Galois Theory

Laura Stemmler
z5535490@ad.unsw.edu.au

2024

Contents

§1 Introduction

Galois theory was primarily developed by the French mathematician Évariste Galois in the 19th century, with additional contributions from mathematicians such as Niels Henrik Abel. The essence of the theory is to transform problems about polynomials into problems about groups. This is accomplished by deriving groups associated with the polynomials, known as Galois groups. Some classical problems that were solved using Galois theory are the following:

- **Can a polynomial be solved by radicals?** We say that a polynomial is solvable by radicals if its roots can be expressed using the usual arithmetic operations along with taking mth roots of the coefficients of the polynomial. It is well known, for example, that a quadratic polynomial is solvable by radicals and its roots are given by the quadratic formula. It turns out that all polynomials of degree ≤ 4 are solvable by radicals, while, in general, polynomials of degree ≥ 5 are not solvable by radicals. This is known as Abel's impossibility theorem, or the Abel-Ruffini theorem. It is unclear whether Abel or Ruffini proved this result first. Ruffini provided a roughly 500-page proof first, though it is uncertain whether it was a complete proof. Later, Abel gave a much more concise and clear 6-page proof of the result.

  The proof shows that a polynomial of degree n is solvable by radicals if the Galois group of the polynomial is a solvable group (roughly meaning it can be split into abelian groups). We will later see that the Galois group of a polynomial is always a subgroup of the symmetric group S_n (the group of permutations on n elements). Using group theory, it is fairly easy to show that the groups S_1, S_2, S_3,and S_4 are solvable, while S_5 is not.

- **Is it possible to trisect an angle using a ruler and a compass?** Suppose that we want to trisect an angle of 60°. Algebraically, angles can be represented by their trigonometric functions, such as their sines or cosines, which give the Cartesian coordinates of the endpoint of a line segment forming the given angle with the initial segment. Thus, trisecting the angle of 60° involves constructing two line segments such that the ratio of their lengths is $\cos(60/3)$. Hence, trisecting 60°, is equivalent to constructing $\cos 20$. Now, a result from Galois theory tells us that a number is constructible if and only if its Galois group is of order a power of 2. The number $\cos 20$ is a root of the polynomial $8x^3 - 6x - 1$, and its corresponding Galois group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (a group of order 3). Since the order of the Galois group is not a power of 2, it follows that it is not possible to trisect the angle 60° using only a ruler and compass.

- **Can one construct of a Heptadecagon (a 17-sided regular polygon) using a ruler and compass?** This was proven to be possible by Gauss when he was a teenager. A heptadecagon corresponds to the group $(\mathbb{Z}/17\mathbb{Z})^*$, a cyclic group of order 16. Since the order of the group is a power of 2, you can construct the heptadecagon using a ruler and a compass.

Main Idea of Galois Theory:
As mentioned above, Galois theory associates groups with polynomials. The Galois group of a polynomial is derived in the following way: Given a polynomial $a_n x^n + \cdots + a_0$ with rational coefficients, consider the field generated by its roots $\alpha_1, \ldots, \alpha_n$, and define the Galois group as the set of permutations of the roots that preserve all algebraic relations between them.

For example, the polynomial $x^5 - 2$ has roots

$$\alpha_1 = \sqrt[5]{2},\ \alpha_2 = \sqrt[5]{2}\zeta,\ \alpha_3 = \sqrt[5]{2}\zeta^2,\ \alpha_4 = \sqrt[5]{2}\zeta^3,\ \alpha_5 = \sqrt[5]{2}\zeta^4,$$

where ζ is a primitive 5th root of unity. Some algebraic relations among the roots are $\alpha_1\alpha_3 = \alpha_2^2$, and $\alpha_2/\alpha_1 = \alpha_4/\alpha_3$. Thus, we cannot arbitrarily permute these roots and expect to preserve these relations. For this particular set of roots, there are 20 permutations that preserve their relations (compare this with the size of S_5, which is 120).

The formulation of the Galois group as the set of permutations of the roots of a polynomial that preserve their relations is how mathematicians used to think of it. Nowadays, we use a more flexible formulation. We consider an extension of fields $K \subseteq L$, and the Galois group is defined as the group of symmetries of L that fix all elements of K. For example, the Galois group of the extension $\mathbb{R} \subseteq \mathbb{C}$ contains two elements: the identity and complex conjugation. Thus, the Galois group is of order 2 and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Main Theorem in Galois Theory:
Suppose $K \subseteq L$ is a Galois extension (meaning the order of the Galois group is equal to the degree of the extension: $|\text{Galois group}| = [L : K] = \dim_K L$). Then the subfields M with $K \subseteq M \subseteq L$ correspond exactly to subgroups of the Galois group.

Applications of Galois Theory:

- Langlands Program: The Langlands Program is a set of conjectures about the connections between number theory and geometry. It suggests that representations of Galois groups of fields L, with $\mathbb{Q} \subseteq L$, are related to modular forms. Here is an example of this correspondence: Wiles proved Fermat's Last Theorem by starting with a potential solution to Fermat's equation, which leads to an associated elliptic curve (due to Frey). This elliptic curve has an action of the Galois group of the rationals. Wiles showed that from the elliptic curve, one can obtain a modular form. He used the representation of the Galois group to construct the modular form, and most of his paper is a study of the action of the Galois group. Ribet showed that the modular form construction is not possible, thereby proving Fermat's Last Theorem.

- Algebraic Topology: Galois groups are analogous to Fundamental groups in algebraic topology. A field extension $K \subseteq L$ corresponds to a covering space, and the Galois group of $K \subseteq L$ corresponds to the fundamental group of the base space of the covering space. Additionally, algebraic closures correspond to universal covering spaces.

Classical Open Problem in Galois Theory:
Given a finite group G, does there exist a Galois extension K of $\mathbb{Q}$ such that the Galois group of K over $\mathbb{Q}$ is isomorphic to G? This question, known as the inverse Galois problem, has been resolved for many classes of groups, including solvable groups and abelian groups. However, the proof in full generality is still an open problem.

§2 Field Extensions

Definition 2.1 (Field Extension)**.** A pair of fields K and L such that $K \subseteq L$. We often denote it as L/K.

Examples. $\mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{R} \subseteq \mathbb{C}$ are field extensions.

The definition of a field extension will prove to be quite important. The reason is that, if we want to understand a field L, we typically begin by first understanding a smaller field L_0, and then build a chain of fields from L_0 to L: $L_0 \subseteq L_1 \subseteq \cdots \subseteq L$. Thus, we prove results about L by studying L_0 and progressing through the intermediate fields.

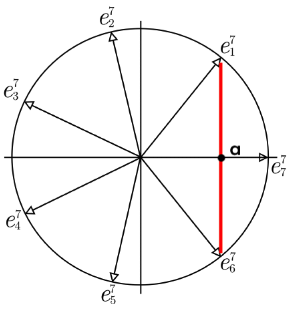
Definition 2.2 (Degree of an Extension)**.** The degree of L/K, denoted $[L : K]$, is the dimension of L as a vector space over K. L/K is said to be finite if $[L : K] < \infty$. Galois theory mostly deals with finite extensions.

Examples. $[\mathbb{C} : \mathbb{R}] = 2$ and $[\mathbb{R} : \mathbb{Q}] = \infty$.

Definition 2.3 (Algebraic and Transcendental Elements)**.** Let $K \subseteq L$ be an extension of fields. An element $\alpha \in L$ is called algebraic over K if α is the root of a polynomial $p(x)$ with coefficients in the field K. Otherwise, α is said to be transcendental. If α is algebraic, the degree of α is equal to the minimal degree of $p(x)$.

Examples of Algebraic and Transcendental Numbers:

- The element $\alpha = \sqrt[5]{2} \in \mathbb{R}$ is an algebraic number over $\mathbb{Q}$ of degree 5, with minimal polynomial $x^5 - 2 = 0$.
- The numbers π and e are transcendental over the rationals. Hermite proved e is transcendental and Lindemann proved π is transcendental.
- Consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}(x)$, where $\mathbb{Q}(x)$ is the field of rational functions over $\mathbb{Q}$. Then x is transcendental over $\mathbb{Q}$.
- Is $\alpha = \cos 2\pi/7 \in \mathbb{R}$ algebraic over $\mathbb{Q}$? Note that $\alpha = \frac{\zeta+\zeta^{-1}}{2}$ where $\zeta = e^{2\pi i/7}$. In the complex plane:



> The irreducible polynomial of ζ is $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$. From this we want to find an irreducible polynomial satisfied by α. Let's divide by ζ^3: $\zeta^{-3} + \zeta^{-2} + \zeta^{-1} + 1 + \zeta + \zeta^2 + \zeta^3 = 0$. Now notice that $(2\alpha)^3 + (2\alpha)^2 - 4\alpha - 1 = 0$. Hence, α is algebraic over $\mathbb{Q}$.

There is a simple criterion we can apply to determine if a number is algebraic. Before stating the criterion, let us first recall a method of constructing finite extensions:

Suppose $p(x)$ is an irreducible polynomial in $K[x]$. Then $K[x]/(p(x))$ is a field. Why? Clearly, the quotient is a ring, so all we have to check is whether inverses exist. Let $q(x) \in K[x]/(p(x))$ with $q \neq 0$. Since $p(x)$ is irreducible, $p(x)$ and $q(x)$ are coprime in $K[x]$. Therefore, we can find polynomials $a(x)$ and $b(x)$ such that $a(x)q(x) + b(x)p(x) = 1$ using the Euclidean algorithm. Thus, $a(x)$ is the inverse of $q(x)$ in $K[x]/(p(x))$. Since every nonzero element of this ring has an inverse, it follows that $K[x]/(p(x))$ is a field. Hence, $K[x]/(p(x))$ is a finite extension of K of degree equal to the degree of p.

Proposition 2.4. *Suppose we have fields $K \subseteq M$. Then $\alpha \in M$ is algebraic over K if and only if α is contained in a finite extension of K.*

Proof. ($\Rightarrow$) Suppose α is algebraic. Then α is a root of $p(x) \in K[x]$ where p can be assumed to be irreducible. There is a well-defined field isomorphism

$$K[x]/(p(x)) \xrightarrow{x \mapsto \alpha} F(\alpha).$$

Hence, $F(\alpha)$ is a field of dimension $\deg p$, and thus, a finite extension of K containing α.
($\Leftarrow$) Suppose α is contained in a finite extension L of K, with $[L : K] = n < \infty$. Consider the set $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$, which consists of $n + 1$ elements. These elements are in an n-dimensional vector space over K. Therefore, there must be a non-trivial linear relation among them: $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, where $a_i \in K$ and they are not all zero. This is a polynomial satisfied by α, so α is algebraic over K. ∎

Theorem 2.5. *If $K \subseteq L \subseteq M$, then $[M : K] = [M : L][L : K]$.*

Proof. Pick a basis $x_1, \dots, x_m$ of L/K, where $m = [L : K]$. Pick a basis $y_1, \dots, y_n$ of M/L, where $n = [M : L]$. Then, the set of products x_iy_j for $1 \leq i \leq m$ and $1 \leq j \leq n$ forms a basis for the vector space M over the field K. ∎

Proposition 2.6. *If $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha + \beta$, $\alpha\beta$, α/β, $\alpha - \beta$.*

Proof. Note $K \subseteq K(\alpha)$ is a finite extension, as is $K(\alpha) \subseteq K(\alpha, \beta)$ (because α and β are algebraic). Since these two extensions are finite $K(\alpha, \beta)$ is a finite extension of K. So any element in $K(\alpha, \beta)$ is algebraic over K. And $K(\alpha, \beta)$ contains $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β. ∎

Proposition 2.7. *If α is a root of a polynomial with algebraic coefficients, then α is algebraic.*

Proof. Assume $K \subseteq L$ and α is a root of the polynomial $a_0 + \cdots + a_{n-1}x^{n-1} + x^n = 0$, where the a_i are algebraic. Consider the following chain of fields:

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

The first n extensions are finite extensions because we assume all the a_is are algebraic. The last extension is finite too because we have $a_0 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. So $K(a_0, \ldots, a_{n-1}, \alpha)$ is a finite extension of K, and therefore, α is algebraic. ■

We mentioned earlier that e and π are transcendental. It is a very hard open problem to answer if $e + \pi$ and $e\pi$ are transcendental. However, the following theorem tells us at least one of them must be transcendental.

Theorem 2.8. *$e + \pi$ or $e\pi$ is transcendental.*

Proof. Look at $x^2 + (e + \pi)x + e\pi$. The roots are e and π. If $e + \pi$ and $e\pi$ are both algebraic, this implies the roots of the polynomial, e and π, are algebraic, which we know is not true. So $e + \pi$ and $e\pi$ cannot both be algebraic. ■

§3 Splitting Fields

Given a field K and a polynomial $p(x) \in K[x]$, can we find an extension $K \subseteq L$ so that all roots of p are in L, meaning p factors into linear factors in the ring $L[x]$? We would also like L to be the smallest possible extension, which is equivalent to saying L is generated by the roots of p over K. A field with these two properties is called a splitting field of K.

Definition 3.1 (Splitting Field)**.** The splitting field of a polynomial $p(x) \in K[x]$ over the field K, is the field extension L/K such that

(i) p factors into linear factors in $L[x]$,

(ii) and L is generated by the roots of p over K.

Examples of Splitting Fields:

- $p(x) = x - a_0 \in K[x]$. The splitting field is K.
- $p(x) = x^2 + a_1x + a_0 \in K[x]$. If this polynomial is reducible, then the splitting field is K. Otherwise, we construct a new field L:

  $$L := K[x]/(p(x)).$$

  L is a field because p is irreducible and it contains all roots of p. It is a splitting field of p.
- $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. This polynomial is irreducible over $\mathbb{Q}$. Define

  $$L := \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2).$$

  The field L contains one of the roots of p, but it does not the other two roots, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$, where ω is a cube root of unity. This is because L is contained in $\mathbb{R}$ so it can't contain the other two complex roots. In L, p splits into

  $$p(x) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2}),$$

  where $x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2}$ is an irreducible factor over L. We adjoin a root of $x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2}$ to L to form a new field

  $$M := L[y]/(y^2 + \sqrt[3]{2}y + \sqrt[3]{2^2}).$$

  So we have $K \subseteq L \subseteq M$ and M is the splitting field. Since $K \subseteq L$ is a degree 3 extension and $L \subseteq M$ is a degree 2 extension, we have $K \subseteq M$ is a degree 6 extension.

- $p(x) = 8x^3 + 4x^2 - 4x - 1 \in \mathbb{Q}[x]$. The roots are $\cos 2\pi/7, \cos 4\pi/7$, and $\cos 6\pi/7$. We can check p is irreducible and form the field extension $\mathbb{Q} \subseteq \mathbb{Q}/(p(x))$ of degree 3. We can write $\cos 4\pi/7$ as $2(\cos 2\pi/7)^2 - 1$. So if we adjoin one of the roots to $\mathbb{Q}$, we automatically adjoin the other roots. So $\mathbb{Q}/(p(x))$ is the splitting field and it's of degree 3.

- $p(x) = x^4 + 1 \in \mathbb{Q}[x]$. This polynomial is irreducible. If α is a root, then so are α^3, α^5, and α^7 (they are all roots of unity). So if you adjoin one root of this polynomial to the rational numbers, we automatically adjoin the other roots. So the splitting field is $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(x^4 + 1)$ and it is of degree 4.

Theorem 3.2 (Existence of Splitting Fields)**.** *For every polynomial $p(x) \in K[x]$, there exists an extension L of K such that L is the splitting field of p over K.*

Proof. Let K be a field and let p be a polynomial in $K[x]$ not necessarily irreducible, so $p = p_1 p_2 \cdots p_1$ where p_i are irreducible in $K[x]$. Set $K_1 = K[x]/p_1(x)$ where deg $p_1 > 1$. Over K_1, p will split more than over K because p_1 is going to split as a linear factor. Repeat with K_1 and some other p_i: set $K_2 = K_1[x]/(p_i(x))$. We can continue reducing the factors of p until they are all of degree 1. This gives us a splitting field of p over K. ■

The constructive proof of splitting fields does not make it entirely obvious that splitting fields are unique up to isomorphism, since at each step we had a choice of what roots to adjoin. The next theorem tells us that splitting fields are isomorphic as extensions. This means that if there are two splitting fields L and L' over K, then there is an isomorphism between L and L' such that the following diagram commutes:

$$\begin{tikzcd}
L \arrow[rr, "\cong"] & & L' \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

This is stronger than saying L is isomorphic to L' as fields.

Theorem 3.3 (Uniqueness of Splitting Fields)**.** *Any two splitting fields of p over K are isomorphic as extensions.*

Proof. Restatement of Theorem: Suppose we have a field K and an isomorphism to a field K'. Suppose we have a splitting field of p over K, L, and a splitting field of p' over K', L', where p' is the image of p under the isomorphism between K and K'.

$$\begin{tikzcd}
L \arrow[r, "?"] & L' \\
K \arrow[u, hook] \arrow[r, "\simeq"] & K' \arrow[u, hook]
\end{tikzcd}$$

We wish to construct an isomorphism from L to L'. We can do this in an even more general setting: instead of assuming L is a splitting field, assume L is generated by some roots of p and assume L' contains all roots of p'. So L may be smaller than a splitting field for p and L' may be a larger than the splitting field of p'.

We start by factorizing p over K, so $p = p_1 p_2 \cdots$ where p_i irreducible in $K[x]$. Extend K to a field $K_1 = K(\alpha)$, the field generated by a root of p_1. Now, $p' = p_1' p_2' \cdots$ and by assumption L' contains all the roots from p_1', say β_1 is one of those roots. Define a map from K_1 to K_1' which sends α_1 to β_1. We continue like this:

$$\begin{tikzcd}
\vdots & \vdots \\
K_2 = K_1(\alpha_2) \arrow[u, hook] \arrow[r] & K_2' = K_1'(\beta_2) \arrow[u, hook] \\
K_1 = K(\alpha_1) \arrow[u, hook] \arrow[r] & K_1' = K'(\beta_1) \arrow[u, hook] \\
K \arrow[u, hook] \arrow[r, "\simeq"] & K' \arrow[u, hook]
\end{tikzcd}$$

We can construct a map of fields from L to L'. In particular, we see that deg L/K $\leq$ deg L'/K' because we have embedded L into L'. We can reverse the argument so deg $L'/K' \leq$ deg L/K. Hence, deg $L/K =$ deg L'/K'. Since they have the same dimension as vector spaces, they must be isomorphic.

■

Problem: is it **a** splitting field or **the** splitting field? Meaning, is there a canonical way of describing the splitting field of a polynomial over a field? Suppose you have an isomorphism between L and L':

$$\begin{tikzcd}
L \arrow[rr, "\cong"] & & L' \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

This isomorphism is not unique. This is a minor book-keeping problem.
Example: the splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C} = \mathbb{R}[i]$. You could also say the splitting field is $\mathbb{R}[j]$, you could map i to j or $-j$.

§4 Algebraic Closure

Definition 4.1 (Algebraic Closure of a Field)**.** Let K be a field. We extend K to a field $\overline{K}$ such that

(i) every polynomial in $K[x]$ factors into linear factors over $\overline{K}$,

(ii) and $\overline{K}$ is generated by roots of polynomials in $K[x]$.

We call $\overline{K}$ the algebraic closure of K.

Construction of Algebraic Closures

Theorem 4.2. *Every field has an algebraic closure.*

Proof. Suppose the field K is countable, so the polynomial ring $K[x]$ is also countable. We can list all the polynomials in $K[x]$ as $p_1, p_2, p_3, \cdots$. Let K_1 be the splitting field of p_1, K_2 be the splitting field of p_2, and so on. Set $\overline{K} = \bigcup K_i$. If K is uncountable, we do something similar by well-ordering the polynomials p_i using the axiom of choice. ■

Definition 4.3 (Algebraically Closed Field)**.** A field L is called algebraically closed if all polynomials in $L[x]$ have roots in L.

We would ideally like for the algebraic closure of a field to be an algebraically closed field. Otherwise, the definition of algebraic closure does not make much sense. So, is it true? We want any polynomial in $\overline{K}[x]$ to have roots in $\overline{K}$. Suppose $p(x) \in \overline{K}[x]$, so $p(x) = x^n + a_{n-1}x^{n-1} + \cdots a_0$ where $a_i \in \overline{K}$. Let α be a root of p. Consider the following extensions of fields:

$$K \subseteq K[a_0, a_1, \dots, a_n] \subseteq K[a_0, a_1, \dots, a_n, \alpha].$$

The field $K[a_0, a_1, \dots, a_n]$ is certainly contained in $\overline{K}$. We want to show $K[a_0, a_1, \dots, a_n, \alpha]$ is also contained in $\overline{K}$. Note that the extension $K \subseteq K[a_0, a_1, \dots, a_n]$ is finite because all the a_i are algebraic over K, as is the extension $K[a_0, a_1, \dots, a_n] \subseteq K[a_0, a_1, \dots, a_n, \alpha]$ because α satisfies a polynomial of coefficients in $K[a_0, a_1, \dots, a_n]$. Therefore, the extension $K \subseteq K[a_0, a_1, \dots, a_n, \alpha]$ is finite. Hence, α is algebraic over K. This means α is the root of a polynomial with coefficients in K and we showed any such polynomial splits in $\overline{K}$. So α is in $\overline{K}$ and thus, any algebraic closure is an algebraically closed field.

Weaker Construction:

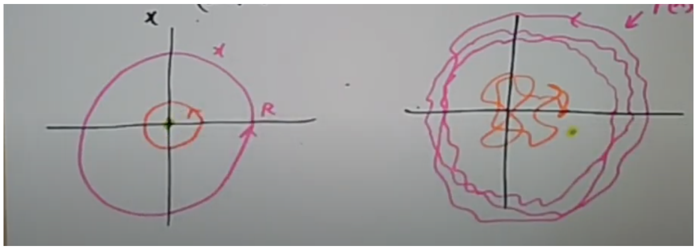
Suppose that instead of asking to find a field containing all the roots of polynomials, we ask the following: Can we find a field L such that $K \subseteq L$ and every element of L has a square root in L? An algebraic closure would have this property but we would like to construct a smaller field that is only closed under taking square roots, and we would like it to be the smallest possible field. Take K_1 to be K adjoin all of the square-roots of elements in K. Set K_2 be K_1 adjoin all the square-roots of elements in K_1, and so on. We can continue this an infinite number of times. Set $L = \bigcup K_i$. Then, L is closed under square-roots and L is generated from K by the usual field operations $+, -, \times, /$ and $\sqrt{\cdot}$.

Note. We could have used a similar argument for the construction of algebraic closures: set K_1 equal to the field generated by all roots of polynomials with coefficients in K_0, K_2 is generated by all roots of polynomials with coefficients in K_1, and so on. Taking the union of the K_i gives us the algebraic closure. This would save us from having to prove that K_1 is algebraically closed. But this is a sloppier argument.

Why do we care about fields closed under square-roots? It is related to problems like squaring a circle or trisecting an angle, and numbers that can be constructed by ruler and compass (Euclidean numbers).

Examples of Algebraically Closed Fields:

- $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$. This is known as the *The Fundamental Theorem of Algebra* which says that the field of complex numbers is algebraically closed. There are several different proofs of this theorem:
  - Liouville gave a proof using complex analysis.
  - There is an algebraic proof which we will go over later.
  - Here is a very short topological proof using winding numbers:
    Suppose $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{C}[x]$. If $|X| = R$ sufficiently large, then $|X^n| > |a_{n-1}X^{n-1} + \cdots + a_0|$. In the complex plane:

    What happens to the values of the polynomial $p(x)$? X^n goes around the origin n times, but it is perturbed slightly by $a_{n-1}X^{n-1} + \cdots + a_0$. It will still go around the origin n times. Imagine making the circle smaller and smaller. We can no longer assume it will go over the origin n times. If we make R even smaller it will look like a point in the complex plane. So it goes around the origin zero times. So there must be some intermediate circle that passes through the origin. So for any $x^n + f(x)$ has zero if $|f(x)| < |x^n|$ for $|x| = R$ fixed.
- $\mathbb{Q} \subseteq \mathbb{C}$ - these are called the *algebraic numbers*. They are the elements of $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. Algebraic number theory is devoted to studying just this field.

- Apart from the two fields mentioned thus far in the list, it is quite hard to think of "natural" examples of algebraic closures. There is one other one, the field of *Puiseux series*. The Laurent series are the power series $\mathbb{C}[[x]][x^{-1}]$ (for example, $x^{-3}e$ is a Laurent series). Puiseux series are a variation of this: $\bigcup_{n\geq 1}\mathbb{C}[[x^{1/n}]][x^{-1/n}]$ (an example is $x^{1/2}+2$). Newton showed (without the definition of algebraic closure) that this field is algebraically close.

Uniqueness of Algebraic Closures

Theorem 4.4. *Any two algebraic closures of a field K are isomorphic.*

However, this isomorphism is not unique and there is no way of making it canonical. So you cannot speak of *the* algebraic closure of a field. This becomes a problem in category theory where you might ask if $K \mapsto \overline{K}$ is a functor. It's difficult to make it into a functor because it is not clear what isomorphism to take. There is another analogous problem like this in algebraic topology: the problem of defining the fundamental group of a topological space X.

§5 Finite Fields

We are going to use splitting fields in order to classify finite fields. In particular, we are going to use the polynomial $x^{p^n} - 1$, where p is prime and n is an integer ≥ 1, to do so. We will see that all finite fields are of order p^n, and that for each prime power p^n, there is a finite field of that order unique up to isomorphism.

Recall. Fields can have characteristics $0, 2, 3, 5, 7, 11, \cdots$. The characteristic of a field is the kernel of the map $\mathbb{Z} \to$ Field. If a field has characteristic 0, then it contains $\mathbb{Q}$, so it can't possibly be finite. If a field has characteristic p, then it contains $\mathbb{Z}/p\mathbb{Z}$ (the finite field of order p – also written as F_p), but the field itself does not have to be finite.

Proposition 5.1. *The order of any finite field is a power of a prime.*

Proof. If F is finite, then it must be of characteristic p for some prime p, and so $F_p \subseteq F$. So F is a vector space over F_p. If the dimension of F as a vector space over F_p is n, then $|F| = p^n$. Hence, the order of any finite field must be the power of some prime. ■

Notation. We use p to denote a prime and q to denote some power of p, so $q = p^n$ where $n \in \mathbb{N}^+$. A finite field of order q will be denoted by $GF(q)$ (it stands for Galois Field–Galois was one of the first to investigate them). It is also denoted by F_q, $GF(p^n)$, and F_{p^n}.

Proposition 5.2. *For any given prime power, there is a unique field of that order.*

Existence:
Let L be the splitting field of $x^q - x \in F_p[x]$. So $F_p \subseteq L$. Look at the roots of $x^q - x$. We will show that the roots form a field. To do so, all there is to show is the roots are closed under $+, -, \times, /$.
Multiplication: Let x and y be roots so $x^q = x$ and $y^q = y$. Then $(xy)^q = xy$.
Addition: If $x^q = x$ and $y^q = y$, then $(x+y)^q = x + y$ because we are in a field of characteristic p.

We can also check all the roots are distinct. A polynomial has distinct roots if it is coprime to its derivative. The derivative of $x^q - x$ is $qx^{q-1} - 1$ which is equal to -1. It is coprime to its derivative, so it has q distinct roots. So the set of roots is the splitting field of $x^q - x$ and it's of order p^n.

Definition 5.3 (Frobenius Endomorphism)**.** $\varphi(a) := a^p$. If $p \neq 0$, then $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(a+b) = \varphi(a) + \varphi(b)$. So φ is a homomorphism from the ring to itself. If we look at the roots of $x^q - x = 0$, this is equivalent to sating $\varphi(x)^n = x$. The roots of $x^q - x$ are the fixed points of $\varphi^n(x) = x$. This is why the roots of are closed under addition and multiplication, because they are the fixed points of an automorphism.

Uniqueness:
All we need to do is show any finite field of order q is a splitting field of $x^q - x$. So we

show all elements $a \in$ finite field are roots of $x^q - x$. For $a = 0$ it is trivial. If $a \neq 0$, then $a \in F^*$ and $|F^*| = q - 1$. And by Lagrange's theorem, $a^{q-1} = 1$, thus $a^q = a$. Hence, any two finite fields of order q are isomorphic.

Examples of Finite Fields:
How do we write an explicit finite field of order $q = p^n$? Choose an irreducible polynomial f in $F_p[x]$ of degree n. Then

$$GF(q) = \frac{F_p[x]}{(f)}.$$

Examples when $p = 2$:
Irreducible polynomials over $F_2[x]$:

$$\begin{aligned}
&\text{degree 1 polynomials: } x,\ x+1 \\
&\text{degree 2 polynomials: } x^2+x+1 \\
&\text{degree 3 polynomials: } x^3+x+1,\ x^3+x^2+1 \\
&\text{degree 4 polynomials: } x^4+x+1,\ x^4+x^3+x^2+x+1,\ x^4+x^3+1 \\
&\qquad\qquad\qquad\vdots
\end{aligned}$$

- Finite field of order $4 = 2^2$: There is only one finite field of order 4

  $$F_2[\omega]/(\omega^2 + \omega + 1).$$

  The elements of this field are $\{0, 1, \omega, \omega + 1\}$.

- Finite field of order $8 = 2^3$: There are two fields of order 8:

  $$F_2[x]/(x^3 + x + 1)$$

  has elements $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$. And

  $$F_2[y]/(y^3 + y^2 + 1)$$

  is also a field of order 8. What is an isomorphism between these two fields? Notice that $(y + 1)^3 = y^3 + y^2 + y + 1 = y$, so $(y + 1)^3 + (y + 1) + 1 = 0$. This is the irreducible polynomial of x. So $x \mapsto y + 1$ gives you an isomorphism between them.

ISO (International Standards Organization) Finite Fields
What is the canonical finite field of order p^n? For example, there are three possible irreducible polynomials we can choose from when constructing a finite field of order

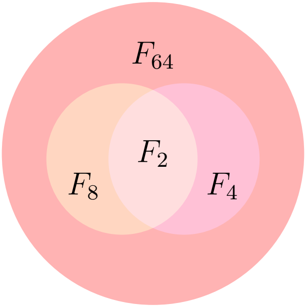
$16 = 2^4$. We present reasons as to why we might choose one irreducible polynomial over the others:

$x^4 + x + 1$: 1st in lexicographic order
$x^4 + x^3 + x^2 + x + 1$: Symmetric, it's roots are the four primitive 5th roots of unity
$x^4 + x^3 + 1$: In reverse order, $1 + x^3 + x^4$, this polynomial comes first

There is no clear choice of irreducible polynomial. So there is no canonical way of choosing a standard finite field. We even have this problem even for degree 2 polynomials: $x^2 - a$. How do you choose $a \in F_p$ that is not a square?

Note that the roots of $x^q - x$ are all the elements of F_q. This allows us to find the number of irreducible polynomials of given degree.

Question: How many irreducible polynomials of degree 6 over F_2 are there?
First, we have $F_{p^m} \subseteq F_{p^n}$ if and only if m divides n. This is because F_{p^n} is a vector space over F_{p^m}, and conversely, if m divides n, F_{p^m} is the set of roots of the polynomial $x^{p^m} - x$ inside the field F_{p^n}. Let's look at the field F_{64}. This field has $64 = 2^6$ elements. Inside it is the field F_{2^3} which has 8 elements, the field F_{2^2} with four elements, and they overlap in the field F_2 with 2 elements.



The two elements in F_2 satisfy irreducible polynomial of degree 1. The 6 remaining elements in F_8/F_2 have irreducible polynomials of degree 3. And the two other elements in F_4 have irreducible polynomial of degree 2.

There are then 54 elements whose irreducible polynomial has degree 6 in F_{64}. This gives the factorization of $x^{64} - x$: $x^{64} - x$ is the product of 9 polynomials of degree 6, 1 polynomial of degree 2, 2 polynomials of degree 3, and 2 polynomials of degree 1.

We can write out the factorization of a polynomial explicitly. For $x^{64} - x$ it is a little bit long but for the field of order 16 we have :

$$x^{16} - x = x(x-1)(x^2 + x + 2)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

§6 Normal Extensions

Throughout this lecture, we assume $K \subseteq L$ is an algebraic extension. Suppose $p \in K[x]$ is irreducible and has a root in L. Are all the other roots of p in L too?

Some extensions we have seen before:

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ does not have this property. The extension contains only one of the roots of $p(x) = x^3 - 2$.
- $p(\alpha) = 8\alpha^3 + 4\alpha^2 + 4\alpha - 1 = 0$. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ contains all the roots.

Definition 6.1 (Normal Field Extension)**.** An algebraic field extension is said to be normal if it satisfies any of the following equivalent conditions:

(i) Any polynomial $p \in K[x]$ that is irreducible and has a root in L, factors into linear factors in $L[x]$.

(ii) L is the splitting field over K of some set of polynomials.

(iii) $K \subseteq L \subseteq \overline{K}$. Any automorphism of $\overline{K}$ fixing all elements of K, maps L to L.

(i) $\Rightarrow$ *(ii)***:**
Take an irreducible polynomial p_α for each $\alpha \in L$. Then L is a splitting field of the set of polynomials $\{p_\alpha \mid \alpha \in L\}$.

(ii) $\Rightarrow$ *(iii)***:**
Suppose L is the splitting field of a set of polynomials $\{p_\alpha\}$. An automorphism σ of $\overline{K}/K$ maps a set of polynomials p_α to itself because σ acts trivially on K. L is the set of roots of all p_α in $\overline{K}$. So L is fixed by σ.

(iii) $\Rightarrow$ *(i)***:**
Suppose $p(x)$ is an irreducible polynomial in $K[x]$ with a root $\alpha \in L$. Observe that for any root β of p in $\overline{K}$, there is an automorphism σ of $\overline{K}$ taking α to β. This is because both α and β are roots of the same irreducible polynomial, so $K(\alpha)$ and $K(\beta)$ are both isomorphic to $K[x]/p(x)$.

$$\begin{tikzcd}
K(\beta) \arrow[r, "\subseteq"] & \overline{K} \\
K(\alpha) \arrow[u] \arrow[r, "\subseteq"] & \overline{K} \arrow[u]
\end{tikzcd}$$

We can extend the automorphism from $\overline{K}$ to $\overline{K}$ with $\sigma(\alpha) = \beta$. By assumption, $\sigma(L) = L$ and $\alpha \in L$, so $\beta = \sigma(\alpha) \in L$.

Examples of Normal Extensions:

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ is a normal extension because it is the splitting field of $x^3 - 2$.
- If $K \subseteq L$ has degree 2, it is a normal extensions.
  Proof: If $L = K(\alpha)$, then $\alpha^2 + b\alpha + c = 0$ for some b and c in K. The roots α and β satisfy $\alpha + \beta = -b$, so $\beta = -b - \alpha \in L$.

Next ask the following question:
Suppose $K \subseteq L \subseteq M \subseteq \overline{K}$, where $K \subseteq L$ is normal and $L \subseteq M$ is normal. Is $K \subseteq M$ normal?
No. Here is a fake proof:
We want to show $\sigma(M) \subseteq M$, where $\sigma \in Aut(\overline{K}/K)$. First σ maps L to L because the extension is normal. Then σ on L over M must map M to M because the extension is normal. QED.

Counterexample:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

Both extensions are degree 2 so they are both normal. However, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal because $x^4 - 2$ has four roots $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}i$. Suppose σ maps $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{2})$. What do we mean by σ fixes $\mathbb{Q}(\sqrt{2})$? Is it $\sigma(\mathbb{Q}(\sqrt{2})) \subseteq \mathbb{Q}(\sqrt{2})$? Or $\sigma(\alpha) = \alpha$ for every $\alpha \in \mathbb{Q}(\sqrt{2})$? In this case σ acts non-trivially.

The term normal for normal extension is closely related to the term normal for normal subgroup in group theory. We will see that intermediate extensions turn out to be normal if and only if they correspond to normal subgroups of the Galois group.

§7 Separable Extensions

Let $K \subseteq L$ be an extension of fields.

Definition 7.1 (Separable Polynomial)**.** A polynomial in $K[x]$ is called separable if it has no multiple roots in $\overline{K}$. This is equivalent to saying f and f' are coprime in $K[x]$.

Definition 7.2 (Separable Element over a Field)**.** An element $\alpha \in L$ is called separable over K if it is the root of a separable polynomial in $K[x]$.

Definition 7.3 (Separable Extension)**.** The extension $K \subseteq L$ is called separable if all $\alpha \in L$ are separable over K.

Examples of Separable Extensions:

- If $K \subseteq L$ and the characteristic of K is 0, then L is separable over K. If f is irreducible then deg f' = deg f - 1, assuming f is not constant. Thus, f and f' are coprime. Hence, f has distinct roots. This fails if the characteristic of K is $p > 0$ because degf' can be less than the deg$f$ - 1. We might have $(f, f') \neq 1$ for f irreducible if $f' = 0$.
- Set $L = k(t)$, where k is a field of characteristic > 0, and set $K = k(t^p)$. So $K \subseteq L$ is an extension of degree p, t satisfies the irreducible polynomial $x^p - t^p \in k(t^p)[x]$. This polynomial is irreducible over $k(t^p)$, but over $k(t)$ is factorizes as $(x - t)^p$. So all roots are the same. Moreover, its derivative is zero. This is an example of an extension that is not separable.
- All extensions of finite fields are separable. If $F_{p^m} \subseteq F_{p^n}$, then all elements of F_{p^n} are roots of $x^{p^n} - x$. This polynomial is separable (it has p^n roots which are all the elements in F_{p^n}, or you can look at its derivative which is -1).

Separable & Normal Extensions

Suppose f is the irreducible polynomial of $\alpha \in L$. Then L being normal implies all roots of f are in L. And L separable implies all roots of f are distinct. So if L is both normal and separable, then f has n distinct roots in L where n is the degree of f.

Purely Inseparable Extensions

This is the opposite notion to separable extensions. These are extensions $K \subseteq L$ with $p = charK$, such that for any $\alpha \in L$, α is a root of $x^{p^n} = a$ for some $a \in K$ and $n \geq 1$. Over an algebraic closure, it factors as $(x - \sqrt[p^n]{a})^{p^n}$, so this polynomial has only one distinct root over its algebraic closure. They are as far as possible from being separable. If you have an arbitrary algebraic extension you can break it up into a separable extension and a purely inseparable extension:

$$K \subseteq K^{\text{sep}} \subseteq L,$$

where $K \subseteq K^{\text{sep}}$ is separable and $K^{\text{sep}} \subseteq L$ is purely inseparable. You construct this by setting K^{sep} to be all the elements of L that are separable over K.

§8 Galois Extensions

Definition 8.1 (Galois Group)**.** Let $K \subseteq M$ be a finite extension of fields. Define the Galois Group of K/M to be $G = Gal(M/K) =$ Automorphisms of M fixing all elements of K.

Definition 8.2 (Finite Galois Extension)**.** A finite extension that satisfies any of the following equivalent conditions.

(i) M is normal and separable over K.

(ii) $[M : K] = |G|$. For any field extension, $|G| \leq [M : K]$. So the symmetry group of M is as large as possible in Galois extensions.

(iii) $K = M^G$ where M^G is the fixed points of M under G.

(iv) M is a splitting field of a separable polynomial over K.

(v) If $K \subseteq L \subseteq M$ as fields and $I \subseteq H \subseteq G$ as groups, the main theorem in Galois theory says there is a one to one correspondence between the subextensions L and the subgroups H. The correspondece is given by $L \mapsto Gal(M/L)$, and $H \mapsto M^H$. For Galois extensions, these maps are inverses of each other and the correspondence is inclusion reversing.

Example:

- If G is a finite group acting on a field M, then $M^G \subseteq M$ is a Galois extension. Example:
  Take $M = k(x_1, x_2, x_3, x_4, x_5)$, the field of rational functions in 5 independent variables, acted on by S_5 which acts as permutations of x_1 up to x_5. Then $M^G = k(e_1, \cdots, e_5)$, where $e_1 = x_1 + x_2 + \cdots x_5$, $e_2 = x_1x_2 + x_1x_3 + \cdots, \cdots$, $e_5 = x_1x_2x_3x_4x_5$, and $\text{Gal}(M/M^G) = S_5$. More generally, for any subgroup $H \subseteq S_5$, $\text{Gal}(M/M^H) = H$.

  We can do this with any symmetric group. By Cayley's theorem, any finite group is contained in a symmetric group.

Inverse Galois Problem

Can we find an extension of $\mathbb{Q}$ with Galois group H? This is a much harder problem. It is still unsolved in general.

Lemma 8.3. *Suppose $K \subseteq M$ and $G = Gal(M/K)$, then $|G| \leq [M : K]$. More generally, we can ask how many extension homomorphisms from M to some field X are there that makes the following diagram commute?*

$$\begin{tikzcd}
K \arrow[r, "\subseteq"] \arrow[d] & M \arrow[dl, dashed] \\
X &
\end{tikzcd}$$

There are at most $[M : K]$ homomorphisms. If we take $X = M$, this proves $|G| \leq [M : K]$.

Proof. M is finite over K, so suppose $M = K(\alpha_1, \cdots, \alpha_n)$. Consider the following chain of fields

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq M.$$

How many homomorphisms are there to the field X?

$$\begin{tikzcd}
K \arrow[r, "\subseteq"] \arrow[d] & K(\alpha_1) \arrow[dl, dashed] \\
X &
\end{tikzcd}$$

α_1 is a root of irreducible polynomial p_1 of degree $[K(\alpha_1) : K]$. A homomorphism must map α_1 to a root of p_1 in X. Once you've mapped α_1 to a root, that determines the homomorphism. How many roots of p_1 are there in X? The number of these in X is $\leq deg(p_1)$ which is $[K(\alpha_1) : K]$. We repeat:

$$\begin{tikzcd}
K(\alpha_1) \arrow[r, "\subseteq"] \arrow[d] & K(\alpha_1, \alpha_2) \arrow[dl, dashed] \\
X &
\end{tikzcd}$$

The number of extensions of the map $K(\alpha) \to X$ to $K(\alpha_1, \alpha_2)$ is at most $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$. So the total number of extensions from $K \to X$ to $K(\alpha_1, \alpha_2) \to X$ is at most the product $[K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] = [K(\alpha_1, \alpha_2) : K]$.

By continuing this argument, we see the number of maps from M to X is at most $[M : K]$. ■

First Four Implications in Definition of Galois Extension:

- $(iv) \Rightarrow (i)$ is trivial.
- $(i) \Rightarrow (ii)$. We wish to show normal plus separable implies $[M : K] = |G|$.
  We have $K \subseteq M \subseteq \overline{K}$. Fact: M/K is separable implies there are exactly $[M : K]$ extensions $M \to \overline{K}$. The proof of this is almost identical to the one of the lemma.

$$\begin{tikzcd} K \arrow[r, "\subseteq"] \arrow[d] & K(\alpha_1) \arrow[dl, dashed] \\ \overline{K} & \end{tikzcd}$$

This time the number of homomorphisms from $K(\alpha_1)$ to $\overline{K}$ is exactly $[K(\alpha_1) : K]$ because α_1 is separable so p_1 has $[K(\alpha_1) : K]$ distinct roots, and $\overline{K}$ is the algebraic closure so it contains all the roots of p_1.

Now M/K normal implies any homomorphism $K \to \overline{K}$ maps M into M, because M is the splitting field of some polynomial $p \in K[x]$, M contains all the roots of p, and any homomorphisms maps roots to roots. So it must map M to M. So we have

$$\begin{tikzcd} K \arrow[r, "\subseteq"] \arrow[d] & M \arrow[dl, dashed] \\ \overline{K} & \end{tikzcd}$$

From separability, the number of extensions $M \to \overline{K}$ is $[M : K]$. From normality, maps from $K \to \overline{K}$ fix M. So the extensions $M \to \overline{K}$ are all in the Galois group of M/K. Therefore $|G| \geq [M : K]$. Together with the Lemma, we have $[M : K] = |G|$.

- $(ii) \Rightarrow (iii)$. Show $[M : K] = |G| \Rightarrow K = M^G$.
  We have $K \subseteq M^G \subseteq M$. By the product formula
  $$[M : K] = [M : M^G][M^G : K].$$
  By the lemma:
  $$[M : K] \geq |Gal(M/M^G)|[M^G : K].$$
  The extension M/M^G has $|G|$ automorphisms, which by assumption equals $[M : K]$. Hence,
  $$[M : K] \geq [M : K][M^G : K].$$
  Thus, $[M^G : K] = 1$, which means $M^G = K$.

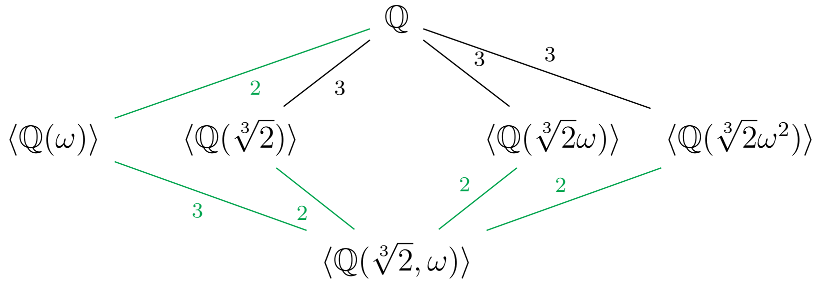
- $(iii) \Rightarrow (iv)$. Show $K = M^G \Rightarrow M$ is the splitting field of a separable polynomial. Pick $\alpha \in M$. Look at all the conjugates of α under G: $\alpha, \beta, \gamma, \cdots$. So β might equal $g_1\alpha$ and γ might equal $g_2\alpha$ and so on. Let α, β, γ all be distinct (do not include the conjugate in the set if it's repeated). Set $p(x) = (x - \alpha)(x - \beta)(x - \gamma)\cdots$. First, p is separable by construction. Secondly, it is fixed by G. So the coefficients are in $M^G = K$ by assumption. So $p \in K[x]$. So any $\alpha \in M$ is a root of a separable polynomial in $K[x]$ with all roots in M. So M is the splitting field of a separable polynomial.

§9 Examples of Galois Extensions

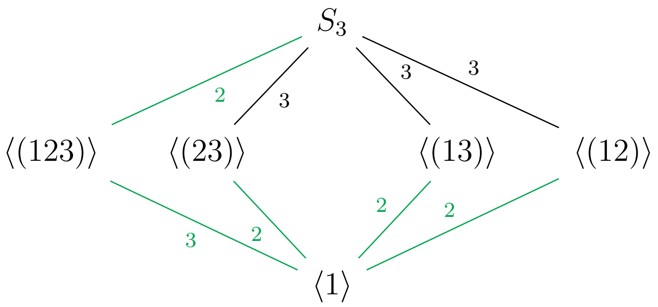
This lecture will focus on condition (v) in the definition of a finite Galois extension. The theorem states that for any finite Galois extension $K \subseteq M$, there is a one to one correspondence between subfields of M containing K and subgroups of the Galois group of M over K.

Examples of the Galois Correspondence:

- $\mathbb{R} \subseteq \mathbb{C}$. The Galois group has two elements : $Gal(\mathbb{C}/\mathbb{R}) = \{1, z \mapsto \bar{z}\}$. There are two subfields of $\mathbb{C}$ containing $\mathbb{R}$: $\mathbb{R}$ and $\mathbb{C}$. The larger field corresponds to the smaller subgroup, so $\{1\}$ corresponds to $\mathbb{C}$ and $\{z \to \bar{z}\}$ corresponds to $\mathbb{R}$.
- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega^2+\omega+1 = 0$. This extension is Galois and its Galois group is isomorphic to S_3 on the three roots of unity: $\sqrt[3]{2}.\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. The subfields of the extension with their degrees are represented in the following diagram:


$\mathbb{Q}$
2
3
3
3
$\langle\mathbb{Q}(\omega)\rangle$
$\langle\mathbb{Q}(\sqrt[3]{2})\rangle$
$\langle\mathbb{Q}(\sqrt[3]{2}\omega)\rangle$
$\langle\mathbb{Q}(\sqrt[3]{2}\omega^2)\rangle$
3
2
2
2
$\langle\mathbb{Q}(\sqrt[3]{2}, \omega)\rangle$

The corresponding subgroups of the Galois group are

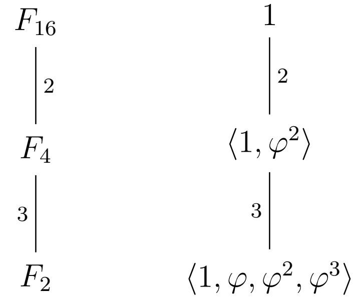


We can ask which extensions are normal and which subgroups are normal (they are both colored green in this example). The subgroup S_3 permutes the subgroups $(23), (13), (12)$ under conjugation (it forms a conjugacy class of three subgroups). Similarly, the Galois group permutes the three corresponding subfields under conjugation. Normal subfields correspond exactly to normal subgroups. The lattice of subfields looks exactly like the lattice of subgroups.

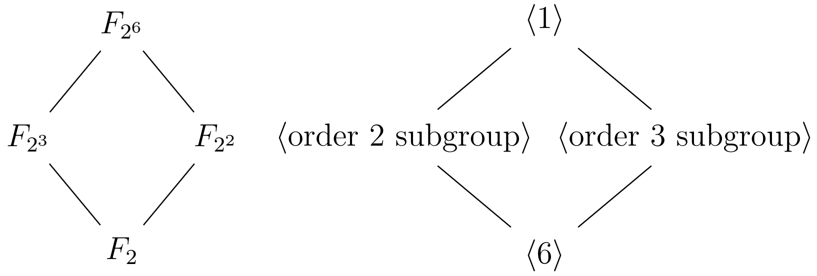
- $\mathbb{F}_2 \subseteq \mathbb{F}_{16}$. What is the Galois group? One obvious automorphism, φ, takes $a \mapsto a^2$, because $a \mapsto a^p$ in characteristic p is a homomorphism (the Frobenius homomorphism). We see then,

  $$\begin{aligned}\varphi^2 &: a \mapsto a^4,\\ \varphi^3 &: a \mapsto a^8,\\ \varphi^4 &: a \mapsto a^{16} = a.\end{aligned}$$

  So φ generates a cyclic group of order 4. The order of the Galois group is equal to the order of the extension which is $[F_{16} : F_2] = 4$. So we have found the full Galois group. The Galois group is $\langle\varphi\rangle$ of order 4. Similarly, if $F_p \subseteq F_{p^n}$, the Galois group is cyclic generated by $a \mapsto a^p$. This is one of the reasons why finite fields are easy to deal with: the Galois groups are cyclic which are easy to understand.

  
  F_{16}
  2
  F_4
  3
  F_2
  1
  2
  $\langle 1, \varphi^2\rangle$
  3
  $\langle 1, \varphi, \varphi^2, \varphi^3\rangle$

  Another example is:

  
  F_{2^6}
  F_{2^3}
  F_{2^2}
  F_2
  $\langle 1\rangle$
  $\langle$order 2 subgroup$\rangle$
  $\langle$order 3 subgroup$\rangle$
  $\langle 6\rangle$

- $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$, where $\zeta^7 = 1$, $\zeta = e^{2\pi i/7}$. The polynomial $x^7 - 1$ is not irreducible, it equals $(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$ where $x^6+x^5+x^4+x^3+x^2+x+1$ is irreducible. The other roots include $\zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6$. The extension is separable because it is characteristic 0, and normal because it is the splitting field of a polynomial, so it is a Galois extension.

  Its Galois Group: any automorphism must map ζ to one of the other roots. So $\sigma(\zeta) = \zeta^i$ for $i = 1, 2, \cdots, 6$. We also see $(\zeta^i)^j = \zeta^{ij}$. The Galois group is $(\mathbb{Z}/7\mathbb{Z})^*$ under the operation of multiplication mod 7. The Galois group is cyclic of order 6. A generator of the might be 3: $3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$. A cyclic group of order 6 has 4 subgroups:

$$\begin{tikzcd}[column sep=small]
 & \{1\} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\{1,6\} \arrow[dr, dash, "3"'] & & \{1,2,4\} \arrow[dl, dash, "2"] \\
 & \{1,2,3,4,5,6\} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\zeta) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\zeta+\zeta^{-1}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\zeta+\zeta^2+\zeta^4) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The element $\zeta + \zeta^{-1}$ equals $2\cos 2\pi/7$, so the cubic extension is $\mathbb{Q}(\cos 2\pi/7)$. The other extension is a quadratic extension and any quadratic extension is generated by the square-root of something. Let $\alpha = \zeta + \zeta^2 + \zeta^4$, this is a good candidate for the field because it is invariant under $\{1,2,4\}$. We have $\alpha^2 = \zeta^2 + \zeta^4 + \zeta + 2\zeta^3 + 2\zeta^6 + 2\zeta^5$. We get $\alpha^2 + \alpha + 2 = 2(\zeta^0 + \zeta^1 + \zeta^2 + \cdots \zeta^6) = 0$. So $\alpha = (-1 \pm \sqrt{-7})/2$. so The field is $\mathbb{Q}(\sqrt{-7})$.

§10 Main Theorem

We restate the Galois Correspondence Theorem and provide a proof.

Theorem 10.1 (Galois Correspondence)**.** *Let $K \subseteq M$ be a finite Galois extension and let G be the Galois group of M/K. If $K \subseteq L \subseteq M$ as fields and $I \subseteq H \subseteq G$ as groups, then there is a one to one correspondence between the subextensions L and the subgroups H. The correspondence is given by $L \mapsto Gal(M/L)$ and $H \mapsto M^H$. These maps are inverses of each other.*

Let $K \subseteq M$ be a finite Galois extension. There are two parts two proving the correspondence:

1. For L intermediate field, we want to show $L = M^{Gal(M/L)}$. It's obvious $L \subseteq M^{Gal(M/L)}$.
2. On the other hand, we also want to show that for H subgroup of the Galois group, $H = Gal(M/M^H)$. Again, it's obvious $H \subseteq Gal(M/M^H)$.

In both cases, to prove the equalities, all we have to do is show both sets have the same size. Then, since one set is contained in the other, they must be the same set.

What do we mean by size?
For a subgroup H of the Galois group size(H) $= |H|$, and for an intermediate field L size(L) $= [M : L]$. This way the size of L will turn out to be the size of the corresponding group.

Hence, our two new objectives are proving:

1. If $H \mapsto M^H$, show $|H| = [M : M^H]$.
2. If $L \mapsto Gal(M/L)$, then $[M : L] = |Gal(M/L)|$.

(i) We showed earlier that M/M^H is Galois, so $|H| = [M : M^H]$ is automatically true.

(ii) Suppose $K \subseteq L \subseteq M$.

$$|Gal(M/K)| = \sum_{maps\ L \to M\ fixing\ K} (number\ of\ extensions\ from\ Im(L)\ to\ M)$$

The number of maps $L \to M$ is at most $[L : K]$. And the number of extensions from $Im(L)$ to M is at most $[M : L]$. So

$$|Gal(M/K)| \leq [L : K][M : L] \leq [M : K].$$

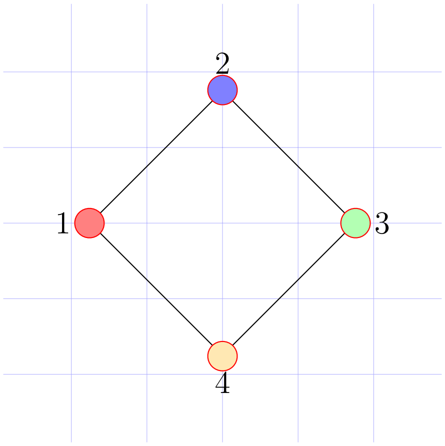
Since, M/K is Galois, $|Gal(M/K)| = [M : K]$. This tells us then that the number of maps extending $Im(L)$ to M is $[M : L]$. So $|Gal(M/L)| = [M : L]$.

What if $K \subseteq M$ is *not* Galois? We look at $K \subseteq M^G \subseteq M$ and $G = Gal(M/K)$. Then we get a 1-1 correspondence between subgroups of G and subextensions $K \subseteq L \subseteq M$ with $M^G \subseteq L$. So we can't tell what is going on between K and the field M^G.

Example of Galois Extension and Correspondence.

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$$

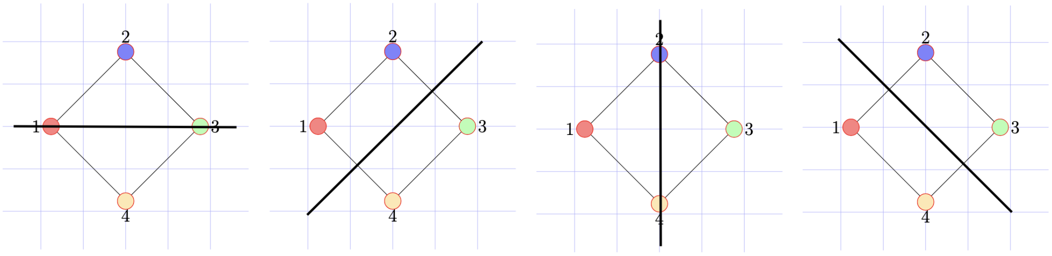
Obvious subextensions: $\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[4]{2}, i)$. Galois group:



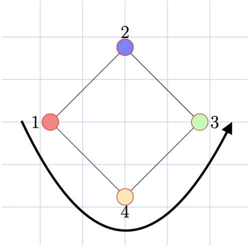
The four fourth roots are : $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$. These form a square and the Galois group must act as permutations of these. In fact, the Galois group must act as the group of symmetries of the square because the Galois group must preserve negation. So the Galois group is a subgroup of the set of automorphisms of the square. On the other hand, the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is degree 4, and the extension $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ is degree 2, so the Galois extension is of degree 8. The group of symmetries of the square has order 8, so the Galois group is all of the symmetries of the square.

Subgroups of the Dihedral group of order 8:

- Trivial subgroup $\{1\}$.
- Subgroups of order 2:
  Reflections



and rotation by 180 degrees



- Subgroups of order 4: the set of symmetries of the rectangle is a subgroup of order 4 of the square. Another order 4 subgroup is rotation by 90 degrees.
- Subgroup of order 8: D_8.

What are the fields corresponding to each subgroup?

We find extra hidden intermediate fields.

Conjugates. The corresponding subfields are conjugates. Almost everything is a normal extension.

§11 Heptadecagon

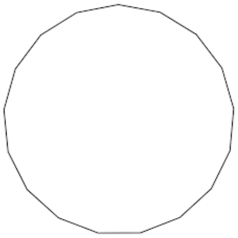


Figure 1: Heptadecagon

From Greek, *hepta* means 7 and *deca* means 10, so a *heptadecogon* is a 17-sided polygon. This lecture is on how to construct a heptadecagon using a ruler and compass.

Definition 11.1 (Constructible Number)**.** A positive real number r is constructable if given a line segment of unit length, we can construct a line segment of length r using a ruler and compass in a finite number of steps.

The definition of constructible number given above is not very easy to work with. The following proposition provides a more useful definition, though we do not present a proof for it.

Proposition 11.2. *A number is constructible if and only if we can construct it from* $\mathbb{Q}$ *using the operations* $+, -, \times, /, \sqrt{}$.

Here comes the theorem that uses Galois theory and proves why we can construct a Heptadecagon.

Theorem 11.3. *A number* α *is constructable if and only if* α *is contained in a normal extension of* $\mathbb{Q}$ *of degree* 2^n*,* $n \geq 0$*.*

Proof. Suppose α is constructable and consider the following chain of fields:

$$K_0 = \mathbb{Q} \subseteq K_1 = K(\sqrt{\alpha_0}) \subseteq K_2 = K_1(\sqrt{\alpha_1}) \subseteq \cdots \subseteq K_n(\alpha).$$

All the subextensions $K_i \subseteq K_{i+1}$ in this chain of the form are of degree 2. So α is in an extension of degree 2^n. But K_n may not be normal. For example, we might have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{\sqrt{2}})$, $\mathbb{Q}(\sqrt{\sqrt{2}})/\mathbb{Q}$ is not a normal extension because it does not contain the complex square roots of 2. So we need to slightly modify this proof. Consider instead the following chain of fields:

$$K_0 = \mathbb{Q} \subseteq K_1 = K_0(\sqrt{\alpha_0}) \subseteq K_2 = K_1(\sqrt{\alpha_1}, \sqrt{\bar{\alpha}_1}) \subseteq K_3 = K_2(\sqrt{\alpha_2}, \sqrt{\alpha_2'}, \sqrt{\alpha_2''}, \cdots) \subseteq \cdots$$

We define K_2 to be K_1 adjoin the square-root of α_1 and the square root of all its conjugates (the roots of the polynomial in the field extension), and we define the rest of the extensions similarly. So $K_0 \subseteq K_1$ is a degree 2 extension, $K_1 \subseteq K_2$ is a degree a power of 2 extension, etc. Hence, α is in a normal extension of a power of 2.

For the other implication, let α be in a normal extension of degree 2^n. Since we are in characteristic 0, it is a separable extension, and thus a Galois extension. Hence, the Galois group G is of order 2^n. Any group of order 2^n is nilpotent. So we can find a chain of subgroups

$$G_n \geq G_{n-1} \geq \cdots \geq G_0 = 1$$

such that each subgroup is normal in the one before and each has index 2 in the previous one. The corresponding fields:

$$Q \leq K_1 \leq K_2 \leq \cdots \leq K_n$$

Each of the field extensions is degree 2. So each K_{i+1} can be generated over K_i by taking the square root of some element. For example, if $\alpha \in K_2$, then $\alpha^2 + a\alpha + b = 0$ for some $b, a \in K_1$. We can write α using the quadratic formula. Hence, α is a constructible number. ■

Example:

- *We cannot construct a regular 7-sided polygon.*
  Constructing a 7-sided polygon is the same as constructing the number $\cos 2\pi/7$. The minimal polynomial of $\cos 2\pi/7$ is of degree 3. So any extension containing $\cos 2\pi/7$ has degree divisible by 3 by the multiplicative formula of degrees, so it is not a power of 2.

Constructing p-sided polygons:
Constructing a p-sided polygon is more or less the same as constructing a p-th root of unity. Recall that the polynomial $x^p - 1$ is not irreducible, but $x_0 + x^1 + \cdots x^{p-1}$ is by Eisenstein's Criterion. Suppose

$$\zeta = \cos 2\pi/p + i \sin 2\pi/p.$$

The other roots of the polynomial are the other p-th roots of unity: $\zeta, \zeta^2, \cdots, \zeta^{p-1}$. So the extension $\mathbb{Q}(\zeta)$ is normal and separable. This is also called a cyclotomic extension (meaning it is generated by roots of unity).
We can work out its Galois group: any automorphism in the Galois group is determined by what it maps ζ to and ζ must be mapped to another root of unity, $\zeta \rightarrow \zeta^i$ for $i \in (\mathbb{Z}/p\mathbb{Z})^*$. The group operation in the group is just multiplication since $(\zeta^i)^j = \zeta^{ij}$. So the Galois group is $(\mathbb{Z}/p\mathbb{Z})^*$. We know it is the whole group because we know the order of the Galois group is $p-1$ and we found $p-1$ automorphisms in $(\mathbb{Z}/p\mathbb{Z})^*$.

When can we construct p-sided polygons? When $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ has degree a power of 2. So whenever

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1 = 2^n$$

for some n. In other words, when $p = 1 + 2^n$ for some n. These are the famous Fermat primes. Fermat proved that n must be a power 2 so the Fermat primes are $2, 3, 5, 17, 257, 65537, \cdots$. The Greeks knew how to construct regular polygons with 2, 3, and 5 sides. More than 2000 years later, Gauss showed you can construct polygons with 17, 257, and 65537 sides.

How to give an explicit description of ζ in terms square-roots: When $p = 17$, the Galois group is $(\mathbb{Z}/17\mathbb{Z})^*$. This is cyclic group generated by the number 3. It has subgroups of size 1, 2, 4, 8, and 16:

$$1 \subseteq \{1, 16\} \subseteq \{1, 4, 13, 16\} \subseteq \{1, 2, 4, 8, 9, 13, 15, 16\} \subseteq \{1, 2, \cdots, 16\}.$$

By the Galois correspondence theorem, we have a corresponding chain of fields

$$\mathbb{Q}(\zeta) \supseteq ? \supseteq ? \supseteq ? \supseteq \mathbb{Q}.$$

We would like to find the generators of the missing fields and express each intermediate field in terms of adjoints of square-roots. Let's look at the first extension corresponding to $1 \subseteq \{1, 16\}$. We would like a field that is fixed by 1 and 16. An obvious candidate is $\zeta^1 + \zeta^{16}$. Notice that the subgroup $\{1, 16\}$ has various cosets: $\{1, 16\}, \{2, 15\}, \{3, 14\}, \cdots$. There are corresponding elements $\zeta^1 + \zeta^{16}, \zeta^2 + \zeta^{15}, \zeta^3 + \zeta^{14}, \cdots$, and these are all conjugates of $\zeta^1 + \zeta^{16}$ under the Galois group. We can do the same thing with the subgroup $\{1, 4, 13, 16\}$, its cosets are $\{2, 8, 9, 15\}$, $\{3, 12, 5, 14\}$, and $\{6, 7, 10, 11\}$. The subgroup $\{1, 2, 4, 8, 9, 13, 15, 16\}$ has only two cosets: $\{1, 2, 4, 8, \cdots\}$ and $\{3, 5, 6, 7, \cdots\}$. For every coset you can write a corresponding sum over ζ. For example, for the subgroups of $\{1, 4, 13, 16\}$ we have corresponding sums: $\zeta^1 + \zeta^4 + \zeta^{13} + \zeta^{14}$, $\zeta^2 + \zeta^8 + \zeta^9 + \zeta^{15}, \cdots$.

§12 Fundamental Theorem of Algebra

The Fundamental Theorem of Algebra states that the complex numbers form an algebraically closed field. It was conjectured around the 17th century, although it was difficult to state at the time because the complex numbers had not yet been properly defined or understood. The first proof of this theorem is attributed to either Gauss or Argand, both around the 1800s. Interestingly, the proofs of the Fundamental Theorem of Algebra use very little, if any, algebra because the real and complex numbers are not algebraic objects. What we can do, however, is provide a proof that minimizes the amount of analysis required.

We will make the following assumptions in our proof:

(i) Any polynomial in $\mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$. This is obvious from the intermediate value theorem and the completeness of $\mathbb{R}$. if we were working over the rational numbers, this would not be true because $\mathbb{Q}$ is not complete.

(ii) $\mathbb{C}$ has no extensions of degree 2. This is equivalent to saying that the square root of any element in $\mathbb{C}$ is also in $\mathbb{C}$.

Proof. Consider $\mathbb{R} \subseteq \mathbb{C} \subseteq X$, where X is any finite normal extension of $\mathbb{R}$ containing $\mathbb{C}$. To show that $\mathbb{C}$ is algebraically closed, it is enough to show $X = \mathbb{C}$. This would show $\mathbb{C}$ has no nontrivial finite field extension.

The field extension $X/\mathbb{R}$ is a finite Galois extension because it is normal, and $\mathbb{R}$ has characteristic 0, so the extension is separable as well. Let G be the finite Galois group of $X/\mathbb{R}$. By the Galois correspondence, the subgroups of G correspond to extensions $\mathbb{R} \subseteq L \subseteq X$. Assumption (i) tells us that any nontrivial extension $\mathbb{R} \subseteq L$ must be of even degree because minimal polynomials are of even degree (since if the degree were odd, one of the roots would be in $\mathbb{R}$). Hence, if a subgroup of G has odd index, it must be the trivial subgroup G. Now, suppose H is the subgroup of G corresponding to $\mathbb{C}$, so $H = Gal(X/\mathbb{C})$. Then extensions of $\mathbb{C}$ correspond to subgroups of H. Assumption (ii) tells us H has no subgroups of index 2. In summary, we have

(i) G has no subgroups of odd index, and

(ii) $H \subseteq G$ has no subgroups of index 2.

We would like to show H is trivial.

Facts from Group Theory: Pick a Sylow 2-subgroup of G. This has odd index because Sylow 2 subgroups always have index. So by (1) it is G. So G has order 2^n for some n (property of Sylow groups. So H has order 2^m for some m, so it is nilpotent. so if H has order > 1 it has subgroup index 2. And H can have a subgroup of index 2 so $|H| = 1$.

■

§13 Primitive Elements

Definition 13.1 (Primitive Element)**.** If K and M are fields such that $M = K(\alpha)$ for some α, then α is called the primitive element.

Suppose $K \subseteq M$ is a finite extension of fields, so $M = K(\alpha_1, \cdots, \alpha_n)$ for some α_i. We would like to understand when is M generated by a primitive element. It turns out that if M/K is separable, then M is generated by a primitive element.

Lemma 13.2. *If M/K is separable and finite, then there are only a finite number of intermediate extensions $K \subseteq L \subseteq M$.*

Proof. Extend K to a larger normal and separable extensions of M:

$$K \subseteq M \subseteq N.$$

Then K/N is a Galois extension and $Gal(K/N)$ is finite. By the Galois correspondence theorem, subgroups of $Gal(K/N)$ correspond to intermediate fields between K and N. There are a finite number of subgroups, hence, there are a finite number of intermediate fields between K and M. ■

Proposition 13.3. *If M/K is a finite and separable extension then M is generated by a primitive element.*

Idea: Choose α not in any extensions L with $K \subseteq L \subseteq M$, $L \neq M$. To do so, we need to show M is not the union of all the intermediate extensions not equal to M.

Lemma 13.4. *Suppose K is an infinite field and M is a finite dimensional vector space. Then M is not the union of a finite number of proper subspaces of M.*

Proof. By induction on the number of subspaces.
Let $V_1, V_2, \cdots, V_{k-1}, V_k$ be proper subspaces of M. Pick an element x that is not in $V_1, V_2, \cdots, V_{k-1}$. Pick another element y not in V_k. Draw the line through these two points. This line is not contained in any V_i, so it has at most one point in common with any of the subspaces $V_1, \cdots, V_k$. The line has an infinite number of points because K is infinite, so it must have an infinite number of points not in any V_i. Thus, M cannot be a union of a finite number of subspaces. ■

Corollary 13.5. *By Lemma 13.2 and Lemma 13.3, if K is infinite and M/K is separable, then $M = K(\alpha)$ for some α.*

What if K is finite?

Proof. Look at M^*. This is a cyclic group so any generator of it generates the field M and is primitive. Why is M^* cyclic? Any finite subgroup of M^* for any field M is cyclic. The reason for this is if G is a finite subgroup of M^*, then G has at most n solutions to $g^n = 1$. And this condition implied G is cyclic (any finite abelian group is a product of cyclic groups). ■

there is no proof that works for both finite and infinte fields.

Examples:

- $K \subseteq MK[\sqrt{2}, \sqrt{3}]$. The subfields are $K, K[\sqrt{2}], K[\sqrt{3}], K[\sqrt{6}], M$. We would like to find an element that is not in the subfields $K, K[\sqrt{2}], K[\sqrt{3}], K[\sqrt{6}]$

  $$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

  In order for it to not be in any of these subfields we nee at least two of a, b, c, d to be nonzero. Then the element is primitive.

- *Inseparable Extensions*:
  Let k be a field of characteristic $p > 0$. Consider the field of rational functions in two variables $k(t, u)$. We have $k(T, U) \subseteq k(t, u)$ where $T = t^p$ and $U = u^p$. If $a \in k(t, u)$, then $a^p \in k(T, U)$. This is because the Frobenius mapping $\varphi(a) = a^p$ is a field homomorphism and it maps $k(T, U)$ into $k(t, u)$, because it maps a set of generators of $k(T, U)$ and since it is a homomorphism, it must map all of $k(t, u)$ into $k(T, U)$. If $a \in k(t, u)$, a is a root of $x^p - b = 0$ $b \in k(T, U)$. So it generates a field od degree p. The extension $k(T, U) \subseteq k(t, u)$ has degree p^2. So there are no primitive elements. Note the extension $k(T, U) \subseteq k(t, u)$ is finite but has an infinite number of subextensions.

§14 Abel-Ruffini Theorem

This is the very famous theorem stating that the general quintic cannot be solved by radicals. We will work over a field of characteristic 0, such as $\mathbb{Q}$. There are additional complications for fields of characteristic > 0.

Definition 14.1 (Solvable Group)**.** A group G is solvable if there is a chain of subgroups

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is a normal subgroup of G_{i+1} and G_{i+1}/G_i is abelian. In other words, G can be split up into abelian or cyclic subgroups.

Example. S_1, S_2, S_3, S_4 are solvable, but S_5 is not.

Definition 14.2 (Solvable Extension)**.** An extension is solvable if its Galois group is solvable.

We will show that if α can be expressed by radicals over a field K of characteristic 0, then α is contained in a finite solvable Galois extension of K. Then, in order to show that the 5th degree polynomial cannot be solved by radicals, our task is to find a polynomial of degree 5 whose Galois group is non-solvable. There is one easy way to do this: recall

$$\mathbb{Q}(x_1, \cdots, x_5)^{S_5} = \mathbb{Q}(e_1, \cdots, e_5),$$

where the e_is are the elementary symmetric functions ($e_1 = \sum_{i=1}^5 x_i$, $e_2 = \sum_{i,j} x_i x_j$, $\cdots$). Consider the polynomial

$$x^5 - e_1x^4 + e_2x^3 - e_3x^2 + e_4x - e_5.$$

This polynomial has roots $x_1, \cdots, x_5$. And since S_5 is not solvable, this means $x_1, \cdots, x_5$ cannot be expressed in radicals using $e_1, \cdots e_5$.

Thus, we cannot write down a formula to solve the general quintic. However, this does not mean that there are no quintic equations that can be solved by radicals. In fact, there are 5th-degree polynomials with integer coefficients whose roots can be expressed using radicals. For example, we know the roots of $x^5 - 2$ are $\{\sqrt[5]{2}\zeta^i \mid \zeta^5 = 1, i = 0, 1, \cdots, 4\}$. So, the next natural question to ask is: can we find a polynomial with integer coefficients whose Galois group is non-solvable? We consider different cases:

- *Suppose $f(x) \in \mathbb{Z}[x]$ is irreducible, degree 5, and has exactly 2 complex roots.* For example, the polynomial $x^5 - 4x + 2$ has this property, and we can verify it by drawing its graph. It is also irreducible by Eisenstein's criterion. Its Galois group is a subgroup of S_5, the set of permutations of the roots. Moreover, the order of the Galois group is divisible by 5 because the polynomial is irreducible, and adjoining a root creates a degree 5 extension. Thus, G contains a 5-cycle. Since there are exactly 2 non-real roots, G contains a transposition, which corresponds to complex conjugation.

Any subgroup of S_5 containing a transposition and a 5-cycle is equal to the whole of S_5. To see this suppose H is a subgroup containing the transposition (12). Then some power of the 5-cycle will map 1 to 2. Hence, we can relabel the other roots and assume H contains the 5-cycle (12345). The conjugates of (12) under the (12345) are $(12), (23), (34), (45)$ and (51). These generate the S_5. So the roots of this polynomial cannot be solved by radicals.

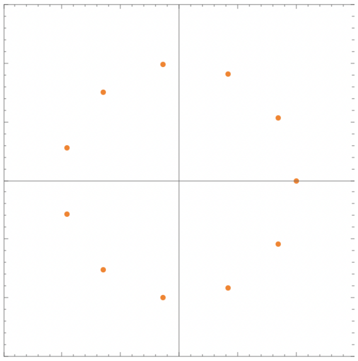
- *What if $f(x) \in \mathbb{Z}[x]$ is irreducible, of degree 5, and has exactly 4 complex roots?*
  In this case, we do know of an irreducible polynomial that can be solved by radicals: $x^5 - 2$. How do we find the splitting field of $x^2 - 2$?

  (i) Add in the 4 primitive 5th roots of 1. So $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ where $\zeta^5 = 1$. The Galois group of $\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ is $(\mathbb{Z}/5\mathbb{Z})^*$.

  (ii) Add in the 5th root of 2. So $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta, \sqrt[5]{2})$. The Galois group of $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta, \sqrt[5]{2})$ is $\mathbb{Z}/5\mathbb{Z}$ because we multiply the 5th root of 2 by any root of unity.

  The extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta, \sqrt[5]{2})$ is normal and of order 20. Moreover, $\mathbb{Z}/5\mathbb{Z}$ is a normal subgroup of G and $G/(\mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^*$. So we have a solvable extension, and thus we can solve it by radicals.

- *What about an example with 0 complex roots?*
  This does not have to be non-solvable either. We could take $2\cos 2\pi/11 = \zeta + \zeta^{-1}$ where ζ is a primitive 11th root of unity.



If we project down all the roots of unity onto the real line, we get the numbers $\cos 2\pi/11, \cos 4\pi/11, \cdots$. In total we get 5 elements. We can ask what is the Galois group of the field generated by these elements? The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $(\mathbb{Z}/11\mathbb{Z})^{]}*$ which is cylic of order 10. And the Galois group of $\cos 2\pi/11/\mathbb{Q}$ is isomorphic to a cyclic group of order 5. so we have an irreducible polynomial with 5 real roots $\cos 2\pi/11, \cos 4\pi/11, \cdots$. Its Galois group is cyclic of order 5 so solvable.

Theorem 14.3 (Abel's Theorem). *If an equation is solvable by radicals, then its Galois extension is solvable.*

Proof. Suppose $f(x)$ is a polynomial in $K[x]$. We are going to construct the Galois extension in several steps.

(i) Adjoin all the necessary roots of unity K: $K \subseteq K(\zeta)$, where the order of ζ is large enough so that every radical we are taking is a radical of order dividing n. Take this to be a splitting field of $x^n - 1$. we are in characteristic 0, so this is a separable polynomial. The elements of the Galois group take $\zeta \mapsto \zeta^i$ where $i \in (\mathbb{Z}/n\mathbb{Z})^*$. As usual, if we compose the automorphisms $\zeta \mapsto \zeta^i$ and $\zeta \mapsto Z^j$ we get the automorphism that maps $\zeta \mapsto \zeta^{ij}$. thus the Galois group is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, it is abelian, and therefore solvable.

(ii) $K_1 = K(\zeta)$. $K_2 = K_1(\sqrt[n]{\alpha_1})$ where $\alpha \in K_1$. and $K_3 = K_2(\sqrt[m]{\alpha_2})$. We build up a tower of fields. This is not quite right. The problem is K_n might not be normal. Recall the example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{\sqrt{2}})$. what we should really do is take the square root of the conjugates as well. so $\subseteq \mathbb{Q}(\sqrt{\sqrt{2}, \sqrt{\sqrt{-2}}})$. So $K_2 = K_1(\sqrt[n]{\alpha_1, \sqrt[n]{\text{all conjugates of } \alpha_1}}$, $K_3 = K_2(\sqrt[m]{\alpha_2, \sqrt[n]{\text{all conjugates of } \alpha_2}}$. Then each of these fields are going to be normal.

What does the Galois group of this look like? What is the Galois group of $L(\sqrt[n]{\alpha}/L$ where L contains the nth roots of 1. the galois group consists of elements $\sqrt[n]{\alpha} \mapsto \sqrt[n]{\alpha}\zeta^k$ for some $k \in \mathbb{Z}/n\mathbb{Z}$. We can see that composition of these elements correspond to addition in $\mathbb{Z}/n\mathbb{Z}$. So the Galois group of this is a subgroup of $\mathbb{Z}/n\mathbb{Z}$. It is a subgroup of a cyclic group, so it is abelian. So every time we add a nth root we get a normal extension with a cyclic Galois group. So we get a chain of fields

$$K_0 \subseteq * \subseteq * \subseteq \cdots \subseteq K$$

such that each of the extensions is a normal extension with Galois group abelian either contained in $(\mathbb{Z}/n\mathbb{Z})^*$ or $\mathbb{Z}/n\mathbb{Z}$. The whole extension is normal and Galois because we are in char 0. So we've got a chain of fields such that each field is an abelian extension of the one earlier. The corresponding Galois groups

$$G_m \supseteq G_{m+1} \supseteq \cdots \supseteq 1$$

Each of these groups is a normal subgroup of the earlier and the quotient is abelian. So the Galois group of the whole extension is solvable. This completes the sketch of Abel's theorem.

■

Converse Statement: If $K \subseteq M$ and the Galois group of K over M is solvable, can we represent elements of M using radicals?

The answer turns out to be no in general. We will discuss this problem when in characteristic p. But it is true in characteristic 0.

Problem: suppose $K \subseteq L$ is a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$ where p is prime. What can we say about the extension L/K? This will be the topic of the next lecture?

§15 Kummer Extensions

In the previous lecture, we saw that if we can solve a polynomial by radicals, this is closely related to the Galois group being solvable, at least in characteristic 0. We would like to determine if the converse statement is true: If the Galois group of a field extension is solvable, does this mean we can solve the corresponding polynomial by radicals?

If the Galois group is solvable then it can be split up into cyclic groups (of the form $\mathbb{Z}/n\mathbb{Z}$). This suggests the following problem: Given a Galois extension $K \subseteq M$ whose Galois group is $\mathbb{Z}/n\mathbb{Z}$, what can we say about M? In particular, is M of the form $K(\sqrt[n]{a})$?

In general, the answer is no. However, we will show that $M = K(\sqrt[n]{a})$ for some $a \in K$ when the following assumptions hold:

(i) K contains all the nth roots of unity.

(ii) The characteristic of K does not divide n.

(iii) n is prime (this assumption is not that important).

So how do we find such a?

Suppose the Galois group $\mathbb{Z}/n\mathbb{Z}$ is generated by some element σ, so $\sigma^n = 1$. If a exists, the roots of $x^n = a$ are $\{\sqrt[n]{a}\zeta^i \mid \zeta \text{ is a primitive } n\text{th root of } 1\ , \zeta^n = 1, i = 0, 1, \cdots, n-1\}$. Since we assume the characteristic does not divide n, so $1, \zeta, \ldots, \zeta^{n-1}$ are distinct. The element of the Galois group σ must map $\sqrt[n]{a}$ to some other nth root of a. Let's just say $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$.

Forget momentarily that M is a field and think of it instead as a vector space over K and think of σ as a linear transformation. This just means forget about the multiplicative structure on M and that σ preserves this multiplicative structure. Then $\sqrt[n]{a}$ is an eigenvector of σ with eigenvalue ζ.

So we look for eigenvectors of σ on M. We know $\sigma^n = 1$, so possible eigenvalues are $1, \zeta, \zeta^2, \ldots$.

Problem: Do enough eigenvectors exist? In other words, is σ diagonalizable? yes because we assume $\zeta \in K$ and the characteristic of K does not divide n.

Example. Suppose $n = 3$ and let $v \in M$. Then we can find the following eigenvectors and eigenvalues of σ: then we can find eigenvalues by taking $v + \sigma v + \sigma^2 v$. This is fixed by σ. summed over G. We can also take $v + \omega\sigma v + \omega^2\sigma^2 v$ where ω is ζ, $\omega^3 = 1$. This has eigenvalue ω^{-1} because we are summing over the group generated by $\omega\sigma$. We can also take $v + \omega^2\sigma v + \omega\sigma^2 v$ this has eigenvalue ω.

Eigenvectors	Eigenvalues
$v+\sigma v+\sigma^2 v$	1
$v+\omega\sigma v+\omega^2\sigma^2 v$	ω^{-1}
$v+\omega^2\sigma v+\omega\sigma^2 v$	ω

Eigenvectors	Eigenvalues
$\alpha_1+\alpha_2+\alpha_3=-1$	1
$\alpha_1+\omega\alpha_2+\omega^2\alpha_3$	ω^{-1}
$\alpha_1+\omega^2\alpha_2+\omega\alpha_3$	ω

Then

$$\begin{aligned}\text{Sum of the three eigenvectors} &= 3v+(1+\omega+\omega^2)\sigma v+(1+\omega^2+\omega)\sigma^2 v\\ &= 3v\end{aligned}$$

So

$$v=\frac{1}{3}(\text{sum of 3 eigenvectors}).$$

Note that the assumption that the characteristic of the field is not equal to 3 is important for this last statement. So any vector can be written as the sum of eigenvalues, so σ is diagonalizable.

Pick an eigenvector with eigenvalue not equal to 1. We can do this because if everything had eigenvalue 1, everything would be fixed by σ, and σ is nontrivial automorphism. Say $\sigma t=\zeta t$, then $\sigma(t^n)=t^n\in K$, t^n is fixed by the Galois group so $t^n\in K$. Thus, $M=K(\sqrt[n]{T})$ where $T=t^n$.

Example. $x^3+x^2-2x-1=0$. The roots are $\alpha_1=2\cos 2\pi/7, \alpha_2=2\cos 2\pi/7, \alpha_3=2\cos 6\pi/7$.

the Galois group is $\mathbb{Z}/3\mathbb{Z}$. $\alpha_1\mapsto\alpha_2\mapsto\alpha_3\mapsto\alpha_1$. We want to solve this cube roots. Find eigenvectors: Take an element and sum it over the Galois group: $\alpha_1+\sigma\alpha_1+\sigma^2\alpha_1=\alpha_1+\alpha_2+\alpha_3=-1$ where ω is the cube roots of unity. The cubes of these vectors are in the field $\mathbb{Q}(\omega)$ because they are fixed by σ. The cubes:

So $\alpha_1=\frac{1}{3}$

Vectors	Cubes
$\alpha_1+\alpha_2+\alpha_3$	-1
$\alpha_1+\omega\alpha_2+\omega^2\alpha_3$	$21\omega+14$
$\alpha_1+\omega^2\alpha_2+\omega\alpha_3$	$21\overline{\omega}+14$

§16 Cubics and Quartics

Quadratic. (Warm up)

$$ax^2 + bx + c = 0$$

The roots of this polynomial generates an extension of degree 2 whose Galois group is cyclic of order 2. Suppose the roots are α and β. If σ is the nonzero element of the Galois group, then $\sigma(\alpha) = \beta$ and $\sigma(\beta) = \alpha$. The key idea is to try to find an eigenvalue and eigenvector of certain elements of the Galois group. In this case, we find that -1 is an eigenvalue of σ with eigenvector $\alpha - \beta$. We know $(\alpha - \beta)^2 \in K$. Now $(\alpha - \beta)^2 = (b^2 - 4ac)/a^2$ and $\alpha + \beta = -b/a$. From these two equations we can solve for α and β and get the usual equation for the quadratic.

Cubic.

$$x^3 + bx + c = 0$$

If we are not working over a field of characteristic 3, we can get rid of the coefficient of x^2 by adding something to x.

It was solved by Ferro, and possibly, independently by Tortaglia. It's difficult to know exactly what happened, because both mathematicians kept their work secret. At the time in Italy, the way you got a mathematical job was by challenging a professor to a mathematical duel.

Take the roots to be α, β, γ. Take the Galois group to be S_3 (technically it is a subgroup of S_3). S_3 has a composition series: $1 \subseteq A_3 \subseteq S_3$. $1 \subseteq A_3$ is a $\mathbb{Z}/3\mathbb{Z}$ and $A_3 \subseteq S_3$ is $\mathbb{Z}/2\mathbb{Z}$. The fixed point fields we get from this give us a tower of fields:

$$K(\alpha, \beta, \gamma) \supseteq ? \supseteq K.$$

Assume K contains all the cube roots of unity. The missing field is generated by some element fixed by A_3 and it is an eigenvector of A_3 over S_3. S_3/A_3 to act on it as -1 (the nontrivial element to act on it as -1). The obvious thing to try is

$$\Delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$$

$$\Delta = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$$

It's a polynomial in the coefficients: you can work out

$$\Delta^2 = -4b^3 - 27c^2$$

The missing field is $K(\Delta)$, by taking square root of the expression.

We need to take a cub root to go from $K(\Delta)$ to $K(\alpha, \beta, \delta)$. We look at the sum of the roots: $\alpha + \beta + \gamma = 0$. Take

$$y = \alpha + \omega^2\beta + \omega\gamma$$

$$z = \alpha + \omega\beta + \omega^2\gamma$$

These are eigenvectors of σ, where $\sigma^3 = 1$, $\sigma : \alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$. We know from theory of Kummer extensions that $y^3, z^3 \in K(\Delta)$. Doing some algebra we get:

$$y^3 = -27/2c + 3\sqrt{3}i/2\Delta$$

$$z^3 = -27/2c - 3\sqrt{3}i/2\Delta$$

We can work out y and z by taking cube roots. We can find $\alpha = (y+z)/3$.

Example. $x^3 + x + 1 = 0$. We find that $-4b^3 - 27c^2 = -31$. $\Delta = \sqrt{-31}$. $y = \sqrt[3]{-27/2 - 3\sqrt{3}i\sqrt{-31}/2}$ and $z = \sqrt[3]{-27/2 + 3\sqrt{3}i\sqrt{-31}/2}$. We can solve for α.

Quartics. Solved by guy called Ferrari.

$$x^4 + ax^2 + bx + c = 0$$

S_4 contains the following chain of subgroups:

§17 Frobenius Endomorphism

Suppose R is a ring of characteristic p ($p = 0$) where p is a prime. If we define $\phi(a) := a^p$, then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$, thus ϕ is an endomorphism of the ring.

For finite fields F_{p^n}, ϕ is an automorphism and it generates the Galois group.

For general rings or fields, the Frobenius map need not be an automorphism. For instance, if we look at the field $k(x)$ where k is a field of characteristic p, then the image is contained in $k(x^p)$ which is definitely smaller than the field $k(x)$.

There is a way of getting a Frobenius automorphism in characteristic zero. And this gives one of the very few easy ways of constructing explicit elements of Galois groups. (The other easy way is to use complex conjugation)

Easy case: Suppose we have a Galois extension of $\mathbb{Q} \subseteq M$. Suppose $M = \frac{\mathbb{Q}[x]}{(f(x))}$, where $f(x) \in \mathbb{Z}[x]$ and has leading coefficient 1. $x^n + a_{n-1}x^{n-1} + \cdots + a_0$. We want to reduce M modulo p, but this makes no sense. Define $R = \mathbb{Z}[x]/f(x)$ which is a free $\mathbb{Z}-$ module of rank n.

§18 Discriminants

The discriminant of a finite field extension $K \subseteq M$.

Recall that if V is a finite dimension vector space over K. Suppose it has a symmetric bilinear form $(,)$. Then we can define the discriminant of this form as follows: Pick a basis $v_1, \cdots, v_n$ of V and look at the matrix

$\begin{pmatrix} (v_1, v_1) & (v_1, v_2) & \cdots \\ (v_2, v_1) & & \end{pmatrix}$ the determinant of this matrix is called the discriminant. Problem: It depends on the choice of basis. Suppose you choose a new basis $W = \{w_1, \cdots, w_n\}$. How does the discriminant change? $W = AV$ for some non-singular matrix A. So the discriminant with respect to W is $A^2 disc(V)$. So the discriminant is a well defined element of K up to multiplication by $(K^*)^2$ If the discriminant is $\neq 0$, then it is a well-defined element of $K^*/(K^*)^2$. If we have a field extension, then we have a bilinear form on M$(,)$ defined by $(a, b) = Tr(a, b)$. We now have the following problem: Calculate the discriminant of M. It can be 0: $k(t^p) \subset k(t)$. The trace for this is always 0, so $(,) = 0$ and the discriminant is 0.

We will prove it is always nonzero for separable extensions.

suppose M is separable and finite over K. So $M = K(\alpha)$ for some α.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots a_0 = 0$$

minimal polynomial

Recall a polynomial also has a discriminant given by $\prod_{i<j}(\alpha_i - \alpha_j)^2$ where the α_i are roots.

§19 Sylow Theorems

If we have a finite group G, any subgroup H has order dividing the order of G. We can ask the converse: suppose d is a number that divides $|G|$, does G have a subgroup of order d?

Example. $G =$ rotations of the tetrahedron. Then G has order 12, but G has no subgroup of order 6.

Theorem 19.1 (Sylow Theorem)**.** *Suppose p^n is the largest power of p dividing the order of a group G. Then*

(i) G has subgroups of order p^n – called Sylow p-subgroups.

(ii) The number of Sylow p-subgroups is 1 mod p and divides $|G|$.

(iii) All Sylow p-subgroups conjugate.

(iv) Any subgroup of order p is in a Sylow p-subgroups.

Proof. (i) *Existence:*
Induction on the order of G:
Suppose G has a proper subgroup H of index coprime to p. Then $p^n||H|$ and $|H| < |G|$. So H has a subgroup of order p^n, so $|G|$ does. Otherwise, assume all proper subgroups of G have index divisible by p. Then $|G| =$ center of G + $\sum_{\text{conj. classes of size ¿1}}$ size of the conjugacy class. The size of a conjugacy class of size > 1 is the index of a subgroup of $|G|$, so the sum is divisible by p. Hence, the center of G is divisible by p. So G has an element of order p in the center.

Look at $G/\langle g \rangle$ where $g^p = 1$, $g \neq 1$, and g is in the center. Pick the Sylow p-subgroup S of $G/\langle p \rangle$ $S = p^{n-1}$

Look at $G \to G/\langle p \rangle$ which maps $S \mapsto S'$. The inverse image S' of S has order p^n, so it is a Sylow p-subgroup of G. EHnce, every finite group has Sylow p-subgroups.

(ii) Suppose S and T are Sylow $p-$subgroups with $S \neq T$.

■