Fundamental theorems of Galois theory

Andry N. Rabenantoandro

Talk given at the postgraduate seminar at Stellenbosch University
on the 3rd of September 2012

Abstract

Let $L$ be an algebraic Galois extension of $K$. The fundamental theorem of Galois theory for finite extensions describes nicely a bijective correspondance between the subgroups of $\text{Gal}(L/K)$ and the intermediate fields extensions of $K$ contained in $L$. On the other hand, for infinite Galois extensions it turns out that there are more groups than intermediate fields extensions. However, there exists a one to one correspondance between the intermediate fields and the subgroups of $\text{Gal}(L/K)$ that arise as closed sets of a canonical topology defined on $\text{Gal}(L/K)$: the Krull topology. In this talk I would like to give a description of these fundamental theorems.

The main reference for the talk is the book of Patrick Morandi entitled "Field and Galois theory". I find it particularly nice, with a lot of examples, and it gives a nice treatment of the Galois theory of infinite extensions which is not always treated in the many books at our disposal.

1 Introduction

The aim of this talk is to give the audience an idea of what is involved in the so called fundamental theorems of Galois theory without too much technical details. In this line we will avoid to "prove" and instead give simple examples as illustrations.

The Abel-Ruffini Theorem states that, in general, polynomial equations of degree $\geq 5$ in one variable are not solvable by radicals. There are of course polynomials that can be solved by radicals, for example $(x - 1)^n$ for $n \in \mathbb{N}$, and those that can’t be so solved like $x^5 - x + 1 = 0$. Evariste Galois was the first to give the precise criterion for a polynomial equation to be or not to be solvable by radicals by looking at the permutation group of the roots: it was the birth of Galois Theory. The modern formulation of Galois theory in terms of automorphisms of fields extensions was initiated among others by Artin, Dedekind, kronecker and constitutes a "bridge" between group theory and field theory. This is the approach we are going to adopt.
It is worth saying that Galois theory have been used to solve many other old mathematical problems: compass and straightedge construction, characterization of regular constructible polygons, trisection of angles using compass and straightedge, ... but we will not worry about that.

We shall need a good acquaintance with field theory to state our main theorems, so let’s start by that.

2 Field Theory

From now on \( L \) will be an algebraic extension of the field \( K \), which roughly means that every element of \( L \) is a root of some \( f(x) \in K[x] \), for example \( [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \) and \( [\mathbb{C} : \mathbb{R}] \) are algebraic extensions.

**Definition 2.1.** The *Galois group* of \( L \) over \( K \) is defined by \( \text{Gal}(L/K) := \{ \sigma \in \text{Aut}(L) / \sigma(a) = a \ \forall a \in K \} \) i.e. the set of all the automorphisms of \( L \) that leave the elements of \( K \) fixed.

**Definition 2.2.** For \( S \subseteq \text{Aut}(L) \), the *fixed field* of \( S \) is defined by \( \text{Fix}(S) := \{ a \in L / \sigma(a) = a \ \forall \sigma \in S \} \).

We say that a polynomial \( f(x) \in K[x] \) splits over \( L \) if \( f(x) = a \prod (x - \alpha_i) \in K[x] \) for some \( \alpha_1, \ldots, \alpha_n \in L \) and \( a \in K \).

**Definition 2.3.** Let \( P \) be a family of polynomials \( \in K[x] \). Then \( L \) is said to be a splitting field of \( P \) over \( K \) if each \( f \in P \) splits over \( L \) and \( L = K(X) \) where \( X \) is the set of all the roots of all the elements of \( P \).

For instance \( \mathbb{C} \) is the splitting field of \( x^2+1 \) (we mean \( \{x^2+1\} \) over \( \mathbb{R} \) since \( \mathbb{C} = \mathbb{R}(i, -i) \)), \( \mathbb{F}_2(\alpha) \) is the splitting field of \( x^2+x+1 \) over \( \mathbb{F}_2 \) where \( \alpha \) is the class of \( x \) in \( \mathbb{F}_2[x]/(x^2+x+1) \) and the roots being \( \alpha \) and \( \alpha + 1 \). The splitting fields always exists and the existence rely on Zorn’s lemma (equivalent to the axiome of choice).

**Definition 2.4.** \( L \) is normal over \( K \) if \( L \) is the splitting field of a family of polynomials over \( K \). An equivalent statement is that every irreducible polynomial in \( K[x] \) which has a root in \( L \) factors into linear factors in \( L[x] \).\(^2\)

For example the above extension \( [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \) is normal but \( [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \) is not since the minimal polynomial of \( \sqrt[3]{2} \), which is \( x^3 - 2 \), is irreducible over \( \mathbb{Q} \) and has only one root in \( \mathbb{Q}(\sqrt[3]{2}) \) (the two other roots are non real). Any extension of degree two is normal.

An irreducible polynomial \( f(x) \in K[x] \) is said to be separable over \( K \) if \( f \) has no repeated roots in any splitting field and a polynomial \( g(x) \in K[x] \) is separable over \( k \) if all its irreducible factors are separable over \( K \).

---

\(^1\)It is indeed a field
\(^2\)There are others equivalent statements but we stick ourselves to these two.
Definition 2.5. Let $\alpha \in L$, we say that $\alpha$ is separable over $K$ if $\min(K, \alpha)$ is separable over $K$. If every element of $L$ is separable over $K$ then $L$ is said to be a separable extension of $K$.

Every algebraic extension of a field of characteristic zero is separable. On the other hand $\mathbb{F}_q(x)/\mathbb{F}_q(x^p)$ (where $p$ is a prime and $q = p^s$ for some $s$) is not separable since $\min(\mathbb{F}_q(x^p), x) = t^p - x^p$ has only $x$ as root.

The notion of normality and separability are the two conditions that a field extension must have for it's Galois group to be "well behaved". Let's illustrate what we mean by "well behaved" with an example.

Example 2.6. The following describes how Galois solved the problem of solvability by radicals of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n$. Consider the set \{\(a_1, \ldots, a_n\}\} of the roots of $f$ in a splitting field, the $a_i$ are distinct since $f$ is irreducible over $\mathbb{Q}$ (irreducible polynomial over a field of characteristic zero is separable). Now, let $G$ be the group of all the permutations of \{\(a_1, \ldots, a_n\}\} that leave the algebraic relations\(^3\) between the roots true, $G$ is called the Galois group of $f$. For example, $x^2 - 2$ is irreducible over $\mathbb{Q}$ and the roots are $a_1 = \sqrt{2}$ and $a_2 = -\sqrt{2}$ which satisfy the algebraic relation $x_1 + x_2 = 0$. The permutation that swap $a_1$ and $a_2$ leaves this relation true ($x_2 + x_1 = 0$).

Galois proved that $f$ is solvable by radicals if and only if the group $G$ is solvable\(^4\), this gives us a shift to group theory. We can interpret this in the modern language of field extensions: the group $G$ is in fact $\text{Gal}(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q})$, the set of all the elements of $\text{Aut}(\mathbb{Q}(a_1, \ldots, a_n))$ that leave $\mathbb{Q}$ fixed (more precisely $\text{Fix}(\text{Gal}(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}) = \mathbb{Q}$), and $\sigma \in \text{Gal}(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q})$ is determined by the image of the $a_i$'s (which are still roots of $f$, and this give a permutation of the roots!). The fact that $\sigma$ is an automorphism expresses the preservation of the "truth" of the algebraic relations between the $a_i$'s. The extension $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}$ is a typical example of extensions that are both normal and separable.

Definition 2.7. The extension $L/K$ is said to be Galois if the following equivalent statements hold:

(i) $L$ is both normal and separable,

(ii) $\text{Fix}(\text{Gal}(L/K)) = K$.

There are still other equivalent statements that we do not give here.

3 Finite extension

We let $L/K$ be a finite Galois extension. We can now describe the intermediate fields extensions $F$ of $K$ contained in $L$ in terms of the Galois groups $\text{Gal}(L/F)$. This allows one to translate questions about the intermediate fields into problems about (finite) groups.

\(^3\) An algebraic relation between the $a_i$'s is an equation of the form $P(a_1, \ldots, a_n) = 0$ where $P \in \mathbb{Q}[x_1, \ldots, x_n]$.

\(^4\) See any good book on group theory.
Theorem 3.8. (Fundamental theorem of Galois theory) The map \( F \mapsto \text{Gal}(L/F) \) from the set of all intermediate fields extensions of \( K \) contained in \( L \) to the set of all subgroups of \( \text{Gal}(L/K) \) defines a bijective inclusion reversing correspondence, the inverse is given by \( H \mapsto \text{Fix}(H) \). Furthermore, \( |\text{Gal}(L/F)| = [L : F] \) and \( [F : K] = [\text{Gal}(L/K) : \text{Gal}(L/F)] \). Moreover, \( \text{Gal}(L/F) \triangleleft \text{Gal}(L/K) \) if and only if \( F \) is Galois over \( K \) and when this holds we have \( \text{Gal}(F/K) \cong \text{Gal}(L/F)/\text{Gal}(L/K) \).

This theorem tells us that there is a certain symmetry between the intermediate fields and the subgroups of \( \text{Gal}(L/K) \). However, if the extension is infinite this symmetry breaks down: not all the subgroups of \( \text{Gal}(L/K) \) arise as a Galois group of the form \( \text{Gal}(L/F) \) for some intermediate extension \( F \), there are more subgroups than extensions. There is however an analogue of Theorem 3.8 which describes the subgroups that arise as Galois groups of some intermediate extensions by introducing a topology on \( \text{Gal}(L/K) \) called the Krull topology, in reference to Wolfgang Krull who first introduced the idea in the 1920’s.

4 Infinite extension

4.1 A bit of topology
In this section we define topological notions that we will need in the formulation of the fundamental theorem, we assume basics on topology.

Let \( X \) be a given non-empty set. A natural question is whether we can generate a topology on \( X \), of course apart from the trivial and discrete topology. The answer is yes in general. It can be done by specifying the neighbourhoods of all the points, a basis of the open sets among other methods.

Theorem 4.9. Let \( \mathcal{B} \) be a non-empty family of subsets of \( X \) satisfying the following conditions:

\((B_1)\) For \( x \in X \) there exists \( U \in \mathcal{B} \) such that \( x \in U \).

\((B_2)\) For \( U_1, U_2 \in \mathcal{B} \), if \( x \in U_1 \cap U_2 \) then there exists \( U \in \mathcal{B} \) such that \( x \in U \subseteq U_1 \cap U_2 \).

Then there is a unique topology \( \tau \) on \( X \) such that \( \mathcal{B} \) is a basis of \( \tau \). More precisely,

\[ \tau = \{ \bigcup_{i \in I} U_i : (U_i)_{i \in I} \text{ is a family of elements of } \mathcal{B} \} \cup \{ X, \emptyset \} \]

For example the family of all the open intervals is a basis of the usual topology on \( \mathbb{R} \), the open sets of \( (\mathbb{R}, |\cdot|) \) are the unions of open intervals. The set of all the open balls is a basis of the topology on \( (\mathbb{C}, |\cdot|) \). We can easily check that the family \( \mathcal{B} = \{ [x, q)/x \in \mathbb{R}, q \in \mathbb{Q}, q > x \} \) is a basis of a topology on \( \mathbb{R} \).
4.2 The fundamental theorem

We let \( L/K \) be a Galois extension eventually infinite. Let

\[
\mathcal{I} = \{ F/K \subseteq F \subseteq L, [F : K] < \infty \text{ and } F/K \text{ is Galois} \}
\]

\[
\mathcal{N} = \{ N \subseteq G/N = \text{Gal}(L/F) \text{ for some } F \in \mathcal{I} \}
\]

Lemma 4.10. If \( N_1, N_2 \in \mathcal{N} \) then \( N_1 \cap N_2 \in \mathcal{N} \).

Consider the set \( \mathfrak{B}_k = \{ \sigma N/\sigma \in \text{Gal}(L/K), N \in \mathcal{N} \} \). We can easily check that \( \mathfrak{B}_k \) satisfies the conditions \((B_1)\) and \((B_2)\) in Theorem 4.9: if \( \sigma \in \sigma N \) for all \( N \in \mathcal{N} \), if \( \delta \in \sigma_1 N_1 \cap \sigma_2 N_2 \) then \( \sigma_1 N_1 \cap \sigma_2 N_2 = \delta(N_1 \cap N_2) \) and \( N_1 \cap N_2 \in \mathcal{N} \).

The topology generated on \( \text{Gal}(L/K) \) for which \( \mathfrak{B}_k \) is a basis is called the Krull topology and it makes \( \text{Gal}(L/K) \) into a topological group\(^5\). This topology is compact, Hausdorff and totally disconnected since it coincides with the profinite topology that we get by considering \( \text{Gal}(L/K) \) as the inverse limit of the topological groups \( \text{Gal}(L/F) \) where \( F \) runs through \( \mathcal{I} \), this is just another way of looking at the topological structure defined by the krull topology and we will not get into that too much.

We can now state the main theorem:

**Theorem 4.11.** (Fundamental theorem of infinite Galois theory) With the Krull topology on \( \text{Gal}(L/K) \), the map \( F \longmapsto \text{Gal}(L/F) \) from the set of all intermediate fields extensions of \( K \) contained in \( L \) to the set of all the closed subgroups of \( \text{Gal}(L/K) \) defines a bijective inclusion reversing correspondence, the inverse is given by \( H \longmapsto \text{Fix}(H) \). Furthermore, if \( F \longmapsto H \) and \( H \longmapsto F, \mid \text{Gal}(L/K) : H \mid < \infty \) if and only if \( [F : K] < \infty \) if and only if \( H \) is open. When this holds, \( \mid \text{Gal}(L/K) : H \mid = [F : K] \). Moreover, \( H \triangleleft \text{Gal}(L/K) \) if and only if \( F \) is Galois over \( K \), and \( \text{Gal}(F/K) \cong \text{Gal}(L/K)/H \). If \( \text{Gal}(F/K) \cong \text{Gal}(L/K)/H \) is endowed with the quotient topology, the above isomorphism is also a homeomorphism.

If the extension \( L/K \) is finite then the Krull topology on \( \text{Gal}(L/K) \) coincides with the discrete topology and any subgroup is closed. Thus we recover the fundamental theorem for finite extensions.

---

\(^5\)A group with a topological structure compatible with the group operations.