Vol. 11, No. 1, February 1979
Printed in Belgium

On the Characterization of Local Fields by Their Absolute Galois Groups

Moshe Jarden

Department of Mathematics, Tel-Aviv University, Ramat-Aviv, Tel-Aviv, Israel

(19)

AND

Jürgen Ritter

FB 3-Mathematik, TU Berlin, D-1000 Berlin 12

Communicated by P. Roquette

Received December 2, 1977

For finite field extensions of the field of Henselian p-adic rational numbers necessary and sufficient conditions are given which state that the fields have isomorphic absolute Galois groups; it is thereby supposed that a p-th root of unity (a 4-th when $p = 2$) belongs to the fields. Also examples are discussed.

This paper is mainly concerned with (infinite) Galois theory of p-adic fields containing $\mathbf{Q}_p(\zeta_p)$, the cyclotomic field arising from adjoining a p-th root of unity (4th if $p = 2$) to the Henselian field $\mathbf{Q}_p$ of p-adic rational numbers. Precisely, we determine all finite extensions E of $\mathbf{Q}_p(\zeta_p)$ that have the same type of algebraic extensions, that is, those which have isomorphic absolute Galois groups.

The result obtained reads somewhat more complicated than the analogous one in the *global* case conjectured by Neukirch [11] and finally proved by Uchida [14], Iwasawa [5], and Ikeda [3, 4]:

Let k_1 and k_2 be two algebraic number fields which have isomorphic absolute Galois groups (i.e. isomorphic as topological groups). Then k_1 and k_2 are isomorphic fields.

Recently Uchida [15] extended this theorem to the case, where k_1 and k_2 are two algebraic function fields of one variable over finite constant fields.

The following question naturally arises: What are the common properties of *local* fields that have isomorphic absolute Galois groups.[1]

[1] For a connection between the local and global case in this context we refer to the first part of [8]; in case of characteristic 0 see also [12], in case of characteristic $\neq 0$ [15].

In characteristic $\neq 0$ it turns out quite easily that the two local fields have to be isomorphic when considered as abstract fields [8]. In characteristic zero, however, we [8] were able to give examples of non-isomorphic local fields still having isomorphic Galois groups (see also Yamagata [16]).

To formulate precisely the result obtained in the latter case let us fix some notation:

K, L are always finite extensions of $\mathbf{Q}_p$;

K^0, L^0 are the maximal *abelian* subextensions in K and L, respectively, over $\mathbf{Q}_p$;

$n = n_K = | K : \mathbf{Q}_p |$ is the absolute field degree of K (correspondingly n_L);

G_K is the absolute Galois group of K, that is, the group of all field automorphisms of an algebraic closure of K which leave K elementwise fixed. This group is to be considered as a topological group in the Krull topology [1, Chapter 5]. G_L is defined correspondingly.

Finally let ζ_{p^i} denote a primitive p^i-th root of unity.

Now our *Theorem* reads as follows:

If $\zeta_p \in K$ (and $\zeta_4 \in K$ if $p = 2$), then the field L has absolute Galois group G_L isomorphic to G_K if and only if $n_L = n_K$ and $L^0 = K^0$.

For the proof we shall need some more notation:

$f = f_K$ is the residue class degree of K over the prime field $\mathbf{Z}/p\mathbf{Z}$; $q = p^f$;

$r = r_K = \max \{i : \zeta_{p^i} \in K\}$;

$r + d = r_K + d_K = \max \{j : \zeta_{p^j} \in K_{tr}\}$, here K_{tr} is the maximal tamely ramified algebraic extension of K;

$\eta := \zeta_{p^{r+d}}$.

In the following we will mostly restrict ourselves to the case where

$$r = r_K \geqslant 1 \text{ if } p \neq 2 \text{ and } r = r_K \geqslant 2 \text{ if } p = 2;$$

the other case will be dealt with in a subsequent paper.

Now ζ_p being an element of K, the extension $K(\eta)/K$ has to be unramified. Hence there is an unique rational integer s between 1 and $p^{r+d} - 1$, which is determined by the equation

$$\eta^{\varphi_K} = \eta^s,$$

where φ_K denotes a Frobenius automorphism of K in G_K. This number $s = s_K$ turns out to be an important parameter when G_K is described by generators and relations [6, 7, 9].

1. Proof of the Theorem

Let us begin by stating a well-known fact based on local class field theory, which gives information on K itself by knowing only G_K. At this time we do not assume $r \geqslant 1$.

LEMMA 1. *G_K, as a topological group, determines the invariants n, f, r and d of K.*

For the sake of completeness we shall repeat a proof of the lemma (see also [8]).

Fix some integer $m \geqslant 1$ and consider the maximal abelian extension E_m of K of exponent m. Its Galois group $G(m) = G(E_m/K)$ is the maximal abelian factor group of G_K of exponent m; from local class field theory it is isomorphic with $K^\times/K^{\times^m}$. Now

$$K^\times \simeq \mathbf{Z} \times W_{q-1} \times W_{p^r} \times \hat{\mathbf{Z}}_p{}^n,$$

where W_{p^r}, W_{q-1} denote the groups of roots of unity in K of order p^r and $q-1$, respectively, and $\hat{\mathbf{Z}}_p{}^n$ the n-fold direct product of the additive group of p-adic integers [9, p. 78].

Now, if E denotes the maximal abelian algebraic extension of K and G its Galois group over K, then E is clearly the union of all fields E_m and hence G is the projective limit of the groups $G(m)$, that is,

$$G \simeq \hat{\mathbf{Z}} \times W_{q-1} \times W_{p^r} \times \hat{\mathbf{Z}}_p{}^n = \prod_{l \neq p} \hat{\mathbf{Z}}_l \times W_{q-1} \times W_{p^r} \times \hat{\mathbf{Z}}_p^{n+1},$$

where (in the first term) $\hat{\mathbf{Z}}$ is the completion of $\mathbf{Z}$ and where (in the second term) the product is taken over all prime numbers $l \neq p$. Since G is obviously the maximal abelian factor group of G_K we see that G_K indeed determines f, r, and n.

Finally we have to compute d from G_K. The field $K(\zeta_{p^{r+1}})$ belongs to a normal subgroup of G_K, which index is p or a divisor of $p-1$, according to $r \geqslant 1$ or $r = 0$. Obviously there are only finitely many such subgroups. Now, by what we have seen just before, we can decide which one of these belongs to $K(\zeta_{p^{r+1}})$ and, moreover, whether the extension $K(\zeta_{p^{r+1}})/K$ will be ramified or not. If not, continue this procedure.

The next lemma turns out to be very useful when dealing with fields K and L whose absolute Galois groups are isomorphic. It says, roughly speaking, that the *pure extensions* of K and L mutually correspond under the given isomorphism of their groups. As a corollary we shall get the fact that the Frobenius number s, introduced above, is determined by G_K already (which fact by itself could also be deduced more directly).

LEMMA 2. *Assume $\sigma : G_K \to G_L$ is an isomorphism. Let U be the subgroup of G_K belonging to the pure extension $K' = K(\alpha)$ of degree m and with $\alpha^m = a \in K$. Then the fixed field L' of $\sigma U \leqslant G_L$ is a pure extension of L, and it can be generated by some m-th root β of an element $b \in L$ of the same value as a.*

First of all σ induces an isomorphism (which we denote again by σ) of G_K^{ab} with G_L^{ab}, the maximal abelian factor groups of G_K and G_L, respectively. Also, we fix a Frobenius automorphism φ_K of K in G_K and do not change notation when φ_K is considered as element of G_K^{ab}.

Now, by local class field theory, there is a canonical injection of $K^\times$ into G_K^{ab} induced by the reciprocity map θ. Hence we can identify the elements $x \in K^\times$ with the automorphisms $\theta(x)$, i.e. with the automorphisms $\varphi_K^{w(x)}\tau_x$, where $w(x)$ is the value of x, and where τ_x runs through the inertia subgroup T_K of G_K^{ab}, the precise image of the unit group of K.

By doing the same with L instead of K and noting that because of the preceeding lemma $\sigma(T_K) = T_L$, we shall get an isomorphism $\tilde{\sigma}$ from $K^\times$ onto $L^\times$ once we have shown that

$$\sigma(\varphi_K) \equiv \varphi_L \bmod T_L .$$

Moreover, from the properties of the reciprocity map θ [1, p. 144] it follows first that $x \in K$ and $\tilde{\sigma}(x) \in L$ will have the same value, and second, that the attaching of $\tilde{\sigma}$ to σ is compatible with extensions of fields in the sense that the corresponding isomorphism $\tilde{\sigma}' : K'^\times \to L'^\times$ continues our $\sigma : K^\times \to L^\times$ (K' and L' may here be quite arbitrary Galois-corresponding extensions of K and L, respectively).

The fact $\sigma(\varphi_K) \equiv \varphi_L \bmod T_L$ is due to Uchida [15]; for the moment we take it for granted and pursue the proof of our lemma.

Let $b = \tilde{\sigma}(a) \in L$ and $\beta = \tilde{\sigma}'(\alpha) \in L'$. Then a and b have the same value and $\beta^m = \tilde{\sigma}'(\alpha^m) = \tilde{\sigma}(a) = b$. So, thanks to Uchida's isomorphism $\tilde{\sigma}$, it remains only to check that $L' = L(\beta)$. Call this latter field L''; then, working with $\tilde{\sigma}''^{-1}$ instead of $\tilde{\sigma}'$, we get an extension K''/K, inside of K', in which some root of the polynomial $x^m - a$ will lie. Because of the irreducibility of this polynomial over K, the field K'' has to be equal to K' and therefore $L'' = L'$.

To finish the proof of our lemma we have to come back to the congruence $\sigma(\varphi_K) \equiv \varphi_L \bmod T_L$. For this we will now, for the convenience of the reader, reproduce Uchida's argument. Let us state this as

LEMMA 3. *Let $\sigma : G_K \to G_L$ be an isomorphism. Then, if φ_K is a Frobenius automorphism of K, $\sigma(\varphi_K)$ is a Frobenius automorphism of L.*

Proof [15]. Fix some integer m prime to p and let ζ be a root of unity of order m. Then, by lemma 1, σ induces an isomorphism of the groups belonging to $K(\zeta)$ and $L(\zeta)$. Choose further some prime element π of K. Then

$K(\sqrt[m]{\pi})$ is a totally tamely ramified extension of K belonging to, say, U, a subgroup of G_K. On account of lemma 1 the fixed field of $\sigma(U) \leqslant G_L$ has to be a totally tamely ramified extension of L, and hence can be generated by some m-th root of $\tilde{\pi}$, $\tilde{\pi}$ a suitable prime element of L [9, p. 78].

Now φ_K, being a Frobenius automorphism of K, maps ζ to ζ^q. We shall compute what the effect of the conjugation of τ with φ_K will be, where we choose for τ some representative in G_K of a generating automorphism of $K(\zeta, \sqrt[m]{\pi})/K(\zeta)$. To that end put

$$\tau(\sqrt[m]{\pi}) = \sqrt[m]{\pi} \cdot \zeta^j \qquad \text{and} \qquad \varphi_K^{-1}(\sqrt[m]{\pi}) = \sqrt[m]{\pi} \cdot \zeta^k :$$

$$\varphi_K \tau \varphi_K^{-1}(\sqrt[m]{\pi}) = \varphi_K(\sqrt[m]{\pi}\, \zeta^k \cdot \zeta^j) = \sqrt[m]{\pi}\, \zeta^{jq} = \tau^q(\sqrt[m]{\pi}),$$

that is $\varphi_K \tau \varphi_K^{-1} = \tau^q$, considered here as elements in $\mathrm{Gal}(K(\zeta, \sqrt[m]{\pi})/K)$. After applying σ we get: $\sigma(\varphi_K)\, \sigma(\tau)\, \sigma(\varphi_K)^{-1} = \sigma(\tau)^q$ (to be read in Gal $(L(\zeta, \sqrt[m]{\tilde{\pi}})/L)$), and consequently also $\sigma(\varphi_K)$ maps ζ to ζ^q (observe that from what we have seen above, $\sigma(\tau)$ represents a generating automorphism of $L(\zeta, \sqrt[m]{\tilde{\pi}})/L(\zeta)$).

Because $q_K = q_L$, it follows, by varying m over all positive integers prime to p, that $\sigma(\varphi_K)$ is a Frobenius automorphism of L.

Now we are in a good position to prove that the group G_K determines also the natural number $s = s_K$ of K when $r \geqslant 1$.

COROLLARY. *Suppose $\zeta_p \in K$. Then the type of isomorphism of the group G_K, considered as a topological group, determines s.*

For this, let $\sigma : G_K \to G_L$ be an isomorphism. Thanks to lemma 1 we know already that $r_K = r_L$ and $d_K = d_L$, so it remains to show that

$$\eta^{s_K} = \eta^{\varphi_K} \overset{!}{=} \eta^{\varphi_L} = \eta^{s_L},$$

where we remind the reader of our convention that η is a $r + d - th$ root of unity.

Let π be a prime element of K and let α be an $r + d - th$ root of π. Then, as lemma 2 tells us, the fixed field L' of σU, U being the subgroup in G_K belonging to $K(\alpha)$, is of the form $L' = L(\beta)$ with $\beta^{r+d} = \tilde{\pi}$, where $\tilde{\pi}$ is a prime element of L. Therefore we can proceed as in the last proof: we compute the action of φ_K on some representative τ of a generating automorphism of $K(\eta, \alpha)/K(\eta)$, and get $\varphi_K \tau \varphi_K^{-1} = \tau^{s_K}$ (in $\mathrm{Gal}(K(\eta, \alpha)/K)$). Applying σ to this equation gives $(\sigma\varphi_K)(\sigma\tau)(\sigma\varphi_K)^{-1} = (\sigma\tau)^{s_K}$ (in $\mathrm{Gal}(L(\eta, \beta)/L)$). If we compute $(\sigma\varphi_K)(\sigma\tau)(\sigma\varphi_K)^{-1}$ directly, keeping in mind that $\sigma\varphi_K = \varphi_L$ and $\sigma\tau$ is some respresentative of a generating automorphism of $L(\eta, \beta)/L(\eta)$, we get $\varphi_L(\sigma\tau)$

$\varphi_L^{-1} = (\sigma\tau)^{s_L}$ (in $\mathrm{Gal}(L(\eta, \beta)/L)$), that is, $s_K \equiv s_L \bmod p^{r+d}$, and this finally means $s_K = s_L$.

Lemmas 1 and 4 state that the numbers $n, f, r + d$, and s are invariants not only of K, but also of G_K, if $\zeta_p \in K$. Results of Jakovlev ($p \neq 2$) [7] and Zel'venskiĭ ($p = 2$) [17] show that the converse is also true: G_K, as a topological group, is fully determined by the parameters $n, f, r + d$, and s, when again $\zeta_p \in K$ is assumed and, when $p = 2$, $\zeta_4 \in K$. We do not need here the precise relations which hold between suitable chosen $n + 3$ generators of the profinite group G_K as given in [7] and [17], but only the fact that the cited four natural numbers are a complete system of parameters to describe G_K, cf. also [6], [9].[2]

So, for the proof of our theorem, we are left with the description of all fields L having the same invariants n, f, r, d, and s as K—where, from now on, we assume that $\zeta_p \in K$ and, for $p = 2$, $\zeta_4 \in K$.

As a first step we look for common subfields of all such L. From the invariance of f and r we get at once that $A_{f,r} \subset L$, where $A_{f,r}$ is defined to be the cyclotomic field $\mathbf{Q}_p(\zeta_{p^r(q-1)})$.

Now let us begin considering abelian extensions E of $\mathbf{Q}_p$ which contain $A_{f,r}$ of index p. This is done by using the local version of Kronecker-Weber's theorem which says that the abelian extensions of $\mathbf{Q}_p$ are just the subfields of the cyclotomic field extensions of $\mathbf{Q}_p$.

Therefore we can imbed the field E in some cyclotomic field $A_{m,t}$; observe here that for reasons of ramification each cyclotomic field extension of $\mathbf{Q}_p$ is in fact of the type $A_{m,t}$. Since $A_{f,r} \subset A_{m,t}$ we must have $f \mid m$ and $r \leqslant t$. By the way, as there are only finitely many possibilities for E [10, p. 54] we can assume that both m and t do not vary with the E. Now, the Galois group G of $A_{m,t}/A_{f,r}$ is the direct product of two cyclic subgroups of orders m/f and p^{t-r}, which correspond to the unramified extension $A_{m,r}/A_{f,r}$ and to the p-extension $A_{f,t}/A_{f,r}$, respectively, the last one being cyclic, too, since we assumed that $r \geqslant 1$ and, if $p = 2$, $r \geqslant 2$. Therefore G contains at most $p + 1$ subgroups of order p and hence, as follows from the duality theory of finite abelian groups, also at most $p + 1$ subgroups of index p, that is, there are at most $p + 1$ possibilities for the fields E. Since all the $p + 1$ subextensions of $A_{fp,r+1}/A_{f,r}$ of index p are indeed abelian extensions of $\mathbf{Q}_p$ which lie over $A_{f,r}$ of degree p, these are exactly the possible fields E.

We have proved:

[2] From a recent paper "On the Galois group of p-closed extensions of a local field" by Helmut Koch (to be published) we noticed that the system of generators and relations given by Jakovlev is in fact no such system for G_K. Koch proves, however, that G_K is determined (up to isomorphism) by our parameters.

LEMMA 4. *Let E be an extension of degree p of the cyclomotic field $A_{f,r}$. Then E is abelian over $\mathbf{Q}_p$ if and only if E is contained in $A_{fp,r+1}$.*

In the same way we can prove that the degree $| L^0 : A_{f,r} |$ is a power of p. In fact, if $| L^0 : A_{f,r} | = p^k \cdot u, p \nmid u$, then, because of the Sylow subgroup theorem applied to the abelian extension $L^0/A_{f,r}$, there is an intermediate field M between L^0 and $A_{f,r}$ having relative degree $u = | M : A_{f,r} |$ over $A_{f,r}$. Now, as M is an abelian extension of $\mathbf{Q}_p$, it is contained in some field $A_{m,t}$. Since the relative Galois group G of $A_{m,t}$ over $A_{f,r}$ is of the type $\mathbf{Z}/(m/f) \times \mathbf{Z}/p^{t-r}$ and since u is prime to p, the subgroup of G belonging to M must contain the factor $\mathbf{Z}/p^{t-r}$. If $u \neq 1$ this would imply that the residue degree of M is bigger than f which is impossible, however, since $M \subset L^0$.

Now we shall take the invariant d into account and prove

LEMMA 5. $| L^0 : A_{f,r} | = p^d$.

We prove this by induction on d, keeping in mind that the degree is a power of p.

Suppose first $d = 0$. Then $L(\zeta_{p^{r+1}})/L$ is a ramified extension of degree p. If $p \,||\, L^0 : A_{f,r} |$, then some abelian extension E of $\mathbf{Q}_p$, containing $A_{f,r}$ of index p, will lie in L. This E has to have the same r^-- and f^--invariant, that is $r_E = r$ and $f_E = f$, because it lies between $A_{f,r}$ and L. Considering Fig. 1[3] we

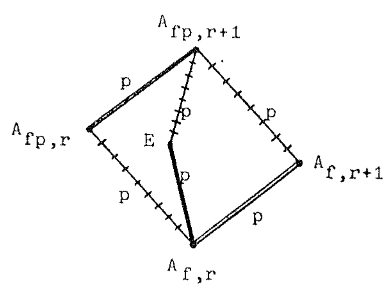

FIGURE 1

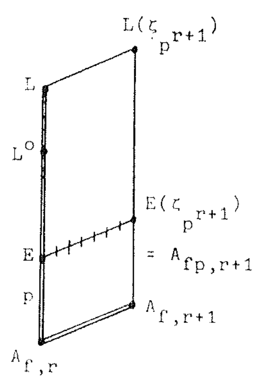

FIGURE 2

[3] ++ means: unramified extension; == means: totally ramified extension.

conclude from Lemma 5 that $E(\zeta_{p^{r+1}})/E$ is an unramified extension of degree p. But this leads (see Fig. 2) to the contradiction that, on the one hand, as we have seen just before, $L(\zeta_{p^{r+1}})/L$ is a totally ramified extension but, on the other hand, it shall contain the unramified subextension $E(\zeta_{p^{r+1}})/E$.

Now suppose $d \geqslant 1$. Then $L(\zeta_{p^{r+1}})/L$ is an unramified extension of degree p, and it will therefore contain $A_{fp,r+1}$. Now L intersects $A_{fp,r+1}$ in a subfield E of degree p over $A_{f,r}$, and consequently $p \mid\mid L^0 : A_{f,r} \mid$. Note that E is obviously different from $A_{f,r+1}$ and $A_{fp,r}$.

We have $f_{L(\zeta_{p^{r+1}})} = f \cdot p$ and $r_{L(\zeta_{p^{r+1}})} = r + 1$.[4] Also, $d_{L(\zeta_{p^{r+1}})} = d - 1$.

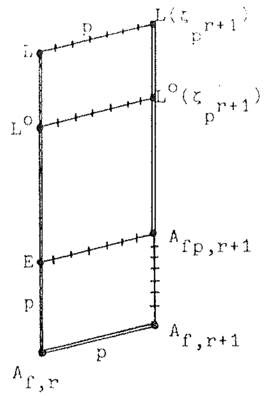

FIGURE 3

Clearly in Fig. 3 $L^0(\zeta_{p^{r+1}})$ is the maximal abelian subfield over $\mathbf{Q}_p$ of $L(\zeta_{p^{r+1}})$ — for otherwise, if $L(\zeta_{p^{r+1}})^0$ were a bigger field, the intersection $L(\zeta_{p^{r+1}})^0 \cap L$ would have to be bigger than L^0, too, since $L \cdot A_{f,r+1} = L(\zeta_{p^{r+1}})$ and since L is linearly disjoint from $A_{f,r+1}$ over $A_{f,r}$. But this contradicts the maximality of L^0 in L. By the induction hypothesis we can therefore assume that $L^0(\zeta_{p^{r+1}})$ has degree p^{d-1} over $A_{fp,r+1}$. Hence the degree of L^0 over $A_{f,r}$ is p^d.

COROLLARY. *Let $A/\mathbf{Q}_p$ be an abelian extension of absolute residue degree $f_A = f$, with $r_A = r$, and with $\mid A : A_{f,r} \mid = p^d$. Then*

(a) $d = d_A$

(b) $A/A_{f,r}$ *is cyclic*

(c) $A(\zeta_{p^{r+d}}) = A_{fp^d,r+d}$.

First of all, (a) follows at once from the preceding lemma. Using the proof of that lemma (especially figure (1)) one shows by induction, first, that $A(\zeta_{p^{r+d}}) = A_{fp^d,r+d}$, second, that A is linearly disjoint from $A_{f,r+d}$ over $A_{f,r}$, and, finally, that $A(\zeta_{p^{r+d}})/A_{f,r+d}$ is an unramified extension, hence cyclic. It follows that $\mathrm{Gal}(A/A_{f,r}) \simeq \mathrm{Gal}(A(\zeta_{p^{r+d}})/A_{f,r+d})$ is also cyclic.

[4] Notice that this is also true if $p = 2$, since in this case we assume that $r \geqslant 2$.

Next we take the invariant s into consideration and prove

LEMMA 6. $s_{L^0} = s$.

It follows from the corollary and from lemma 5 that $r_{L^0} = r$ and that $d_{L^0} = d$, hence also $\eta_{L^0} = \eta$. So let φ_L be the Frobenius automorphism of $L(\eta)/L$, so that $\eta^{\varphi_L} = \eta^s$. The restriction of φ_L onto $L^0(\eta)$ trivially coincides with the Frobenius automorphism of $L^0(\eta)/L^0$, since L and L^0 have the same absolute residue degree f. From this the lemma follows.

Now to distinguish L^0 from all the possible abelian field extension $A/\mathbf{Q}_p$ with $f_A = f$, $r_A = r$, and $| A : A_{f,r} | = p^d$, we still have to make sure of the following

LEMMA 7. *Let A_1, A_2 be two abelian field extensions of $\mathbf{Q}_p$ that contain $A_{f,r}$ and suppose $f_{A_i} = f$, $r_{A_i} = r$, and $| A_i : A_{f,r} | = p^d$ for $i = 1, 2$. If $s_{A_1} = s_{A_2}$ then $A_1 = A_2$.*

For the proof look at the following fields diagram, which is based on the corollary to lemma 5 (Fig. 4)

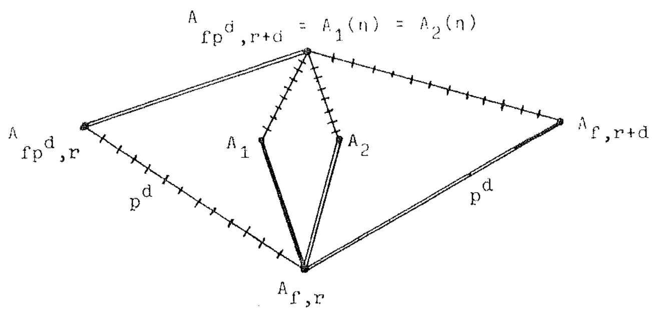

FIGURE 4

Let φ_1 and φ_2 be the Frobenius automorphism of $A_1(\eta)/A_1$ and $A_2(\eta)/A_2$, respectively. Then clearly the restrictions of φ_i, $i = 1, 2$, to $A_{fp^d,r}$ coincide with the Frobenius automorphism of $A_{fp^d,r}/A_{f,r}$. If we now think of φ_1 and φ_2 as automorphisms of $A_{fp^d,r+d}/A_{f,r}$, having fixed fields A_1 and A_2, respectively, we see that the φ_i are fully determined by their restrictions to $A_{fp^d,r}$ and $A_{f,r+d}$, that is, by the corresponding s_i.

Now we are ready for our announced theorem.

THEOREM. *Suppose K has the invariants f, $r \geqslant 1$ ($r \geqslant 2$, if $p = 2$), d, and s. Then L will have the same invariants if and only if $L^0 = K^0$. In particular, $G_L \simeq G_K$ is equivalent to $n_L = n_K$ & $L^0 = K^0$.*

Proof. The necessity of the condition $L^0 = K^0$ was proved in the lemmas 5 to 7. We still have to show that the condition is sufficient, too.

Now, L has to be totally ramified over L^0, otherwise L^0 would not be maximal abelian in L. Also, $r_L = r_{L^0}$. This allows us to apply lemma 5 to get $p^d = | L^0 : A_{f,r} |$. Finally, from lemma 6 we get the desired s.

2. Examples

Define the Galois class of K to consists of all fields L having absolute Galois group G_L isomorphic to G_K. If $\zeta_p \in K$ and, for $p = 2$, also $\zeta_4 \in K$, we shall denote, in view of our theorem, this class by $(n, K^0)_p$. Now let us get some impression how large the Galois class of K is. To that end we shall look at two classes and see what can happen here.[5]

(1) There are three distinct fields L_1, L_2, L_3 in $((p-1)\,p, \mathbf{Q}_p(\zeta_p))_p$ such that:

(1a) L_1 and L_2 are both *normal* over $\mathbf{Q}_p$ and have isomorphic relative Galois groups;

(1b) L_3 is *not normal* over $\mathbf{Q}_p$.

(2) There are two distinct *normal* extensions L_1, L_2 over $\mathbf{Q}_p$ belonging to $((p-1)\,p^3, \mathbf{Q}_p(\zeta_{p^2}))_p$ which have *non-isomorphic* relative Galois groups over $\mathbf{Q}_p$.

The cases (1) and (2) work only for primes $p \neq 2$; if the reader is also interested in similar examples of classes $(n, K^0)_2$[6] we refer him to the somewhat troublesome computations of the last sections of [8].

To (1): Define $L_1 = \mathbf{Q}_p(\zeta_p, \sqrt[p]{p})$, $L_2 = \mathbf{Q}_p(\zeta_p, \sqrt[p]{p+1})$, $L_3 = \mathbf{Q}_p(\zeta_p, \sqrt[p]{\zeta_p - 1})$. Then obviously $L_1/\mathbf{Q}_p$ and $L_2/\mathbf{Q}_p$ are normal extensions having relative Galois groups both isomorphic to the semi-direct product $\mathbf{Z}/p\mathbf{Z} \cdot \mathbf{Z}/(p-1)\,\mathbf{Z}$. In particular, $L_1{}^0 = L_2{}^0 = \mathbf{Q}_p(\zeta_p)$.

It remains to show that the Eisenstein extension $L_3/\mathbf{Q}_p(\zeta_p)$ is not normal over $\mathbf{Q}_p$, for then clearly $L_3{}^0 = \mathbf{Q}_p(\zeta_p)$, too. Now, if $L_3/\mathbf{Q}_p$ were normal, then surely $\sqrt[p]{\zeta_p{}^2 - 1}$ would have to belong to L_3, and from this and Kummer theory we should be able to deduce an equation $\zeta_p{}^2 - 1 = (\zeta_p - 1)^j \cdot a^p$, where $1 \leqslant j \leqslant p-1$ and $a \in \mathbf{Q}_p(\zeta_p)$. Assuming this equation

[5] The examples given are taken from our paper [8].

[6] Using the theorem of the preceeding section one can actually simplify these computations. We have the following examples: (1′) To $(8, \mathbf{Q}_2(\zeta_8))_2$ belong: $\mathbf{Q}_2(\zeta_8, \sqrt{\zeta_4 - 1})$, $\mathbf{Q}_2(\zeta_4, \sqrt[4]{2})$, $\mathbf{Q}_2(\zeta_8, \sqrt{\zeta_8 - 1})$. The first two fields are normal extensions of $\mathbf{Q}_2$ with Galois groups both isomorphic to the diehedral group D_8; the third is not normal over $\mathbf{Q}_2$. (2′) In $(32, \mathbf{Q}_2(\zeta_{16}))_2$ there are two normal field extensions of $\mathbf{Q}_2 : \mathbf{Q}_2(\zeta_{16}, \sqrt{\zeta_8 - 1}, \sqrt{\zeta_8{}^3 - 1})$ and $\mathbf{Q}_2(\zeta_{16}, \sqrt[4]{\zeta_4 - 1})$. Their relative Galois groups, having different numbers of elements of order two, are not isomorphic.

to be true we proceed as follows. We divide it by $\zeta_p - 1$ and apply the valuation of $\mathbf{Q}_p(\zeta_p)$ to get

$$0 = j - 1 + p \cdot w(a),\ w(a) \text{ denoting the } \mathbf{Q}_p(\zeta_p)\text{-value of } a.$$

It follows $j = 1$ and consequently $\zeta_p + 1 = a^p$. Now reducing modulo $\zeta_p - 1$, which is a prime element in $\mathbf{Q}_p(\zeta_p)$, we obtain $a^p \equiv 2 \bmod \zeta_p - 1$ and, on account of the fact that the residue field of $\mathbf{Q}_p(\zeta_p)$ contains only p elements, we have $a \equiv 2 \bmod (\zeta_p - 1)$. This forces $\zeta_p + 1 \equiv a^p \equiv 2 \bmod (\zeta_p - 1)^2$ because of $p \equiv 0 \bmod (\zeta_p - 1)^2$. Hence $\zeta_p - 1 \equiv 0 \bmod (\zeta_p - 1)^2$, which is a contradiction.

To (2): Define $L_1 = \mathbf{Q}_p(\zeta_{p^2}, \sqrt[p^2]{p})$ and $L_2 = \mathbf{Q}_p(\zeta_{p^2}, \sqrt[p]{p}, \sqrt[p]{p+1})$.
Then it is easily seen that both extensions are indeed normal over $\mathbf{Q}_p$ of degree $(p-1)p^3$. Since $L_1/\mathbf{Q}_p(\zeta_{p^2})$ is a cyclic extension, $Z := \mathbf{Q}_p(\zeta_{p^2}, \sqrt[p]{p})$ is the only subfield of L_1 of degree p over $\mathbf{Q}_p(\zeta_{p^2})$, and consequently $L_1^0 = \mathbf{Q}_p(\zeta_{p^2})$, as Z contains the non-normal subextension $\mathbf{Q}_p(\sqrt[p]{p})/\mathbf{Q}_p$.
We leave it as an exercise to examine that the $p + 1$ fields

$$\mathbf{Q}_p(\zeta_{p^2}, \sqrt[p]{p}),\ \mathbf{Q}_p(\zeta_{p^2}, \sqrt[p]{p^j(p+1)}) \qquad (0 \leqslant j \leqslant p-1)$$

are just the intermediate fields between $\mathbf{Q}_p(\zeta_{p^2})$ and L_2. Obviously, no one of these turns out to be abelian over $\mathbf{Q}_p$, so that also $L_2^0 = \mathbf{Q}_p(\zeta_{p^2})$.
Now look at the p-Sylow-subgroups of $\mathrm{Gal}(L_1/\mathbf{Q}_p)$ and $\mathrm{Gal}(L_2/\mathbf{Q}_p)$. These are already for reasons of order the groups $\mathrm{Gal}(L_1/\mathbf{Q}_p(\zeta_p))$ and $\mathrm{Gal}(L_2/\mathbf{Q}_p(\zeta_p))$, respectively. The first one contains the cyclic subgroup $\mathrm{Gal}(L_1/\mathbf{Q}_p(\zeta_{p^2}))$ of order p^2, but the second one is elementary abelian. This proves that $L_1/\mathbf{Q}_p$ and $L_2/\mathbf{Q}_p$ have nonisomorphic relative Galois groups.

Observe that something more can be learned from this example, namely, that *there is no possibility of continuing some given isomorphism between the absolute Galois groups of L_1 and L_2 to an automorphism of the absolute Galois group of the common maximal abelian subfield $L_1^0 = L_2^0 = \mathbf{Q}_p(\zeta_{p^2})$.* For otherwise the relative groups $\mathrm{Gal}(L_1/L_1^0)$ and $\mathrm{Gal}(L_2/L_2^0)$ would have to be isomorphic, but this is surely wrong, as these groups are up to isomorphism the groups $\mathbf{Z}/p^2\mathbf{Z}$ and $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, respectively.

Finally we would like to consider the class of a *normal tamely ramified* extension $K/\mathbf{Q}_p$. In a certain sense these classes are rather small: If $p = 2$, it turns out that K is the only normal extension over $\mathbf{Q}_p$ in its class. For odd primes, however, we do have to make some further assumption to be sure of an analogous result.
Let K^z be the maximal tamely ramified subextension of some $K/\mathbf{Q}_p$ and let e' be the quotient $|K^z : \mathbf{Q}_p|/f$. Then the following is true:

PROPOSITION. *Suppose the normal extensions K and L over $\mathbf{Q}_p$ have iso-*

morphic absolute Galois groups. Suppose further that e' is relatively prime to $p - 1$. Then $K^z = L^z$.

Proof. K^z, being a tamely ramified extension of $\mathbf{Q}_p$, can be written as $K^z = \mathbf{Q}_p(\zeta, \sqrt[e']{p\zeta^d})$, where ξ is a root of unity of order $p^f - 1$ and $0 \leqslant d < gcd(e', p^f - 1)$, cf. [2, p. 242]. As $K/\mathbf{Q}_p$ is normal $K^z/\mathbf{Q}_p$ must be normal, too. Hence $e' \mid p^f - 1$ and $\zeta^{d(p^f-1)/e'} \in \mathbf{Q}_p$.

If $d \neq 0$ then the order of $\zeta^{d(p^f-1)e'}$ is $e'/gcd(d, e')$, and consequently this number must divide $p - 1$, contrary to the assumption. Hence $d = 0$, i.e. $K^z = \mathbf{Q}_p(\zeta, \sqrt[e']{p})$. In the same way one proves that $L^z = \mathbf{Q}_p(\zeta, \sqrt[e']{p})$; note that because of our first lemma $e'_K = e'_L$.

Let us add here two remarks. First of all, as the last proof shows, we can drop the assumption that K and L are normal over $\mathbf{Q}_p$, if instead of $gcd(e', p - 1) = 1$ we require that $gcd(e', p^f - 1) = 1$.

Secondly, if $p \neq 2$, the condition of e' being relatively prime to $p - 1$ implies $r = 0$.

In this connection consider the Galois class of the normal tamely ramified field extension $K = \mathbf{Q}_p(\zeta_e, \sqrt[e]{p})$ over $\mathbf{Q}_p$, where p is an odd prime and $e = p^{p-1} - 1$. We contend that this is just the class $(e(p - 1), \mathbf{Q}_p(\zeta_{ep}))_p$, and, moreover, that this class indeed contains a second normal tamely ramified extension $L/\mathbf{Q}_p$. Now $\mathbf{Q}_p(\zeta_e)$ is obviously the maximal unramified subfield of K; it is of degree $p - 1$ over $\mathbf{Q}_p$ because the residue field of the unramified extension of degree $p - 1$ over $\mathbf{Q}_p$ has to have exactly $p^{p-1} - 1$ elements $\neq 0$. Furthermore $\zeta_p \in K$ since

$$\sqrt[p-1]{-p} = \zeta_e^{d/2}(\sqrt[e]{p})^d, \qquad \text{where} \quad d = e/p - 1,$$

and

$$\mathbf{Q}_p(\sqrt[p-1]{-p}) = \mathbf{Q}_p(\zeta_p) \quad [2, \text{p. } 214].$$

It follows that K^0 contains $\mathbf{Q}_p(\zeta_{ep}) = A_{p-1,1}$. As the degree $\mid K^0 : A_{p-1,1} \mid$ divides $\mid K : \mathbf{Q}_p \mid / \mid \mathbf{Q}_p(\zeta_{ep}) : \mathbf{Q}_p \mid = (p - 1)\, e/(p - 1)^2 = d$, and as d is relatively prime to p, we conclude in view of lemma 5 that $K^0 = \mathbf{Q}_p(\zeta_{ep})$.

We now take L to be the field $\mathbf{Q}_p(\zeta_e, \sqrt[e]{p\zeta_e{}^d})$. Then L is also a normal tamely ramified extension over $\mathbf{Q}_p$ of degree $e(p - 1)$ [2, p. 242], but $L \neq K$ since $1 < d < e$ [2, p. 242]. This L turns out to be a second normal field within the class $(e(p - 1), \mathbf{Q}_p(\zeta_{ep}))_p$ because of the relation

$$\sqrt[p-1]{-p} = \zeta_e^{(d/2)-(d/p-1)} \sqrt[e]{p\zeta_e{}^d},$$

note here that $p^{p-1} \equiv 1 \bmod (p - 1)^2$.

We finish with an example in case $p = 2$, which shows that the proposition will no longer be valid if we drop the assumption that $L/\mathbf{Q}_2$ has to be normal.

Let K be the normal field $\mathbf{Q}_2(\zeta_{12}, \sqrt[3]{2})$ and L the field $\mathbf{Q}_2(\zeta_{12}, \sqrt[3]{2\zeta_3})$. Then clearly both fields belong to the class $(12, \mathbf{Q}_2(\zeta_{12}))_2$, owing to the fact that the degrees $|K : \mathbf{Q}_2(\zeta_{12})| = |L : \mathbf{Q}_2(\zeta_{12})| = 3$ are odd. Furthermore, $K^z = \mathbf{Q}_2(\zeta_3, \sqrt[3]{2}) \neq L^z = \mathbf{Q}_2(\zeta_3, \sqrt[3]{2\zeta_3})$ since $L^z/\mathbf{Q}_2$ is not normal (see the proof for L_3 in (1)).

References

1. J. W. S. Cassels and A. Fröhlich, "Algebraic Number Theory," Academic Press, London/New York, 1967.
2. H. Hasse, "Zahlentheorie," Akademie-Verlag, Berlin, 1963.
3. M. Ikeda, Completeness of the absolute Galois group of the rational number field, *Crelle J.* **291** (1977), 1–21.
4. M. Ikeda, On automorphisms of Galois groups, to appear.
5. K. Iwasawa, On the automorphisms of Galois groups, (1975), manuscript.
6. K. Iwasawa, On Galois groups of local fields, *Trans. Amer. Math. Soc.* **80** (1955), 448–469.
7. A. V. Jakovlev, The Galois group of the algebraic closure of a local field, *Math. USSR-Izv.* **2** (1968), 1231–1269.
8. M. Jarden and J. Ritter, Local fields with isomorphic absolute Galois groups, (1976), manuscript.
9. H. Koch, "Galoissche Theorie der p-Erweiterungen," Deutscher Verlag der Wissenschaften, Berlin, 1970.
10. S. Lang, "Algebraic Number Theory," Addison–Wesley, Reading, Mass., 1970.
11. J. Neukirch, Kennzeichnung der p-adischen und der endlich algebraischen Zahlkörper, *Invent. Math.* **6** (1969), 296–314.
12. J. Neukirch, Über die absoluten Galoisgruppen algebraischer Zahlkörper, *Astérisque* **41–42** (1977), 67–79.
13. J. Neukirch, "Klassenkörpertheorie," BI, Mannheim, 1969.
14. K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc.*, in press.
15. K. Uchida, Isomorphisms of Galois groups of algebraic function fields, to appear.
16. S. Yamagata, A counter example for the local analogy of a theorem by Iwasawa and Uchida, *Proc. Japan Acad.* **52** (1976), 276–278.
17. I. G. Zel'venskiĭ, On the algebraic closure of a local field for $p = 2$, *Math. USSR-Izv.* **6** (1972), 925–937.