TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 226, 1977

FUNCTION FIELDS WITH ISOMORPHIC GALOIS GROUPS

BY

ROBERT J. BOND

ABSTRACT. Let K be a local field or a global field of characteristic p. Let G_K be the Galois group of the separable closure of K over K. In the local case we show that G_K, considered as an abstract profinite group, determines the characteristic of K and the number of elements in the residue class field. In the global case we show that G_K determines the number of elements in the constant field of K as well as the zeta function, genus and class number of K. Let K' be another global field of characteristic p and assume we have λ: $G_K \to G_{K'}$, an isomorphism of profinite groups. Then K and K' have the same constant field, zeta function, genus and class number. We also prove that the idele class groups and divisor class groups of K and K' are isomorphic. If E is a finite extension of k, the constant field of K and K', we show that the E-rational points of the Jacobian varieties of K and K' are isomorphic as $G(E/k)$-modules. If $K = K'$ and $\bar{K} = \bar{k}K$ where $\bar{k}$ is the algebraic closure of k, we prove that $\lambda(G_{\bar{K}}) = G_{\bar{K}}$ and the induced automorphism of $G(\bar{K}/K)$ is the identity.

Introduction. Let K be a field and K_s a separable closure of K. Let G_K be the Galois group of K_s over K. Consider the following general question: what information about K is obtained from G_K considered as an abstract profinite group?

In [2], Neukirch considered the case where K is an algebraic number field and obtained some very definitive results. For example, he showed that if K is normal over Q, then G_K determines K completely. More explicitly, if K and K' are finite normal extensions of Q and G_K and $G_{K'}$ are isomorphic algebraically and topologically as profinite groups, then $K = K'$.

In this paper we consider first the case where K is a local field, i.e. a field complete with respect to a discrete rank one valuation with finite residue class field, and second where K is a function field in one variable with finite field of constants.

In the local case, we show that G_K determines the characteristic of K and the number of elements in the residue class field. In the global case, we show that G_K determines the number of elements in the exact field of constants as well as the zeta function, genus and class number of K.

Received by the editors August 5, 1975.

AMS (MOS) subject classifications (1970). Primary 12A55, 12A65; Secondary 14G15.

Key words and phrases. Local field, function field, Galois cohomology groups, zeta function, norm residue symbol, Jacobian variety.

Next we consider two global fields K and K' of char p and assume that their corresponding Galois groups G_K and $G_{K'}$ are isomorphic algebraically and topologically as profinite groups. From the above results we know that K and K' have the same constant field, the same zeta function, genus and class number. We then obtain isomorphisms between certain arithmetic groups associated to K and K'; e.g. their divisor class groups and idele class groups. We also show that the multiplicative groups of nonzero elements of K and K' are isomorphic. We prove that if k is the constant field of K and K', E a finite extension of k, $\mathfrak{J}$ and $\mathfrak{J}'$ the associated Jacobian varieties of K and K', then the groups of E-rational points $\mathfrak{J}(E)$ and $\mathfrak{J}'(E)$ are isomorphic as $G(E/k)$-modules.

Finally, suppose $K = K'$; i.e. we have an automorphism λ: $G_K \to G_K$. If $\bar{K} = \bar{k}K$ where $\bar{k}$ is the algebraic closure of k, then $\lambda(G_{\bar{K}}) = G_{\bar{K}}$. We prove that the induced automorphism of $G(\bar{K}/K)$ is the identity.

I wish to thank my thesis advisor Professor Michael Rosen of Brown University for his advice and encouragement in the preparation of this paper.

1. **Local results.** Let K be a local field and k its residue class field. If char $K = 0$ and char $k = p$, then K is a finite extension of the p-adic rationals Q_p. If K and k both have char p, then K is a field of formal power series in one variable with coefficients in k.

We let K_s be a separable closure of K and let G_K be the Galois group of K_s over K. If A is a discrete G_K-module, $H^q(G_K, A)$ is the qth cohomology group of G_K with coefficients in A.

We now define a group invariant of G_K which will determine the characteristic of K and $|k|$, the number of elements in k.

DEFINITION. Let G be a profinite group and p a prime number. The *p-characteristic of G* is:

$$\chi_p(G) = 1 + \sup_{(n,p)=1} \left\{ \frac{1}{n} \left| H^1(G, Z/nZ) \right| \right\}.$$

Here, Z/nZ is a trivial G-module.

Note that if G is isomorphic to another profinite group G', then $\chi_p(G) = \chi_p(G')$.

THEOREM 1.1. *Let K be a local field and k its residue class field. Assume k has characteristic p. Then $\chi_l(G_K)$ is infinite for all primes $l \neq p$ and $\chi_p(G_K) = |k|$.*

PROOF. Let n be prime to char K. Then $H^1(G_K, Z/nZ)$ is dual to K^*/K^{*n} by local class field theory. In particular, if n is prime to char k, then $|H^1(G_K, Z/nZ)| = n|\mu_n|$ where $|\mu_n|$ is the number of nth roots of unity in K. Since $k^* = k - \{0\}$ is cyclic of order prime to p and K has a primitive nth

root of unity iff k does, $|k^*| = \sup_{(n,p)=1} |\mu_n|$. Hence $\chi_p(G_K) = |k|$.

Let l be a prime $\neq p$. If K has char p and n is divisible by p, it is known that $|H^1(G_K, Z/nZ)| = \infty$ and hence $\chi_l(G_K) = \infty$. If K is a p-adic field, then for any $m \geq 1$,

$$(1/p^m)|H^1(G_K, Z/p^mZ)| = p^{m[K:Q_p]}|\mu_{p^m}|$$

by local class field theory. Therefore,

$$\sup_{m \geq 1} \frac{1}{p^m} |H^1(G_K, Z/p^mZ)| = \infty \quad \text{and} \quad \chi_l(G_K) = \infty.$$

COROLLARY 1.2. *G_K determines the characteristic of K and $|k|$.*

COROLLARY 1.3. *Suppose that K and K' are two local fields with residue class fields k and k' respectively. If G_K and $G_{K'}$ are isomorphic as profinite groups, then K and K' have the same characteristic and $|k| = |k'|$.*

2. **Global results.** In this section, K is a function field in one variable with finite field of constants k, char $k = p$. As before, G_K is the Galois group of K_s over K. We will show that G_K determines $|k|$, the zeta function, genus and class number of K. In [2], Neukirch used a cohomological invariant to associate prime ideals of a number field K_0 with subgroups of G_{K_0}. Following this idea, we use the p-characteristic defined in §1 to recover information about the prime divisors of K. We consider subgroups $G_L \subset G_K$ whose fixed fields L are Hensel fields.

The next result yields a characterization of Hensel fields L from their Galois groups G_L. The proof is almost identical to the proof done by Neukirch in [2, Theorem 1], for the characteristic 0 case. If l is a prime, $\mathrm{cd}_l(G)$ is the lth cohomological dimension of the profinite group G.

PROPOSITION 2.1. *Let F be a global field of* char p *and L a separable extension of F such that G_L is solvable and $\mathrm{cd}_l(G) = 2$ for all primes $l \neq p$. Then there is a unique valuation on L making it a Hensel field.*

DEFINITION. Let G_0 be a profinite group, G a closed subgroup of G_0 and p a prime. We call G an *$S_{p,m}$ group* if G is solvable, $\mathrm{cd}_l(G) = 2$ for all $l \neq p$, $\mathrm{cd}_p(G) = 1$ and $\chi_p(G) = p^m$. We call G a *maximal $S_{p,m}$ subgroup of G_0* if, whenever $G \subset G' \subset G_0$ and G' is an $S_{p,n}$ group for some n, then $G = G'$.

PROPOSITION 2.2. *If L is a separable extension of K, then the following are equivalent*:

(1) *L is a Hensel field with respect to a discrete valuation v whose residue class field has p^m elements. In addition, if $\bar{v}$ is the unique extension of v to K_s, then L is the decomposition field of $\bar{v}$ over K.*

(2) *G_L is a maximal $S_{p,m}$ subgroup of G_K.*

PROOF. Suppose (1) holds. We will denote the restriction of v to K by v also. If K_v is the completion, then $G_L \approx G_{K_v}$ and therefore G_L is an $S_{p,m}$ group by Theorem 1.1 and the well-known properties of the Galois group of a local field. The maximality follows easily from the fact that L is the decomposition field of $\bar{v}$ over K.

Conversely, if G_L is a maximal $S_{p,m}$ subgroup of G_K, by Proposition 2.1, there is a unique valuation v making L a Hensel field. If L' is the decomposition field of $\bar{v}$ over K, then $G_{L'}$ is an $S_{p,n}$ group for some n and thus $L = L'$ by maximality.

We can now associate prime divisors of K with subgroups of G_K. Assume $|k| = p^f$. Let $M_{p,m}(K)$ be the set of all maximal $S_{p,m}$ subgroups of G_K. If $G \in M_{p,m}(K)$, then by Proposition 2.2, $G = G_L$ where L is a Hensel field with respect to a discrete valuation v whose residue class field has p^m elements. Let P be the prime divisor of K associated to the valuation of K lying below v. Since the residue class field k_P has p^m elements, $p^m = p^{fd}$ where d is the degree of P. Thus we have a mapping $\phi_{K,m}$ of $M_{p,m}(K)$ to $\mathfrak{S}_m$, the set of prime divisors of K of degree m/f. Now $\phi_{K,m}$ is onto by Proposition 2.2 and $\phi_{K,m}(G_1) = \phi_{K,m}(G_2)$ iff G_1 and G_2 are conjugate in G_K. So $\phi_{K,m}$ induces a one-to-one and onto map $\overline{\phi_{K,m}}$: $\overline{M_{p,m}(K)} \to \mathfrak{S}_m$ where $\overline{M_{p,m}(K)}$ is the set of conjugacy classes of elements of $M_{p,m}(K)$.

Now let G be a profinite group and p a prime. Consider the set M of all possible finite products $\prod_H \chi_p(H)^{n_H}$ where each H is a maximal $S_{p,m}$ subgroup of G for some m and each n_H is an integer.

Let $\chi^{(p)}(G) = \inf\{n \in M: n \geqslant 2\}$.

THEOREM 2.3. $\chi^{(p)}(G_K) = |k|$.

PROOF. K has a divisor $P_1^{n_1}P_2^{n_2} \cdots P_r^{n_r}$ of degree 1. If $d_i = \deg P_i$, for each $i = 1, 2, \ldots, r$, there is a maximal S_{p,fd_i} subgroup $G_{L_i} \subset G_K$. Since $\chi_p(G_{L_i}) = |k_{P_i}| = p^{fd_i}$, we have $\prod_{i=1}^r \chi_p(G_{L_i})^{n_i} = p^f = |k|$. Hence $\chi^{(p)}(G_K) \leqslant |k|$.

Now consider any finite product $\prod_{i=1}^s \chi_p(H_i)^{m_i}$. Then $\chi_p(H_i) = |k_{\rho_i}|$ where ρ_i is the prime associated to H_i. If $g_i = \deg \rho_i$, we get $\prod_{i=1}^s \chi_p(H_i)^{m_i} = p^{f\sum g_i m_i} = |k|^{\sum g_i m_i}$.

If $\sum g_i m_i \leqslant 0$, then $\prod_{i=1}^s \chi_p(H_i)^{m_i} \leqslant 1$ and if $\sum g_i m_i \geqslant 1$, $\prod_{i=1}^s \chi_p(H_i)^{m_i} \geqslant |k|$. Hence $\chi^{(p)}(G_K) \geqslant |k|$ and the equality follows.

COROLLARY 2.4. *G_K determines the zeta function, genus and class number of K.*

PROOF. If P is a prime divisor of K, $NP = P^{f\deg P} = |k_P|$. Therefore

$$\zeta_K(s) = \prod_P (1 - NP^{-s})^{-1} = \prod_P \left(1 - |k_P|^{-s}\right)^{-1}$$

$$= \prod_H \left(1 - \chi_p(H)^{-s}\right)^{-1}$$

where H runs through a set of representatives of elements of $\overline{M_{p,m}(K)}$. Hence the zeta function is determined by G_K. From well-known properties of the zeta function it follows that G_K also determines the genus and class number of K.

Suppose now that we have two global fields K and K' of char p. We can now give some relationships between K and K' under the assumption that G_K and $G_{K'}$ are isomorphic as profinite groups.

Recall that K can be realized as the field of k-rational functions on a complete nonsingular curve Γ defined over k. The Jacobian $\mathcal{J}$ of Γ is an abelian variety defined over k of dimension g = genus of k. We also have Γ' and $\mathcal{J}'$ associated to K'.

THEOREM 2.5. *If G_K and $G_{K'}$ are isomorphic as profinite groups, then:*

(1) *K and K' have the same constant field, the same zeta function, genus and class number.*

(2) *K is a rational function field if and only if K' is.*

(3) *$\mathcal{J}$ and $\mathcal{J}'$ are isogenous. In particular, if $g = 1$, Γ and Γ' are isogenous elliptic curves.*

(4) *If $g > 1$ and $K' \subset K$, then $K' = K$.*

(5) *If $g = 1$, there are monomorphisms $\alpha\colon K \to K'$ and $\beta\colon K' \to K$ such that K' is unramified over $\alpha(K)$ and K is unramified over $\beta(K')$.*

PROOF. (1) follows immediately from Theorem 2.3 and Corollary 2.4. To see (2) note that K is a rational function field iff $g = 0$ and K has a prime divisor of degree 1. $\mathcal{J}$ and $\mathcal{J}'$ are abelian varieties with the same zeta function since K and K' have the same zeta function. A theorem of Tate, [5], then implies (3).

To prove (4), we use the Riemann-Hurwitz genus formula which says that $2g - 2 = [K\colon K'](2g - 2) + D$ where D is the degree of the different divisor of K over K'. Since $D \geqslant 0$ and $g > 1$, we have $[K\colon K'] = 1$ and $D = 0$. So $K' = K$.

The monomorphisms in (5) are induced by the isogenies $\Gamma' \to \Gamma$ and $\Gamma \to \Gamma'$. The unramified part follows from the Riemann-Hurwitz genus formula.

3. **The isomorphism theorems.** From now on, we'll assume that we have two function fields K and K' over a finite field of constants k and that $|k| = p^f$. We will also assume that we have $\lambda\colon G_K \to G_{K'}$, an isomorphism of profinite groups.

The key to strengthening the results of Theorem 2.5 is the following.

THEOREM 3.1. *Let $\mathfrak{S}_K$ and $\mathfrak{S}_{K'}$ be the sets of prime divisors of K and K' respectively. Then there is a set-theoretic map $\theta_K\colon \mathfrak{S}_K \to \mathfrak{S}_{K'}$ which is one-to-*

one and onto and such that $\deg \theta_K(P) = \deg P$ *for all primes* P *of* K.

PROOF. Recall that we have a one-to-one and onto map $\overline{\phi_{K,m}}$: $\overline{M_{p,m}(K)} \to \mathfrak{S}_m$. Similarly, we have $\overline{\phi_{K',m}}$: $\overline{M_{p,m}(K')} \to \mathfrak{S}'_m$. Now the isomorphism λ induces a one-to-one correspondence between $\overline{M_{p,m}(K)}$ and $\overline{M_{p,m}(K')}$, so by composition we get a one-to-one and onto map θ_m: $\mathfrak{S}_m \to \mathfrak{S}'_m$. The maps θ_m induce a map θ_K: $\mathfrak{S}_K \to \mathfrak{S}_{K'}$ which is one-to-one and onto and preserves the degree of a prime.

If L is a finite separable extension of K, then $\lambda(G_L) = G_{L'}$ where L' is finite separable over K'. So we have corresponding notation $\mathfrak{S}_L$, $\mathfrak{S}_{L'}$ and θ_L: $\mathfrak{S}_L \to \mathfrak{S}_{L'}$. We now analyse the relationship between θ_L and θ_K and in the case where L is Galois over K we consider the action of an element of $G(L/K)$ on a prime of L and its effect on θ_L.

PROPOSITION 3.2. *Let* P *be a prime of* K *and* ρ *a prime of* L *above* P. *Let* $P' = \theta_K(P)$ *and* $\rho' = \theta_L(\rho)$. *Then* ρ' *lies above* P', $e(\rho'/P') = e(\rho/P)$ *and* $f(\rho'/P') = f(\rho/P)$ *where* e *and* f *denote the ramification index and relative degree respectively.*

PROOF. If E is the constant field of L, then it is also the constant field of L'. Let $|E| = p^{ft}$. Let $d_P = \deg P$, $d_\rho = \deg \rho$, $m_P = fd_P$ and $m_\rho = jtd_\rho$. Then $\rho = \phi_{L,m_\rho}(G_M)$ and $P = \phi_{K,m_P}(G_N)$ where G_M is a maximal S_{p,m_ρ} subgroup of G_L and G_N is a maximal S_{p,m_P} subgroup of G_K. M and N are Hensel fields with respect to valuations w and v and their residue class fields have p^{m_ρ} and p^{m_P} elements respectively. Also, M and N are the decomposition fields of $\bar{w}$ and $\bar{v}$ over L and K respectively. So $M \supset N$.

The valuations w and v lie over the valuations associated to ρ and P. If M' is the fixed field of $\lambda(G_M)$ and N' the fixed field of $\lambda(G_N)$, then $M' \supset N'$ and M' and N' are Hensel fields with respect to valuations w' and v' which extend the valuations associated to ρ' and P' in L' and K' respectively. From uniqueness of valuations in Hensel fields, it follows that $v' = w'|N'$ and therefore ρ' lies over P'.

Now $td_\rho = f(\rho/P)d_P$ and $td_{\rho'} = f(\rho'/P')d_{P'}$. Also $d_\rho = d_{\rho'}$ and $d_P = d_{P'}$. Hence $f(\rho/P) = f(\rho'/P')$ and since $[M : N] = [M' : N']$ we have $e(\rho/P) = e(\rho'/P')$.

COROLLARY 3.3. *If* L *is an unramified extension of* K, *then* L' *is an unramified extension of* K'.

PROPOSITION 3.4. *Let* L *be a finite Galois extension of* K *and* ρ *a prime of* L. *Then if* $\sigma \in G_K$, $\theta_L(\sigma\rho) = \lambda(\sigma)\theta_L(\rho)$.

PROOF. Let v be the valuation of L associated to ρ and $\tilde{v}$ the valuation associated to $\tilde{\rho} = \sigma\rho$. Then $\tilde{v}(x) = v(\sigma^{-1}x)$ for all $x \in L$. If the residue class

field of the completion L_v has p^m elements, then $\rho = \phi_{L,m}(G_M)$ where M is a Hensel field with valuation w extending v. Also, M is the decomposition field of $\bar{v}$ over L.

Let $\tilde{M} = \sigma M$. Then $G_{\tilde{M}} = \sigma G_M \sigma^{-1}$ and since G_M is a maximal $S_{p,m}$ subgroup of G_L, so is $G_{\tilde{M}}$. Hence $\tilde{M}$ is a Hensel field with valuation $\tilde{w}$ and $\tilde{M}$ is the decomposition field of $\tilde{w}$ over L. It is easy to see that $\tilde{w}$ is the valuation given by $\tilde{w}(x) = w(\sigma^{-1}x)$ and that $\tilde{w}$ extends $\tilde{v}$. If M' is the fixed field of $\lambda(G_M)$ and $\tilde{M}'$ the fixed field of $\lambda(G_{\tilde{M}})$, then $G_{\tilde{M}'} = \lambda(\sigma)G_M\lambda(\sigma)^{-1}$ so that $\tilde{M}' = \lambda(\sigma)M'$. Now we know that M' is a Hensel field with valuation w' lying above the valuation v' associated to $\rho' = \theta_L(\rho)$ in L'. Then as above we can show that $\tilde{M}'$ is a Hensel field with valuation $\tilde{w}'$ lying above the valuation $\tilde{v}'$ associated to $\lambda(\sigma)\rho'$. Therefore, $\theta_L(\sigma\rho) = \lambda(\sigma)\rho' = \lambda(\sigma)\theta_L(\rho)$.

COROLLARY 3.5. *The isomorphism* λ: $G_K \to G_{K'}$ *induces an isomorphism* λ_1: $G(L/K) \to G(L'/K')$. *Let* G_ρ *be the decomposition subgroup of* $G(L/K)$ *with respect to the prime* ρ *of* L. *Let* $\rho' = \theta_L(\rho)$. *Then if* $\sigma \in G_\rho$, $\lambda_1(\sigma) \in G_{\rho'}$.

The following lemma follows easily from Theorem 2.5.

LEMMA 3.6. *Let* k_1 *be a finite extension of* k, $K_1 = k_1K$ *and* $K_1' = k_1K'$. *Then* $\lambda(G_{K_1}) = G_{K_1'}$. *In particular, if* $\bar{k}$ *is the algebraic closure of* k, $\bar{K} = \bar{k}K$, $\bar{K}' = \bar{k}K'$, *then* λ *induces an isomorphism* $\bar{\lambda}$: $G(\bar{K}/K) \to G(\bar{K}'/K')$.

Recall that $G_k \approx \hat{Z}$, the inverse limit of all finite cyclic groups and is generated by the Frobenius automorphism ϕ_k defined by $\phi_k(x) = x^{p^f}$ for all $x \in \bar{k}$. There is a natural isomorphism $G_k \to G(\bar{K}/K)$ and ϕ_K, the image of ϕ_k under this isomorphism, is called the Frobenius automorphism of K.

Let $\bar{\lambda}$: $G(\bar{K}/K) \to G(\bar{K}'/K')$ be the isomorphism induced by λ. Let $\phi_{K'} = \bar{\lambda}(\phi_K) \in G(\bar{K}'/K')$. Then $\phi_{K'}$ generates $G(\bar{K}'/K')$ but it is not obvious that $\phi_{K'}$ is the Frobenius automorphism of K'; i.e. the image of ϕ_k under the natural isomorphism $G_k \to G(\bar{K}'/K')$. However we will show in §4 that $\phi_{K'}$ is in fact the Frobenius automorphism of K'.

In what follows we make use of the local and global norm residue symbols of class field theory. We give a brief description. For details, see the Artin-Tate notes [1].

Let L be a complete local field of char p with finite residue class field l. Let ϕ be the Frobenius automorphism which generates G_l. The local norm residue symbol is a monomorphism $(\ ,\ L)$: $L^* \to G_L^{ab} = G(L^{ab}/L)$ where L^{ab} is the maximal abelian extension of L. The image of $(\ ,\ L)$ is $W_L = \{\tau \in G_L^{ab}: \tau|L^{nr} = \phi_L^n$ for some integer $n\}$, where L^{nr} is the maximal unramified extension of L and ϕ_L is the image of ϕ under the natural isomorphism $G_l \to G(L^{nr}/L)$.

Now let L be a function field in one variable with finite constant field l. Again let ϕ be the Frobenius automorphism generating G_l. For each prime ρ of L, let L_ρ be the completion and l_ρ the residue class field. If $d_\rho = \deg \rho$, then ϕ^{d_ρ} is the Frobenius automorphism generating G_{l_ρ}. If J_L is the idele group and C_L the idele class group of L, then we have the global norm residue symbol $(\ , L)$: $C_L \to G_L^{ab}$, a monomorphism whose image is $W_L = \{\tau \in G_L^{ab}: \tau|\bar{l}L = \phi_L^n$ for some integer $n\}$ where $\bar{l}$ is the algebraic closure of l and ϕ_L is the Frobenius automorphism of L. In addition, if $\bar{\alpha} \in C_L$, $\alpha = (\alpha_\rho) \in J_L$, then $(\bar{\alpha}, L) = \prod_\rho (\alpha_\rho, L_\rho)$, the product being taken over all prime divisors ρ of L.

Now the existence of these local and global symbols depends on the choice of the generator $\phi \in G_l$. If we choose another generator of G_l, we get another local symbol for a local field and another global symbol for a global field. But these new symbols behave in the same way as the old ones do, the only change being the replacement of the Frobenius (and its canonical images) by the new generator in the above description. A discussion of this fact can be found in [3].

Now we return to our given function fields K and K' with finite constant field k. For K we will choose a global symbol $(\ , K)$ generated by the Frobenius automorphism $\phi_k \in G_k$. The corresponding local symbols $(\ , K_P)$ will be generated by $\phi_k^{d_P}$ for each prime P of K; $d_P = \deg P$. For K' we will choose another generator of G_k as follows: recall that ϕ_K is the Frobenius automorphism generating $G(\bar{K}/K)$ and $\phi_{K'} = \bar{\lambda}(\phi_K)$. Then $\phi_{K'}$ is the image of some $\phi_k' \in G_k$ under the isomorphism $G_k \to G(\bar{K}/K')$. So we choose ϕ_k' to generate a global symbol $(\ , K')$ and the corresponding local symbols $(\ , K_{P'})$ will be generated by $\phi_k'^{d_{P'}}$ for each prime P' of K'; $d_{P'} = \deg P'$.

The image of $(\ , K)$ is $W_K = \{\tau \in G_K^{ab}: \tau|\bar{K} = \phi_K^n$ for some $n\}$ and the image of $(\ , K')$ is $W_{K'} = \{\tau \in G_{K'}^{ab}: \tau|\bar{K'} = \phi_{K'}^n$ for some $n\}$. If P and P' are primes of K and K' respectively, let ϕ_P be the Frobenius automorphism generating $G(K_P^{nr}/K_P)$ and let $\phi_{P'}$ be the generator of $G(K'^{nr}_{P'}/K'_{P'})$ which is the image of $\phi_k'^{d_{P'}}$ under the isomorphism $G_{k_\rho} \to G(K'^{nr}_{P'}/K'_{P'})$. Then the images of the local symbols are $W_P = \{\tau \in G_{K_P}^{ab}: \tau|K_P^{nr} = \phi_P^n$ for some $n\}$ and $W_{P'} = \{\tau \in G_{K'_{P'}}^{ab}: \tau|K'^{nr}_{P'} = \phi_{P'}^n$ for some $n\}$.

PROPOSITION 3.7. *The idele class groups C_K and $C_{K'}$ are isomorphic as abelian groups.*

PROOF. The global norm residue symbols imply that $C_K \approx W_K$ and $C_{K'} \approx W_{K'}$. Now λ induces an isomorphism λ_a: $G_K^{ab} \to G_{K'}^{ab}$. Since $\bar{\lambda}(\phi_K) = \phi_{K'}$, it follows that $\lambda_a(W_K) = W_{K'}$. Hence $W_K \approx W_{K'}$ and $C_K \approx C_{K'}$.

If we denote the isomorphism from C_K to $C_{K'}$ by μ, it can be described as follows: if $\bar{\alpha} \in C_K$, then $(\bar{\alpha}, K) \in W_K$, so $\lambda_a(\bar{\alpha}, K) \in W_{K'}$. Hence $\lambda_a(\bar{\alpha}, K)$

$= (\bar{\alpha}', K')$ where $\bar{\alpha}' \in C_{K'}$. So we define $\mu(\bar{\alpha}) = \bar{\alpha}'$. In other words, $\lambda_a(\bar{\alpha}, K) = (\mu(\bar{\alpha}), K')$.

PROPOSITION 3.8. *Let P be a prime of K and $P' = \theta_K(P)$ the corresponding prime of K'. Then there is an isomorphism ω_P: $K_P^* \to K_{P'}'^*$ such that* $\operatorname{ord}_{P'} \omega_P(x) = \operatorname{ord}_P x$ *for all* $x \in K_P^*$.

PROOF. From the local norm residue symbols we have $K_P^* \approx W_P$ and $K_{P'}'^* \approx W_{P'}$. So to get our desired isomorphism we will show that λ induces an isomorphism λ_P: $W_P \to W_{P'}$.

We can describe $G_{K_P}^{ab}$ as a subgroup of G_K^{ab} as follows: if L_0 is a finite abelian extension of K_P, then there is a finite abelian extension L of K and a prime ρ of L lying above P such that $L_\rho = L_0$. (See [1, p. 99].) So $G(L_0/K_P) \approx G(L_\rho/K_P) \approx G_\rho = \{\sigma \in G(L/K): \sigma\rho = \rho\}$. It follows that

$$G_{K_P}^{ab} \approx \operatorname{proj\,lim} G_\rho \subset \operatorname*{proj\,lim}_{L/K \text{ abelian}} G(L/K) = G_K^{ab}.$$

Now by Corollary 3.5, if L is finite abelian over K, ρ a prime of L, $\rho' = \theta_L(\rho)$, then λ induces an isomorphism λ_ρ: $G_\rho \to G_{\rho'}$. Furthermore these maps λ_ρ are compatible with the maps defining the above inverse limit. So by passing to the limit, we obtain an isomorphism λ_P: $G_{K_P}^{ab} \to G_{K'_{P'}}^{ab}$.

We now claim that $\lambda_P(W_P) = W_{P'}$. To see this note that $K_P^{nr} = \bar{K}K_P$ and so $G(K_P^{nr}/K_P) \approx G(\bar{K}/\bar{K} \cap K_P)$ and we can consider $G(K_P^{nr}/K_P)$ as a subgroup of $G(\bar{K}/K)$. Under this identification, $\phi_P = \phi_K^{d_P}$ since the residue class field k_P of K_P has $|k|^{d_P}$ elements. Similarly, $\phi_{P'} = \phi_{K'}^{d_{P'}}$. Hence $\bar{\lambda}(\phi_P) = \bar{\lambda}(\phi_K^{d_P}) = \phi_K^{d_P} = \phi_{K'}^{d_{P'}} = \phi_{P'}$. Thus $\bar{\lambda}(W_P) = W_{P'}$. But $\bar{\lambda} = \lambda_P | G(K_P^{nr}/K_P)$ and so $\lambda_P(W_P) = W_{P'}$.

More precisely, we have ω_P: $K_P^* \to K_{P'}'^*$ defined as follows: if $x \in K_P^*$, $\lambda_P(x, K_P) = (\omega_P(x), K'_{P'})$. To see that $\operatorname{ord}_P x = \operatorname{ord}_{P'} \omega_P(x)$, let $x' = \omega_P(x)$. Then

$$\begin{aligned}\phi_{P'}^{\operatorname{ord}_{P'} x'} &= (x', K'_{P'}) | K_{P'}'^{nr} = \lambda_P(x, K_P) | K_{P'}'^{nr} \\ &= \bar{\lambda}\big((x, K_P) | K_P^{nr}\big) = \bar{\lambda}\big(\phi_P^{\operatorname{ord}_P x}\big) = \phi_{P'}^{\operatorname{ord}_P x}.\end{aligned}$$

So $\phi_{P'}^{\operatorname{ord}_{P'} x'} = \phi_{P'}^{\operatorname{ord}_P x}$ and hence $\operatorname{ord}_P x = \operatorname{ord}_{P'} x'$.

COROLLARY 3.9. *Let J_K and $J_{K'}$ denote the idele groups of K and K'. Then there is an isomorphism ω: $J_K \to J_{K'}$ such that if $\alpha = (\alpha_P) \in J_K$ and $\omega(\alpha) = (\alpha'_{P'})$, $P' = \theta_K(P)$, then* $\operatorname{ord}_P \alpha_P = \operatorname{ord}_{P'} \alpha'_{P'}$.

COROLLARY 3.10. *There is an isomorphism γ: $K^* \to K'^*$ such that* $\operatorname{ord}_P x = \operatorname{ord}_{P'} \gamma(x)$ *for all $x \in K^*$. In addition, the following diagram commutes:*

$$\begin{array}{ccccccccc}
(1) & \longrightarrow & K^* & \longrightarrow & J_K & \xrightarrow{\pi} & C_K & \longrightarrow & (1) \\
 & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle \mu} & & \\
(1) & \longrightarrow & K'^* & \longrightarrow & J_{K'} & \xrightarrow{\pi'} & C_{K'} & \longrightarrow & (1)
\end{array}$$

where π and π' are the canonical maps and ω and μ are the isomorphisms defined above.

PROOF. The map γ is induced by ω. It is well defined and an isomorphism since by global class field theory the second square commutes.

The isomorphism theorems that we want to establish can be stated as one major result.

THEOREM 3.11. *Consider the following diagram for K:*

$$\begin{array}{ccccccccc}
 & & (1) & & (1) & & (1) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
(1) & \longrightarrow & k^* & \longrightarrow & U_K & \longrightarrow & U_K/k^* & \longrightarrow & (1) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
(1) & \longrightarrow & K^* & \longrightarrow & J_K & \longrightarrow & C_K & \longrightarrow & (1) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
(1) & \longrightarrow & P_K & \longrightarrow & D_K & \longrightarrow & Cl_K & \longrightarrow & (1) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & (1) & & (1) & & (1) & &
\end{array}$$

where U_K is the group of idele units, D_K the group of divisors of K, P_K the group of principal divisors and Cl_K the divisor class group. Then there is an isomorphism between this diagram and the corresponding diagram for K' such that all possible squares commute.

PROOF. We already have isomorphisms ω: $J_K \to J_{K'}$, μ: $C_K \to C_{K'}$ and γ: $K^* \to K'^*$. The isomorphism θ: $D_K \to D_{K'}$ is induced by θ_K in the natural way. It is easy to check that it is compatible with ω. The other isomorphisms are easily defined from the above isomorphisms and that the squares commute follows from straightforward diagram chasing.

COROLLARY 3.12. *The isomorphism $Cl_K \to Cl_{K'}$ induces an isomorphism θ_0: $Cl_K^0 \to Cl_{K'}^0$ of the divisor classes of degree zero of K and K' respectively.*

4. The Jacobian varieties of K and K'. Again let $\mathcal{J}$ and $\mathcal{J}'$ be the Jacobian varieties of K and K'. In this section, we will show that, given a finite extension E of k, the groups of E-rational points $\mathcal{J}(E)$ and $\mathcal{J}'(E)$ are isomorphic as $G(E/k)$-modules. This result allows us to reprove that $\mathcal{J}$ and $\mathcal{J}'$ are isogenous with a slightly stronger statement; namely, for each prime number $l \neq p$, there is an isogeny from $\mathcal{J}$ to $\mathcal{J}'$ whose kernel has order prime to l. In the course of this proof, we will prove that λ induces the identity automorphism of G_k.

Let L be a finite Galois extension of K and let L' be the fixed field of $\lambda(G_L)$. Since $G_L \approx G_{L'}$, we obtain an analogue of Theorem 3.11 for L and L'. In particular, we have an isomorphism $\omega_L: J_L \to J_{L'}$ of the idele groups of L and L'.

Now J_L is a $G(L/K)$-module as follows: Let $\sigma \in G_K$, $\bar{\sigma}$ its canonical image in $G(L/K)$. If ρ is a prime of L, L_ρ the completion, σ induces $\sigma_\rho: L_\rho^{ab} \to L_{\sigma\rho}^{ab}$. $\sigma_\rho \in G_{K_P}$ if ρ lies over P in K. If $\alpha = (\alpha_\rho) \in J_L$, then we define $(\bar{\sigma}\alpha)_{\sigma\rho} = \sigma_\rho \alpha_\rho$. Similarly, $J_{L'}$ is a $G(L'/K')$-module.

PROPOSITION 4.1. *$\omega_L(\bar{\sigma} \cdot \alpha) = \lambda_1(\bar{\sigma})\omega_L(\alpha)$ for all $\alpha \in J_L$, $\sigma \in G_K$, where λ_1: $G(L/K) \to G(L'/K')$ is induced by λ.*

PROOF. Let ρ be a prime of L and $\rho' = \theta_L(\rho)$. As seen in the proof of Proposition 3.8, λ induces an isomorphism $\lambda_\rho: G_{L_\rho}^{ab} \to G_{L'_{\rho'}}^{ab}$. We also have $\lambda_{\sigma\rho}$: $G_{L_{\sigma\rho}}^{ab} \to G_{L'_{\sigma'\rho'}}^{ab}$ where $\sigma' = \lambda(\sigma)$. Let $\sigma_\rho: L_\rho^{ab} \to L_{\sigma\rho}^{ab}$ be as defined above. Then

(*) $\lambda_{\sigma\rho}(\sigma_\rho \tau \sigma_\rho^{-1}) = \sigma'_{\rho'} \lambda_\rho(\tau) \sigma_{\rho'}'^{-1}$ for all $\tau \in G_{L_\rho}^{ab}$; $\sigma'_{\rho'}: L_{\rho'}'^{ab} \to L_{\sigma'\rho'}'^{ab}$.

From a property of the local norm residue symbol (see [4, p. 205]), we have:

(**) $(\sigma_\rho \alpha, L_{\sigma\rho}) = \sigma_\rho(\alpha, L_\rho)\sigma_\rho^{-1}$ for all $\alpha \in L_\rho^*$.

Recall that, by Proposition 3.8, for each prime ρ of L, we have an isomorphism $\omega_\rho: L_\rho^* \to L_{\rho'}'^*$. We claim that for each $\alpha \in L_\rho^*$, $\omega_{\sigma\rho}(\sigma_\rho \alpha) = \sigma'_{\rho'} \omega_\rho(\alpha)$. To see this, note that by the definition of $\omega_{\sigma\rho}$, we have

$$\lambda_{\sigma\rho}(\sigma_\rho \alpha, L_{\sigma\rho}) = (\omega_{\sigma\rho}(\sigma_\rho \alpha), L'_{\sigma'\rho'}).$$

On the other hand, using (*) and (**), we have

$$\lambda_{\sigma\rho}(\sigma_\rho \alpha, L_{\sigma\rho}) = (\sigma'_{\rho'} \omega_\rho(\alpha), L'_{\sigma'\rho'}).$$

This proves the claim.

Now if $\alpha = (\alpha_\rho) \in J_L$, then

$$\begin{aligned}(\omega_L(\bar{\sigma} \cdot \alpha))_{\sigma'\rho'} &= \omega_{\sigma\rho}((\bar{\sigma} \cdot \alpha)_{\sigma\rho}) = \omega_{\sigma\rho}(\sigma_\rho \alpha_\rho) \\ &= \sigma'_{\rho'} \omega_\rho(\alpha_\rho) = (\bar{\sigma}' \omega_L(\alpha))_{\sigma'\rho'}.\end{aligned}$$

Therefore, $\omega_L(\bar{\sigma} \cdot \alpha) = \bar{\sigma}' \omega_L(\alpha) = \lambda_1(\bar{\sigma})\omega_L(\alpha)$.

COROLLARY 4.2. *Let E be the constant field of L and L' and let $\delta_L: E^* \to E^*$ be the isomorphism for L and L' corresponding to the isomorphism $k^* \to k^*$ defined in Theorem* 3.11 *for K and K'. Then for each $x \in E^*$, $\bar{\sigma} \in G(L/K)$, $\delta_L(\bar{\sigma}x) = \lambda_1(\bar{\sigma})\delta_L(x)$.*

We are now in a position to prove that $\bar{\lambda}$ maps the Frobenius of K to the Frobenius of K'. We first need a lemma, whose proof is elementary.

LEMMA 4.3. *Let k be a finite field and E a finite extension of k of degree n. Let $f: E^* \to E^*$ be an isomorphism such that $f(\sigma x) = \sigma' f(x)$ for all $x \in E^*$ and all $\sigma \in G(E/k)$; $1 < r < n$. Then $r = 1$; i.e. f is a $G(E/k)$-morphism.*

PROPOSITION 4.4. *$\bar{\lambda}(\phi_K)$ is the Frobenius automorphism of K'.*

PROOF. Apply Corollary 4.2 where L is a finite constant field extension of K. Then use Lemma 4.3 and pass to the inverse limit.

We have now proved the following result.

THEOREM 4.5. *Any isomorphism $\lambda: G_K \to G_{K'}$ induces the identity automorphism of G_k.*

PROPOSITION 4.6. *Let $\theta_{0,L}: Cl_L^0 \to Cl_{L'}^0$ be the isomorphism of Corollary* 3.12 *applied to L and L'. Then, if $\bar{\sigma} \in G(L/K)$ and $\bar{D} \in Cl_L^0$, $\theta_{0,L}(\bar{\sigma} \cdot \bar{D}) = \lambda_1(\bar{\sigma})\theta_{0,L}(\bar{D})$.*

PROOF. Immediate from Proposition 3.4.

COROLLARY 4.7. *Let E be a finite extension of k, $L = EK$ and $L' = EK'$. Then Cl_L^0 and $Cl_{L'}^0$ are isomorphic as $G(E/k)$-modules.*

PROOF. Let ϕ be the Frobenius of $G(E/k)$. Let $\overline{\phi_K}$ and $\overline{\phi_{K'}}$ be the images of ϕ under the natural isomorphisms $G(E/k) \to G(L/K)$ and $G(E/k) \to G(L'/K')$. From the proof of Proposition 4.4, we know that $\lambda_1(\overline{\phi_K}) = \overline{\phi_{K'}}$. The result then follows from Proposition 4.6.

THEOREM 4.8. *Let $\mathcal{J}$ and $\mathcal{J}'$ denote the Jacobian varieties of K and K' respectively. If E is a finite extension of k, then the groups of E-rational points $\mathcal{J}(E)$ and $\mathcal{J}'(E)$ are isomorphic as $G(E/k)$-modules. Also, $\mathcal{J}(\bar{k})$ and $\mathcal{J}'(\bar{k})$ are isomorphic as G_k-modules.*

PROOF. Apply Corollary 4.7, using the fact that $\mathcal{J}(E) \approx Cl_L^0$ and $\mathcal{J}'(E) \approx Cl_{L'}^0$ as $G(E/k)$-modules. $\mathcal{J}(\bar{k}) \approx \text{ind lim } \mathcal{J}(E)$ and it is easy to see that the isomorphisms $\mathcal{J}(E) \to \mathcal{J}'(E)$ commute with the maps defining the direct limit.

COROLLARY 4.9. *For each prime $l \neq p$, there is an isogeny $g_l: \mathcal{J} \to \mathcal{J}'$ such that $|\ker g_l|$ is prime to l.*

PROOF. If $l \neq p$, we have the Tate modules $T_l\mathcal{J}$ and $T_l\mathcal{J}'$ which are G_k-modules. The isomorphism $\mathcal{J}(\bar{k}) \to \mathcal{J}'(\bar{k})$ of Theorem 4.8 induces α_l: $T_l\mathcal{J} \to T_l\mathcal{J}'$, an isomorphism of G_k-modules. By a theorem of Tate ([5]),

$$\operatorname{Hom}(\mathcal{J}, \mathcal{J}') \otimes_Z Z_l \approx \operatorname{Hom}_{G_k}(T_l\mathcal{J}, T_l\mathcal{J}')$$

where Z_l is the group of l-adic integers. The image of α_l in $\operatorname{Hom}(\mathcal{J}, \mathcal{J}') \otimes_Z Z_l$ under this isomorphism can be approximated by elements of $\operatorname{Hom}(\mathcal{J}, \mathcal{J}')$. Taking an element close enough, we get g_l: $\mathcal{J} \to \mathcal{J}'$ which induces an isomorphism $\tilde{g}_l$: $T_l\mathcal{J} \to T_l\mathcal{J}'$. Then g_l is an isogeny and $(\ker g_l)_{(l)} \approx T_l\mathcal{J}/\operatorname{im} \tilde{g}_l = (0)$.

5. **Automorphisms of G_K.** In this last section, we consider the case where $K = K'$; i.e. λ is an automorphism of G_K. We have one major result which follows easily from Lemma 3.6 and Proposition 4.4.

THEOREM 5.1. *If L is a constant field extension of K, then $\lambda(G_L) = G_L$ and the induced automorphism λ_1 of $G(L/K)$ is the identity. In particular, if $\bar{K} = \bar{k}K$, then $\lambda(G_{\bar{K}}) = G_{\bar{K}}$ and the induced automorphism of $G(\bar{K}/K)$ is the identity; i.e. $\lambda(\sigma)|\bar{K} = \sigma|\bar{K}$.*

BIBLIOGRAPHY

1. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1968. MR **36** #6383.

2. J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314. MR **39** #5528.

3. D. S. Rim and G. Whaples, *Global norm-residue map over quasi-finite field*, Nagoya Math. J. **27** (1966), 323–329. MR **34** #4252.

4. J. P. Serre, *Corps locaux*, 2nd ed., Hermann, Paris, 1968.

5. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR **34** #3749.

DEPARTMENT OF MATHEMATICS, BOSTON COLLEGE, CHESTNUT HILL, MASSACHUSETTS 02167