Galois Theory

Vishal Raman

December 29, 2020

These notes are part of my in-depth review of Galois Theory. I will be following the lectures of Professor Richard Borcherds along with supplemental notes from the classic Galois Theory text from E. Artin. Any mistakes and typos are my own - kindly direct them to my inbox.

Contents

§1 Introduction

The main use of Galois Theory is to take problems about polynomials and translate them into problems in Group theory. The corresponding group is called the **Galois group**.

§1.1 Example: Solving Polynomials

Can a polynomial be solved be radicals? This is well known for polynomials of degree 2, given by the quadratic formula. Can we do this for higher degree polynomials? Yes, for polynomials up to degree 4. However, no for general polynomials of degree at least 5. The corresponding problem using Galois theory is a Galois group which is a subgroup of S_n. A polynomial can be solved by radicals if the subgroup is **solvable**, that is, it can be split into a product of Abelian groups.

§1.2 Example: Geometric Constructions

We try to trisect the angle of 60° using ruler and compass. This would correspond to factoring a polynomial which has roots $\cos 20^\circ, \ldots$. This turns out to correspond to a Galois group $\mathbb{Z}/3\mathbb{Z}$. It turns out that being able to construct an object is related to the Galois group being of an order of a power of 2, so it fails in this case.

Another famous example is Gauss's construction of the heptadecagon, which has 17 sides. Though it is very difficult to construct by hand, the Galois group of the corresponding polynomial is $(\mathbb{Z}/17\mathbb{Z})^* = \mathbb{Z}/16\mathbb{Z}$, so it is constructable.

§1.3 Main Idea of Galois Theory

Given a polynomial $a_n x^n + \cdots + a_0$ over $\mathbb{Q}[x]$, we look at the field generated by the roots of the polynomial, $\alpha_1, \alpha_2, \ldots, \alpha_n$. The **Galois group** is the permutations of $\alpha_1, \ldots, \alpha_n$ preserving all algebraic relations between the roots. It is clear that the Galois group is always some subgroup of S_n.

For $x^5 - 2$, we have roots $2^{1/5}, 2^{1/5}\zeta, 2^{1/5}\zeta^2, 2^{1/5}\zeta^3, 2^{1/5}\zeta^4$, where ζ is a fifth root of unity. We have algebraic relations $\alpha_1\alpha_3 = \alpha_2^2$, $\alpha_2/\alpha_1 = \alpha_4/\alpha_3, \ldots$. It turns out the subgroup of permutations has order 20, rather than 120.

If we consider a field extension $K \subseteq L$, the Galois group of the extension is the symmetries of L fixing all elements of K. For example, if we take $\mathbb{R} \subseteq \mathbb{C}$, the Galois group consists of 1 and complex conjugation.

Theorem 1

Suppose $K \subseteq L$ is a Galois extension. That is, the order of the Galois group is L, which is the dimension of L as a vector space over K. Then, subfields M with $K \subseteq M \subseteq L$ correspond exactly to the subgroups of the Galois group.

§1.4 Applications

- The Langlands program: Galois groups of fields L, $\mathbb{Q} \subseteq L$ are related to modular forms. An example of a modular form is the discriminant function

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n) = q - 24q + 252q^2 + \ldots$$

  where the coefficients of Ramanujan's $\tau(n)$ function.

Wiles used this to prove Fermat's Last theorem, namely he related the solution of Fermat's Last theorem to an Elliptic curve and he related this to a Modular Form by considering the action of the Galois group. Then, Ken Ribet showed that the modular form is not possible, which proves the theorem.

- The Galois group is related to the Fundamental group. If we have an extension $K \subseteq L$, this corresponds to a covering space. The Galois group corresponds to the fundamental group of the base space. The algebraic closure of a field corresponds to a universal covering space.

Inverse Galois Problem: Given a finite group G, is there an extension K of $\mathbb{Q}$ so that the Galois group of K is G? This is true for many groups, but the problem is completely open in general.

§2 Field Extensions

§2.1 Algebraic Numbers

Definition 2.1. A field extension is a pair of fields $K \subseteq L$, denoted L/K.

In Galois Theory, it is sometimes helpful to start with smaller fields and build up to the full field. The most basic example is given by $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

The degree of a field extension L/K, denoted by $[L : K]$ is the dimension of L as a vector space over K. The field extension is called finite if it has finite degree.

Definition 2.2. Suppose we have $K \subseteq L$ and $\alpha \in L$. α is called **algebraic** over K if it is a root of a polynomial $p(x) \in K[x]$. Otherwise, it is called **transcendental**. The degree of $\alpha$is the degree of an irreducible polynomial p where α is a root.

- It is clear that $2^{1/5}$ is algebraic since it is the root of $x^5 - 2 = 0$.
- The reals π, e are transcendental.
- The real $\alpha = \cos 2\pi/7$ is algebraic. Note that $\alpha = \frac{\zeta+\zeta^{-1}}{2}$ where $\zeta = e^{2\pi i/7}$. We can apply a clever transformation to $1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 0$ to find a polynomial relation in terms of α.
- Is $e + \pi$ transcendental? Is $e\pi$ transcendental? We can show that $e + \pi$ or $e\pi$ is transcendental.

  Consider $x^2 - (e + \pi)x + e\pi$. If $e + \pi$ and $e\pi$ are both algebraic then e, π are algebraic, a contradiction.

§2.2 Algebraic Extensions

Theorem 2

If we have $K \subseteq M$, $\alpha \in M$ is algebraic over K if and only if it is contained in a finite extension of K.

Proof. If α is contained in a finite extension L, with $[L : K] = n < \infty$, then consider $1, \alpha, \alpha^2, \ldots, \alpha^n$, which are $n + 1$ elements of an n-dimensional vector space. So we have a non-trivial linear relation in terms of these elements which is zero, which gives a polynomial relation of α.

Suppose $p(x)$ is an irreducible polynomial in $K[x]$. Then, if we consider $K[x] \setminus (p)$, this is a field. It is obviously a ring, but the existence of inverses needs to be verified. Suppose we have an element $q(x) \in K[x] \setminus (p)$, with $q \neq 0$. Then q, p are coprime in $K[x]$ since p is irreducible. Then, we can find $a(x)q(x) + b(x)p(x) = 1$ using the Euclidean algorithm. Hence, $a(x)$ is the inverse of $q(x)$.

If α is algebraic, then α is a root of $p(x) \in K[x]$ with p irreducible. Consider the field $\frac{K[x]}{(p)}$. This contains K and we can map this field in L with the map $x \mapsto \alpha$, which also contains K. The image is a field in L containing α, and the field has dimension of the degree of p so it is finite. □

Consider a tower of extensions $K \subseteq L \subseteq M$. Then, $[M : K] = [M : L][L : K]$. Pick a basis $x_1, \ldots, x_m$ of L/K and pick a basis $y_1, \ldots, y_n$ for M/L and check that $x_i y_j$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ form a basis for the vector space M over K.

Theorem 3

If $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha + \beta, \alpha\beta, \alpha/\beta, \alpha - \beta$.

Example 2.3

Consider $2^{1/2} + 2^{1/3} + 2^{1/5}$. It is hard to come up with a polynomial relation with this element, but is algebraic as the sum of algebraic elements.

Proof. Consider $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$, which are finite extensions, which gives the desired result, since the elements are algebraic relations of α and β. □

Theorem 4

($K \subseteq L$) If α is the root of a polynomial with algebraic coefficients, then α is algebraic.

Proof. For a polynomial $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, take

$$K \subseteq K(a_0) \subseteq K(a_0, a_1) \subseteq \cdots \subseteq K(a_0, \ldots, a_{n-1}) \subseteq K(a_0, \ldots, a_{n-1}, \alpha),$$

which are all finite extensions. It follows that α is algebraic. □