TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 189, 1974

EXPLICIT CLASS FIELD THEORY FOR RATIONAL FUNCTION FIELDS(1)

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 $\mathbf{F}_q$ (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 $\mathbf{Q}$ is "explicit" in the sense that one can write down a sequence of polynomials whose roots generate the maximal abelian extension of $\mathbf{Q}$, and one can describe concretely how a given $\mathbf{Q}$-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 $\mathbf{Q}$ by adjoining the torsion points of $\mathbf{Z}$ 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 $\mathbf{F}_q$ of q elements. Of the $q^3 - q$ generators of k over $\mathbf{F}_q$ pick one, say T, and consider the polynomial subring $R_T = \mathbf{F}_q[T]$ of k. Carlitz makes R_T act as a ring of endomorphisms on the additive group of k^{ac}, the algebraic closure of k. For $M \in R_T$, the action of M is given by a separable polynomial

---

Received by the editors March 10, 1972.

AMS (MOS) subject classifications (1970). Primary 12A65, 12A35.

Key words and phrases. Rational function field over a finite field, explicit class field theory, cyclotomic extensions.

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

with coefficients in R_T whose set of roots Λ_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 $\mathbf{Q}$.

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_∞ of T. In a previous paper [3], he had defined an analytic function $\psi(u)$ on k_∞, the completion of k at P_∞, 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 ω_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 ω_M and, therefore, of the R_T action. He noted also that the roots of ω_M are expressible in the form $\psi((A/M)\xi)$ where ξ is a "transcendental element" lying in the completion of the algebraic closure of k_∞ and A is in R_T. Thus, the elements of Λ_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 $\mathbf{Q}$. 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_∞ 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 $\mathbf{Q}$ (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_∞ 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 $\mathbf{F}_q$.

1. The R_T action. As above, k is the field of rational functions over the finite field $\mathbf{F}_q$ of q elements. We arbitrarily choose a generator T of k and put $R_T = \mathbf{F}_q[T]$, the polynomial subring of k generated by T over $\mathbf{F}_q$. 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 $\mathbf{F}_q$-algebra $\mathrm{End}(k^{ac})$ of all $\mathbf{F}_q$-endomorphisms of the additive group of k^{ac} contains the Frobenius automorphism φ defined by $\varphi(u) = u^q$ and the map μ_T defined by $\mu_T(u) = Tu$. Since R_T is a polynomial ring over $\mathbf{F}_q$, the substitution $T \mapsto \varphi + \mu_T$ yields a ring homomorphism $R_T \to \mathrm{End}(k^{ac})$ 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

$$u^M = M(\varphi + \mu_T)(u). \tag{1.1}$$

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

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

$$u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} \cdot u^{q^i} \tag{1.2}$$

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

Proof. Since each element of R_T is an $\mathbf{F}_q$-linear combination of powers of T, it suffices to verify the proposition for the special case $M = T^d$. The endomorphisms φ and μ_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 $\mu_T^s \circ \varphi^i$. Since $(\mu_T^s \circ \varphi^i)u = T^s u^{q^i}$, we see that u^M is indeed a polynomial in u of the form (1.2). For $i = d$, there is a unique term φ^d and $\varphi^d(u) = u^{q^d}$. For $i = 0$, there is a unique term μ_T^d and $\mu_T^d(u) = T^d u$. For $0 < i < d$, there is a unique term with maximum s, namely $\varphi^i \circ \mu_T^{d-i} = \mu_T^{(d-i)q^i} \circ \varphi^i$. This completes the proof.

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

(a) $$\begin{bmatrix} \alpha M + \beta N \\ i \end{bmatrix} = \alpha \cdot \begin{bmatrix} M \\ i \end{bmatrix} + \beta \cdot \begin{bmatrix} N \\ i \end{bmatrix} \quad \text{for } \alpha, \beta \in \mathbf{F}_q.$$

(b) $$\begin{bmatrix} T^{d+1} \\ i \end{bmatrix} = T \cdot \begin{bmatrix} T^d \\ i \end{bmatrix} + \begin{bmatrix} T^d \\ i-1 \end{bmatrix}^q.$$

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

Definition 1.2. Let Λ_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, Λ_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 Λ_M is finite of order q^d and is therefore a vector space over $\mathbf{F}_q$ 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 $\left[{M \atop 0}\right] = M$. The proposition follows immediately.

The structure of the R_T-module Λ_M will now be determined. As one might expect from the analogous cyclotomic theory, Λ_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*

$$\Lambda_M = \sum_{P|M} \Lambda_{P^n}, \tag{1.3}$$

and the sum is direct.

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

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

Proof. Let $d = \deg P$. The proof goes by induction on n. For $n = 1$, Λ_P is a vector space over $R_T/(P)$. Since both $R_T/(P)$ and Λ_P contain q^d elements, Λ_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 Λ_{P^k} is cyclic by the induction hypothesis, one can therefore choose $\lambda \in \Lambda_{P^{k+1}}$ so that λ^P generates Λ_{P^k}. This λ 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 Λ_P. Now $\lambda^{P^k} \in \Lambda_P$ is not zero since λ^P generates Λ_{P^k}. Therefore, since Λ_P is a 1-dimensional vector space over $R_T/(P)$, there is a $B \in R_T$ such that $\mu - \lambda^A = \lambda^{P^k B}$. We conclude that $\mu = \lambda^{A+P^k B}$. Therefore, λ generates $\Lambda_{P^{k+1}}$, and the proof is complete.

Theorem 1.6. *The R_T-module Λ_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 Λ_M is cyclic, Λ_M is itself cyclic. Therefore, Λ_M is naturally isomorphic to the quotient of R_T by the annihilator ideal of Λ_M. Clearly, the ideal (M) is contained in that annihilator. On the other hand, both Λ_M and $R_T/(M)$ have q^d elements, where $d = \deg M$. Therefore, (M) must equal the annihilator of Λ_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 $R_T/(M)$.

Corollary 1.8. *The cyclic R_T-module Λ_M has exactly $\Phi(M)$ generators. In fact, if λ is a given generator and $A \in R_T$, then λ^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_∞ 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 Λ_M. Let λ be a generator of Λ_M over R_T (Theorem 1.6). Since λ^A is a polynomial in λ 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 Λ_M. Also, since Λ_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 Λ_M are all integral over R_T since by Proposition 1.1 the leading coefficient of u^M belongs to $\mathbf{F}_q$.

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 λ of Λ_M. Since λ also generates the field extension, every $\sigma \in G_M$ is determined by its action on λ. We must have $\sigma(\lambda) = \lambda^A$ for some A relatively prime to M since σ must map a generator of Λ_M to another generator. Further, this A does not depend on the choice of the generator λ. 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_∞ 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 λ be a generator of Λ_M. Then $R_T[\lambda]$ is a subring of I_M, and its discriminant $D(\lambda)$ divides the divisor of $\mathrm{Norm}(f'(\lambda))$ where

$f(u)$ is any polynomial over R_T which has λ 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_∞, 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 $u^{P^n} = (u^{P^{n-1}})^P = u^{P^{n-1}} \cdot f(u)$ 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 Λ_M. Therefore,

$$\pm P = \prod_A \lambda^A \tag{2.1}$$

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

$$\pm P = (\text{unit}) \cdot \lambda^{\Phi(M)}. \tag{2.2}$$

The ramification number e_P of P is therefore greater than $\Phi(M)$. But also $e_P \leq [k(\Lambda_M): k] \leq \Phi(M)$. 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 $M = \alpha \prod P^n$, where each P is a monic irreducible, then the total ramification of $k(\Lambda_{P^n})$ at P shows that each extension $k(\Lambda_{P^n})/k$ for P dividing M is linearly disjoint from the composite of the remaining ones. Therefore,

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

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 λ be a generator of Λ_M. From the proof of Proposition 2.2,

$$f(u) = \prod_A (u - \lambda^A) \tag{2.3}$$

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 $\operatorname{ord}_{\mathfrak{p}}\lambda = 1$, and the same holds true of the generator λ^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 φ_P of $k(\Lambda_M)$ which takes λ in Λ_M to λ^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 λ to λ^L for suitable $L \in R_T$. By definition, we have $\lambda^L \equiv \lambda^{q^d}$ (mod $\mathfrak{p}$) where $\mathfrak{p}$ is a prime of $k(\Lambda_M)$ lying over P. But also $\lambda^P \equiv \lambda^{q^d}$ (mod $\mathfrak{p}$) by the above proposition. Now

$$u^M = \prod_{A \bmod M} (u - \lambda^A).$$

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

$$M = \prod_{A \bmod M} (\lambda^B - \lambda^A) \qquad (A \not\equiv B)$$

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

3. **The ramification at P_∞.** The fundamental fact about the ramification at P_∞ in $k(\Lambda_M)/k$ is that it is *tame*:

Theorem 3.1. *Let $M \in R_T$, $M \neq 0$. Then P_∞ 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 P_∞ splits.

Theorem 3.2. *Let $M = P^n$ where P is a monic irreducible in R_T with* $\deg P = d$. *Then P_∞ splits into $\Phi(M)/(q-1)$ prime divisors in $k(\Lambda_M)$. The ramification number e_∞ 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 P_∞. 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 P_∞). Schematically, we have

$$k \rightarrow k(\Lambda_P) \rightarrow k(\Lambda_M),$$

$$P_\infty \leftarrow \mathfrak{p} \leftarrow \mathfrak{P}.$$

I show first that $e_\mathfrak{p} = q - 1$ and $f_\mathfrak{p} = 1$ 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_∞. 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, $g(u) = h(u^{q-1})$ 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_∞ be the completion of k at P_∞, and let v_∞ be the normalized valuation on k_∞. Then $v_\infty(f_i(T)) = -\deg f_i(T) = -(d-i)q^i$. To get the Newton polygon of $h(u)$ over k_∞, one plots the points $\beta_i = ((q^i-1)/(q-1), -(d-1)q^i)$ for $0 \leq i \leq d$. A short calculation shows that the slope of the line segment joining β_i and β_{i+1} is just $-(d-i)(q-1)+q$. Since the slopes increase strictly with i, the points β_i must be exactly the vertices of the Newton polygon of $h(u)$. For the points β_0 and β_1, we find the slope $-d(q-1)+q$, which shows that $h(u)$ has a root θ in k_∞ with $v_\infty(\theta) = d(q-1)-q$. Now because $g(u) = h(u^{q-1})$, the completion $k(\Lambda_P)_\mathfrak{p}$ of $k(\Lambda_P)$ at $\mathfrak{p}$ is gotten from k_∞ by adjoining a root λ of $u^{q-1} - \theta = 0$. Therefore, since $v_\infty(\theta)$ and $q-1$ are relatively prime, the extension $k(\Lambda_P)_\mathfrak{p}/k_\infty$ is totally ramified of degree $q-1$. Hence, $e_\mathfrak{p} = q-1$ and $f_\mathfrak{p} = 1$.

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 λ such that $v_\mathfrak{p}(\lambda) = d(q-1)-q$. Now as $u^P = u \cdot g(u)$,

$$u^M = u^{P^n} = (u^{P^{n-1}})^P = u^{P^{n-1}} \cdot g(u^{P^{n-1}})$$

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

$$\gamma_{-1} = (0, v_\mathfrak{p}(\lambda)) = (0, d(q-1)-q)$$

and

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

for $0 \leq i \leq d(n-1)$. A short calculation shows that the slope from γ_{-1} to γ_0 is $-(q-1)dn+q$ and that the slope from γ_i to γ_{i+1} for $i \geq 0$ is $-(q-1) \cdot (dn-d-i)+q$. Again, these slopes increase strictly with i so that the vertices of the Newton polygon of $u^{P^{n-1}} - \lambda$ over $k(\Lambda_P)_\mathfrak{p}$ are exactly the γ_i. The segment from γ_{-1} to γ_0 shows that $u^{P^{n-1}} - \lambda$ has a root in $k(\Lambda_P)_{\mathfrak{p}}$. Since the extension is Galois, this means that $\mathfrak{p}$ 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 $\mathfrak{D}$ be the different of the extension $k(\Lambda_M)/k$, where $M = P^n$, P monic, and* $\deg P = d$. *Then*

$$\mathfrak{D} = \mathfrak{P}^s \cdot \prod_{\mathfrak{p} | P_\infty} \mathfrak{p}^{q-2} \tag{4.1}$$

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_∞ are ramified, so only such primes divide $\mathfrak{D}$. Since the ramification at $\mathfrak{p}$ for $\mathfrak{p} \mid P_\infty$ is tame, $\mathfrak{p}$ appears in the different with exponent $e_{\mathfrak{p}} - 1 = q - 2$. Hence, everything is proved except for the value of s.

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

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

and hence

$$P^n = \lambda^{P^{n-1}} \cdot f'(\lambda). \tag{4.2}$$

Since $\lambda^{P^{n-1}} \in \Lambda_P$, the norm of $\lambda^{P^{n-1}}$ is the $\Phi(M)/\Phi(P)$ power of its norm from $k(\Lambda_P)_{\mathfrak{P}}$ to k_P, and this latter norm is just $\pm P$. Therefore, on taking norms in (4.2), we find that $(\mathrm{Norm}\, f'(\lambda)) = (P)^s$ where $s = n \cdot \Phi(M) - (\Phi(M)/\Phi(P)) = n \cdot \Phi(M) - q^{d(n-1)}$.

Now let $\mathfrak{D}_P$ be the different of $k(\Lambda_M)_{\mathfrak{P}}/k_P$. Then $\mathfrak{D}_P = \mathfrak{P}^t = (\lambda)^t$ for some t. Since $D = \mathrm{Norm}(D_P) = (\mathrm{Norm}\, \lambda)^t = (P)^t$, 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*

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

Proof. By the Hurwitz formula,

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

The degree of $\mathfrak{D}$ 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 $\psi: J \to \mathrm{Gal}(A/k)$ 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 ψ on the roots of one of these polynomials is given by another polynomial which also we can write down.

In constructing A and ψ, 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_∞/k. These extensions are defined (as subfields of k^{ac}) 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 $u^{q^\nu} - u$ 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 $\mathbf{Z}$ in its ideal topology. It is generated as a topological group by the unique automorphism **Frob** of E/k whose restriction to the algebraic closure of $\mathbf{F}_q$ 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 $(R_T/(M))^*$, and G_T acts on K_T via its quotient groups $(R_T/(M))^*$ as described in §2.

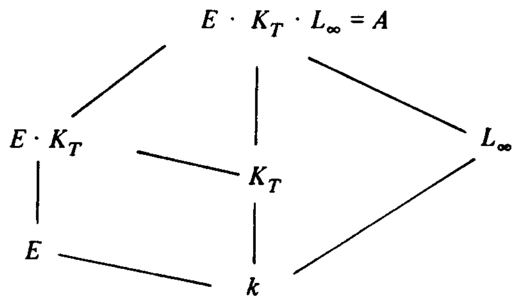
The composite $E \cdot K_T$ in k^{ac} cannot be the maximal abelian extension of k since by Theorem 3.1 it contains no finite subextension in which P_∞ is wildly ramified. That part of the maximal abelian extension of k in which P_∞ is wildly ramified can be constructed by using $1/T$ instead of T as 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 λ be a generator of the $R_{1/T}$ module $\Lambda_{T^{-\nu-1}}$. Any polynomial N in $1/T$ over $\mathbf{F}_q$ with nonzero constant term acts on F_ν by way of the automorphism which takes λ to λ^N. In particular, we can identify $\mathbf{F}_q^*$ with the group of automorphisms τ_β $(\beta \in \mathbf{F}_q^*)$ which take λ to $\lambda^\beta = \beta\lambda$. Let L_ν be the fixed field of $\mathbf{F}_q^*$ in F_ν. Since $[F_\nu : k] = q^\nu(q-1)$ and $[F_\nu : L_\nu] = q - 1$, the extension L_ν/k is Galois of degree q^ν. By Proposition 2.2, $P_\infty = 1/T$ is totally ramified in F_ν/k and hence totally and wildly ramified in L_ν/k. It is clear that

$L_\nu \subset L_{\nu+1}$. We put $L_\infty = \bigcup_{\nu=1}^{\infty} L_\nu$. Since the Galois group of L_ν/k is naturally identified with the group G_ν of polynomials in $1/T \bmod (1/T)^{\nu+1}$ which have constant term 1, the Galois group G_∞ of L_∞/k is the projective limit of these groups. In other words, G_∞ is the multiplicative group in the ring of formal power series $\mathbf{F}_q[[1/T]]$ consisting of those power series with constant term 1. And G_∞ acts on L_∞/k via its quotients $\bmod (1/T)^{\nu+1}$.

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

(5.1)



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_∞/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_∞ because it is contained in the composite of a finite constant field extension of k and some $k(\Lambda_M)$. And each L_ν is totally ramified at P_∞ with ramification number p^ν. Therefore, $(E \cdot K_T) \cap L_\nu = k$, which implies that $E \cdot K_T/k$ and L_∞/k are linearly disjoint. This leaves E/k and K_T/k. To prove these two extensions linearly disjoint, it suffices to show that $k(\Lambda_M) \cap E = k$ for every polynomial M in R_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 $M = P^\nu \cdot M'$, $P \nmid M'$, 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 ψ. Having introduced the field A, our next task is to construct the group homomorphism $\psi: J \to \mathrm{Gal}(A/k)$. This we do by writing J as a direct product of four of its subgroups and then building ψ on each factor separately. The map ψ is trivial on one factor and on the other three factors maps into the Galois groups of E/k, K_T/k and L_∞/k respectively. Before describing this decomposition of J, it is convenient to introduce some notational conventions.

Given a prime divisor $\mathfrak{p}$ of k, the completion of k at $\mathfrak{p}$ is denoted by $k_\mathfrak{p}$. The valuation ring of $k_\mathfrak{p}$ is denoted by $\mathfrak{o}_\mathfrak{p}$, and the maximal ideal and group of units of $\mathfrak{o}_\mathfrak{p}$ are denoted by $\mathfrak{p}$ and $\mathfrak{U}_\mathfrak{p}$ respectively. Our choice of the generator T of k yields a canonical uniformizer $\pi_\mathfrak{p}$ in $\mathfrak{o}_\mathfrak{p}$ defined by

(a) $\pi_\mathfrak{p} = P$ if $\mathfrak{p} \neq P_\infty$, where P is the unique monic irreducible in R_T such that $\mathrm{ord}_\mathfrak{p}(P) = 1$, and

(b) $\pi_\mathfrak{p} = 1/T$ if $\mathfrak{p} = P_\infty$.

This uniformizer having been chosen, every element $x \in k_\mathfrak{p}^*$ can be written in the form

$$x = u\pi_\mathfrak{p}^\nu \tag{6.1}$$

for suitable $u \in \mathfrak{U}_\mathfrak{p}$ and $\nu \in \mathbf{Z}$ which are uniquely determined. We put $\mathrm{sgn}_\mathfrak{p}(x) = \bar{u}$, where $\bar{u}$ is the canonical image of u in the residue class field of $\mathfrak{o}_\mathfrak{p}$. Clearly, $\mathrm{sgn}_\mathfrak{p}$ is a multiplicative homomorphism from $k_\mathfrak{p}^*$ onto $(\mathfrak{o}_\mathfrak{p}/\mathfrak{p})^*$. We identify $\alpha \in \mathbf{F}_q^* \subset k_\mathfrak{p}$ with $\mathrm{sgn}_\mathfrak{p}(\alpha)$. Further, let $V_\mathfrak{p} = \mathrm{Ker}(\mathrm{sgn}_\mathfrak{p})$ and $k_\mathfrak{p}^{(1)} = V_\mathfrak{p} \cap \mathfrak{U}_\mathfrak{p}$. Since $k_\mathfrak{p}^{(1)}$ is open in $V_\mathfrak{p}$ (as $\mathfrak{U}_\mathfrak{p}$ is open in $k_\mathfrak{p}$), (6.1) shows that $V_\mathfrak{p}$ is isomorphic as a *topological* group with $k_\mathfrak{p}^{(1)} \times \mathbf{Z}$.

Now suppose $\mathfrak{i}$ is an idèle in J. Define "divisors" $\partial(\mathfrak{i})$ and $d_T(\mathfrak{i})$ for $\mathfrak{i}$ as follows:

$$\partial(\mathfrak{i}) = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{i}_\mathfrak{p})} \quad \text{(all primes of } k) \tag{6.2}$$

is the usual divisor, which is an element of the divisor group $\mathfrak{D}_k$ of k; and

$$d_T(\mathfrak{i}) = \mathrm{sgn}_\infty(\mathfrak{i}_\infty) \cdot \prod_{P \neq P_\infty} \pi_P^{\mathrm{ord}_P(\mathfrak{i}_P)} \tag{6.3}$$

which is an element of k^*. One sees immediately that ∂ and d_T are *epimorphisms* from J onto the groups $\mathfrak{D}_k$ and k^* respectively.

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

$$\mathrm{U}_T \cong \prod_{P \neq P_\infty} \mathfrak{U}_P \tag{6.4}$$

as a topological group.

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

$$\mathfrak{i} = d_T(\mathfrak{i}) \cdot \mathfrak{i}^* \qquad (\mathfrak{i}^* \in \mathrm{U}_T \times V_\infty) \tag{6.5}$$

where $d_T(\mathfrak{i})$ is a diagonal idèle as described in (A) above. By (6.1), the decomposition (6.5) is the only way of writing $\mathfrak{i}$ as a product of an element of k^* and an element of $\bigcup_T \times V_\infty$. Therefore, J is the direct product $k^* \times \bigcup_T \times V_\infty$ as a group; and since $\bigcup_T \times V_\infty$ is an open subgroup of J, J is even isomorphic to this direct product as a topological group. Finally, since $V_\infty = k_\infty^{(1)} \times \mathbf{Z}$, we get

(6.6) $$J \cong k^* \times \bigcup_T \times k_\infty^{(1)} \times \mathbf{Z}$$

both algebraically and topologically. For given $\mathfrak{i} \in J$, we write $\mathfrak{i}$ as the product

(6.7) $$\mathfrak{i} = d_T(\mathfrak{i}) \cdot \mathfrak{i}_T \cdot \mathfrak{i}_\infty \cdot \mathfrak{i}_{\mathbf{Z}}$$

given by the decomposition (6.6).

The group $\bigcup_T$ 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 $\bigcup_T$ on K_T which identifies $\bigcup_T$ with G_T. Suppose given an idèle $\mathfrak{i}$ in $\bigcup_T$ and a monic polynomial M in R_T. We will describe how $\mathfrak{i}$ 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 $A \equiv \mathfrak{i}_P \pmod{P^n}$ for every P dividing M, and this polynomial is unique mod M. From the discussion in §2, this A mod M determines a unique automorphism τ_A of $k(\Lambda_M)/k$ which takes $\lambda \in \Lambda_M$ to λ^A. We get a homomorphism $\psi_T^M\colon \bigcup_T \to \mathrm{Gal}(k(\Lambda_M)/k)$ defined by $\psi_T^M(\mathfrak{i}) = \tau_A$. The reader can verify for himself that ψ_T^M is continuous (discrete topology on the finite group) and that $M \mid N$ implies that the restriction of ψ_T^N to $k(\Lambda_M)$ is just ψ_T^M. Taking the limit, one gets a continuous homomorphism $\psi_T\colon \bigcup_T \to G_T$. This ψ_T is easily seen to be injective and to have an image which is dense in G_T. Therefore, since $\bigcup_T$ is compact, ψ_T is an isomorphism.

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

Finally, we define a monomorphism $\psi_{\mathbf{Z}}\colon \mathbf{Z} \to G_E$ into the Galois group of E/k by requiring that $\psi_{\mathbf{Z}}(1) = \mathbf{Frob}$. This $\psi_{\mathbf{Z}}$ is certainly continuous since $\mathbf{Z}$ has the discrete topology.

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

(6.8) $$\psi(\mathfrak{i}) = \psi_T(\mathfrak{i}_T^{-1}) \cdot \psi_\infty(\mathfrak{i}_\infty^{-1}) \cdot \psi_{\mathbf{Z}}(\mathfrak{i}_{\mathbf{Z}}).$$

Our preceding remarks yield the following

Theorem 6.1. *The map ψ 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 ψ 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, $A \subset A^*$ and so one has the restriction homomorphism res: $\mathrm{Gal}(A^*/k) \to \mathrm{Gal}(A/k)$. We will show that res $\circ\, \psi^* = \psi$. Since both ψ and ψ^* have kernel k^*, this will show that $A = A^*$, and hence $\psi = \psi^*$, by Galois theory. Now, in order to prove that res $\circ\, \psi^* = \psi$, it suffices to prove for every idèle $\mathfrak{i}$ in J that $\psi^*(\mathfrak{i})$ and $\psi(\mathfrak{i})$ restrict to the same automorphism on each finite subextension of A/k. In fact, it is enough to show that $\psi(\mathfrak{i})$ and $\psi^*(\mathfrak{i})$ 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_ν/k for $\nu \geq 1$.

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 $\psi^*(\mathfrak{i})$ from $\mathrm{Gal}(A^*/k)$ to $\mathrm{Gal}(F/k)$ induces a homomorphism from J to $\mathrm{Gal}(F/k)$ which, by abuse of language, we also denote by ψ^*. From class field theory, one has the following characterization of this ψ^* (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* $\mathfrak{p}$ *coordinate for* $\mathfrak{p} \in S$. *Then ψ^* is the unique homomorphism* $J \to \mathrm{Gal}(F/k)$ *such that*

(a) *ψ^* is continuous.*

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

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

Therefore, if we check that ψ satisfies conditions (a), (b) and (c) on all such extensions, then we will be done. We already know that ψ satisfies (a) and (b), so we have only to look at (c). Call an idèle $\mathfrak{i} \in J$ a $\mathfrak{p}$-*blip* if it has a unit in each coordinate except $\mathfrak{p}$ and if its $\mathfrak{p}$ coordinate is $\pi_\mathfrak{p}$. Since every idèle in J^S can be written as the finite product of $\mathfrak{p}$-*blips* and inverses of $\mathfrak{p}$-blips for various $\mathfrak{p}$ not in S (clear!), it suffices to check (c) for $\mathfrak{i}$ a $\mathfrak{p}$-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 $S = \{P_\infty\}$. Let $\mathfrak{i}$ be a $\mathfrak{p}$-blip for $\mathfrak{p} = P \neq P_\infty$. Then $\partial(\mathfrak{i}) = \mathfrak{p}$, and one easily checks that $(\mathfrak{p}, F/k) = (\mathbf{Frob})^{\deg \mathfrak{p}}$ on F/k. On the other hand, the P_∞ coordinate of $\mathfrak{i} \cdot d_T(\mathfrak{i})^{-1}$ is P^{-1}, and $\mathrm{ord}_\infty(P^{-1}) = \deg P = \deg \mathfrak{p}$. Therefore, $\mathfrak{i}_\mathbf{Z} = \deg \mathfrak{p}$ and hence $\psi(\mathfrak{i}) = \psi_\mathbf{Z}(\mathfrak{i}) = (\mathbf{Frob})^{\deg \mathfrak{p}}$ on F/k by definition. Thus, ψ 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 P_∞ can ramify. Therefore, take $S = \{P, P_\infty\}$. Suppose that $\mathfrak{i} \in J^S$ is a $\mathfrak{p}$-blip for $\mathfrak{p} = Q$, a finite prime different from P. Then since $d_T(\mathfrak{i}) = Q$, the P coordinate of $\mathfrak{i}$ is Q^{-1}. Since $\mathfrak{i}$ acts on $k(\Lambda_M/k)$ via its P coordinate, we see that

$\psi(\mathbf{i}) = \psi_T(\mathbf{i}_T^{-1})$ on $k(\Lambda_M)$ is the automorphism which maps λ to λ^Q for every $\lambda \in \Lambda_M$. But, according to Corollary 2.5, this automorphism is the Artin symbol at $Q = \partial(\mathbf{i})$.

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

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 ψ: $J \to$* Gal(A/k) *constructed in* §6 *is the reciprocity law homomorphism.*

In particular, we see that A and ψ 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 ψ, 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_∞ 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.

2. L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 167–182.

3.———, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.

4. J. W. S. Cassels and A. Frolich (Editors), *Algebraic number theory*, Academic Press, New York, 1967.

5. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387. MR **30** #3094.

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