An Analogue of Artin-Schreier Theorem

Moshe Jarden

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

Introduction

Let \( v \) be an absolute value of \( \mathbb{Q} \), let \( \hat{\mathbb{Q}} \) be the completion of \( \mathbb{Q} \) with respect to \( v \) and let \( \mathbb{Q}_v = \hat{\mathbb{Q}} \cap \hat{\mathbb{Q}}_v \) be the algebraic subfield of \( \hat{\mathbb{Q}}_v \). Then \( \mathbb{Q}_v \) has the following two properties:

(A) \( \mathbb{Q}_v \) has no non-trivial automorphisms, in particular \( \mathbb{Q}_v \) is a Galois extension of no proper subfield.

(B) \( \mathbb{Q}_v \) has no proper subfield of a finite co-degree.

(The co-degree of a subfield \( E \) of \( F \) is simply the degree of \( F \) over \( E \).)

If \( v \) is archimeadean, then \( \mathbb{Q}_v = \hat{\mathbb{Q}} \cap \mathbb{R} \), and (B) is a consequence of the famous (cf. Jacobson [5, p. 316]).

Artin-Schreier Theorem. If a proper subfield of an algebraically closed field has a finite co-degree, then this co-degree is equal to 2.

If \( v \) is non-archimeadean, then \( \mathbb{Q}_v = \hat{\mathbb{Q}} \cap \hat{\mathbb{Q}}_v \), and (B) is a consequence of

F. K. Schmidt Theorem. A field \( F \) which is not separably closed can be Henselian with respect to at most one rank-1 valuation (see [14]).

Note that the Galois group \( G(\mathbb{Q}_v) = \sigma(\hat{\mathbb{Q}}_v/\mathbb{Q}_v) \) is finitely generated (cf. Jakovlev [6] and Zel'Venskii [18]). Hence \( \mathbb{Q}_v \) is of the form \( \hat{\mathbb{Q}}(\sigma) \), where \( (\sigma_1, \ldots, \sigma_e) \in G(\mathbb{Q})^e \) and \( \hat{\mathbb{Q}}(\sigma) \) is the fixed field in \( \hat{\mathbb{Q}} \) of \( \sigma_1, \ldots, \sigma_e \). The \( e \)-tuples that appear as generators of \( G(\mathbb{Q}_v) \), for all \( v \), are “special”, because, as was shown in [7, Theorem 2.5 and Lemma 2.9], they form only a zero set in \( G(\mathbb{Q})^e \) with respect to the Haar measure \( \mu \) (see [8, Sect. 4] for more details on the Haar measure of \( G(\mathbb{Q})^e \)). If we replace those special \( (\sigma) \)'s with arbitrary ones, then (A) and (B) may become false. Indeed take \( E = \hat{\mathbb{Q}}(\tau_1, \ldots, \tau_d) \) for some \( \tau_1, \ldots, \tau_d \in G(\mathbb{Q}) \) and let \( F \) be a proper finite Galois extension of \( E \). Then \( F = \hat{\mathbb{Q}}(\sigma_1, \ldots, \sigma_e) \) for some \( \sigma_1, \ldots, \sigma_e \in G(\mathbb{Q}) \) and \( F \) has certainly none of the properties (A) and (B). By choosing \( \tau_1, \ldots, \tau_d \) and \( F \) appropriately, one can actually achieve every \( e \) in this way.

0025-5831/79/0242/0193/$01.60
In [8] it was however conjectured that those counter examples are exceptional. More precisely, the following conjecture was made.

If $K$ is a Hilbertian field, then for almost all $(\sigma) \in G(K)^e$ we have:

(C) $K_\sigma(\sigma)$ is a Galois extension of no proper subfield that contains $K$.

(D) $K_\sigma(\sigma)$ has no proper subfield of finite co-degree that contains $K$.

In establishing this conjecture three weaker theorems were proved:

(E) Let $K$ be a global field. Then for almost all $(\sigma) \in G(K)^e$, the centralizer of $\langle \sigma \rangle$ in $G(K)$ is equal to $\langle \sigma \rangle$ if $e = 1$, and is trivial if $e \geq 2$ [8, Theorem 14.1].

(F) Let $K$ be a Hilbertian field, then for almost all $(\sigma) \in G(K)^e$, the field $K_\sigma(\sigma)$ contains no formally real subfield of finite co-degree that contains $K$ [8, Theorem 12.2].

(G) (D) is true for $e = 1$ [8, Theorem 13.1].

In this work we make a further major step in proving the conjecture and prove:

(H) Let $K$ be a Hilbertian field. Then for almost all $(\sigma) \in G(K)^e$ the field $K_\sigma(\sigma)$ is a Galois extension of no proper subfield of a finite co-degree that contains $K$.

If $K$ is a global field, then for almost all $(\sigma) \in G(K)^e$ we have:

(I) $K_\sigma(\sigma)$ is a Galois extension of no proper subfield that contains $K$.

(J) If $E$ is a subfield of $K_\sigma(\sigma)$ that contains $K$ such that $K_\sigma(\sigma)/E$ is a finite separable extension, then $\left[K_\sigma(\sigma):E\right]$ divides $e - 1$.

(K) If $1 \leq e \leq 5$, then $K_\sigma(\sigma)$ is a separable extension of no proper subfield of a finite co-degree that contains $K$.

Note that (J) is an analogue of Artin-Schreier theorem. As a consequence of (I) we supply in Sect.9 a counter example to an infinite analogue of Iwasawa-Uchida's theorem.

**Notation**

$\mathbb{Q}$ = the field of rational numbers.
$\mathbb{R}$ = the field of real numbers.
$\mathbb{C}$ = the field of complex numbers.
$\mathbb{Q}_p$ = the field of $p$-adic numbers.
$K_\sigma$ = the separable closure of a field $K$.
$K$ = the algebraic closure of $K$.
$K_{ab}$ = the maximal abelian of $K$.
$K^{(p)}$ = the maximal $p$-extension of $K$.
$N(\sigma)$ = the fixed field of $e$ automorphisms $\sigma_1, \ldots, \sigma_e$ of a field $N$.
$\text{rank}(G) \leq e$ = the pro-finite group $G$ is generated by $e$ elements.
$e_p(K)$ = rank$(\mathcal{G}(K^{(p)}/K))$.
$\langle \sigma_1, \ldots, \sigma_e \rangle$ = the closed subgroup generated by elements $\sigma_1, \ldots, \sigma_e$ of $G$.
$\Gamma^e$ = the free pro-finite group generated by $e$ elements.
$\zeta_n$ = a primitive $n$-th root of unity.

1. **The Maximal $p$-Extension of a Field**

For a field $E$ and a prime $p$ we denote by $E^{(p)}$ the maximal $p$-extension of $E$. The rank of $\mathcal{G}(E^{(p)}/E)$ is denoted by $e_p(E)$. If $E \subseteq F \subseteq E^{(p)}$ is an intermediate field, then
$E^{(p)} = F^{(p)}$, since $E^{(p)}$ has no proper $p$-extensions. If $E'$ is an algebraic extension of $E$ which is linearly disjoint from $E^{(p)}$, then there is an epimorphism $\mathcal{G}(E^{(p)}/E') \to \mathcal{G}(E^{(p)}/E)$ and hence $e_p(E') \geq e_p(E)$.

**Lemma 1.1.** Let $p$ be a prime and let $E$ be a field, which is not formally real if $p = 2$. Then $\mathcal{G}(E^{(p)}/E)$ is a torsion free group.

**Proof.** If $\mathcal{G}(E^{(p)}/E)$ contains an element of a finite order, then there exists a field $E \subseteq F \subseteq E^{(p)}$ such that $[E^{(p)}:F] = p$. This however contradicts Theorem 2 of Whaples [17], which implies that $[F^{(p)}:F] = \infty$.

Lemma 1.1 will be used in order to satisfy one of the conditions of the following

**Theorem of Serre.** If a torsion free pro-$p$ group $G$ contains an open free pro-$p$ subgroup, then $G$ is free too (see [15, p. 413]).

A complement to Serre's theorem is:

**Nielsen-Schreier Formula.** Let $C$ be either the category of pro-finite groups or the category of pro-$p$ groups. Let $G$ be a free $C$-group of a finite rank and let $H$ be an open subgroup of $G$. Then $H$ is also free and

$$\text{rank}(H) - 1 = (G:H)(\text{rank}(G) - 1)$$

(see [1, p. 108]).

### 2. Abelian Extensions of Hilbertian Fields

In [8, p. 286] it was proved that if $K$ is a Hilbertian field, then $\langle \sigma_1, \ldots, \sigma_e \rangle \cong \hat{F}_{e}$ for almost all $(\sigma \in G(K)^{\circ})$ (this is the "Free Generators Theorem"). In this section we prove the analogous result for the group $\mathcal{G}(K_{ab}/K)$.

**Lemma 2.1.**
Let $K$ be a field and let $t$ be a transcendental element over $K$. Then every finite Abelian group can be realized over $K(t)$.

**Proof.** If $\text{char}(K) = p \neq 0$, then, by a result of Lenstra, every finite abelian group $A$ can be realized over a finitely generated, purely transcendental extension of $K$, since the field generated over $K$ by a root of unity is a cyclic extension of $K$ (see [12, p. 322, Corollary 7.5]). By Hilbert irreducibility theorem, which $K(t)$ satisfies, we get that $A$ can be realized also over $K(t)$.

For $\text{char}(K) = 0$, the lemma can be found in Frey [3].

**Corollary 2.2.** If $K$ is a Hilbertian field, then every finite abelian group can be realized over $K$.

The corollary can be strengthened in the following way:

**Theorem 2.3.** Let $K$ be a Hilbertian field and let $A$ be a finite abelian group. Then there exists a linearly disjoint sequence $K_1, K_2, K_3, \ldots$ of Galois extensions of $K$ such that $\mathcal{G}(K_i/K) \cong A$ for every $i \geq 1$.

---

1 The author is indebted to Wulf-Dieter Geyer for calling his attention to Whaples result.
Theorem 2.3 is a consequence of Corollary 1.2 and the following general

Lemma 2.4. Let \( K \) be a field and let \( G \) be a finite group. Suppose that the direct power \( G^n \) is realizable over \( K \) for every \( n \). Then there exists a linearly disjoint sequence \( K_1, K_2, K_3, \ldots \) of Galois extensions of \( K \) such that \( \mathcal{G}(K_i/K) \cong G \) for every \( i \geq 1 \).

Proof. Suppose, by induction, that \( m \) linearly disjoint Galois extensions \( K_1, \ldots, K_m \) of \( K \) have been constructed, such that \( \mathcal{G}(K_i/K) \cong G \) for \( i = 1, \ldots, m \). The field \( L = K_1 \cdots K_m \) has only a finite number, say \( n \), of subfields that contain \( K \). By assumption, there exists a Galois extension \( M \) of \( K \) such that \( \mathcal{G}(M/K) \cong G^{n+1} \). \( M \) is therefore the composition of \( n+1 \) linearly disjoint Galois extensions \( M_1, \ldots, M_{n+1} \) of \( K \) such that \( \mathcal{G}(M_i/K) \cong G \). Among the \( M_i \)'s there must be one such that \( M_j \cap L = K \), since otherwise \( M_1 \cap L, \ldots, M_{n+1} \cap L \) are \( n+1 \) distinct subfields of \( L \) that contain \( K \), which is a contradiction to the definition of \( n \). Define therefore \( K_{m+1} \) to be one of the \( M_i \)'s for which \( M_j \cap L = K \). Then \( K_1, \ldots, K_m, K_{m+1} \) are linearly disjoint over \( K \).

The sequence \( K_1, K_2, K_3, \ldots \) thus constructed satisfies the conclusion of the lemma.

3. The Normalizer of \( \langle \sigma_1, \ldots, \sigma_e \rangle \) in \( G(K) \), for \( K \) Hilbertian

Lemma 3.1. If \( K \) is a Hilbertian field, then for almost all \( (\sigma) \in G(K)^e \), for all fields \( K \leq E \leq K_\sigma(\sigma) \) and for all primes \( p \) we have \( e_p(E) \geq e \).

Proof. It suffices to prove that for a given prime \( p \), for almost all \( (\sigma) \in G(K)^e \) and for all fields \( K \leq E \leq K_\sigma(\sigma) \) we have \( e_p(E) \geq e \).

Indeed, by Theorem 2.3, there exists a linearly disjoint sequence \( K_1, K_2, K_3, \ldots \) of Galois extensions of \( K \) such that \( \mathcal{G}(K_i/K) \cong (\mathbb{Z}/p\mathbb{Z})^e \) for every \( i \geq 1 \). Let \( \sigma_1, \ldots, \sigma_e \) be generators of \( \mathcal{G}(K_i/K) \) and let

\[
S = \bigcup_{i=1}^{\infty} \{ (\sigma) \in G(K)^e | \sigma_i | K_i = \sigma_i \}.
\]

Then \( \mu(S) = 1 \), by [8, Lemma 4.1].

Suppose that \( (\sigma) \in S \) and let \( K \subseteq E \subseteq K_\sigma(\sigma) \) be an intermediate field. Let \( i \) be a positive integer such that \( \sigma_j | K_i = \sigma_i \) for \( j = 1, \ldots, e \). Then \( K_i \cap \sigma_j(\sigma) = K \), hence \( K_i \cap E = K \) too. It follows that \( (\mathbb{Z}/p\mathbb{Z})^e \) is a homomorphic image of \( \mathcal{G}(E^{(p)}/E) \). Hence \( e_p(E) \geq e \).

Theorem 3.2. Let \( K \) be a Hilbertian field. Then for almost all \( (\sigma) \in G(K)^e \) the field \( K_\sigma(\sigma) \) is a Galois extension of no proper subfield of a finite co-degree that contains \( K \).

Proof. Denote by \( S \) the set of all \( (\sigma) \in G(K)^e \) that satisfy a) \( \langle \sigma \rangle \cong \mathbb{F}_e \).

b) For all primes \( p \) and for all fields \( E \) between \( K \) and \( K_\sigma(\sigma) \) we have \( e_p(E) \geq e \).

c) \( K_\sigma(\sigma) \) contains no formally real subfield of a finite co-degree that contains \( K \).

By the free generators theorem, by Lemma 3.1 and by (F) of the introduction, \( S \) has the measure 1.

Let \( (\sigma) \in S \) and let \( F = K_\sigma(\sigma) \). Assume that there exists a field \( K \leq E \leq F \) such that \( F/E \) is a finite non trivial Galois extension. Let \( p \) be a prime divisor of \([F:E]\). By
Sylow's theorem there exists a field $E \subseteq E_1 \subseteq F$ such that $F/E_1$ is a Galois extension of degree $p$. Without loss of generality we can assume that $E_1 = E$.

The group $G(E^{(p)}/E)$ is a torsion-free $p$-group, by Lemma I.1. It contains the free pro-$p$ group $G(E^{(p)}/F)$ of rank $e$ and of index $p$ as a closed subgroup. Hence, by the theorem of Serre $G(E^{(p)}/E)$ is a free pro-$p$ group. The rank $e_p(E)$ satisfies the Nielsen-Schreier Formula $(e-1)=p(e_p(E)-1)$. Hence $e > e_p(E)$, which is a contradiction to b).

4. The Maximal $p$-Extension of Fields Underneath $K_s(\sigma)$

Having proved theorem (H) for arbitrary Hilbertian fields, we turn now to the proofs of Theorems (I), (J), and (K) for global fields $K$. In this section we consider fields $K \subseteq E \subseteq K_s(\sigma)$ and give sufficient conditions for $G(E^{(p)}/E)$ to be free. We shall use results from local class field theory. They are incorporated in the following lemma, which is a combination of Theorem 9.1, 9.3, and 9.7 of Koch [9].

**Lemma 4.1.** Let $E$ be an algebraic extension of a global field $K$. Suppose that for every non archimedean absolute value $v$ of $E$ and for every prime number $l$, the degree $[E K_v : E]$ is divisible by $l^\omega$. Suppose further that $E$ is not formally real. Then $G(E^{(p)}/E)$ is a free pro-$p$ group for every prime $p$.

The condition $"l^\omega [E K_v : E]"$ is certainly satisfied if $E_K$ is algebraically closed, because then $E K_v$ contains the separable closure of $\bar{K}_v$. We give here an additional sufficient condition for the condition to be true.

**Lemma 4.2.** Let $M$ be a non-archimedean local field and let $\tau \in G(M)$. Then $l^\omega$ divides $[M_{\tau}(\tau):M]$ for every prime $l$.

**Proof (Neukirch).** Let $l$ be a prime such that $l^\omega$ does not divide $[M_{\tau}(\tau):M]$. Without loss of generality we can assume that $\zeta_l \in M$. Our assumption implies that $N = M_{\tau}(\tau) \cap M^{(0)}$ is a finite extension of $M$. Further $M^{(0)} = N^{(0)}$ and $G(N^{(0)}/N)$ is a pro-cyclic group. This however contradicts Theorems 10.3 and 10.4 of Koch [9], according to which the rank of $G(L^{(0)}/L)$ is at least 2.

**Lemma 4.3.** Let $K$ be a global field. Then for almost all $(\sigma) \in G(K)^e$, the field $K_s(\sigma)$ has the following property: Suppose that $K_s(\sigma)$ is an algebraic separable extension of a field $E$ that contains $K$ such that $K_s(\sigma)/E$ is either finite or a pro-cyclic extension. Then for every algebraic extension $E'$ of $E$ and every prime $p$, the group $G(E^{(p)}/E')$ is pro-$p$ free.

**Proof.** Denote by $S$ the set of all $(\sigma) \in G(K)^e$ with the following properties:

a) The completion of $K_s(\sigma)$ under every absolute value is algebraically closed.

b) There does not exist a field $K \subseteq E \subseteq K_s(\sigma)$ of finite co-degree which is formally real.

By [2, Lemma 5.3] and by (F), $S$ has measure 1.

Let $(\sigma) \in S$ and let $F = K_s(\sigma)$. Let $E, E'$ be fields such that $K \subseteq E \subseteq F$, such that $F/E$ is either finite or a pro-cyclic extension and such that $E'$ is an algebraic extension of $E$. Then $E$ and hence $E'$ satisfies the conditions of Lemma 4.1 by a), b), by Artin-Schreier theorem and by Lemma 4.2. It follows that $G(E^{(p)}/E')$ is free for every prime $p$. 
5. The Trivial Normalizer Theorem, for $K$ global

We recall that a non trivial pro-$p$ group $G$ is free if and only if $\text{cd}(G)=1$ (cf. Ribes [13, p. 235]).

**Lemma 5.1.** Let $G$ be a pro-$p$ group and let $H$ be a normal closed subgroup of $G$. Suppose that both $H$ and $G/H$ are non trivial free pro-$p$ groups and $H$ is finitely generated. Then $G$ is not free.

**Proof.** Our assumptions imply that $\text{cd}(H)=\text{cd}(G/H)=1$. Further $H^1(H,F_p)$ is finite. It follows that

$$\text{cd}(G)=\text{cd}(H)+\text{cd}(G/H)=2$$

(cf. Ribes [13, p. 221]). Hence $G$ is not free.

**Theorem 5.2.** If $K$ is a global field, then for almost all $(\sigma)\in G(K)^e$ the field $K_\sigma(\sigma)$ is a Galois extension of no proper subfield that contains $K$, i.e. $\langle \sigma \rangle$ is its own normalizer in $G(K)$.

**Proof.** Denote by $S$ the set of all $(\sigma)\in G(K)^e$ such that:

a) $\langle \sigma \rangle \cong \hat{F}_e$.

b) If $E_1 \subset K_\sigma(\sigma)$ and $K_\sigma(\sigma)/E_1$ is a pro-cyclic extension, then $\mathcal{G}(E_{1}^{(p)}/E_1)$ is a free pro-$p$ group for every prime $p$.

c) $K_\sigma(\sigma)$ is a Galois extension of no proper subfield of a finite co-degree that contains $K$.

By the free generators theorem, by Lemma 4.3 and by Theorem 3.2, $S$ is of measure 1.

Let $(\sigma)\in S$ and let $F=K_\sigma(\sigma)$. Assume that there exists a proper subfield $E$ of $F$ such that $\mathcal{G}(F/E)$ is Galois. By c) the group $\mathcal{G}(F/E)$ is torsion free. Hence, by Sylow theorem for pro-finite groups there exists a field $E_1 \subset F$ such that $\mathcal{G}(F/E_1) \cong \hat{Z}_p$ for some prime $p$. By a), $\mathcal{G}(F^{(p)}/F)$ is a non trivial free pro-$p$ group. Hence $\mathcal{G}(E_1^{(p)}/E_1)$ cannot be free, by Lemma 5.1. This is however a contradiction to b).

6. On the Bottom Conjecture

We come now to the analogue of Artin-Schreier theorem.

**Theorem 6.1.** Let $K$ be a global field and let $e \geq 2$. Then for almost all $(\sigma)\in G(K)^e$, the field $F=K_\sigma(\sigma)$ has the following property:

If $F$ is a finite separable extension of a field $E$ that contains $K$, then $[F:E]$ divides $e-1$.

Moreover, let $F'$ be the Galois closure of $F/E$, let $p$ be a prime and let $q$ be the largest power of $p$ that divides $[F':E]$. Then $q \leq [F':F]$.

**Proof.** Denote by $S$ the set of all $(\sigma)\in G(K)^e$ such that:

a) $\langle \sigma \rangle \cong \hat{F}_e$.

b) For every prime $p$ and for every field $E \subset K_\sigma(\sigma)$ such that $K_\sigma(\sigma)/E$ is separable algebraic, $e_p(E) \geq e$.

c) For every prime $p$ and fields $E \subset E'$ such that $K_\sigma(\sigma)$ is a finite separable extension of $E$ and $E'$ is an algebraic extension of $E$, the group $\mathcal{G}(E'^{(p)}/E)$ is free.
Then $S$ has measure 1, by the free generators theorem, by Lemma 3.1, and by Lemma 4.3.

Let $(\sigma) \in S$ and let $F, E,$ and $F'$ be as in the theorem. Let further $p$ be a prime and let $E_1 = F \cap E^{(p)}$. Then $e_p(E_1) \leq e$, since $\mathcal{G}(E^{(p)}/E_1)$ is a homomorphic image of $\mathcal{G}(F^{(p)}/F)$. On the other hand we have, by b), that $e_p(E_1) \geq e$. Hence $e_p(E_1) = e$. Now $\mathcal{G}(E^{(p)}/E_1)$ is a closed subgroup of the free pro-$p$ group $\mathcal{G}(E^{(p)}/E)$, hence $e = 1$ $= [E_1 : E] (e_p(E) - 1)$, by Nielsen-Schreier formula. An additional use of b) implies $e_p(E) \geq e$. It follows that $e_p(E) = e$ and that $[E_1 : E] = 1$, i.e. $F \cap E^{(p)} = E$.

Denote by $p^i$ and $p^j$ the largest powers of $p$ that divide $[F : E]$ and $[F' : F]$, respectively, and let $q = p^{i+j}$. By Sylow’s theorem there exists a field $E \preceq E' \preceq F$ such that $[F' : E'] = q$. The degree $[E' : E]$ is prime to $p$, hence $E'$ is linearly disjoint from $E^{(p)}$ over $E$, hence
\[ e_p(E') \geq e. \] (1)

Also $F'/E'$ is a $p$-extension and $\mathcal{G}(E'^{(p)}/E')$ is a free pro-$p$ group, by c). Hence
\[ e_p(E') - 1 = q(e_p(E') - 1). \] (2)

Another application of Nielsen-Schreier formula gives
\[ \text{rank}(G(F')) - 1 = [F' : F](e - 1), \]
and since $e_p(E') = \text{rank}(G(F'))$ we obtain
\[ e_p(F') - 1 = [F' : F](e - 1). \] (3)

Using (1)–(3) we get that $q \leq [F' : F]$ and that $p^i$ divides $e - 1$. Since this is true for every $p$ we have that $[F : E]$ divides $e - 1$.

Our last main result is the proof of the bottom conjecture in some cases.

**Corollary 6.2.** Let $K$ be a global field and let $1 \leq e \leq 5$. Then for almost all $(\sigma) \in G(K)$ the field $K_1(\sigma)$ is a separable extension of no proper subfield $E$ of a finite co-degree that contains $K$.

**Proof.** The corollary is true for $e = 1$, by (G) and suppose therefore that $e \geq 2$. Use the notation of Theorem 6.1, let $(\sigma) \in S$ and $F = K_1(\sigma)$. Assume that there exists a field $E \preceq F$ such that $F/E$ is a finite proper separable extension.

If $e = 2$, then $[F : E]$ divides 1, which is a contradiction.

If $e = 3$, then $[F : E] = 2$. Hence $F/E$ is Galois, hence $F' = F$, $q = 2$ and $1 \geq 2$, a contradiction.

If $e = 4$, then $[F : E] = 3$ and $[F' : F]$ divides 2. Hence $q = 3$ and $2 \geq 3$, a contradiction.

Suppose that $e = 5$. Then $[F : E]$ equals 2 or 4. The case $[F : E] = 2$ gives a contradiction as in the case $e = 3$. Suppose therefore that $[F : E] = 4$. Then $[F' : F]$ divides 6. If 2 divides $[F' : F]$ then for $p = 2$ we have that $q = 8$, hence $6 \geq 8$, a contradiction. Otherwise $q = 4$, hence $3 \geq 4$, again a contradiction.

7. Infinite Counter Examples to Iwasawa-Uchida’s Theorem

Iwasawa and Uchida independently proved in [4] and [16] the following

**Theorem.** Let $K$ and $L$ be two number fields and let $\alpha : G(K) \to G(L)$ be an isomorphism of their Galois groups. Then $\alpha$ is induced by an inner automorphism of $G(\mathbb{Q})$. In particular $K$ is isomorphic to $L$. 
Our first counter example shows that the theorem does not remain true if the condition "\(K\) and \(L\) are number fields" is replaced by "\(K\) and \(L\) are algebraic extensions of \(\mathbb{Q}\)". Indeed, by Corollary 7.2 of [8] there exists a subset \(S\) of \(G(\mathbb{Q})^e\) of cardinality \(2^{8e}\) such that \(\langle \sigma \rangle \simeq \tilde{F}_e\) for every \(\sigma \in S\), but \(\tilde{Q}(\sigma) \neq \tilde{Q}(\sigma')\) for every two distinct \(e\)-tuples \((\sigma)\) and \((\sigma')\) in \(S\).

A consequence of Iwasawa-Uchida's theorem is the following

**Corollary.** Let \(K\) be a number field. Then \(G(K)\) is a complete group if and only if \(\text{Aut}\ K\) is a trivial group.

Now, Theorem 5.2 can be rephrased for \(Q\) as:

**Theorem 7.1.** The group \(\text{Aut}\ \tilde{Q}(\sigma)\) is trivial for almost all \((\sigma)\in G(\mathbb{Q})^e\).

Consider therefore, for \(e \geq 2\), a \((\sigma)\in G(\mathbb{Q})^e\) such that \(\langle \sigma \rangle \simeq \tilde{F}_e\) and such that \(\text{Aut}\ \tilde{Q}(\sigma)\) is trivial. It is known that \(\tilde{F}_e\) has a trivial center (cf. [8, Theorem 16.1]), but \(\tilde{F}_e\) is not a complete group, since it has automorphisms which are not inner. For example, if \(z_1, \ldots, z_e\) are generators of \(\tilde{F}_e\), then the automorphism induced by the map \((z_1, \ldots, z_e) \mapsto (z_1^{-1}, \ldots, z_e^{-1})\) is not inner. It follows that the corollary is false if \(K\) is replaced by \(\tilde{Q}(\sigma)\).

References

4. Iwasawa, K.: Automorphisms of Galois groups of number fields (manuscript)

Received December 5, 1977