REGULAR NORMAL EXTENSIONS OVER COMPLETE FIELDS*

BY

O. F. G. SCHILLING

The local class field theory completely settles all problems pertaining to the abelian extensions of a complete field. All abelian extensions can be described in terms of norm class groups and it can readily be decided which abelian groups can be realized as Galois groups. In this paper we want to attack a more general problem. We consider non-abelian normal extensions of the ground field whose degrees are powers of a prime which is distinct from the characteristic of the residue class field. We construct an infinite normal extension which acts as an universal field. The algebraic approximation of this field yields complete information on the algebraic structure of the field and its Galois group over the ground field. It is shown that the Galois group contains an everywhere dense subgroup which completely suffices to describe the Galois theory. The structure of this group is readily determined. To a certain extent it is a generalization of the fuchsian groups of the classical theory of algebraic functions. The analogy is rather striking. We thus can associate to the given rational prime and the ground field an abstract infinite discrete group which can be considered as a universal covering group with respect to the given prime. All finite groups which can be realized as Galois groups are homomorphic maps of this infinite group. Finally, we associate to certain non-abelian extensions factor groups which are defined in terms of division algebras over the ground field. These factor groups are isomorphic with the respective Galois groups of the fields under consideration. We thus obtain another generalization of local class field theory. In our proofs we make ample use of the ramification theory and local class field theory.

Let k be a field which is complete with respect to a discrete valuation of rank one. Suppose that $\mathfrak{o}$ is the ring of all integers in k and that $\mathfrak{l}=(\lambda)$ is the prime ideal of $\mathfrak{o}$. We shall assume that the residue field $\mathfrak{o}/\mathfrak{l}$ of k is a finite Galois field containing $l^{\nu}=q$ elements. Let $p\neq 2$ be a prime such that $q-1\equiv 0 \pmod{p}$. Then k contains the pth roots of unity.† In the sequel we shall sup-

* Presented to the Society, October 28, 1939; received by the editors January 31, 1940. This paper was received by the editors of the Annals of Mathematics August 15, 1939, accepted by them, and later transferred to these Transactions.

† Since k is supposed to be complete, Hensel's irreducibility criterion implies the existence of the $(q-1)$st roots of unity in k. Cf. [4]. The number [4] refers to the reference in the bibliography at the end of this paper.

pose once and for all that k and p are fixed. The structure theory of complete fields yields that k is either a field of $\mathfrak{l}$-adic numbers over the rational l-adic field or a field of formal power series in one variable over the Galois field of q elements (cf. [7, 11, 12.2]).

LEMMA 1. *The maximal abelian extension A of exponent p over k has a Galois group of type (p, p). The field A contains the unramified extension U of degree p over k.*

Proof.† The field A is the join of all radical extensions $k(a^{1/p})$, $a \neq 0$ in k, for k contains the pth roots of unity. Hence, by the general theory of radical extensions, we must investigate the structure of the factor group k^*/k^{*p}, where k^* denotes the multiplicative group of the field k. Let $\{\epsilon\}$ be the group of all units in k which are congruent to 1 (mod $\mathfrak{l}$). We first assert that $\{\epsilon\} = \{\epsilon^p\}$, that is, every unit ϵ is the pth power of a suitable unit $\eta \in \{\epsilon\}$. We shall construct a solution η of $x^p - \epsilon = 0$ by successive approximation. Since $\epsilon \equiv 1 \pmod{\mathfrak{l}}$, we can put $\eta_1 = 1$. Suppose that we already constructed a unit η_i such that $\epsilon \equiv \eta_i^p \pmod{\mathfrak{l}^{i+1}}$. We set $\eta_{i+1} = \eta_i + x_{i+1}\lambda^{i+1}$ where x_i is to be determined in a fixed set of representatives for $\mathfrak{o}/\mathfrak{l}$. We require

$$\epsilon \equiv \eta_{i+1}^p \pmod{\mathfrak{l}^{i+2}}.$$

Consequently, we have $\epsilon \equiv (\eta_i + x_{i+1}\lambda^{i+1})^p \pmod{\mathfrak{l}^{i+2}}$, or $\epsilon \equiv \eta_i^p + p\eta_i^{p-1}x_{i+1}\lambda^{i+1} \pmod{\mathfrak{l}^{i+2}}$; thus

$$(\epsilon - \eta_i^p)(p\eta_i^{p-1})^{-1} \equiv x_{i+1}\lambda^{i+1} \pmod{\mathfrak{l}^{i+2}},$$

for $(p, \mathfrak{l}) = 1$ by assumption. Hence

$$(\epsilon - \eta_i^p)(p\eta_i^{p-1})^{-1}\lambda^{-(i+1)} \equiv x_{i+1} \pmod{\mathfrak{l}},$$

that is, x_{i+1} is uniquely determined by ϵ. Thus k^{*p} contains the group $\{\epsilon\}$. Since k is a complete field, every element $a \in k$ has a unique representation as $\omega^\alpha \lambda^\beta \epsilon$ where ω denotes a fixed primitive $(q-1)$st root of unity and λ a fixed prime element of k. Hence $k^* \pmod{k^{*p}}$ has ω and λ as independent generating representatives. Since $q - 1 \equiv 0 \pmod{p}$, the group k^*/k^{*p} has type (p, p). Consequently, the field A is given as $k(\lambda^{1/p}, \omega^{1/p})$. Obviously, the cyclic unramified field U of degree p over k is contained in A. This completes the proof of the lemma.

Suppose that p^μ is the *highest power* of p which divides $q-1$. Then the maximal abelian extension of exponent p^μ has degree $p^{2\mu}$ and its Galois group has type (p^μ, p^μ). Now let $i > \mu$. We want to find the order of the factor group

† We repeat here Hensel's arguments for sake of completeness. Cf. [5.1].

k^*/k^{*p^i}. Obviously the prime element λ is a representative of order p^i. Consider now the factor group $\{\omega\}/\{\omega^{p^i}\}$. We find for its order

$$[\{\omega\}:\{\omega^{p^i}\}] = [\{\omega\}:\{\omega^p\}] \cdots [\{\omega^\mu\}:\{\omega^{\mu+1}\}][\{\omega^{\mu+1}\}:\{\omega^{\mu+2}\}]\cdots[\{\omega^{p^i-1}\}:\{\omega^{p^i}\}].$$

Hence by the index principle of group theory (considering $\omega\to\omega^p$ as a homomorphism), $[\{\omega\}:\{\omega^{p^\mu}\}]=[\{\omega\}:\{\omega^{p^i}\}]=p^\mu$ for $p^\mu \| q-1$. Thus, we have

LEMMA 2. *The index* $[k^*:k^{*p^i}]=p^{i+\mu}$ *if* $i>\mu$ *and* p^{2i} *if* $i\leqq\mu$.

Suppose now that K is an arbitrary normal extension of k whose degree is a power of p. Let $G=\{x, y, \cdots\}$ be the Galois group of K/k. The elements $xyx^{-1}y^{p-1}$ generate an invarant subgroup G^* of G whose factor group G/G^* has type $(p, p, \cdots, p)$ (cf. [12.1]). Let K^* be the field which corresponds to G^*.

THEOREM 1. *The Galois group of any normal extension K of degree* p^n *over k can always be generated by two elements.*

Proof. Let G^* be the group $\{xyx^{-1}y^{p-1}\}$. Then the minimal number of generators of G is equal to the number of invariants of G/G^*. This number of invariants is not greater than 2 for $[K^*:k]=[G:G^*]\leqq[A:k]=p^2$ by Lemma 1.

A normal field K over k of degree p^n shall be called a *regular* extension of k.

We now want to construct a *universal field* $N^{(p)}$ over k which contains all regular extensions K. Let $A=A_1$ be the maximal abelian extension of exponent p over k. Since $k\subset A_1$, that is, the pth roots of unity lie in A_1, we can repeat this construction. Let $k\subset A_1\subset A_2\subset\cdots\subset A_{i-1}\subset A_i\subset\cdots$ be the infinite tower of relative maximal abelian extensions of exponent p; that is, $[A_i:A_{i-1}]=p^2$, the Galois groups $G(A_i, A_{i-1})$ having type (p, p). A theorem of local class field theory yields that A_i is normal over k, the degree being p^{2i}. Namely, the class group $A_i^{*p}{}_{-1}$ which belongs to A_i/A_{i-1} is left invariant by all elements of $G(A_{i-1}, k)$ (cf. [3]). Consequently, the join $N^{(p)}=\sum A_i$ is an infinite normal extension of k.

THEOREM 2. *The field* $N^{(p)}/k$ *is universal, that is, it contains all regular fields* K/k.

Proof. The Galois group G of K/k contains a series of normal subgroups $\overline{G}_i$ such that $\overline{G}_i/\overline{G}_{i+1}$ are cyclic groups of order p. Let

$$k\subset K_1\subset K_2\subset\cdots\subset K_i\subset\cdots\subset K$$

be the associated chain of subfields (cf. [12.1]). In order to prove our assertion we compare this chain with the defining chain $k\subset A_1\subset A_2\subset\cdots$ of $N^{(p)}$.

We have $K_1 \subset A_1$, for K_1 is a cyclic extension of degree p over k. Consider now the cyclic extension K_2 of K_1. Then either $K_2 = A_1$ or $K_2 \neq A_1$. In the second case the join K_2A_1 is a cyclic extension of degree p over A, as a consequence of the Galois theory. Consequently $K_2A_1 \subset A_2$ by construction of A_2. We can continue this process. Thus, ultimately $K \subset A_j$, $\not\subset A_{j-1}$ where the index j is uniquely determined by the given field K.

An immediate consequence of Theorem 2 is the fact that the Galois group G of a regular field K is a homomorphic map $G^{(p)}/S(K)$ of the Galois group $G^{(p)}$ belonging to the universal field $N^{(p)}/k$. We therefore must investigate the structure of $G^{(p)}$ if we want to get information on the various groups G.

Let G_i be the Galois group of an arbitrary but fixed extension A_i over k. Then Theorem 1 implies that G_i can be generated by 2 elements σ_i, τ_i. We shall select σ_i, τ_i such that σ_i generates the inertial group of A_i with respect to k. The group $\{\sigma_i\}$ is an invariant subgroup of G_i and its order is equal to p^i, for A_i contains the unramified field U_{p^i} (of degree p^i over k) as maximal unramified subfield (inertial field) (cf. [4]). Thus

$$G_i/\{\sigma_i\} = G(U_{p^i}, k).$$

The group $G(U_{p^i}, k)$ has order p^i and is generated by an element τ_i^*. Thus, if τ_i denotes a representative of τ_i^* in G_i, we get

$$\{\sigma_i, \tau_i\} = G_i, \qquad \sigma_i^{p^i} = \tau_i^{p^i} = 1, \qquad \tau_i^{-1}\sigma_i\tau_i = \sigma_i^{g_i}$$

where g_i is a prime residue modulo p^i. The group G_{i-1} is a homomorphic map of G_i. Let S_i denote the invariant subgroup of G_i which belongs to A_{i-1}. Then $G_i/S_i \cong G_{i-1}$. It is immediately seen, as a consequence of our selection of the generators σ_i, τ_i, that $S_i = \{\sigma_i^{p^{i-1}}, \tau_i^{p^{i-1}}\}$. Hence we can select the generators σ_{i-1}, τ_{i-1} as the maps of σ_i, τ_i on G_{i-1}. Whence $\tau_{i-1}^{-1}\sigma_{i-1}\tau_{i-1} = \sigma_{i-1}^{g_i} = \sigma_{i-1}^{g_{i-1}}$ and consequently $g_i \equiv g_{i-1} \pmod{p^{i-1}}$.

Next we want to normalize the exponents g_i to an integer g such that $\tau_i^{-1}\sigma_i\tau_i = \sigma_i^g$ for all i. We shall prove this statement by constructing two elements σ, τ in the infinite Galois group of $N^{(p)}/k$ whose homomorphic images in G_i have the required properties.

Suppose that p is an odd rational prime. Denote by V the valuation which is given by p.

LEMMA 3. *Let a be a p-adic integer such that $p^\mu \| a-1$, $\mu \geqq 1$; then there exists a p-adic integer h such that $a^h = 1+p^\mu$. In other words, the p-adic units which are congruent to* 1 (mod p^μ) *form an ideal cyclic group which is generated by any* $a \equiv 1\ (p^\mu)$, $a \not\equiv 1\ (p^{\mu+1})$.

Proof. The exponent h for which $a^h = 1+p^\mu$ will be constructed by suc-

cessive p-adic approximation. Let $a=1+bp^{\mu}$ where b is a p-adic integer of value 0. Suppose that we already found integers $h_1, \cdots, h_j$ for which

$$h_\nu \equiv h_{\nu-1} \pmod{p^{\nu-1}}, \qquad \nu = 1, 2, \cdots, j, \tag{1}$$

and

$$a^{h_\nu} \equiv 1 + p^{\mu} \pmod{p^{\mu+\nu}}, \qquad \nu = 1, 2, \cdots, j. \tag{2}$$

The first number h_1 is easily determined. Namely, we require

$$a^{h_1} = (1 + bp^{\mu})^{h_1} = 1 + h_1 bp^{\mu} + p^{2\mu}c, \qquad V(c) \geqq 0.$$

Since $b \not\equiv 0 \pmod{p}$, we can determine h_1 by the congruence $h_1 b \equiv 1 \pmod{p}$. Consequently,

$$a^{h_1} \equiv 1 + p^{\mu} \pmod{p^{\mu+1}}.$$

In the general case we propose to find an integer h_{j+1} as $h_j + r_j p^j$ where r_j has to be determined. Such a number h_{j+1} surely satisfies condition (1). In order to show that condition (2) can be realized we proceed as follows. We must have

$$a^{h_{j+1}} = a^{h_j} a^{p^j r_j} = (1 + p^{\mu} + sp^{\mu+j})(1 + bp^{\mu})^{r_j p^j}$$

where s is a p-adic integer by induction. Next

$$a^{r_j p^j} = (1 + bp^{\mu})^{r_j p^j} = 1 + r_j bp^{\mu+j} + \sum_{\kappa=2}^{r_j p^j} C_{r_j p^j, \kappa} (bp^{\mu})^{\kappa}.$$

We now show that the value of the sum on the right hand exceeds $\mu+j$. The binomial coefficients $C_{r_j p^j, \kappa} = B_j$ have the form $p^j r_j (\kappa!)^{-1} d$ where $V(d) \geqq 0$. Hence

$$V(B_j) \geqq j - V(\kappa!) \geqq j - \kappa(p-1)^{-1},$$

for $V(\kappa!) = (\kappa - s_\kappa)(p-1)^{-1}$ where $s_\kappa \geqq 0$ (cf. [5.2]). Thus

$$\begin{aligned} V(B_j (bp^{\mu})^{\kappa}) &\geqq \mu\kappa + j - \kappa(p-1)^{-1} = \mu + j + \mu(\kappa - 1) - \kappa(p-1)^{-1} \\ &\geqq \mu + j + \mu(\kappa - 1) - \kappa/2 \geqq \mu + j + (\kappa - 1) - \kappa/2 > \mu + j, \end{aligned}$$

provided that $\mu \geqq 1$, $p \geqq 3$, $\kappa \geqq 3$. If $\kappa = 2$, then

$$B_j (bp^{\mu})^2 = r_j p^j (r_j p^j - 1) 2^{-1} b^2 p^{2\mu} = p^{2\mu+j} d,$$

where d is a p-adic integer. Consequently,

$$V(B_j (bp^{\mu})^2) = 2\mu + j \geqq \mu + j + 1.$$

Hence, in general, $a^{p^j r_j} = 1 + br_j p^{\mu+j} + tp^{\mu+j+1}$, where $V(t) \geqq 0$. Returning to $a^{h_{j+1}}$ we get

$$a^{h_{j+1}} = (1 + p^\mu + sp^{\mu+j})(1 + br_jp^{\mu+j} + tp^{\mu+j+1})$$
$$\equiv 1 + p^\mu + (s + br_j)p^{\mu+j} \pmod{p^{\mu+j+1}}.$$

Since $b \not\equiv 0 \pmod{p}$, we can determine r_j as a solution of $s+br_j \equiv 0 \pmod{p}$. Hence the induction is completed. The numbers h_j form a convergent p-adic sequence. Let $\lim_{j\to\infty} h_j = h$. Then

$$a^h = a^{\lim h_j} = \lim_{j\to\infty} a^{h_j} = 1 + p^\mu.$$

LEMMA 4. *The Galois group G_i of A_i/k is given by the relations $\sigma_i^{p^i} = \tau_i^{p^i} = 1$, $\tau_i^{-1}\sigma_i\tau_i = \sigma_i^{1+p^\mu}$ where $a - 1 = p^\mu \cdot r$, $(r, p) = 1$.*

Proof. Let $G^{(p)}$ be the infinite Galois group of $N^{(p)}/k$. As usual we define $G^{(p)}$ as the group of vectors $(\rho_1, \cdots, \rho_i, \cdots)$ where (cf. [6])

$$\rho_i \in G_i, \quad \rho_i \pmod{S_i} = \rho_{i-1}, \qquad i = 1, 2, \cdots.$$

Application of the ramification theory of infinite normal extensions yields that $G^{(p)}$ contains two elements σ, τ^* having the following properties. The element σ is a generator of the inertial group of $N^{(p)}/k$, that is, the elements of the inertial group are powers σ^c where the c's are p-adic integers. The group of the inertial field of $N^{(p)}/k$ is ideal cyclic and generated by a residue class $\tau^* \pmod{\{\sigma\}}$ where $\tau^* \in G^{(p)}$ (cf. [6]). Since the inertial group is an invariant subgroup of $G^{(p)}$, we have $\tau^{*-1}\sigma^*\tau^* = \sigma^a$ where a is a p-adic integer. Since $\lim_{i\to\infty} G_i = N^{(p)}$, we have $\sigma = (\sigma_1, \cdots, \sigma_i, \cdots)$, $\sigma_i \in G_i$, and $\tau^* = (\tau_1^*, \cdots, \tau_i^*, \cdots)$, $\tau_i^* \in G_i$. Moreover, $\tau_i^{*-1}\sigma_i\tau_i^* = \sigma_i^{a_i}$ where $a_i \equiv a \pmod{p^i}$ and $\sigma_i^{p^i} = \tau_i^{*p^i} = 1$ according to the selection of the elements σ, τ^* in $G^{(p)}$.

We now want to apply Lemma 3 in order to normalize the exponents g_i. Consider for this purpose the norm groups $N_iA_i^*$ which belong to the various fields A_i/k; N_i denotes the norm taken from A_i to k. Observing that N_i can be split up into the various relative norms from A_j to A_{j-1} and that A_j is the maximal abelian extension of type (p, p) over A_{j-1}, we get $N_iA_i^* = k^{*p^i}$. Hence

$$[k^* : N_iA_i^*] = p^{2i} \quad \text{if} \quad i \leqq \mu$$
$$= p^{\mu+i} \quad \text{if} \quad i > \mu.$$

A theorem of local class field theory yields† that

(i) A_i is an abelian extension of type (p^i, p^i) over k if $i \leqq \mu$,

(ii) A_i is a non-abelian extension of degree p^{2i} over k if $i > \mu$ and the group $N_iA_i^*$ belongs to the maximal abelian subfield $A_\mu U_{p^i}$ of A_i.

Since G_μ is the *last* Galois group in the approximation of $G^{(p)}$ which is abelian, we must have $a \equiv 1 \pmod{p^\mu}$, $a \not\equiv 1 \pmod{p^{\mu+1}}$. Hence there exists,

† [3, 10]. We mean the "Abgrenzungssatz" of local class field theory.

by Lemma 3, a p-adic integer h such that $a^h = 1 + p^\mu$. Consequently, we can change τ^* to a new element $\tau = \tau^{*h}$ in $G^{(p)}$ such that

$$\tau^{-1}\sigma\tau = \sigma^{1+p^\mu}.$$

Namely, $\tau^{*-1}\sigma\tau^* = \sigma^a$ implies $\tau^{*-h}\sigma\tau^{*h} = \sigma^{a^h} = \sigma^{1+p^\mu}$. Hence, also $\tau_i^{-1}\sigma_i\tau_i = \sigma_i^{1+p^\mu}$, $i = 1, 2, \cdots$.

LEMMA 5. *Let L be an infinite normal extension of the abstract field R and let Γ be the (topologized) Galois group of L/R. Suppose that Δ is a subgroup of Γ. Then Δ is everywhere dense in Γ if and only if whenever W/R is a finite normal subfield of L every automorphism of W/R can be extended to an automorphism of Δ.*†

Proof. We first note that a group Δ as described in the lemma is sufficient to describe the Galois theory of the finite extensions W/R which lie in L. An alternate formulation of the conditions of the lemma is this:

If $L \supset W \supset R$, $[W:R]$ finite, and if $\Delta(W)$ is the subgroup of Δ leaving the elements of W fixed, then $\Delta/\Delta(W)$ is isomorphic to $G(W, R)$.

Suppose now that Δ is an everywhere dense subgroup of Γ. We want to prove that the Galois theory for finite extensions $R \subset W \subset L$ can be described in terms of Δ. Let ρ be an arbitrary automorphism of $G(W, R)$. We can extend ρ to an automorphism ρ' of Γ. Since Δ is everywhere dense in Γ and since the automorphisms leaving W elementwise fixed constitute a neighborhood N of the unit in Γ, there exists an element δ in Δ such that $\delta\rho'^{-1}$ lies in N. Thus, δ lies in $N\rho'$ or δ induces ρ on W. Conversely, the possibility of describing the Galois theory for finite extensions W/R by means of a subgroup Δ of Γ implies that Δ is everywhere dense in Γ. Let ρ' be any automorphism of Γ and let $N(W)$ be any neighborhood of the unit in Γ, that is, $N(W)$ is defined by a finite subfield W/R of L. Then there exists, by hypothesis, an element δ in Δ such that δ agrees with ρ' on W, that is, $\delta\rho'^{-1}$ induces the identity on W. Hence $\delta\rho'^{-1}$ is an element of $N(W)$. This means that Δ is an everywhere dense subgroup of Γ.

THEOREM 3. *The group $\{\sigma, \tau; \tau^{-1}\sigma\tau = \sigma^{1+p^\mu}\} = F^{(p)}$ is an everywhere dense subgroup of $G^{(p)}$. The Galois theory for finite subfields of $N^{(p)}/k$ can be described in terms of the subgroup $F^{(p)}$.*

Proof. By Lemma 5 it suffices to prove the first part of the theorem. The topology of $G^{(p)}$ is given by the chain of homomorphisms $G_i \to G_{i-1}$, explicitly

$$\sigma_{i-1} = \sigma_i \pmod{\{\sigma_i^{p^{i-1}}, \tau_i^{p^{i-1}}\}}, \qquad \tau_{i-1} = \tau_i \pmod{\{\sigma_i^{p^{i-1}}, \tau_i^{p^{i-1}}\}}.$$

† The author wants to thank Professor Saunders MacLane for valuable suggestions in the proofs of Lemmas 3, 5.

In other words, we get an isomorphic representation of G_{i-1} by reducing the exponents of the elements $\rho_i=\sigma_i^{\alpha}\tau_i^{\beta}$ in G_i modulo p^{i-1} and changing the subscript i to $i-1$. Since $\sigma_i^{p^i}=\tau_i^{p^i}=1$, the exponents α, β of the element $\rho_i \in G_i$ are p-adic integers reduced modulo p^i. Next we remark that $\{\sigma^{p^i}, \tau^{p^i}\}$ is an invariant subgroup F_i of $F^{(p)}$. Namely, we have

$$\begin{aligned}\tau^{-1}\sigma^{p^i}\tau &= \tau^{-1}\sigma\tau\tau^{-1}\sigma\tau\cdots\tau^{-1}\sigma\tau\\ &= \sigma^{1+p^{\mu}}\sigma^{1+p^{\mu}}\cdots\sigma^{1+p^{\mu}}\\ &= \sigma^{(1+p^{\mu})p^i} = (\sigma^{p^i})^{1+p^{\mu}} \in \{\sigma^{p^i}, \tau^{p^i}\}.\end{aligned}$$

Next $\sigma\tau\sigma^{-1}=\tau\sigma^{p^{\mu}}$; hence

$$\sigma\tau^{p^i}\sigma^{-1} = \sigma\tau\sigma^{-1}\sigma\tau\sigma^{-1}\cdots\sigma\tau\sigma^{-1} = \tau\sigma^{p^{\mu}}\tau\sigma^{p^{\mu}}\cdots\tau\sigma^{p^{\mu}} = \tau^{p^i}(\sigma^{p^i})^x$$

where $x=[(1+p^{\mu})^{p^i}-1]p^{-i}$. Thus $F^{(p)}/F_i\cong G_i$. In other words, we obtain G_i from $F^{(p)}$ by reducing the exponents α, β of $\sigma^{\alpha}\tau^{\beta}$ (α, β are rational integers) modulo p^i and attaching the subscript i to σ, τ. Consequently, every element $\rho=(\rho_1, \cdots, \rho_i, \cdots)$ of $G^{(p)}$ can be approximated by a sequence $\rho^{(i)}=\sigma^{\alpha(i)}\tau^{\beta(i)}$, $i=1, 2, \cdots$, where the $\alpha(i)$, $\beta(i)$ are integers such that

$$\rho_i = \rho^{(i)} \pmod{S^{(i)}} = \sigma^{\alpha(i)}\tau^{\beta(i)} \pmod{F^{(i)}}$$

for every i, where $G^{(p)}/S^{(i)}\cong G_i$. This proves that $F^{(p)}$ is an everywhere dense subgroup of $G^{(p)}$. We remark that the closure $G^{(p)}$ of $F^{(p)}$ is obtained by admitting for the exponents α, β of $\rho=\sigma^{\alpha}\tau^{\beta}$ arbitrary p-adic integers instead of rational integers. The closure of F_i in $G^{(p)}$ is equal to $S^{(i)}$ and $S^{(i)} \cap F^{(p)}=F_i$. This follows immediately from the imbedding of $F^{(p)}$ in $G^{(p)}$.

THEOREM 4. *A finite group G of order p^n can be realized as the Galois group of a reguar extension K/k if and only if it is a homomorphic map of the group $F^{(p)}=\{\sigma, \tau; \tau^{-1}\sigma\tau=\sigma^{1+p^{\mu}}\}$.*

Proof. Let K be an arbitrary regular extension of k. Then $K \subseteq A_i$, i sufficiently large, by Theorem 2. Then, by Theorem 3, the Galois group G of K is a homomorphic map of $F^{(p)}$. Conversely, suppose that $G\cong F^{(p)}/T$. Then, by the second half of Theorem 3, there exists at least one field $K \supset k$ whose Galois group is isomorphic with G. The field K belongs to T. However, T need not be uniquely determined by G, for the homomorphism $F^{(p)}\to G$ can, in general, be realized by various invariant subgroups T. The number of groups T corresponding to a given group G is finite. Namely, the argument which we used to prove that $K \subset A_i$ shows that i is bounded by n, where $[K:k]=p^n$. Hence $G\cong G(K, k)=G_i/G(A_i, K)=(F^{(p)}/F_i)/(T/F_i)$. We remark that $T^{(1)} \neq T^{(2)}$ implies that the closures in $G^{(p)}$ of T_1, T_2, respectively, are also distinct provided that $T^{(1)}$ and $T^{(2)}$ have finite indices under $F^{(p)}$.

It is relatively easy to determine the exact number of regular fields K with prescribed Galois group of small order. We want to discuss briefly the simplest case. Suppose that $\mu=1$, that is, $q-1=p\cdot r$, $(r, p)=1$. Then A_2 is a non-abelian extension of degree p^4 over k. Its Galois group is given by the relations

$$\Sigma^{p^2}=\Gamma^{p^2}=1, \qquad \Gamma^{-1}\Sigma\Gamma=\Sigma^{1+p}.$$

Now let G be an arbitrary group of order p^3. Since the commutative cases are already settled by local class field theory, we investigate the non-abelian cases. There are two distinct types of non-abelian groups of order p^3:

(α) $\sigma^{p^2}=\tau^p=1$, $\tau^{-1}\sigma\tau=\sigma^{1+p}$ and

(β) $\sigma^p=\tau^p=\rho^p=1$, $\rho=\sigma\tau\sigma^{-1}\tau^{-1}$, $\rho^{-1}\sigma\rho=\sigma$, $\tau^{-1}\sigma\tau=\sigma$, $\rho^{-1}\tau\rho=\tau\sigma$ (cf. [2]).

A simple computation yields that both groups are homomorphic maps of $G_2=\{\Sigma, \Gamma\}$. Hence every type has at least one realization as the Galois group $G(K)$ of a regular field $K\subset A_2$. Moreover, every K which belongs to either type (α) or type (β) must be contained in A_2. Since these fields K are non-abelian extensions of k, they all must contain the field A_1. This field A_1 belongs [12.1] to the group $G_2^*=\{\Sigma\Gamma\Sigma^{-1}\Gamma^{p-1}\}$ of G_2. Since $K\supset A_1$, we also have $G/G^*\cong G_2/G_2^*$ where G^* is defined in the same fashion as G_2^*. Moreover, $G_2/S'(K)=G(K)$. Hence, by the homomorphism principle of group theory, $S'(K)\subset G_2^*$. Thus, the fields K are found among the cyclic extensions of degree p over A_1. There are $p+1$ such extensions for G_2^* has $p+1$ invariant subgroups of order p, as follows from the structure of G_2. Namely, $G_2^*=\{G_2'; X^p, X\in G_2\}$ where G_2' is the commutator group of G_2 (cf. [12.1]). Consequently $G_2^*=\{\Sigma^p, \Gamma^p\}$ for $\Sigma^{-1}\Gamma^{-1}\Sigma\Gamma=\Gamma^p\in\{\Sigma^p, \Gamma^p\}$. Moreover $\Gamma^{-p}\Sigma\Gamma^p=\Sigma$ and $\Gamma^{-1}\Sigma^p\Gamma=\Sigma^p$.

Consider now the invariant subgroup $\{\Sigma^p\}$ of G_2. Its factor group $G_2/\{\Sigma^p\}$ is abelian and has type (p, p^2). The associated field, belonging to G_2', is $U_{p^2}k(\lambda^{1/p})$.

The factor group $G_2/\{\Gamma^p\}$ is non-abelian. It has type (α).

The $p-1$ different subgroups given by $\{\Sigma^{ip}\Gamma^{jp}\}$ have factor groups which belong to type (β). This is easily verified.

Combining these results we can state the following theorem.

THEOREM 5. *If $p\|q-1$, then k has exactly one regular extension of type (α) and exactly $(p-1)$ distinct regular extensions of type (β).*

The infinite discrete group $F^{(p)}$ can be considered as a generalization of the fuchsian groups of the classical theory of algebraic functions to l-adic number fields. The analogy is rather striking. We may interpret it as follows. The substitution $\tau\in F^{(p)}$ corresponds to the unramified extensions, that is,

to the fundamental group of the classical case. The substitution $\sigma \in F^{(p)}$ corresponds to the substitution of signature $\lim_{i\to\infty} p^{-i}=p^{-\infty}$ around the given branch point of the underlying Riemann surface. Moreover, the commutator group $F^{(p)\prime}$ of $F^{(p)}$ is given by $\tau^{-1}\sigma\tau\sigma^{-1}=\sigma^{p^\mu}$ as is readily verified. The factor group $F^{(p)}/F^{(p)\prime}$ has type (p^μ, p^∞). Using the ramification theory of infinite normal extensions of an l-adic number field, one sees that the subfield L belonging to $F^{(p)\prime}$ is given as $k(\lambda^{1/p^\mu})U_\infty^{(p)}$ where $U_\infty^{(p)}$ denotes the join of all unramified extensions of degree p^i $(i=1, 2, \cdots)$ over k (cf. [6]). We remark that $F^{(p)}/F^{(p)\prime}=\{\tau, \sigma; \sigma^{p^\mu}=1\}$ is the generalization of the Betti group belonging to a given branch point with signature $1/p^\mu$.

The equivalent to the multiplicative functions belonging to a fuchsian group is given by the multiplicative group $N^{(p)*}$ of the universal field. The field $N^{(p)}$ contains all $p^{i+\mu}$th roots of unity ω_i and all radicals $\lambda^{1/p^i}=\lambda_i$, $i=1, 2, \cdots$. Since k is supposed to contain the pth roots of unity, we have $U_\infty^{(p)}=k(\omega_1, \omega_2, \cdots, \omega_i, \cdots)$. Moreover, the construction of $N^{(p)}$ as $\sum A_i$ implies that $\lambda_i \in N^{(p)}$. Hence

$$N^{(p)} = k(\omega_1, \cdots, \omega_i, \cdots; \lambda_1, \cdots, \lambda_i, \cdots).$$

The groups $\{\omega_i, \lambda_i\}$ which are generated by the elements ω_i, λ_i—for a fixed λ in k—form a multiplicative subgroup $M^{(p)}$ of $N^{(p)*}$. The complete closure $\overline{N^{(p)}}$ of $N^{(p)}$ consists of all sums $\Phi\Psi\sum_{j=0}^{\infty}\Phi_j\Psi_j=P$ where $\Phi, \Phi_j \in \{\omega_i\}, \Psi, \Psi_j \in \{\lambda_i\}$ such that $V(\Psi_j)\to\infty$ where V denotes the valuation of $N^{(p)}$;† $V(\Psi_0)=0$, $\Phi_0\neq 0$. Thus $N^{(p)}$ consists of all elements of $\overline{N^{(p)}}$ which are algebraic over k.

Now let K be an arbitrary regular finite extension of k. The structure theory of complete fields yields that K is complete and that it is uniquely determined by the root of unity $\omega(K)$ of highest order which is contained in K and a prime element $\lambda(K)$ of K:

$$K = \left(\omega(K)^a\lambda(K)^b\sum_{j=0}^{\infty}\omega(K)^{c_j}\lambda(K)^j\right),$$

the c_j residues modulo the order of $\omega(K)$ (cf. [7, 11, 12.2]).

According to Theorem 2 we have $K \subseteq A_i$, where i is sufficiently large. Since $A_i=k(\lambda_i, \omega_i)$, we have

$$\omega(K) = \omega_i^{\alpha(K)}, \qquad \lambda(K) = \omega_i^{\beta(K)}\lambda_i^{\delta(K)}\cdot\epsilon_i$$

where ϵ_i is a unit of A_i which is congruent to 1 (mod (λ_i)).

Let $\{\rho\}$ be the Galois group of A_i/K. Then

$$\lambda(K) = \lambda(K)^\rho = (\omega_i^{\beta(K)}\lambda_i^{\delta(K)}\epsilon_i)^\rho = (\omega_i^{\beta(K)}\lambda_i^{\delta(K)})^\rho\epsilon_i^\rho.$$

† [9]. By Hensel's criterion applied to relatively complete fields.

Hence $(\omega_i^{\beta(K)}\lambda_i^{\delta(K)})^{\rho-1}=\epsilon_i^{1-\rho}$ for all ρ. The unit $\epsilon_i^{1-\rho}$ lies in $\{\epsilon_i\}$; moreover $\{\omega_i, \lambda_i\} \cap \{\epsilon_i\}=1$. Thus, $\epsilon_i^{1-\rho}=1$ for all ρ. For ρ effects a multiplication of λ_i by a root of unity according to the definition of λ_i as a radical. Hence $\epsilon_i \in K$. Thus, $\lambda(K)\cdot\epsilon_i^{-1}=\lambda'(K)=\omega_i^{\beta(K)}\lambda_i^{\delta(K)}$. In other words, the prime element $\lambda(K)$ of K can be normalized in such a way that it lies in $\{\lambda_i, \omega_i\}$.

The group $F^{(p)}$ acts as operator group on $M^{(p)}$. Arranging the elements of $M^{(p)}$ as follows: $\{\{\omega_1, \lambda_1\}, \cdots, \{\omega_i, \lambda_i\}\}$, and observing that $F^{(p)}$ is everywhere dense in $G^{(p)}$, it follows that this representation of $F^{(p)}$ as operator group is an isomorphic one. Let S be an arbitrary normal subgroup of finite index under $F^{(p)}$. Denote by $M(S)$ the subgroup of all elements in $M^{(p)}$ which are left invariant by S. Since S contains some S_i belonging to a field A_i, it follows that $M(S) \subseteq \{\omega_i, \lambda_i\}$. We already noticed before that the field of S is a uniquely determined subfield $K(S)$ of A_i. Hence we can apply the result concerning the normalization of the prime element of $K(S)$. It follows that $M(S)$ is equal to $\{\omega_i, \lambda_i\} \cap K(S)$. In order to determine the maximal root of unity $\omega(S)$ and the normalized prime element $\lambda(S)$ of $K(S)$ we proceed as follows. Since $M(S)$ is a finite group contained in $\{\omega_i, \lambda_i\}$, it has a minimal base of at most 2 elements. Let $\lambda(S)$ be an element of $M(S)$ such that $V(\lambda(S))$ is minimal. Then take for $\omega(S)$ an arbitrary other element of value 0 which has maximal order. The elements $\lambda(S)$, $\omega(S)$, thus selected, obviously have the required properties. These results which are implied by the fact that we have to deal with (discrete) complete fields can be interpreted in the following fashion. The group $M^{(p)}$ is the minimal set of multiplicative functions over k which suffices to describe all finite regular fields. Somehow the elements ω_i correspond to the unramified algebraic functions—obtained from normalized integrals of third kind—of the classical case. The λ_i correspond to ramified algebraic functions with one prescribed pole. Of course, this analogy is rather superficial.

We now want to interpret the Galois groups G_i of the fields A_i/k in terms of certain factor groups of division algebras over k.

Let D_i be the normal division algebra of degree p^i over k which is given by the following relations. The algebra D_i is to consist of all finite sums $\sum_{j,k=1}^{p^i} a_{j,k}\Omega_i^j\Lambda_i^k$, where $a_{j,k}$ are elements of k and Ω_i, Λ_i satisfy the relations

(i) $\Lambda_i^{p^i}=\lambda$,

(ii) Ω_i is a primitive $(q^{p^i}-1)$st root of unity,

(iii) $\Lambda_i^{-1}\Omega_i\Lambda_i=\Omega_i^q$ (cf. [4]).

Let $\mathfrak{P}_i$ be the two-sided prime ideal of D_i and $\{E_i\}$ the totality of all units in D_i which are congruent to 1 (mod $\mathfrak{P}_i$). Obviously, the set $\{E_i\}$ is a group.

LEMMA 6. *Every element of* $\{E_i\}$ *is a* p^i*th power.*

Proof. Let E_i be an arbitrary element of $\{\mathrm{E}_i\}$. Then $\mathrm{E}_i = 1 + B_i$ where $V_{\mathfrak{p}_i}(B_i) > 0$. Consider the subfield $K(B_i)$ of D_i. It contains E_i. Hence, by the proof of Lemma 1, $\mathrm{E}_i = \mathrm{H}^{p^i}$ where H is a suitable unit which is congruent to 1 modulo the prime ideal of $k(B_i)$. Since $\mathrm{H} \in k(B_i) \subset D_i$, the assertion of the lemma is obvious.

THEOREM 6. *The factor group $D_i^*/D_i^{*p^i}$ can be generated by two elements Λ_i^*, Ω_i^* satisfying the relations*

$$\Lambda_i^{*p^i} = \Omega_i^{*p^i} = 1, \qquad \Lambda_i^{*-1}\Omega_i^*\Lambda_i^* = \Omega_i^{*q}.$$

Proof. We first remark that the group $D_i^{*p^i}$ which is generated by the p^ith powers of all nonzero elements in D_i^* is an invariant subgroup of the multiplicative group D_i^*. The group $D_i^{*p^i}$ contains the unit group $\{\mathrm{E}_i\}$, by Lemma 6. Thus, Λ_i and Ω_i can be considered as representatives of $D_i^*/D_i^{*p^i}$. The defining relations of D_i and the fact that $\{\mathrm{E}_i\}$ is an invariant subgroup of D_i^* imply that every class of $D_i^*/D_i^{*p^i}$ can be represented as $\Lambda_i^{\alpha_i}\Omega_i^{\beta_i}D_i^{*p^i}$ where $0 \leqq \alpha_i, \beta_i < p^i$. Hence $\Lambda_i^* = \Lambda_i \pmod{D_i^{*p^i}}$ and $\Omega_i^* = \Omega_i \pmod{D_i^{*p^i}}$ have the required properties.

We can suppose that the Galois group G_i of A_i/k is given by the relations $\sigma_i^{p^i} = \tau_i^{p^i} = 1$, $\tau_i^{-1}\sigma_i\tau_i = \sigma_i^q$. Namely, $q-1$ is exactly divisible by p^μ.

THEOREM 7. *The Galois group G_i of A_i/k is isomorphic with the factor group $D_i^*/D_i^{*p^i}$ of D_i.*

Proof. The asserted isomorphism is an immediate consequence of Theorem 6 and Lemma 4. We let correspond $\sigma_i \to \Omega_i^*$, $\tau_i \to \Lambda_i^*$.

The group $D_i^{*p^i}$ can be considered as the generalization of the norm groups appearing in local class field theory. We can obtain $D_i^{*p^i}$ by the following construction. Consider the norm group $N_iA_i^* = k^{*p^i}$ which belongs to the field A_i/k. Let $\mathfrak{N}_i$ denote the reduced norm of D_i over k. Then $D_i^{*p^i}$ is the subgroup H of maximal index in D_i^* such that $\mathfrak{N}_iH = N_iA_i^*$. This follows immediately if one observes that $\mathfrak{N}_iD_i^* = k^*$, and that Λ_i, Ω_i, $\{\mathrm{E}_i\}$ form a base for all elements of D_i^*. The requirement $\mathfrak{N}_iH = N_iA_i^*$ implies certain congruence conditions for the exponents occurring in the multiplicative representation of the elements in H in terms of the base Λ_i, Ω_i, $\{\mathrm{E}_i\}$. Since $\mathfrak{N}_i$ is an abelian multiplicative function on D_i^*, it follows that H is a normal subgroup of D_i^*.

Now let $D_i^{*\prime}$ be the *maximal* subgroup of D_i^* such that $\mathfrak{N}_iD_i^{*\prime} = N_iA_i^*$. Using the homomorphism principle on groups we get

$$[D_i^* : D_i^{*\prime}] = [D_i^*/D_i^{*p^i} : D_i^{*\prime}/D_i^{*p^i}] = [k^* : N_iA_i^*].$$

The last index is equal to $[G_i : G_i']$, where G_i' denotes the commutator group

of G_i (cf. [1, 8, 10]). Hence $D_i^{*\prime}/D_i^{*p^i}$ is the commutator group of $D_i^*/G_i^{*p^i}$, for $D_i^*/D_i^{*p^i}\cong G_i$ by Theorem 7. Thus, $D_i^{*\prime}/D_i^{*p^i}\cong G_i'$. The latter group is a cyclic group which is generated by the commutator $\tau_i^{-1}\sigma_i\tau_i\sigma_i^{-1}=\sigma_i^{q-1}$. Namely, the structure of A_i/k implies that $A_i=U_{p^i}k(\lambda^{1/p^\mu})(\lambda^{1/p^\mu})$ is a cyclic extension of degree $p^{i-\mu}$ over $U_{p^i}k(\lambda^{1/p^\mu})$. The latter field A_i' obviously belongs to G_i' according to the local class field theory. We have

$$[D_i^*:D_i^{*p^i}] = [\mathfrak{N}_iD_i^*:\mathfrak{N}_iD_i^{*p^i}][X_1:Y_1],$$
$$p^{2i} = [k^*:N_iA_i^*][X_1:Y_1] = p^{i+\mu}p^{i-\mu}, \qquad \text{if } i>\mu.$$

Here X_1 denotes the group of elements in D_i^* whose reduced norms are equal to 1 and similarly, Y_1 the appropriate subgroup of $D_i^{*p^i}$. These statements yield that $D_i^{*\prime}/D^{p^i}$ is represented by a root of unity. For this we only have to take into account the structure of D_i^* and the multiplicative properties of $\mathfrak{N}_i$. It is therefore not so astounding that the Galois groups G_i can be described by factor groups of D_i^*. The algebra D_i contains the $(q^{p^i}-1)$st roots of unity and hence the $p^{\mu+i}$th roots of unity, for the maximal unramified subfield U^{p^i} of D_i has relative degree p^i over k. Consequently U_{p^i} must be given by ω^{1/p^i}, where ω is a primitive $(q-1)$st root of unity in k, for we supposed $q-1\equiv 0\ (p)$.

The field A_i' can be obtained as follows. Consider the group $D_i^*/D_i^{*p^i}$ and reduce it modulo the commutator group $D_i^{*\prime}/D_i^{*p^i}$. Then $\Lambda_i^{*p^\mu}=\lambda^*$ and $\Omega_i^{*p^i}=\omega^*$. Consider λ^* and ω^* as the elements λ, ω in k. Then the solutions x_i, y_i of $x_i^{p^\mu}=\lambda$, $y_i^{p^i}=\omega$ define the field A_i'.

In order to obtain A_i itself, we associate to $D_i^*/D_i^{*p^i}$ the group $\tilde{A}_i$ given by the relations $X_i^{p^i}=\lambda$, $Y_i^{p^i}=\omega$. Then $A_i=k(X_i, Y_i)$. This is to a certain extent the generalization of the theory of radical fields to normal regular extensions.

Suppose now that K is an arbitrary regular normal extension of k. Then $K\subseteqq A_i$ for some A_i by Theorem 2. To the field K there corresponds a uniquely determined invariant subgroup $\overline{H}$ of G_i such that $G(K, k)\cong G_i/\overline{H}$. The local class field theory yields that $G(K, k)/G^*(K, k)'\cong k^*/N_KK^*$, where $G(K, k)'$ denotes the commutator group of $G(K, k)$ and N_KK^* stands for the norm class group of K with respect to k. Theorem 7 implies the existence of a unique invariant subgroup H of D_i^* such that $D_i^*/H\cong G(K, k)$.

THEOREM 8. *Let K be an arbitrary normal regular extension of k such that $K\subseteqq A_i$, then $[k^*:\mathfrak{N}_iH]=[k^*:N_KK^*]$.*

Proof. The first isomorphism theorem of group theory yields that there exists an invariant subgroup $\overline{R}$ of G_i such that $G_i/\overline{R}\cong G(K, k)/G(K, k)'$. Hence $\overline{R}\supseteqq G_i'$ by the properties of the commutator group G_i'. Trans-

ferring $\overline{R}$ to D_i^*, we obtain an invariant subgroup R of D_i^* for which $D_i^*/R \cong G(K, k)/G(K, k)' \cong k^*/N_K K^*$; $R \supseteq D_i^{*\prime}$. Next consider the index $[D_i^*:H]$. Applying the multiplicative mapping N_i to D_i^* and H, we get

$$[D_i^*:H] = [\mathfrak{N}_i D_i^*: \mathfrak{N}_i H][D_i^{*\prime}:D_i^{*\prime} \cap H] = [k^*: \mathfrak{N}_i H][D_i^{*\prime}:D_i^{*\prime} \cap H].$$

The second isomorphism theorem of group theory yields

$$D_i^{*\prime}/D_i^{*\prime} \cap H \cong D_i^* \cup H/H.$$

Consequently, $[k^*:\mathfrak{N}_i H] = [D_i^*:H \cup D_i^{*\prime}]$. Namely, the inclusion $D_i^* \supseteq H \cup D_i^{*\prime} \supseteq H$ implies

$$[D_i^{*\prime} \cup H:H] = [D_i^*:H][D_i^*:D_i^{*\prime} \cup H]^{-1}.$$

Thus $[D_i^*:H] = [k^*:\mathfrak{N}_i H][D_i^*:H][D_i^*:D_i^{*\prime} \cup H]^{-1}$. Since D_i^*/R is an abelian group, we have $R \supseteq D_i^{*\prime}$, by the properties of the commutator group $D_i^{*\prime}$. Hence $R \supseteq D_i^{*\prime} \cup H$. But also $D_i^{*\prime} \cup H \subseteq R$ for R/H is the commutator group of D_i^*/H. Consequently, $D_i^{*\prime} \cup H = R$.

Application of N_i to the groups D_i^* and $D_i^* \cup H$ yields

$$\begin{aligned}[D_i^*:D_i^{*\prime} \cup H] &= [\mathfrak{N}_i D_i^*: \mathfrak{N}_i D_i^{*\prime} \cap H][D_i^{*\prime}:D_i^{*\prime} \cup (H \cap D_i^{*\prime})] \\ &= [k^*: \mathfrak{N}_i H].\end{aligned}$$

Finally, $[k^*:N_K K^*] = [k^*:\mathfrak{N}_i H]$ for $D_i^*/R \cong G(K, k)/G(K, k)'$.

Finally we want to indicate briefly that the theory of regular normal extensions K/k cannot be developed with respect to a fixed division algebra D_i of degree p^i over k. It would be natural to require that every Galois group G is a homomorphic map of D_i^*. In analogy to the theory of abelian fields (which can be described by subgroups of k^*) we would require that all units $\{\mathrm{E}_i\}$ of D_i are contained in the subgroups H of D_i^* belonging to the arbitrarily given field K/k. Namely, the set of units $\mathrm{E}_i^{(j)} \equiv ((\Lambda_i)^j)$ form an invariant subgroup of the totality of *all* units in D_i. The index of this subgroup turns out to be equal to $q^{p^i j-1}(q^{p^i}-1)$. Thus $p^{\mu p^i} \| q^{p^i j-1}(q^{p^i}-1)$ for D_i contains no units of higher p-order than $p^{\mu p^i}$, as follows from the algebraic theory of splitting fields of D_i. Hence the class groups H which supposedly can be associated to the fields K/k must contain E_i. Consequently, any such invariant group H of D_i must contain $\{\Omega_i^m\} \cup \{\Lambda_i^s\}$ for suitable chosen integers m, s. Since D_i contains only roots of unity of bounded p-order, the possible exponents are bounded, say $m \leqq m_0$. If $m > m_0$, then $\{\Omega_i^m\} \cup \{\Lambda_i^s\} = \{\Omega_i^{m_0}\} \cup \{\Lambda_i^s\}$. We have a similar fact in local class field theory. There the ramification exponents $e(K)$ of regular fields are bounded by p^μ. The reason being that the ground field k does not contain sufficiently may roots of unity. Such roots of unity always are needed to describe the class groups of ramified abelian extensions. In

other words, in the abelian case the regular extensions are made up by a ramified extension of degree p^μ and an unramified extension of arbitrarily high degree (cf. [10]). A similar situation prevails in the general case. Having fixed an algebra D_i, we only can describe by means of D_i such regular fields K which contain a normal subfield whose ramification degree is not greater than $p^{\mu p^i}$. One also could arrive at this result by purely group theoretical analysis. The structure of $D_i^*/\{\Omega_i^m\} \cup \{\Lambda_i^s\}$ can easily be determined. One observes that not all G_i can be homomorphic maps of some suitable $D_i^*/\{\Omega_i^m\} \cup \{\Lambda_i^s\}$. Hence, by virtue of Theorem 2, not every G can be described as a homomorphic map of D_i^*. These considerations indicate why the totality of all algebras D_i is required for our generalization of local class field theory.

Bibliography

1. Y. Akizuki, *Eine homomorphe Zuordnung der Elemente der galoisschen Gruppe zu den Elementen einer Untergruppe der Normklassengruppe*, Mathematische Annalen, vol. 112 (1936).

2. W. Burnside, *Theory of Groups of Finite Order*.

3. C. Chevalley, *La théorie du symbole de restes normiques*, Journal für die reine und angewandte Mathematik, vol. 169 (1933).

4. H. Hasse, *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Mathematische Annalen, vol. 104 (1930).

5. K. Hensel, (1) *Allgemeine Theorie der Kongruenzklassengruppen und ihrer Invarianten in algebraischen Zahlkörpern*, Journal für die reine und angewandte Mathematik, vol. 147 (1917); (2) *Zahlentheorie*, Berlin and Leipzig.

6. J. Herbrand, *Théorie arithmétique des corps de nombres de degré infini*, II. *Extensions algébriques de degré infini*, Mathematische Annalen, vol. 108 (1933).

7. S. MacLane, *Subfields and automorphisms of p-adic fields*, Annals of Mathematics, (2), vol. 40 (1939).

8. T. Nakayama, *Über die Beziehungen zwischen den Faktorensystemen und der Normklassengruppe eines galoisschen Erweiterungskörpers*, Mathematische Annalen, vol. 112 (1936).

9. A. Ostrowski, *Untersuchungen zur arithmetischen Theorie der Körper*, Mathematische Zeitschrift, vol. 39 (1935).

10. F. K. Schmidt, *Zur Klassenkörpertheorie im Kleinen*, Journal für die reine und angewandte Mathematik, vol. 162 (1930).

11. O. Teichmüller, *Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper*, Journal für die reine und angewandte Mathematik, vol. 176 (1936).

12. E. Witt, (1) *Konstruktion von galoisschen Körpern der Charakteristik p mit gegebener Gruppe der Ordnung p^n*, Journal für die reine und angewandte Mathematik, vol. 174 (1936); (2) *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n*, Journal für die reine und angewandte Mathematik, vol. 176 (1936).

University of Chicago,
Chicago, Ill.