EXPLICIT CLASS FIELD THEORY FOR RATIONAL FUNCTION FIELDS(*)

BY

D. R. HAYES

ABSTRACT. Developing an idea of Carlitz, I show how one can describe explicitly the maximal abelian extension of the rational function field over \( \mathbb{F}_q \) (the finite field of \( q \) elements) and the action of the idèle class group via the reciprocity law homomorphism. The theory is closely analogous to the classical theory of cyclotomic extensions of the rational numbers.

The class field theory of the rational numbers \( \mathbb{Q} \) is “explicit” in the sense that one can write down a sequence of polynomials whose roots generate the maximal abelian extension of \( \mathbb{Q} \), and one can describe concretely how a given \( \mathbb{Q} \)-idèle class operates on each of these roots via the reciprocity law homomorphism (see [1, Chapter 7]). A similar program can be carried out for imaginary quadratic fields using the theory of elliptic curves (see [4, Chapter 13]). These results are quite old, having originally been conceived by Kronecker in the late 19th century. More recently, Lubin and Tate [5] have given such an explicit description of the class field theory for any local field using the theory of formal groups. All of these results use the same basic procedure: A ring of “integers” in the ground field is made to act on part of the algebraic closure of that field, and the maximal abelian extension is gotten essentially by adjoining the torsion points of that action. For example, one obtains the maximal abelian extension of \( \mathbb{Q} \) by adjoining the torsion points of \( \mathbb{Z} \) acting by exponentiation on the multiplicative group of the field of algebraic numbers.

This paper contains a similar explicit description for the class field theory of a rational function field (over a finite field of constants). The main idea comes from a paper of Carlitz [2], the aim of which was to develop an analog of the cyclotomic polynomial for the ring of polynomials over a finite field. In brief, this Carlitz cyclotomic theory goes as follows: Let \( k \) be the field of rational functions over the finite field \( \mathbb{F}_q \) of \( q \) elements. Of the \( q^3 - q \) generators of \( k \) over \( \mathbb{F}_q \) pick one, say \( T \), and consider the polynomial subring \( R_T = \mathbb{F}_q[T] \) of \( k \). Carlitz makes \( R_T \) act as a ring of endomorphisms on the additive group of \( k^\times \), the algebraic closure of \( k \). For \( M \in R_T \), the action of \( M \) is given by a separable polynomial

(*) The major part of the work on this paper was carried out while the author held an NSF Postdoctoral Fellowship.

Received by the editors March 10, 1972.


Key words and phrases. Rational function field over a finite field, explicit class field theory, cyclotomic extensions.
with coefficients in \( R_T \) whose set of roots \( \Lambda_M \) (the \( M \)-torsion points of \( k^{ac} \)) generate a finite abelian extension field \( k(\Lambda_M) \) of \( k \). The properties of these extensions are quite similar to those of the cyclotomic extensions of \( \mathbb{Q} \).

Carlitz arrives at his definition of the \( R_T \) action in a remarkable way. The choice of \( T \) singles out an “infinite prime” of \( k \), namely the unique pole \( P_\infty \) of \( T \). In a previous paper [3], he had defined an analytic function \( \psi(u) \) on \( k_\infty \), the completion of \( k \) at \( P_\infty \), with properties closely resembling those of the function \( \exp(ix) \) on the real numbers. This \( \psi(u) \) is defined by an everywhere convergent power series with coefficients from \( k \). Carlitz then notices that for a given \( M \in R_T \), \( \psi(Mu) = \omega_M(\psi(u)) \) where \( \omega_M \) is a uniquely determined additive polynomial over \( R_T \). The properties of \( \psi(u) \) made it evident that the action \( M \cdot u = \omega_M(u) \) gives the additive group of \( k^{ac} \) the structure of an \( R_T \)-module. Carlitz was able to give a purely algebraic description of \( \omega_M \) and, therefore, of the \( R_T \) action. He noted also that the roots of \( \omega_M \) are expressible in the form \( \psi(A/M)\xi \) where \( \xi \) is a “transcendental element” lying in the completion of the algebraic closure of \( k_\infty \) and \( A \) is in \( R_T \). Thus, the elements of \( \Lambda_M \) are the values of an analytic function at the rational points of the form \( A/M \). For the details, I refer the reader to the original papers.

Carlitz makes a careful study of the polynomials \( \omega_M(u) \) and proves the analog of the theorem which states that the cyclotomic polynomial is irreducible over \( \mathbb{Q} \). In §§1–4 below, I give an exposition of Carlitz’ results in the language of modern algebraic number theory. A discussion of how the prime \( P_\infty \) splits in \( k(\Lambda_M) \) is also included. This question does not arise naturally in Carlitz’ set-up, but it is crucial for the application to the class field theory of \( k \). For what it is worth, I also calculate the different of \( k(\Lambda_M) \) when \( M \) is a power of an irreducible and thereby get a formula for the genus of \( k(\Lambda_M) \) in that case.

§§5, 6 and 7 are modeled after the usual explicit construction of the norm residue symbol for cyclotomic extensions of \( \mathbb{Q} \) (see Chapter 7 of [1] or Chapter 7 of [4]). It turns out that the extensions \( k(\Lambda_M) \) together with the constant field extensions almost generate the maximal abelian extension of \( k \). What is lacking is a piece containing the extensions where \( P_\infty \) is wildly ramified. This piece is constructed out of the theory which results from the choice of \( 1/T \) as generator instead of \( T \).

It is perhaps surprising that the results come by using endomorphisms of the additive group of \( k^{ac} \). Note however that the formal group law constructed from \( \pi T + T^q \) in the Lubin-Tate theory is just \( X + Y \) in the equicharacteristic case. This gives some hope that the additive group might be used in a similar way to do explicit class field theory for an arbitrary function field in one variable over \( \mathbb{F}_q \).

1. The \( R_T \) action. As above, \( k \) is the field of rational functions over the finite field \( \mathbb{F}_q \) of \( q \) elements. We arbitrarily choose a generator \( T \) of \( k \) and put \( R_T = \mathbb{F}_q[T] \), the polynomial subring of \( k \) generated by \( T \) over \( \mathbb{F}_q \). Most of the results will be relative to this choice of \( T \), although this fact is suppressed (more or less) in the notation.
Let \( k^{ac} \) be the algebraic closure of \( k \). The \( \mathbb{F}_q \)-algebra \( \text{End}(k^{ac}) \) of all \( \mathbb{F}_q \)-endomorphisms of the additive group of \( k^{ac} \) contains the Frobenius automorphism \( \varphi \) defined by \( \varphi(u) = u^q \) and the map \( \mu_T \) defined by \( \mu_T(u) = Tu \). Since \( R_T \) is a polynomial ring over \( \mathbb{F}_q \), the substitution \( T \mapsto \varphi + \mu_T \) yields a ring homomorphism \( R_T \rightarrow \text{End}(k^{ac}) \) which provides \( k^{ac} \) with the structure of an \( R_T \)-module. If we write \( u^M \) for the action of \( M \in R_T \) on \( u \in k^{ac} \), then we have

\[
(1.1) \quad u^M = M(\varphi + \mu_T)(u).
\]

Note that for \( \alpha \in \mathbb{F}_q \), \( \alpha^\varphi = \alpha u \), so that our \( R_T \) action respects the \( \mathbb{F}_q \)-algebra structure of \( k^{ac} \).

**Proposition 1.1.** If \( d = \deg M \), then

\[
(1.2) \quad u^M = \sum_{i=0}^{d} \left[ \begin{array}{c} M \\ i \end{array} \right] \cdot u^{q^i}
\]

where each \( \left[ \begin{array}{c} M \\ i \end{array} \right] \) is a polynomial in \( R_T \) of degree \( (d - i)q^i \). Further \( \left[ \begin{array}{c} M \\ 0 \end{array} \right] = M \) and \( \left[ \begin{array}{c} M \\ d \end{array} \right] \) is the leading coefficient of \( M \).

**Proof.** Since each element of \( R_T \) is an \( \mathbb{F}_q \)-linear combination of powers of \( T \), it suffices to verify the proposition for the special case \( M = T^d \). The endomorphisms \( \varphi \) and \( \mu_T \) do not commute but rather obey the rule \( \varphi \circ \mu_T = \mu_T^q \circ \varphi \). Therefore, one can write \( (\varphi + \mu_T)^d \) as a sum of terms of the form \( \mu_T^{d-i} \circ \varphi^i \). Since \( (\mu_T^{d-i} \circ \varphi^i)u = T^i u^{q^i} \), we see that \( u^M \) is indeed a polynomial in \( u \) of the form \( (1.2) \). For \( i = d \), there is a unique term \( q^d \) and \( q^d(u) = u^{q^d} \). For \( i = 0 \), there is a unique term \( \mu_T^d \) and \( \mu_T^d(u) = T^d u \). For \( 0 < i < d \), there is a unique term with maximum \( s \), namely \( \varphi^i \circ \mu_T^{d-i} = \mu_T^{d-i} \circ \varphi^i \). This completes the proof.

Put \( \left[ \begin{array}{c} M \\ i \end{array} \right] = 0 \) for \( i < 0 \) and \( i > \deg M \). In calculating the polynomial \( \left[ \begin{array}{c} M \\ i \end{array} \right] \), one can make use of the following easily established properties:

\[
(a) \quad \left[ \begin{array}{c} \alpha M + \beta N \\ i \end{array} \right] = \alpha \cdot \left[ \begin{array}{c} M \\ i \end{array} \right] + \beta \cdot \left[ \begin{array}{c} N \\ i \end{array} \right] \quad \text{for} \quad \alpha, \beta \in \mathbb{F}_q.
\]

\[
(b) \quad \left[ \begin{array}{c} T^d+1 \\ i \end{array} \right] = T \cdot \left[ \begin{array}{c} T^d \\ i \end{array} \right] + \left[ \begin{array}{c} T^d \\ i-1 \end{array} \right] ^q.
\]

In [2, Equation 1.6], Carlitz gives an explicit formula for these polynomials.

**Definition 1.2.** Let \( \Lambda_M \) denote the set of \( M \)-torsion points of \( k^{ac} \), i.e., the set of zeros of the polynomial \( u^M \). Since \( R_T \) is commutative, \( \Lambda_M \) is an \( R_T \)-submodule of \( k^{ac} \).

**Proposition 1.3.** As a polynomial in \( u \) over \( k \), \( u^M \) is separable of degree \( q^d \), where \( d = \deg M \). The submodule \( \Lambda_M \) is finite of order \( q^d \) and is therefore a vector space over \( \mathbb{F}_q \) of dimension \( d \).
Proof. From Proposition 1.1, we see that $u^M$ is of degree $q^d$ in $u$ and that its derivative with respect to $u$ is just $[u^M] = M$. The proposition follows immediately.

The structure of the $R_T$-module $\Lambda_M$ will now be determined. As one might expect from the analogous cyclotomic theory, $\Lambda_M$ turns out to be a cyclic $R_T$-module.

**Proposition 1.4.** Let $M = \alpha \prod P^n$ be a factorization of $M$ into powers of monic irreducibles. Then

$$\Lambda_M = \sum_{P | M} \Lambda_{P^n},$$

and the sum is direct.

**Proof.** This follows from the general theory of modules over principal ideal domains. In fact, $\Lambda_{P^n}$ is the $P$-primary submodule of $\Lambda_M$, and so (1.3) is the canonical decomposition of $\Lambda_M$ into its $P$-primary components.

**Proposition 1.5.** If $M = P^n$, where $P$ is irreducible, then $\Lambda_M$ is a cyclic $R_T$-module.

**Proof.** Let $d = \deg P$. The proof goes by induction on $n$. For $n = 1$, $\Lambda_P$ is a vector space over $R_T/(P)$. Since both $R_T/(P)$ and $\Lambda_P$ contain $q^d$ elements, $\Lambda_P$ is 1-dimensional, hence cyclic over $R_T/(P)$, and hence cyclic over $R_T$. Now assume the proposition true for $n = k$, $k \geq 1$. The map $u \mapsto u^P$ from $\Lambda_{P^{k+1}} \to \Lambda_{P^k}$ is surjective since its domain, kernel and range contain respectively $q^{d(k+1)}$, $q^d$ and $q^{dk}$ elements. Since $\Lambda_{P^k}$ is cyclic by the induction hypothesis, one can therefore choose $\lambda \in \Lambda_{P^{k+1}}$ so that $\lambda^P$ generates $\Lambda_{P^k}$. This $\lambda$ will generate $\Lambda_{P^{k+1}}$ over $R_T$. To prove it, let $\mu \in \Lambda_{P^{k+1}}$ be given. Then choose $A \in R_T$ such that $\mu^P = \lambda^PA$. Then $\mu - \lambda^A$ belongs to $\Lambda_P$. Now $\lambda^{PA} \in \Lambda_P$ is not zero since $\lambda^P$ generates $\Lambda_{P^k}$. Therefore, since $\Lambda_P$ is a 1-dimensional vector space over $R_T/(P)$, there is a $B \in R_T$ such that $\mu - \lambda^A = \lambda^{PA}B$. We conclude that $\mu = \lambda^{PA+B}$. Therefore, $\lambda$ generates $\Lambda_{P^{k+1}}$, and the proof is complete.

**Theorem 1.6.** The $R_T$-module $\Lambda_M$ is naturally isomorphic to $R_T/(M)$ for every $M \neq 0$ in $R_T$.

**Proof.** Since by Propositions 1.4 and 1.5 each of the $P$-primary components of $\Lambda_M$ is cyclic, $\Lambda_M$ is itself cyclic. Therefore, $\Lambda_M$ is naturally isomorphic to the quotient of $R_T$ by the annihilator ideal of $\Lambda_M$. Clearly, the ideal $(M)$ is contained in that annihilator. On the other hand, both $\Lambda_M$ and $R_T/(M)$ have $q^d$ elements, where $d = \deg M$. Therefore, $(M)$ must equal the annihilator of $\Lambda_M$, and the proof is complete.

**Definition 1.7.** If $M \in R_T$, $M \neq 0$, then $\Phi(M)$ is the order of the group of units of $R_T/(M)$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Corollary 1.8. The cyclic $R_T$-module $\Lambda_M$ has exactly $\Phi(M)$ generators. In fact, if $\lambda$ is a given generator and $A \in R_T$, then $\lambda^A$ is a generator if and only if $A$ and $M$ are relatively prime.

2. The fields $k(\Lambda_M)$. One knows that, with one exception, the prime divisors of the rational function field $k$ correspond one-to-one to the monic irreducible polynomials $P$ in $R_T$. The exception is the unique pole $P_\infty$ of $T$, the “infinite prime.” For convenience, I will use the symbol “$P$” to denote both a monic irreducible and the prime divisor to which it corresponds. No confusion should arise.

Consider now the extension field $k(\Lambda_M)$ of $k$ which arises by adjoining to $k$ the elements of the finite module $\Lambda_M$. Let $\lambda$ be a generator of $\Lambda_M$ over $R_T$ (Theorem 1.6). Since $\lambda^A$ is a polynomial in $\lambda$ with coefficients from $R_T$, $\lambda^A \in k(\lambda)$ for every $A \in R_T$. It follows that one can obtain $k(\Lambda_M)$ by adjoining to $k$ a single generator of $\Lambda_M$. Also, since $\Lambda_M$ is the set of zeros of the separable polynomial $u_M$ over $R_T \subset k$, the extension $k(\Lambda_M)/k$ is finite and Galois. Further, the elements of $\Lambda_M$ are all integral over $R_T$ since by Proposition 1.1 the leading coefficient of $u_M$ belongs to $F$.

Let $G_M$ be the Galois group of $k(\Lambda_M)/k$. The action of $G_M$ commutes with the $R_T$-action since the $R_T$-action is given by a polynomial over $k$. Choose a generator $\lambda$ of $\Lambda_M$. Since $\lambda$ also generates the field extension, every $\sigma \in G_M$ is determined by its action on $\lambda$. We must have $\sigma(\lambda) = \lambda^A$ for some $A$ relatively prime to $M$ since $\sigma$ must map a generator of $\Lambda_M$ to another generator. Further, this $A$ does not depend on the choice of the generator $\lambda$. Therefore, the map $\sigma \mapsto A \pmod{M}$ is a well-defined injection of $G_M$ into the group of units of $R_T/(M)$. One easily verifies that this injection is a group homomorphism. We have thus proved the following

Theorem 2.1. The Galois group $G_M$ is isomorphic to a subgroup of the group of units of $R_T/(M)$. The Galois extension $k(\Lambda_M)/k$ is abelian, and $[k(\Lambda_M): k] \leq \Phi(M)$.

This last theorem does not tell the whole story since actually the map from $G_M$ into the group of units of $R_T/(M)$ is an isomorphism. One way to prove it is to examine the ramification at the prime divisors which correspond to the irreducible factors of $M$, just as one does in the usual cyclotomic theory.

Proposition 2.2. Suppose $M = P^n$ where $P$ is a monic irreducible polynomial in $T$ with $\deg P = d$. Then every prime divisor of $k$ except $P$ and $P_\infty$ is unramified in $k(\Lambda_M)$, and the ramification number of $P$ is $\Phi(M) = q^{dn} - q^{d(n-1)}$.

Proof. Let $I_M$ be the integral closure of $R_T$ in $k(\Lambda_M)$. Since $R_T$ is a Dedekind ring, so is $I_M$. We must determine which finite prime divisors of $k$ divide the discriminant $D(I_M)$ of $I_M$ over $R_T$. Let $\lambda$ be a generator of $\Lambda_M$. Then $R_T[\lambda]$ is a subring of $I_M$, and its discriminant $D(\lambda)$ divides the divisor of Norm($f'(\lambda)$) where
$f(u)$ is any polynomial over $R_T$ which has $\lambda$ as a root. Take $f(u) = u^M$. Then, by Proposition 1.1, $f'(u) = M = P^n$, a constant polynomial over $R_T$. Therefore, $P$ is the only prime divisor of $R_T$ which enters into $D(\lambda)$. Since $D(I_M)$ divides $D(\lambda)$, it follows that $P$ is the only prime divisor of $R_T$ which divides $D(I_M)$. Therefore, except maybe for $P_\infty$, the only ramification of the extension $k(\Lambda_M)/k$ occurs at $P$.

In order to calculate the ramification number at $P$, proceed as follows: Note first that $u^P = (u^{p^{-1}})^P = u^{p^{-1}} \cdot f(u)$ for some polynomial $f(u)$ over $R_T$ since $u$ divides $u^P$ by Proposition 1.1. Therefore, $f(u) = u^{P^n}/u^{P^n-1} = P +$ higher terms. The roots of $f$ are obviously exactly the generators of the module $\Lambda_M$. Therefore,

$$f(u) = \prod_A \lambda^A$$

where $A$ runs over a set of representatives of the group of units of $R_T/(M)$. Now $\lambda$ divides $\lambda^A$ in $I_M$ since $u$ divides $u^A$. By symmetry, $\lambda^A$ also divides $\lambda$. Therefore, $\lambda^A = (\text{unit}) \cdot \lambda$. Substituting this in (2.1), we find that

$$\pm P = (\text{unit}) \cdot \lambda^{\Phi(M)}.$$

The ramification number $e_P$ of $P$ is therefore greater than $\Phi(M)$. But also $e_P \leq [k(\Lambda_M): k] = \Phi(M)$. Therefore, $e_P = [k(\Lambda_M): k] = \Phi(M)$. This completes the proof.

The main result is a corollary of this last proposition:

**Theorem 2.3.** The extension $k(\Lambda_M)/k$ has degree $\Phi(M)$, and the Galois group $G_M$ is isomorphic to the group of units of $R_T/(M)$.

**Proof.** By Theorem 2.1, it is enough to prove that the degree equals $\Phi(M)$. For $M = P^n$, this follows from Proposition 2.2. If $M$ has the factorization $M = \prod P^n$, where each $P$ is a monic irreducible, then the total ramification of $k(\Lambda_P)/k$ at $P$ shows that each extension $k(\Lambda_P)/k$ for $P$ dividing $M$ is linearly disjoint from the composite of the remaining ones. Therefore,

$$[k(\Lambda_M): k] = \prod_{P|M} [k(\Lambda_P): k] = \prod_{P|M} \Phi(P^n) = \Phi(M),$$

and the proof is complete.

One last result is needed for use in §§4 and 7 below. The analogous result in the cyclotomic theory can be proved directly from properties of binomial coefficients. One can devise a similar direct proof which works here, but we give a proof based on Proposition 2.2.

**Proposition 2.4.** If $M = P^n$, where $P$ is a monic irreducible in $R_T$, then $f(u) = u^{P^n}/u^{P^n-1}$ is an Eisenstein polynomial over $R_T$ at $P$.

**Proof.** Let $\lambda$ be a generator of $\Lambda_M$. From the proof of Proposition 2.2,

$$f(u) = \prod_A (u - \lambda^A)$$
where \( A \) runs through a set of representatives of the group of units of \( R_T/(M) \).

Let \( \mathfrak{p} \) be the unique prime divisor of \( k(\Lambda_M) \) lying over \( P \). From (2.2) and the total ramification at \( P \), it follows that \( \text{ord}_P \lambda = 1 \), and the same holds true of the generator \( \lambda^A \). Therefore, (2.3) shows that the coefficients of all but the highest order term in \( f(u) \) belong to the valuation ring at \( \mathfrak{p} \) and hence are divisible by \( P \) in \( R_T \). Since the constant coefficient is \( P \), \( f(u) \) is Eisenstein, and the proof is complete.

**Corollary 2.5.** Suppose \( P \) is a finite prime of \( k \) which does not divide \( M \). Then the automorphism \( \varphi_P \) of \( k(\Lambda_M) \) which takes \( \lambda \) in \( \Lambda_M \) to \( \lambda^P \) is that given by the Artin symbol.

**Proof.** Let \( d = \deg P \). Consider a given generator \( \lambda \in \Lambda_M \). Let the Artin symbol take \( \lambda \) to \( \lambda^L \) for suitable \( L \in R_T \). By definition, we have \( \lambda^L = \lambda^{\mathfrak{p}} \pmod{\mathfrak{p}} \) where \( \mathfrak{p} \) is a prime of \( k(\Lambda_M) \) lying over \( P \). But also \( \lambda^P = \lambda^{\mathfrak{p}} \pmod{\mathfrak{p}} \) by the above proposition. Now

\[
u^M = \prod_{A \mod M} (u - \lambda^A).
\]

Taking the derivative of both sides of this equation and recalling that the derivative of \( u^M \) is just \( M \), we get

\[
M = \prod_{A \mod M} (\lambda^B - \lambda^A) \quad (A \neq B)
\]

for every \( B \) in \( R_T \). Since \( P \) does not divide \( M \), this means that the \( \lambda^A, A \mod M \), have distinct images in the residue class field at \( \mathfrak{p} \). Therefore, \( \lambda^P = \lambda^L \) implies that \( \lambda^P = \lambda^L \). But an automorphism of \( k(\Lambda_M) \) is determined by its action on \( \lambda \). So \( \varphi_P \) is the Artin symbol at \( P \).

3. **The ramification at \( \mathfrak{P}_0 \)**. The fundamental fact about the ramification at \( \mathfrak{P}_0 \) in \( k(\Lambda_M)/k \) is that it is tame:

**Theorem 3.1.** Let \( M \in R_T, M \neq 0 \). Then \( \mathfrak{P}_0 \) is tamely ramified in \( k(\Lambda_M)/k \).

It suffices by the usual arguments to prove this theorem in the special case \( M = P^n \) where \( P \) is a monic irreducible in \( R_T \). For this special case, I prove a better theorem which shows precisely how \( \mathfrak{P}_0 \) splits.

**Theorem 3.2.** Let \( M = P^n \) where \( P \) is a monic irreducible in \( R_T \) with \( \deg P = d \). Then \( \mathfrak{P}_0 \) splits into \( \Phi(M)/(q - 1) \) prime divisors in \( k(\Lambda_M) \). The ramification number \( e_\infty \) is given by \( e_\infty = q - 1 \) at each of these primes, and the degree of inertia is 1.

**Proof.** Let \( \mathfrak{P} \) be any prime divisor of \( k(\Lambda_M) \) lying over \( \mathfrak{P}_0 \). Since the extension \( k(\Lambda_M)/k \) is Galois of degree \( \Phi(M) \), it suffices to prove that \( e_\mathfrak{P} = q - 1 \) and \( f_\mathfrak{P} = 1 \). Let \( \mathfrak{p} \) be a prime divisor of \( k(\Lambda_P) \subset k(\Lambda_M) \) which lies under \( \mathfrak{P} \) (and hence over \( \mathfrak{P}_0 \)). Schematically, we have
I show first that $e^p = q - 1$ and $f_p = 1$ and then that $\mathfrak{p}$ splits completely in $k(\Lambda_M)/k(\Lambda_P)$. Since $e$ and $f$ multiply in towers, this will yield the theorem. The proof is an exercise in drawing Newton polygons.

First consider $\mathfrak{p}$ over $P_p$. The field $k(\Lambda_P)$ is gotten by adjoining to $k$ any root of the irreducible polynomial $g(u) = u^p - u$. From Proposition 1.1, $g(u) = h(u^{ap})$ where

$$h(u) = \sum_{i=0}^{d} f_i(T) \cdot u^{(q^i-1)/(q-1)} = f_0(T) + f_1(T)u + \cdots$$

and $\deg f_i = (d-i)q^i$. Let $k_\infty$ be the completion of $k$ at $P_p$, and let $v_\infty$ be the normalized valuation on $k_\infty$. Then $v_\infty(f_i(T)) = -(d-i)q^i$. To get the Newton polygon of $h(u)$ over $k_\infty$, one plots the points $\beta_i = ((q^i - 1)/(q - 1), -(d - i)q)$ for $0 \leq i \leq d$. A short calculation shows that the slope of the line segment joining $\beta_i$ and $\beta_{i+1}$ is just $-(d - i)(q - 1) + q$. Since the slopes increase strictly with $i$, the points $\beta_i$ must be exactly the vertices of the Newton polygon of $h(u)$. For the points $\beta_0$ and $\beta_1$, we find the slope $-(d(q - 1) + q$, which shows that $h(u)$ has a root $\theta$ in $k_\infty$ with $v_\infty(\theta) = d(q - 1) - q$. Now because $g(u) = h(u^{ap})$, the completion $k(\Lambda_P)_p$ of $k(\Lambda_P)$ at $\mathfrak{p}$ is gotten from $k_\infty$ by adjoining a root $\lambda$ of $u^{ap} - \theta = 0$. Therefore, since $v_\infty(\theta)$ and $q - 1$ are relatively prime, the extension $k(\Lambda_P)_p/k_\infty$ is totally ramified of degree $q - 1$. Hence, $e^p = q - 1$ and $f_p = 1$.

The next problem is to determine how $\mathfrak{p}$ splits in the extension $k(\Lambda_M)/k(\Lambda_P)$. Let $v_\mathfrak{p}$ be the (normalized) valuation of $k(\Lambda_P)$ at $\mathfrak{p}$. From the previous paragraph, $g(u)$ has a root $\lambda$ such that $v_\mathfrak{p}(\lambda) = d(q - 1) - q$. Now as $u^p = u \cdot g(u)$,

$$u^p = u^{ap} = (u^{ap-1})^p = u^{ap-1} \cdot g(u^{ap-1})$$

so that $k(\Lambda_M)$ comes by adjoining to $k$ any root of $g(u^{ap-1})$. Therefore, $k(\Lambda_M)$ is gotten from $k(\Lambda_P)$ by adjoining a root of $u^{ap-1} - \lambda = 0$. To calculate the Newton polygon of $u^{ap-1} - \lambda$, one plots the points $\gamma_1 = (0, v_\mathfrak{p}(\lambda)) = (0, d(q - 1) - q)$ and

$$\gamma_i = (q^i, v_\mathfrak{p}(f_i(T))) = (q^i, -(q - i)(d - 1)q)$$

for $0 \leq i \leq d(n - 1)$. A short calculation shows that the slope from $\gamma_1$ to $\gamma_0$ is $-(q - 1)d(n - q)$ and that the slope from $\gamma_i$ to $\gamma_{i+1}$ for $i \geq 0$ is $-(q - 1) \cdot (d(n - d - i)) + q$. Again, these slopes increase strictly with $i$ so that the vertices of the Newton polygon of $u^{ap-1} - \lambda$ over $k(\Lambda_P)_p$ are exactly the $\gamma_i$. The segment
EXPLICIT CLASS FIELD THEORY

from $\gamma_1$ to $\gamma_0$ shows that $u^{p^{n-1}} - \lambda$ has a root in $k(\Lambda_P)$. Since the extension is Galois, this means that $v$ splits completely in $k(\Lambda_M)$. This completes the proof.

4. Calculation of the different and genus. Throughout this section, $M = P^n$ where $P$ is a monic irreducible in $T$. The enterprising reader can write down a formula for the different for arbitrary $M$ by using the functorial properties of the different and the results given here.

Theorem 4.1. Let $D$ be the different of the extension $k(\Lambda_M)/k$, where $M = P^n$, $P$ monic, and $\deg P = d$. Then

$$D = \mathfrak{P}^s \cdot \prod_{\mathfrak{p} | P_\mathfrak{p}} \mathfrak{p}^{q-2}$$

where $\mathfrak{P}$ is the unique prime of $k(\Lambda_M)$ lying over $P$ and $s = n \cdot \Phi(M) - q^{d(n-1)}$.

Proof. Only primes lying over $P$ or $P_\mathfrak{p}$ are ramified, so only such primes divide $D$. Since the ramification at $v$ for $v | P_\mathfrak{p}$ is tame, $v$ appears in the different with exponent $e_v - 1 = q - 2$. Hence, everything is proved except for the value of $s$.

To find $s$, go local and calculate the different of $k(\Lambda_M)_{P}/k_P$. This extension is totally ramified of degree $\Phi(M)$, and $k(\Lambda_M)_{P}$ is generated over $k_P$ by a single root $\lambda$ of $f(u) = u^{n}/u^{n-1}$. By Proposition 2.4, $f(u)$ is Eisenstein at $P$, which implies that the powers $\lambda^i$ for $0 \leq i < \Phi(M)$ constitute an integral basis for the extension. Therefore, the discriminant $D$ of the extension is the ideal generated by $\text{Norm}(f'(\lambda))$. Now $u^{n} = u^{n-1} \cdot f(u)$ and the derivatives of $u^{n}$ and $u^{n-1}$ are respectively the constants $P^n$ and $P^{n-1}$ by Proposition 1.1. Therefore,

$$P^n = P^{n-1} \cdot f(u) + u^{n-1} \cdot f'(u)$$

and hence

$$P^n = \lambda^{n} \cdot f'(\lambda).$$

Since $\lambda^{n} \in \Lambda_P$, the norm of $\lambda^{n}$ is the $\Phi(M)/\Phi(P)$ power of its norm from $k(\Lambda_P)_{P}$ to $k_P$, and this latter norm is just $\pm P$. Therefore, on taking norms in (4.2), we find that $(\text{Norm} f'(\lambda)) = (P)^t$ where $t = n \cdot \Phi(M) - (\Phi(M)/\Phi(P)) = n \cdot \Phi(M) - q^{d(n-1)}$.

Now let $D_P$ be the different of $k(\Lambda_M)_{P}/k_P$. Then $D_P = \mathfrak{P} = (\lambda)^t$ for some $t$. Since $D = \text{Norm}(D_P) = (\text{Norm} \lambda)^t = (P)^t$, we see on comparing exponents that $t = s$. This completes the proof.

Corollary 4.2. Let $g_M$ denote the genus of $k(\Lambda_M)/k$. Then

$$2g_M - 2 = (dq^n - dn - q)(\Phi(M)/(q - 1)) - dq^{d(n-1)}.$$

Proof. By the Hurwitz formula,

$$2g_M - 2 = -2 \cdot \Phi(M) + \deg(D).$$

The degree of $D$ is easily calculated from (4.1) and is found to yield the result.
5. The extension $A/k$. Our aim now is to show how the theory developed in §§1-4 can be used to construct the maximal abelian extension $A$ of $k$ and the reciprocity law homomorphism $\psi: J \to \text{Gal}(A/k)$ from the group of $k$-idèles $J$ into the Galois group of $A/k$. These constructions will be “explicit” in the sense that:

(a) $A/k$ is the composite of certain of its finite subextensions, each one of which is generated by the roots of a polynomial which we can write down, and

(b) the action of an element of $J$ via $\psi$ on the roots of one of these polynomials is given by another polynomial which also we can write down.

In constructing $A$ and $\psi$, we proceed in an elementary fashion using only basic algebraic number theory. But in order to show that our construction does in fact yield the maximal abelian extension of $k$ and the reciprocity law homomorphism, we must appeal to class field theory in the end. One can make shorter proofs if he is willing to introduce the class field theory at an earlier stage in the constructions.

We begin by constructing $A$ as the composite of three pairwise linearly disjoint extensions $E/k$, $K_T/k$ and $L_\infty/k$. These extensions are defined (as subfields of $k^{ae}$) as follows:

(i) $E/k$ is the union of all the “constant field extensions” of $k$. In other words, $E$ is gotten by adjoining to $k$ all roots of the polynomials $u^\nu - u$ for $\nu = 1, 2, 3, \ldots$. The Galois group $G_E$ of $E/k$ is the projective limit of all the finite cyclic groups and is therefore isomorphic to the completion of $\mathbb{Z}$ in its ideal topology. It is generated as a topological group by the unique automorphism $\text{Frob}$ of $E/k$ whose restriction to the algebraic closure of $F_q$ in $E$ is the Frobenius automorphism $u \mapsto u^q$.

(ii) $K_T/k$ is the union of all the fields $k(\Lambda_M)$ for all polynomials $M$ in $R_T$. Thus, $K_T$ is gotten by adjoining to $k$ all roots of the polynomials $u^M, M$ in $R_T$. By Theorem 2.3, the Galois group $G_T$ of $K_T/k$ is the projective limit of the multiplicative groups $(R_T/(M))^\times$, and $G_T$ acts on $K_T$ via its quotient groups $(R_T/(M))^\times$ as described in §2.

The composite $E \cdot K_T$ in $k^{ae}$ cannot be the maximal abelian extension of $k$ since by Theorem 3.1 it contains no finite subextension in which $P_\nu$ is wildly ramified. That part of the maximal abelian extension of $k$ in which $P_\nu$ is wildly ramified can be constructed by using $\sqrt{\beta}$ instead of $T$ as our generator for $k$.

(iii) Viewing the theory in §1 for $1/T$ as the generator instead of $T$, put $F_\nu = k(\Lambda_{T^{\nu-1}})$ for $\nu = 1, 2, 3, \ldots$. Let $\lambda$ be a generator of the $R_{1/T}$ module $\Lambda_{T^{\nu-1}}$. Any polynomial $N$ in $1/T$ over $F_\nu$ with nonzero constant term acts on $F_\nu$ by way of the automorphism which takes $\lambda$ to $\lambda^N$. In particular, we can identify $F_q^\times$ with the group of automorphisms $\tau_\beta$ ($\beta \in F_q^\times$) which take $\lambda$ to $\lambda^\beta = \beta \lambda$. Let $L_{\nu}$ be the fixed field of $F_q^\times$ in $F_\nu$. Since $[F_\nu: k] = q^{\nu}(q - 1)$ and $[F_\nu: L_{\nu}] = q - 1$, the extension $L_{\nu}/k$ is Galois of degree $q^{\nu}$. By Proposition 2.2, $E_\infty = 1/T$ is totally ramified in $F_{\infty}/k$ and hence totally and wildly ramified in $L_\infty/k$. It is clear that
$L_r \subset L_{r+1}$. We put $L_\infty = \bigcup_{r=1}^{\infty} L_r$. Since the Galois group of $L_r/k$ is naturally identified with the group $G_r$ of polynomials in $1/T \bmod (1/T)^{r+1}$ which have constant term $1$, the Galois group $G_\infty$ of $L_\infty/k$ is the projective limit of these groups. In other words, $G_\infty$ is the multiplicative group in the ring of formal power series $\mathbb{F}_\ell[[1/T]]$ consisting of those power series with constant term $1$. And $G_\infty$ acts on $L_\infty/k$ via its quotients $\bmod (1/T)^{r+1}$.

Definition 5.1. Put $A = E \cdot K_T \cdot L_\infty$, where the composite is taken inside the fixed algebraic closure $k_{\text{ac}}$ of $k$.

Proposition 5.2. The extensions $E/k$ and $K_T/k$ are linearly disjoint, and their composite $E \cdot K_T/k$ is linearly disjoint from $L_\infty/k$. Therefore, the Galois group of $A/k$ is naturally isomorphic with the product $G_E \times G_T \times G_\infty$.

Proof. Any finite subextension of $E \cdot K_T/k$ is tamely ramified at $P_\infty$ because it is contained in the composite of a finite constant field extension of $k$ and some $k(A_M)$. And each $L_r$ is totally ramified at $P_\infty$ with ramification number $p_r$. Therefore, $(E \cdot K_T) \cap L_r = k$, which implies that $E \cdot K_T/k$ and $L_\infty/k$ are linearly disjoint. This leaves $E/k$ and $K_T/k$. To prove these two extensions linearly disjoint, it suffices to show that $k(A_M) \cap E = k$ for every polynomial $M$ in $K_T$. We use induction on the degree of $M$. For $\deg M = 0$, the result is clear. Assume it true for all polynomials $M'$ of degree strictly less than $\deg M$ and put $M = P \cdot M'$, $P \nmid M'$, where $P$ is some monic irreducible dividing $M$. Then we have the tower $k \subset k(\Lambda_{M'}) \subset k(\Lambda_M)$. By hypothesis, $k(\Lambda_{M'}) \cap E = k$. Therefore, if $k(\Lambda_M) \cap E \neq k$, then $k(\Lambda_M)/k(\Lambda_{M'})$ must contain a constant field extension. But any extension of the prime divisor $P$ of $k$ is totally ramified in $k(\Lambda_M)/k(\Lambda_{M'})$. Therefore, we must have $k(\Lambda_M) \cap E = k$, and the proof is complete.

6. The homomorphism $\psi$. Having introduced the field $A$, our next task is to construct the group homomorphism $\psi : J \to \text{Gal}(A/k)$. This we do by writing $J$ as a direct product of four of its subgroups and then building $\psi$ on each factor separately. The map $\psi$ is trivial on one factor and on the other three factors maps into the Galois groups of $E/k$, $K_T/k$ and $L_\infty/k$ respectively. Before describing this decomposition of $J$, it is convenient to introduce some notational conventions.
Given a prime divisor \( \nu \) of \( k \), the completion of \( k \) at \( \nu \) is denoted by \( k_{\nu} \). The valuation ring of \( k_{\nu} \) is denoted by \( o_{\nu} \), and the maximal ideal and group of units of \( o_{\nu} \) are denoted by \( p_{\nu} \) and \( U_{\nu} \) respectively. Our choice of the generator \( T \) of \( k \) yields a canonical uniformizer \( \pi_{\nu} \) in \( o_{\nu} \) defined by

(a) \( \pi_{\nu} = P \) if \( \nu \neq P_{\infty} \), where \( P \) is the unique monic irreducible in \( R_{T} \) such that \( \text{ord}_{\nu}(P) = 1 \), and
(b) \( \pi_{\nu} = 1/T \) if \( \nu = P_{\infty} \).

This uniformizer having been chosen, every element \( x \in k_{\nu}^* \) can be written in the form

\[
(6.1) \quad x = \nu^{r} \pi_{\nu}^{s} 
\]

for suitable \( u \in U_{\nu} \) and \( v \in \mathbb{Z} \) which are uniquely determined. We put \( \text{sgn}_{\nu}(x) = u \), where \( u \) is the canonical image of \( u \) in the residue class field of \( o_{\nu} \). Clearly, \( \text{sgn}_{\nu} \) is a multiplicative homomorphism from \( k_{\nu}^* \) onto \( (o_{\nu}/\nu)^* \). We identify \( \alpha \in F_{\nu}^* \subset k_{\nu} \) with \( \text{sgn}_{\nu}(\alpha) \). Further, let \( V_{\nu} = \text{Ker}(\text{sgn}_{\nu}) \) and \( k_{\nu}^{(1)} = V_{\nu} \cap U_{\nu} \).

Since \( k_{\nu}^{(1)} \) is open in \( V_{\nu} \) (as \( U_{\nu} \) is open in \( k_{\nu} \)), (6.1) shows that \( V_{\nu} \) is isomorphic as a topological group with \( k_{\nu}^{(1)} \times \mathbb{Z} \).

Now suppose \( \mathfrak{l} \) is an idèle in \( J \). Define “divisors” \( \partial(\mathfrak{l}) \) and \( d_{T}(\mathfrak{l}) \) for \( \mathfrak{l} \) as follows:

\[
(6.2) \quad \partial(\mathfrak{l}) = \prod_{\nu} \nu^{\text{ord}_{\nu}(\mathfrak{l})} \quad \text{(all primes of } k) 
\]

is the usual divisor, which is an element of the divisor group \( \mathbb{D}_{k} \) of \( k \); and

\[
(6.3) \quad d_{T}(\mathfrak{l}) = \text{sgn}_{\infty}(\mathfrak{l}_{\infty}) \cdot \prod_{P \neq P_{\infty}} \pi_{P}^{\text{ord}_{P}(\mathfrak{l}_{P})} 
\]

which is an element of \( k^* \). One sees immediately that \( \partial \) and \( d_{T} \) are epimorphisms from \( J \) onto the groups \( \mathbb{D}_{k} \) and \( k^* \) respectively.

Finally, we define some subgroups of \( J \): (A) \( k^* \) sitting as a discrete subgroup of \( J \) along the diagonal; (B) \( V_{\infty} = k_{\infty}^{(1)} \times \mathbb{Z} \) sitting inside \( k_{\infty}^* \), which is identified as the group of idèles having \( 1 \) at every coordinate except the \( P_{\infty} \) coordinate; (C) the subgroup \( \cup_{T} \) consisting of the idèles which have \( 1 \) in the \( P_{\infty} \) coordinate and a \( P^{-} \) unit in the \( P \) coordinate for every \( P \neq P_{\infty} \). From the definition of the \( J \) topology, \( k_{\infty}^* \) inherits its usual topology from \( J \) under the identification in (B), and

\[
(6.4) \quad \cup_{T} \cong \prod_{P \neq P_{\infty}} U_{P} 
\]

as a topological group.

We are now in a position to describe the decomposition of \( J \). Given an idèle \( \mathfrak{l} \), write

\[
(6.5) \quad \mathfrak{l} = d_{T}(\mathfrak{l}) \cdot \mathfrak{l}^* \quad (\mathfrak{l}^* \in \cup_{T} \times V_{\infty}) 
\]
where \( d_T(l) \) is a diagonal idèle as described in (A) above. By (6.1), the decomposition (6.5) is the only way of writing \( l \) as a product of an element of \( k^* \) and an element of \( U_T \times V^\infty \). Therefore, \( J \) is the direct product \( k^* \times U_T \times V^\infty \) as a group; and since \( U_T \times V^\infty \) is an open subgroup of \( J \), \( J \) is even isomorphic to this direct product as a topological group. Finally, since \( V^\infty = k^{(1)}_\infty \times \mathbb{Z} \), we get

\begin{equation}
J \cong k^* \times \bigcup_T k^{(1)}_\infty \times \mathbb{Z}
\end{equation}

both algebraically and topologically. For given \( l \in J \), we write \( l \) as the product

\begin{equation}
l = d_T(l) \cdot l_T \cdot l_\infty \cdot l_\mathbb{Z}
\end{equation}

given by the decomposition (6.6).

The group \( U_T \) is actually isomorphic to the Galois group \( G_T \) of \( K_T/k \) in a natural way. In fact, we can give a constructive definition of the natural action of \( U_T \) on \( K_T \) which identifies \( U_T \) with \( G_T \). Suppose given an idèle \( l \) in \( U_T \) and a monic polynomial \( M \) in \( R_T \). We will describe how \( l \) acts on \( k(\Lambda M)/k \). Suppose \( M = \prod P^n \) is the canonical factorization of \( M \). By the Chinese remainder theorem, there is a polynomial \( A \) in \( R_T \) such that \( A \equiv 1 \pmod{P^n} \) for every \( P \) dividing \( M \), and this polynomial is unique \( \pmod{M} \). From the discussion in §2, this \( A \pmod{M} \) determines a unique automorphism \( \tau_\lambda \) of \( k(\Lambda M)/k \) which takes \( \lambda = \Lambda M \) to \( \lambda^4 \). We get a homomorphism \( \psi_M^\mathfrak{F} : U_T \rightarrow \text{Gal}(k(\Lambda M)/k) \) defined by \( \psi_M^\mathfrak{F}(l) = \tau_\lambda \). The reader can verify for himself that \( \psi_M^\mathfrak{F} \) is continuous (discrete topology on the finite group) and that \( M \mid N \) implies that the restriction of \( \psi_M^\mathfrak{F} \) to \( k(\Lambda M) \) is just \( \psi_M^\mathfrak{F} \). Taking the limit, one gets a continuous homomorphism \( \psi_T : U_T \rightarrow G_T \). This \( \psi_T \) is easily seen to be injective and to have an image which is dense in \( G_T \). Therefore, since \( U_T \) is compact, \( \psi_T \) is an isomorphism.

We have already noted in (iii) of §5 that the Galois group \( G_\infty \) of \( L_\infty/k \) is isomorphic to \( k^{(1)}_\infty \) and indicated how \( k^{(1)}_\infty \) acts on \( L_\infty \) via its quotients. Let \( \psi_\infty : k^{(1)}_\infty \rightarrow G_\infty \) be this isomorphism.

Finally, we define a monomorphism \( \psi_Z : \mathbb{Z} \rightarrow G_E \) into the Galois group of \( E/k \) by requiring that \( \psi_Z(1) = \text{Frob} \). This \( \psi_Z \) is certainly continuous since \( \mathbb{Z} \) has the discrete topology.

We can now define our homomorphism \( \psi : J \rightarrow \text{Gal}(A/k) \). Recall that \( \text{Gal}(A/k) = G_T \times G_\infty \times G_E \) by Proposition 5.2. Given \( l \in J \), we write \( l \) in the form (6.7) and then put

\begin{equation}
\psi(l) = \psi_T(l_T^{-1}) \cdot \psi_\infty(l_\infty^{-1}) \cdot \psi_Z(l_\mathbb{Z}).
\end{equation}

Our preceding remarks yield the following

**Theorem 6.1.** The map \( \psi \) defined by (6.8) is a continuous homomorphism from \( J \) into the Galois group of \( A/k \) with kernel \( k^* \).

We show in the next section that \( \psi \) is in fact the reciprocity law homomorphism for \( k \).
7. **ψ is the reciprocity law homomorphism.** Let \( A^*/k \) be the maximal abelian extension of \( k \), and let \( \psi^*: J \to A^* \) be the reciprocity law homomorphism. Since \( A/k \) is abelian, \( A \subseteq A^* \) and so one has the restriction homomorphism \( \text{res}: \text{Gal}(A^*/k) \to \text{Gal}(A/k) \). We will show that \( \text{res} \circ \psi^* = \psi \). Since both \( \psi \) and \( \psi^* \) have kernel \( k^* \), this will show that \( A = A^* \), and hence \( \psi = \psi^* \), by Galois theory. Now, in order to prove that \( \text{res} \circ \psi^* = \psi \), it suffices to prove for every idèle \( i \) in \( J \) that \( \psi^*(i) \) and \( \psi(i) \) restrict to the same automorphism on each finite subextension of \( A/k \). In fact, it is enough to show that \( \psi(i) \) and \( \psi^*(i) \) agree on the subextensions of \( A/k \) of the form:

(i) constant field extensions,

(ii) \( k(\Lambda_M)/k \) where \( M = P^n \) is a power of a monic irreducible in \( R_T \),

(iii) \( L_{k(r)}/k \) for \( r \geq 1 \).

Indeed, from our previous work it follows that every finite subextension of \( A/k \) is contained in a composite of subextensions of the above three types.

Suppose then that \( F/k \) is a finite extension of type (i), (ii), or (iii) above. The restriction of \( \psi^*(i) \) from \( \text{Gal}(A^*/k) \) to \( \text{Gal}(F/k) \) induces a homomorphism from \( J \) to \( \text{Gal}(F/k) \) which, by abuse of language, we also denote by \( \psi^* \). From class field theory, one has the following characterization of this \( \psi^* \) (see [4, Chapter 7, §4]):

Let \( S \) be any finite set of primes of \( k \) which contains at least all those primes which ramify in \( F/k \), and let \( J^S \) denote the group of idèles which have a 1 in the \( v \) coordinate for \( v \in S \). Then \( \psi^* \) is the unique homomorphism \( J \to \text{Gal}(F/k) \) such that

(a) \( \psi^* \) is continuous.

(b) \( \psi^*(k) = 1 \).

(c) \( \psi^*(i) = (\delta(i), F/k) \) for all \( i \in J^S \), where \( (\ , F/k) \) is the Artin symbol.

Therefore, if we check that \( \psi \) satisfies conditions (a), (b) and (c) on all such extensions, then we will be done. We already know that \( \psi \) satisfies (a) and (b), so we have only to look at (c). Call an idèle \( i \in J \) a \( v \)-blip if it has a unit in each coordinate except \( v \) and if its \( v \) coordinate is \( \pi_v \). Since every idèle in \( J^S \) can be written as the finite product of \( v \)-blips and inverses of \( v \)-blips for various \( v \) not in \( S \) (clear!), it suffices to check (c) for \( i \) a \( v \)-blip. This we now proceed to do.

**Case 1.** \( F/k \) is a finite constant field extension. No prime ramifies, but for convenience we take \( S = \{\pi_v\} \). Let \( i \) be a \( v \)-blip for \( v = P \neq \pi_v \). Then \( \delta(i) = v \), and one easily checks that \( (v, F/k) = (\text{Frob})^{\deg p} \) on \( F/k \). On the other hand, the \( \pi_v \) coordinate of \( i \cdot d_T(i)^{-1} \) is \( P^{-1} \), and \( \text{ord}_v(P^{-1}) = \deg P = \deg v \). Therefore, \( i_\pi = \deg v \) and hence \( \psi(i) = \psi_z(i) = (\text{Frob})^{\deg p} \) on \( F/k \) by definition. Thus, \( \psi \) satisfies (c) in this case.

**Case 2.** \( F/k \) is \( k(\Lambda_M)/k \) for \( M = P^n \). We know by Proposition 2.2 that only \( P \) and \( \pi_v \) can ramify. Therefore, take \( S = \{P, \pi_v\} \). Suppose that \( i \in J^S \) is a \( v \)-blip for \( v = Q \), a finite prime different from \( P \). Then since \( d_T(i) = Q \), the \( P \) coordinate of \( i \) is \( Q^{-1} \). Since \( i \) acts on \( k(\Lambda_M/k) \) via its \( P \) coordinate, we see that
\(\psi(i) = \psi_T(i_{T^{-1}})\) on \(k(\Lambda_M)\) is the automorphism which maps \(\lambda\) to \(\lambda^q\) for every \(\lambda \in \Lambda_M\). But, according to Corollary 2.5, this automorphism is the Artin symbol at \(Q = \sigma(i)\).

**Case 3.** \(F/k\) is \(L_\nu/k\) for some \(\nu \geq 1\). We take \(S = \{T, P_\nu\}\) since only these primes can ramify. Let \(i\) be a \(\nu\)-blip in \(F^S\) where \(\nu = P\), a finite prime different from \(T\). The \(P_\nu\) coordinate of \(i \cdot d_T(i)^{-1}\) is \(P^{-1} = (P^{-1}T^d)(1/T)^d\), where \(d = \deg P\), and \(P^{-1}T^d\) is a unit at \(P_\nu\). Therefore, \(i_{\nu} = P^{-1}T^d\) and \(i_{P_\nu}^{-1} = P/T^d\). Now \(P/T^d = \alpha P\) where \(\alpha \neq 0\) is the constant coefficient of \(P\) and \(P\) is a monic polynomial in \(1/T\) gotten by reversing the coefficients of \(\alpha^{-1}P\). Since \(\text{ord}_P P = \text{ord}_P(P/T^d) = \text{ord}_P P = 1\), we see that \(P\) is the canonical uniformizer at \(\nu\) for the theory with \(1/T\) for the generator of \(k\). By definition, the automorphism \(\psi(i) = \psi_T(i_{\nu}^{-1})\) on \(L_\nu/R\) is the restriction of the automorphism of \(F_\nu = k(\Lambda_{T^{-1}})\) which carries \(\lambda \in \Lambda_{T^{-1}}\) to \(\lambda^q\). But the restriction of this automorphism to \(L_\nu\) is the same as the restriction of the automorphism which takes \(\lambda\) to \(\lambda^q\), because the automorphism of \(F_\nu\) associated to \(\alpha \in F_\nu^*\) fixes \(L_\nu\). Now the automorphism taking \(\lambda \rightarrow \lambda^q\) is the Artin symbol in \(F_\nu\) at \(\nu\) by Corollary 2.5, and therefore its restriction to \(L_\nu\) is the Artin symbol in \(L_\nu\) at \(\nu\).

We have now proved the following

**Theorem 7.1.** The extension \(A/k\) constructed in §5 is the maximal abelian extension of \(k\), and the homomorphism \(\psi: J \rightarrow \text{Gal}(A/k)\) constructed in §6 is the reciprocity law homomorphism.

In particular, we see that \(A\) and \(\psi\) do not depend upon our original choice of the generator \(T\).

We can also use Theorem 7.1 to give another characterization of \(A\).

**Theorem 7.2.** The maximal abelian extension of \(k\) is the composite \(K_T \cdot K_{1/T}\).

**Proof.** From the explicit construction of \(\psi\), one sees easily that the group of idèles fixing \(K_T\) (resp. \(K_{1/T}\)) is \(k_* \cdot k_\infty\) (resp. \(k_* \cdot k_T\)), where the completions \(k_T\) and \(k_\infty\) are identified with subgroups of \(J\) in the usual way. Since the intersection of these two subgroups is \(k_*\), we are done.

**References**

1. E. Artin and J. Tate, *Class field theory*, Notes Distributed by the Department of Mathematics, Harvard University, Cambridge, Mass.

**Department of Mathematics, University of Massachusetts, Amherst, Massachusetts 01002**