Galois Theory and Some Applications

Aparna Ramesh

July 19, 2015

Introduction

In this project, we study Galois theory and discuss some applications. The theory of equations and the ancient Greek problems were the initial motivations for the theory of Galois to come into being. However, in present-day mathematics, Galois theory is ubiquitous. Whether it is a coding theorist or a cryptographer working with finite fields or a geometer working with Riemann surfaces or a number theorist interested in problems involving prime numbers, they all employ Galois theory in a crucial manner.

We begin by discussing the basic notions and results in Galois theory. We discuss also in detail the Galois theory of polynomials of degrees up to 4 first, where we recall how formulae similar to those arising in the solution of quadratic equations exist for degrees 3 and 4 also. We describe the fundamental theorem of Galois theory and show how to draw important consequences like: (i) the three Greek problems, (ii) the impossibility of such formulae for roots to exist for general polynomials of degree 5 or more, (iii) constructibility of regular polygons by a straightedge and compasses, and (iv) the fundamental theorem of algebra. There are numerous applications of Galois theory which are not so well known as to appear in any text books; we will look at a couple of non-standard applications in the area of number theory which are solved using Galois theory.

Support problem:
Given positive integers $a, b > 1$ with the property that for every n, the prime numbers dividing $a^n - 1$ also divide $b^n - 1$, does it follow that b is a power of a?
The analysis of this problem depends on Kummer theory, which is the study of Galois extensions whose Galois groups are abelian.

Reducibility mod p of irreducible integral polynomials:
If P is a polynomial with integer coefficients which is irreducible, is it necessary that it must be irreducible modulo some prime number?
The answer turns out to be dependent on the existence or not, of an element of order deg (f) in the Galois group of f. Consequently, the answer is 'yes' if deg f is prime and 'not necessarily yes' when deg f is composite.

1 Field Theory

1.1 Definition

We start by recalling that a field is a set F together with two binary operations $+$ and $\cdot$ on F such that (F,+) is an Abelian Group (having additive identity 0) and (F - $\{0\}$, $\cdot$) is also an Abelian Group, and the following distributive law holds :

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Usually, we suppress the dot of the multiplication and use juxtaposition for the multiplication.

1.2 Basic Terminology

1. Characteristic of a Field

   The *characteristic* of a field F is defined to be the smallest positive integer p such that

   $$p \cdot 1 = 0$$

   if such a p exists, and is defined to be 0 otherwise. Here 1 denotes the identity of F.

2. Prime Subfield

   The *Prime subfield* of a field F generated by the multiplicative identity 1 of F .

3. Extension Field

   If K is a field containing the subfield F, then K is said to be an *Extension Field* or simply an *extension* of F , denoted K/F or by the diagram

   $$\begin{array}{c} K \\ | \\ F \end{array}$$

   The Field F is sometimes called the *Base Field* of the extension.

4. Degree

   The *Degree* of a field extension K/F, denoted by $[K : F]$, is the dimension of K as a vector space over F. The extension is said to be finite if $[K : F]$ is finite and infinite otherwise.

5. Simple Extension

   If the field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be a *simple* extension of F and the element α is called the *primitive element* for the extension.

6. Algebraic

   The element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F\ [X]$.

   If α is not algebraic it is said to be transcendental.

7. Splitting Field

   The extension field K of F is called a *Splitting Field* for the polynomial $f(x)$ if $f(x)$ factors completely into linear factors in $K[X]$ and $f(x)$ does not factor completely in to factors over any proper subfield of K containing F.

8. Primitive n^{th} root of unity

   A generator of the cyclic group of all n^{th} roots of unity is called a Primitive n^{th} root of unity. If ω is a Primitive n^{th} root of unity then, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ where ϕ is called the **Euler Phi function**.

9. Cyclotomic Field of n^{th} root of unity

   The field $\mathbb{Q}(\zeta)$ is called the *cyclotomic Field of n^{th} root of unity*

10. Separable Polynomial

    A polynomial over F is called *separable* if it has no multiple roots. A polynomial which is not separable is called *inseparable*

11. Automorphism

    An isomorphism σ of K with itself is called an *automorphism* of K. We denote the collection of all automorphisms of K by $\mathrm{Aut}(K)$.

    An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to *fix* an element $\alpha \in K$ if

    $$\sigma\alpha = \alpha$$

12. $\mathrm{Aut}(K/F)$

    Let K/F be an extension field. Then $\mathrm{Aut}(K/F)$ is the collection of automorphisms of K which fix F.

13. Fixed Field

    If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all elements of H is called *fixed field* of H.

14. Normal Extension

    An algebraic field extension L/K is said to be *Normal* if L is the Splitting field of the family of polynomials $K[X]$.

2 Galois Theory

2.1 Definitions

1. Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois Extension* if $\mid \mathrm{Aut}(K/F) \mid = [K{:}F]$

2. If K/F is Galois the group of automorphisms $\mathrm{Aut}(K/F)$ is called the *Galois Group* of K/F, denoted by $\mathrm{Gal}(K/F)$.

3. If $f(x)$ is a separable polynomial over F, then the *Galois Group of $f(x)$ over F* is the Galois group of the splitting field of $f(x)$ over F.

2.2 Important Results

1. Aut(K) is a group under composition and Aut(K/F) is a subgroup.
2. Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \text{Aut}(K/F)$, $\sigma\ \alpha$ is a root of the minimal polynomial for α over F.
3. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.
4. Let K/F be any finite extension. Then

$$\mid Aut(K/F) \mid \leq [K : F]$$

with equality if and only if F is the fixed field of Aut(K/F).

2.3 Characterizations of Galois extensions K/F

1. K/F are the splitting fields of separable polynomials over F.
2. K/F are the fields where F is precisely the set of elements fixed by Aut(K/F)
3. K/F are the fields with [K:F] = $\mid$ Aut(K/F) $\mid$.
4. K/F are finite, normal and separable extensions.

3 Fundamental Theorem of Galois Theory

Let K/F be a Galois extension and set G=Gal(K/F). Denote by E subfields of K containing F and H the subgroups of G.Then there is a bijection:

$$\begin{array}{ccc} K & & 1 \\ | & & | \\ E & \leftrightarrow & H \\ | & & | \\ F & & G \end{array}$$

given by the correspondence

$$E \rightarrow \{\text{elements of G fixing E}\}$$
$$\{\text{the fixed field of H}\} \leftarrow H$$

which are inverses to each other. Under this correspondence ,

1. (inclusion reversing) If E_1, E_2 correspond to H_1, H_2 respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \subseteq H_1$.
2. we have [K:E] = $\mid H \mid$ and [E:F] = $\mid G$:$H \mid$ the index of H in G
3. Also , K/E is always Galois, with Galois group Gal(K/E) = $\mid H \mid$:

$$\begin{array}{c} K \\ | \quad H \\ E \end{array}$$

4. E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group

$$Gal(E/F) \cong G/H$$

More generally, even if H is not necessarily normal in G, the isomorphisms of E into a fixed algebraic closure of F containing K which fix F are in one to one correspondence with the cosets $\{ \sigma\ H\}$ of H in G.

5. If E_1, E_2 correspond to H_1, H_2 respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$.

4 Some Classical Applications

Having discussed the basic notions and properties of Galois extensions in the previous section, we shall now start with some applications. In this section, we look at classical problems. Later on, we briefly describe some applications which are modern or which are not well-known.

4.1 The classical Straightedge and Compass constructions

Ancient Greek mathematicians were restricted in their Geometric constructions by the fact that very few instruments were available to them for this construction. At that time, the only available instruments were the straightedge (unmarked) and compasses. Using just these two, they were able to carry out a number of constructions- line segments could be divided into any number of equal parts, angle bisections, construction of a square of the same area as that of a given polygon etc. However, even this process had its limitations.

First we shall understand algebraically the construction of lengths using a straightedge and compass. Then, we shall look at the four famous constructions that the Greeks could not perform.

4.1.1 Construction of lengths

Let 1 denote the fixed unit length. By denoting any distance by $a \in \mathbb{R}$, we can think of distances as the elements of the real number $\mathbb{R}$. We can then construct the usual Cartesian plane $\mathbb{R}^2$. Any point (x,y) in it is constructible starting with the distance 1 if and only if its coordinates x and y are constructible elements of $\mathbb{R}$.Every construction using a straightedge and compass consists of a series of operations:

1. connecting two points by a given straight line
2. finding a point of intersection of two straight lines.
3. drawing a circle with given radius and center

4. finding the point(s) of intersection of a line and a circle or of two circles.

Given two lengths a and b, one can construct using a straightedge and compass, the lengths $a \pm b$, ab and a/b. Similarly we can construct $\sqrt{a}$ for a given a.Thus we see that all straightedge and compass constructions give all algebraic operations of addition, subtraction multiplication and division as well as square root of constructible elements. This gives us the understanding that the collection of constructible elements is a *subfield* of $\mathbb{R}$.

From the length 1, we can construct all rational numbers $\mathbb{Q}$.In $\mathbb{R}^2$ any (x,y) having rational coordinates can be constructed. More elements in $\mathbb{R}$ can be constructed by taking square root, so that we get a collection of constructible elements from 1 in $\mathbb{R}$ that is larger than $\mathbb{Q}$.

Let us now consider the first of the four constructions mentioned above. The equation of a straight line passing through two points with coordinates in a field F is given by:

$$ax + by - c = 0 \tag{1}$$

where $a, b, c \in F$

To find the point of intersection of two lines we simultaneously solve the two equations. The solution will also be elements of F.

Now, the constructions of the remaining two types involves the intersection of a circle with a straight line or another circle. The equation of a circle of center (h,k) and radius r is given by:

$$(x - h)^2 + (y - k)^2 = r^2 \tag{2}$$

where $h, k, r \in F$

In the case of intersection of a circle with a straight line we are looking at the solution obtained by simultaneously solving equations (1) and (2). By substituting for y in terms of x from equation (1) in equation (2), we get a quadratic equation in x. This implies that the point of intersection lies in a **Quadratic Extension of** F.

Consider the equation of another circle centered at (h',k') having radius r'.

$$(x - h')^2 + (y - k')^2 = r'^2 \tag{3}$$

where $h', k', r' \in F$ Subtraction of equation (3) from (2) gives

$$2(h' - h)x + 2(k' - k)y = r^2 - h^2 - k^2 - r'^2 - h'^2 - k'^2 \tag{4}$$

This is the intersection of a circle with a straight line, which is discussed above.

Thus we see that, given a collection of constructible elements, we can construct all elements of the subfield F of $\mathbb{R}$ generated by these elements. Furthermore, any straightedge and compass operations on the elements of F results in elements which are at most in the Quadratic Extension of F. Quadratic Extensions have degree 2 and the extension degrees are multiplicative. Hence any $\alpha \in \mathbb{R}$ obtained from elements of subfield F, will be an element of an extension K of F of degree which is a power of 2. For some m,

$$[K : F] = 2^m \tag{5}$$

Since $[F(\alpha) : F]$ divides the extension degree in (5), it must be a power of 2.

The above explanation can be stated in the following proposition:
Proposition 1:
If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset R$ by a series of compass and straightedge constructions then

$$[F(\alpha) : F] = 2^k \tag{6}$$

for some integer k≥0.

4.1.2 Doubling the Cube

We shall look at whether or not it is possible to construct a cube of volume twice that of a given cube using a straight edge and compass.
A cube of volume 2 has sides of length $\sqrt[3]{2}$. The minimal polynomial of $\sqrt[3]{2}$ is x^3 -2. But

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

which is not a power of 2. So the construction is not possible.

4.1.3 Trisecting the Angle

Let angle θ be constructible. A point p at a unit distance from the origin and angle θ from the X-axis in $\mathbb{R}^2$, shows that $\cos\theta$ and $\sin\theta$ can be constructed. Conversely if $\cos\theta$ and $\sin\theta$ can be constructed, then so can the point at an angle of θ from the X-axis. Certain angles like 180° can be trisected. But this is not always possible. We shall prove this using a counter example. Let $\theta =$ 60°. Then $\cos\theta = \frac{1}{2}$. We have the formula,

$$\cos\theta = 4\cos^3(\frac{\theta}{3}) - 3\cos(\frac{\theta}{3})$$

At $\theta = 60°$

$$4(\beta)^3 - 3\beta - \frac{1}{2} = 0$$

where $\beta = \cos(\frac{\theta}{3})$. Then,

$$8(\beta)^3 - 6\beta - 1 = 0$$

$$(2\beta)^3 - 3(2\beta) - 1 = 0$$

Then $\alpha = 2\beta$ is a real number between 0 and 2 satisfying the equation

$$\alpha^3 - 3\alpha - 1 = 0$$

As in the case with doubling the cube, since

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

the construction is not possible.

4.1.4 Squaring the Circle

We shall now determine whether it is possible to construct a square of area π. Consider a circle of radius 1. Then its area is π. To construct a square of the same area would require the construction of a line segment of length $\sqrt{\pi}$, which is transcendental over $\mathbb{Q}$. Thus, since $\mathbb{Q}(\sqrt{\pi})$ is not algebraic over $\mathbb{Q}$, the degree $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is not a power of 2, and the construction is not possible.

4.1.5 Constructibility of regular polygons

Recall from section 1 the definition of Euler's phi function $\phi(n)$. We shall prove that a regular n- gon is constructible if and only if $\phi(n)$ is a power of 2, by showing that a regular n-gon is constructible if and only if the central angles $2\pi/n$ are constructible and this occurs if and only if $\cos(2\pi/n)$ is a constructible number.

$$\text{Let } \omega = e^{2\pi i/n} = cos(2\pi/n) + isin(2\pi/n)$$

be a Primitive n$^{\text{th}}$ root of unity. Then $cos(2\pi/n) = \frac{1}{2}(\omega + \omega^{-1})$, since $\omega^{-1} = cos(2\pi/n) - isin(2\pi/n)$. Thus $cos(2\pi/n) \in \mathbb{Q}(\omega)$.
However,$\cos(2\pi/n) \in \mathbb{R}$ and $\omega \notin \mathbb{R}$, so $\mathbb{Q}(\omega) \neq \mathbb{Q}(\cos(2\pi/n))$. But ω is a root of $x^2 - 2cos(2\pi/n)x + 1$, and so $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/n))] = 2$ Therefore if $\cos(2\pi/n)$ is constructible, then $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ is a power of 2. Hence, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ is also a power of 2.
Conversely, suppose that $\phi(n)$ is a power of 2. The field $\mathbb{Q}(\omega)$ is a Galois extension of $\mathbb{Q}$ with Abelian Galois group. If $H = Gal(\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/n)))$ by the theory of finite Abelian groups there is a chain of subgroups

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_r = H$$

with $|H_{i-1} - H_i| = 2$. If $L_i = \mathcal{F}(H_i)$, then $[L_i : L_{i+1}] = 2$, thus $L_i = L_{i+1}(\sqrt{u_i})$ for some u_i.Since $L_i \subseteq \mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{R}$, each of the $u_i \geq 0$. Since the square root of a constructible number is constructible, we see that everything in $\mathbb{Q}(\cos(2\pi/n))$is constructible. Thus $\cos(2\pi/n)$ is constructible and hence so is a regular n-gon.

4.2 Fundamental theorem of Algebra

The field $\mathbb{C}$ is Algebraically closed
Proof:
Let us first take a look at the 2 results that will be used in the proof:

1. There are no nontrivial finite extensions of $\mathbb{R}$ of odd degree.
2. There are no quadratic extensions of $\mathbb{C}$.

Let L be a finite extension of $\mathbb{C}$. Since characteristic of $\mathbb{R}$ is 0, the field L is separable over $\mathbb{R}$, and L is also a finite extension of $\mathbb{R}$. Let N be the normal closure of $L/\mathbb{R}$. To prove the theorem we prove $N = \mathbb{C}$. Let $G = Gal(N/\mathbb{R})$. Then

$$|G| = [N : \mathbb{R}] = [N : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2[N : \mathbb{C}]$$

is even. Let H be 2-sylow subgroup of G, and let E be the fixed field of H. Then $|G : H| = [E : \mathbb{R}]$ is odd. Since the only odd extension of $\mathbb{R}$ is $\mathbb{R}$ itself, $G = H$ is a 2-group. Then Gal$(N/\mathbb{C})$ is also a 2-group. Since 2-groups have subgroups of all orders dividing it, if this group is non-trivial, there would exist a quadratic extension of $\mathbb{C}$ which is not possible since $\mathbb{C}$ has no quadratic extensions. Hence $N = \mathbb{C}$

5 Symmetric Groups

Let A be any nonempty set and let S be the set of all bijections from A to itself. The set S is a group under function composition $\circ$ since:

1. if $\sigma, \tau \in S$, then $\sigma \circ \tau \in S$
2. function composition is associative in general.
3. the permutation $1 \in S$ defined by $1(a) = a$, $\forall a \in A$.
4. for every mapping σ, $\exists$ an inverse mapping σ^{-1} satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$

This is called the symmetric group on A. When $A = \{1, 2, 3, \ldots n\}$ the symmetric group on A is called **Symmetric Group of degree n** denoted by S_n. It has order $n!$. A **cycle** of a S_n is a string of integers which represents the element of S_n which cyclically permutes these integers and fixes the rest.The product of all the cycles is called the **cycle decomposition of** σ. A 2-cycle is called a **Transposition**. Every element of S_n maybe written as a product of transpositions.

5.1 Alternating Group

Let $\sigma \in S_n$. Let $x_1, x_2, \ldots, x_n$ be independent variables and let Δ be the polynomial

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

For n=4, i.e. $\sigma = (1234)$

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1)$$

In general we get for any n,

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Collecting together all the changes in sign,

$$\sigma(\Delta) = \pm\Delta, \forall \sigma \in S_n$$

For each $\sigma \in S_n$ let

$$\epsilon(\sigma) = \begin{cases} +1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

σ is called an even permutation if $\epsilon(\sigma) = 1$ and an odd permutation if $\epsilon(\sigma) =$ -1 The **Alternating Group of degree n** denoted A_n is the set of even permutations.

6 Galois group of Polynomials

6.1 Definitions

1. Let $x_1, x_2, \ldots, x_n$ be indeterminates. The **Elementary symmetric functions** $s_1, s_2, \ldots, s_n$ are defined by

$$s_1 = x_1 + x_2 + \cdots + x_n$$

$$s_2 = x_1x_2 + x_1x_3 \cdots + x_{n-1}x_n$$

$$\vdots$$

$$s_n = x_1x_2 \ldots x_n$$

   i.e.,the i^{th} symmetric function s_i of $x_1, x_2, \ldots, x_n$ is the sum of all products of the x_j's taken i at a time.

2. The **general polynomial of degree n** is the polynomial

$$(x - x_1)(x - x_2) \ldots (x - x_n)$$

   whose roots are the indeterminates $x_1, x_2, \ldots, x_n$. It is important to note that

$$(x-x_1)(x-x_2)\ldots(x-x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \quad (7)$$

3. A rational function $f(x_1, x_2, \ldots, x_n)$ is called **symmetric** if it has not changed by any permutation of the variables $x_1, x_2, \ldots, x_n$.

4. The **Discriminant** D of $x_1, x_2, \ldots, x_n$ is given by

$$D = \prod_{1 \le i < j \le n} (x_i - x_j)^2$$

   It is a symmetric function in $x_1, x_2, \ldots, x_n$ and hence is an element of $F(s_1, s_2, \ldots, s_n)$

5. If $f(x)$ is irreducible over the field K, then given any two roots of $f(x)$ there is an automorphism in the Galois group G of $f(x)$ which maps one root to another. Then the group G is said to be a **Transitive Group**.

6.2 Important results on Symmetric Functions

1. **Preposition 2**:

   The fixed field of the symmetric group S_n acting on the field of rational functions in n variables $F(x_1, x_2, \ldots, x_n)$ is the field of rational functions in the elementary symmetric functions $F(s_1, s_2, \ldots, s_n)$.

2. **Fundamental Theorem on Symmetric Functions**:

   Any symmetric function in the variables $x_1, x_2, \ldots, x_n$ is a rational function in the elementary symmetric functions $s_1, s_2, \ldots, s_n$.

3. **Theorem 1** *:The general polynomial* $x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$ *over the field* $F(s_1, s_2, \ldots, s_n)$ *is separable with Galois group* S_n*.*

   One rephrases the above statement as asserting that a general polynomial of degree n has splitting field whose Galois group is the full symmetric group S_n.

4. **Proposition 3**

   If characteristic of F is not 2 then the permutation $\sigma \in S_n$ is an element of A_n , if and only if it fixes the square root of the discriminant D.

5. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ then the discriminant of the polynomial is
$$D = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$
   It is zero if and only if the polynomial is not separable.

6. The Galois group of polynomial $f(x) \in F[X]$ is a subgroup of A_n, if and only if the discriminant $D \in F$ is the square of an element F.

7. **Theorem 2** *:Let* $f(x) \in K[X]$ *be a separable polynomial in degree* n

   (i) If f(x) is irreducible in $K[X]$ *then its Galois group over* K *has order divisible by* n*.*

   (ii) The polynomial $f(x)$ *is irreducible in* $K[X]$ *if and only if its Galois group over* K *is a transitive subgroup of* S_n*.*

8. **Theorem 3** *:Let* $f(x) \in K[X]$ *be a separable polynomial in degree* n*. If* K *does not have characteristic 2, the Galois group of* $f(x)$ *over* K *is a subgroup of* A_n *if and only is discriminant of f is a square in* K*.*

We start by discussing the Galois theory of polynomials of small degrees.

6.3 Polynomials of degree 2

Let α and β be the 2 roots of the polynomial

$$f(x) = x^2 + ax + b$$

Then by result 5 of section 6.2 the discriminant of the polynomial is

$$D = (\alpha - \beta)^2$$

By equation 7 we have ,

$$D = s_1^2 - 4s_2 = (-a)^2 + 4b = a^2 - 4b$$

The polynomial is separable if and only if $D \neq 0$. By result 6 of section 6.2 the above polynomial has Galois group A_2 if and only if $a^2 - 4b$ is a rational square.

6.4 Polynomials of degree 3

Consider the cubic polynomial

$$f(x) = x^3 + ax^2 + bx + c$$

Substituting for x as y- $\frac{a}{3}$ we get

$$g(y) = y^3 + py + q \tag{8}$$

where

$$p = \frac{1}{3}(3b - a^2) \qquad\qquad q = \frac{1}{27}(2a^3 - 9ab + 27c)$$

Let us assume the roots of the polynomial to be α, β and γ, we get

$$g(y) = (y - \alpha)(y - \beta)(y - \gamma)$$

Differentiating we get,

$$\begin{aligned} D_y g(y) &= (y - \alpha)(y - \beta) + (y - \alpha)(y - \gamma) + (y - \beta)(y - \gamma) \\ &= 3y^2 + p \end{aligned}$$

Then

$$\begin{aligned} D_y g(\alpha) &= (\alpha - \beta)(\alpha - \gamma) \\ D_y g(\beta) &= (\beta - \alpha)(\beta - \gamma) \\ D_y g(\gamma) &= (\gamma - \alpha)(\gamma - \beta) \end{aligned}$$

Taking product we see that

$$\begin{aligned} D &= [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2 \\ &= -D_y g(\alpha) D_y g(\beta) D_y g(\gamma) \\ &= -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) \\ &= -[27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3] \end{aligned}$$

From equation 8,

$$\begin{aligned} s_1 &= 0 \\ s_2 &= p = \alpha\beta + \beta\gamma + \gamma\alpha \\ s_3 &= -q = -\alpha\beta\gamma \end{aligned}$$

Making the above substitutions in D, we get

$$-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3 \tag{9}$$

$$D = -4p^3 - 27q^2 \tag{10}$$

$$= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \tag{11}$$

6.5 Polynomials of degree 4

Consider the quartic polynomial

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \tag{12}$$

Substituting for x as $x = y - \frac{a}{4}$,

$$g(y) = y^4 + py^2 + qy + r \tag{13}$$

$$\begin{aligned} p &= \frac{1}{8}(-3a^2 + 8b) \\ q &= \frac{1}{8}(a^3 - 4ab + 8c) \\ r &= \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d) \end{aligned}$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of equation (13). Consider the elements

$$\begin{aligned} \theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ \theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ \theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \end{aligned}$$

By simple calculations we get the symmetric functions to be

$$\begin{aligned} s_1 &= 2p \\ s_2 &= p^2 - 4r \\ s_3 &= -q^2 \end{aligned}$$

with $\theta_1, \theta_2, \theta_3$ as the roots of the polynomial

$$h(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

From the formula of discriminant for a cubic polynomial we get

$$\begin{aligned} D &= 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3 \\ &= -128b^2d^2 - 4a^3c^3 + 16b^4d - 4b^3c^2 - 27a^4d^2 + 18abc^3 + 144a^2bd^2 - 192acd^2 \\ &+ a^2b^2c^2 - 4a^2b^3d - 6a^2c^2d + 144bc^2d + 256d^3 - 27c^4 - 80ab^2cd + 18a^3bcd \end{aligned}$$

The above equation for the discriminant of a quartic can be simplified for different polynomials as follows:

$$Disc(x^4 + ax + b) = -27a^4 + 256b^3 \tag{14}$$

$$Disc(x^4 + ax^2 + b) = 16b(a^2 - 4b)^2 \tag{15}$$

6.6 Galois group of Cubics

We shall write theorem 3 for a cubic polynomial.

Theorem 4 *:Let $f(x) \in K[X]$ be a separable irreducible cubic polynomial. Let K not have characteristic 2. If discriminant of f is a square in K then the Galois group of $f(x)$ over K is A_3. If disc f is not a square then the Galois group of $f(x)$ over K is S_3.*

Let us look at a few examples.

$f(x)$	disc f	Galois group
$x^3 - x - 1$	-23	S_3
$x^3 - 3x - 1$	81	A_3
$x^3 - 4x - 1$	229	S_3
$x^3 - 5x - 1$	473	S_3
$x^3 - 6x - 1$	837	S_3

Table 1: Examples of Galois group of cubics over $\mathbb{Q}$

In table 1 we look at polynomials of the type $x^3 - ax - 1$ for $1 \leq a \leq 6, a \neq 2$. $x^3 - 2x - 1$ has been left out because it is reducible. Using equation (10) we calculate the discriminant for each polynomial. We make the following observations from table 1:

1. Since $x^3 - 3x - 1$ has a perfect square as the discriminant, it has Galois group A_3 by theorem 4.
2. The rest of the polynomials have Galois group S_3 since their discriminant are not perfect squares.
3. If a cubic polynomial has Galois group A_3 over $\mathbb{Q}$ we see that every root of that polynomial generates the same field extension of $\mathbb{Q}$ and all the roots are real since at least one root is.But the converse need not be true. The polynomial $x^3 - 4x - 1$ has all real roots but has Galois group S_3.

It is important to check if the polynomial is irreducible before applying theorem 4. Here are a few more examples of irreducible cubics over $\mathbb{Q}$ that have Galois group A_3.

$f(x)$	disc f	Roots
$x^3 - 3x - 1$	9^2	$r, \quad r^2 - r - 2, \quad -r^2 + 2$
$x^3 - x^2 - 2x + 1$	7^2	$r, \quad r^2 - r - 1, \quad -r^2 + 2$
$x^3 + x^2 - 4x + 1$	13^2	$r, \quad r^2 + r - 3, \quad -r^2 - 2r + 2$
$x^3 + 2x^2 - 5x + 1$	19^2	$r, \quad r^2 + 2r - 4, \quad -r^2 - 3r + 2$

Table 2: Examples of cubics having Galois group A_3 over $\mathbb{Q}$

In the table 2 we see that all 3 roots of every polynomial has been listed in terms of one of the roots r. From this we can see that the 3 elements of $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$ are, as each automorphism is determined by its effect on r.

Corollary 1:
For any integer k, set $a = k^2 + k + 7$. The polynomial $x^3 - ax + a$ is irreducible over $\mathbb{Q}$ and has Galois group A_3.
Proof:
If a is an odd number then

$$x^3 - ax + a \equiv x^3 + x + 1(mod 2)$$

is irreducible over $\mathbb{Q}$, since $x^3 + x + 1$ is irreducible mod 2. The value of the discriminant is given by

$$-4(-a)^3 - 27a^2 = a^2(4a - 27)$$

For the polynomial to have Galois group A_3 we need $(4a - 27)$ to be a square.

$$4a - 27 = c^2$$
$$a = \frac{1}{4}(c^2 + 27)$$

Since c has to be odd, we make the substitution $c = 2k + 1$

$$a = \frac{1}{4}(4k^2 + 4k + 28) = k^2 + k + 7$$

For any integer k, $k^2 + k + 7$ is odd, so if we denote this value by a then $x^3 - ax + a$ has Galois group A_3 over $\mathbb{Q}$.

Theorem 5 *Let K not have characteristic 2 and $f(x) \in K[X]$ be a separable cubic with discriminant Δ . If r is one root of $f(x)$ then a splitting field of $f(x)$ over K is $K(r,\sqrt{\Delta})$. In particular, if $f(x)$ is a reducible cubic then its splitting field over K is $K(\sqrt{\Delta})$.*

Proof:
Without the loss of generality let $f(x)$ be monic. Let the roots of $f(x)$ be r, r', r''. Write $f(x) = (x - r)g(x)$ so that r' and r'' are the roots of $g(x)$. In particular, $g(r) \neq 0$. By the quadratic formula for $g(x)$ over $K(r)$,

$$K(r, r', r'') = K(r)(r', r'') = K(r)(\sqrt{discg})$$

Since $f(x)$ is monic, so is $g(x)$ and disc $f = g(r)^2$ disc g, so
$K(r,\sqrt{\text{disc}g}) = K(r,\sqrt{\text{disc}f}) = K(r,\sqrt{\Delta})$
If $f(x)$ is reducible, we can take for r above a root of $f(x)$ in K. Then
$K(r,\sqrt{\Delta}) = K(\sqrt{\Delta})$.

6.7 Galois Group of Quartics

By theorem 2 we see that the only possible Galois groups of separable irreducible quartics are the transitive subgroups of S_4.

Type	S_4	A_4	D_4	$\mathbb{Z}/4\mathbb{Z}$	V
(1,1,1,1)	1	1	1	1	1
(1,1,2)	6		2		
(2,2)	3	3	3	1	3
(1,3)	8	8			
(4)	6		2	2	
sum	24	12	8	4	4

Table 3: Transitive subgroups of S_4

where,
S_4 - The symmetric group of degree 4
A_4 - The alternating group of degree 4
D_4 - The dihedral group of order 4
$\mathbb{Z}/4\mathbb{Z}$ - The quotient group, group of remainders modulo 4.
V - The Klein's four-group $\mathbb{Z}/2\mathbb{Z}$ X $\mathbb{Z}/2\mathbb{Z}$
(1,1,1,1) - Identity permutation
(1,1,2) - Transposition
(2,2) - Product of 2-cycles
(1,3) - 3-cycles
(4) - 4-cycles
The transitive subgroups of S_4 isomorphic to

- D_4 are $\langle(1234),(13)\rangle$, $\langle(1324),(12)\rangle$, $\langle(1243),(14)\rangle$
- $\mathbb{Z}/4\mathbb{Z}$ are $\langle(1234)\rangle$, $\langle(1243)\rangle$, $\langle(1324)\rangle$
- V is {(1), (12)(34), (13)(24), (14)(23)}

We make the following observations from the table 3:

1. The only transitive subgroups of S_4 which are inside A_4 are A_4 and V.
2. The only transitive subgroups of S_4 with size divisible by 3 are S_4 and A_4.
3. The only transitive subgroups of S_4 containing a transposition are S_4 and D_4.

Let us consider a monic irreducible quartic polynomial in $K[X]$ having roots r_1, r_2, r_3, r_4 and Disc $f \neq 0$. Then

$$f(x) = x^4 + ax^3 + bx^2 + cx + d = (x - r_1)(x - r_2)(x - r_3)(x - r_4) \qquad (16)$$

The Galois group of separable irreducible cubics is determined by the the value of the discriminant; whether or not its a perfect square. We will see that the Galois group of a Quartic polynomial is determined by an associated cubic polynomial. We can find the polynomial from roots in the splitting field of $f(x)$ over K by finding an expression in the roots of $f(x)$ which has only 3 possible images under the Galois group.Since the Galois group is in S_4, we look for a polynomial in 4 variables which, under all 24 permutations of the variables, has 3 values. One possibility is

$$x_1x_2 + x_3x_4$$

Under S_4, acting on $F(x_1, x_2, x_3, x_4)$, $x_1x_2 + x_3x_4$ can be moved to

$$x_1x_2 + x_3x_4, \quad x_1x_3 + x_2x_4, \quad x_1x_4 + x_2x_3$$

When we specialize $x_i \to r_i$ these become

$$r_1r_2 + r_3r_4, \quad r_1r_3 + r_2r_4, \quad r_1r_4 + r_2r_3$$

It might not be the case that these are all K-conjugates, since not all 24 permutations of the r_i's have to be in the Galois Group. Let us look at the cubic :

$$(x - (r_1r_2 + r_3r_4))(x - (r_1r_3 + r_2r_4))(x - (r_1r_4 + r_2r_3))$$

Since the 3 factors are permuted among themselves by any element of the Galois group , which in this case is a subgroup of S_4, the coefficients of the above polynomial are symmetric polynomials in r_i's. So the coefficients must be in K by Galois theory.

$$(x-(r_1r_2+r_3r_4))(x-(r_1r_3+r_2r_4))(x-(r_1r_4+r_2r_3)) = x^3+Ax^2+Bx+C \quad (17)$$

Expanding we get,

$$\begin{aligned}
A &= -(r_1r_2 + r_3r_4 + r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3) = -b \\
B &= r_1^2r_2r_3 + r_1r_2^2r_4 + r_1r_3^2r_4 + r_2r_3r_4^2 + r_1^2r_2r_4 + r_1r_2^2r_3 + r_1r_3r_4^2 \\
&\quad + r_2r_3^2r_4 + r_1^2r_3r_4 + r_1r_2r_3^2 + r_1r_2r_4^2 + r_2^2r_3r_4 \\
C &= -(r_1r_2 + r_3r_4)(r_1r_3 + r_2r_4)(r_1r_4 + r_2r_3)
\end{aligned}$$

From the symmetric function theorem,

$$\begin{aligned}
B &= s_1s_3 - 4s_4 = ac - 4d \\
C &= -(s_1^2s_4 + s_3^2 - 4s_2s_4) = -(a^2d + c^2 - 4bd)
\end{aligned}$$

Then equation (17) becomes,

$$x^3 + Ax^2 + Bx + C = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd)$$

Cubic Resolvent : When $f(x)$ is a quartic with roots r_1, r_2, r_3, r_4 its *Cubic Resolvent* $R_3(x)$ is the cubic polynomial given by equation (17). When f(x) is monic

$$R_3(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d + c^2 - 4bd)$$

which may be reducible or irreducible. When $a = b = 0$,

$$f(X) = x^4 + cx + d \implies R_3(x) = x^3 - 4dx - c^2 \quad (18)$$

Theorem 6 *The quartic $f(x)$ and its cubic resolvent $R_3(x)$ have the same discriminant. In particular, $R_3(x)$ is separable since $f(x)$ is separable.*

Theorem 7 *Let G_f be the Galois group of $f(x)$ over K. Then G_f can be described in terms of whether or not the discriminant of f is a square in K and if $R_3(x)$ is reducible or irreducible in $K[X]$ as shown in the table below.*

disc f	$R_3(x)$ in $K[X]$	G_f
Not square	irreducible	S_4
Square	irreducible	A_4
Not square	reducible	D_4 or $\mathbb{Z}/4\mathbb{Z}$
Square	reducible	V

Table 4:

Proof:
Let us look at each case separately.

- Disc f is not a square and $R_3(x)$ is irreducible over K

  Since $R_3(x)$ is irreducible over K, and has its roots in the splitting field of $f(x)$ over K; adjoining a root of $R_3(x)$ to K gives us a cubic extension of K inside the splitting field of $f(x)$. Therefore the order of G_f is divisible by 3 and 4. This is possible only if G_f is either S_4 or A_4. Since Disc f is not a square, by theorem 3, $G_f \nsubseteq A_4$. This implies that $G_f = S_4$

- Disc f is a square and $R_3(x)$ is irreducible over K

  By the reasoning mentioned in the case above G_f is either S_4 or A_4. Since Disc f is a square, by theorem 3, $G_f \subset A_4$. This implies that $G_f = A_4$

- Disc f is not a square and $R_3(x)$ is reducible over K

  Since Disc f is not a square, by theorem 3, $G_f \nsubseteq A_4$. Thus the only possibilities are $S_4, D_4, \mathbb{Z}/4\mathbb{Z}$. We will now eliminate the possibility of G_f being S_4.

  By table 3 what distinguishes S_4 from the other 2 is that it contains 3-cycles. If $G_f = S_4$ then $(123) \in G_f$. If we apply this automorphism to the roots of R_3 in its Galois group, it carries them through a single orbit.

  $$r_1r_2 + r_3r_4 \mapsto r_1r_3 + r_2r_4 \mapsto r_1r_4 + r_2r_3 \mapsto r_1r_2 + r_3r_4$$

  These numbers are distinct since $R_3(x)$ is separable. At least one root of $R_3(x)$ lies in K, so the G_f- orbit of that root is just itself, not three numbers. This is a contradiction.

- Disc f is a square and $R_3(x)$ is reducible over K

  Since Disc f is a square, by theorem 3, $G_f \subset A_4$. From table 3 $G_f = A_4$ or $G_f = V$. Like in the previous case we eliminate the first possibility. What distinguishes S_4 from V, is that it contains 3-cycles.If $G_f = A_4$, applying a 3-cycle of A_4 to a root of $R_3(x)$ shows that all the roots of $R_3(x)$ are in a single G_f-orbit, which is a contradiction to $R_3(x)$ being reducible and separable over K. Therefore, $G_f = V$.

Let us take a look at a few examples.

$f(x)$	disc f	$R_3(x)$	G_f
$x^4 - x - 1$	-283	$x^3 + 4x - 1$	S_4
$x^4 + 2x + 2$	$101 \cdot 4^2$	$x^3 - 8x - 4$	S_4
$x^4 + 8x + 12$	576^2	$x^3 - 48x - 64$	A_4
$x^4 + 3x + 3$	$21 \cdot 15^2$	$(x+3)(x^2 - 3x - 3)$	D_4 or $\mathbb{Z}/4\mathbb{Z}$
$x^4 + 5x + 5$	$2 \cdot 55^2$	$(x-5)(x^2 + 5x + 5)$	D_4 or $\mathbb{Z}/4\mathbb{Z}$
$x^4 + 36x + 63$	4320^2	$(x-18)(x+6)(x+12)$	V

Table 5: Examples of Galois group computations over $\mathbb{Q}$

Corollary 2:
With the notation as in theorem 7, $G_f = V$ if and only if $R_3(x)$ splits completely over K and $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$ if and only if $R_3(x)$ has a unique root in K.
Proof:
From table 4 when Disc f is a square and $R_3(x)$ is reducible over K, then $G_f = V$. By theorem 6 since, Disc $R_3(x)$ =Disc f, we can restate it as :$G_f = V$ if and only if Disc $R_3(x)$ is a square in K and $R_3(x)$ is reducible over K. By theorem 5 a splitting field of $R_3(x)$ over K is $K(r,\sqrt{discR_3})$, where r is any root of $R_3(x)$. Therefore, $G_f = V$ if and only if Disc R_3 splits completely over K.
From table 4 when Disc f is not a square and $R_3(x)$ is reducible over K, then $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$. By theorem 6 Disc $R_3(x)$ = Disc f, we can restate it as; $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$ if and only if Disc $R_3(x)$ is not a square in K and $R_3(x)$ is reducible over K. By theorem 5, this implies that $R_3(x)$ has root in K but not splitting completely over K, which is the same as saying $R_3(x)$ has a unique root in K.

Theorem 8 *Let $f(x)$ be an irreducible quartic in $\mathbb{Q}[X]$. If $G_f = \mathbb{Z}/4\mathbb{Z}$ then Disc $f > 0$. Therefore if $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$ and Disc $f < 0$, $G_f = D_4$.*

Proof:
If $G_f = \mathbb{Z}/4\mathbb{Z}$ then the splitting field of $f(x)$ over $\mathbb{Q}$ has degree 4.Any root of $f(x)$ already generates an extension of $\mathbb{Q}$ with degree 4, so the field generated over K by one root of $f(x)$ contains all the other roots. Therefore if $f(x)$ has one real root it has 4 real roots. Thus the number of real roots of $f(x)$ is either 0 or 4.
Case (i): $f(x)$ has 0 real roots.
Then all 4 roots are imaginary, i.e. they are complex conjugates. Let $z, \bar{z}, w$ and $\bar{w}$ be the roots of $f(x)$. Then Disc f is the square of

$$(z-\bar{z})(z-w)(z-\bar{w})(\bar{z}-w)(\bar{z}-\bar{w})(w-\bar{w}) = |z-w|^2|z-\bar{w}|^2(z-\bar{z})(w-\bar{w}) \quad (19)$$

The differences $(z - \bar{z})$ and $(w - \bar{w})$ are purely imaginary (since z and w are not real), so their product is real and nonzero. Thus when we square equation (19) we find that Disc $f > 0$.
Case (ii):
If $f(x)$ has 4 real roots then the product of the product of the difference of its roots is real and nonzero , so Disc $f > 0$.
Let us look at an example for the above theorem:

The polynomial $x^4 + 4x^2 - 2$ which is irreducible by the Eisenstein criterion, has discriminant -18432 (by equation (15)) and cubic resolvent is as follows:

$$x^3 - 4x^2 + 8x - 32 = (x - 4)(x^2 + 8)$$

Applying theorem (7) and table (4) we get that $G_f = D_4$ or $\mathbb{Z}/4\mathbb{Z}$. By theorem (8), since the discriminant is negative, the Galois group must be D_4.
Remark:
The theorem (8) does not distinguish between D_4 and $\mathbb{Z}/4\mathbb{Z}$ when Disc $f > 0$.

6.8 Distinguishing D_4 and $\mathbb{Z}/4\mathbb{Z}$

Theorem 7 tells us that the Galois group of a Quartic is D_4 or $\mathbb{Z}/4\mathbb{Z}$ when it's discriminant is not a square and when the cubic resolvent of the polynomial is reducible over K. Corollary 2 tells us that, then R_3 has a unique root in K.

Theorem 9 (Kappe, Warren) *:*
Let K be a field not of characteristic 2. Let

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[X] \tag{20}$$

and $\Delta = Disc\ f$. Suppose Δ is not a square in K and $R_3(x)$ is reducible in $K[X]$ with unique root $r' \in K$. Then $G_f = \mathbb{Z}/4\mathbb{Z}$ if the polynomials $x^2 + ax + (b - r')$ and $x^2 - r'x + d$ split over $K(\sqrt{\Delta})$ and $G_f = D_4$ otherwise.

Proof:
Let r_1, r_2, r_3, r_4 be the roots of $f(x)$ so that $r' = r_1r_2 + r_3r_4$. Both D_4 or $\mathbb{Z}/4\mathbb{Z}$ as subgroups of S_4 contain 4-cycles. The following table the effect of each 4-cycle in S_4 on $r_1r_2 + r_3r_4$, if the 4-cycle were in the Galois group, is described.

$(abcd)$	$(abcd)(r_1r_2 + r_3r_4)$
(1234)	$r_2r_3 + r_4r_1$
(1432)	$r_4r_1 + r_2r_3$
(1243)	$r_2r_4 + r_1r_3$
(1342)	$r_3r_1 + r_4r_2$
(1324)	$r_3r_4 + r_2r_1$
(1423)	$r_4r_3 + r_1r_2$

We observe from the table that each root of $R_3(x)$ appears twice. Since $r_1r_2 + r_3r_4$ is fixed by G_f the only possible 4-cycles in G_f are (1324) and (1432) (from table). Since they both are each others' inverses and fix $r_1r_2 + r_3r_4$, both are in G_f.

Let $\sigma = (1324)$
If $G_f = \mathbb{Z}/4\mathbb{Z}$ then $G_f = \langle\sigma\rangle$. If $G_f = D_4$ then from subsection 6.7 we see that

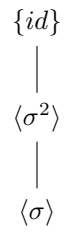
$$G_f = \langle(1324), (12)\rangle \tag{21}$$
$$= \{(1), (1324), (12)(34), (1432), (12), (34), (13)(24), (14)(23)\} \tag{22}$$

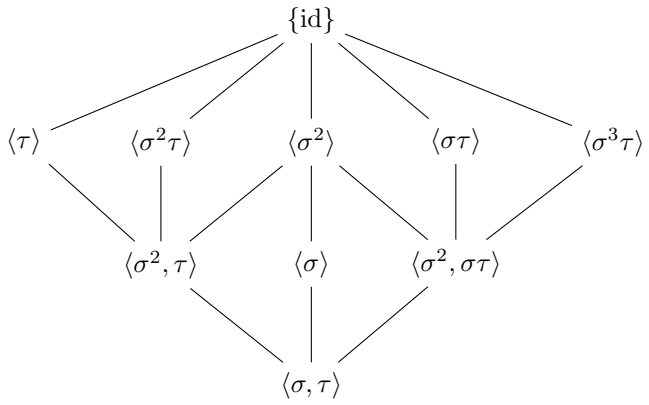
and the elements fixing r_1 are (1) and (34). Let $\tau = (34)$. Then we have

1	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
(1)	(1324)	(12)(34)	(1432)	(34)	(13)(24)	(12)	(14)(23)

Table 6: Products of σ and τ

The subgroup lattices(upside down) of $\langle\sigma\rangle$ and $\langle\sigma,\tau\rangle$ are given:





Corresponding to the above subgroup latices we have the subfield lattices of the splitting field, where L in both cases denotes the unique quadratic extension of K inside $K(r_1)$

- if $G_f = \mathbb{Z}/4\mathbb{Z}$ then L corresponds to $\langle\sigma^2\rangle$
- if $G_f = D_4$ then L corresponds to $\langle\sigma^2, \tau\rangle$

Since Δ is not a square in K $[K(\sqrt{\Delta}) : K] = 2$.
If $G_f = \mathbb{Z}/4\mathbb{Z}$, then $L = K(\sqrt{\Delta})$ since there is only one quadratic extension of K in the splitting field.
If $G_f = D_4$ then let us look at how $K(r_1)$, $K(r_3)$ and $K(\sqrt{\Delta})$ correspond to $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$ and $\langle\sigma^2, \sigma\tau\rangle$. Order of D_4 is 8.

- Since $[K(r_1)\colon K] = 4$ the corresponding subgroup in D_4 of $K(r_1)$ must be of order 2 and fixes r_1. From table 6 this corresponds to $\langle\tau\rangle$.
- Since $[K(r_3)\colon K] = 4$ the corresponding subgroup in D_4 of $K(r_3)$ must be of order 2 and fixes r_3. From table 6 this corresponds to $\langle\sigma^2\tau\rangle$.
- Since $[K(\sqrt{\Delta})\colon K] = 2$ the corresponding subgroup in D_4 of $K(r_3)$ must be of order 4 and is the even permutations in the Galois group and is

{(1),(12)(34),(13)(24),(14)(23)}. From table 6 this corresponds to $\langle \sigma^2, \sigma\tau \rangle$.

Although the two cases $G_f = \mathbb{Z}/4\mathbb{Z}$ and $G_f = D_4$ differ a lot, let us develop a few common ideas regarding the quadratic extensions $K(r_1)/L$ and L/K.
If $G_f = \mathbb{Z}/4\mathbb{Z}$, $\mathrm{Gal}(K(r_1)/L) = \{1\ ,\ \sigma^2\ \}$.
If $G_f = D_4$, $\mathrm{Gal}(K(r_1)/L) = \langle \sigma^2, \tau \rangle / \langle \tau \rangle = \{1\ ,\ \sigma^2\ \}$.
So in both cases, the L- conjugate of r_1 is

$$\sigma^2(r_1) = r_2$$

and the minimal polynomial of r_1 over L must be

$$(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1 r_2$$

Therefore $r_1 + r_2$ and $r_1 r_2$ are in L. Since $[K(r_1)\colon K] = 4$, this polynomial is not in $K[X]$:

$$r_1 + r_2 \notin K \text{ or } r_1 r_2 \notin K \tag{23}$$

If $G_f = \mathbb{Z}/4\mathbb{Z}$ then $\mathrm{Gal}(L/K) = \langle \sigma \rangle / \langle \sigma^2 \rangle = \{1, \bar{\sigma}\}$ and if $G_f = D_4$ then $\mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle / \langle \sigma^2, \tau \rangle = \{1, \bar{\sigma}\}$
The coset of σ in $\mathrm{Gal}(L/K)$ represents the nontrivial coset both times, so $L^\sigma = K$. That is, an element of L fixed by σ is in K. Since

$$\begin{aligned} \sigma(r_1 + r_2) &= r_3 + r_4 \\ \sigma(r_1 r_2) &= r_3 r_4 \end{aligned}$$

the polynomials

$$(x - (r_1 + r_2))(x - (r_3 + r_4)) = x^2 - (r_1 + r_2 + r_3 + r_4)x + (r_1 + r_2)(r_3 + r_4) \tag{24}$$

$$(x - r_1 r_2)(x - r_3 r_4) = x^2 - (r_1 r_2 + r_3 r_4)x + r_1 r_2 r_3 r_4 \tag{25}$$

have coefficients in $L^\sigma = K$.
The linear coefficient in equation (24) is a and the constant term is

$$\begin{aligned} (r_1 + r_2)(r_3 + r_4) &= r_1 r_3 + r_1 r_4 + r_2 r_3 + r_2 r_4 \\ &= b - (r_1 r_2 + r_3 r_4) \\ &= b - r' \end{aligned}$$

so equation (24) equals $x^2 + ax + (b - r')$. The quadratic polynomial (25) is $x^2 - r'x + d$.
When $r_1 + r_2 \notin K$ the polynomial (24) is irreducible in $K[X]$, so its discriminant is not a square in K.
When $r_1 + r_2 \in K$ the polynomial (24) has a double root and its discriminant is 0.
Similarly equation (25) has a discriminant that is not a square in K or is 0.
Therefore the splitting field of (24) or (25) over K is either L or K and (23) tells us at least one of (24) and (25) has a nonsquare discriminant in K.
Since $r_1 + r_2$ and $r_1 r_2$ are in L and $[L : K] = 2$, each one generates L over K if it is not in K. This happens for at least one of the two numbers by (23).
First suppose $G_f = \mathbb{Z}/4\mathbb{Z}$. Then $L = K(\sqrt{\Delta})$, since their roots are in L.

Next suppose $G_f = D_4$. Then $L \neq K(\sqrt{\Delta})$. By (23) at least one of (24) or (25) is irreducible over K, so its roots generate L over K and therefore are not in $K(\sqrt{\Delta})$. Thus the polynomial (24) or (25) will be irreducible over $K(\sqrt{\Delta})$ if it's irreducible over K.
Since the conclusions about the two quadratic polynomials over $K(\sqrt{\Delta})$ are different depending on whether G_f is $\mathbb{Z}/4\mathbb{Z}$ or D_4 these conclusions tell us the Galois group.

6.9 General polynomials of degree ≥ 5

The pinnacle of Galois's theory is his theorem on solvability by radicals. We do not discuss this in detail but merely outline it.
Throughout this section, we take K to be a field of characteristic 0.
A polynomial $f \in K[X]$ is said to be *solvable by radicals over K* if there exists a finite tower of finite field extensions

$$K \subset K_1 \subset K_2 \subset \cdots \subset K_r$$

such that $K_i = K_{i-1}(a_i)$ for some a_i with some power $a_i^{n_i} \in K_{i-1}$ or $a_i^{p_i} - a_i \in K_{i-1}$ for some prime p_i and such that the splitting field of f over K is contained in K_r.
Recall that a finite group G is said to be *solvable* if the derived series

$$G_1 = G, G_2 = [G, G], G_3 = [G_2, G_2], \cdots$$

becomes the trivial group at some finite stage (that is, $G_n = \{1\}$ for some $n \geq 1$).
The basic theorem can be stated as:
Galois's Theorem
Let f be a polynomial of degree n over a field K of characteristic 0, and L be a splitting field of f over K. Then, the Galois group of the Galois extension L/K is solvable if and only if f is solvable by radicals over K.
Indeed, this theorem is the origin of the word "solvable" in the context of group theory. Now, we saw earlier that the general polynomial of degree n has Galois group equal to the full symmetric group S_n. Using the group-theoretic property that S_n is not a solvable group when $n \geq 5$, one has:
Corollary (Galois)
A general polynomial of degree $n \geq 5$ cannot be solved by radicals; that is, there is no single expression in $n + 1$ variables involving addition, multiplication, and taking r-th roots which when applied to the $n + 1$ coefficients of each polynomial of degree n gives its roots.

7 Two non-standard applications

In this section, we describe two applications which are not found in textbooks of Galois theory as they require some additional features. We merely outline these applications.

7.1 The support problem

Let x, y be positive integers such that each prime divisor of $x^n - 1$ also divides $y^n - 1$ for every n. What can we say about the relation between x and y?
For instance, if y is a power of x, the above property holds. We may ask whether the converse also holds. This problem came to be known as the 'support problem' because one calls the 'support' of a natural number a to be the set of its prime divisors. The support problem can be proved using Kummer theory.
Basically, Kummer theory is a correspondence between abelian extensions of a field and subgroups of the n-th powers. This works if the field has enough n-th roots of unity. A more precise statement is:
If K contains the n-th roots of unity, then abelian extensions L of K whose Galois groups have exponent n correspond bijectively to subgroups Ω of K^* containing $(K^*)^n$ via $L \mapsto K^* \cap (L^*)^n$ and its inverse map $\Omega \mapsto K(\Omega^{1/n})$.
The support problem is, in reality, a local-global theorem. To explain:
For a prime p not dividing the numerator and denominators of x and y, look at the order of x mod p; viz., the smallest n such that $p|(x^n - 1)$. We have $p|(y^n - 1)$ so that the order of y mod p divides n, the order of x. A simple exercise in the cyclic group $\mathbb{Z}_p^*$ shows that y must be a power of x mod p.
Therefore, the support theorem says that if y is a power of x modulo p for any prime p, then y is actually a power of x; this is what Kummer theory accomplishes. We do not say any more about it here.

7.2 Polynomials reducible modulo all primes

Consider any integral polynomial f of degree > 1. Then, it is an elementary exercise to show that there are infinitely many primes p such that not divide any of the integers $f(n)$ as n varies over integers. In other words, f does not have roots modulo p. More generally, let us ask:
Question: *If f is an irreducible integral polynomial, is it necessarily irreducible modulo some prime p?*
The answer to this turns out to be 'yes and no' !
It is "yes" if the degree is prime and "no" if it is composite!
In what follows, we show how such questions are attacked and how the earlier lemma is proved. Recall from basic Galois theory that if f is an irreducible, integral polynomial of degree n, its Galois group is a subgroup of the permutation group S_n, permuting the roots transitively.
The answer to the question above lies in knowing whether or not $Gal(f)$ has an element of order n, where $\deg(f) = n$.
Therefore, if $\mathrm{Gal}(f)$ does not contain an element of order n, then f is reducible modulo every prime!
Now, $\mathrm{Gal}(f)$ is a transitive subgroup of S_n and, hence, its order is a multiple of n.
If n is a prime, then evidently $Gal(f)$ must contain an element of order p by Cauchy's theorem.
On the other hand, if n is composite, $\mathrm{Gal}(f)$ may or may not contain an element of order n.
Hilbert showed that the polynomial $x^4 - 10x^2 + 1$ is irreducible over the integers whereas it is reducible modulo each prime (this latter property is

verified using the quadratic reciprocity law). For Hilbert's example, the Galois group is isomorphic to Klein's four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

References

[1] David S.Dummit and Richard M.Foote, *Abstract Algebra*. John Wiley & Sons, USA, Third edition.

[2] Patrick Morandi, *Field and Galois Theory*, Springer-verlang, New york, 1996.

[3] Keith Conrad, *Galois groups of Cubics and Quartics (not in characteristic 2)*.

[4] Ian Stewart, *Galois Theory*, Chapman & Hall, Third edition.

[5] Michael Artin, *Algebra*, PHI learning pvt ltd, New Delhi, 2011.