorem 16.1 and the formula for $[F' : F'']$ obtained in §13. The latter formula involves the product $\prod e_p$ of the ramification orders for all prime divisors $p$. Part of this will cancel against the product $\prod e_p$ over all finite prime divisors, as in (5) of §11. There remains the product $\prod e_{p_\infty}$ over the infinite $p$'s. This is just $2^\rho$, where $\rho$ is the number of infinite prime divisors of $k$ ramified in $K/k$. All told, the basic index $J = J(\Gamma)$ is

$$J = n^* n^{-1} \omega(A', E)\omega(\mathfrak{A}', (A'))^{-1} J(E)\left[J(\mathfrak{A}^{\#})\right]^{-1} 2^{\rho},$$

$$J(E) = [UE : E^{1-\sigma}][FE : TE]^{-1}, \tag{15}$$

$$J(\mathfrak{A}^{\#}) = [U\mathfrak{A}^{\#} : \mathfrak{A}^{\#1-\sigma}][F\mathfrak{A}^{\#} : T\mathfrak{A}^{\#}]^{-1}.$$

## CHAPTER III. FACTOR SETS OF UNITS

17. **The Herbrand unit group.** The analysis of the index $J(E)$ entering in our formula is based on the explicit structure of the group $E$ of units. This in turn depends on the classification of the infinite prime divisors of $k$ and $K$. Recall that a prime divisor $p = p_\infty$ of $k$ is called real or complex according as

([41]) With $\Gamma$ as set of operators.

([42]) Lemma 2 of §9 obviously generalizes to the kind of direct product we consider here.

the corresponding complete field $k_p$ is the real or the complex field (see §2). The infinite prime divisors of $k$ then fall into three classes according to the types of their divisors in $K$ (see [5]):

(1) $p_{\infty,i}$ $(i=1, \cdots, \rho_1)$ real in $k$, with $n$ real divisors in $K$,

(2) $p_{\infty,i}$ $(i=\rho_1+1, \cdots, r_1)$ real in $k$, with $n/2$ complex divisors in $K$,

(3) $p_{\infty,i}$ $(i=r_1+1, \cdots, r_1+r_2)$ complex in $k$, with $n$ complex divisors in $K$.

In each case let $P_{\infty,i}$ be any one prime divisor of $p_{\infty,i}$, while $\Delta(P_{\infty,i})$ is the corresponding decomposition group (composed of all automorphisms of $\Gamma$ which leave fixed the valuation belonging to $P_{\infty,i}$). For a prime divisor of the first or the third type, $\Delta(P_{\infty,i})$ consists only of the identity, and $P_\infty \mid p_\infty$ is said to be *unramified*. For a prime divisor of the second type, $\Delta(P_{\infty,i})$ is a cyclic group of order 2, while $P_\infty \mid p_\infty$ is *ramified*. For all cases, set

(4) $\delta_i$ = the generator of the decomposition group $\Delta(P_{\infty,i})$,

(5) $K_i$ = the decomposition field of $P_{\infty,i}$ (the field left invariant by $\delta_i$).

Then in case (2), $\delta_i$ has order $2=[K:K_i]$, while in cases (1) and (3), $\delta_i=1$ and $K=K_i$.

The unit group of $k$ contains $r=r_1+r_2-1$ independent units $\epsilon_1, \cdots, \epsilon_r$ which, together with a suitable root of unity, generate the whole group of units in $k$. For the same reason there will be a maximum of $R=n\rho_1+(n/2)(r_1-\rho_1)+nr_2-1$ independent units in $K$. Herbrand's generalization of Minkowski's theorem [5, 23, 25, 26] asserts that one can find in $K$ $r+1$ units $H_1, H_2, \cdots, H_{r+1}$ which with their conjugates $H_i^\sigma$ and with the units $\epsilon_1, \epsilon_2, \cdots, \epsilon_r$ will generate a group of units which has finite index in the whole group $E$ of all units in $K$. Furthermore, the multiplicative relations between these units are all consequences of the simple relations[43]

$$H_i^{\delta_i} = H_i, \qquad N_i H_i = 1 \qquad (i = 1, \cdots, r+1), \tag{6}$$

where $N_i$ denotes the relative norm of $K_i/k$. By an Herbrand group $E^*$ of units in $K$ we mean a group generated by such a basis $\epsilon_i$, $H_i$, $H_i^\sigma, \cdots$. In other words, $E^*$ is a direct product

$$E^* = \epsilon_1 \times \cdots \times \epsilon_r \times H_1 \times \cdots \times H_{r+1} \tag{7}$$

of infinite cyclic groups $\epsilon_i$, each generated by a basic unit $\epsilon_i$ of $k$, and of groups $H_i$, where each $H_i$ is generated by a unit $H_i$ and its conjugates

$$H_i = \{H_i, H_i^\sigma, \cdots\}. \tag{8}$$

---

[43] This provides the proper number of units. If $p_{\infty,i}$ is unramified, $H_i$ and its conjugates provide $n-1$ independent units, $\epsilon_i$ one more; if $p_{\infty,i}$ is ramified, $H_i=\mathfrak{P}_i$ and its conjugates $H_i^\sigma$ provide $n/2-1$ independent units, the total number being in agreement with the value of $R$.

The groups $\epsilon_i$ and $H_i$ which figure in (7) are groups which have $\Gamma$ as group of operators. They can be described in purely group theoretical language. Thus $\epsilon_i$ is an infinite cyclic group with a generator $\epsilon_i$ which is invariant under all operators of $\Gamma$.

To describe the group $H_i$ belonging to an unramified prime divisor $p_{\infty,i}$, consider first the operator free abelian group $G(\Gamma)$ belonging to any finite group $\Gamma$ of order $n$. As in Hall's paper ([17]) the group $G(\Gamma)$ is an abelian group with $n$ free generators $G^\sigma$, one for each element $\sigma$ in $\Gamma$. To these generators the elements $\tau$ of $\Gamma$ are to be applied by the rule $(G^\sigma)^\tau = G^{\tau\sigma}$. In this group $G(\Gamma)$ the elements left unaltered by all operators of $\Gamma$ form an infinite cyclic subgroup $N(\Gamma)$ which is generated by the "norm" $NG = G^{1+\sigma+\tau+\cdots}$. The quotient group $G(\Gamma)/N(\Gamma)$ belonging to this subgroup $N(\Gamma)$ is then isomorphic to the unit group $H_i = H$. This quotient group is an abelian group with $n$ generators $H^\sigma$(44) subject only to the relation $NH = 1$. We call this quotient group $H = G(\Gamma)/N(\Gamma)$ an *abstract unramified unit group*:

$$(9) \qquad H = \{H, H^\sigma, H^\tau, \cdots\}, \qquad \prod_\sigma H^\sigma = 1, \qquad (H^\sigma)^\tau = H^{\tau\sigma}.$$

In the ramified case let $\delta = \delta_i$ be the generator of the decomposition group of some ramified prime divisor $P_{\infty,i}$, and let $\Gamma$ be decomposed modulo the subgroup $\{1, \delta\}$ into left cosets

$$\Gamma = \sigma_1\{1, \delta\} + \sigma_2\{1, \delta\} + \cdots + \sigma_g\{1, \delta\}, \qquad g = n/2.$$

Then the *abstract $\delta$-ramified unit group* is an abelian group described by generators

$$(10) \qquad \mathfrak{P}^{\sigma_1}, \mathfrak{P}^{\sigma_2}, \cdots, \mathfrak{P}^{\sigma_g}, \qquad \text{with } \mathfrak{P}^{\sigma_1}\mathfrak{P}^{\sigma_2}\cdots\mathfrak{P}^{\sigma_g} = 1.$$

The operators of $\Gamma$ are applied to this group according to the rules

$$(11) \qquad (\mathfrak{P}^{\sigma_i})^\tau = \mathfrak{P}^{\tau\sigma_i}, \qquad \mathfrak{P}^{\sigma_i\delta} = \mathfrak{P}^{\sigma_i}, \qquad i = 1, 2, \cdots, g.$$

The Herbrand group $E^*$ of (7) is thus represented as a direct product whose factors are

$r$ infinite cyclic groups,

$\rho_1 + r_2$ abstract unramified unit groups,

$r_1 - \rho_1$ abstract $\delta_i$-ramified unit groups belonging to the prime divisors $p_{\infty,i}$ of type (2).

18. **Reduction to the Herbrand unit group.** The formula of Theorem 11.2 involves the units of $K$ in the index

(44) Each $H^\sigma$ is the coset of the original generator $G^\sigma$.

$$J(E) = [UE:E^{1-\sigma}][FE:TE]^{-1}. \tag{1}$$

We desire to relate this index to the corresponding index for the Herbrand unit group $E^*$

$$J(E^*) = [UE^*:E^{*1-\sigma}][FE^*:TE^*]^{-1}. \tag{2}$$

THEOREM 18.1. *The indices involved in $J(E^*)$ are both finite, and*

$$J(E) = J(E^*)\{[E:E^*]^{n-1}[\epsilon:\epsilon \cap E^*][FE:FE^*]^{-1}\} \tag{3}$$

*where all the indices on the right are finite, and where $\epsilon \cap E^*$ is the group of all units of $k$ which lie in the Herbrand group $E^*$.*

**Proof.** We first show why the indices in (3) are finite. If $E_\sigma$ is the group of all vectors with components in the group $E$, with a similar meaning for $E_\sigma^*$, then $E_\sigma$ is the $n$-fold direct product of $E$ by itself, so that

$$[E_\sigma:E_\sigma^*] = [E:E^*]^n$$

is finite. Apply next the homomorphism $E_\sigma \to TE_\sigma$. By definition, the subgroup of $E_\sigma$ mapped onto the identity is the group $UE$ of crossed characters. Then, by the homomorphism principle of §9,

$$[E:E^*]^n = [TE:TE^*][UE:UE^*],$$

where both indices on the right must be finite. This may be written as

$$[UE:UE^*] = [E:E^*]^n[TE:TE^*]^{-1}. \tag{4}$$

Secondly, apply the homomorphism which carries a unit $E$ into a vector with components $E^{1-\sigma}$. The subgroup mapped on the identity is $\epsilon$, the group of units in $k$. Hence

$$[E:E^*] = [E^{1-\sigma}:E^{*1-\sigma}][\epsilon:\epsilon \cap E^*], \tag{5}$$

where both indices on the right are finite.

Next we return to the index $J(E)$. In the numerator the index $[UE:E^{1-\sigma}]$ suggests two chains of groups $UE \supset E^{1-\sigma} \supset E^{*1-\sigma}$ and $UE \supset UE^* \supset E^{*1-\sigma}$ which join the same groups $UE$ and $E^{*1-\sigma}$. The whole index $[UE:E^{*1-\sigma}]$ is known to be finite. It can be computed in two ways from these chains, with the result

$$[UE:E^{1-\sigma}] = [UE^*:E^{*1-\sigma}][UE:UE^*][E^{1-\sigma}:E^{*1-\sigma}]^{-1}.$$

Inserting the values of these indices from (4) and (5), we get

$$[UE:E^{1-\sigma}] = [UE^*:E^{*1-\sigma}][E:E^*]^{n-1}[\epsilon:\epsilon \cap E^*][TE:TE^*]^{-1}. \tag{6}$$

One may similarly run two chains from $FE$ to $TE^*$, through the intermediate

groups $FE^*$ and $TE$. The indices $[FE:TE]$, $[TE:TE^*]$ are known to be finite, hence the indices are all finite and

$$[FE:TE] = [FE^*:TE^*][FE:FE^*][TE:TE^*]^{-1}. \tag{7}$$

Division of formula (6) by (7) yields the desired reduction formula (3).

19. **The correction factor for the reduction.** The replacement of the index $J(E)$ by the corresponding index $J(E^*)$ for the Herbrand unit group involves a "correction factor" found in equation (3) of §18,

$$\phi = J(E)/J(E^*) = [E:E^*]^{n-1}[\epsilon:\epsilon \cap E^*][FE:FE^*]^{-1}. \tag{1}$$

In the computations for the cyclic case in the classical theory it turns out([45]) that the corresponding correction factor is always 1, which is to say that the indices involving the units can be computed directly from the Herbrand group $E^*$ itself instead of from $E$. It would be convenient to have also $\phi=1$ in general([46]). This is not the case. We shall prove $\phi=1/2$ for a suitably selected pair of fields $K$, $k$.

Before actually proving this assertion we shall establish some lemmas reducing the problem to a simpler problem involving "normalized" factor sets.

Let $\Gamma$ be the four group, with generators $\gamma$, $\beta$:

$$\Gamma = \{1, \gamma, \beta, \gamma\beta\}, \qquad \gamma^2 = \beta^2 = 1, \qquad \beta\gamma = \gamma\beta = \delta. \tag{2}$$

A factor set $E_{\sigma,\tau}$ determines a group extension of the unit group $E$ by the group $\Gamma$. Any such group extension is completely determined by the multiplication table for elements $u_\gamma$ and $u_\beta$ which represent the two generating cosets $\gamma$ and $\beta$ in the extension. This multiplication table([47]) has the following form

$$u_\gamma E = E^\gamma u_\gamma, \qquad u_\beta E = E^\beta u_\beta, \qquad \text{(for any } E\text{)}, \tag{3}$$

$$u_\gamma^2 = C, \qquad u_\beta^2 = B, \qquad u_\beta u_\gamma = D u_\gamma u_\beta, \tag{4}$$

where $C$, $B$, and $D$ lie in the group $E$. The multiplication determined by this table will be associative if and only if $C$, $B$, and $D$ satisfy the conditions

$$C^\gamma = C, \qquad B^\beta = B, \qquad D^{1+\gamma} = C^{\beta-1}, \qquad D^{1+\beta} = B^{1-\gamma}. \tag{5}$$

The necessity of these conditions is readily proved by "multiplying out" in two different associations the products $u_\gamma^3$, $u_\beta^3$, $u_\beta^2 u_\gamma$ and $u_\beta u_\gamma^2$. Thus, any group

---

([45]) See Theorem 19.2 below.

([46]) This was actually conjectured by Deuring in a letter to Hasse in 1933, relating to some investigations on the principal ideal theorem of Hilbert.

([47]) Similar normalizations considered as generalizations of the formulas for cyclic algebras were used in the investigations of Dickson on crossed products [14]. Our normalization is a special case of the normalization of factor sets for abelian groups as set forth in [43, pp. 95–97].

extension of $E$ by $\Gamma$ is determined by a vector of three constants $\{C, B, D\}$ satisfying (5).

The fact that any group extension can be normalized in this form means that there is a homomorphic mapping of the factor sets $E_{\sigma,\tau}$ onto the "normalized" factor sets. To obtain explicitly this homomorphism, let the factor set $E_{\sigma,\tau}$ generate a group extension in which the representatives $v_\sigma$ of the cosets $\sigma$ multiply according to the table $v_\sigma v_\tau = E_{\sigma,\tau} v_{\sigma\tau}$. A corresponding normalized factor set then can be obtained by setting $u_\gamma = v_\gamma$, $u_\beta = v_\beta$ and computing $C$, $B$, and $D$ from the table of the $E_{\sigma,\tau}$'s. One finds

$$C = E_{\gamma,\gamma} E_{1,1}, \qquad B = E_{\beta,\beta} E_{1,1}, \qquad D = E_{\beta,\gamma} E_{\gamma,\beta}^{-1}. \tag{6}$$

These formulas provide a homomorphic mapping

$$FE = E_{\sigma,\tau} \rightarrow \{C, B, D\}. \tag{7}$$

What factor sets $E^{(0)}_{\sigma,\tau}$ are mapped by this homomorphism onto the identity? If $E^{(0)}_{\sigma,\tau}$ belongs to the multiplication table $v_\sigma v_\tau = E^{(0)}_{\sigma,\tau} v_{\sigma\tau}$, then $u_\beta = v_\beta$ and $u_\gamma = v_\gamma$ multiply as in (4) with constants $C = B = D = 1$. Furthermore the two remaining coset representatives must have the form $v_1 = E_1$, $v_\delta = E_\delta v_\beta v_\gamma$, where $E_1$ and $E_\delta$ are elements([48]) of $E$. From these constants we may calculate the whole multiplication table, getting

$$E^{(0)}_{\sigma,\tau} = E_\sigma E_\tau^\sigma / E_{\sigma\tau}, \qquad \text{where } E_\beta = E_\gamma = 1. \tag{8}$$

Furthermore, the given factor set $E^{(0)}_{\sigma,\tau}$ uniquely determines the two constants $E_1$ and $E_\delta$ as $E_1 = E^{(0)}_{1,1}$, $E_\delta = E^{(0)}_{\delta,\beta}$. Conversely, any two elements $E_1$ and $E_\delta$ determine through the formulas (8) a factor set $E^{(0)}_{\sigma,\tau}$ which has the property that it is mapped by the homomorphism (7) on the identity. Hence (8) provides an isomorphism

$$\{E_1, E_\delta\} \leftrightarrow E^{(0)}_{\sigma,\tau} \tag{9}$$

between the group of pairs $E_1$, $E_\delta$ and the group $E^{(0)}_{\sigma,\tau}$. An analogous isomorphism applies to the group $E^*$.

Now apply the homomorphism (7) to the index $[FE : FE^*]$. This maps $FE$ on the whole group of vectors $\{C, B, D\}$, because any such vector determines a group extension and hence a factor set of which it is the map. Furthermore, this homomorphism carries the group $FE^*$ of factor sets belonging to the Herbrand subgroup $E^*$ into the group $\{C^*, B^*, D^*\}$ of vectors from $E^*$ satisfying (5). Therefore, by the homomorphism principle,

$$[FE : FE^*] = [\{C, B, D\} : \{C^*, B^*, D^*\}]\,[E^{(0)}_{\sigma,\tau} : (E^*_{\sigma,\tau})^{(0)}].$$

The second index, involving the group of factor sets mapped by (7) into the identity, may be computed by (9) as

([48]) That is to say, they are part of a vector $E_\sigma$ used to transform a factor set.

$$[E^{(0)}_{\sigma,\tau}:(E^*_{\sigma,\tau})^{(0)}] = [\{E_1, E_\delta\}:\{E_1^*, E_\delta^*\}] = [E:E^*]^2.$$

This proves

LEMMA 1. *If* $\Gamma$ *is the four group, the factor set index is*

$$[FE:FE^*] = [\{C, B, D\}:\{C^*, B^*, D^*\}][E:E^*]^2, \tag{10}$$

*where the elements* $C, B, D$ *of* $E$ *(or* $C^*, B^*$, *and* $D^*$ *of* $E^*$*) are restricted by the associativity conditions* (5).

LEMMA 2. *If* $\Gamma$ *is the four group, the unit "correction factor" of* (1) *is*

$$\phi = [E:E^*][D:D^*]^{-1}[\epsilon:\epsilon \cap E^*]^{-1}, \tag{11}$$

*where* $D$ *is the group of all elements in* $E$ *for which there exist solutions* $B$ *and* $C$ *of the equations* (5), *and* $D^*$ *is analogously defined in* $E^*$.

**Proof.** The group of vectors $\{C, B, D\}$ of equation (10) may be mapped on the group $D$ described in the lemma by the homomorphism

$$\{C, B, D\} \to D. \tag{12}$$

The vectors thereby mapped into the identity ($D=1$) are the vectors $\{C, B\}$ which satisfy the relations (5) with $D=1$, or $C^\gamma = C^\beta = C$, $B^\beta = B^\gamma = B$. These relations mean that $C$ and $B$ are both invariant under all elements of the Galois group $\Gamma$, which is to say that $C$ and $B$ are both units in the group $\epsilon$. The group mapped by (12) on the identity is therefore $\{\epsilon, \epsilon, 1\}$, so

$$[\{C, B, D\}:\{C^*, B^*, D^*\}] = [D:D^*][\epsilon:\epsilon \cap E^*]^2. \tag{13}$$

Inserting the values (13) and (10) in the correction index (1) we get the assertion of the lemma.

We remark in passing that the conclusion (11) is still valid if $\Gamma$ is an abelian group which is the direct product of two cyclic groups with generators $\beta$ and $\gamma$ of respective orders $s$ and $t$, provided the condition (5) is replaced by

$$C^\gamma = C, \quad B^\beta = B, \quad D^{1+\gamma+\cdots+\gamma^{t-1}} = C^{\beta-1}, \quad D^{1+\beta+\cdots+\beta^{s-1}} = B^{1-\gamma}. \tag{14}$$

Consider now the particular field[49] $K = R(15^{1/2}, (-2)^{1/2})$ which is normal over the field of rational numbers $R$ and has the four group as Galois group.

LEMMA 3. *The only units in* $R(15^{1/2}, (-2)^{1/2})$ *are* $\pm\eta^m$, *where* $\eta = 4+15^{1/2}$.

**Proof.** One verifies at once that the only roots of unity present in $K$ are $\pm 1$. In the quadratic subfield $R(15^{1/2})$ it is known that the units are all of the form $\pm\eta^m$. Let $N$ denote the norm from $K$ to $R(15^{1/2})$. Then $N(\eta) = \eta^2$. Since

[49] In the elaborate search which ultimately led to this example, considerable use was made of the tables for units in the back of Sommer's textbook [35].

there can be only one independent unit in the totally complex field $K$, any other unit $E$ in $K$ is dependent on $\eta$, hence has $NE = \pm\eta^{m_0}$ for some $m_0 \neq 0$. We can therefore prove that $\pm\eta^m$ exhaust the whole unit group of $K$ if we can assert that no unit $E$ has $NE = \pm\eta$.

Since $E$ is an integer, it is readily shown that $E$ must have the form

$$E = (a + b15^{1/2} + c(-2)^{1/2} + d(-30)^{1/2})2^{-1} \qquad (a, b, c, d \text{ are integers}).$$

If one calculates $NE$, one finds that $NE = -\eta$ is impossible, while $NE = \eta$ leads to the diophantine equations

$$a^2 + 15b^2 + 2c^2 + 30d^2 = 16, \qquad 2ab + 4cd = 4.$$

By trial of a small number of cases it results that these equations have no integral solutions. Thus the lemma is proved.

THEOREM 19.1. *There exists a normal extension $K/k$ with the four group as Galois group for which the correction factor $\phi$ of* (1) *is different from* 1.

**Proof.** Take the field $K = R(15^{1/2}, (-2)^{1/2})$. The Herbrand group $E^*$ of this field is any group of units generated by a unit P invariant under the automorphism carrying $K$ into its complex conjugate. The unit $P = \eta$ is such a unit, hence we may take for $E^*$ the group of all $\eta^m$. Then $E$ is the direct product $E = \{\pm 1\} \times E^*$, where $\{\pm 1\}$ is a cyclic group of order 2. One verifies readily that if $D = -1$ the equations (5) defining the parameter $D$ have a solution $B = C = 1$. Hence the group $D$ is given as $\{\pm 1\} \times D^*$. Finally, $\epsilon = \{\pm 1\}$, $\epsilon \cap E^* = 1$. With these values in the formula (11) for the correction factor we get $\phi = 2/4 = 1/2$.

The result for this particular field has been checked directly, independently of the normalized factor sets, by the laborious process of explicitly solving the associativity conditions for all factor sets $E_{\sigma,\tau}$ in the unit group $\{\pm\eta^m\}$. Using the normalization again, the unit group has been computed also for the fields $R(30^{1/2}, (-2)^{1/2})$, $R(42^{1/2}, (-2)^{1/2})$, $R(2^{1/2}, (-1)^{1/2})$. In these three cases one finds again that $\phi = 1/2$. The first two cases have unit groups isomorphic to the group of our example $R(15^{1/2}, (-2)^{1/2})$, while in the third case the unit group involves more roots of unity.

The correction factor $\phi$ is not the same for all fields with the four group. For the field $R(3^{1/2}, (-2)^{1/2})$ it turns out to be 1.

THEOREM 19.2. *If the Galois group $\Gamma$ of $K/k$ is cyclic, the correction factor $\phi$ is* 1([50]).

**Proof.** The proof depends on a normalization of the factor sets $FE$ which appear in formula (1). Just as in the formula (9) of §2, each factor set of

([50]) This theorem simply asserts that the correction factor $\phi$ of (1) does in fact behave like the analogous correction factor of the cyclic theory.

units $E_{\sigma,\tau}$ for a cyclic group with the generator $\lambda$ determines a single quantity $C$ which functions as the usual "normalized" factor set,

$$C = \prod_{i=0}^{n-1} E_{\lambda^i,\lambda}. \tag{15}$$

The associativity condition becomes $C^\lambda = C$, so that $C$ is a unit $\epsilon$ in the base field $k$. The equation (15) thus provides a homomorphic mapping $E_{\sigma,\tau} \to C$ of the group $FE$ onto the units $\epsilon$ of $k$. This mapping carries $FE^*$ into $\epsilon \cap E^*$, and one may establish as in Lemma 1 above that the factor sets $E^{(0)}_{\sigma,\tau}$ mapped by (15) into 1 have the form of transformation sets $E^{(0)}_{\sigma,\tau} = E_\sigma E^\sigma_\tau E^{-1}_{\sigma\tau}$ for which $E_\lambda = 1$. By the homomorphism principle we have

$$[FE:FE^*] = [\epsilon:\epsilon \cap E^*][E_\sigma:E_\sigma^*] = [\epsilon:\epsilon \cap E^*][E:E^*]^{n-1}.$$

According to (1) this proves $\phi = 1$.

20. **An additional reduction for unit factor sets.** In this section we give another way of reducing the basic index involving the units, $J(E) = [UE:E^{1-\sigma}]/[FE:TE]$. The result will also be used to get an estimate for $[FE:FE^*]$ and for the correction factor $J(E)/J(E^*)$. The group $E$ may be analyzed into the subgroup $\epsilon$ and the groups

(1) $\quad \mathrm{Z} =$ all roots of unity in $K$; $\zeta = \mathrm{Z} \cap k$;

(2) $\quad B =$ all units $E$ with $NE$ a root of unity $\zeta$;

(3) $\quad \Omega = B\epsilon$.

We introduce also the integer $y = [\mathrm{Z}:1]$.

Under the homomorphism $A \to A^\nu$ the subgroup mapped on 1 is the group Z, hence the isomorphisms

$$E^\nu \cong E/\mathrm{Z}, \qquad B^\nu \cong B/\mathrm{Z}, \qquad \epsilon^\nu \cong \epsilon/\zeta. \tag{4}$$

Clearly these isomorphisms hold also if $y$ is replaced by any proper multiple of $[\mathrm{Z}:1]$.

THEOREM 20.1. *The index $J(E)$ is given by*

$$J(E) = J(B^\nu)J(\epsilon^\nu)J(\mathrm{Z})\omega(E, B)\omega(B, \mathrm{Z})/[E:B\epsilon],$$

*where each $\omega$ represents a deficiency index, where for any group $R$ $J(R) = [UR:R^{1-\sigma}]/[FR:TR]$, and where $[E:B\epsilon]$ depends on the norms within $\epsilon$ as in*

$$[E:B\epsilon] = [NE:\epsilon^n]/[NE \cap \zeta:\zeta^n].$$

Since $\epsilon$ is generated by $\zeta$ and $r$ independent units $\epsilon_1, \cdots, \epsilon_r$ of infinite order, $\epsilon^\nu$ is isomorphic to a subgroup of the group generated by $\epsilon_1, \cdots, \epsilon_r$. Hence $\epsilon^\nu$ is the direct product of $r$ infinite cyclic groups. As will subsequently

be shown (§21, (4) and §23), one may then compute that $J(\epsilon^\nu) = [\Gamma:\Gamma']^{-r}$, where $\Gamma'$ is the commutator subgroup of $\Gamma$.

The proof of Theorem 20.1 will depend on systematic use of the subgroup $\Omega$ of $E$, as defined in (3). The index $[E:\Omega]$ can be evaluated in several different ways.

LEMMA 1. *The index* $[E:\Omega]$ *is finite and is given by*

$$[E:\Omega] = [E^\nu:\Omega^\nu], \tag{5}$$

$$[E:\Omega] = [NE:\epsilon^n]/[NE \cap \zeta:\zeta^n], \tag{6}$$

$$[E:\Omega] = [(E^{1-\sigma})^\nu:(\Omega^{1-\sigma})^\nu][E^{1-\sigma} \cap \mathrm{Z}_\sigma:\mathrm{Z}^{1-\sigma}]. \tag{7}$$

**Proof.** If $[E:\Omega]$ is finite, the expression (5) is obtained at once by applying the homomorphism principle to the map $E \to E^\nu$, for the elements mapped thereby into 1 all lie in the subgroup $\mathrm{Z}$ of $\Omega$. To get (6), apply the homomorphism $E \to NE$, with the result

$$\begin{aligned}[E:\Omega] &= [NE:N\Omega] = [NE:(NB)\epsilon^n] = [NE:(NE \cap \zeta)\epsilon^n] \\ &= [NE:\epsilon^n]/[(NE \cap \zeta)\epsilon^n:\epsilon^n],\end{aligned}$$

for $NB \subset \zeta$ by the very definition of $B$. Since $NE$ is a subgroup of $\epsilon$, $[NE:\epsilon^n]$ is less than the finite index $[\epsilon:\epsilon^n]$, which proves that $[E:\Omega]$ and all other indices here present are finite. If one observes that the intersection of $(NE \cap \zeta)$ with $\epsilon^n$ consists of all roots of unity in $k$ which are $n$th powers, and hence is just $\zeta^n$, this formula will give the result (6) by the reduction principle (§9).

Finally, to prove (7), apply the successive homomorphisms $E \to E^{1-\sigma} \to (E^{1-\sigma})^\nu$. They give

$$[E:\Omega] = [E^{1-\sigma}:\Omega^{1-\sigma}] = [(E^{1-\sigma})^\nu:(\Omega^{1-\sigma})^\nu][E^{1-\sigma} \cap \mathrm{Z}_\sigma:\Omega^{1-\sigma} \cap \mathrm{Z}_\sigma].$$

This will give (7), if we can prove that $\Omega^{1-\sigma} \cap \mathrm{Z}_\sigma = \mathrm{Z}_\sigma$. By definition, $\Omega = B\epsilon$, so $\Omega^{1-\sigma} = B^{1-\sigma}$. Since $B$ contains all units with norms in $\zeta$, $B \supset \mathrm{Z}$ and $B^{1-\sigma} \cap \mathrm{Z}_\sigma \supset \mathrm{Z}^{1-\sigma}$. Conversely, suppose that $B$ is a unit of norm $NB = \zeta$ with $B^{1-\sigma} = \mathrm{Z}_\sigma$ for all $\sigma$. Then $(B^{1-\sigma})^\nu = \mathrm{Z}_\sigma^\nu = 1$, so $(B^\nu)^{1-\sigma} = 1$, and $B^\nu = \epsilon$ is in $k$. Therefore $NB^\nu = \zeta^\nu = 1 = \epsilon^n$, so the unit $\epsilon$ must be a root of unity. But $B^\nu = \epsilon$, so $B$ is also a root of unity $\mathrm{Z}$. Therefore $B^{1-\sigma} \cap \mathrm{Z}_\sigma \subset \mathrm{Z}^{1-\sigma}$, and the lemma is established.

LEMMA 2. *If* $R$ *and* $S$ *are* $\Gamma$*-allowable subgroups of* $K$ *such that* $[R:S]$ *and* $[FR:TR]$ *are both finite, then* $[FR:FS]$ *and* $[FS:TS]$ *are finite.*

**Proof.** The index $[FR:FS]$ can be written formally as

$$[FR:FS] = [FR:(TR)(FS)][(TR)(FS):FS].$$

The first index does not exceed $[FR:TR]$, and the second can be changed by the reduction principle to $[TR:FS \cap TR]$, which does not exceed

$[TR:TS]$. The latter index is finite, and bounded by $[R:S]^n$. Hence $[FR:FS]$ is finite. Therefore $[FS:TS]$ is finite, because it can be expressed as $[FR:TR][TR:TS]/[FR:FS]$.

The expression $J(E)$ of the theorem has as denominator the index $[FE:TE]$. This may be reduced by applying the homomorphism $A \to A^\nu$, to get

$$[FE:TE] = [(FE)^\nu:(TE)^\nu][FZ:TE \cap FZ]. \tag{8}$$

Here $[FE:TE]$ is known to be finite, while $[E:E^\nu]$ is also finite because $E$ has a finite number of generators. Therefore $[FE:FE^\nu]$ and $[FE^\nu:TE^\nu]$ are both finite indices (Lemma 2). The latter may be introduced in (8) if we divide by the deficiency index $\omega(E, Z) = [FE^\nu:(FE)^\nu]$ (see Theorem 15.1). The subgroup $\Omega^\nu$ of (3) may be introduced in terms of the finite indices $[FE^\nu:F\Omega^\nu]$ and $[TE^\nu:T\Omega^\nu]$. Then

$$\begin{aligned}[FE:TE] = {} & [FE^\nu:F\Omega^\nu][F\Omega^\nu:T\Omega^\nu][TE^\nu:T\Omega^\nu]^{-1} \\ & \times [FZ:TZ][TE \cap FZ:TZ]^{-1}[\omega(E, Z)]^{-1}.\end{aligned} \tag{9}$$

The index involving $TE^\nu$ and $T\Omega^\nu$ may be found by a homomorphic map of the group $(E^\nu)_\sigma$ of vectors with components in $E^\nu$, as

$$\begin{aligned}[(E^\nu)_\sigma:(\Omega^\nu)_\sigma] &= [TE^\nu:T\Omega^\nu][UE^\nu:U\Omega^\nu], \\ [TE^\nu:T\Omega^\nu] &= [E^\nu:\Omega^\nu]^n[UE^\nu:U\Omega^\nu]^{-1}.\end{aligned} \tag{10}$$

In (9) we next attack $[FE^\nu:F\Omega^\nu]$ by the norm homomorphism

$$[FE^\nu:F\Omega^\nu] = [N(FE^\nu):N(F\epsilon^\nu)].$$

One proves easily that the norm of a factor set is itself a factor set. The group $N(F\epsilon^\nu) = (F\epsilon^\nu)^n$ is then contained in $F(N\epsilon^\nu) = F(\epsilon^{n\nu})$. Since each element of $\epsilon^{n\nu}$ has a unique $n$th root, the two groups are equal, or $N(F\epsilon^\nu) = F(\epsilon^{n\nu})$. On the other hand, the index $[F(NE^\nu):N(FE^\nu)]$ is a deficiency index $\omega(E^\nu, B^\nu)$ belonging to the norm homomorphism. All told

$$[FE^\nu:F\Omega^\nu] = [F(NE^\nu):F(\epsilon^{n\nu})]/\omega(E^\nu, B^\nu).$$

Now $NE^\nu$ and $\epsilon^{n\nu}$ are both subgroups of finite index in the group $\epsilon^\nu$, which is a direct product of $r$ cyclic groups. Hence both $NE^\nu$ and $\epsilon^{n\nu}$ are themselves direct products of $r$ cyclic groups. Therefore $[F(NE^\nu):T(NE^\nu)] = [F(\epsilon^{n\nu}):T(\epsilon^{n\nu})]$; in fact, they are each equal to $[\Gamma:\Gamma']^r$, by §21, (4). The factor sets on the right in the last equation may therefore be replaced by transformation quantities,

$$[FE^\nu:F\Omega^\nu] = [T(NE^\nu):T(\epsilon^{n\nu})]/\omega(E^\nu, B^\nu). \tag{11}$$

Since each $NE^\nu$ is invariant under any $\sigma$, every crossed character of $\Gamma$ in the group $NE^\nu$ is an ordinary character of $\Gamma$ in $NE^\nu$. But $\Gamma$ is finite and $(NE)^\nu$

contains no element of finite order, so that all these ordinary characters are 1. This means that the homomorphism $(NE^\nu)\to T(NE^\nu)_\sigma$ which carries a vector into a transformation quantity is an isomorphism. With this isomorphism, the last equation becomes

$$[FE^\nu:F\Omega^\nu] = [NE^\nu:\epsilon^{n\nu}]^n/\omega(E^\nu, B^\nu).$$

On the other hand, the homomorphism $NE\to(NE)^\nu$ gives

$$[NE^\nu:\epsilon^{n\nu}] = [NE:\epsilon^n]\cdot[NE\cap\zeta:\zeta^n]^{-1} = [E:\Omega],$$

according to (6). These two formulas, combined with (11), yield

$$[FE^\nu:F\Omega^\nu] = [E:\Omega]^n/\omega(E^\nu, B^\nu). \tag{12}$$

The deficiency index $\omega$ which is present here may be reformulated by combination with the deficiency $\omega(E, \mathrm{Z})$ present in (9). By the norm homomorphism

$$\omega(E, \mathrm{Z}) = [FE^\nu:(FE)^\nu] = [N(FE^\nu):N(FE)^\nu][FB^\nu:(FB)^\nu],$$

while

$$\omega(E^\nu:B^\nu) = [F(NE^\nu):N(FE^\nu)], \qquad \omega(E, B) = [F(NE^\nu):N(FE)^\nu].$$

Combining these results, we find

$$\omega(E, \mathrm{Z})\omega(E^\nu, B^\nu) = \omega(E, B)\omega(B, \mathrm{Z}). \tag{13}$$

Turn now to the numerator $[UE:E^{1-\sigma}]$ of the expression $J(E)$. To each vector in the principal genus $UE$ apply the homomorphism $UE\to(UE)^\nu$. Then

$$[UE:E^{1-\sigma}] = [(UE)^\nu:(E^\nu)^{1-\sigma}][U\mathrm{Z}:E^{1-\sigma}\cap \mathrm{Z}_\sigma]. \tag{14}$$

We may introduce the group $U(E^\nu)\supset(UE)^\nu$ by

LEMMA 3. *The index* $[UE^\nu:(UE)^\nu]$ *is finite, and is given by*

$$[UE^\nu:(UE)^\nu] = [TE\cap F\mathrm{Z}:T\mathrm{Z}]. \tag{15}$$

**Proof.** Let $U'E$ temporarily denote all those vectors $E_\sigma$ of units such that the transformation set $TE$ consists of roots of unity. Then $U'E$ contains the crossed characters $UE$, and the homomorphism $T$ gives

$$[U'E:UE] = [TE\cap F\mathrm{Z}:1] = [TE\cap F\mathrm{Z}:T\mathrm{Z}][T\mathrm{Z}:1].$$

Since Z is a finite group, the indices involved here are all finite. On the other hand, the crossed characters $U(E^\nu)$ are all $\nu$th powers of elements in this temporary group $U'E$, so the homomorphism $UE\to(UE)^\nu$ will prove

$$[U'E:UE] = [U(E^\nu):(UE)^\nu][\mathrm{Z}_\sigma:U\mathrm{Z}].$$

This proves that the desired index $[U(E^v):(UE)^v]$ is finite. Furthermore we get (15) by comparing these two expressions for $[U'E:UE]$, observing that $[\mathrm{Z}_\sigma:U\mathrm{Z}]=[T\mathrm{Z}:1]$ by the very definition of the crossed characters $U\mathrm{Z}$.

Using the result of Lemma 3, we may now rewrite (14) as

$$(16)\quad [UE:E^{1-\sigma}]=[UE^v:(E^v)^{1-\sigma}][U\mathrm{Z}:\mathrm{Z}^{1-\sigma}][TE\cap F\mathrm{Z}:T\mathrm{Z}]^{-1}[E^{1-\sigma}\cap \mathrm{Z}_\sigma:\mathrm{Z}^{1-\sigma}]^{-1}.$$

The first index in this formula may be transferred to the group $\Omega^v S$ since $[E^v:\Omega^v]$ is finite, so are $[UE^v:U\Omega^v]$ and $[(E^v)^{1-\sigma}:(\Omega^v)^{1-\sigma}]$. Therefore

$$[UE^v:(E^v)^{1-\sigma}] = [UE^v:U\Omega^v][U\Omega^v:(\Omega^v)^{1-\sigma}][(E^v)^{1-\sigma}:(\Omega^v)^{1-\sigma}]^{-1}.$$

On substitution in (16) and application of (7) this gives an expression for $[UE:E^{1-\sigma}]$ as

$$(17)\quad [UE^v:U\Omega^v][U\mathrm{Z}:\mathrm{Z}^{1-\sigma}][U\Omega^v:(\Omega^v)^{1-\sigma}][TE\cap F\mathrm{Z}:T\mathrm{Z}]^{-1}[E:\Omega]^{-1}.$$

The results can now be combined to give $J(E)=[UE:E^{1-\sigma}]/[FE:TE]$ by dividing the expression (17) for the numerator by the expression (9) for the denominator, using (10) and (12) for substitutions. The result is

$$(18)\quad J(E) = J(\Omega^v)J(\mathrm{Z})\omega(E,\mathrm{Z})\omega(E^v,B^v)[E:\Omega]^{-1}.$$

Since $\Omega^v=B^v\epsilon^v$, and since $E^v$ contains no roots of unity, and hence no elements in the group $B^v$ of elements of norm 1, $\Omega^v$ is a direct product $B^v\times\epsilon^v$. The corresponding $J$ index is therefore also a product $J(\Omega^v)=J(B^v)J(\epsilon^v)$. Putting this in (18), reducing the product of the two deficiency indices as in (13) and replacing $[E:\Omega]$ by (6), the result (18) becomes that of Theorem 1.

The indices involved in this expression for $J(E)$ are all reasonably explicit except for $J(B^v)$. As indicated in (4), the group $B^v$ here may be replaced by $B^x$, where $x=[E:E^*]$ is the index of the Herbrand group. Hence the problem is essentially that of computing $[FB^x:TB^x]$, the number of group extensions of a certain subgroup $B^x$ of the Herbrand group. The computations of §§22, 23 solve this problem for the special case when $B^x$ is a subgroup isomorphic to the group $H^*$ generated by all the Herbrand units of norm 1.

This type of computation can also be employed to give a new expression for the correction factor of §19.

THEOREM 20.2. *For an Herbrand subgroup $E^*$ of $E$*

$$J(E)/J(E^*) = [J(B^v)/J(H^*)]J(\mathrm{Z})\omega(E,B)\omega(B,\mathrm{Z})[E:B\epsilon]^{-1},$$

*where $H^*$ is the subgroup of $E^*$ consisting of all units of norm* 1.

This conclusion can be obtained by a suitable direct analysis of the correction factor, using the index $x=[E:E^*]$ much as the index $y$ of the above computation. A quicker method is to apply the computation underlying Theorem 20.1 to the group $E^*$ as if $E^*$ were the whole unit group of a field. Since

$\epsilon^* = E^* \cap k$, the Herbrand group is as in §17 the direct product $E^* = \epsilon^* \times H^*$, and contains no roots of unity. The result analogous to Theorem 20.1, using $y = 1$, is then

$$J(E^*) = J(H^*)J(\epsilon^*)\omega(E^*, H^*)/[E^* : H^*\epsilon^*].$$

But $E^* = H^* \times \epsilon^*$ means that the deficiency index $\omega$ here must be 1, because every factor set in $H^*$ is automatically a factor set in $E^*$ and thus a homomorphic image of a factor set in $E^*$. Furthermore $\epsilon^*$ is isomorphic to $\epsilon^\nu$, as both are free abelian groups on $r$ generators. Hence $J(\epsilon^*) = J(\epsilon^\nu)$. This result, combined with Theorem 20.1, then gives the formula of Theorem 20.2.

21. **Extensions of unit groups.** The denominator of the index $J(E^*)$ is $[FE^* : TE^*]$, the number of group extensions of the Herbrand unit group $E^*$ by the Galois group $\Gamma$. Since $E^*$ is a direct product (see the end of §17), this index reduces at once to

$$[FE^* : TE^*] = \left( \prod_{i=1}^{r} [F\epsilon_i : T\epsilon_i] \right) \left( \prod_{i=1}^{r+1} [FH_i : TH_i] \right). \tag{1}$$

Here the index $[F\epsilon_i : T\epsilon_i]$ is simply the number of group extensions of an infinite cyclic group $\epsilon_i$ by the Galois group $\Gamma$, it being assumed that $\epsilon_i$ lies in the center of the resulting extension(51). These group extensions can be counted by the character method applied in §5, to $p$-primary factor sets of ideals. In fact, the group extension problem is formally exactly that of finding the number of classes of $p$-primary factor sets in the special case when $p$ is a prime ideal(52) of $K$. The number of such classes was shown in Theorem 5.5 to be the index $[\Delta(P) : \Delta(P)']$ of the commutator group $\Delta(P)'$. Since the formal analogue of the decomposition group $\Delta(P)$ is the whole group $\Gamma$, we find in this case

$$[F\epsilon_i : T\epsilon_i] = [\Gamma : \Gamma'], \qquad \Gamma' \text{ the commutator group of } \Gamma. \tag{2}$$

The index (1) thus reduces to the following group-theoretic expression.

THEOREM 21.1. *The number of classes of associated factor sets from the Herbrand unit group $E^*$ is*

$$[FE^* : TE^*] = [\Gamma : \Gamma']^r [FH : TH]^{\rho_1 + r_2} \prod_{p_\infty} [F\mathfrak{P}_\delta : T\mathfrak{P}_\delta] \tag{3}$$

*where $H$ is the abstract unramified unit group of* (9) *in* §17, $\mathfrak{P}_\delta$ *is the abstract $\delta$-ramified unit group of* (10), (11) *in* §17, *the product is taken over all $p_\infty$ which are ramified in $K/k$ and $\delta = \delta(P_\infty)$, where $P_\infty \mid p_\infty$.*

The group-theoretic indices in (3) can be evaluated in some special cases.

(51) That is to say, the coset belonging to each $\sigma$ induces in $\epsilon_i$ the identity automorphism.

(52) In this case the $p$-primary ideals form an infinite cyclic group.

If $\Gamma$ is abelian and is the direct product of cycles of orders $m_1, \cdots, m_t$, then([53])

$$[FH:TH] = \prod_{i<j} (m_i, m_j). \tag{4}$$

Exactly the same formula holds for an abstract ramified group P, as will be proved by the computations([54]) of §22. These results prove

THEOREM 21.2. *Let $\Gamma$ be an abelian group represented as the direct product of $t$ cyclic groups of respective orders $m_1, m_2, \cdots, m_t$. Then*

$$[FE^*:TE^*] = [\Gamma:\Gamma']^r \left[ \prod_{i<j} (m_i, m_j) \right]^{r+1} \tag{5}$$

*where $(m_i, m_j)$ denotes the greatest common divisor of $m_i$ and $m_j$.*

22. **The number of extensions for a unit group.** This section is devoted to group-theoretic computations leading to

THEOREM 22.1. *If* P *is an abstract ramified unit group belonging to an abelian group $\Gamma$ which is the direct product of cyclic groups of orders $m_0, \cdots, m_s$, then the number of group extensions of* P *by $\Gamma$ is*

$$[F\mathrm{P}:T\mathrm{P}] = \prod_{i<j} (m_i, m_j); \qquad i, j = 0, \cdots, s. \tag{1}$$

The ramified unit group P is defined with reference to an automorphism $\delta$ of order 2 in $\Gamma$ ($\delta$ is the generator of the decomposition group of a corresponding infinite prime divisor of $K$). Write the abelian group $\Gamma$ as a direct product of $s+1$ cyclic groups $\{\alpha_i\}$,

$$\Gamma = \{\alpha_0\} \times \{\alpha_1\} \times \cdots \times \{\alpha_s\}; \qquad \text{order of } \alpha_i = m_i. \tag{2}$$

A simple computation shows that this representation may be so modified that the given $\delta$ lies in one of the cycles, as

$$\delta = \alpha_0^r, \qquad m_0 = 2r. \tag{3}$$

In each coset of $\Gamma$ modulo $\{1, \delta\}$ there is a representative of the form

$$\beta = \alpha_0^{e_0} \alpha_1^{e_1} \cdots \alpha_s^{e_s}; \qquad 0 \leqq e_0 < r, \ 0 \leqq e_i < m_i, \ (i \neq 0), \tag{4}$$

with an exponent less than $r$ for $\alpha_0$.

By definition, the abelian group P is generated by elements $\mathrm{P}^\beta$ subject

([53]) Dr. A. H. Clifford has pointed out to us that this product is exactly the order of the multiplicator $\mathfrak{M}$ of $\Gamma$ in Schur's theory of collineations (see [15, 36]). Moreover, Clifford and MacLane in [12] have proved by more general methods that $FH/TH$ is isomorphic to $\mathfrak{M}$ whenever $\Gamma$ is solvable.

([54]) We omit the analogous computations for (4), since the result is given by [12].

to the relations(55)

$$\prod_{\beta} \mathrm{P}^{\beta} = 1, \qquad \mathrm{P}^{\delta} = \mathrm{P}. \tag{5}$$

Any element $A$ of P can be expressed in the form

$$A = \prod_{\beta} \mathrm{P}^{a(\beta)\beta} = \mathrm{P}^{\Sigma a(\beta)\beta} = \exp\left(\sum_{\beta} a(\beta)\beta\right), \tag{6}$$

("exp" for convenience!). Since $\mathrm{P}^{\delta} = \mathrm{P}$, it is convenient to define the integer $a(\gamma)$ for all $\gamma$ in $\Gamma$ by the convention $a(\beta\alpha_0^r) = a(\beta\delta) = a(\beta)$. Because of the first relation of (5), the representation (6) is not unique; the exponents $a(\beta)$ may all be changed simultaneously to $a(\beta)+g$, for any integer $g$. We call $g$ a *change of gauge.*

In any group extension $\mathfrak{E}$ of P by $\Gamma$ pick a fixed representative $u_i = u(\alpha_i)$ for the cosets $\alpha_i$ of $\mathfrak{E}/\mathrm{P} \simeq \Gamma$. Then use for any element $\gamma$ of $\Gamma$ the special representatives generated by the $u_i$,

$$u(\alpha_0^{e_0}\alpha_1^{e_1}\cdots\alpha_s^{e_s}) = u_0^{e_0}u_1^{e_1}\cdots u_s^{e_s}, \qquad 0 \leqq e_i < m_i. \tag{7}$$

The multiplication table for these representatives is then

$$u_i^{m_i} = C_i, \qquad u_j u_i = D_{ij} u_i u_j \qquad (i < j;\ i, j = 0, \cdots, s); \tag{8}$$

these constants $C_i$ and $D_{ij}$ from P form a *normalized factor set.* The multiplication table for $\mathfrak{E}$ is completed by the commutation rule

$$u_i A = A^{\alpha_i} u_i \qquad \text{(for all } A \text{ in P)}. \tag{9}$$

If the original coset representatives are changed to $v_i = A_i u_i$, for constants $A_0, \cdots, A_s$ in P, the constants $C_i$ and $D_{ij}$ of the factor set are multiplied respectively by the transformation quantities

$$N_i A_i, \qquad A_j^{1-\alpha_i} A_i^{\alpha_j - 1} \qquad (i < j,\ i, j = 0, \cdots, s); \tag{10}$$

here $N_i$ (the "relative norm for $\alpha_i$") denotes the expression

$$N_i A_i = A^{1+\alpha+\cdots+\alpha^{m-1}}, \qquad (\alpha = \alpha_i,\ m = m_i). \tag{11}$$

The factor set $\{C_i, D_{ij}\}$ must satisfy the associativity conditions(56)

$$C_i^{\alpha_i} = C_i, \qquad C_i^{\alpha_j - 1} = N_i D_{ij}, \qquad D_{ij}^{\alpha_k - 1} D_{jk}^{\alpha_i - 1} D_{ki}^{\alpha_j - 1} = 1 \tag{12}$$

for all $i, j, k$, with $D_{ji} = D_{ij}^{-1}$ and $D_{ii} = 1$. Our problem is to count the number

(55) Here and subsequently $\beta$ denotes an index which runs over the elements (4).

(56) The fact that these conditions are necessary and sufficient to insure associativity is proved by Zassenhaus [43, p. 97]. His $A_{i,k}$ is our $D_{ki}$.

of non-equivalent solutions of these equations, where two solutions are called equivalent if their quotient is a transformation set (10). A preliminary is

**Step I. Removal of the constants $C_i$.**

LEMMA 1. *For each group extension $\mathfrak{E}$ of* P *by* $\Gamma$ *there is a normalized factor set with $C_i=1$, for $i=1, \cdots, s$.*

**Proof.** If $C_i$ is written in the exponent form of (6), then

$$C_i = \exp\Big(\sum_\beta c_i(\beta)\beta\Big), \qquad C_i^{\alpha_i} = \exp\Big(\sum_\beta c_i(\alpha_i^{-1}\beta)\beta\Big). \tag{13}$$

According to the associativity condition (12) these two representations can only differ by a change of gauge $g_i$, so (12) becomes

$$c_i(\alpha_i^{-1}\beta) = c_i(\beta) + g_i \qquad (\text{all } \beta;\ i = 0, \cdots, s). \tag{14}$$

For a fixed $i$, add these equations over all $\beta$. Since $\sum_\beta c_i(\alpha_i^{-1}\beta) = \sum_\beta c_i(\beta)$, each $g_i=0$. Therefore $c_i(\beta)=c_i(\beta\alpha_i^k)$ for every $k$. If $\beta'$ runs over the elements $\beta$ of (4) which do not involve $\alpha_i$ (i.e., which have $e_i=0$), the $C_i$ of (13) becomes

$$C_i = \exp\Big[\sum_{\beta'} (\beta' + \beta'\alpha_i + \cdots + \beta'\alpha_i^{m_i-1})c_i(\beta')\Big]; \qquad (i \neq 0). \tag{15}$$

The sum $(1+\alpha+\cdots+\alpha^{m-1})$ is the exponent involved in the norm $N_i$ of (11), so $C_i=N_i(\exp\sum_{\beta'}c_i(\beta'))$. This means that $C_i$ is a transformation quantity $N_iA_i$ for a suitable $A_i$, so that this transformation will reduce $C_i$ to 1, q.e.d.

For $i=0$ the argument fails. Since $\beta$ involves $\alpha_0^e$ only up to $e=r-1$, (15) becomes

$$C_0 = \exp\Big[\sum_{\beta'} (\beta' + \beta'\alpha_0 + \cdots + \beta'\alpha_0^{r-1})c_0(\beta')\Big]; \qquad (\beta' \text{ in } \{\alpha_1, \cdots, \alpha_s\}). \tag{16}$$

The corresponding transformation quantity $N_0A_0$ is (with $\alpha=\alpha_0$)

$$N_0A_0 = A_0^{1+\alpha+\cdots+\alpha^{m-1}} = A_0^{(1+\alpha+\cdots+\alpha^{r-1})(1+\alpha^r)} = A_0^{2(1+\alpha+\cdots+\alpha^{r-1})},$$

for $\alpha^r=\delta$ leaves $A_0$ fixed. The exponents in $N_0A_0$ are all even, so $C_0$ of (16) can be brought to this form only if its exponents $c_0(\beta')$ become even after a change of gauge. This proves

LEMMA 2. *The constant $C_0$ may be reduced to* 1 *by a transformation quantity if and only if its exponents $c_0(\beta')$ satisfy $c_0(\beta')\equiv c_0(1) \pmod 2$ for every $\beta'$ in the group generated by $\alpha_1, \cdots, \alpha_s$.*

Henceforth we consider only factor sets reduced, as in Lemma 1, to

$$C_1 = C_2 = \cdots = C_s = 1, \qquad N_1A_1 = \cdots = N_sA_s = 1. \tag{17}$$

**Step II. Construction and counting of the invariants.** The essential device for our computation is the reduction of factor sets in P to factor sets of integers. This is done by using the *trace* of each element $A$ of the group P,

$$a = t(A) = t\left\{\exp \sum_{\beta} a(\beta)\beta\right\} \equiv \sum_{\beta} a(\beta) \pmod{n/2}, \tag{18}$$

where $n = m_0 m_1 \cdots m_s$ is the order of the group $\Gamma$. The change of gauge $a(\beta) \to a(\beta) + g$ changes the sum over $n/2$ terms $\beta$ by $(n/2)g$, hence $t(A)$ is uniquely determined modulo $n/2$. Furthermore

$$t(AB) \equiv t(A) + t(B), \qquad t(A^\gamma) \equiv t(A) \pmod{n/2}. \tag{19}$$

Therefore $t$ is an operator-homomorphism of the group P of units on the additive group of integers modulo $n/2$, so $t$ maps the given factor set $\{C_0, D_{ij}\}$ onto a factor set of integers

$$c_0 \equiv t(C_0), \qquad d_{ij} \equiv t(D_{ij}) \qquad (i < j,\ i, j = 0, \cdots, s). \tag{20}$$

The homomorphism $t$ applied to the associativity conditions (12) yields 0 for every term of the form $B^{\alpha-1}$, because $t(B^\alpha) = t(B)$. There remain only the conditions derived from the norms in (12). The norm $N_i B$ of (11) contains $m_i$ exponents, so $t(N_i B) = m_i t(B)$, and the associativity conditions (12) yield the trace conditions

$$m_i d_{ij} \equiv 0 \pmod{n/2}, \qquad m_j d_{ij} \equiv 0 \pmod{n/2}. \tag{21}$$

These must hold for all $i \neq j$, with $d_{ji} = -d_{ij}$.

LEMMA 3. *The number of integers $d_{ij}$ modulo $n/2$ which satisfy a trace condition* (21) *is the g.c.d.* $(m_i, m_j)$.

*Case* 1: $0 < i < j$. Here (21) states that $d_{ij}$ is a multiple of the integers $n/2m_i$ and $n/2m_j$. The smallest such multiple is the l.c.m. $[n/2m_i, n/2m_j]$; the the number of multiples (mod $n/2$) is

$$(n/2)[n/2m_i, n/2m_j]^{-1} = m_i m_j n[m_j n, m_i n]^{-1} = (m_i, m_j),$$

according to the relation $(m_i, m_j)[m_i, m_j] = m_i m_j$.

*Case* 2. $i = 0$, $n/m_0 \equiv 0 \pmod 2$. Here $n/2m_0$ is an integer, so the argument proceeds exactly as in Case 1.

*Case* 3. $i = 0$, $n/m_0 \not\equiv 0 \pmod 2$. The congruence $m_0 d_{0j} = 2r d_{0j} \equiv 0$ of (21) becomes here $2d_{0j} \equiv 0 \pmod{n/m_0}$. The latter modulus is odd by assumption, so $d_{0j} \equiv 0 \pmod{n/m_0}$. Computations now give $(m_j, r)$ solutions $d_{0j}$. But the hypothesis $n/m_0 \not\equiv 0 \pmod 2$, where $n/m_0 = m_1 \cdots m_j$, means that each $m_j$ must be odd. Therefore $(m_j, r) = (m_j, 2r) = (m_j, m_0)$ is the number of solutions.

Because this lemma gives the same total count $\prod_{i<j}(m_i, m_j)$ as that stated in our theorem, it will suffice to prove that each set of solutions $d_{ij}$ of the trace

conditions (21) is the trace belonging to one and only one group extension. Because a transformation quantity $D_{ij}$ of (10) has trace zero, each group extension $\mathfrak{E}$ determines the trace $d_{ij}$ uniquely. It remains only to prove that each set of solutions $d_{ij}$ is the trace of some factor set and that a factor set with traces $d_{ij}=0$ is a transformation quantity (and so belongs to the unit extension).

**Step III. The realization of invariants by factor sets.** To given $d_{ij}$ we wish to construct a factor set

$$C_0 = \exp\left[\sum_{\beta} c_0(\beta)\beta\right], \qquad D_{ij} = \exp\left[\sum_{\beta} d_{ij}(\beta)\beta\right]. \tag{22}$$

The integral exponents $c_0(\beta)=c(\beta)$ and $d_{ij}(\beta)$ must satisfy the associativity conditions (12). The second condition of (12), after substitution of the expressions (22), takes on the forms (the first for $i=0$, the second for $i\neq 0$)

$$g_{0j} + c_0(\beta\alpha_j^{-1}) - c_0(\beta) = 2\sum_{k=0}^{r-1} d_{0j}(\beta\alpha_0^k), \qquad (j \neq 0, \text{ all } \beta), \tag{23}$$

$$g_{ij} = \sum_{k=0}^{m_i-1} d_{ij}(\beta\alpha_i^k), \qquad (\text{all } j \neq i,\ i \neq 0), \tag{24}$$

where $g_{ij}$ represents a change of gauge. These gauges may be determined in terms of the traces. In (24) let $\beta'$ run through all elements (4) not involving $\alpha_i$. By adding these $n/2m_i$ equations, one gets

$$ng_{ij}/2m_i = \sum_{\beta'} \sum_{k=0}^{m_i-1} d_{ij}(\beta'\alpha_i^k) = \sum_{\beta} d_{ij}(\beta) = d_{ij}.$$

Hence $g_{ij}=2m_id_{ij}/n$. A similar addition of (23) gives $g_{0j}$. For a fixed choice of gauge for $C_0$ and $D_{ij}$ in (22) we have

$$g_{ij} = 2m_id_{ij}/n, \qquad (\text{all } i \neq j). \tag{25}$$

The trace conditions (21) assert that these constants $g_{ij}$ are integers.

Since $t(AB)=t(A)+t(B)$, it will be possible to realize any allowable set of invariants $d_{ij}$ if these invariants can be realized one at a time. The cases $i=0$ and $0<i<j$ behave differently, as we now show by treating the typical cases $d_{12}$ and $d_{01}$.

LEMMA 4. *If $d_{12}$ is a solution of the trace conditions* (21), *with $i=1$, $j=2$, there exists a factor set $\{C_0, D_{ij}\}$ with $C_0=D_{ij}=1$ for $(i, j)\neq(1, 2)$ and with $t(D_{12})=d_{12}$.*

**Proof.** The essential associativity condition is (24) with $i=1$, $j=2$ and $i=2, j=1$; the trace conditions insure that $g_{12}$ and $g_{21}$ are integers. If we regard the exponents $d_{12}(\sigma\alpha_1^h\alpha_2^k) = -d_{21}(\sigma\alpha_1^h\alpha_2^k)$ for fixed $\sigma$ as the terms of an $m_1$ by $m_2$

matrix, condition (24) requires that each column ($h=0, \cdots, m_1-1$) add up to $g_{12}$, and that each row ($k=0, \cdots, m_2-1$) add up to $-g_{21}$. These two requirements are consistent because the sum of all terms by rows is $-m_1g_{21}$, by columns is $m_2g_{12}$, and these two sums are equal by (25), with $d_{12}=-d_{21}$. The requirements may be met by making the matrix $\|d_{12}(\sigma\alpha_1^h\alpha_2^k)\|$ zero except in the first row and column, as

$$d_{12}(\sigma\overset{h}{\alpha_1}\overset{k}{\alpha_2}) = 0,\ d_{12}(\sigma\overset{h}{\alpha_1}) = -g_{21},\ d_{12}(\sigma\overset{k}{\alpha_2}) = g_{12}\ (h, k \neq 0),$$

$$d_{12}(\sigma) = g_{12} + g_{21} + m_1g_{21} = g_{12} + g_{21} - m_2g_{12}.$$

For any $\sigma=\alpha_0^{e_0}\alpha_3^{e_3}\cdots\alpha_s^{e_s}$ in the group generated by the remaining $\alpha$'s we take these equations as defining the quantity $D_{12}$. They satisfy the associativity conditions (24), as may be seen by substitution. Furthermore this definition is independent of the choice of $\sigma$, so the resulting $D_{12}$ is invariant under any $\alpha\neq\alpha_1$ and $\alpha_2$. Therefore $D_{12}^{\alpha^{-1}}=1$. Every other $D_{ij}$ is to be 1, so the last associativity condition connecting any three $D$'s as in (12) is satisfied, and the lemma holds.

LEMMA 5. *If $d_{01}$ is a solution of the trace conditions* (21) *with $i=0$ and $j=1$, there exists a factor set $\{C_0, D_{ij}\}$ with $D_{ij}=1$ for $(i, j)\neq(0, 1)$ and with $t(D_{01})=d_{01}$.*

**Proof.** Much as in the proof of Lemma 3, a separate treatment is necessary in the case when $m_1\equiv 0 \pmod 2$ (i.e., when $\alpha_1$ has an even order).

*Case* 1. $m_1\not\equiv 0 \pmod 2$. If we set $C_0=1$, the associativity conditions ((24) with $j=0$, $i=1$ and (23) with $j=1$) become

$$\sum_{k=0}^{m_1-1} d_{01}(\sigma\overset{h}{\alpha_0}\overset{k}{\alpha_1}) = -g_{10}, \qquad \sum_{h=0}^{r-1} d_{01}(\sigma\overset{h}{\alpha_0}\overset{k}{\alpha_1}) = g_{01}/2.$$

By (25) the integers $g_{10}$ and $g_{01}$ satisfy $m_1g_{01}=-m_0g_{10}$. Since $m_0=2r$ is even and $m_1$ is odd, $g_{01}$ must be even and $g_{01}/2$ is an integer. These equations again specify the row and column sums of a matrix, and may be solved exactly as in the previous lemma.

*Case* 2. $m_1\equiv 0 \pmod 2$. We choose $d_{10}=-d_{01}$. By the trace condition on $d_{01}$, the constants $g_{01}$ and $g_{10}$ of (25) are integers, and by (25) they satisfy $m_1g_{01}=-m_0g_{10}$. We no longer choose $C_0=1$, but set instead

$$C_0(\sigma\overset{h}{\alpha_0}\overset{k}{\alpha_1}) = kg_{01}, \qquad (\sigma = \alpha_2^{e_2}\cdots\alpha_s^{e_s};\ h=0, \cdots, r-1;\ k=0, \cdots, m_1-1). \tag{26}$$

For $\beta=\sigma\alpha_0^h\alpha_1^k$ the quantity $c_0(\beta\alpha_1^{-1})-c_0(\beta)$ of (23) is, according to this agreement, $(k-1)g_{01}-kg_{01}=-g_{01}$, provided $k\neq 0$. If $k=0$, it is $(m_1-1)g_{01}$. Therefore (23) and (24) give the associativity conditions

$$(27)\qquad \sum_{h=0}^{r-1} d_{01}(\sigma\alpha_0^h) = m_1 g_{01}/2, \qquad \sum_{h=0}^{r-1} d_{01}(\sigma\alpha_0^h\alpha_1^k) = 0, \qquad (k \neq 0),$$

$$(28)\qquad \sum_{k=0}^{m_1-1} d_{01}(\sigma\alpha_0^h\alpha_1^k) = -g_{10}, \qquad (\sigma = \alpha_2^{e_2}\cdots\alpha_s^{e_s}).$$

These requirements once more specify consistent row and column sums for a matrix $\|d_{01}(\sigma\alpha_0^h\alpha_1^k)\|$. A solution is given by

$$(29)\qquad d_{01}(\sigma\alpha_0^h\alpha_1^k) = 0, \quad (k \neq 0); \qquad d_{01}(\sigma\alpha_0^h) = -g_{10},$$

where $\sigma$ again is any element in the subgroup generated by $\alpha_2, \cdots, \alpha_s$. These formulas provide a construction of a $D_{01}$ from the given integer $d_{01}$. Because the formulas (29) do not depend on $\sigma$, $D_{01}^{\alpha} = D_{01}$ for any $\alpha$ not $\alpha_0$ or $\alpha_1$. For this reason all the associativity conditions of (12) are satisfied if the remaining $D_{ij}$ are all 1. This proves the lemma. Combination of these results proves

LEMMA 6. *Any set of integral solutions $d_{ij}$ of the trace conditions* (21) *is the trace of some factor set* $\{C_0, D_{ij}\}$.

In Case 2 of the proof of Lemma 5 the use of the constant $C_0 \neq 1$ is essential (at least whenever $g_{01} \not\equiv 0 \pmod 2$). One may show by examples that this is the case; the result will subsequently throw some light on the relation of the ramified group P to Schur's multiplicator.

LEMMA 7. *For some abelian groups* $\Gamma$ *there is a factor set* $\{C_0, D_{ij}\}$ *with* $t(C_0) \not\equiv 0 \pmod{n/2}$.

**Proof.** The expression $C_0$ constructed in (26) has

$$t(C_0) \equiv (n/2)(m_1 + 1)g_{01}/2.$$

This will satisfy $t(C_0) \equiv 0 \pmod{n/2}$ only if $m_1$ is odd or $g_{01}$ is even. Sometimes neither will be the case, as for instance when $\Gamma = \{\alpha_0\} \times \{\alpha_1\}$ with $\alpha_0$ of order 2, $\alpha_1$ of order 6. Then $m_1 = 6 \equiv 0 \pmod 2$, $n = 12$, and the constant $d_{01} = 3$ satisfies the trace condition. It gives $g_{01} = 1$ by (25). Hence $t(C_0) = 6(7/2) = 21 \not\equiv 0 \pmod 6$. Since $t(C_0)$ cannot be altered, mod 2, by the insertion of any transformation quantities (10), the factor set so constructed cannot be equivalent to any factor set with $C_0 = 1$.

**Step IV. The reduction of factor sets with zero traces.**

LEMMA 8. *If a factor set* $\{C_0, D_{ij}\}$ *has traces* $t(D_{ij}) = d_{ij} \equiv 0 \pmod{n/2}$, *then* $C_0$ *may be reduced to* 1 *by a suitable transformation set*

**Proof.** By suitable choice of gauge in (22), all $d_{ij}$ are zero identically. Then $g_{0j} = 0$ by (25), so the associativity condition (23) makes $c_0(\beta\alpha_j^{-1}) - c_0(\beta) \equiv 0 \pmod 2$. By applying this repeatedly for all $j = 1, \cdots, s$, one proves

$c_0(\beta') \equiv c_0(1) \pmod 2$ for every $\beta'$ in the group generated by $\alpha_1, \cdots, \alpha_s$. According to Lemma 2, $C_0$ may then be reduced to 1.

After this reduction the associativity conditions (12) satisfied by any one constant $D_{ij}$ have the form

$$N_i D_{ij} = 1, \qquad N_j D_{ij} = 1, \qquad t(D_{ij}) \equiv 0 \pmod{n/2}. \tag{30}$$

The essential step is the demonstration that each $D$ which satisfies conditions of this form may be removed by an appropriately chosen transformation quantity. This is essentially accomplished by a lemma related closely to a lemma of Clifford's [12].

LEMMA 9. *If an element $D$ in the unit group* P *satisfies conditions $t(D) \equiv 0 \pmod{n/2}$ and $N_i D = 1$, there exists in* P *an element $A$ such that $D = A^{1-\alpha}$, where $\alpha = \alpha_i$. The quantity $A$ may be so constructed that, for every $j \neq i$, $N_j D = 1$ implies $N_j A = 1$ and $D = D^{\alpha j}$ implies $A = A^{\alpha j}$.*

**Proof.** Write $D = \exp\left(\sum_\beta d(\beta)\beta\right)$. The hypothesis $t(D) \equiv 0$ means that $d = \sum_\beta d(\beta) \equiv 0 \pmod{n/2}$. By a suitable choice of gauge for $D$ we may actually get $d = 0$. The hypothesis $N_i D = 1$ may now be expressed in terms of the exponents $d(\beta)$ exactly as in (23) and (24). Because the trace $d$ is zero, the gauges $g_{ij}$, computed as in (25), are also zero, so the condition $N_i D = 1$ becomes

$$\sum_h d(\beta \alpha_i^h) = 0 \qquad (h = 0, \cdots, m_i - 1). \tag{31}$$

We seek an $A = \exp\left\{\sum_\beta a(\beta)\beta\right\}$ to satisfy the equation $A^{1-\alpha} = D$, where $\alpha = \alpha_i$. In terms of the exponents $a(\beta)$ this equation is

$$a(\beta) - a(\beta\alpha^{-1}) = d(\beta) + g \qquad (g \text{ a constant for all } \beta). \tag{32}$$

To solve this explicitly, write $\beta = \tau\alpha^e$ in such wise that $\tau$ involves only the generators $\alpha_j \neq \alpha$, and try

$$a(\tau\alpha^e) = \sum_{k=0}^{e} d(\tau\alpha^k), \qquad (e = 0, 1, \cdots, m_i - 1, \text{ if } i \neq 0). \tag{33}$$

If $e = m_i$, then $\tau\alpha^e = \tau$ and this equation is still valid in virtue of the hypothesis (31). Therefore (33) holds for every integer $e \geqq 0$. By substitution we then find that this proposed $A$ does satisfy the required condition (32), with a gauge $g = 0$.

The case $\alpha = \alpha_0$ may be treated by a minor modification of this argument. For a solution $A$ we need define the exponent $a(\tau\alpha^e)$ only in the range $e = 0, \cdots, r-1$, where $r = m_0/2$. Again we adopt (33) as the definition in this range. Since the original exponents $d$ satisfy $d(\beta\alpha^r) = d(\beta)$, the hypothesis (31) may now be written $2\sum_h d(\beta\alpha_0^h) = 0$, where $h$ runs from 0 to $r-1$. There-

fore (33) again holds for all integers $e$ outside the original range of definition, and we have constructed $A$ to satisfy $a(\beta\alpha^r)=a(\beta)$, as desired.

The construction (33) gives an element $A$ with the added properties asserted in the lemma. Because $t(D)=0$, an added hypothesis $N_jD=1$ would again mean

$$\sum_h d(\beta\alpha_j^h) = 0, \qquad (h = 0, 1, \cdots, m_j - 1). \tag{34}$$

On the other hand, $N_jA$ is by definition

$$N_jA = \exp\left\{\sum_\beta a(\beta)\beta\left(\sum_h \alpha_j^h\right)\right\} = \exp\left\{\sum_\beta\left(\sum_{h'} a(\beta\alpha_j^{h'})\beta\right)\right\}.$$

Set $\beta=\tau\alpha^e$, and compute each exponent, by (33), as

$$\sum_h a(\tau\alpha^e\alpha_j^h) = \sum_{h=0}^{m_j-1}\sum_{k=0}^{e} d(\tau\alpha^k\alpha_j^h) = \sum_k\sum_h d(\tau\alpha^k\alpha_j^h).$$

This sum is 0, by the hypothesis (34); hence $N_jA=1$.

Suppose next that $D=D^{\alpha_j}$. Exactly as in the argument in (14), this means that the exponents satisfy $d(\beta)=d(\beta\alpha_j)$. With the definition (33) one then has also $a(\beta)=a(\beta\alpha_i)$, hence $A=A^{\alpha_i}$, q.e.d.

By this lemma, any individual $D_{ij}$ may be reduced. For example $N_0D_{01}=N_1D_{01}=1$ by the associativity conditions (30), so there must exist an $A_0$ with $A_0^{1-\alpha_1}=D_{01}$ and $N_0A_0=1$. According to the formulas (10) for transformation quantities, a change $v_0=A_0^{-1}u_0$ in the coset representation will then replace $D_{01}$ by 1 without disturbing the normalization $C_0=1$ already achieved in Lemma 8. This process continues as in

LEMMA 10. *If $1\leqq k\leqq s$, every factor set $\{C_i, D_{ij}\}$ with traces $t(D_{ij})\equiv 0$ is similar to a factor set with $C_i=1$ for all $i$ and $D_{ij}=1$ for all $i$ and $j$ which satisfy $0\leqq i<j\leqq k$.*

**Proof.** The above reduction of $D_{01}$ takes care of the case $k=1$. Assume by induction that the lemma is true for $k-1$, and by a second induction that $D_{0k}=\cdots=D_{j-1\,k}=1$ (the case $j=0$ will be included in the induction argument). For the next constant $D_{ik}$ use at long last the third associativity condition of (12), which enforces a relation between three constants $D$. For each $i<j$ the constants $D_{ij}$ and $D_{ki}=D_{ik}^{-1}$ have already been made equal to 1, so this third condition becomes $D_{jk}^{\alpha-1}=1$ for $\alpha=\alpha_0, \cdots, \alpha_{j-1}$. The other conditions on $D_{jk}$ are $N_jD_{jk}=N_kD_{jk}=1$. By Lemma 9 there exists an $A_k$ with

$$D_{jk} = A_k^{1-\alpha_j}, \qquad N_kA_k = 1, \qquad A_k^{\alpha_0} = \cdots = A_k^{\alpha_{j-1}} = A.$$

Make the corresponding change $v_k=A_k^{-1}u_k$ in the coset representatives (7). According to the list of transformation quantities (10), this change reduces

$D_{jk}$ to 1 and modifies each of $C_k$ and $D_{ik}$ for $i=0, \cdots, j-1$ by 1. In other words, the new reduction $D_{jk}=1$ is accomplished without disturbance of the results of previous reductions. This completes the induction, and proves

LEMMA 11. *Every factor set with traces zero is similar to* 1.

With this lemma the proof of Theorem 1 of this section is complete. Our argument has actually shown that the group of classes of factor sets is isomorphic to the additive group of traces $d_{ij}$. Each trace by itself gives a cyclic group of order $(m_i, m_j)$, hence

THEOREM 22.2. *The group* $F\mathrm{P}/T\mathrm{P}$ *of group extensions of* P *by an abelian group* $\Gamma$ *is the direct product of cyclic groups of orders* $(m_i, m_j)$, *for all* $0 \leqq i < j \leqq s$.

For an unramified unit group $H$ exactly the same two theorems are true; they have been established by more general arguments than ours in Clifford [12]. It is proved there that $FH/TH$ is isomorphic to the multiplicator $\mathfrak{M}$ of $\Gamma$ in an algebraically closed field of characteristic $\infty$. This multiplicator can be represented by factor sets of $n$th roots of unity or, equally well, of integers modulo $n$, but the resulting factor sets of integers can always be normalized so that the constants for $c_i = u_i^{m_i}$ are all 0. In the unramified case, the trace maps the group $FH/TH$ isomorphically on this representation of the multiplicator $\mathfrak{M}$, as is proved by Clifford. In the ramified case the group $F\mathrm{P}/T\mathrm{P}$ is still isomorphic to the multiplicator, in virtue of Theorem 22.2; however, the trace $t(A)$ no longer provides an isomorphic map of $F\mathrm{P}/T\mathrm{P}$ on $\mathfrak{M}$. This curious anomaly is a consequence of Lemma 7 above, which asserts that for the ramified case the constant $C_0$ cannot always be reduced to 1, although it can be so reduced in the case of the multiplicator.

23. **Crossed characters for abstract unit groups.** The index $J(E^*)$ for the Herbrand unit group $E^*$ has as numerator $[UE^*:E^{*1-\sigma}]$, the number of classes of crossed characters (see §7) of $\Gamma$ in $E^*$. Since $E^*$ is a direct product (see the end of §17), this index can be written as a product

$$(1) \qquad [UE^*:E^{*1-\sigma}] = \prod_{i=1}^{r} [U\epsilon_i:\epsilon_i^{1-\sigma}] \prod_{i=1}^{r+1} [UH_i:H_i^{1-\sigma}].$$

The first $r$ factors in (1) involve the number of classes of crossed characters of $\Gamma$ in an infinite cyclic group $\epsilon_i$ generated by one of the $r$ chosen independent units $\epsilon_i$ of $\epsilon \cap E^*$. Since the elements of $\epsilon$ are invariant under the operators of $\Gamma$, it results that these crossed characters are all ordinary characters. But $\Gamma$ is a finite group, hence it has no non-trivial ordinary characters in an infinite cyclic group. The first product in (1) is therefore 1.

The second product in (1) involves both ramified and unramified unit groups $H_i$. Consider for the moment a ramified group P, associated with an automorphism $\delta$ of order 2, which generates the corresponding decomposition

group. As in definition (10) of §17, the group P then has $n/2$ generators $P^{\sigma_i}$, where $\sigma_i$ are representatives of the left cosets of $\Gamma$ modulo $\{1, \delta\}$. An element $A$ of the group P can be represented (but not uniquely!) in the form

$$A = P^{a_1\sigma_1}P^{a_2\sigma_2}\cdots P^{a_m\sigma_m}, \qquad m = n/2. \tag{2}$$

We again associate with $A$ the "trace" as an essential invariant([57]),

$$a = t(A) \equiv a_1 + a_2 + \cdots + a_m \pmod{m}. \tag{3}$$

Since the representation (2) of $A$ can be altered only by using the relation $1 = P^{\sigma_1}\cdots P^{\sigma_m}$, the function $t(A)$ is uniquely determined by $A$, modulo $m$. Furthermore

$$\begin{aligned} t(AB) &\equiv t(A) + t(B) \pmod{m}, \\ t(A^\tau) &\equiv t(A) \pmod{m}, \qquad \tau \text{ in } \Gamma. \end{aligned} \tag{4}$$

Given a crossed character $U(\sigma)$ of $\Gamma$ in this group P, we define

$$\chi(\sigma) = t[U(\sigma)], \qquad \text{all } \sigma \text{ in } \Gamma. \tag{5}$$

The definition of a crossed character (§7) implies at once that this function is an (ordinary) character of $\Gamma$ in the group of integers modulo $m$, with

$$\chi(\sigma\tau) \equiv \chi(\sigma) + \chi(\tau) \pmod{m}. \tag{6}$$

We say that a crossed character $U$P lies in the principal genus $G$P if and only if the corresponding function $\chi$ is the identity, so that the principal genus consists of all functions $G(\sigma)$ on $\Gamma$ to P with the properties

(*23.1) $G(\sigma\tau) = G(\sigma)[G(\tau)]^\sigma$, $t(G_\sigma) \equiv 0 \pmod{m}$.

By using the homomorphism which carries each crossed character $U$ into the character $\chi$ of (5), we shall prove

THEOREM 23.1. *For a ramified abstract unit group* P *whose decomposition group is generated by* $\delta$ $(\delta^2 = 1)$ *the number of classes of crossed characters is given by*

$$[U\mathrm{P}:\mathrm{P}^{1-\sigma}] = [G\mathrm{P}:\mathrm{P}^{1-\sigma}][\Gamma:\{\Gamma', \delta\}], \tag{7}$$

*where the first index measures the number of classes of crossed characters in the principal genus, while the second factor is the index in* $\Gamma$ *of the subgroup generated by* $\delta$ *and the commutator group* $\Gamma'$.

**Proof.** The index $[\Gamma:\{\Gamma', \delta\}]$ is simply the number of (ordinary) characters of the abelian factor group $\Gamma/\{\Gamma', \delta\}$. The homomorphism principle of §9 applied to the map $U \to \chi$ will therefore yield the conclusion (7) directly,

([57]) The character group of $P$ in the group of real numbers modulo 1 is a cyclic group generated by $\chi(A) = t(A)/m$. This is the reason for the importance of $t$.

once we prove that the characters $\chi$ obtained by this homomorphism are indeed the characters of $\Gamma/\{\Gamma', \delta\}$. To achieve this goal we prove two lemmas, from which the desired description of the $\chi$ will follow immediately.

LEMMA 1. *For any $\sigma$ in $\{\Gamma', \delta\}$, $\chi(\sigma)\equiv 0 \pmod m$.*

**Proof.** This lemma asserts that $\chi$ can be considered as a character defined for the cosets of the factor group $\Gamma/\{\Gamma', \delta\}$. First observe that (6) shows that $\chi(\sigma)\equiv 0 \pmod m$ whenever $\sigma$ is a commutator in $\Gamma'$. It remains only to prove $\chi(\delta)\equiv 0 \pmod m$. By the definition (5), $\chi(\delta)\equiv t[U(\delta)]$. As in (2), we use for $U(\delta)$ the notation

$$U(\delta) = \prod_{i=1}^{m} \mathrm{P}^{d_i\sigma_i}, \qquad \chi(\delta) \equiv \sum_{i=1}^{m} d_i \pmod m. \tag{8}$$

For a crossed character, $U_\sigma U_\tau^\sigma = U_{\sigma\tau}$, by definition. With $\sigma=\tau=1$ and $\sigma=\tau=\delta$ this gives the conclusions

$$U(1) = 1, \qquad [U(\delta)]^{1+\delta} = U(\delta^2) = 1. \tag{9}$$

We proceed to express the second of these conditions in terms of the exponents $d_i$ entering into the value $\chi(\delta)$ of (8). For

$$[U(\delta)]^\delta = \prod_{i=1}^{m} (\mathrm{P}^{d_i\sigma_i})^\delta = \prod_{i=1}^{m} \mathrm{P}^{d_i\delta\sigma_i} = \prod_{i=1}^{m} \mathrm{P}^{d_i\sigma_j}$$

where $\sigma_j$ $(j=j_i)$ is the representative belonging to the left coset $\sigma_j\{1, \delta\}$ in which the product $\delta\sigma_i$ lies. The correspondence $i\leftrightarrow j_i=j$ is an involution, so $\sum d_i\sigma_j=\sum d_j\sigma_i$ and

$$[U(\delta)]^{1+\delta} = \prod_{i=1}^{m} \mathrm{P}^{d_i\sigma_i} \prod_{i=1}^{m} \mathrm{P}^{d_i\sigma_j} = \prod_{i=1}^{m} \mathrm{P}^{s_i\sigma_i}$$

where $s_i=d_i+d_j$. This product is 1 by (9), and this must be a consequence of the basic relation $\prod_{i=1}^{m}\mathrm{P}^{\sigma_i}=1$ for our abstract ramified unit group P. There is therefore an integer $g$ such that

$$d_i + d_j = g, \qquad i = 1, 2, \cdots, m, j = j_i. \tag{10}$$

If $i=1$ belongs to the coset of 1, $j_i$ is also 1. Consequently $g=d_1+d_1=2d_1$ is even. If $i$ runs over all integers from 1 to $m$, so does $j_i$. Adding (10) over all $i$, we get

$$2\sum_{i=1}^{m} d_i = gm, \qquad \sum_{i=1}^{m} d_i = (g/2)m \equiv 0 \pmod m.$$

According to the formula (8) for $\chi(\delta)$, this yields $\chi(\delta)\equiv 0 \pmod m$, as required for the lemma.

LEMMA 2. *Any character* $\chi$ *of* $\Gamma/\{\Gamma', \delta\}$ *can be realized as a trace* (5) *of some crossed character* $U$P.

**Proof.** We observe first that $\delta$ has order 2, whence $\{\Gamma', \delta\}$ has even order and $\Gamma/\{\Gamma', \delta\}$ has as order a divisor of $m=n/2$. This means that any one of the $[\Gamma:\{\Gamma', \delta\}]$ characters of the abelian quotient group $\Gamma/\{\Gamma', \delta\}$ can in fact be expressed as a homomorphic mapping $\sigma\rightarrow\chi(\sigma)$ of $\Gamma$ on the integers modulo $m$. As is well known, the representation of the abelian group $\Gamma/\{\Gamma', \delta\}$ as a direct product of cyclic groups makes it possible to write any character of $\Gamma/\{\Gamma', \delta\}$ as a product of characters, each of which is defined on a cyclic quotient group of $\Gamma$. To consider such a sample quotient group, let $\Omega\supset\{\Gamma', \delta\}$ be a subgroup of $\Gamma$ such that $\Gamma/\Omega$ is cyclic of order $h$, and let $\alpha$ be a representative of some coset of $\Gamma/\Omega$ which generates this cyclic group. Then any $\sigma$ in $\Gamma$ can be written as

$$\sigma = \alpha^i\omega; \qquad i = 0, 1, \cdots, h-1; \ \omega \text{ in } \Omega, \ \alpha^h \text{ in } \Omega. \tag{11}$$

To realize all possible characters $\chi$ of $\Gamma$ by crossed characters it will thus suffice to realize any character of the form

$$\begin{aligned} &\chi(\alpha) \equiv m/h \pmod m, \\ &\chi(\omega) \equiv 0 \pmod m, \qquad \text{all } \omega \text{ in } \Omega. \end{aligned} \tag{12}$$

Let $\Omega$ be decomposed modulo $\{1, \delta\}$ into $m/h$ left cosets, $\Omega=\sum_i\omega_i\{1, \delta\}$, with representatives $\omega_i$. Define next an element $C$ in P by the equations

$$C = \prod_i \mathrm{P}^{\omega_i}, \qquad j = 1, 2, \cdots, m/h. \tag{13}$$

This element $C$ has the properties

$$\begin{aligned} &t(C) \equiv m/h \pmod m, \\ &C^\omega = C, \qquad \text{for } \omega \text{ in } \Omega. \end{aligned} \tag{14}$$

In terms of this element $C$ we propose to define for every group element $\sigma$, given as in (11), a value

$$U(\alpha^i\omega) = C^{1+\alpha+\cdots+\alpha^i}, \qquad \sigma = \alpha^i\omega, \tag{15}$$

of a crossed character $U(\sigma)$. This definition is given only for $i=0, \cdots, h-1$, but the formula holds good for all values of $i$, because $\alpha^h$ lies in $\Omega$ and because the definition of $C$ implies that $C^{1+\alpha+\cdots+\alpha^{m-1}}=1$. With the formula (15), so generalized, a straightforward computation then shows that the function $U(\sigma)$ is a crossed character. By (14) and (15)

$$\begin{aligned} \chi(\alpha) &= t[U(\alpha)] = t(C) \equiv m/h \pmod m, \\ \chi(\omega) &= t(C^0) \equiv 0 \pmod m. \end{aligned}$$

Therefore this crossed character does realize the sample character $\chi$ given in (12). This completes the proof of Lemma 2 and with it, of Theorem 23.1.

It remains to consider the unramified abstract unit groups $H$. In such a group an arbitrary element $A = \prod_\sigma H^{a(\sigma)\sigma}$ again has a trace, given by

$$t(A) \equiv \sum_\sigma a(\sigma) \pmod{n}. \tag{16}$$

The principal genus consists of those functions $G$ on $\Gamma$ to $H$ which satisfy

(*23.2) $G(\sigma\tau) = G(\sigma)[G(\tau)]^\sigma$, $t[G(\sigma)] \equiv 0 \pmod{n}$.

The subsequent argument proceeds as in the ramified case, with appropriate simplifications. The result is

THEOREM 23.2. *For an unramified abstract unit group $H$ the number of classes of crossed characters of $\Gamma$ in $H$ is*

$$[UH:H^{1-\sigma}] = [GH:H^{1-\sigma}][\Gamma:\Gamma'], \tag{17}$$

*where $GH$ is the principal genus, $\Gamma'$ the commutator group.*

In many cases this approach will actually yield explicit answers. For a solvable group $\Gamma$, A. H. Clifford has shown [12] that the principal genus index in the unramified case is 1,

$$[GH:H^{1-\sigma}] = 1. \tag{18}$$

The authors have extended Clifford's proof to the ramified case, for $\Gamma$ abelian.

These results can be combined to give the number of crossed characters for the whole Herbrand unit group $E^*$. For the ramified cases this will involve the index $[\Gamma:\{\Gamma', \delta\}]$ which will have the value $[\Gamma:\Gamma']$ or $[\Gamma:\Gamma']2^{-1}$ according as the automorphism $\delta$ of order 2 does or does not lie in the commutator group $\Gamma'$. Now $\delta$ was introduced as a generator of the decomposition group of a factor $P_\infty$ of one of the ramified infinite prime divisors $p_\infty$ of $K/k$. The field of elements left invariant by $\delta$ is then the largest subfield of $K$ in which $p_\infty$ is unramified. Consequently the statement that $\delta$ lies in $\Gamma'$ is equivalent to the statement that $p_\infty$ is unramified in the field $K'$ corresponding to $\Gamma'$. Only in this case is the index $[\Gamma:\{\Gamma', \delta\}]$ equal to $[\Gamma:\Gamma']$. All told, the $r_1 - \rho_1$ ramified unit groups $P_i$ contribute to the crossed character formula (1) a term $[\Gamma:\Gamma']^{r_1-\rho_1} 2^{-\rho'}$, where

(*23.3) $\rho' =$ the number of infinite prime divisors of $k$ which are ramified in $K'$.

The combination of Theorems 23.1 and 23.2 yields

THEOREM 23.3. *The number of classes of crossed characters for any Herbrand unit group $E^*$ is*

$$(19)\qquad [UE^*:E^{*1-\sigma}] = [\Gamma:\Gamma']^{r+1}[GH:H^{1-\sigma}]^{\rho_1+r_2}2^{-\rho'}\prod_{p\infty}[GP:P^{1-\sigma}],$$

*where $H$ is an abstract unramified unit group, and where the last product is taken over all the unit groups $P=P_\delta$ belonging to the ramified prime divisors $p_\infty$ of $K/k$, while $GH$, $GP$ refer to the principal genus defined in* (*23.1), (*23.2).

## CHAPTER IV. THE FINAL FORMULA

24. **The composite result.** The unit index $J(E)$ has now been evaluated in terms of the correction factor $\phi=J(E)/J(E^*)$ and in the explicit computations of Theorems 23.3 and 22.1. If these results are put in the formula (15) of §16, we obtain

THEOREM 24.1. *For any normal extension $K/k$ and any module $M$ which involves all prime divisors $p$ of $k$ ramified in $K/k$, the least common multiple $J=J(\Gamma)$ of the orders of the elements of the Galois group $\Gamma$ can be expressed as*

$$(1)\qquad J = n^*n^{-1}\omega(A', E)\omega(\mathfrak{A}', (A'))^{-1}2^{\rho}J(A^{\#})^{-1}J(E),$$

*where $J(\mathfrak{A}^{\#})=[U\mathfrak{A}^{\#}:\mathfrak{A}^{\#1-\sigma}][F\mathfrak{A}^{\#}:T\mathfrak{A}^{\#}]^{-1}$ depends only on the structure of the class group $\mathfrak{A}^{\#}$, while $J(E)$ depends only on the structure of the group of units in $K$, by*

$$(2)\qquad \begin{aligned} J(E) &= \phi[\Gamma:\Gamma']2^{-\rho'}\{[GH:H^{1-\sigma}][FH:TH]^{-1}\}^{\rho_1+r_2} \\ &\quad\cdot\prod_{i=1}^{\rho}\{[GP_i:P_i^{1-\sigma}][FP_i:TP_i]^{-1}\}. \end{aligned}$$

*Alternately, $J(E)$ may be expressed by the formula of Theorem* 20.1. *All the indices appearing in these formulas are finite.*

We pause to identify the various invariants which appear in these formulas. In $J$, $n^*$ is an integer which is a divisor of $n$ and a multiple of $J(\Gamma)$, as given explicitly by formula (*13.4);

$\Gamma'$ = the commutator group of $\Gamma$;

$\rho'$ = the number of infinite prime divisors in $k$ ramified in the commutator subfield $K'$ of $K$;

$\mathfrak{A}^{\#}$ = the groups of ideal classes in $K$;

$A'(\mathfrak{A}')$ = the groups of numbers (ideals) in $K$ which are relatively prime to $M$.

The class group enters in the numerator only in terms of $[F\mathfrak{A}^{\#}:T\mathfrak{A}^{\#}]$, the number of extensions of $\mathfrak{A}^{\#}$ by $\Gamma$, in the denominator only in terms of $[U\mathfrak{A}^{\#}:\mathfrak{A}^{\#1-\sigma}]$, the number of classes of crossed characters (see §7) of $\mathfrak{A}^{\#}$. The groups $A'$, $\mathfrak{A}'$

occur only in connection with the deficiency invariants which were defined in §15.

In the unit index (2) the correction factor $J(E)J(E^*)^{-1}=\phi$ is the quantity considered in §19. It need not be 1, as it would be in the cyclic case. It depends on the position of the Herbrand unit group $E^*$ within the whole group $E$ of units in $K$.

$\rho$ = the number of infinite prime divisors $p$ of $k$ ramified in $K$;

$\rho_1+r_2$ = the number of infinite prime divisors $p$ of $k$ which are unramified in $K$;

$H$ = the abstract unramified unit group for $\Gamma$;

$\mathrm{P}_i$ = the abstract ramified unit groups belonging to $\delta_i$: the generator of a decomposition group for the $i$th ramified infinite prime divisor of $k$.

It should be noted that the group $H$, as described in §17, depends only on the Galois group $\Gamma$ of $K/k$ and not on the further structure of $K/k$, while the various groups $\mathrm{P}_i$ depend only on $\Gamma$ and the position in $\Gamma$ of the automorphisms $\delta_i$. Each $\delta_i$ may be described as an automorphism in $\Gamma$ of order 2, such that the corresponding ramified infinite prime divisor $p_{\infty,i}$ of $k$ has a factor $P_i$ which is unramified in the subfield of $K$ left invariant by $\delta_i$.

The groups $H$ enter into the formula (2) in two fashions:

(a) through the number $[FH:TH]$ of extensions of $\Gamma$ by $H$, and

(b) through the number $[GH:H^{1-\sigma}]$ of classes of crossed characters in the "principal genus" of crossed characters, defined by (*23.2).

These quantities are explicitly computed in the case of abelian groups, as stated in §§22 and 23. Furthermore $\Gamma=\Gamma'$ in these cases.

THEOREM 24.2. *If the Galois group $\Gamma$ of $K/k$ is an abelian group, the direct product of $t$ cyclic groups of the respective orders $m_i$, then the least common multiple $J=[m_1, \cdots, m_t]$ is*

$$J = \phi n^*\{\omega(A', E)\omega(\mathfrak{A}', (A'))^{-1}\}J(\mathfrak{A}^{\#})^{-1}\left\{\prod_{i<j}(m_i, m_j)\right\}^{-r-1} \tag{3}$$

*where $r+1$ is the number of infinite prime divisors of $k$.*

The quantities which appear in our formulas (1) and (2) are all invariants of the extension $K/k$. This follows at once from the definition of the quantities, except for the quotient $\phi=J(E)J(E^*)^{-1}$ and the deficiency invariants $\omega$, which apparently depend on the module $M$. That the deficiency invariants $\omega$ are in fact independent of $M$, if $M$ has the properties of Theorem 24.1, was shown in §16. Since all the other indices in the formulas (1) and (2) are then invariants of the field $K/k$, it follows that the correction factor $\phi$ is an invari-

ant, too. In other words, $\phi$ is independent of the particular way in which the Herbrand unit group is chosen.

The invariants of $K/k$ which we have connected here are, roughly speaking, of four types: well recognized invariants, such as $\Gamma'$, $\rho_1$, $\rho'$, $n^*$ (in essence); invariants depending on the number of certain group extensions of groups belonging to $K/k$; invariants having to do with crossed characters; the invariant $\phi$ depending upon the explicit structure of $E$. In particular, all these invariants can be defined without reference to the auxiliary notion of factor set, except in the case of the invariant $\phi$.

One may also specialize the composite formula to the cyclic case. The invariant $n^*$ is a divisor of the order $n$ and also a multiple of the order $n$, so that $n^*=n$. The correction factor $\phi$ is 1 according to Theorem 19.1. The order of the multiplicator $\prod_{i<j}(m_i, m_j)$ is always 1.

THEOREM 24.3. *If $Z/k$ is a cyclic extension of $k$ with the class group $\mathfrak{A}^\#$, then the number $[F\mathfrak{A}^\#: T\mathfrak{A}^\#]$ of group extensions of this class group by the Galois group is related to the number of crossed characters of the Galois group in $\mathfrak{A}^\#$ by the equation*

$$\omega(\mathfrak{A}', (A'))\,[U\mathfrak{A}^\#:\mathfrak{A}^{\#1-\sigma}] = \omega(A', E)\,[F\mathfrak{A}^\#: T\mathfrak{A}^\#]. \tag{4}$$

*If the cyclic field and all its subfields have class number* 1, *all the terms in the equation* (4) *turn out to be* 1.

25. **Examples.** As an illustration and check of our composite formula we consider in this section some examples of biquadratic fields. We take biquadratic fields over the field of all rational numbers which have, with all their quadratic subfields, the class number 1.

The field $K=R(7^{1/2}, i)$, with $i=(-1)^{1/2}$, is the join of two quadratic fields, $R(i)$ and $R(7^{1/2})$, each of which is known[58] to have class number 1. By Hilbert's form of a theorem of Dirichlet [27, p. 51] the class number of $K$ is a factor of the product of the class numbers of $R(i)$ and $R(7^{1/2})$. Hence in $K$ every ideal is principal. The same is true for the third quadratic subfield $R((-7)^{1/2})$ of $K$. The terms involving the deficiency $\omega$ and the terms involving ideal classes $\mathfrak{A}^\#$ in the final formula for the abelian case are there all 1, hence formula (3) of §24 becomes

$$J = n^*(J(E)J(E^*)^{-1})\left[\prod_{i<j}(m_i, m_j)\right]^{-1}. \tag{1}$$

The Galois group of $K/R$ is the four group, so the least common multiple $J$ of the orders of the group elements is 2. The order $\prod_{i<j}(m_i, m_j)$ of the multiplicator turns out to be 2. The quantity $n^*$ can be computed, as in §13, in terms of the ramification orders of the various rational primes in $K$. The three

[58] See the list of quadratic fields in the back of [35].

quadratic subfields $R(7^{1/2})$, $R(i)$, $R((-7)^{1/2})$ have respectively the discriminants $7\cdot 2^2$, $-4$, and 7. It follows then that the only ramified prime divisors for $K/R$ are 2, 7, and $p_\infty$, the infinite prime divisor of $R$. The ramification orders are $e_1=e_7=e_\infty=2$. All the ramification orders are thus divisors of the index $J$, so that, according to Theorem 13.2, $n^*=n=4$.

Finally, the correction factor $J(E)J(E^*)^{-1}$ may be found directly, by the normalization method of §19, if one first computes the group $E$ of units in $K$. In the field $R(7^{1/2})$ the basic unit is $\rho=8+3(7^{1/2})$. By a computation resembling that in Lemma 3 of §19 one finally discovers that $\rho$ is the relative norm of a unit $\eta=(3+7^{1/2})(1+i)2^{-1}$ in the field $K$. One then shows that every unit in $K$ has the form $i^a\eta^b$. In the Galois group of $K/k$ let $\beta$, $\gamma$, and $\delta$ denote respectively the automorphisms which leave fixed the subfield $R(i)$, $R(7^{1/2})$, and $R((-7)^{1/2})$. The generating units $i$ and $\eta$ then behave under the various automorphisms as follows:

$$i^\beta = i, \qquad i^\gamma = i^\delta = i^3,$$

$$\eta^\beta = i\eta^{-1}, \qquad \eta^\gamma = i^3\eta, \qquad \eta^\delta = \eta^{-1}.$$

As an Herbrand subgroup one may choose the group generated by the unit $\mathrm{P}=i^3\eta^2$, which has the appropriate behaviour, $\mathrm{P}^\beta=\mathrm{P}$, $\mathrm{P}^{1+\gamma}=1$, relative to the generator $\beta$ of the decomposition group $\{1,\beta\}$ belonging to the only infinite prime divisor of $R$. The correction factor then involves the groups $D$ and $D^*$ defined in Lemma 2 of §19. One finds that $D$ is the group generated by $i$ and $\eta^2$, while $D^*=E^*$. Therefore

$$J(E)J(E^*)^{-1} = [E:E^*][D:D^*]^{-1}[\epsilon:1]^{-1} = 8(4\cdot 2)^{-1} = 1.$$

These values, substituted in (1), give an identity.

A similar check has been carried out for the field $R(2^{1/2}, i)$. The ramifications are $e_\infty=2$, $e_2=4$, consequently $n^*=2$. The class numbers for this field and its quadratic subfields are again all 1, so that (1) holds. The group of units $E$ is generated by a primitive 8th root of unity $\lambda=(1+i)(2^{1/2})^{-1}$ and by $\rho=1+2^{1/2}$. The unit $\rho^2$ may serve as generator of the Herbrand subgroup $E^*$. One finds $D^*=E^*$, while $D$ is generated by $i$ and $\rho^2$, whence the correction factor $J(E)J(E^*)^{-1}$ is 2. This again checks equation (1).

Another biquadratic field with class number 1 and with quadratic subfields of class number 1 is $R(3^{1/2}, i)$. The equation (1) again holds, this time with $e_2=e_3=e_\infty=2$, $n^*=4$, $E=\{\lambda, (1+3^{1/2})(1+i)2^{-1}\}$, $\lambda$ a primitive 12th root of unity, and $J(E)J(E^*)^{-1}=1$.

## Chapter V. Generalization of the classical symbols

26. **A conductor for factor sets.** One can construct an analogue to the conductor of the classical theory if one recalls that the conductor of a cyclic field $Z/k$ can be defined in terms of the local conductors (see [37]). For a local

cyclic extension $Z_P/k_p$ the conductor $c(Z_P/k_p)=p^h$ is defined as the smallest power of $p$ such that $a\equiv 1 \pmod{p^h}$ implies that $a$ is a norm.

We first prove the existence of a power of $P$ which will have the analogous property for factor sets. Consider a normal extension $K_P/k_p$ of degree $m_p=m$ with Galois group $\Delta(P)=\Delta$. Denote by $A_P=A$ the multiplicative group of the field $K_P$. Let $A_{\xi,\eta}$ denote the components of the factor sets in $FA$, while $TA$ are the analogous transformation quantities(59).

THEOREM 26.1. *For any normal extension $K_P/k_p$ there is a non-negative power $P^h$ of the prime divisor $P$ of $K_P$ such that every factor set $FA$ with components $F_{\xi,\eta}\equiv 1 \pmod{P^h}$ is a transformation set; in other words,*

$$F_{\xi,\eta}\equiv 1 \pmod{P^h} \text{ implies } F_{\xi,\eta}=TB_\xi \qquad \text{for suitable } B_\xi \text{ in } A. \tag{1}$$

**Proof.** Consider first the case where $P$ is a finite prime divisor, so that (1) is an ordinary congruence modulo the ideal $P^h$. As in the cyclic case, we may then furnish a proof by using the $P$-adic logarithm, $\log A$, and the corresponding exponential, $\exp[(\log A)/m]$. The exponent $h$ may be chosen so large that these expressions are uniquely defined(60) whenever $A\equiv 1 \pmod{P^h}$. Each such $A$ then has in $K_P$ a unique $m$th root, $B=\exp[(\log A)/m]$. For any factor set $F_{\xi,\eta}$ of (1) there will thus be a set of $m$th roots

$$B_{\xi,\eta}=\exp[(\log F_{\xi,\eta})/m]. \tag{2}$$

The associativity conditions for this set can then be derived from the conditions for $F_{\xi,\eta}$ by elementary properties of exponent and logarithm. Consequently $F_{\xi,\eta}=B_{\xi,\eta}^m$ is the $m$th power of a factor set, so it is a transformation set(61) by Lemma 1 of §1.

It remains to establish (1) in the case when $P$ is an infinite prime divisor. To insure the validity of the theorem in this case, we must use a new convention as to congruences modulo such a divisor. An infinite prime divisor $p_\infty$ of $k$ is in effect an isomorphic map $\psi_p(a)=a'$ of $k$ in a subfield $k'$ of the field of all complex numbers. The valuation belonging to $p_\infty$ is the valuation $\|a\|=|a'|$ induced on $k$ by the natural valuation of $k'$. If $p_\infty$ is real(62), then

$$a\equiv 1 \pmod{p_\infty} \qquad \text{if and only if } \psi_p(a)>0. \tag{3}$$

On the other hand, if $p_\infty$ is complex(63), we define

(59) We omit the subscripts $P$. Of course, all terms are defined with respect to $P$.

(60) According to [23, p. 149], it suffices to take $h\geqq[s/(p_0-1)]+1+t$, where $p_0$ is the rational belonging to $p$ and where $V_P(p_0)=s$, $V_P(m)=t$ in the $P$-adic valuation $V_P$ of $K_P$, normalized by $V_P(P)=1$. Logarithm and exponential are also defined by Chevalley [10].

(61) This proof is a slight variant of the one given by Tannaka [38, Theorem 2]. We do not follow his exposition because in his conductor in the large he has omitted the (essential) infinite prime divisors.

(62) In other words, if $k'$ consists of real numbers.

(63) In other words, if $k'$ contains complex numbers.

(4) $a \equiv 1 \pmod{p_\infty}$ if and only if $a \neq 0$,

(5) $a \equiv 1 \pmod{p_\infty^2}$ if and only if $\psi_p(a)$ is real and positive.

A congruence modulo $p_\infty^h$, $h>2$, is to have the same meaning as the same congruence for $p_\infty^2$. This congruence (5) is an acceptable definition, because the elements $\equiv 1 \pmod{p_\infty^2}$ do form a multiplicative subgroup of the group of all nonzero elements of $k$.

These conventions differ at (5) from the usual ones (see [20, 22]). Our reasons for the adoption of such a definition are: first, we need a congruence modulo $p_\infty^2$ which is not trivially true for all $a \neq 0$; secondly, the convention (5) agrees with the convention as to the ramifications. For, let $k_\infty$ be the field of real numbers, $K_\infty$ the field of complex numbers. Then the prime divisor $p_\infty$[64] of $k_\infty$ is ramified in $K_\infty$, with $p_\infty = P_\infty^2$, according to the usual convention. The possible congruences then agree for any $a$ in $k_\infty$:

(6) $a \equiv 1 \pmod{p_\infty}$ if and only if $a \equiv 1 \pmod{P_\infty^2}$.

In other words, the formal decomposition $p_\infty = P_\infty^2$ may be actually substituted in congruences. This possibility of substitution may be readily extended to the decomposition of any $p_\infty$ in a normal extension $K/k$, which would not be possible with the conventions of Hasse.

The infinite case of Theorem 26.1 is embodied in the following:

THEOREM 26.2. *Let $A_{\sigma,\tau}$ be a factor set of complex numbers belonging to the (cyclic) Galois group of the field $K_\infty$ of complex numbers over the field $k_\infty$ of real numbers. Then $A_{\sigma,\tau} \equiv 1 \pmod{P_\infty^2}$ implies that $A_{\sigma,\tau}$ is a transformation set from $K_\infty$, provided this congruence is interpreted as in* (5).

**Proof.** The proof will depend on the analysis of the algebra determined by $A_{\sigma,\tau}$ as a quaternion algebra. The Galois group $\Delta$ of $K_\infty/k_\infty$ is a cyclic group of two elements $\{1, \zeta\}$. Consequently the crossed product $(K_\infty/k_\infty, \Delta, A_{\sigma,\tau})$ has a cyclic generation $(K_\infty/k_\infty, \zeta, a)$ where the constant $a$ in the normalized generation may be computed as $a = A_{\zeta,\zeta}A_{1,1}$. The condition $A_{\zeta,\zeta} \equiv A_{1,1} \equiv 1 \pmod{P_\infty^2}$ means that $a$ is real and positive, hence a norm in $K_\infty/k_\infty$. The algebra is therefore a total matric algebra, as asserted in Theorem 26.2.

The local conductor $C_P(K/k)$ for any $P$ of $K$ may be defined as the least power $P^h$, with $h \geqq 0$, for which the conclusion (1) of Theorem 26.1 will hold for the corresponding local extension. The conjugate prime divisors $P^\sigma$ of $P$ determine equivalent extensions, thus

(7) $$[C_P(K/k)]^\sigma = C_{P^\sigma}(K/k).$$

The characteristic property of these local conductors can be stated "in the large" as follows:

---

[64] That is to say, the natural valuation.

THEOREM 26.3. *Let $F$, $G$ be two factor sets for $\Gamma$ in $K$, such that at every prime divisor $p$ of $k$ one has for at least one factor $P$ of $p$ the multiplicative congruences*

$$F_{\zeta,\eta} \equiv G_{\zeta,\eta} \pmod{C_P(K/k)}; \qquad \zeta, \eta \text{ in } \Delta(P). \tag{8}$$

*Then one can conclude $F \sim G$; that is, that there is a transformation set $TA$ with*

$$F = GTA.$$

**Proof.** The hypothesis, as a multiplicative congruence, means that the quotient factor set $FG^{-1}$ satisfies the conditions $(FG^{-1}) \equiv 1 \pmod{C_P(K/k)}$, for all $P$. According to formula (7) of §2 this factor set $(FG^{-1})_{\zeta,\eta}$ is exactly one giving the local component $(K, \Gamma, FG^{-1})_p$ of the algebra determined by $FG^{-1}$. The congruences (1) therefore just suffice to insure that every local component is similar to one, which in turn implies $FG^{-1} \sim 1$ in the large, by the fundamental theorem for algebras over algebraic number fields.

As a matter of fact, the congruences (8) in this theorem need only be assumed for a finite number of prime divisors $P$.

THEOREM 26.4. *The local conductor $C_P(K/k)$ is 1 if and only if $P$ is unramified in $K/k$.*

**Proof.** This conclusion is trivial for an infinite prime divisor $P$. For a finite $P$ we recall the convention ([20, 23])

$$A \equiv 1 \pmod{P^0} \qquad \text{if and only if } A \text{ is relatively prime to } P. \tag{9}$$

Suppose first that $P$ is unramified in $K/k$. Then the requirement $F_{\zeta,\eta} \equiv 1 \pmod{P^0}$ means that $F_{\zeta,\eta}$ is relatively prime to $P$. But by Theorem 12.1 a factor set of $P$-adic units is always similar to 1 for an unramified local extension. Hence $P^0$ is the local conductor. Conversely, suppose that the power $P^0$ functions as the local conductor. This means that every factor set of units is similar to 1. According to Theorem 12.1 the factor sets of local units yield a group of algebras with order equal to the ramification order $e_p$. Therefore they can all be similar to 1 only if $e_p = 1$.

This theorem suggests that we introduce as the conductor for factor sets of $K/k$ the finite divisor

$$C(K/k) = \prod_P C_P(K/k). \tag{10}$$

This conductor need not agree with the ordinary conductor for abelian (noncyclic) fields. We remark that our principal class (see §6) $T\mathfrak{A}'(F'')$ contains the "ray" modulo $C(K/k)$. This is a strict generalization of the classical results, provided we take for the module $M$ a multiple of $C(K/k)$.

Theorem 12.1 can also be used to obtain a somewhat closer estimate of the size of the conductor. According to this theorem, the $e$th power of any

factor set of local units is similar to 1. To make $F\sim 1$ we may then, as in (2), represent $F$ as the $e$th power of a set: $B_{\zeta,\eta} = \exp[(\log F_{\zeta,\eta})/e_p]$; $\zeta, \eta\ \Delta(P)$. The original congruence $F_{\zeta,\eta}\equiv 1 \pmod{P^h}$ must then have a module $h$ so chosen as to make the exponential and logarithmic series converge. Let $V_P$ be the $P$-adic valuation of $K$, and assume

$$V_P(e_p) = r, \qquad V_P(p_0) = s,$$

$p_0$ the rational prime which is divisible by $P$.

Then, if $h > s/(p_0-1)$, $\log F$ converges and has $P$-adic order $h$. The exponential function has as argument a quantity $(\log F)/e_p$ of $P$-adic order $h-r$. To insure the convergence of the exponential series this must again exceed (see [23, p. 149]) $s/(p_0-1)$. Therefore $h > r+s/(p_0-1)$ suffices.

THEOREM 26.5. *If a finite prime divisor $P$ is ramified in $K/k$ in such a fashion that $P^r$ is the highest power dividing the ramification order $e_p$, while $P^s$ is the highest power dividing the rational prime $p_0$, then the local conductor $C_P(K/k)$ is a divisor of $P^h$, where $h = r+1+[s/(p_0-1)]$.*

COROLLARY. *If a finite prime divisor $P$ has no higher ramifications in a normal extension $K/R$ of the field of rational numbers, and if $P$ is ramified in $K/R$ and relatively prime to 2, then the local conductor $C_P(K/k)$ is $P$.*

In the case of a cyclic extension the factor sets can be normalized to single quantities. It follows that the conductor for factor sets is identical with the ordinary conductor([65]).

27. **A generalized norm residue symbol.** The investigations of Chevalley and Hasse [9, 11, 21, 22] showed that the norm residue symbols $((a, Z)/p)$ for a cyclic field $Z/k$ can be defined purely locally, in terms of the invariants of the corresponding algebra $(Z, \lambda, a)$. In a similar fashion, crossed products may be used to define a generalized "*norm residue*" symbol for a factor set $F$ of a normal extension([66]) $K/k$. Unlike the classical symbol, this new symbol is not an element of the Galois group $\Gamma$ of $K/k$, but its formal properties are similar to the ordinary ones (see [20, Part II]).

Let $F$ be a factor set for $K/k$, $p$ a prime divisor of $k$, and define

$$(*27.1)\quad (K/k, F; p) = \exp(\mu_p/n) = e^{2\pi i \mu_p/n},$$

where

$$\mu_p = \mu_p(K/k, \Gamma, F) \equiv \mu(K/k, \Gamma, F)_p \pmod{n}$$

is the additive invariant, mod $n$, of the algebra determined by $F$. Immediately one establishes the following properties of this symbol:

([65]) [37, Theorem 3]. Here also other inequalities for the conductor are given.

([66]) The introduction of such a general symbol is originally a suggestion due to Hasse.

$$(K, F_1; p)(K, F_2; p) = (K, F_1F_2; p), \tag{1}$$

$$(K, F; p)^{-1} = (K, F^{-1}; p), \tag{2}$$

$$(K, TA; p) = 1. \tag{3}$$

Hence the norm residue symbol maps the group $FA/TA$ of similarity classes of factor sets homomorphically in the cyclic group of $n$th roots of unity.

To further analyze (3), recall that the $p$-component of a crossed product (see §2, (7)) is $(K, \Gamma, F)_p \sim (K_P, \Delta(P), F \cap \Delta)$ where $F \cap \Delta$ is the factor set consisting of those elements $F_{\zeta,\eta}$ of $F$ whose indices $\zeta$, $\eta$ lie in the decomposition group $\Delta = \Delta(P)$ of a fixed factor $P$ of $p$. Hence

$$(K, F; p) = 1 \quad \text{if and only if } F \cap \Delta \sim 1. \tag{4}$$

In terms of the local conductor $C_P$, this may be written as

$$(K, F; p) = 1 \quad \text{if and only if } (F \cap \Delta)(TA_P)^{-1} \equiv 1 \pmod{C_P} \tag{5}$$

for a suitable transformation set[67] $TA_P$. In terms of multiplicative congruences (see [10, 20, 23]), this last congruence can be written as $F_{\zeta,\eta} \equiv (A_P)_\zeta (A_P)_\eta^\zeta (A_P)_{\zeta\eta}^{-1} \pmod{C_P}$. This result specifies the sense in which our symbol is a "norm residue" symbol. Thus we have proved

THEOREM 27.1. *The symbol $(K, F; p)$ depends only on the (multiplicative) residue classes of the elements $F_{\zeta,\eta}$ modulo the conductor $C_P$, where $\zeta$, $\eta$ run over the elements in the decomposition group of some prime factor $P$ of $p$ in $K$.*

THEOREM 27.2. *If $(K, F; p) = 1$ for every factor set $F$, then $p$ is totally decomposed in $K$; that is, $p$ has in $K$ $n$ distinct prime factors $p = P_1P_2 \cdots P_n$.*

**Proof.** If $P$ is not totally decomposed in $K$, then each factor $P$ of $p$ has a decomposition group $\Delta(P)$ of order $[K_P : k_p] = m_p$ greater than 1. If $l$ is any rational prime factor of the degree $m_p$, there must then be a local algebra $S_p$ which has the invariant $\mu(S_p) = n/l \not\equiv 0 \pmod{n}$. By Theorem 14.1 the algebra $S_p$ is the component of an algebra $S$ in the large. Any factor set $F$ for such an algebra $S$ would have $(K, F; p) \neq 1$, counter to the assumption of the theorem. The sum relation[68] for the invariants of an algebra implies a product formula for the norm residue symbol

$$\prod_p (K, F; p) = 1. \tag{6}$$

The question of the existence of a factor set $F$ with certain given values for $(K, F; p)$ is identical with the question (see §§13–14) of the existence of actual algebras $S$ with specified local components.

Consider next a normal subfield $L/k$ of $K$, belonging to the subgroup $\Lambda$

[67] The associated vector $(A_P)_\zeta$ has components in $K_P$ for $\zeta$ in $\Delta$.

[68] As stated in the proof of Theorem 6.1.

of $\Gamma$. Let $F_\Lambda = F'$ be a factor set belonging to $L/k$. A formula of the theory of algebras (see [13, p. 63]) expresses the crossed product given by $F'$ as a crossed product for $K/k$ by the relation

$$(L/k, \Gamma/\Lambda, F') \sim (K/k, \Gamma, F' \cup \Gamma), \tag{7}$$

where $F' \cup \Gamma$ is the factor set obtained by extension of $F'$ with $\Gamma$, as in

$$F' \cup \Gamma = \{F_{\sigma,\tau}\} \qquad \text{where } F_{\sigma,\tau} = F'_{\sigma\Lambda,\tau\Lambda} = F'_{\bar{\sigma},\bar{\tau}}, \tag{8}$$

for $\bar{\sigma}$, $\bar{\tau}$ in $\Gamma/\Lambda$ and $\sigma$, $\tau$ arbitrary representatives of the cosets $\bar{\sigma}$, $\bar{\tau}$. The factor set $F' \cup \Gamma$ is "$\Lambda$-*symmetric*." In general, a factor set $F_{\sigma,\tau}$ is called $\Lambda$-symmetric if the components $F_{\sigma,\tau}$ depend only on the position of $\sigma$ and $\tau$ in the cosets of $\Gamma/\Lambda$.

Since similar algebras have the same invariants, (8) yields

$$(L/k, F'; p) = (K/k, F' \cup \Gamma; p). \tag{9}$$

This rule determines $(K, F; p)$ only for those factor sets $F$ which are similar to $\Lambda$-symmetric factor sets(69). Rule (9) is the analogue of the simple rule "$((a, K)/p)$ induces $((a, L)/p)$" of the classical theory.

Consider next an arbitrary finite extension $L$ of the base field $k$, which "translates" the extension $K/k$ to the extension $KL/L$. The Galois group of the join $KL/L$ is isomorphic to that subgroup $\Lambda$ of $\Gamma$ which leaves fixed all elements of the intersection $K \cap L$. On a crossed product the extension of the base field $k$ to $L$ has the effect (see [13, p. 61]):

$$(K/k, \Gamma, F)_L \sim (KL/L, \Lambda, F \cap \Lambda), \tag{10}$$

where $F \cap \Lambda$ is the factor set whose components are those elements $F_{\sigma,\tau}$ of $F$ which have subscripts $\sigma$ and $\tau$ in the group $\Lambda$. On the other hand (see [28, Theorem 5]), it can be shown that for any prime divisor $q$ in $L$ the $q$-invariant of an extended algebra $S_L$ is obtained by multiplying the additive $p$-invariant (mod 1) of $S$ by $h = [L_q : k_p]$, where $q \mid p$. In terms of the norm residue symbol, these two facts may be combined as the "*translation law*"

$$(K/k, F; p)^h = (KL/L, F \cap \Lambda; q). \tag{11}$$

A special case of (11) is the rule for a subfield: if $k \subset L \subset K$, while $P' \nmid p$ is a prime divisor in $L$, $\Lambda$ the corresponding group, then

$$(K/L, F \cap \Lambda; P') = (K/k, F; p)^h \tag{12}$$

where $h = [L_{P'} : k_p]$.

Consider a field $K$ which is the join over $k$ of two fields $K_1$ and $K_2$, each normal over $k$. In the Galois group $\Gamma$ of $K/k$ each automorphism $\sigma$ induces

(69) Even if $F$ is not $\Lambda$-symmetric, its local component $F \cap \Delta$ at some of the $P \mid p$ may be so symmetric; this makes possible a slight extension of (9).

an automorphism $\sigma_1$ of $K_1/k$ and an automorphism $\sigma_2$ of $K_2/k$. Since $K$ is generated by $K_1$ and $K_2$, the original $\sigma$ is uniquely determined by its homomorphic maps $\sigma_1$ and $\sigma_2$, so $\sigma$ may be represented by the formal product([70]) $\sigma=\sigma_1\sigma_2$. As in (7) a crossed product $(K_1/k, \Gamma_1, F_1)$ for the first extension is similar to a crossed product $(K_1K_2/k, \Gamma, \overline{F})$, where the factor set $F$ is obtained from $F_1$ by the formulas (8) as

$$\overline{F}_{\sigma_1\sigma_2,\tau_1\tau_2} = F_{1;\sigma_1,\tau_1}, \qquad \sigma_1\sigma_2 \text{ and } \tau_1\tau_2 \text{ in } \Gamma. \tag{13}$$

The crossed products $(K_2/k, \Gamma_2, F_2)$ are similarly extended. For the direct product of two such algebras, we then have

$$(K_1/k, \Gamma_1, F_1) \times (K_2/k, \Gamma_2, F_2) \sim (K_1K_2/k, \Gamma, \overline{F}) \tag{14}$$

where the factor set $\overline{F}$ is given by formulas such as (13)

$$\overline{F}_{\sigma_1\sigma_2,\tau_1\tau_2} = F_{1;\sigma_1,\tau_1}F_{2;\sigma_2,\tau_2} \qquad \text{with } \sigma_1 \text{ and } \tau_1 \text{ in } \Gamma_1,\ \sigma_2 \text{ and } \tau_2 \text{ in } \Gamma_2.$$

This means that the matrix of $\overline{F}$ is obtained from the *Kronecker product* $F_1 \otimes F_2$ of the given matrices by taking that submatrix belonging to the group $\Gamma$ (see [34, p. 691]). This yields for the norm residue symbols a rule

$$(K_1K_2/k, (F_1 \otimes F_2) \cap \Gamma; p) = (K_1/k, F_1; p)(K_2/k, F_2; p). \tag{15}$$

Formula (15) is a direct generalization of one of the rules for the ordinary norm residue symbol (see [20, Part II, p. 27, (8)]).

The rules for the values taken on by the classical norm residue symbol (see [20, Part II, p. 35, VI and VII]) break down in our case. The $p$-invariant of an algebra $S$ always has the form $x(n/m_p)$ for an integer $x$. Hence the corresponding norm residue symbol is an $m_p$th root of unity. Not all such roots need occur, because not all local algebras are components of algebras in the large (see §14).

THEOREM 27.3. *If $p$ is unramified in $K/k$, the norm residue symbol $(K/k, F; p)$ for variable factor sets $F$ takes on all values* exp $(1/m_p)$ *in a cyclic group of order $m_p$. If $p$ is ramified, the norm residue symbol takes on some, but not necessarily all, of these values.*

For factor sets $F$ which are relatively prime to a given prime divisor $p$ the corresponding local factor set consists of $P$-adic units, and the results of Theorems 14.4 and 14.5 determine the range of values of the norm residue symbol in this case.

THEOREM 27.4. *If $p$ is unramified in $K/k$, the norm residue symbol $(K/k, \Gamma; p)$ for variable factor sets $F$ which are relatively prime to $p$ is always* 1. *If $p$ is ramified, the norm residue symbol for $F$ relatively prime to $p$ takes on all*

([70]) Here $\sigma_1$ is an automorphism of $K_1$ (not of $K$). This formula represents $\Gamma$ as a subgroup of the direct product $\Gamma_1 \times \Gamma_2$ of the groups $\Gamma_1$ and $\Gamma_2$ of $K_1/k$, $K_2/k$, respectively.

*values* $\exp(y/(e_p, \bar{n}))$, *with* $y$ *integral, in a cyclic group of order* $(e_p, \bar{n})$. *Here* $\bar{n}=\bar{n}_i$ *is determined from* $p=p_i$ *as in Theorem* 14.5.

28. **A generalized Artin symbol.** The invariants of ideal factor sets, as introduced in §4, may be used to set up an Artin symbol resembling the symbol $(K/\mathfrak{a})$ of the classical theory ([20, Part II]). The ideal $\mathfrak{a}$ which is relatively prime to the conductor is to be replaced by a factor set $\mathfrak{F}$ of ideals which are relatively prime to the conductor $C(K/k)$. We define[71]

$$*(28.1)\quad (K\,|\,\mathfrak{F})=(K/k;\mathfrak{F})=\exp\{\textstyle\sum_p \mu_p(\mathfrak{F})n^{-1}\},$$

where the sum is to be taken over all unramified prime divisors $p$ for $K/k$, while $\mu_p$ is to be the invariant defined in (*5.6). In terms of the explicit formula §5, (16) for this invariant we may also write, for any factor $P$ of $p$,

$$(1)\qquad (K\,|\,\mathfrak{F}) = \exp\left\{\sum_p \sum_{j=0}^{m-1} m^{-1}V_P(\mathfrak{F}_{\delta^j,\delta})\right\}$$

where $V_P(\mathfrak{A})$ denotes the $P$-adic order of an ideal $\mathfrak{A}$, while $\delta=[(K/k)/P]$ is the Frobenius automorphism for $P$, of order $m=m_p$.

Our symbol may be obtained for any $\mathfrak{F}$ once its values are known for the $p$-primary factor sets. We know that the invariant $\mu_p(\mathfrak{F})$ depends solely on the $p$-primary factor $\mathfrak{F}^{(p)}$ of $\mathfrak{F}$. Specifically, any $\mathfrak{F}$ which is relatively prime to the conductor can be represented uniquely by a product

$$(2)\qquad \mathfrak{F} = \mathfrak{F}^{(1)}\mathfrak{F}^{(2)}\cdots\mathfrak{F}^{(s)},$$

where $\mathfrak{F}^{(i)}$ is a $p_i$-primary factor set, while $p_1, p_2, \cdots, p_s$ are all the various (unramified) prime divisors of $k$ involved in $\mathfrak{F}$. Since $\mu_i(\mathfrak{F})=\mu_i(\mathfrak{F}^{(i)})$, we have

$$(3)\qquad (K\,|\,\mathfrak{F}) = (K\,|\,\mathfrak{F}^{(1)})(K\,|\,\mathfrak{F}^{(2)})\cdots(K\,|\,\mathfrak{F}^{(s)}).$$

For a $p$-primary factor set $\mathfrak{F}^{(p)}$ all invariants $\mu_q(\mathfrak{F}^{(p)})$ for $q\neq p$ are zero, so the original definition of the symbol may be rephrased as

$$(4)\qquad (K\,|\,\mathfrak{F}^{(p)}) = \exp\{\mu_p(\mathfrak{F}^{(p)})/n\}.$$

The equations (4), (3), (2) might have been adopted to define the Artin symbol $(K\,|\,\mathfrak{F})$. Alternatively, (4) may be inverted to give a definition of the $p$-invariants in terms of the Artin symbol:

$$(5)\qquad \mu_p(\mathfrak{F}) = (n/2\pi i)\log[(K\,|\,\mathfrak{F}^{(p)})],$$

where $\mathfrak{F}^{(p)}$ denotes the $p$-primary factor of the given ideal factor set $\mathfrak{F}$.

THEOREM 28.1. *The Artin symbol affords an isomorphic mapping* $\mathfrak{F}\to(K\,|\,\mathfrak{F})$ *of the group* $F\mathfrak{A}'/T\mathfrak{A}'(F'')$ *onto the group of* $J$*th roots of unity.*

---

(71) We let $\exp u = e^{2\pi i u}$.

The quotient group in question is exactly the group whose order was computed in Theorem 6.1. Much as in Artin's reciprocity theorem, the Artin symbol thus furnishes an explicit realization of the isomorphism of the class group $F\mathfrak{A}'/T\mathfrak{A}'(F'')$ to a substitute for the Galois group ($J$th roots of unity).

**Proof.** To show that $\mathfrak{F}\to(K\,|\,\mathfrak{F})$ is a homomorphism, we need only refer to the corresponding properties of the invariant $\mu_p(\mathfrak{F})$, as given in §5. We find

$$(K\,|\,\mathfrak{F}_1)(K\,|\,\mathfrak{F}_2) = (K\,|\,\mathfrak{F}_1\mathfrak{F}_2), \tag{6}$$

$$(K\,|\,\mathfrak{F})^{-1} = (K\,|\,\mathfrak{F}^{-1}), \tag{7}$$

$$\mathfrak{F}_1 \sim \mathfrak{F}_2 \text{ implies } (K\,|\,\mathfrak{F}_1) = (K\,|\,\mathfrak{F}_2). \tag{8}$$

Lemma 5.1, combined with the Tschebotareff density theorem, indicates that every $J$th root of unity appears as the value of some Artin symbol $(K\,|\,\mathfrak{F})$. If $\mathfrak{F}$ is taken as the principal ideal $(F'')$, then by Theorem 6.1 $\mathfrak{F}$ has the same invariants as the algebra $(K/k, \Gamma, F'')$. The sum of these invariants is 0 (mod $n$), hence

$$\mathfrak{F} \text{ in } (F'') \text{ implies } (K\,|\,\mathfrak{F}) = 1. \tag{9}$$

It remains only to prove

$$(K\,|\,\mathfrak{F}) = 1 \text{ implies } \mathfrak{F} \text{ lies in } T\mathfrak{A}'(F''). \tag{10}$$

But $(K\,|\,\mathfrak{F}) = 1$ means according to definition (*28.1) that $\sum_p \mu_p(\mathfrak{F}) \equiv 0 \pmod{n}$. This implies that the invariants $\mu_p(\mathfrak{F})$ are the invariants of an actual algebra $S'$ relatively prime to $M$. By Theorem 6.2, $S'$ has a crossed product representation with a factor set $(F'')$. By Theorem 5.4, $\mu_p((F'')) \equiv \mu_p(S') \equiv \mu_p(\mathfrak{F})$, so that, by Theorem 5.2, $\mathfrak{F}(F'')^{-1}$ is a transformation set $T\mathfrak{A}'$, as asserted.

Since the norm residue symbol can also be defined (see §27) in terms of invariants of algebras, we may obtain it from the Artin symbol, applied to the $p$-primary component $(F)^{(p)}$ of a factor set of principal ideals

$$(K, F; p) = (K\,|\,(F)^{(p)}), \quad \text{if } p \text{ is unramified in } K/k. \tag{11}$$

According to Lemma 4 of §5 the $p$-invariants $\mu_p((F)^{(p)})$ run over all multiples of $nm_p^{-1}$. Hence we obtain the following result, which resembles the determination of the decomposition of unramified prime divisors in terms of the abelian class groups (see [20, Part II]).

THEOREM 28.2. *If $p$ is unramified in $K/k$ the degree $f = m_p$ of a prime factor of $p$ is the least integer $f$ such that $(K\,|\,\mathfrak{F}^{(p)})^f = 1$ for every $p$-primary factor set $\mathfrak{F}^{(p)}$.*

*Remark.* In general not every coset of $F\mathfrak{A}'/T\mathfrak{A}'(F'')$ will contain $p$-primary factor sets. The least common multiple $J(\Gamma)$ may be a proper multiple of every residue class degree $f$ which is permitted by the structure of the Galois group. The simplest example is furnished by fields $K/k$ with the sym-

metric group of 3 letters as the Galois group. Here $J(\Gamma)=2,3$ and $f=2,3$. Thus, the two classes of order 6 in the cyclic group $F\mathfrak{A}'/T\mathfrak{A}'(F'')$ are free from primary factor sets. This is another instance which illustrates the discrepancy between the classical class field theory and our theory.

The cosets which contain primary factor sets can easily be determined by means of Theorem 28.1. A coset contains a $p$-primary factor set if its order in the class group is equal to a permissible residue class degree of an unramified prime divisor. These degrees are exactly the orders of the cyclic subgroups of $\Gamma$, as follows from the ramification theory. Now $J(\Gamma)$ is the least common multiple of the orders of the group elements, hence $J(\Gamma)\equiv 0 \pmod f$ for every possible $f$. The Frobenius density theorem then proves that at least one class of order $f$ must contain infinitely many primary factor sets.

Consider next the symbol referred to a subfield $L$ of $K$ such that

$$k \subset L \subset K, \qquad L/k \text{ normal.} \tag{12}$$

If $\Lambda$ is the subgroup of $\Gamma$ belonging to $L$, then the Galois group of $L/k$ is $\Gamma/\Lambda$. If a prime divisor $P$ of $K$ has a multiple $Q$ in $L$, then the Frobenius automorphism $[(K/k)/P]=\delta$ of $P$ induces in $\Gamma/\Lambda$ the Frobenius automorphism $[(L/k)/Q]=\delta\Lambda=\zeta$ of $Q$ (see [20, Part II, p. 6, Rule III]). A factor set $\mathfrak{G}$ for $\Lambda$ can be extended to a factor set $\mathfrak{F}$ for $K$ by the rules

$$\mathfrak{F}_{\sigma,\tau} = \mathfrak{G}_{\sigma\Lambda,\tau\Lambda}; \tag{13}$$

the result is a $\Lambda$-symmetric factor set of $K$. By (1), the Artin symbol is

$$(K \mid \mathfrak{F}) = \exp\left\{ \sum_p \sum_{j=0}^{m-1} m^{-1} V_P(\mathfrak{F}_{\zeta^j,\zeta}) \right\}, \qquad m = m_p.$$

The order $V_P$ is the same as $V_Q$, since $p$ is unramified, while the order $n_p$ of the automorphism $\zeta$ is a divisor $n_p=m_p/r$ of the order $m_p$ of $\delta$, so this equation becomes

$$(K \mid \mathfrak{F}) = \exp\left\{ \sum_p (r/m_p) \sum_i V_Q(\mathfrak{G}_{\zeta^i,\zeta}) \right\}, \qquad i = 0, 1, \cdots, n_p - 1.$$

Since $r/m_p=1/n_p$, this yields the result

$$(K/k; \mathfrak{F}) = (L/k; \mathfrak{G}). \tag{14}$$

Given the situation (12), with $\mathfrak{F}$ defined by (13), this gives the Artin symbol $(K \mid \mathfrak{F})$ for the $\Lambda$-symmetric sets $\mathfrak{F}$.

On the other hand, one may consider the symbol for $K/L$.

THEOREM 28.3. *If the subgroup $\Lambda$ of $\Gamma$ corresponds to the subfield $L \subset K$, while $\mathfrak{F}' \cap \Lambda$ denotes that part of the factor set $\mathfrak{F}'$ which refers to the subgroup $\Lambda$, then*

$$(K/L; \mathfrak{F}' \cap \Lambda) = (K/k; \mathfrak{F}')^d, \qquad \text{where } d = [L:k]. \tag{15}$$

This is a special case of the following general "translation law" for the norm residue symbol:

THEOREM 28.4. *Let $L$ be any finite extension of $k$ such that the intersection $L \cap K$ belongs to the subgroup $\Lambda$ of $\Gamma$. Then*

$$(KL/L; \mathfrak{F}' \cap \Lambda) = (K/k, \mathfrak{F}')^d \qquad \text{where } d = [L:k]. \tag{16}$$

**Proof.** It will suffice to prove (16) for the case of a $p$-primary factor set $\mathfrak{F} = \mathfrak{F}^{(p)}$, where $p$ is unramified in $K/k$. Let the decomposition of $p$ in $L$ be

$$p = q_1^{e_1} q_2^{e_2} \cdots q_h^{e_h}, \qquad N_{L/k} q_j = p^{f_j} \qquad (j = 1, \cdots, h). \tag{17}$$

In the join $KL$ choose for each $j$ a factor $Q_j$ of $q_j$, and let $P_j$ be the prime factor of $Q_j$ which lies in $K$. The translation rule for the ordinary Artin symbol asserts that $q_j$ is unramified in $KL/L$ and that the Frobenius automorphism $\delta_j$ of $Q_j$ (see [20, Part II, p. 8]) is

$$\delta_j = [(KL/L)/Q_j] = [(K/k)/P_j]^{f_j}.$$

Since the original Frobenius automorphism $\delta = [(K/k)/P_j]$ has order $m_p$, the derived automorphism $\delta_j$ must have the order

$$n_j = m_p (m_p, f_j)^{-1}, \qquad \text{where } N_{KL/L} Q_j = q_j^{n_j}.$$

In $L$ the only primary components of $\mathfrak{F}$ are the $q_j$-primary ones, for $j = 1, \cdots, h$. Hence the translated Artin symbol has by definition the value

$$(KL/L; \mathfrak{F} \cap \Lambda) = \exp \left\{ \sum_{j=1}^{h} n_j^{-1} \left( \sum_{t=0}^{n_j - 1} W_j[\mathfrak{F}_{\delta_j^t, \delta_j}] \right) \right\},$$

where $W_j$ denotes the valuation belonging to $Q_j$. Since $P_j \mid p$ is unramified, the ramification order of $Q_j \mid P_j$ must be exactly the ramification order $e_j$ which figures in the decomposition (17). Therefore the power $W_j[\mathfrak{A}]$ to which $Q_j$ divides any ideal $\mathfrak{A}$ of $K$ is $e_j$ times the power $V_j[\mathfrak{A}]$ to which $P_j$ divides the same ideal, and

$$(KL/L; \mathfrak{F} \cap \Lambda) = \exp \left\{ \sum_{j=1}^{h} (e_j/n_j) \left( \sum_{t=0}^{n_j - 1} V_j[\mathfrak{F}_{\delta^t, \delta}] \right) \right\}.$$

But the order $V_j$ of the product involved here was computed in (18) of Lemma 5.7, and is $(n_j f_j / n) \mu_p(\mathfrak{F})$, where $r = n_j$ is the order of the cyclic group on $\delta_j$, while $t = f_j$ is the exponent in $\delta_j = \delta^t$. Therefore

$$(KL/L; \mathfrak{F} \cap \Lambda) = \exp \left\{ \sum_{j=1}^{h} (e_j f_j / n) \mu_p(\mathfrak{F}) \right\}. \tag{18}$$

But $\sum e_i f_i$ is exactly the degree $d=[L:k]$, while exp $\{\mu_p(\mathfrak{F})/n\}$ is exactly $(K|\mathfrak{F})$ by (4). Therefore (18) gives the desired conclusion (16) of the theorem.

This translation law seems superficially out of agreement with the analogous law (see [20, Part II]) for the norm residue symbol, because in that case the exponent was $[L_q:k_p]$, while here it is $[L:k]$. The divergence disappears if one recalls that the factor set $\mathfrak{F}^{(p)}$ splits up into $h$ $p$-primary factor sets over $L$, each of which involves an exponent $[L_q:k_p]$, for a total $[L_q:k_p]h=[L:k]$. This remark may be explicitly checked by using the theorem of (11).

As in §27 we may consider the case of the join $K=K_1K_2$ of two normal fields, and a factor set $(\mathfrak{F}_1\otimes\mathfrak{F}_2)\cap\Gamma$ obtained from the Kronecker product of two ideal factor sets $\mathfrak{F}_1$ and $\mathfrak{F}_2$ which are relatively prime to the conductor of $K/k$. This factor set can be represented as a product([72])

$$[(\mathfrak{F}_1\otimes I_2)\cap\Gamma]\cdot[(I_1\otimes\mathfrak{F}_2)\cap\Gamma],$$

to each factor of which the subfield rule (14) for symmetric factor sets may be applied. The result is

$$(19)\qquad (K_1K_2\,|\,(\mathfrak{F}_1\otimes\mathfrak{F}_2)\cap\Gamma)=(K_1\,|\,\mathfrak{F}_1)\cdot(K_2\,|\,\mathfrak{F}_2).$$

## BIBLIOGRAPHY

A. A. ALBERT

1. *Modern Higher Algebra*, Chicago, 1937.
2. *Structure of Algebras*, American Mathematical Society Colloquium Publications, vol. 24, 1939.
3. (With H. Hasse.) *A determination of all normal division algebras over an algebraic number field*, these Transactions, vol. 34 (1932), pp. 722–730.

Y. AKIZUKI

4. *Eine homomorphe Zuordnung der Elemente der Galoisschen Gruppe zu den Elementen einer Untergruppe der Normklassengruppe*, Mathematische Annalen, vol. 112 (1936), pp. 566–571.

E. ARTIN

5. *Über Einheiten relativ-galoisscher Zahlkörper*, Journal für die reine und angewandte Mathematik, vol. 167 (1932), pp. 153–156.

R. BAER

6. *Erweiterungen von Gruppen und ihren Isomorphismen*, Mathematische Zeitschrift, vol. 38 (1934), pp. 375–416.
7. *Automorphismen von Erweiterungsgruppen*, Actualités Scientifiques et Industrielles, vol. 205, Paris, 1935.

R. BRAUER, H. HASSE, AND E. NOETHER

8. *Beweis eines Hauptsatzes in der Theorie der Algebren*, Journal für die reine und angewandte Mathematik, vol. 167 (1932), pp. 399–404.

C. CHEVALLEY

9. *La théorie du symbole de restes normiques*, Journal für die reine und angewandte Mathematik, vol. 169 (1932), pp. 141–157.
10. *Sur la théorie du corps de classes pour les corps finis et les corps locaux*, Journal of the Faculty of Science, University of Tokyo, section 1, vol. 2 (1933), pp. 365–474.

([72]) Here $I_j$ denotes the unit matrix of $[K_j:k]$ rows and columns.

11. *La théorie du corps de classes*, Annals of Mathematics, vol. 41 (1940), pp. 394–418.

A. H. CLIFFORD AND S. MACLANE

12. *Factor sets of a group and its abstract unit group*, forthcoming in these Transactions.

M. DEURING

13. *Algebren*, Ergebnisse der Mathematik, vol. 4, Berlin, 1934.

L. E. DICKSON

14. *New division algebras*, these Transactions, vol. 28 (1926), pp. 207–234.

R. FRUCHT

15. *Über die Darstellungen endlicher abelscher Gruppen durch Kollineationen*, Journal für die reine und angewandte Mathematik, vol. 166 (1931), pp. 16–29.

W. GRUNWALD

16. *Ein algebraisches Existenztheorem für algebraische Zahlkörper*, Journal für die reine und angewandte Mathematik, vol. 169 (1933), pp. 103–107.

M. HALL

17. *Group rings and extensions* I, Annals of Mathematics, vol. 39 (1938), pp. 220–234.

H. HASSE AND K. HENSEL

18. *Über die Normenreste eines relativ-zyklischen Körpers vom Primzahlgrad l nach einem Primteiler* $\mathfrak{l}$ *von l*, Mathematische Annalen, vol. 90 (1923), pp. 262–278.

H. HASSE

19. *Zwei Existenztheoreme für algebraische Zahlkörper*, Mathematische Annalen, vol. 95 (1925), pp. 229–238.

20. *Bericht über neuere Untersuchungen und Probleme der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, Supplementary Volume 6 (1930).

21. *Theory of cyclic algebras over an algebraic number field*, these Transactions, vol. 34 (1932), pp. 171–214.

22. *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Mathematische Annalen, vol. 107 (1933), pp. 731–760.

23. *Klassenkörpertheorie*, mimeographed lecture notes, Marburg, 1933.

K. HENSEL

24. *Die Verallgemeinerung des Legendreschen Symbols für allgemeine algebraische Körper*, Journal für die reine und angewandte Mathematik, vol. 147 (1916), pp. 233–248.

J. HERBRAND

25. *Nouvelle démonstration et généralisation d'un théorème de Minkowski*, Comptes Rendus de l'Académie des Sciences, Paris, vol. 191 (1930), p. 1282.

26. *Sur les unités d'un corps algébrique*, ibid., vol. 192 (1931), p. 24.

D. HILBERT

27. *Collected Papers*, vol. 1.

G. KÖTHE

28. *Erweiterung des Zentrums einfacher Algebren*, Mathematische Annalen, vol. 107 (1932), pp. 761–766.

S. MACLANE (AND O. F. G. SCHILLING)

29. *Normal algebraic number fields*, Proceedings of the National Academy of Sciences, vol. 26 (1940), pp. 122–125.

M. MORIYA

30. *Über die Klassenzahl eines relativ-zyklischen Zahlkörpers von Primzahlgrade*, Japanese Journal of Mathematics, vol. 10 (1933), pp. 1–18.

T. NAKAYAMA

31. *Über die Beziehungen zwischen den Faktorensystemen und der Normklassengruppe eines Galoisschen Erweiterungskörpers*, Mathematische Annalen, vol. 112 (1936), pp. 85–91.

E. NOETHER

32. *Hyperkomplexe Systeme und ihre Beziehungen zur kommutativen Algebra und Zahlentheorie*, Verhandlungen des Internationalen Kongresses, Zürich (1932), vol. 1, pp. 189–195.
33. *Der Hauptgeschlechtssatz für relativgaloissche Zahlkörper*, Mathematische Annalen, vol. 108 (1933), pp. 411–419.

O. F. G. SCHILLING

34. *A generalization of local class field theory*, American Journal of Mathematics, vol. 60 (1938), pp. 667–704.

J. SOMMER

35. *Vorlesungen über Zahlentheorie*, Berlin, 1907.

I. SCHUR

36. *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik, vol. 132 (1907), pp. 85–137.

T. TANNAKA

37. *Eine Bemerkung über den Normensatz relativ-Galoisscher Zahlkörper*, Proceedings of the Imperial Academy of Tokyo, vol. 9 (1933), pp. 565–567.
38. *Über eine Indexrelation*, Science Reports of the Tôhoku Imperial University, (1), vol. 23 (1934–1935), pp. 343–358.

A. WEIL

39. *Remarques sur les résultats récents de C. Chevalley*, Comptes Rendus de l'Académie des Sciences, Paris, vol. 203 (1936), p. 208.
40. *Zur algebraischen Theorie der algebraischen Funktionen*, Journal für die reine und angewandte Mathematik, vol. 179 (1938), pp. 129–133.

E. WITT

41. *Zwei Regeln über verschränkte Produkte*, Journal für die reine und angewandte Mathematik, vol. 173 (1935), pp. 191–192.

B. L. VAN DER WAERDEN

42. *Moderne Algebra*, Part I, 2d edition, Berlin, 1939.

H. ZASSENHAUS

43. *Lehrbuch der Gruppentheorie*, Leipzig, 1937.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.
UNIVERSITY OF CHICAGO,
CHICAGO, ILL.