An Introduction to Galois Theory

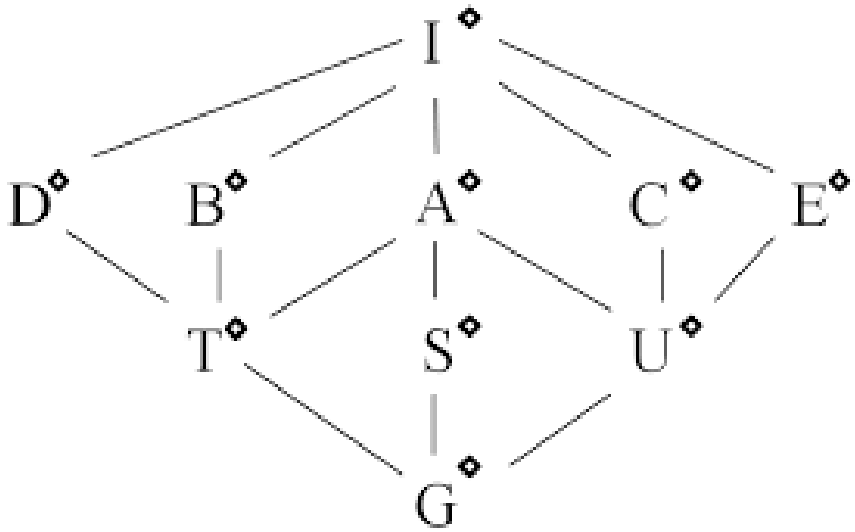
Allison Ramasami James Hazelden

12 December 2017

What is Galois Theory?

Galois Theory provides a connection between Group Theory and Field Theory. It originated with the study of polynomials in higher dimensions and arbitrary fields.

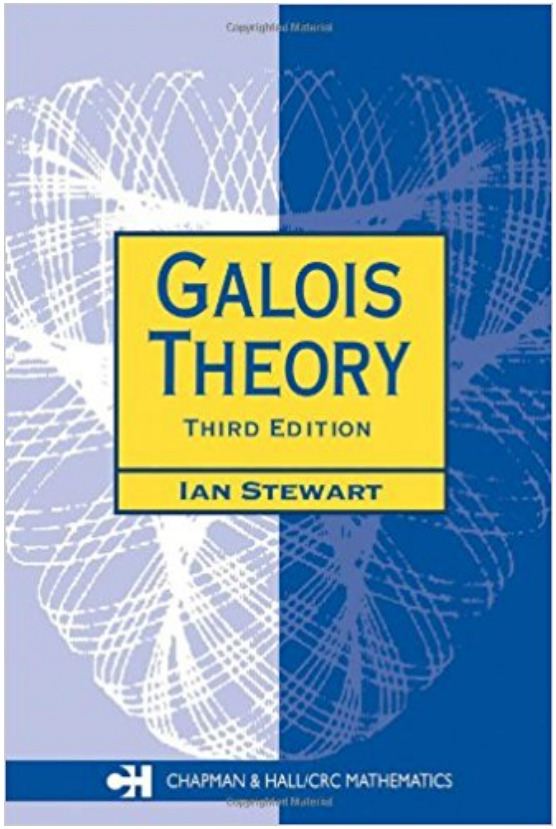
(a) Évariste Galois



(b) Lattice of Galois groups

The Book

Nearly everything we say in this talk comes from Ian Stewart's *Galois Theory*, third edition.



Groups

Definition 1.1

A *group*, $(G, \cdot)$ is a set with a binary operation $\cdot$ such that

1. G is closed under $\cdot$.
2. $\cdot$ is associative.
3. $\cdot$ has identity and inverses.

A group is called *abelian* if the binary operation is also commutative.

A common example of a group is $(\mathbb{Z}_n, +)$, the group of integers mod n under addition. This group is also abelian.

Fields

Definition 1.2

A *field*, $(F, +, \cdot)$, is a set with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, that satisfies these properties:

1. F is closed under $+$ and $\cdot$.
2. $+$ and $\cdot$ are associative and commutative.
3. There is an additive identity 0 and a multiplicative identity 1, where 0 and 1 are distinct.
4. $+$ and $\cdot$ have inverses.
5. $+$ and $\cdot$ obey a distributive law: if $a, b, c \in F$ then $a \cdot (b + c) = a \cdot b + a \cdot c$.

As an example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields.

Subfields

Definition 1.3

A set E is said to be a *subfield* of F if $E \subseteq F$ and E is a field under the same operations as F.

A sufficient condition for a subset of a field to be a subfield is that it is closed under addition, multiplication, additive inverses and multiplicative inverses. An example of a subfield is $\mathbb{Q}$: it is a subfield of $\mathbb{R}$ and $\mathbb{C}$.

Homomorphisms

Definition 1.4

Let F, G be fields. A *field homomorphism* is a function $f : F \to G$ such that for all $a, b \in F$:

1. $f(a + b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$

Note that on the left hand side, we are doing an operation in F, but on the right hand side, we are doing the same operation but in G. A homomorphism can be thought of as a structure-preserving map: it not only maps F to G, but preserves the additive and multiplicative structures of these fields.

Homomorphisms

There are different types of homomorphisms depending on the function at hand:

- A monomorphism is an injective homomorphism.
- An isomorphism is a bijective homomorphism.
- An automorphism is an isomorphism from a field to itself.

A field that is isomorphic to another can be thought of as simply a copy with different "labels" for the elements. The isomorphism essentially just "re-labels" the elements, while preserving the structure.

Polynomials

Definition 1.5

A *polynomial* f over some field F is a function of the form $a_0 + a_1 \cdot t + a_2 \cdot t^2 + ... + a_n \cdot t^n$, where t is an arbitrary indeterminate and $a_i \in F$.

Definition 1.6

An element α of F is said to be a *zero* or *solution* of a polynomial f if $f(\alpha) = 0$.

Polynomials

Definition 1.7

The *degree* of a polynomial p, denoted $\deg(p)$, is the largest exponent that occurs in the polynomial.

Definition 1.8

A polynomial is *monic* if the coefficient on the highest degree term is 1.

Definition 1.9

A polynomial is *reducible* over K if it is the product of two polynomials with coefficients in K of smaller degree. Otherwise it is *irreducible* over K.

Field Extensions

For the remainder of this talk, when we refer to a field, it will always be a subfield of $\mathbb{C}$. While Galois theory is certainly possible and interesting with other fields, we only need $\mathbb{C}$.

Definition 2.1

A *field extension* $L : K$ is an monomorphism $f : K \hookrightarrow L$.

As an example, $\mathbb{R}$ is a field extension of $\mathbb{Q}$ since there is an inclusion map $f : \mathbb{Q} \to \mathbb{R}$. This definition is quite formal, so we will not work with it much.

Field Extensions

Definition 2.2

If A is a set and K is a subfield of $\mathbb{C}$, then the field $K(A)$ is the smallest subfield of $\mathbb{C}$ containing K and A. We say that $K(A)$ is obtained by *adjoining* the elements of A to K.

We note that any field of this form is a field extension of K, and this is the type of extension we will be dealing with for the talk. Here are some examples:

1. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. $\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c\sqrt[3]{3}^2 \mid a, b, c \in \mathbb{Q}\}$.
3. $\mathbb{Q}(\sqrt{5}, i) = \{a + b\sqrt{5} + ci + di\sqrt{5} \mid a, b, c, d \in \mathbb{Q}\}$.

Field Extensions

Proposition 2.3

Any subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

Proof.

Let K be a subfield of $\mathbb{C}$. Then K necessarily contains 0 and 1: otherwise it would not be a field. Because K is closed under addition and additive inverses, we must also get all of $\mathbb{Z}$ in K. Because K is closed under multiplication and multiplicative inverses, we must get all of $\mathbb{Q}$. □

Types of Field Extensions

Definition 2.4

A field extension $L : K$ is *simple* if $L = K(\alpha)$, where $\alpha \in L$.

We will denote the extension $K(\alpha) : K$ instead of $L : K$ for the rest of this talk.

Definition 2.5

Let K be a subfield of $\mathbb{C}$. A number α is *algebraic* over K if there is a polynomial p with coefficients in K such that $p(\alpha) = 0$. Otherwise, α is said to be *transcendental* over K.

We will say algebraic for algebraic over $\mathbb{Q}$ and transcendental for transcendental over $\mathbb{Q}$.

Types of Field Extensions

Definition 2.6

Let $L : K$ be a simple field extension, where $L = K(\alpha)$. Then,

1. $L : K$ is an *algebraic extension* if α is algebraic over K.
2. $L : K$ is a *transcendental extension* if α is transcendental over K.

As an example, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is an algebraic extension because $\sqrt{2}$ is a zero of the polynomial $p(t) = t^2 - 2$.
$\mathbb{Q}(\pi) : \mathbb{Q}$ is a transcendental extension because π is transcendental over $\mathbb{Q}$.

Classifying Simple Extensions

Can we classify all possible simple extensions, up to isomorphism? To do this, we first need to introduce some notation. If K is a field, then we denote

- The polynomial ring $K[t]$ to be the set of all polynomials with indeterminate t and coefficients in K.
- $K(t)$ as the set of rational expressions $\frac{p(t)}{q(t)}$, where $p, q \in K[t]$.

We note that $K(t)$ is a simple transcendental extension of K.

Classifying Simple Extensions

We mentioned up to isomorphism on the previous slide, but what is an isomorphism of field extensions?

Definition 2.7

An isomorphism of two field extensions $K : L$ and $K' : L'$ is a map f such that

1. f is a field isomorphism between L and L'.
2. $f|_K$ is a field isomorphism between K and K'.

Intuitively, we want the big fields L and L' to be isomorphic for the extensions to be isomorphic. If K and K' are different, then f should induce an isomorphism between these two fields because $K \subseteq L$.

Classifying Simple Extensions

Proposition 2.8

Let $L : K$ be a field extension, and $\alpha \in L$. Then there is a unique monic polynomial $p \in K[t]$ such that $p(\alpha) = 0$ and p has minimal degree.

Proof.

We can make any polynomial monic by dividing by the coefficient on the highest degree term, so this is not an issue. To show uniqueness, suppose p, q are two different polynomials such that $p(\alpha) = q(\alpha) = 0$ and both have minimal degree. Then the polynomial $p - q$ is nonzero, has α as a zero and has smaller degree than p and q, since they are both monic. But then $p - q$ has minimal degree, which is a contradiction. □

Classifying Simple Extensions

We call this unique monic polynomial the *minimal polynomial* of α over K.

Lemma 2.9

If m is the minimal polynomial of α over a subfield K of $\mathbb{C}$, then m is irreducible.

Proof.

Suppose m is reducible. Then $m(\alpha) = p(\alpha)q(\alpha) = 0$, so either $p(\alpha) = 0$ or $q(\alpha) = 0$. But then m is not the minimal polynomial, which is a contradiction. □

Classifying Simple Extensions

Before we can give a classification of simple extensions, we must discuss polynomial congruences, which proceeds in a very similar manner to number theory.

Definition 2.10

Let $a, b, m \in K[t]$. We say

$$a \equiv b \pmod{m}$$

if $m \mid a - b$ in $K[t]$.

Similar to integers, $\equiv \pmod{m}$ is an equivalence relation, and addition and multiplication mod m are well defined operations.

Classifying Simple Extensions

Definition 2.11

We define the ring $K[t]/\langle m \rangle$ as the set of equivalence classes of $K[t]$ under the equivalence relation $\equiv \pmod{m}$.

This is technically just a quotient ring modulo an ideal, but the description given here gives a better idea of what is going on in the ring. We note that this ring is a field if and only if m is irreducible.

Classifying Simple Extensions

Now that we have the background out of the way, we can finally classify simple extensions.

Theorem 2.12

Let $K(\alpha) : K$ be a transcendental extension. Then it is isomorphic to the field extension $K(t) : K$ of rational expressions in the indeterminate t.

Classifying Simple Extensions

Proof.

Define the map $f : K(t) \to K(\alpha)$ as

$$\frac{p(t)}{q(t)} \mapsto \frac{p(\alpha)}{q(\alpha)}.$$

We can check that f is a field isomorphism whose restriction to K is the identity map, so these extensions are isomorphic. □

Classifying Simple Extensions

Theorem 2.13

Let $K(\alpha) : K$ be an algebraic extension, and m be the minimal polynomial of α over K. Then there is an isomorphism $f : K(\alpha) \to K[t]/\langle m \rangle$ such that $f|_K$ is the identity.

Proof.

Define $f : K[t]/\langle m \rangle \to K(\alpha)$ by $[p(t)] \mapsto p(\alpha)$, where $[p(t)]$ is the equivalence class of $p(t)$. f is well defined because $f(m(t)) = 0$, and we can verify this is a field isomorphism whose restriction to K is the identity. □

Classifying Simple Extensions

Theorem 2.14

Let $K(\alpha) : K$ and $K(\beta) : K$ be field extensions such that α and β have the same minimal polynomial m. Then these field extensions are isomorphic.

Proof.

Since the big fields $K(\alpha)$ and $K(\beta)$ are isomorphic to $K[t]/\langle m \rangle$, so they are isomorphic to each other. □

Classifying Simple Extensions

With these last couple theorems, we can completely classify simple extensions:

1. There is only one simple transcendental extension up to isomorphism.
2. Algebraic extensions are determined by the minimal polynomial of the element we adjoin.

Degree of a Field Extension

If we have a field extension $L : K$, then we can think of L as a vector space over K in the following sense:

- If $\lambda \in K$ and $v \in L$, then λv is scalar multiplication.
- If $u, v \in L$ then $u + v$ is addition.

Thinking about the field extension in this way, we define the degree of a field extension.

Definition 2.15

The degree of a field extension $[L : K]$ is the dimension of L considered as a vector space over K.

Recall that the dimension of a vector space is the cardinality of any basis of the space.

Degree of a Field Extension

Here are some examples:

1. The extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is the set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. We can then see its degree is 2, as a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is the set $\{1, \sqrt{2}\}$.
2. The extension $\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}$ is the set $\{a + bi + c\sqrt{5} + di\sqrt{5} \mid a, b, c, d \in \mathbb{Q}\}$. Its degree is 4, because a corresponding basis for the extension is the set $\{1, i, \sqrt{5}, i\sqrt{5}\}$.

Degree of a Field Extension

Theorem 2.16

Let $K(\alpha) : K$ be a field extension. If the extension is transcendental, then $[K(\alpha) : K]$ is infinite. If the extension is algebraic, then $[K(\alpha) : K] = \deg(m)$, where m is the minimal polynomial of α over K.

Proof.

If the extension is transcendental, then the set $\{1, \alpha, \alpha^2, \dots\}$ is linearly independent. Since any linearly independent set can be extended to a basis, the degree of the extension is infinite. If the extension is algebraic, then the set $\{1, \alpha, \dots, \alpha^{\deg(m)-1}\}$ is a basis for the space. Therefore the extension has degree $\deg(m)$. □

The Tower Law

While our current methods to determine the degree of an extension do work, they can be quite tedious and confusing if the extension is very complicated. Fortunately, there is an easier way:

Theorem 2.17

Let $K \subseteq M \subseteq L$ be fields. Then

$$[L : K] = [L : M][M : K].$$

Note that if $[L : M]$ or $[M : K]$ are infinite, then $[L : K]$ is infinite as well, and vice versa.

Proof.

Suppose $\{x_i\}_{i \in I}$ is a basis for $M : K$, and $\{y_j\}_{j \in J}$ is a basis for $L : M$. Then one can verify $\{x_i y_j\}_{i \in I, j \in J}$ is a basis for $L : K$. □

The Tower Law

Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$. Then using the Tower Law,

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

We can see that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and it turns out because $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ as well. So the total degree is $2 \cdot 2 = 4$.

The Tower Law

While this works, it can be made more general in the following sense:

Theorem 2.18 (Tower Law)

Let $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$. Then

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0]$$

Proof.

Induct on n and use the previous theorem. □

The Tower Law

We call an extension *finite* if its degree is finite.

Lemma 2.19

An extension $L : K$ is finite if and only if $L = K(\alpha_1, \ldots, \alpha_n)$, where each α_i is algebraic over K.

Proof.

If $L = K(\alpha_1, \ldots, \alpha_n)$ and each α_i is algebraic, then its degree can be shown to be finite by the tower law.
If $L : K$ is finite, suppose its degree is n. Then let $x \in L$, and observe the set $\{1, x, \ldots, x^n\}$ is linearly dependent because it has size $n + 1$. So $a_0 + a_1 x + \cdots + a_n x^n = 0$ where each $a_i \in K$. But this implies x is algebraic over K, so the extension is algebraic. □

Ruler and Compass Constructions

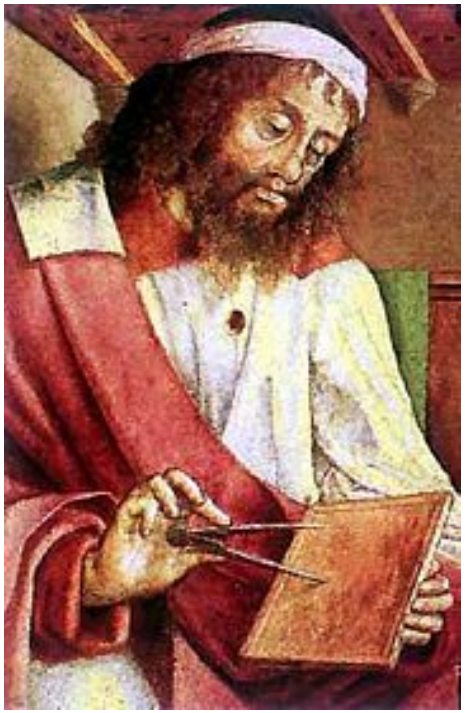
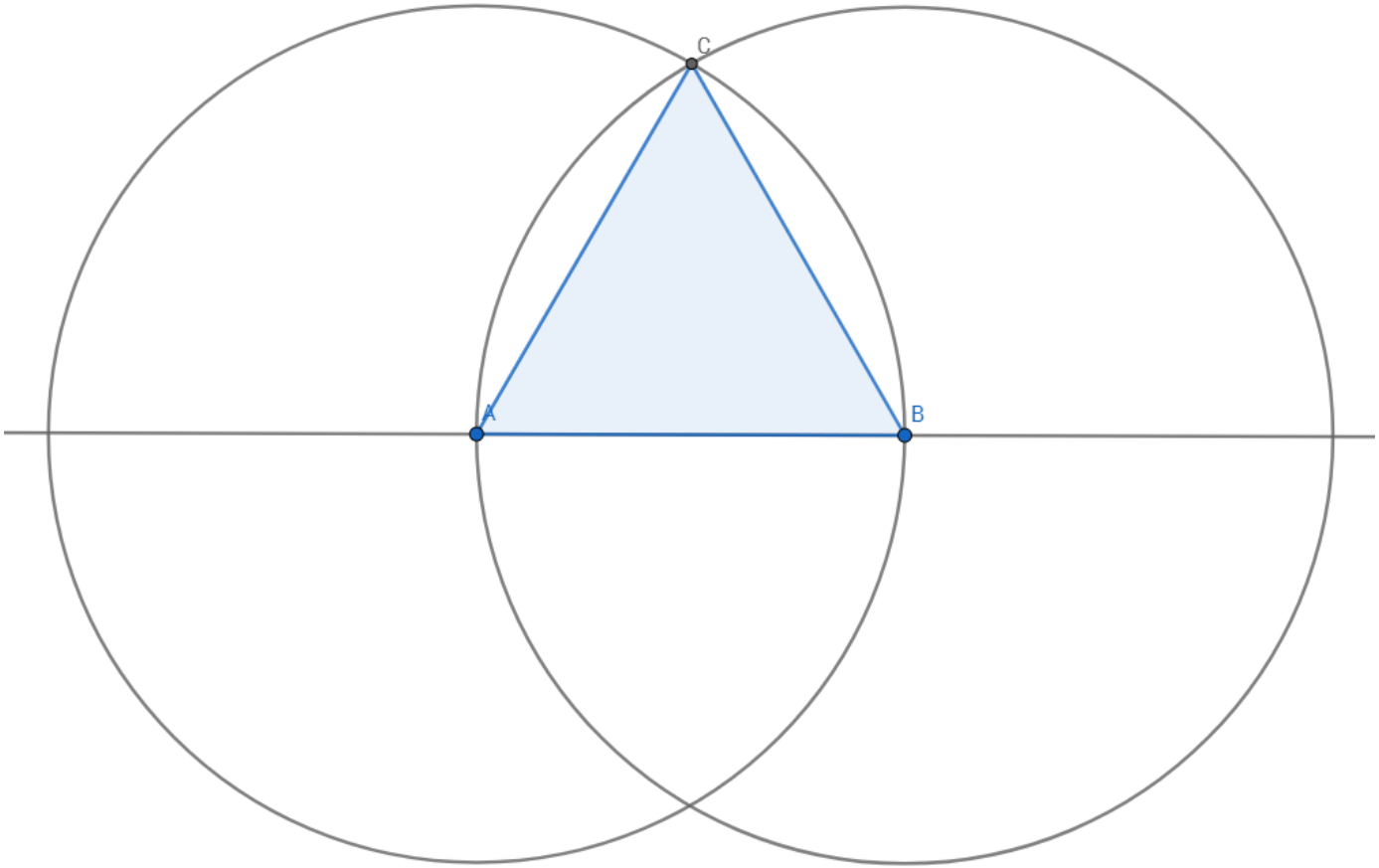


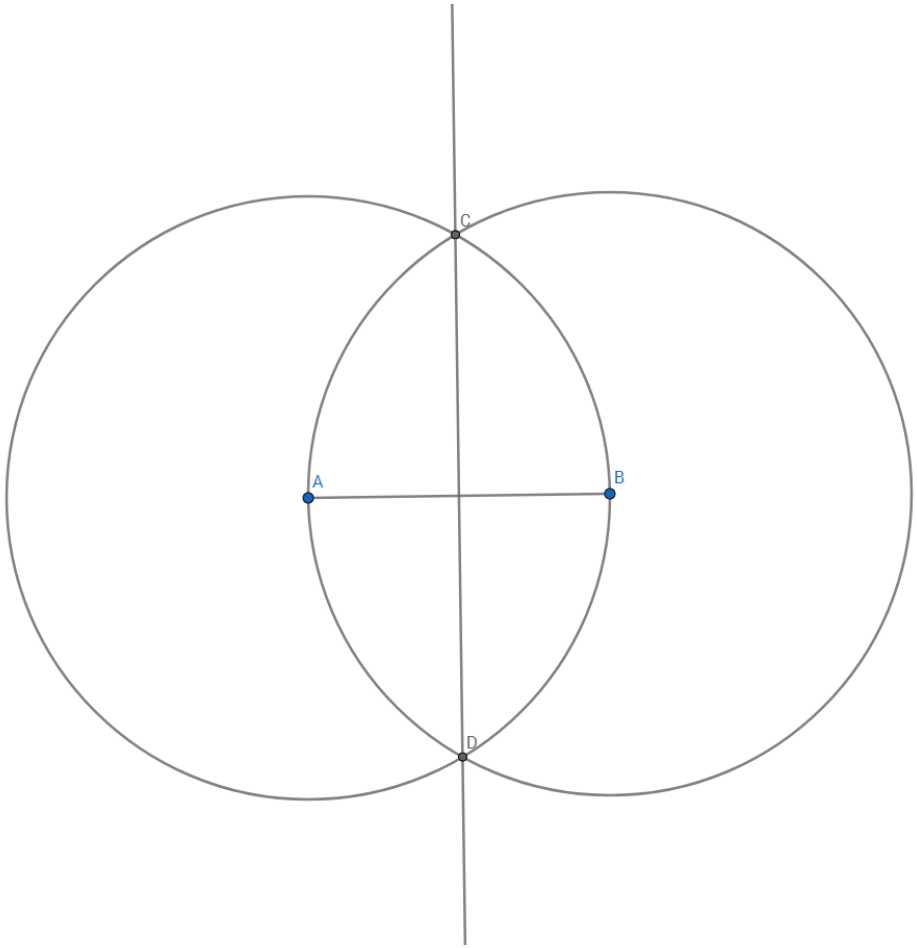
Figure: Euclid

The problem of ruler and compass constructions began with the Ancient Greeks and has been classically studied throughout history. The problem is to construct a shape using only a straight-edge and a compass. We will prove that three classical problems are impossible: *duplicating the cube*, *trisecting the angle*, and *squaring the circle*. First, let's see some examples of possible constructions.

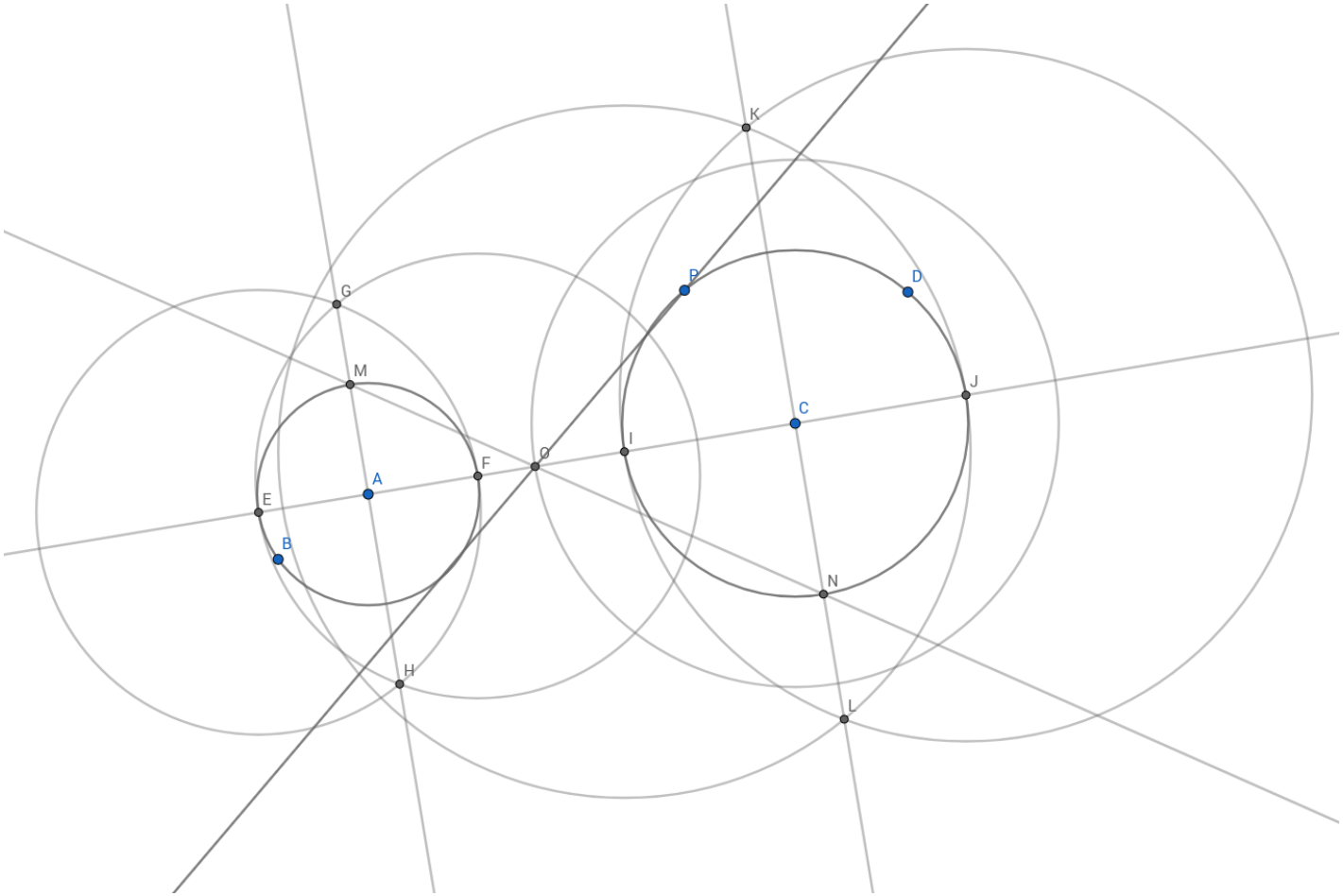
Equilateral Triangle



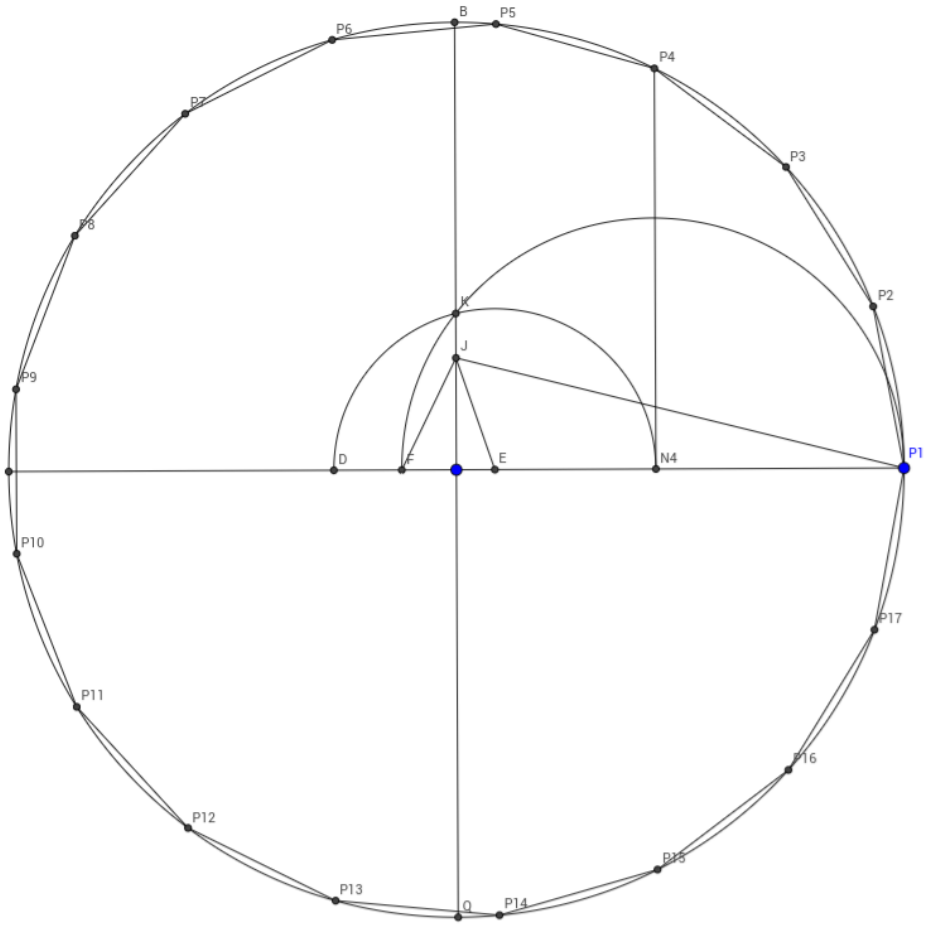
Perpendicular Bisector



Common Tangent to Two Circles



17-Gon


B
P5
P6
P4
P7
P3
P8
P2
K
J
P9
D
F
E
N4
P1
P10
P17
P11
P16
P12
P15
P13
Q
P14

Algebraic Formulation

Definition 3.1

A *ruler and compass construction* is a sequence of applications of the following operations, with $P \subseteq \mathbb{R}^2$:
Ruler: Draw a line through any two points in P,
Compass: Draw a circle whose center is a point in P and whose radius is the distance between two points in P.

Constructibility

Definition 3.2

Let $P_0 \subseteq \mathbb{R}^2$. The points of intersection of any lines and circles drawn using ruler and compass from P_0 are said to be *constructible in one step from* P_0. More generally, a point r is said to be *constructible* if there is a finite sequence of points, $r_1, ..., r_n = r$ such that r_i is constructible from $P_0 \cup \{r_1, ..., r_{i-1}\}$

Constructibility

Lemma 3.3

Let $P \subseteq \mathbb{R}^2$ and let K be the subfield of $\mathbb{R}$ generated by the x and y coordinates in P. Then, if $p = (x, y)$ is constructible in one step from P, x and y are solutions to quadratic equations over K.

Proof.

There are three cases: line intersects with line, line intersects with circle, and circle intersects with circle. In each of these cases, the equations for x or y are reduced to quadratics over K, so we are done. □

Constructibility: Central Theorem

Theorem 3.4

Let r be constructible from $P_0 \subseteq R^2$ by the sequence $r_1, ..., r_n = r$. Define $P_i = P_0 \cup \{r_1, ..., r_i\}$ and K_i to be the subfield of R generated by the x, y coordinates of P_i. With this notation: if $r = (x, y)$ is constructible from P_0, then $[K_0(x) : K_0], [K_0(y) : K_0]$ are powers of 2.

Proof.

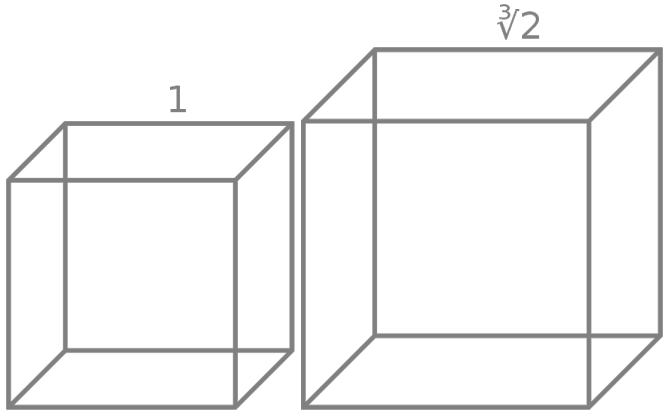
This result is essentially just a generalization of the previous lemma. Just use induction and the tower law. □

Constructibility: Central Theorem

It turns out that this simple theorem is all we need to prove the impossibility of the three constructions we cover. In each case, we prove that if the construction is possible, then we can construct some point that has minimal polynomial with degree not a power of 2. This gives us the desired contradiction. We will cover three different long-standing problems that were resolved with this technique.

Duplicating the Cube

This problem, as with the other two we cover, was first proposed by the Ancient Greeks. The question is this: given the edge of a cube, can we construct a second cube whose volume is double the volume of the original cube? The image should give you a hint: consider the minimal polynomial of $\sqrt[3]{2}$.



Duplicating the Cube

Theorem 3.5

The problem of duplicating the cube using ruler and compass is impossible.

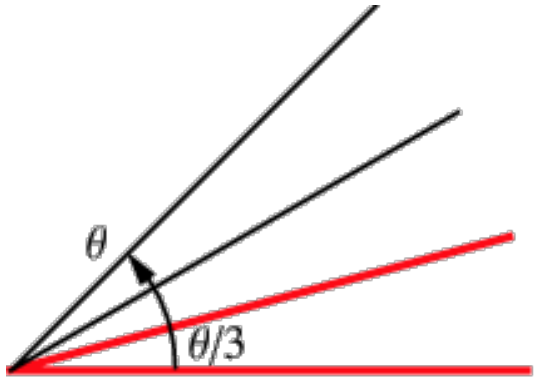
Proof.

We must be able to construct $\alpha = \sqrt[3]{2}$. But this has minimal polynomial $t^3 - 2$ of degree 3. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is not a power of 2. ※ □

Trisecting the Angle

Definition 3.6

This problem is easily stated: given an angle θ construct the angle $\frac{\theta}{3}$ (using ruler and compass).



trisection

Trisecting the Angle

Theorem 3.7

Trisecting the angle is impossible in general. Specifically, the angle $\frac{\pi}{3}$ cannot be trisected with ruler and compass.

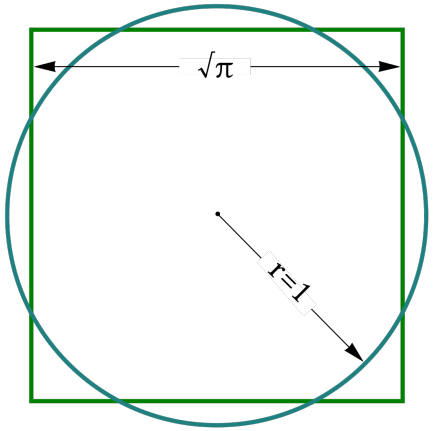
Proof.

We must be able to construct $\beta = 2\cos(\frac{\pi}{9})$. But the triple angle identity, $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$, gives us then that $\beta^3 - 3\beta - 1 = 0$. This polynomial turns out to be irreducible, so this is the minimal polynomial of β, so the extension $\mathbb{Q}(\beta) : \mathbb{Q}$ has degree 3. But for β to be constructible, the extension must have degree a power of 2, but $2^k \neq 3$. ※ □

Squaring the Circle

Definition 3.8

This is the most famous attempted problem of the three. It can be stated as such: given a circle, construct a square with the same area. Claims at solving this problem have been made for over 3000 years! However, Galois Theory shows that it is impossible (with ruler and compass).



Squaring the Circle

Theorem 3.9

The circle cannot be squared using ruler and compass.

Proof.

We have to construct the point $(0, \sqrt{\pi})$. However, if this is constructible, so is the point $(0, \pi)$. But, π is transcendental over $K_0 = \mathbb{Q}$, so the degree $[K_0(\pi) : K_0]$ is infinite and definitely not a power of 2. ※ □

Ruler and Compass Constructions: Summary

So, Galois Theory provides a useful way of looking at ruler and compass constructions and determining what is and isn't constructible. Now, we move on to the the Fundamental Theorem of Galois Theory.

Normal Extensions and Separability

Definition 4.1

Let K be a field. Then a polynomial *splits* over K if it factors into linear factors over K.

As an example, the polynomial $t^2 - 2$ splits over $\mathbb{Q}(\sqrt{2})$, since it factors as

$$t^2 - 2 = (t + \sqrt{2})(t - \sqrt{2}).$$

over $\mathbb{Q}(\sqrt{2})$.
The polynomial $t^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$, since

$$t^3 - 2 = (t - \sqrt[3]{2})(t^2 + \sqrt[3]{2}t + \sqrt[3]{2}^2)$$

and the second factor is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

Normal Extensions and Separability

Definition 4.2

Let K be a field, and $p \in K[t]$ be a polynomial. Then the *splitting field* Σ of p is a field that satisfies

1. p splits over Σ.
2. Σ is the smallest field that does this: if p splits over another field $\Sigma' \supseteq \Sigma$, then $\Sigma = \Sigma'$.

Proposition 4.3

If $p \in K[t]$ and $\alpha_1, \ldots, \alpha_n$ are its roots, then the splitting field of p is simply $K(\alpha_1, \ldots, \alpha_n)$.

Normal Extensions and Separability

Proof.

Clearly, p splits over $K(\alpha_1, \ldots, \alpha_n)$. If p splits over another field $L \subset K(\alpha_1, \ldots, \alpha_n)$, then p will not split over L as it does not contain some root α_i. Therefore the second condition holds. □

Two immediate corollaries of this theorem are that the splitting field is unique and that the extension $\Sigma : K$ has finite degree. This also makes the computation of the splitting field of a polynomial really simple: just adjoin all its roots to the base field, and we have the splitting field. For the example $t^3 - 2$, then its splitting field is $\mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$, where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$.

Normal Extensions and Separability

Definition 4.4

A field extension $L : K$ is *normal* if every irreducible polynomial that has a root in L splits over L.

From the definition, it is not obvious how to determine whether an extension is normal or not.

Theorem 4.5

A field extension $L : K$ is normal and finite if and only if L is the splitting field of some polynomial over K.

Normal Extensions and Separability

Proof.

Suppose $L : K$ is normal and finite. Because it is finite, $L = K(\alpha_1, \ldots, \alpha_n)$ where each α_i is algebraic. Each α_i has a minimal polynomial m_i which is irreducible over K, so we construct the polynomial $f = m_1 \cdots m_n$. L is the splitting field of f because $L = K(\alpha_1, \ldots, \alpha_n)$.

Normal Extensions and Separability

Proof.

Suppose L is the splitting field of $f \in K[t]$. It is finite because it is a splitting field, so we must prove normality. Let $g \in K[t]$ be irreducible and α_1, α_2 be roots of g. The idea is to observe that

$$[L(\alpha_1) : L][L : K] = [L(\alpha_1) : K(\alpha_1)][K(\alpha_1) : K]$$
$$[L(\alpha_2) : L][L : K] = [L(\alpha_2) : K(\alpha_2)][K(\alpha_2) : K].$$

and show the right hand sides of these equations are equal, so $[L(\alpha_1) : L] = [L(\alpha_2) : L]$. This implies if $\alpha_1 \in L$, then $\alpha_2 \in L$ and we are done. □

Normal Extensions and Separability

Definition 4.6

An irreducible polynomial is *separable* over a field K if it has no repeated roots in K.

Over $\mathbb{C}$, every irreducible polynomial is separable. The way to prove this is to show a polynomial p has repeated roots if and only if p and Dp have a non-constant factor in common. Since this is a bit useless in $\mathbb{C}$, we will ignore it for the remainder of this talk.

The Galois Group

Definition 4.7

Let $L : K$ be a field extension. Then a K-automorphism of L is a map $\alpha : L \to L$ such that

1. α is an automorphism of L.
2. If $k \in K$, then $\alpha(k) = k$. In other words, α fixes K.

While this is a complicated definition, one can think of it as a symmetry of the elements we adjoin to K to get L. As an example, the extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ has a $\mathbb{Q}$-automorphism α which sends

1. $\alpha(k) = k$, $k \in \mathbb{Q}$
2. $\alpha(\sqrt{2}) = -\sqrt{2}$

so any polynomial relation that $\sqrt{2}$ satisfies, $-\sqrt{2}$ also satisfies.

The Galois Group

Theorem 4.8

If $L : K$ is a field extension, then the set of all K-automorphisms of L forms a group under function composition.

Proof.

We can check the operation is closed: if α, β are K-automorphisms then $\alpha\beta$ is an automorphism, and if $k \in K$ then $\alpha(\beta(k)) = \alpha(k) = k$. The operation is associative because function composition is associative. The identity is the identity automorphism $\iota(x) = x$, which also fixes K. The inverse of a K-automorphism α is the inverse function α^{-1}, which also fixes K as α fixes K. □

The Galois Group

We call the group of automorphisms above the *Galois group* of the extension $L : K$, which we denote $\Gamma(L : K)$. We will compute two explicit examples of Galois groups: one for $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ and one for $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$.
For $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$, let α be a $\mathbb{Q}$-automorphism. Then

$$\alpha(\sqrt{2})^2 = \alpha(\sqrt{2}^2) = \alpha(2) = 2.$$

From this we can conclude either $\alpha(\sqrt{2}) = \sqrt{2}$ or $\alpha(\sqrt{2}) = -\sqrt{2}$. This actually completely determines the automorphism, because if we take an arbitrary element $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$$\alpha(a + b\sqrt{2}) = \alpha(a) + \alpha(b)\alpha(\sqrt{2}) = a + b\alpha(\sqrt{2}).$$

The Galois Group

So there are two automorphisms in the Galois group:

$$\alpha(a + b\sqrt{2}) = a + b\sqrt{2}$$
$$\beta(a + b\sqrt{2}) = a - b\sqrt{2}$$

so the Galois group is isomorphic to $\mathbb{Z}_2$, the group with two elements.
For the Galois group of $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$, we use the same trick:

$$\alpha(\sqrt[3]{2})^3 = \alpha(\sqrt[3]{2}^3) = \alpha(2) = 2$$

But the only solution to this is $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$, and the Galois group has only one element, the identity.

The Galois Group

Definition 4.9

Let $L : K$ be a field extension. An *intermediate field* M is a subfield of L such that $K \subseteq M \subseteq L$.

Definition 4.10

Suppose $L : K$ is an extension, M is an intermediate field, $G = \Gamma(L : K)$, and H is a subgroup of G. Then M^* is the set of all M-automorphisms of L. $H^\dagger$ is the set of all $x \in L$ such that if $\alpha \in H$, then $\alpha(x) = x$. We call $H^\dagger$ the fixed field of H.

Theorem 4.11

In the definition above, M^* is a subgroup of G and $H^\dagger$ is an intermediate field.

The Galois Group

We can also notice the following two facts:

1. If $M \subseteq N$ are intermediate fields of $L : K$, then $M^* \supseteq N^*$.
2. If $H \subseteq K$ are subgroups of $\Gamma(L : K)$, then $H^\dagger \supseteq K^\dagger$.

We can also observe that if M is an intermediate field and H is a subgroup of $\Gamma(L : K)$, that

1. $M \subseteq M^{*\dagger}$.
2. $H \subseteq H^{\dagger *}$.

This raises a question: when are these inclusions equalities?

Fundamental Theorem of Galois Theory

It turns out this question is answered by the Fundamental Theorem of Galois Theory: specifically, these inclusions are equalities precisely when the extension is normal and separable: we call this a Galois extension. There is an even deeper connection here, however. It turns out that the subgroups of the Galois group correspond exactly with the intermediate fields of the extension by the maps * and †!

Fundamental Theorem of Galois Theory

Theorem 4.12

Suppose $L : K$ is a separable, normal extension with Galois group G. Then if M is an intermediate field and H is a subgroup of G, then

1. $|G| = [L : K]$.
2. * *and* † *are inverses of each other: that is,* $M = M^{*\dagger}$ *and* $H = H^{\dagger *}$.
3. $M : K$ *is normal if and only if* $M^* \triangleleft G$.
4. $[L : M] = |M^*|$.
5. *If* $M : K$ *is normal, then* $\Gamma(M : K)$ *is isomorphic to* $\dfrac{G}{M^*}$.

Fundamental Theorem of Galois Theory

The full proof of this theorem is too large to fit in this presentation, but we can give the idea of the proof here. It relies on monomorphisms rather than automorphisms:

Theorem 4.13

If $\lambda_1, \ldots, \lambda_n$ are distinct monomorphisms, then they are linearly independent.

The trick used in this proof can be used to prove the following theorem:

Theorem 4.14

Let H be a finite subgroup of $\Gamma(L : K)$, and let $M = H^\dagger$. Then $[L : M] = |H|$.

Fundamental Theorem of Galois Theory

We also generalize the idea of a K-automorphism to a K-monomorphism as follows:

Definition 4.15

Suppose $K \subseteq M \subseteq L$ are fields. Then a K-monomorphism is a monomorphism $\alpha : M \to L$ such that if $k \in K$, then $\alpha(k) = k$.

Fundamental Theorem of Galois Theory

With many lemmas and theorems, we arrive at the following big theorem:

Theorem 4.16

If $L : K$ is a finite extension, then the following are equivalent:

1. *$L : K$ is normal.*
2. *There is a finite normal extension N of K containing L such that every K-monomorphism from L to N is a K-automorphism of L.*
3. *For every finite extension M of K containing L, every K-monomorphism from L to M is a K-automorphism of L.*

This, along with the previous theorem allows us to prove nearly all of the Fundamental Theorem.

Fundamental Theorem of Galois Theory

To give a worked example of this in action, we will calculate the Galois group and fixed fields of $\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}$. Since this extension is a splitting field for the polynomial $(t^2-2)(t^2-3)$, we can use the Fundamental Theorem. Suppose α is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Then

$$\alpha(\sqrt{2})^2 = \alpha(\sqrt{2}^2) = \alpha(2) = 2$$
$$\alpha(\sqrt{3})^2 = \alpha(\sqrt{3}^2) = \alpha(3) = 3$$

so $\alpha(\sqrt{2}) = \pm\sqrt{2}$ and $\alpha(\sqrt{3}) = \pm\sqrt{3}$.

Fundamental Theorem of Galois Theory

These facts determine four automorphisms:

$$1 : \alpha(\sqrt{2}) = \sqrt{2},\ \alpha(\sqrt{3}) = \sqrt{3}$$
$$f : \alpha(\sqrt{2}) = -\sqrt{2},\ \alpha(\sqrt{3}) = \sqrt{3}$$
$$g : \alpha(\sqrt{2}) = \sqrt{2},\ \alpha(\sqrt{3}) = -\sqrt{3}$$
$$fg : \alpha(\sqrt{2}) = -\sqrt{2},\ \alpha(\sqrt{3}) = -\sqrt{3}$$

If we look a bit harder at this, we can see there are 5 distinct subgroups of this group. They are $\{1\}$, $\{1, f\}$, $\{1, g\}$, $\{1, fg\}$, and $\{1, f, g, fg\}$.

Fundamental Theorem of Galois Theory

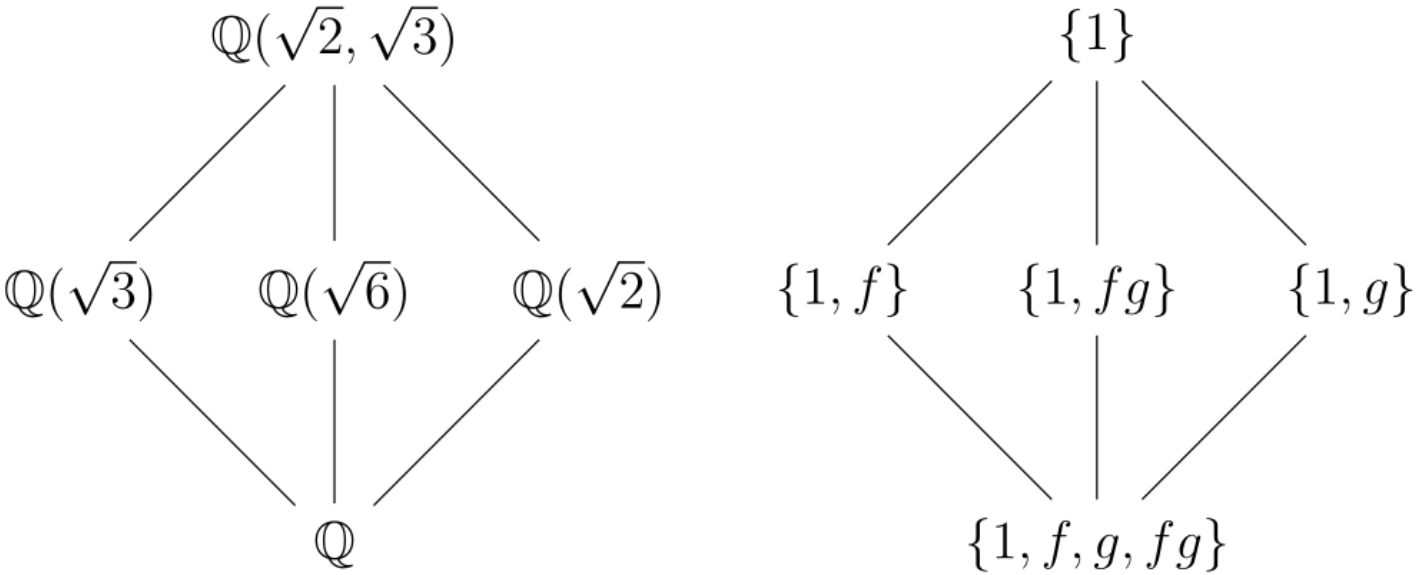
We can now use the Fundamental Theorem to state properties of the original extension: we can find the intermediate fields by finding the fixed fields of all the subgroups of the Galois group. We can see that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$, so the fixed fields are

$$\{1\}^\dagger = \mathbb{Q}(\sqrt{2},\sqrt{3}) \qquad \{1, f, g, fg\}^\dagger = \mathbb{Q}$$
$$\{1, f\}^\dagger = \mathbb{Q}(\sqrt{3}) \qquad \{1, g\}^\dagger = \mathbb{Q}(\sqrt{2}) \qquad \{1, fg\}^\dagger = \mathbb{Q}(\sqrt{6})$$

We also notice that the order of the Galois group is 4, so the degree of the extension should also be 4. We can verify the degree using the Tower Law.

Fundamental Theorem of Galois Theory

These observations can be summed up in the following diagram:



Here the correspondence between subgroups of the Galois group and intermediate fields is clear, and we can also see it reverses inclusions.

Regular Polygons

Now, with this theory in hand, we go back to ruler and compass constructions. The Ancient Greeks knew constructions for the 3-, 5-, and 15-gons and also knew how to construct a regular 2n-gon given a regular n-gon. The natural question, then, is are these all regular polygons that can be constructed by ruler and compass. Gauss showed in 1796 that they are not: constructing the regular 17-gon as shown before. The natural question we ask, then, is what regular polygons are constructible by ruler and compass? First, we must build on the theory a bit.

Regular Polygons

Definition 5.1

We say n is *constructive* if the regular n-gon is constructible by ruler and compass.

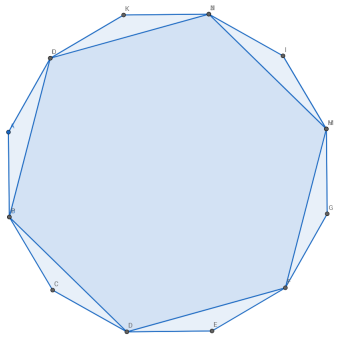
Regular Polygons

Lemma 5.2

If n is constructive and m divides n, then m is constructive.

Proof.

If the n-gon is constructible then join every $\frac{n}{m}$ vertex to construct the regular m-gon. □



Regular Polygons

Lemma 5.3

For any positive integer n, 2^n is constructive.

Proof.

Use induction on n. Each time, bisect the angles of the regular 2^n-gon to get a regular 2^{n+1}-gon. □

Roots of Unity

To describe which polygons are constructible in the language of Galois Theory, we now need a useful notion:

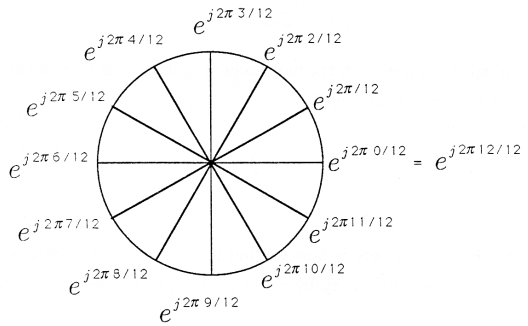
Definition 5.4

The solutions to the polynomial $t^n - 1$ are said to be the *nth roots of unity*. A root of unity ζ is said to be *primitive* if it is not the kth root of unity for any $k < n$.

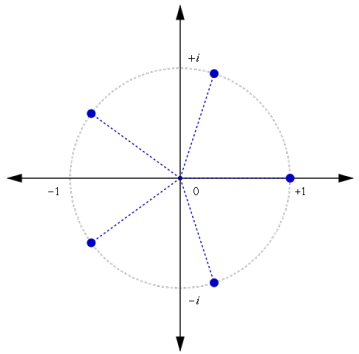
Roots of Unity

Theorem 5.5

In $\mathbb{C}$, the nth roots of unity take the form $e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$ for $k < n$. Here is why we care: in the complex plane, the roots of unity form the vertices of the regular n-gon!



(a) 12th roots of unity



(b) 5th roots of unity

Roots of Unity

Lemma 5.6

Let p be prime, ζ a primitive pth root of unity in $\mathbb{C}$. Then $\mathbb{Q}(\zeta) : \mathbb{Q}$ has degree $p-1$, and, in particular, ζ has minimal polynomial

$$f(t) = 1 + t + ... + t^{p-1}$$

Proof.

Note that $f(t) = \frac{t^p-1}{t-1}$. By definition, ζ is a root of $t^p - 1$, so it is also a solution of $f(t)$. Next, $f(t)$ can be proven to be irreducible by Eisenstein's criterion. □

Regular Polygons

Theorem 5.7

The regular n-gon is constructible by ruler and compass if and only if $n = 2^r p_1 ... p_s$ *where* $r, s \geq 0$, p_i *is an odd prime of the form* $p_i = 2^{2^{r_i}} + 1$ *for positive integers* r_i.

Proof.

The general idea to show necessity is to round the problem down to proving that p_i is of the form $2^{2^{r_i}} + 1$. This follows from the fact that divisors must also be constructive. Showing sufficiency is a little more complicated. We must show that every prime of the form $2^{2^r} + 1$ is constructive. This is done by adjoining the pth root of unity to $\mathbb{Q}$. Show that this extension is Galois, and cyclic and apply the fundamental theorem to round down the degree. □

Regular Polygons

This theorem means that we can construct a regular polygon by ruler and compass if it is of the form 2^n times some sequence of odd primes of the form $2^{2^r} + 1$. Primes of this form are called *Fermat primes*. As of 2017, only 5 Fermat primes are known: they are 3, 5, 17, 257, and 65537. The question of if the number of Fermat primes is finite or not is still an open problem in number theory.

Solubility of the Quintic

We now turn to the problem of the *solubility of the quintic* and polynomials of higher degree. This was Galois' original motivation. A polynomial is soluble if we can find an equation for the roots of any polynomial of that degree using only nested roots. For instance, the quadratic formula just uses second roots. The cubic and quartic formulas also satisfy these criteria. We now show that the quintic and above do not.

Soluble Groups

This notion requires some knowledge of Group Theory that we won't go into detail on here, for the sake of time.

Definition 6.1

A group G is soluble if there is a sequence of normal subgroups $\{1\} = G_0 \triangleleft \ldots \triangleleft G_{n-1} \triangleleft G_n = G$ such that the quotient $\frac{G_{i+1}}{G_i}$ is abelian.

As an example, the group S_3, the symmetric group on 3 elements, is soluble because there is a sequence $\{1\} \triangleleft A_3 \triangleleft S_3$, where $\frac{S_3}{A_3} \cong \mathbb{Z}_2$ and $\frac{A_3}{\{1\}} \cong \mathbb{Z}_3$.

Radical Extensions

Definition 6.2

An extension $L : K$ is radical if there is a sequence

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

where $K_i = K_{i-1}(\beta_i)$, and $\beta_i^{p_i} \in K_{i-1}$, $\beta_i \notin K_{i-1}$.

A radical extension essentially means that we extending by pth roots of elements in the previous extensions. E.g., $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a radical extension by the series $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Soluble Group

Theorem 6.3

The symmetric group S_n is soluble for $n < 5$. Otherwise, it is insoluble.

Notice the 5 above and the fact that we are trying to prove that the 5th degree polynomial is in general insoluble.

The General Polynomial

Definition 6.4

Let K be a field, suppose that $t_1, \ldots, t_n$ are independent transcendental elements over K; i.e., there is no polynomial p over K with $p(t_1, ..., t_n) = 0$. Then the *general polynomial of degree n* "over" K (actually over $K(s_1, ..., s_n)$) is

$$f(t) = t^n - s_1 t^{n-1} + ... - s_{n-1} t^1 + s_n$$

Here the s_i are the elementary symmetric polynomials, defined as

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n \\ s_2 &= t_1 t_2 + t_1 t_3 + \cdots + t_{n-1} t_n \\ &\vdots \\ s_n &= t_1 t_2 \cdots t_n \end{aligned}$$

The General Polynomial

To say a polynomial is solvable is to say that the extension $K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)$ is a radical extension with the previous definition: we can get a formula for the roots in terms of the coefficients of the polynomial and repeated radicals. Now, here is the big theorem:

Theorem 6.5

The Galois group of the splitting field of the general polynomial of degree n, call it Σ, over $K(s_1, ..., s_n)$ is isomorphic to S_n.

The General Polynomial

Proof.

The idea is this: we start with the extension $K(s_1, ..., s_n)$ with the s_is transcendental and independent in K. Then, it can be shown that the t_is must be independent over K. But then we have $n!$ automorphisms of the t_is in $\Sigma : K(s_1, ..., s_n)$. Thus, the Galois group must be isomorphic to S_n. □

Insolubility of the Quintic

Theorem 6.6

Any polynomial of degree 5 or greater is insoluble.

Proof.

Let the degree be $n \geq 5$. We must be able to solve the general polynomial f of degree n by radicals. But the Galois group of f is S_n, which is insoluble for $n \geq 5$. Thus, we cannot solve f by radicals. Q.E.D. □

Thank You!

Questions?