WOMP 2007
Notes about Galois Theory

Asaf Hadari

September 10, 2007

1 Introduction

Galois theory is an incredibly successful and striking algebraic theory.
The main objects investigated in this theory are fields. The main idea is that you can study the structure of a field by studying a certain group of functions from the field to itself, which are in some sense the symmetries of the field.
Before you begin reading these notes, make sure that you recall basic definitions of fields, groups, integral domains, ideals, and linear algebra. If you cannot recall them, run quickly and look them up.

Examples of Fields

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: the fields of rational, numbers real numbers, and complex numbers respectively.
2. $\mathbb{F}_p$: the field of residues modulo the prime p.
3. $\mathbb{F}_q$: the finite field of order q where $q = p^n$ for some prime p and $n \in \mathbb{N}$.
4. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$
5. $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$
6. $\mathbb{Q}_p$: the field of p-adic numbers, where p is a prime.
7. $K(V)$: the field of K-regular functions on V, where K is a field and V is a K-variety.
8. The field of meromorphic functions on a Riemann surface.

Exercise Prove that every field contains exactly one of the following: a field of order p for some prime p, or $\mathbb{Q}$. In the first case, we say that the *characteristic* of the field is p, and in the second case we say that it it 0.

2 Field Extensions

Definition Let K and E be fields. We say that E is an *extension* of K if $K \subset E$.

Notice that in the above defintion, E is also a vector space over K. Its dimension is an important property of this extension.

Definition Let E be an extension of K. The dimension of E as a K vector space is called the *degree* of the extension and is denoted $[E : K]$. If $[E : K] < \infty$ the extension is said to be *finite*.

The examples above illustrate several procedures in which we can construct an extension of that field. The first procedure is the one that creates $\mathbb{R}$ or $\mathbb{Q}_p$ from $\mathbb{Q}$. In these constructions one defines a norm on $\mathbb{Q}$, and completes the field (as a metric space) with respect to this norm. These constructions have strong generalizations and many uses. We will discuss them no further in these notes.

The second procedure gives $\mathbb{C}$ from $\mathbb{R}$, $\mathbb{F}_{p^n}$ from $\mathbb{F}_p$ and $\mathbb{Q}(\sqrt{2})$ from $\mathbb{Q}$. In all of these we take a field K, and add (or *adjoin*) to it some solutions to some polynomial equation with coefficients in K.For instance, to get $\mathbb{C}$, we adjoin the solutions of $x^2+1 = 0$ to $\mathbb{R}$. This is a prototypical example for the kind of extensions we will be looking at - *algebraic extensions*.

Definition Let K and E be fields. We say that E is an *algebraic extension* of K if for all $x \in E$ there exists $f \in K[T]$ such that $f(x) = 0$.

In the example of $\mathbb{R}$ and $\mathbb{C}$, it is also possible to get $\mathbb{C}$ by adjoining the solutions of $x^3 + x = 0$ to $\mathbb{R}$, or any other polynomial that has i as one of its roots. The set of all polynomials that are zero at i is an ideal in $\mathbb{R}[T]$. As $\mathbb{R}[T]$ is a PID, this ideal is generated by a single element. This discussion gives rise to several important defintions.

Definition Let K be a field. A polynomial $f \in K[T]$ is called *irreducible* if it cannot be written as $f = gh$ where $g, h \in K[T]$, $deg(g) < deg(f)$.

Definition Let E be an algebraic extension of K. Let $x \in E$. The *minimal polynomial of x over E*, denoted $irr_K(x)$, is the unique monic generator of the ideal of elements in $K[T]$ that are zero at x.

Notice that i and $-i$ are both solutions to $x^2 + 1 = irr_{\mathbb{R}}(i)$. This means that every polynomial over $\mathbb{R}$ that is 0 at i is also 0 at $-i$. This important relation is generalized in the following definition.

Definition Let E be an algebraic extension of K. Let $x \in E$, and let $f = irr_K(x)$. If $y \in E$ and $f(y) = 0$ then y is said to be *conjugate to x in E*.

Exercise Prove that every finite extension of a field is algebraic (Hint, for any element x, look at the sequence $1, x, x^2, x^3, \ldots$. Is the converse true?

Exercise Let $K \subset E \subset L$ be fields. Prove the identity:

$$[L : K] = [L : E][E : K]$$

.

Exercise

1. Suppose K is a field, and $f \in K[T]$ is irreducible. Prove that the field constructed by adjoining the zeroes of f to K is isomorphic to $K[T]/fK[T]$

2. Prove that $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. Use this fact to explicitly construct a field of order 4.

3. (more difficult) Construct a field of order p^n.

3 Special Extensions

3.1 Separable Extensions

Definition Let E be an algebraic extension of K. We say that E is *separable* if for every $x \in E$, $irr_K(x)$ has no roots of multiplicity greater than 1. K is called *perfect* if every algebraic extension of it is seperable.

Theorem. *Fields of characteristic* 0 *and prime order finite fields are perfect.*

Abel's Primitive Element Theorem. *Suppose E is a finite separable extension of K. Then $E = K(x)$ for some element $x \in E$ (i.e. E is constructed by adjoining x to K).*

Exercise Let $K = \mathbb{F}_2(x)$. Let $E = \mathbb{F}_2(\sqrt{x})$. Show that E is a non-separable extension of K.

3.2 Normal Extensions and Splitting Fields

Definition Let K be a field, let $f \in K[T]$. An extension L of K is called a *splitting field* of f if f can be written as a product of linear factors in L, and L is the smallest field that satisfies this property. Splitting fields exist and are unique up to isomorphism.

Definition A field is called *algebraically closed* if it has no proper algebraic extensions, that is - if every polynomial over the field splits into linear factors.

Definition The *algebraic closure* of K is an algebraic extension of K that in which every polynomial over K splits. Algebraic closures are unique up to isomorphism.

Exercise Prove that an algebraic closure of a field is algebraically closed.

Exercise Prove that the algebraic closure of a countable field is countable.

Exercise What is the algebraic closure of $\mathbb{F}_p$.

Definition Let K be a field and E be an algebraic extension of K. We say that E is a *normal extension* of K if $\forall a \in E$, $irr_K(a)$ splits into linear factors in E. Splitting fields are examples of normal extensions.

Defintion Let K be a field. A *Galois extension* of K is an algebraic normal seperable extension of K.

Exercise Find the splitting field of $T^4 + 2$ over $\mathbb{Q}$. Find a non normal subfield in which the polynomial splits into factors of degree 2.

4 Galois Theory

4.1 Field Automorphims and the Galois Group

As stated in the introduction, the main idea of Galois theory is to study fields by studying a certain group of symmetries of the field. The correct definition of a symmetry is a field automorphism.

Definition Let E be an extension of K. A function $f : E \to E$ is called an *automorphism over* E if it is injective, surjective, a homomorphism of both additive and multiplicative groups, and the identity on E. The set of all such automorphisms is called the *Galois group of E over K*, and denoted $Gal(E|K)$

Suppose $f \in K[T]$. If f splits in E, and σ is an automorphism of E over K, then by virtue of preserving the coeffiecients of f, σ must permute the roots of f. We wish to study automorphism groups as permutation groups on finitely many elements.

Exercise Calculate $Gal(\mathbb{C}|\mathbb{R})$.

Exercise Let $\zeta = e^{\frac{2\pi i}{3}}$. Calculate $Gal(\mathbb{Q}(i, \zeta)|\mathbb{Q})$.

Exercise (a bit trickier) Calculate the Galois group over $\mathbb{Q}$ of the splitting field of $(T^2 - 5)^2 - 24$.

4.2 The Fundamental Theorem of Galois Theory

The fundamental theorem provides a dictionary between the language of algebraic extensions and their subfields, and the Galois group and its subgroups.

Defintion Let E be a Galois extension of K, let $G = Gal(E|K)$, let $H < G$. The *fixed field of* H, denoted $Fix(H)$ is

$$F(H) = \{x \in E | \sigma(x) = x \forall \sigma \in H\}$$

.

This gives us a function from the collection of subgroups of G to the collection of subfields of E. There is also a function in the other way, namely, for a field K $subsetM \subset E$, $Gal(E|M) < Gal(E|K)$. (Exercise: why?). We are now ready to state several of the statements often included in the fundamental theorem of Galois theory.

The Fundamental Theorem. *Let E be a finite Galois extension of K. Let $G = Gal(E|K)$.*

1. *The functions defined above are inverses, i.e. for every $H < G$, $Gal(E|Fix(H)) = H$, and for every subfield $K \subset M \subset E$ we have $Fix(E|M) = M$.*
2. *$Fix(G) = K$, $Fix(< 1 >) = E$.*
3. *$H_1 < H_2 < G \Rightarrow Fix(H_2) \subset Fix(H_1)$, and $K \subset M_1 \subset M_2 \subset E \Rightarrow Fix(M_2) < Fix(M_1)$.*

4. *H is normal in G if and only if $Fix(H)$ is a normal extension of K.*

5. *If $M \subset E$ is a normal extension of K then $Gal(M|K) \cong Gal(E|K)/Gal(E|M)$.*

6. *For $K \subset M \subset E$, $[M : K] = Gal(M|K)$.*

7. *Let $\sigma \in G$, $H < G$, then $Gal(\sigma(Fix(H))|K) = Gal(Fix(H)|K)^{\sigma}$.*

Exercise Prove that in the notation above for $x \in E$ we have that $\Sigma_{\sigma \in G}\sigma(x) \in K$ and $\Pi_{\sigma \in G}\sigma(x) \in K$ (These are called the trace and the norm of x, respectively).

Exercise Calculate the Galois group over $\mathbb{Q}$ of the splitting field of $T^4 + 1$. Calculate all of the subfields of this field.

Exercise Suppose $f = \Pi_i(X - x_i)$ is a polynomial. The discriminant of f is defined to be $\Pi_{i<j}(x_i - x_j)$. Every finite group can be embedded into a symmetric group, but not necessarily into an alternating group. What is the connection between the definition and this statement?

Exercise For all groups of order 5 and under, find an extension of $\mathbb{Q}$ that has that field as a Galois group.

Exercise

1. Prove that the only subgroup of S_5 (the symmetric group on 5 elements) that contains an element of order 5 and a transposition is S_5 itself.

2. Find sufficient conditions for a splitting field over $\mathbb{Q}$ of a polynomial of degree 5 to have a Galois group isomorphic to S_5.

3. Find such a polynomial.

Exercise Remember this theorem. Wait for the lecture on fundamental groups and covering spaces.