# TRANSCENDENTAL GALOIS THEORY

PETE L. CLARK

DISCLAIMER: This is just a draft. I am not sure of the final purpose of this document, so at the moment I have included lots of known results, in particular proofs of the usual Fundamental Theorem of Galois theory (in the finite and then the algebraic case). Seeing such proofs helps (me) to understand the analogies between the Fundamental Theorem presented here and the usual cases.

Also, **CAVEAT EMPTOR**. Many of the assertions here do not appear with complete proofs. The proofs are pretty routine, except for one: at the moment I am just hoping that the claim about Galois closures of genus zero coverings is true. This claim is used to prove what is the most interesting result in the paper: namely, that a transcendental extension $K/F$ is Galois only if $K$ is algebraically closed. Please let me know if you have any ideas about how to prove this claim, and/or how to prove the deduction without it!

## 1. Introduction

The aim of this note is to give an extension of Galois theory to transcendental field extensions. What could, or should, it mean for an arbitrary field extension $K/F$ to be Galois? After reviewing the two traditional cases – finite algebraic extensions and infinite algebraic extensions – we discuss several candidate definitions and recommend for your consideration the following: $K/F$ is **Galois** iff for all subextensions $L$ of $K/F$ we have $K^{\mathrm{Aut}(K/L)} = L$. We can completely characterize the transcendental extensions[1] which satisfy this condition, and in characteristic 0 there are many such extensions. However, in characteristic $p > 0$, no transcendental extension $K/F$ is Galois in our sense: if $x$ is transcendental over $F$, then every automorphism of $K$ which fixes $x^p$ also fixes $x$, so $F(x^p) \subsetneq F(x) \subseteq K^{\mathrm{Aut}(K/F(x^p))}$.

Here is our main result:

**Theorem 1.** *(Fundamental Theorem of Galois Theory) Let $K/F$ be an extension. The following are equivalent:*
*(i) For all subextensions $L$ of $K/F$, $K^{\mathrm{Aut}(K/L)} = L$.*
*(ii) Either $K/F$ is algebraic, normal and separable, or $F$ has characteristic 0 and $K$ is algebraically closed.*

**CAVEAT EMPTOR**: In this draft we succeed in proving only (ii) $\implies$ (i).

I have vaguely wondered about transcendental Galois extensions for several years; perhaps my curiosity was whetted by Galois-like correspondences for fields of automorphic functions in Shimura's text *An Introduction to the Arithmetic Theory of Automorphic Forms*. Over the last year I became interested in the phenomenon that automorphism groups of algebraically closed fields are somehow "very big."

[1] Maybe. See the **CAVEAT EMPTOR** above.

Finally, in February of 2008 I read the first chapter of I. Kaplansky's elegant little book *Fields and Rings*, which galvanized my interest and provided essential clues.

Kaplansky's discussion of Galois theory begins in the setting of "an absolutely arbitrary" field extension $K/F$. The definition of Galois extension that he suggests is simply that $K^{\mathrm{Aut}(K/F)} = F$. We shall call such an extension **weakly Galois** and give some results comparing weakly Galois to Galois extensions. Kaplansky does not address what conditions one should impose on a transcendental extension $K/F$ to get a reasonable "Galois correspondence", but nevertheless his notes contain some preliminary results of a general nature which get specifically applied only to algebraic extensions but are still useful to us in the transcendental case. Moreover there are some enlightening exercises. In summary, Kaplansky clearly had thought deeply about transcendental Galois extensions but did not venture a Galois theory *per se*. We are pleased to offer the present note as a continuation of his ideas.

## 2. Review of Galois theory of algebraic extensions

### 2.1. Statements of the Fundamental Theorems.

The most classical case concerns extensions $K/F$ of finite degree. In this context, the fundamental theorem is as follows:

**Theorem 2.** *(Fundamental theorem of finite Galois theory) Let $K/F$ be a field extension of finite degree.*
*a) The following are equivalent:*
*(i) $K^{\mathrm{Aut}(K/F)} = F$.*
*(ii) $K/F$ is normal and separable.*
*(iii) $K/F$ is the splitting field of a separable polynomial.*
*(iv) $\# \mathrm{Aut}(K/F) = [K : F]$.*
*b) If these equivalent conditions hold then the mappings*

$$\Phi : L \mapsto \mathrm{Aut}(K/L)$$

*and*

$$\Psi : H \mapsto K^H$$

*give bijective, inclusion-reversing correspondences between the lattice of all subextensions $L$ of $K/F$ and the lattice of all subgroups $H$ of $\mathrm{Aut}(K/F)$.*
*c) A subextension $L$ is normal over $K$ iff $\mathrm{Aut}(K/L)$ is normal in $\mathrm{Aut}(K/F)$, and if so $\mathrm{Aut}(K/F)$ is canonically isomorphic to $\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$.*

Parts of this theorem extend to the case of infinite Galois extensions:

**Theorem 3.** *(Fundamental theorem of algebraic Galois theory) Let $K/F$ be an algebraic field extension.*
*a) The following are equivalent:*
*(i) $K^{\mathrm{Aut}(K/F)} = F$.*
*(ii) $K/F$ is normal and separable.*
*(iii) $K/F$ is the splitting field of a set of separable polynomials.*
*b) If these equivalent conditions hold, then $K^{\mathrm{Aut}(K/L)} = L$ for every subextension $L$ of $K/F$.*
*c) A subextension $L$ is normal over $K$ iff $\mathrm{Aut}(K/L)$ is normal in $\mathrm{Aut}(K/F)$, and if so $\mathrm{Aut}(K/F)$ is canonically isomorphic to $\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$.*

Note that there are several parts of Theorem 2 which do not appear in Theorem 3. Both theorems assert that every subextension $L$ is of the form $K^H$ for some subgroup $H$ – in fact, necessarily for $H = \mathrm{Aut}(K/L)$. Theorem 2 also asserts that every subgroup $H$ of $\mathrm{Aut}(K/F)$ is of the form $\mathrm{Aut}(K/L)$ for some subextension $L$ – in fact, necessarily for $L = K^H$. But this fails for all infinite algebraic Galois extensions: there will be subgroups $H$ of $\mathrm{Aut}(K/H)$ which are proper in $\mathrm{Aut}(K/K^H)$. Let us call a subgroup $H$ of $\mathrm{Aut}(K/F)$ **closed** if $H = \mathrm{Aut}(K/K^H)$.

The existence of nonclosed subgroups of $\mathrm{Aut}(K/F)$ in infinite algebraic Galois theory is usually not problematic, because of a nice interpretation of in this case due to W. Krull. By "dualizing" the fact that any algebraic extension $K/F$ is the direct limit of its finite degree normal subextensions, one finds that the automorphism group $\mathrm{Aut}(K/F)$ of an infinite Galois extension is canonically isomorphic to the inverse limit of the Galois groups $\mathrm{Aut}(L/F)$ of the finite degree normal subextensions $L/K$. Endowing each finite quotient with the discrete topology and $G = \mathrm{Aut}(K/F)$ with the inverse limit topology, $G$ becomes a topological group which is an inverse limit of compact, Hausdorff totally disconnected spaces, so is itself a compact, Hausdorff totally disconnected topological group, or a **profinite group**. A subgroup $H \subset G$ is closed with respect to the Krull topology iff it is closed in the above sense: $H = c(H) = \mathrm{Gal}(K/K^H)$. The automorphism group of an infinite algebraic Galois extension has infinitely many closed normal subgroups, whose fixed fields are precisely the normal subextensions $L$ of $K/F$.

In order to see what is going on, it is helpful to consider the correspondence between subgroups of $\mathrm{Aut}(K/F)$ and subextensions of $K/F$ in the most general case.

### 2.2. **The abstract Galois correspondence.**

For an arbitrary field extension $K/F$, define $\mathcal{L} = \mathcal{L}(K/F)$ to be the lattice of subextensions $L$ of $K/F$ and $\mathcal{H} = \mathcal{H}(K/F)$ to be the lattice of all subgroups $H$ of $G = \mathrm{Aut}(K/F)$. Then we have

$$\Phi : \mathcal{L} \to \mathcal{H},\ L \mapsto \mathrm{Aut}(K/L)$$

and

$$\Psi : \mathcal{H} \to \mathcal{F},\ H \mapsto K^H.$$

For $L \in \mathcal{L}$, we write

$$c(L) := \Psi(\Phi(L)) = K^{\mathrm{Aut}(K/L)}.$$

One immediately verifies:

$$L \subset L' \implies c(L) \subset c(L'),\ L \subset c(L),\ c(c(L)) = c(L);$$

these properties assert that $L \mapsto c(L)$ is a **closure operator** on the lattice $\mathcal{L}$ in the sense of order theory. Quite similarly, for $H \in \mathcal{H}$, we write

$$c(H) := \Phi(\Psi(H)) = \mathrm{Aut}(K/K^H)$$

and observe

$$H \subset H' \implies c(H) \subset c(H'),\ H \subset c(H),\ c(c(H)) = c(H),$$

so $c$ is a closure operator on $\mathcal{H}$. A subextension $L$ (resp. a subgroup $H$) is said to be **closed** if $L = c(L)$ (resp. $H = c(H)$). If we write $\mathcal{L}_c$ (resp. $\mathcal{H}_c$) for the subset of closed subextensions (resp. closed subgroups), then one immediately verifies that $\Phi$ and $\Psi$ give mutually inverse bijections between $\mathcal{L}_c$ and $\mathcal{H}_c$.

## 2.3. **Galois connections.**

The abstract Galois correpondencehas been further generalized to the notion of a **Galois connection** between two partially ordered sets, a concept which perhaps deserves to be more widely known. An ("antitone") Galois connection between two partially ordered sets $\mathcal{X}$ and $\mathcal{Y}$ is a pair of set maps $\Phi : \mathcal{X} \rightarrow \mathcal{Y}$, $\Psi : \mathcal{Y} \rightarrow \mathcal{X}$ satisfying:

(GC1) $x_1 \leq x_2 \implies \Phi(x_2) \leq \Phi(x_1)$; $y_1 \leq y_2 \implies \Psi(y_2) \leq \Psi(y_1)$,
(GC2) For $x \in X$, $y \in Y$, $\Phi(x) \leq y \iff \Psi(y) \leq x$.

As above, the composition $\Psi \circ \Phi$ (resp. $\Phi \circ \Psi$) gives a closure operator $x \mapsto c(x)$ on $\mathcal{X}$ (resp. $y \mapsto c(y)$ on $\mathcal{Y}$), and $\Phi$ and $\Psi$ are mutually inverse maps from the subposet $\mathcal{X}_c$ of closed elements of $\mathcal{X}$ to the subposet $\mathcal{Y}_c$ of closed elements of $\mathcal{Y}$.

In case the posets $\mathcal{X}$ and $\mathcal{Y}$ are **lattices** – i.e., for $x_1, x_2 \in \mathcal{X}$ there exists a unique greatest lower bound $x_1 \wedge x_2$ and a unique least upper bound $x_1 \vee x_2$ (and similarly for $\mathcal{Y}$), then $\Phi(x_1 \wedge x_2) = \Phi(x_1) \vee \Phi(x_2)$, $\Phi(x_1 \vee x_2) = \Phi(x_1) \wedge \Phi(x_2)$, $c(x_1 \wedge x_2) = c(x_1) \wedge c(x_2)$, $c(x_1 \vee x_2) = c(x_1) \vee c(x_2)$. By symmetry, the same properties hold for elements of $\mathcal{Y}$. If $\mathcal{X}$ and $\mathcal{Y}$ are **complete lattices** – i.e., unique greatest lower bounds and least upper bounds exist for arbitrary subsets, then all the above relations hold for arbitrary sets of elements.

Example 2.3.1: If $k$ is an algebraically closed field, the map $\Phi$ which associates to an ideal $I$ in $k[x_1, \ldots, x_n]$ the subset $V(I)$ of $k^n$ of simultaneous zeros of the elements of $I$ and the map $\Psi$ which associates to a subset $S \subset k^n$ the ideal $I(S)$ of all polynomials which vanish on every element of $S$ give a Galois connection. It is easy to check (e.g. [3, Thm. IX.2.1, p. 381]) that the closure operator on subsets satisfies $c(S_1 \cup S_2) = c(S_1) \cup c(S_2)$ – note however that this identity is not a formal consequence of the axioms for a Galois connection – and thus $c$ is the topological closure operator for a unique topology on $k^n$ [2, Thm. 8, p. 42], the **Zariski topology**. Identification of the closure operator on ideals is the content of Hilbert's **Nullstellensatz** [3, Thm. IX.1.5, p. 380]:

$$c(I) = \mathrm{rad}(I) = \{f \mid (\exists n \in \mathbb{Z}^+) \ f^n \in I\}.$$

There are many equally familiar and most important examples. The following is a generalization of the abstract Galois correspondence of the previous section.

Example 2.3.2: Let $X$ be a set and $G$ be a group acting on $X$. The maps:

$$\Phi : Y \subset X \mapsto G_Y := \{g \in G \mid \forall y \in Y \ gy = y\},$$

$$\Psi : H \subset G \mapsto X^G := \{y \in X \mid \forall g \in H \ gy = y\}$$

give a Galois connection between the complete lattice $2^X$ of all subsets of $X$ and the complete lattice of all subgroups of $G$.

This formalism gives a "clean, well-lighted place" to work out the relationship between normal subgroups and normal field extensions in classical Galois theory:

**Proposition 4.** *Let $H$ be a subgroup of $G$, $Y$ a subset of $X$ and $\sigma \in G$. We have:*
*a) $\sigma G_Y \sigma^{-1} = G_{\sigma Y}$.*
*b) $\sigma X^H = X^{\sigma H \sigma^{-1}}$.*

Proof: We have $g \in G_{\sigma Y} \iff \forall y \in Y,\ g\sigma y = \sigma y \iff \forall y \in Y,\ \sigma^{-1} g \sigma y = y \iff \sigma^{-1} g \sigma \in G_Y \iff g \in \sigma G_Y \sigma^{-1}$. Similarly, $y \in \sigma X^H \iff \sigma^{-1} y \in X^H \iff \forall h \in h,\ h\sigma^{-1} y = \sigma^{-1} y \iff \forall h \in H,\ (\sigma h \sigma^{-1}) y = y \iff y \in \sigma H \sigma^{-1}$.

We deduce:

**Corollary 5.**
*a) A closed subgroup $H$ of $G$ is normal iff the corresponding closed subset $X^H$ is stable under the action of $G$: $\forall \sigma \in G$, $\sigma X^H = X^H$.*
*b) A closed subset $Y$ of $X$ is stable under the action of $G$ iff the corresponding closed subgroup $G_Y$ is normal in $G$.*
*c) The closure of a normal subgroup (resp. a stable subset) is normal (resp. stable).*

Applying this to the case of a field extension $K/F$, we get:

**Corollary 6.** *Let $L$ be a subextension of the extension $K/F$. Put $G = \mathrm{Aut}(K/F)$.*
*a) If $L = K^{\mathrm{Aut}(K/L)}$, then $L$ is $G$-stable iff $\mathrm{Aut}(K/L)$ is a normal subgroup of $G$.*
*b) If $\mathrm{Aut}(K/L)$ is normal in $G$, then the quotient $\mathrm{Aut}(K/F)/\mathrm{Aut}(L/F)$ is canonically isomorphic to the group of all $F$-algebra automorphisms of $L$ which can be extended to $K$.*

For the (routine) proofs of Corollaries 5 and 6 see pages 19-22 of [1].

### 2.4. **Proofs of the Fundamental Theorems.**

The proof of Theorems 2 and 3 requires more than just the "general nonsense" of Galois connections, of course. We need the following two results:

**Theorem 7.** *For an algebraic field extension $K/F$, TFAE:*
*(i) For every $F$-algebra embedding $\sigma$ of $K$ into an algebraic closure $\overline{K}$, $\sigma(K) = K$.*
*(ii) Every irreducible polynomial $P \in F[t]$ with a root in $K$ splits completely in $K$.*
*(iii) $K^{\mathrm{Aut}(K/F)}/F$ is purely inseparable.*

Proof: ...

In particular we deduce that an algebraic extension $K/F$ satisfies the condition $K^{\mathrm{Aut}(K/F)}) = F$ iff it is normal and separable. It is immediate that if $K/F$ is normal and separable and $L$ is a subextension, then $K/L$ is normal and separable, hence $K^{\mathrm{Aut}(K/L)} = L$.

**Theorem 8.** *(Artin-Kaplansky Index Theorem)*
*a) Let $F \subset L \subset M \subset K$ be fields. Suppose that $L$ is closed and $[M : L] = n < \infty$. Then $M$ is also closed, and $[\mathrm{Aut}(K/L) : \mathrm{Aut}(K/M)] = n$.*
*b) Let $H \subset J \subset \mathrm{Aut}(K/F)$. Suppose that $H$ is closed and $[J : H] = n < \infty$. Then $J$ is also closed, and $[K^H : K^J] = n$.*

Proof: This is Theorem 8 of [1].

The Index Theorem implies that in the case of a finite Galois extension, all subgroups and subextensions are closed, and then the other parts of Theorem 2 follow immediately. In the case of an infinite algebraic extension $K/F$, we know that the extension is normal and separable iff $K^{\mathrm{Aut}(K/F)} = F$. Thus $F$ is closed and by Theorem 8b) every finite subextension $L$ of $K/F$ is also closed. Since every subextension $L$ of the algebraic extension $K/F$ is a directed union of its finite subextensions, the formal lattice-theoretic properties of a Galois connection imply that $L$ is closed as well. This proves Theorem 3.

There is however another part of Theorem 2 which does not generalize to infinite Galois extensions: for a finite extension $K/F$ we have $\# \mathrm{Aut}(K/F) \leq [K : F]$, with equality iff $K/F$ is Galois. When $K/F$ is an infinite algebraic Galois extension, $\mathrm{Aut}(K/F)$ is an infinite group, and condition (iv) of Theorem 2a) is certainly meaningful as an assertion about cardinalities of infinite sets. However it is false:

**Theorem 9.** *Let $K/F$ is an infinite algebraic Galois extension. Then:*
*a)* $[K : F] < \# \mathrm{Aut}(K/F)$.
*b) There is a dense subgroup $H \subset \mathrm{Aut}(K/F)$ with $\#H = \#[K : F]$.*

Proof: ...

This result shows that the automorphism group of an infinite algebraic Galois extension is in some sense **very big**; in particular, a much smaller subgroup, namely the subgroup $H$ of part b), would still have the property $K^H = F$.

## 3. Variations on the definition of Galois

The definition of Galois we suggested in the introduction – $K^{\mathrm{Gal}(K/L)} = L$ for all subextensions $L/K$ – is equivalent to requiring that in the formal Galois correspondence every subextension $L$ is closed, but not necessarily that every subgroup is closed. In making this definition we are making no further concessions than what was necessary to move from finite to infinite algebraic Galois theory, so it seems at least plausible. Let us compare it with several other possible definitions:

Call an extension $K/F$ **classically Galois** if in the formal Galois correspondence we have $c(L) = L$ for every subextension and also $c(H) = H$ for every subgroup. This is how it goes for finite Galois extensions, but of course the case of infinite Galois extensions suggests that this is probably too much to ask. Indeed:

**Theorem 10.** *$K/F$ is classically Galois iff it is finite, normal and separable.*

The theorem was first proved in 1965 by Venkataraman and Soundararajan [5]. However, since a classically Galois extension is Galois, we ought to be able to deduce it from our "fundamental" Theorem 1. We shall do so in Section 4.

Here is another try: since the standard definition of an algebraic Galois extension is one which is algebraic, normal and separable, it seems natural to ponder, at least for a little while, whether one could define normality and separability for arbitrary extensions and then define a Galois extension as one which is normal and separable.

For algebraic extensions, normality and separability can both be characterized in terms of polynomials. So one might define $K/F$ to be **polynomially normal** if every irreducible polynomial in $F$ with a root in $K$ splits completely in $K$, **polynomially separable** if every irreducible polynomial in $F$ with a root in $K$ splits into distinct linear factors in an algebraic closure of $K$, and **polynomially Galois** to be polynomially normal and polynomially separable.

But this can't be what we want, because $K/F$ is polynomially Galois whenever $F$ is algebraically closed, but we may well have $F$ algebraically closed and $\# \operatorname{Aut}(K/F) = 1$; e.g. this happens when $F = \mathbb{C}$ and $K$ is the field of meromorphic functions on a sufficiently general compact Riemann surface of genus $g > 2$. In fact it is easy to see that $K/F$ is polynomially Galois iff the algebraic closure $F^c$ of $F$ in $K$ is Galois over $F$ in the usual sense.

Of course one might conceivably want to try again with a less naive definition of normality. Say that $K/F$ is **normal** if $K^{\operatorname{Aut}(K/F)}$ is algebraic and purely inseparable. Evidently $K^{\operatorname{Aut}(K/F)}) = F$ iff $K/F$ is normal and polynomially separable. We will call a normal, polynomially separable extension **weakly Galois**.

**Proposition 11.** *Let $K/F$ be a field extension.*
*a) If $K/F$ is normal, it is polynomially normal.*
*b) If $K/F$ is polynomially normal and algebraic, it is normal.*
*c) Thus, if $K/F$ is algebraic, it is Galois iff it is weakly Galois.*

Proof: This is just a restatement of Theorem 7.

It is interesting to note that "weakly Galois" is the condition that Kaplansky suggests as the analogue of a Galois extension.[2]

**Theorem 12.** *Let $K/F$ be a purely transcendental extension.*
*a) If $F$ is infinite, $K/F$ is weakly Galois iff it has transcendence degree at least* 1.
*b) If $F$ is finite, $K/F$ is weakly Galois iff it has transcendence degree at least* 2.

Proof: ...

Example (Kaplansky): By Theorem 12, $\mathbb{Q}(t)/\mathbb{Q}$ is weakly Galois. If it were Galois then the finite extension $\mathbb{Q}(t)/\mathbb{Q}(t^3)$ would be Galois; by Proposition 11 this means that it is Galois in the usual sense. But of course $\mathbb{Q}(t)/\mathbb{Q}(t^3)$ is nonnormal: its normal closure contains a primitive cube root of unity.

This example exploits the non-algebraic closure of the base field, but this is not essential: a special case of the Fundamental Theorem is that any nontrivial purely transcendental extension is not Galois.

**Theorem 13.** *A nontrivial finitely generated regular extension $K/F$ of* general type *has* $\operatorname{Aut}(K/F)$ *finite and is therefore not weakly Galois.*

[2]To be precise, Kaplansky does not refer to any field extension as "Galois": where we write "weakly Galois" he writes "normal"; and where we write "normal algebraic" he writes "splitting field."

Proof: REFERENCE??

More precise results are available for one-dimensional function fields:

**Theorem 14.** *For an absolutely integral algebraic curve $C/k$, the extension $k(C)/k$ is weakly Galois iff $k$ is infinite and one of the following conditions hold:*
*(i) $C$ has genus $0$;*
*(ii) $C$ has genus $1$ and its Jacobian $\mathrm{Pic}^0(C)$ has infinitely many $k$-rational points.*

We begin the proof with the following result.

**Lemma 15.** *The extension $k(C)/k$ is Galois iff $G = \mathrm{Aut}(k(C)/k)$ is infinite.*

Proof: We have $k \hookrightarrow k(C)^G \hookrightarrow k(C)$. Clearly $[k(C) : k] = \infty$, so if $G$ is finite, $[k(C) : k(C)^G]$ is finite and then $[k(C)^G : k]$ is infinite, so $k \neq k(C)^G$. Conversely, if $[k(C) : k(C)^G]$ is infinite, then $k(C)/k(C)^G$ is transcendental, and that implies $k(C)^G = k$. (More details would be nice, but this is true...)

Now it is known the automorphism group of any curve $C/k$ is an algebraic group over $k$, so if $k$ is finite, the automorphism group is finite. So suppose $k$ is infinite. If $C$ has genus at least 2, then again it is known that the automorphism group of $C/k$ is finite. If $C$ has genus 1, then $\mathrm{Aut}(C/k)$ contains, as a finite index subgroup, the group $\mathrm{Pic}^0(C)(k)$ of $k$-rational points on the Jacobian. Therefore $k(C)/k)$ is Galois iff the Jacobian has infinitely many $k$-rational points. If $C$ has genus 0, its automorphism group is $PGL_2(k)$ if $C \cong \mathbb{P}^1$; otherwise $C$ corresponds to a division quaternion algebra $B/k$ and the automorphism group is $B^\times/k^\times$. Both of these groups are infinite when $k$ is infinite.

These considerations suggest that it will be difficult to classify all weakly Galois extensions: on the one hand there are many more weakly Galois extensions than Galois extensions. On the other hand Theorem 14 shows that whether a function field is weakly Galois is a rather subtle arithmetic question: e.g. we do not know an algorithm to decide whether an elliptic function field $\mathbb{Q}(E)/\mathbb{Q}$ is weakly Galois.

## 4. Proof of the Fundamental Theorem

### 4.1. Some results on automorphism groups of algebraically closed fields.

**Lemma 16.** *Let $K/L/F$ be a tower of field extensions, with $K$ algebraically closed.*
*a) Any $F$-algebra embedding $\iota : L \hookrightarrow K$ extends to an $F$-algebra embedding $K \hookrightarrow K$.*
*b) Any $F$-algebra automorphism of $L$ extends to an $F$-algebra automorphism of $K$.*

Proof: ...

(What happens for separably closed extensions?)

We will now give a result making precise the slogan that closed subgroups of the automorphism group of an algebraically closed field are "very big."

**Theorem 17.** *Let $K/F$ be an extension of infinite degree, with $K$ algebraically closed of characteristic $0$.*
*a) $\# \mathrm{Aut}(K/F) > [K : F]$.*
*b) There exists $H \subset \mathrm{Aut}(K/F)$, $\#H = [K : F]$ such that $K^H = F$.*

Proof: ...

Proof of Theorem 10: Let $K/F$ be an infinite classically Galois extension. In particular every subextension is closed, i.e., $K/F$ is Galois, so by the Fundamental Theorem the two cases are $K/F$ algebraic, normal and separable, or $K$ algebraically closed of characteristic 0. The first case is covered by Theorem 9 and the second case is covered by Theorem 17.

### 4.2. **Proof of the Fundamental Theorem.**

**Proposition 18.** *Suppose $K/F$ is an extension with $K$ algebraically closed. Then $K^{\mathrm{Aut}(K/F)} = F^{p^{-\infty}}$, the perfect closure of $F$. In particular, if $F$ is perfect and $K$ is algebraically closed then $K/F$ is weakly Galois.*

Let $x$ be an element of $K$ which is not purely inseparable algebraic over $x$. We claim there is an automorphism $\sigma$ of $K$ such that $\sigma(x) \neq x$.

Case 1: $x$ is algebraic over $F$. Then the minimal polynomial $P(t)$ of $x$ over $F$ has at least one distinct root $x'$ in $K$. The map $x \mapsto x'$ determines a unique $F$-algebra isomorphism $\sigma : F[x] \rightarrow F[x']$, which can be extended to an $F$-algebra automorphism $\sigma$ of $\overline{F}$, the algebraic closure of $F$ in $K$. By Lemma 16b), $\sigma$ extends to an automorphism of $K$.
Case 2: $x$ is transcendental over $F$. Then, for instance, the map $x \mapsto x + 1$ induces an $F$-algebra automorphism of the pure transcendental extension $F(x)$, which by Lemma 16b) extends to an automorphism of $K$. This completes the proof.

The implication (i) $\implies$ (ii) in Theorem 1 follows immediately upon applying Proposition 18 to each subextension $L$ of $K/F$.

Conversely, suppose $F$ has characteristic 0, $K/F$ is a transcendental extension. We first reduce to the case of an extension of transendence degree one. Let $\overline{K}$ be an algebraic closure of $K$. Fix a transcendental element $t$ of $K$ and let $\{t, x_i\}$ be a transcendence basis of $K/F$. Put $F' = F(\{x_i\}$, so that we have a tower of fields

$$F \subset F' \subset F'(t) \subset K \subset \overline{K},$$

so it suffices to show that if $K/F'$ is Galois, $\overline{K} = K$.

Let $f(t) \in F'(t)$ be a nonconstant rational function, so that $F'(t)/F'(f(t))$ is a finite extension. If $K/F$ is Galois, then the algebraic extension $K/F'(f(t))$ must be Galois in the usual sense. In particular it must contain the normal closure $M_f$ of $F'(t)/F'(f(t))$. We claim that the compositum of the fields $M_f$ is $\overline{K}$, the algebraic closure of $F'(t)$. (REFERENCE??) This completes the proof of the theorem.

## 5. Normal subgroups

Let $K/F$ be a field extension and $L$ a subextension. As in §$X.X$, we say that $L$ is **stable** if $\sigma(L) \subset L$ for all $\sigma \in \mathrm{Aut}(K/F)$. By considering the action of $\sigma^{-1}$, the condition is seen to be equivalent to $\sigma(L) = L$ for all $\sigma \in \mathrm{Aut}(K/F)$.

Let $K/F$ be a Galois extension. By Corollary 6, a subextension $L$ is stable iff $\mathrm{Aut}(K/L)$ is normal, and if this is the case, the quotient $\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$ is isomorphic to the subgroup of $\mathrm{Aut}(L/F)$ consisting of automorphisms that can be extended to $K$.

Now suppose $K$ is algebraically closed; then by Lemma XX, $\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L) = \mathrm{Aut}(L/F)$. But what are the stable subfields of $K/F$?

**Theorem 19.** *If $K/F$ is an extension with $K$ algebraically closed, then a subextension $L$ is stable iff $L = K$ or $L$ is algebraic and normal over $F$.*

Proof: Let $\overline{F}$ be the algebraic closure of $F$ in $K$ – it is, in particular, an algebraic closure of $F$. Clearly for any $x \in K$ and $\sigma \in \mathrm{Aut}(K/F)$, $x$ is algebraic over $F$ iff $\sigma(x)$ is algebraic over $F$, so that $\overline{F}$ is stable. Moreover, as is well known, if $L$ is a normal algebraic extension of $F$, it is the splitting field of a set $S$ of polynomials with coefficients in $F$, and then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma(L)$ is the splitting field of $\sigma(S) = S$, so $\sigma(L) = L$.

Conversely, of course if $L/F$ is algebraic but not normal, then there exists an irreducible polynomial $P \in F[t]$ with a root $x \in L$ and another root $x' \in \overline{F} \setminus L$, and then we can build an $F$-automorphism of $K$ which sends $x$ to $x'$, so $L$ is not stable. Suppose now that $x \in L$ is transcendental over $L$. By the theory of automorphisms of algebraically closed fields, we know that the orbit of $x$ under $\mathrm{Aut}(K/F)$ is the set of all elements of $K$ which are transcendental over $F$, so if $L$ is stable it must contain all such elements. Moreover, if $y \in K$ is algebraic over $F$ then $x + y$ is transcendental over $F$, so $x + y \in L$ and therefore $x \in L$. That is, $L = K$.

Let $K/F$ be an extension with $K$ algebraically closed. Let $\overline{F}$ be the algebraic closure of $F$ in $K$. Then every proper closed normal subgroup of $\mathrm{Aut}(K/F)$ is contained in $\mathrm{Aut}(K/\overline{F})$. In fact more is true:

**Theorem 20.** *(Lascar, [4]) If $K/F$ is an extension of fields, with both $F$ and $K$ algebraically closed, then* $\mathrm{Aut}(K/F)$ *is a simple group.*

Thus whenever $K$ is algebraically closed we have a short exact sequence

$$1 \to \mathrm{Aut}(K/\overline{F}) \to \mathrm{Aut}(K/F) \to \mathrm{Aut}(\overline{F}/F) \to 1$$

exhibiting $\mathrm{Aut}(K/F)$ as an extension of a **residually finite** group – that is, every nontrivial element remains nontrivial in some finite quotient – by a simple group.

## References

[1] I. Kaplansky, *Fields and rings ...*

[2] J.L. Kelley, *General Topology ...*

[3] S. Lang, *Algebra, Revised 3rd edition. ...*

[4] D. Lascar, **The group of automorphisms of the field of complex numbers leaving fixed the algebraic numbers is simple**. *Model theory of groups and automorphism groups (Balubeuren, 1995)*, 110-114, London Math. soc. Lecture Note Ser., 244, Cambridge Univ. Press, Cambridge, 1997.

[5] M. Venkataraman and T. Soundararajan, *On the completeness of Galois theories.* J. Austral. Math. Soc. 5 (1965), 374-379.