Class Notes

These are notes for Math 121: Galois Theory. These notes are taken from Sid's handwritten notes, which were taken during the Winter 2021 class taught by Professor June Huh. Also, some of the constructions in Lecture 26 are thanks to Adam Inamasu, and the proof of Gauss's Lemma in Lecture 8 is thanks to Victor Yin; they were both students in SUMaC 2022.

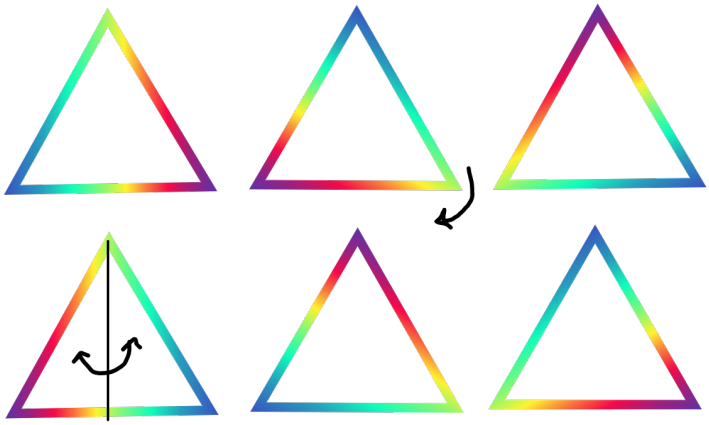
Table of Contents

Lecture 1: Introduction

This class is about *Galois theory*, which is the study of fields and their automorphism groups. We will focus on specific automorphism groups which are interesting to us, and which we will call *Galois groups*.

We can think of these automorphisms as the symmetries of a given set. We care about symmetries that are algebraic in nature. What are examples of such symmetries?

Example 1.1. An example common in algebra class is the **dihedral group**, or the symmetries of a given regular polygon. For example, D_3 is the set of symmetries of an equilateral triangle, which are all compositions of reflecting the triangle across an axis or rotating it:



But we could also have simpler examples of symmetries, such as:

Example 1.2. There are only two symmetries of a stick figure, so the symmetry group is just S_2:

The symmetries that are inherently familiar to us are derived from geometry, but as we built more abstract algebraic structures, we also found arithmetic and algebraic symmetries, developing homomorphisms, isomorphisms, and automorphisms.

We can think of the automorphisms as algebraic symmetries.

As Grothendieck came around, he linked algebra and geometry, using Galois theory to solve many classical problems such as: can we trisect an angle? can we solve a quintic?

Example 1.3. If we consider the set

$$\left\{x \in \mathbb{C} \;\middle|\; x^5 - 2x^4 + x^3 + x^2 - x + 1 = 0\right\},$$

we will find that it is a set of 5 elements whose symmetry group is D_5. Meanwhile, the symmetry group of

$$\left\{x \in \mathbb{C} \;\middle|\; x^4 + x + 1 = 0\right\}$$

is S_4.

It is sort of unclear what the symmetry group of the above sets means in this context, and that is something we will discuss more rigorously later. Right now the important question is: how does the first example relate to $\pentagon$ or the second example relate to rotations of $\square$?

Maybe we can tie the roots of these polynomials to vertices of these polygons somehow...

With that broad introduction, we will move on to some definitions.

We should already know the definition of a field, but as a reivew...

Definition 1.4. A field F is a commutative ring with identity, such that all nonzero elements have inverses. That is, it is a set with two operations, $\cdot$ and $+$, with the following properties:

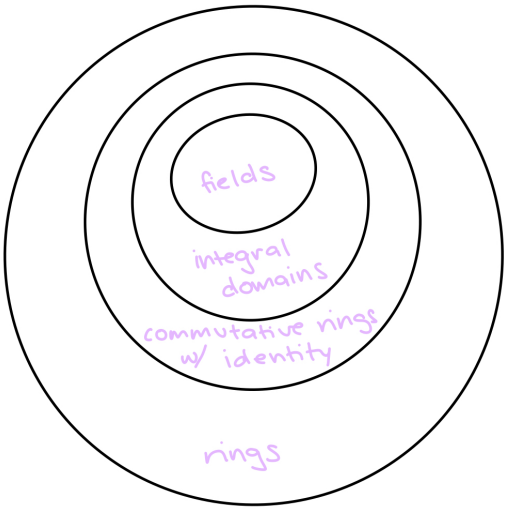
- $F, +$ is an abelian group; that is:
  - $\rightarrow$ $a + b = b + a$ for all $a, b \in F$
  - $\rightarrow$ $a + (b + c) = (a + b) + c$ for all $a, b, c \in F$
  - $\rightarrow$ there exists $0 \in F$ such that $a + 0 = a$ for all $a \in F$
  - $\rightarrow$ for all $a \in F$, there exists $(-a) \in F$ such that $a + (-a) = 0$
- $a \cdot b = b \cdot a$ for all $a, b \in F$
- there exists $1 \in F$ such that $1 \cdot a = a$ for all $a \in F$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in F$
- for all $a, b, c \in F$, $(a + b) \cdot c = a \cdot c + b \cdot c$.
- for all $a \neq 0 \in F$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$

There are many examples of fields that we commonly work with:

Example 1.5.

- $\mathbb{Q}$ and finite extensions
- $\mathbb{R}$ and $\mathbb{C}$ (which are much harder to study than the rationals)
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is prime
- $\mathbb{F}_q$, where q is a prime power
- $\mathbb{Q}_p$, or the p-adic rationals
- $\mathbb{Q}(x), \mathbb{R}(x)$ which are the fields of functions of $\mathbb{Q}[x]$ and $\mathbb{R}[x]$, respectively. these are known as function fields of algebraic varieties

Note that fields are a special category of integral domains, which are a special category of commutative rings with identity:



This means that the theory of rings is very relevant to the theory of fields.

Remark 1.6. The ideals of fields are either $\{0\}$ or the entire field F.

This means that the theory of ideals is trivial for fields. However, it is sometimes still useful to discuss ideals of fields. For example, since we know that the kernel of a field homomorphism is an ideal and cannot contain 1, all field homomorphisms are injective.

Definition 1.7. The **category** of fields is the set of all fields (the objects in the category), along with all homomorphisms between them (the morphisms).

Definition 1.8. A **ring homomorphism** is a map $\varphi : R_1 \to R_2$ such that

- $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R_1$
- $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R_1$
- $\varphi(1) = 1$ (this is not a requirement in D&F)

Definition 1.9. We say that $\mathbb{Z}$ is the **initial object** among rings, which means that for any ring R, there is a unique ring homomorphism $\varphi : \mathbb{Z} \to R$.

Specifically, this is the homomorphism defined by $\varphi(1) = 1$, since then for any $n \in \mathbb{Z}$, $\varphi(n)$ must be $\underbrace{1+1+\cdots+1}_{n \text{ times}}$ by definition of a homomorphism.

Definition 1.10. We say that the **characteristic** of a field F, denoted $\mathrm{ch}(F)$, is the smallest positive $n \in \mathbb{Z}$ such that $\varphi(n) = 0$ in the above map, or 0 if no such n exists.

Note that the characteristic is either 0 or a prime p, since the kernel of our map is an ideal of $\mathbb{Z}$, which means it is either $p\mathbb{Z}$ or 0.

Lecture 2: Examples of Fields

We actually already understand some concepts in Galois theory. For example, consider the complex numbers $\mathbb{C}$.

What are they?

One could say $\mathbb{C}$ is the smallest field extension of $\mathbb{R}$ containing i.

What is i?

It is a root of $x^2 + 1 = 0$. (We will learn that $\mathbb{C}$ is a *splitting field* of $x^2 + 1$ over $\mathbb{R}$.)

But if you accept that $x^2 + 1$ has 1 root, then we must be able to factor it as

$$x^2 + 1 = (x - \alpha_1)(x - \alpha_2).$$

Thus, if it has one root, it must actually have two roots, α_1 and α_2, such that

$$\begin{aligned} \alpha_1 + \alpha_2 &= 0 \\ \alpha_1\alpha_2 &= -1. \end{aligned}$$

Then, i can be α_1 or α_2, but which is it?

You might say it doesn't matter; we can all either of them i and the other one $-i$.

What do we mean when we say it doesn't matter?

Well, if we want $\mathbb{C}$ to be the smallest field containing $\mathbb{R}$ and i, it should consist of all elements of the form $a + bi$, with $a, b \in \mathbb{R}$.

But then,

$$\begin{aligned} (a + bi)(c + di) &= ac + bdi^2 + (bc + ad)i \\ &= ac - bd + (bc + ad)i \end{aligned}$$

since $i^2 + 1 = 0$. But if we have $j = -i$ then

$$\begin{aligned} (a + bj)(c + dj) &= (a - bi)(c - di) \\ &= (ac - bd) - (bc + ad)i \\ &= (ac - bd) + (bc + ad)j, \end{aligned}$$

so the structure of the field remains unchanged, and our choice of root doesn't matter.

In other words,

$$\begin{aligned} \varphi : \mathbb{C} &\to \mathbb{C} \\ a + bi &\mapsto a - bi \end{aligned}$$

is a field isomorphism, which we call *complex conjugation*.

Additionally, we can see that $\varphi^2 = \varphi \circ \varphi = \mathrm{id}$ and $\varphi \mid_{\mathbb{R}} = \mathrm{id} \mid_{\mathbb{R}}$. So we would say that the *Galois group* of $\{x^2 + 1 = 0\}$ is $S_2 = \mathbb{Z}/2\mathbb{Z}$. In this sense, the ambiguity of which choice of i is a feature, not a defect.

Note that in the example we discussed last lecture:

$$\left\{x^5 - 2x^4 + x^3 + x^2 - x + 1 = 0\right\},$$

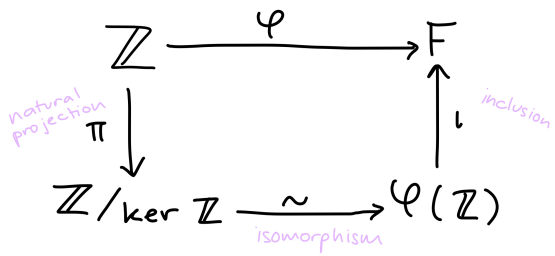
with D_5 symmetry $\pentagon$, there might be symmetry between each point, but not between pairs of points.

Remember again that for a field F, all ideals are either $\{0\}$ or F. This implies that if $\varphi : F \to R$ is a homomorphism from any field to any ring, then since $\ker(\varphi)$ is an ideal of F, it must be 0 or F. But the kernel cannot be F, since $\varphi(1) = 1$, so $\ker(\varphi) = 0$ and φ is injective.

Also, remember that the characteristic of F is the smallest positive integer n such that

$$\underbrace{1 + 1 + \ldots 1}_{n \text{ times}} = 0 \in F,$$

or 0 if no such positive integer exists. Also, remember that if $\mathrm{ch}(F) > 0$ it must be a prime p. The first isomorphism theorem gives us the following diagram:



where $\varphi(\mathbb{Z})$ is an integral domain because it is a subring of F.

Also, remember that if R is a ring, then $R^\times$ is the set of units of R, and it is a group under multiplication.

Let us look at some examples of finite fields.

We know that for any integer n, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. This implies that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n\mathbb{Z}$ is maximal. In $\mathbb{Z}$, the maximal ideals are $p\mathbb{Z}$ where p is prime.

Thus, for any prime p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field of prime order. Note that $\mathbb{F}_p^\times$ includes all nonzero elements of $\mathbb{F}_p$, so $\mathbb{F}_p^\times$ (where the group operation is multiplication) is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$ (where the group operation is addition). This implies that for any $a \in \mathbb{F}_p^\times$, $|a| \mid p - 1$, so

$$a^{p-1} \equiv 1 \pmod{p},$$

which is Euler's theorem.

Proposition 2.1. Let p be a prime. Then, if F is a field of order p, there is a unique isomorphism $\mathbb{F}_p \to F$.

Proof. We know from the definition of characteristic that there is a unique homomorphism $\varphi : \mathbb{Z} \to F$. Clearly, this cannot be injective, so there must be some prime q such that the kernel of φ is $q\mathbb{Z}$ and therefore the image of φ is isomorphic to $\mathbb{Z}/q\mathbb{Z}$. But the image of φ must be some additive subgroup of $(F, +)$ and the only such additive subgroup of a prime group is the group itself. Thus, $q = p$, and we have an isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to $\operatorname{im}\varphi = F$.

Thus, the field of prime order p is unique up to isomorphism. □

Ok, so we have (unique) fields of prime order. Can we construct a field with 4 elements?

We know that a field with 4 elements would need a $0, 1$ and two other elements. So let us say

$$\mathbb{F}_4 = \{0, 1, a, b\}.$$

Then, we need to define how these elements interact with our operators. Let us say we have the following tables:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Then, we can show that $\mathbb{F}_4$ is a field. We can see that $(\mathbb{F}_4, +) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and $(\mathbb{F}_4^\times, \cdot) \cong \mathbb{Z}/3\mathbb{Z}$. What is left is to show the distributive property, which we can check manually.

It also turns out that if F is a field of order 4, there is an isomorphism $\mathbb{F}_4 \to F$. But this isomorphism isn't necessarily unique, while in the prime case we knew our isomorphism was uniquely determined by $\varphi(1) = 1$.

Proof. Let us say that F is a field of order 4. Then, $\mathrm{ch}(F)$ must be a prime factor of 4, so $\mathrm{ch}(F) = 2$. Thus, in F, $1 + 1 = 0$, and for all $a \in F$, $a + a = a(1 + 1) = 0$.

We know that $(F, +)$ must be a group of order 4. There are only two groups of order 4, up to isomorphism, and since every element in F has order at most 2, we get that

$$(F, +) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Since F is a field, we know that $\left|F^\times\right| = 3$, and since there is only one group of order 3, we get that $(F^\times, \cdot) \cong \mathbb{Z}/3\mathbb{Z}$.

Thus, up to isomorphism, $\mathbb{F}_4$ is the unique field of order 4. □

Note that this isomorphism is not unique: $\varphi : \mathbb{F}_4 \to \mathbb{F}_4$ defined by $\varphi(1) = 1$ and $\varphi(a) = b$ is a valid non-identity isomorphism.

But this the only other choice of isomorphism, because we must have $\varphi(1) = 1$ and then the other elements are determined by our choice of $\varphi(a)$, which must be either a or b. Thus, we can say that $\mathbb{F}_4$ has S_2-symmetry.

Lecture 3: Categories

Remember that we constructed $\mathbb{C}$ using the polynomial

$$x^2 + 1 = (x - \alpha_1)(x - \alpha_2),$$

so that we knew $\alpha_1 + \alpha_2 = 0$ and $\alpha_1\alpha_2 = -1$.

We also saw that there is a nontrivial isomorphism $\varphi : \mathbb{C} \to \mathbb{C}$, which fixes $\mathbb{R}$ and has the property that $\varphi^2 = \text{id}$.

Moreover, any isomorphism $\psi : \mathbb{C} \to \mathbb{C}$ that fixes $\mathbb{R}$ is either id or φ. This is because, for any α such that $\alpha^2 + 1 = 0$, we can see that

$$\psi(\alpha)^2 + 1 = \psi(\alpha^2 + 1) = \psi(0) = 0,$$

so either

$$\psi(\alpha_1) = \alpha_2$$
$$\psi(\alpha_2) = \alpha_1$$

or

$$\psi(\alpha_1) = \alpha_1$$
$$\psi(\alpha_2) = \alpha_2,$$

using the fact that ψ is injective, so $\psi(\alpha_1) \neq \psi(\alpha_2)$.

Thus, the Galois group (of ambiguities) of $\mathbb{C}$ is $\mathbb{Z}/2\mathbb{Z}$.

Then, we can consider the field $\mathbb{F}_2 = \{0, 1\}$.
There are only four quadratic polynomials of this group:

$$x^2,\ x^2 + x,\ x^2 + 1,\ x^2 + x + 1.$$

The first one has roots $0, 0$, the second has roots $0, 1$, the third has roots $1, 1$ and the fourth has no roots.

But we can imagine that there are roots of $x^2 + x + 1$ somewhere out there. We can all these roots α_1 and α_2, so that

$$x^2 + x + 1 = (x - \alpha_1)(x - \alpha_2).$$

This means that $\alpha_1 + \alpha_2 = 1$ and $\alpha_1\alpha_2 = 1$. Moreover, we can see that since $\alpha_1^2 + \alpha_1 + 1 = 0$, $\alpha_1^2 = \alpha_1 + 1 = \alpha_2$, and similarly, $\alpha_2^2 = \alpha_1$.

Thus, we get the addition and multiplication tables

$+$	0	1	α_1	α_2
0	0	1	α_1	α_2
1	1	0	α_2	α_1
α_1	α_1	α_2	0	1
α_2	α_2	α_1	1	0

$\cdot$	0	1	α_1	α_2
0	0	0	0	0
1	0	1	α_1	α_2
α_1	0	α_1	α_2	1
α_2	0	α_2	1	α_1

So the smallest field consisting of $\mathbb{F}_2$ and the roots of $x^2 + x + 1$ is $\mathbb{F}_4$. We call this the *splitting field* of $x^2 + x + 1$ over $\mathbb{F}_2$, and similarly we call $\mathbb{C}$ the splitting field of $x^2 + 1$ over $\mathbb{R}$.

We previously described our Galois groups with reference to polynomials. From now on, we will create *field extensions*, as above, and define the Galois group with reference to that extension.

We denote a field extension as $\mathbb{C}/\mathbb{R}$ or $\mathbb{F}_4/\mathbb{F}_2$. Then, we can say that the Galois group of $\mathbb{C}/\mathbb{R}$ is S_2 (with the symmetry $i \leftrightarrow -i$) and the Galois group of $\mathbb{F}_4/\mathbb{F}_2$ is also S_2 (with the symmetry $\alpha_1 \leftrightarrow \alpha_2 = \alpha_1 + 1$).

In these symmetries, the field that we are given (or the field that we are using for the coefficients) must be fixed. We call this the *base field*.

What do we mean by "symmetry" of an object? It is best to describe this using categories.

Definition 3.1. A **category** $\mathcal{C}$ consists of

(1) a class of **objects** for the category, and

(2) for every pair of objects $A, B \in \mathcal{C}$, a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of **morphisms** in $\mathcal{C}$ (where morphisms are maps from A to B)

(3) for every object $A \in \mathcal{C}$, there exists a morphism $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$, which we call the **identity morphism**

(4) for every 3 objects $A, B, C \in \mathcal{C}$, a function

$$\circ : \mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$$

such that for all $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$,

$$f \circ 1_A = f \text{ and } 1_B \circ f = f.$$

Moreover, if we use the notation

$$A \xrightarrow{f} B$$

then for any

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

we have that $(h \circ g) \circ f = h \circ (g \circ f)$

We will mainly focus on the category of rings, where the objects are rings, and the morphisms are ring homomorphisms.

Definition 3.2. A function $A \xrightarrow{f} B$ is an **isomorphism** in $\mathcal{C}$ if there exists $A \xleftarrow[f]{} B$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

For some categories, the isomorphisms are bijective homomorphisms, but this is a more general definition.

Definition 3.3. An **automorphism** of $A \in \mathcal{C}$ is an isomorphism from A to A.

Remark 3.4. We denote the set of automorphisms of $A \in \mathcal{C}$ as $\mathrm{Aut}_{\mathcal{C}}(A)$. This is a subset of $\mathrm{Hom}_{\mathcal{C}}(A, A)$.

We can see that $\mathrm{Aut}_{\mathcal{C}}(A)$ is a group under composition, since we are given that composition is associative and the identity is 1_A, and by the definition of an isomorphism, any $f \in \mathrm{Aut}_{\mathcal{C}}(A)$ has an inverse.

It is also important to note that $\mathrm{Aut}_{\mathcal{C}}(A)$ is not necessarily the entire set $\mathrm{Hom}_{\mathcal{C}}(A, A)$.

Example 3.5. Let $\mathcal{C}$ be the category of sets, where morphisms are functions between sets. Then, we can have the set $S = \{1, 2\}$ and the function $f : \{1, 2\} \to \{1, 2\}$ defined by

$$f(1) = 1$$
$$f(2) = 1.$$

Then, we have that $f \in \mathrm{Hom}_{\mathcal{C}}(S, S)$ but $f \notin \mathrm{Aut}_{\mathcal{C}}(S)$.

Going back to the category of rings (which we denote Ring), we can consider the group $\mathrm{Aut}(\mathbb{C})$. This is an uncountable group, because for any $a \in \mathbb{C}$, $f(x) = x + a$ is a valid automorphism. But if we look at the subgroup of automorphisms of $\mathbb{C}$ which fix $\mathbb{R}$, we get S_2, so we have found some formal notion of the symmetries of $\mathbb{C}/\mathbb{R}$.

To generalize this concept, we can consider a category $\mathcal{C}$ and an object $A \in \mathcal{C}$.

Definition 3.6. We can define the **relative category** $\mathcal{C}_A$ of $\mathcal{C}$ over A.

Here, the objects of $\mathcal{C}_A$ are the morphisms $A \xrightarrow{f} B$ for any $B \in \mathcal{C}$. Then, the morphisms in $\mathcal{C}_A$ are maps from $A \xrightarrow{f_1} B_1$ to $A \xrightarrow{f_2} B_2$. We can see that if we visualize this in the commutative diagram:

$$\begin{array}{ccc} B_1 & \xrightarrow{g} & B_2 \\ & {\scriptstyle f_1}\nwarrow \quad \nearrow{\scriptstyle f_2} & \\ & A & \end{array}$$

that these are just the maps $g \in \mathrm{Hom}_{\mathcal{C}}(B_1, B_2)$ such that $f_2 = g \circ f_1$.

We will really only use this in the category of rings.

Definition 3.7. Let $\iota : K \to F$ be a field homomorphism. Since K is a field, we know that ι is an inclusion map.

Then, the **Galois group** of ι is a group of automorphisms in $\mathcal{C}_K$. This group is denoted $\mathrm{Aut}(F/K)$ or $\mathrm{Gal}(F/K)$.

Concretely, $\mathrm{Gal}(F/K)$ is the set of $g \in \mathrm{Hom}(F, F)$ such that the commutative diagram

$$\begin{array}{ccc} F & \xrightarrow{g} & F \\ & {\scriptstyle \iota}\nwarrow \quad \nearrow{\scriptstyle \iota} & \\ & K & \end{array}$$

holds.

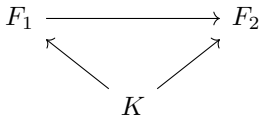
Example 3.8. Tying this back to the beginning of this lecture,

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \cong \mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2) \cong S_2.$$

Lecture 4: The Field of Fractions and the Universal Property

In this course, we mainly care about the category of fields, which we call Fields. In this category, the objects are fields and the morphisms are ring homomorphims.

We work similarly to last lecture. When we are interested in the roots of some polynomial $f(x) \in K[x]$, where K is a field, the relative category Fields_K has objects that are ring homomorphisms from K to any field F, and the morphisms are again commuative diagrams:

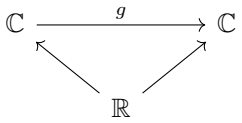


The most important examples are when $K \subseteq F$, because then F is a field extension of K. But since any field homomorphism is injective, we can factor $\iota : K \to F$ into

$$K \cong \iota(K) \subseteq F,$$

so that F is a field extension of the image of K under ι, which is just isomorphic to K.

Example 4.1. We return to our familiar examples, $\mathbb{R} \subseteq \mathbb{C}$ and $\mathbb{F}_2 \subseteq \mathbb{F}_4$. In the relative category $\mathsf{Fields}_{\mathbb{R}}$, the morphisms from $\mathbb{C}$ to $\mathbb{C}$ are the maps g that make the following commutative diagram hold:



But the only such maps are the identity and complex conjugation, as we showed before.

Similarly, we can see that there are only two morphisms from $\mathbb{F}_4$ to itself in the relative category $\mathsf{Fields}_{\mathbb{F}_2}$.

The most interesting field is $\mathbb{Q}$.

What is $\mathbb{Q}$?

It is the field of fractions of the most interesting ring $\mathbb{Z}$.

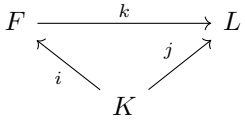
Recall if $R \subseteq F$ is a subring of a field then R must be an integral domain, since if R had zero divisors then so would F.

But if R is an integral domain, is R a subring of a field?

It turns out the answer is yes, and in a canonical way (there is a minimal such field that is unique up to isomorphism).

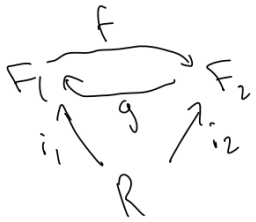
For any integral domain R, there is an injective homorphism $i : R \to F$, where F is a field, with the following universal property:

For any injective map $j : R \to L$, where L is a field, there is a unique $k : F \to L$ such that the diagram

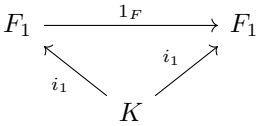


commutes.

From the universal property, we can see directly that F must be unique up to isomorphism. Say we have the injective homomorphisms $i_1 : R \to F_1$, $i_2 : R \to F_2$, both with the universal property. Then, the universal property tells us that there exists a unique f and g such that we get the following commutative diagram:



But we can see that this implies that $g \circ f \circ i_1 = i_1$, but the universal property applied to the following commutative diagram:



tells us that 1_F is the *unique* map with the property that $1_F \circ i_1 = i_1$, so $g \circ f = 1_F$. Similarly, $f \circ g = 1_G$, so f and g are isomorphisms.
Ok, so we have shown that if there is a field F that has this universal property, it is unique up to isomorphism. But how do we know that such a field exists?

We can show that for any integral domain R, the universal property holds for the field of fractions of R. That is, let

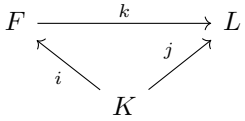
$$F = \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \neq 0 \right\} / \sim,$$

where we are modding out by the equivalence relation

$$\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \text{ when } a_1 b_2 = a_2 b_1.$$

Then, we will show that the universal property holds for $i : R \to F$, where $i(a) = \frac{a}{1}$ for all $a \in R$.

We want to show that for any injective homomorphism $j : R \to L$, where L is a field, there is a map $k : F \to L$ such that



commutes.

Let us think about how to construct this k. We know that $k \circ i(r) = j(r)$ for all $r \in R$, so for all $r \in R$,

$$k\left(\frac{r}{1}\right) = j(r).$$

But then since k is a field homomorphism, we can see that for any $\frac{a}{b} \in F$,

$$k\left(\frac{a}{b}\right) = k(a)k\left(\frac{1}{b}\right) = k(a)k(b)^{-1} = j(a)j(b)^{-1}.$$

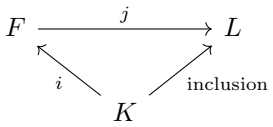
So it is clear that k is uniquely defined, and it is easy to show from this that k is a homomorphism. To see that it is well defined, note that if $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$ then

$$\frac{k\left(\frac{a_1}{b_1}\right)}{k\left(\frac{a_2}{b_2}\right)} = j(a_1)j(b_1)^{-1}j(a_2)^{-1}j(b_2) = j(a_1b_2)j(a_2b_1)^{-1} = 1$$

because $a_1b_2 = a_2b_1$.

Thus, for any integral domain R, the field of fractions of R is the field for which the universal property holds.

Remark 4.2. A common way of getting a ring homomorphism is by inclusion. If $R \subseteq L$ for some field L, then by the universal property, there exists a unique $j : F \to L$ such that the diagram



commutes. Thus, $j(F) \subseteq L$ is a subfield of L containing R and it is the smallest such object.

Corollary 4.3. Any field contains an isomorphic copy of $\mathbb{Q}$ or $\mathbb{F}_p$.

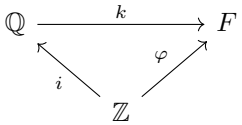
Proof. Remember that $\mathbb{Z}$ is the initial object of Ring, which means that for any field F, there exists a unique homomorphism $\varphi : \mathbb{Z} \to F$, defined by setting $\varphi(1) = 1$.

Then, if φ is not injective, then by the first isomorphism theorem for rings, we know that

$$\mathbb{Z}/\ker\varphi \cong \operatorname{im}\varphi \subseteq F.$$

But as we discussed before, if this map φ is not injective, then $\mathbb{Z}/\ker\varphi \cong \mathbb{F}_p$ for some prime p. Thus, F contains an isomorphic copy of some $\mathbb{F}_p$.

If φ is injective, then the universal property tells us that there exists a unique field homomorphism k such that



commutes. But since k is a field homomorphism, we know it is injective, and therefore $k(\mathbb{Q}) \subseteq F$ is an isomorphic copy of $\mathbb{Q}$. □

Example 4.4. Remember that for an integral domain R, the universal property holds for the field of fractions of R. So we have the following examples of integral domains and their corresponding fields for which the universal property holds:

- $\mathbb{Z} \to \mathbb{Q}$
- $K[X] \to K(x)$ (where $K(x)$ is the field of rational functions of x with coefficients in K)
- $K \to K$ when K is a field

One important question of this class is: can you solve a given polynomial $f(x) \in K[x]$?

In K, the answer is sometimes yes, and sometimes no.

But we know that if we have a field extension $F \supseteq K$, there are more roots of polynomials in $K[x]$.

Example 4.5. The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$, but it does have the root $\sqrt{2} \in \mathbb{R}$.

Is there always a field extension F/K such that we can find $\alpha \in F$ with $f(\alpha) = 0$?

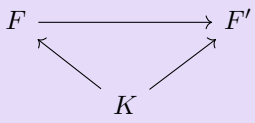
Yes, we will show this soon.

If $\alpha_1 \in F_1/K$ is a root of $f(x)$, and $\alpha_2 \in F_2/K$ is also a root of $f(x)$, is there a relation between the two?

Yep, there is a canonical relation when $f(x) \in K[x]$ is irreducible.

Theorem 4.6. Let $f(x) \in K[x]$ be any irreducible polynomial. Then, there is a field extension F/K and an element $\alpha \in F/K$ which is a root of f.

This extension has the following universal property: for any F'/K and any $\alpha' \in F'/K$ where $f(\alpha') = 0$, there is a unique commutative diagram



that maps α to α'.

Note that the latter part implies $(F/K, \alpha)$ is unique up to isomorphism, by applying the universal property.

We will see that this theorem holds when we take $F = K[x]/(f(x))$, and then α is the equivalence class of x in F.

Remark 4.7. If $f(x) \in \mathbb{Q}[x]$ is an irreducible of degree d, then it has d distinct roots in $\mathbb{C}$.

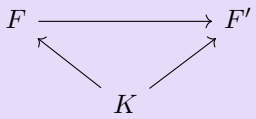
Our convention is that if α is the root of $f(x)$, then $K(\alpha)$ is the field generated by α over K, or the smallest field extension of K that contains α.

Lecture 5: Creating Field Extensions

We left off last lecture with the theorem:

Theorem 5.1. Let $f(x) \in K[x]$ be any irreducible polynomial. Then, there is a field extension F/K and an element $\alpha \in F/K$ which is a root of f.

This extension has the following universal property: for any F'/K and any $\alpha' \in F'/K$ where $f(\alpha') = 0$, there is a unique commutative diagram



that maps α to α'.

We will now prove this.

Proof. Take $F = K[x]/(f(x))$, and let α be the equivalence class of x in F.

We are given that $f(x)$ is irreducible. This means that $(f(x))$ is maximal, so $K[x]/(f(x))$ is a ring modulo a maximal ideal, which is a field.

Moreover, we can see that α is a root of f because

$$f([x]) = [f(x)] = 0$$

because $f(x) \equiv 0 \pmod{f(x)}$.

Then, we will show the universal property. We want a field homomorphism $\varphi : F \to F'$ that maps $\alpha \to \alpha'$. We will first consider the ring homomorphism $\sigma : K[x] \to F'$ defined by $\sigma(g(x)) = g(\alpha')$. Then, we can see that $\ker \sigma$ contains $f(x)$, since $f(\alpha') = 0$ by definition, but it is not the entire ring $K[x]$, since e.g. $\sigma(1) = 1$. So $\ker \sigma$ must be $(f(x))$ since $(f(x))$ is a maximal ideal.

But the first isomorphism theorem tells us that there is an induced isomorphism $K[x]/\ker \sigma \tilde{\to} \operatorname{im} \sigma \subseteq F'$, but this gives us our injective field homomorphism $\varphi : F \to F'$ (by applying the above isomorphism and then an inclusion map into F'). Moreover, we can see that $\varphi(\alpha) = \varphi(x) = \sigma(x) = \alpha'$, as we wanted.

Moreover, the uniqueness of this isomorphism follows from the fact that we can write any element of F as

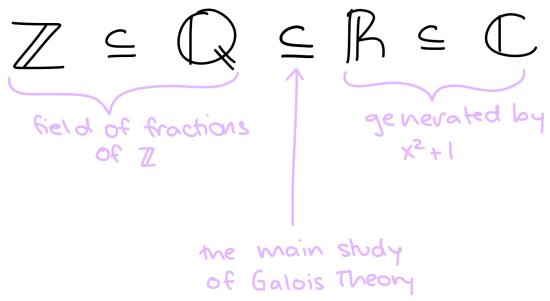
$$\sum_i c_i \alpha^i, \qquad c_i \in K.$$

Then, if we have any homomorphism $\varphi : F \to F'$ where $\varphi(\alpha) = \alpha'$ and $\varphi(c) = c$ for all $c \in K$, we can see that this uniquely determines the image of all our elements, as

$$\begin{aligned} \varphi\left(\sum_i c_i \alpha^i\right) &= \sum_i \varphi(c_i)\varphi(\alpha)^i \\ &= \sum_i c_i \alpha'^i. \end{aligned}$$

□

Example 5.2. We can now define $\mathbb{C}$ as the unique field generated by x^2+1 over $\mathbb{R}$. Much of mathematics is centered around



Example 5.3. We can also defined $\mathbb{F}_4$ as the field generated by a root of x^2+x+1 over $\mathbb{F}_2$.

Corollary 5.4. There is a field $\mathbb{F}_4$ with $|\mathbb{F}_4| = 4$.

Proof. Note that $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible. Then,

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$$

is a field. We can see that it has order 4, because any polynomial $f(x) \in \mathbb{F}_2[x]$ satisfies

$$f(x) = q(x)(x^2+x+1) + r(x),$$

where the degree of $r(x)$ is at most 1, by the division algorithm.

The only polynomials in $\mathbb{F}_2[x]$ of degree at most 1 are $0, 1, x, x+1$. These are all distinct mod x^2+x+1, because otherwise x^2+x+1 would divide a lower-degree nonzero polynomial.

Thus $|\mathbb{F}_4| = 4$. □

Definition 5.5. Let F/K be any field extension, and $S \subseteq F$ be an arbitrary subset. Then, $K(S) \subseteq F$ is the smallest subfield of F containing K and S and it is called the subfield of F **generated by** S **over** K.

We can think of this as the intersection of all subfields of F containing both K and S, since the interesection of subfields is a subfield.

With this definition of subfields generated by S, note that for the F defined in Theorem 5.1, we can write

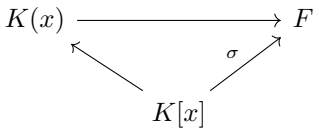
$$F = K(\alpha) = K(\{\alpha\}).$$

Moreover, for any F'/K and $\alpha' \in F'$ with $f(\alpha') = 0$, the subfield $K(\alpha') \subseteq F'$ is isomorphic to F.

Let F/K be any field extension. Let $\alpha \in F$ be any element and consider the map $\sigma : K[x] \to F$ defined by $\sigma(x) = \alpha$. Then, we have one of two cases:

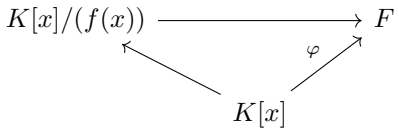
(1) $\ker \sigma = 0$ (σ is injective)
In this case, α is said to be **transcendental over** K because there is no polynomial $f(x) \in K[x]$ such

that $f(\alpha) = 0$. We get the commutative diagram



where $K(x)$ is the rational functions over K. Since $K(x)$ and $K(\alpha)$ both satisfy the universal property, we get that $K(x) \cong K(\alpha)$.

(2) $\ker \sigma \neq 0$
Since $K[x]$ is a PID, we get that $\ker \sigma = (f(x))$ for some unique irreducible monic polynomial $f(x)$, so we get the commutative diagram



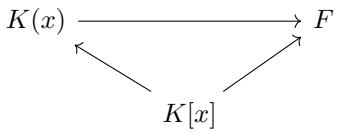
and $K(\alpha) \cong K[x]/(f(x))$. In this case, $f(x)$ is called the **minimal polynomial** of α over K, and α is **algebraic** over K.

Remember that everything is relative to the field we are working in:

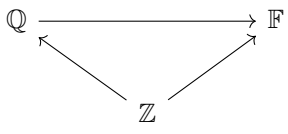
Example 5.6. The element $\pi i \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, but algebraic over $\mathbb{R}$ (since $x^2 + \pi^2$ is the minimal polynomial for πi over $\mathbb{R}$).

Lecture 6: Automorphisms of Field Extensions

Remember from last lecture, if F/K is a field extension and $\alpha \in F$, then either α is transcendental over K, and we have the commutative diagram

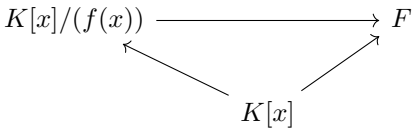


similar to

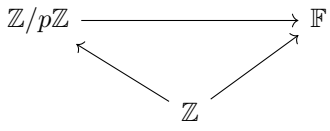


$x \mapsto \alpha$ $\qquad$ $1 \mapsto 1$

or α is algebraic over K and we have the commutative diagram



similar to



$x \mapsto \alpha$ $\qquad$ $1 \mapsto 1$

where $f(x)$ is the unique monic irreducible polynomial that makes the diagram hold, and is called the minimal polynomial of α over K.
So, either $K(\alpha) \cong K(x)$ or $K(\alpha) \cong K[x]/(f(x))$.

Definition 6.1. A field extension F/K is called **algebraic** if every $\alpha \in F$ is algebraic over K. Otherwise, F is **transcendental**.

Now we can try to say something about the symmetries of $K(\alpha)$ over K when α is algebraic.

Theorem 6.2. The number of automorphisms of $K(\alpha)$ that fix K, or $\left|\mathrm{Aut}(K(\alpha)/K)\right|$ equals the number of distinct roots of $f(x)$ in $K(\alpha)$.

Corollary 6.3. $\mathrm{Aut}(K(\alpha)/K)$ is a finite group.

We will look at a few examples of this before actually proving the theorem.

Example 6.4. Consider the polynomial

$$f(x) = x^3 - 2 \in \mathbb{Q}[x].$$

This is irreducible by Eisenstein's criterion.

Then, if α is a root of this polynomial, the only automorphism of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is the identity.

Why?

The roots of $f(x)$ in $\mathbb{C}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where $\omega = e^{2i\pi/3}$. We get the same field $\mathbb{Q}[x]/(x^3-2)$

no matter which root we choose as α, so

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{C}.$$

But clearly neither of the other roots are in this field, since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and cannot have imaginary numbers.

Example 6.5. Consider the polynomial

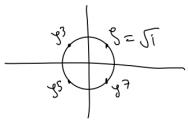
$$f(x) = x^4 + 1 \in \mathbb{Q}[x].$$

Then, we can see that this is irreducible because $f(x)$ is irreducible iff $f(x+1)$ is irreducible, and

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2,$$

which is irreducible by Eisenstein's criterion.

If α is a root of $f(x)$, then there are exactly 4 distinct automorphisms of $\mathbb{Q}(\alpha)/\mathbb{Q}$. This is because the four roots of $x^4 + 1$ are the following:



so if we take α to be any of these, we can express the other three roots as powers of α.

Given these examples, we turn to actually proving the theorem.

Proof of Theorem 6.2. We can write

$$f(x) = c_n x^n + \cdots + c_0,$$

where $c_0, \ldots, c_n \in K$. Moreover, let $\{\alpha_1, \ldots, \alpha_d\}$ be the set of roots of $f(x)$ in $K(\alpha)$.

Then, we can see that for any automorphism $\varphi : K(\alpha) \to K(\alpha)$,

$$\begin{aligned} f(\varphi(\alpha)) &= c_n(\varphi(\alpha))^n + \cdots + c_0 \\ &= \varphi(c_n)\varphi(\alpha^n) + \cdots + \varphi(c_0) \\ &= \varphi(c_n\alpha^n + \cdots + c_0) \\ &= \varphi(0) = 0. \end{aligned}$$

Thus, $\varphi(\alpha)$ must equal α_i for some $i \in 1, \ldots, d$.

Moreover, given any root α_i, there is a unique automorphism $\varphi : K(\alpha) \to K(\alpha)$ such that $\varphi(\alpha) = \alpha_i$, since by the universal property there must be a unique φ such that the following commutative diagram holds:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\varphi} & K(\alpha_1) \\ & \nwarrow \quad \nearrow & \\ & K & \end{array}$$

So there is a bijection of sets

$$\begin{aligned} \mathrm{Aut}(K(\alpha)/K) &\longrightarrow \{\alpha_1, \ldots, \alpha_d\} \\ \varphi &\longmapsto \varphi(\alpha) \end{aligned}$$

□

Example 6.6. Continuing off of Example 6.5, we can see that

$$\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\varphi_1, \varphi_3, \varphi_5, \varphi_7\},$$

where

$$\varphi_1(\alpha) = \alpha,\ \varphi_3(\alpha) = \alpha^3,\ \varphi_5(\alpha) = \alpha^5,\ \varphi_7(\alpha) = \alpha^7.$$

We can manually check that this implies $\varphi_3^2(\alpha) = \varphi_5^2(\alpha) = \varphi_7^2(\alpha) = \alpha$, so all of these automorphisms have order at most 2 and

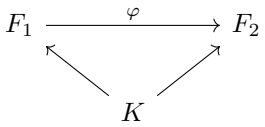
$$\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The most important trivial observation in Galois theory is:

Any morphism $i : K \to F$ makes F a vector space over K; we define scalar multiplication as

$$a \cdot b = i(a)b \qquad \text{for } a \in K, b \in F.$$

When viewing F in this way, we call it a **K-algebra**. If we have the following commutative diagram,



then $\varphi : F_1 \to F_2$ is a morphism of K-algebra.

Some nontrivial consequences are that there is no field $|F| = n$ when $n = 6, 10, 12, 14, \ldots$

Theorem 6.7. If F is a finite field then $|F| = p^n$, where p is prime and n is a positive integer.

Proof. Recall that all fields contain either an isomorphic copy of $\mathbb{F}_p$ where $p = \mathrm{ch}(F)$ or $\mathbb{Q}$ if $\mathrm{ch}(F) = 0$. Since F is finite, it must be the case that $\mathrm{ch}(F) > 0$, so F contains an isomorphic copy of $\mathbb{F}_p$.

Then, since F is finite it must be a finite-dimensional vector space over $\mathbb{F}_p$. Thus, $F \cong \mathbb{F}_p^n$, where $n = \dim_{\mathbb{F}_p} F$. (Here, $\cong$ means a vector space isomorphism, but it doesn't really matter, as long as we have a bijection.) □

Definition 6.8. If F is a finite-dimensional vector space over K, F/K is called a **finite extension**.

In this case, the dimension of F over K is called the **degree** of F/K and is denoted $[F : K]$.

The most important example of a finite extension is $F = K(\alpha)$ where α is algebraic and $f(x)$ is the corresponding minimal polynomial. Then, F is a finite extension of K.

Proposition 6.9. In this case, $[F : K] = \deg(f(x))$.

Proof. Remember that $F = K(\alpha) \cong K[x]/(f(x))$. Then, $K[x]/(f(x))$ is a vector space over K with basis $\{1, x, x^2, \ldots, x^{d-1}\}$ where $d = \deg(f(x))$. This set spans $K[x]/(f(x))$ because by the division algorithm, any polynomial in $K[x]$ is equivalent, mod $f(x)$, to a polynomial of degree at most d. It is linearly independent because if it wasn't then we've found a smaller polynomial with α as a root, contradicting the fact that $f(x)$ was the minimal polynomial. □

Lecture 7: Algebraic Extensions

Let $K \to F$ be a homomorphism between fields. Remember from last lecture that this gives F the structure of a vector space over K.

Example 7.1. Let us say $K = F = \mathbb{Q}(t)$, which is the field of fractions of $\mathbb{Q}[t]$.

(1) If we have the homomorphism $\iota_1 : \mathbb{Q}(t) \to \mathbb{Q}(t)$ defined by $\iota_1(t) = t$, then this homomorphism makes F a 1-dimensional vector space over K.

(2) If we have the homomorphism $\iota_2 : \mathbb{Q}(t) \to \mathbb{Q}(t)$ defined by $\iota_2(t) = t^2$, then this homomorphism makes F a 2-dimensional vector space over K.

$$\begin{array}{ccc} \iota_2(K) = \mathbb{Q}(t^2) & \xrightarrow{\text{inclusion}} & F = \mathbb{Q}(t) \\ & \nwarrow \quad \nearrow_{\iota_2} & \\ & K = \mathbb{Q}(t) & \end{array}$$

In other words, $[\mathbb{Q}(t) : \mathbb{Q}(t^2)] = 2$, and t is algebraic over $\mathbb{Q}(t^2)$ with minimal polynomial $x^2 - t^2 \in \mathbb{Q}(t^2)[x]$.

The most important special case is when $F = K(\alpha)$, and α is algebraic over K with minimal polynomial $f(x)$. We showed last lecture that in this case, F is d-dimensional over K, where $d = \deg(f(x))$.

Example 7.2. We return to our familiar examples.

We know that $\mathbb{C} = \mathbb{R}(i)$, with minimal polynomial $x^2 + 1 = 0$.

This means $\mathbb{C}$ is a vector space over $\mathbb{R}$ with basis $\{1, i\}$, so if we express elements of $\mathbb{C}$ as vectors with respect to this basis, we can express the multiplication map $\times i : \mathbb{C} \to \mathbb{C}$ as

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

since it maps 1 to i and i to -1.

Similarly, $\mathbb{F}_4 = \mathbb{F}_2(i)$, with minimal polynomial $x^2 + x + 1 = 0$. Expressing $\mathbb{F}_4$ as a vector space over $\mathbb{F}_2$, we can see that the multiplication map $\mathbb{F}_4 \xrightarrow{\times i} \mathbb{F}_4$ is

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

since it maps $1 \mapsto i$ and $i \mapsto i + 1$.

Definition 7.3. We say that F/K is **algebraic** if every $\alpha \in F$ is algebraic over K.

Definition 7.4. We say that F/K is **finite** if the vector space F over K is finite-dimensional.

The degree $[F : K]$ of F/K is the dimension of the vector space F over K.

Definition 7.5. We say that F/K is **finitely generated** if $F = K(S)$ for some finite subset $S \subseteq F$.

If $F = K(\alpha)$, where α is algebraic over K, it is clear that F/K is finite and finitely generated. Is it necessarily algebraic?

Example 7.6. We can define the subset $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ as

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

Then, $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ (we will prove this soon).

Then, by definition $\overline{\mathbb{Q}}/\mathbb{Q}$ is algebraic. However, we claim that $\overline{\mathbb{Q}}/\mathbb{Q}$ is not finite.

For any integer $d > 0$, there is an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree d. (e.g. take $f(x) = x^d - 2$).

But then if $\alpha \in \mathbb{C}$ is any root of $f(x)$, we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ and $\mathbb{Q}(\alpha) \subseteq \overline{\mathbb{Q}}$. Since this is true for any degree d, $[\overline{\mathbb{Q}} : \mathbb{Q}]$ cannot be finite.

Even if $\overline{\mathbb{Q}}/\mathbb{Q}$ is not finite, is it finitely generated?

Example 7.7. We know that $\mathbb{Q}(t)/\mathbb{Q}$ is finitely generated because it is generated by t. But it is not finite, because $\mathbb{Q}[t] \subseteq \mathbb{Q}(t)$ and $\{1, t, t^2, \ldots\} \in \mathbb{Q}[t]$ are linearly independent, so $\mathbb{Q}[t]$ is infinite dimensional, and $\mathbb{Q}(t)$ must be as well.

$\mathbb{Q}(t)/\mathbb{Q}$ is not algebraic since it is not finite.

Proposition 7.8. Let F/K be a field extension and $\alpha \in F$ be an arbitrary element. Then, α is algebraic over K if and only if $K(\alpha)/K$ is finite.

Proof. For one direction, we know that if α is algebraic over K, then it has minimal polynomial $f(x) \in K[x]$, and we already showed that this implies $[K(\alpha) : K] = \deg f(x)$, which is finite.

For the other direction, assume that $K(\alpha)/K$ is finite and has dimension d. Then, we know that $\{1, \alpha, \ldots, \alpha^d\}$ cannot be a linearly independent set, so there must exist some $c_0, \ldots, c_d \in K$ such that

$$c_0 + c_1\alpha + \cdots + c_d\alpha^d = 0,$$

and this gives us a polynomial in $K[x]$ which has α as a root. □

Corollary 7.9. If F/K is finite, it must be algebraic.

Proof. We know that for any $\alpha \in F$, $K(\alpha) \subseteq F$, so $K(\alpha)/K$ is finite. From the above proposition, this implies α is algebraic.

Thus, every $\alpha \in F$ is algebraic, so F is algebraic. □

Say we have the field extensions $K \subseteq E \subseteq F$. This gives us the three vector spaces F/K, F/E, and E/K.

If F/K is finite then F/E is finite and E/K is finite. The latter is because E/K is a subspace of F/K, the former is because $K \subseteq E$ so if a set S spans F/K it must also span F/E.

Does the converse also hold?

Theorem 7.10. The dimension $[F : K] = [F : E][E : K]$.

Proof. The dimension of a vector space is the cardinality of its basis. So we can take an arbitrary basis $\{\alpha_i\}_{i\in I}$ of E/K and $\{\beta_j\}_{j\in J}$ of F/E. Then, we claim that $\{\alpha_i\beta_j\}_{i\in I, j\in J}$ is a basis if F/K.

For any $\eta \in F$, we can express $\eta = \sum_j e_j\beta_j$ with all $e_j \in E$, since $\{\beta_j\}$ is a basis for F/E. Then, since $\{\alpha_i\}$ is a basis for E/K, we can express each e_j as $e_j = \sum_i c_{ij}\alpha_i$, where every $c_{ij} \in K$. Combining this, we get

$$\eta = \sum_{i,j} c_{ij}\alpha_i\beta_j,$$

and therefore $\{\alpha_i\beta_j\}$ spans F/K.

To show that $\{\alpha_i\beta_j\}$ is a linearly independent set, say we have some $c_{ij} \in K$ such that

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0.$$

But we can express this as

$$\sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j = 0,$$

and since $\{\beta_j\}$ are linearly independent over E, we know that each $\sum_i c_{ij}\alpha_i$ must equal 0. But since $\{\alpha_i\}$ are linearly independent over K, we get that each $c_{ij} = 0$, so $\{\alpha_i\beta_j\}$ is a linearly independent set over K.

Thus, $\{\alpha_i\beta_j\}_{i\in I, j\in J}$ is a basis of F and $[F : K] = [F : E][E : K]$. □

Corollary 7.11. F/K is finite if and only if F/K is finitely generated by algebraic elements over K.

So knowing that a field extension is finite is equivalent to knowing that it is finitely generated and algebraic!

Proof. We know that if F/K is finite, then by the corollary to Proposition 7.8, it is algebraic. Moreover, if it is finite then we can find a finite basis, and the basis must generate all of F/K, so it is finitely generated.

For the other direction, we know that if F/K is finitely generated by algebraic elements, then we can express F as

$$[K(\alpha_1, \ldots, \alpha_n),$$

where each α_i is algebraic over K. Then, for each $1 \leq \ell \leq n$, we can define

$$F_\ell = K(\alpha_1, \ldots, \alpha_\ell),$$

and we can see that $F_{\ell+1} = F_\ell(\alpha_{\ell+1})$ for all ℓ. This gives us the chain of field extensions:

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F,$$

where each extension in the chain is finite, because the dimension of $F_{\ell+1}/F_\ell$ is just the degree of the minimal polynomial of $\alpha_{\ell+1}$ over F_ℓ. So by Theorem 7.10, we get that

$$[F : K] = \prod_{\ell=0}^{n-1} [F_{\ell+1} : F_\ell],$$

and since $[F_{\ell+1} : F_\ell] \leq [K(\alpha_{\ell+1}) : K]$ for all ℓ, we get that

$$[F : K] \leq \prod_{\ell=1}^{n} [K(\alpha_\ell) : K],$$

which is finite. □

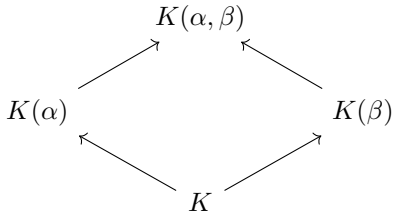
Returning to Example 7.7, we see that $\overline{\mathbb{Q}}/\mathbb{Q}$ is algebraic and *not* finite, so it cannot be finitely generated.

Corollary 7.12. If $\alpha, \beta \in F$ are algebraic over K, then $\alpha + \beta$, $\alpha\beta$, and α^{-1} are also algebraic.

Proof. We know that $K(\alpha)$ and $K(\beta)$ are both finite extensions of K, so $K(\alpha, \beta)$ must also be a finite extension of K. But $\alpha + \beta$, $\alpha\beta$, and α^{-1} are all elements of $K(\alpha, \beta)$, so they must be algebraic over K. □

Thus, we can see that $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ is a subfield.

Let us say that α has minimal polynomial of degree d_1 and β has minimal polynomial of degree d_2 over K. We know that $K(\alpha, \beta)/K$ has dimension at most $d_1 d_2$. Moreover, by the following diagram,

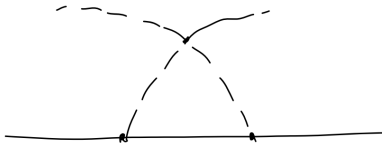


we can see that $[K(\alpha, \beta) : K]$ must be a multiple of both d_1 and d_2.

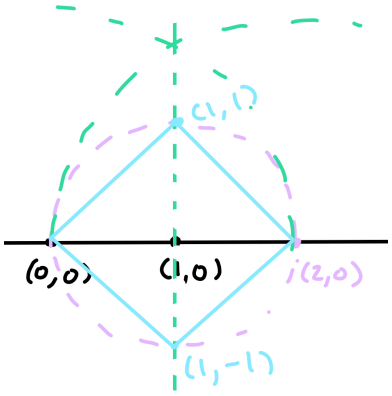
Lecture 8: Straightedge and Compass Constructions I

Given two points on a plane (say $(0,0)$ and $(1,0)$ in $\mathbb{R}^2$) and a straightedge and compass, let's try to do some constructions.

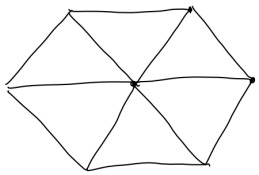
To make a perfect triangle, we already have two points, and we can find the third point by finding an intersection of the circle centered at $(0,0)$ and containing $(1,0)$ and the circle centered at $(1,0)$ and containing $(0,0)$:



Note that this is a 3-gon, and $3 = 2^{2^0} + 1$.
Then, to make a perfect square, we can find $(2,0)$ by drawing the circle centered at $(1,0)$ and passing through $(0,0)$ (in purple). Then, we know that the other two points of this square are at the intersection of the circle and the vertical line passing through $(1,0)$ which we can draw by finding the intersection of the circle centered at $(0,0)$ and passing through $(2,0)$ and the circle centered at $(2,0)$ and passing through $(0,0)$ (in green).



This is a 4-gon, and $4 = 2^2$.
It is also possible (but very difficult) to construct a pentagon in this way. A hexagon is also constructible, just by making 6 triangles.



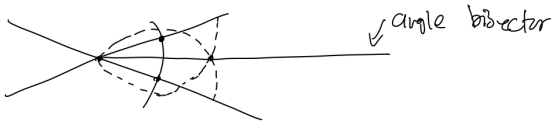
Note that $5 = 2^{2^1} + 1$ and $6 = 2\left(2^{2^0} + 1\right)$.
Can we make a 7-gon?

It turns out we cannot construct a 7-gon in this way, or an 11-gon, or a 13-gon. We *can* construct a 17-gon, and Gauss was able to create a construction, but we cannot construct a 19-gon or a 23-gon.

It is posisble to construct a 257-gon or a 65537-gon. But no other examples of constructible p-gons, for prime p, are known.

Is there a pattern here? It turns out that for a regular p-gon to be constructable, p must be a *Fermat prime*, of the form $2^{2^n}+1$. We will prove this later in the course.

Let's bisect an angle.



This allows us to go from an n-gon to a $2n$-gon.

What about trisecting an angle?

For any finite subset $E \subseteq \mathbb{R}^2$ define $\mathcal{C}(E)$ to be the set of circles in $\mathbb{R}^2$ with center $p \in E$ and radius $|p-q|$ for some $q \in E$, and define $\mathcal{L}(E)$ to be the set of lines in $\mathbb{R}^2$ joining distinct points $p, q \in E$.

Definition 8.1. A point $p \in \mathbb{R}^2$ is **constructible** if there is a sequence

$$p_0 = (0,0), p_1 = (1,0), p_2, \ldots, p_n = p$$

with the following property:
Let $E_i = \{p_0, \ldots, p_i\}$ for every $i \leq n$. Then, for each i, the point p_i is either

(1) the intersection of two lines in $\mathcal{L}(E_{i-1})$

(2) an intersection of a line in $\mathcal{L}(E_{i-1})$ and a circle in $\mathcal{C}(E_{i-1})$

(3) an intersection of distinct circles in $\mathcal{C}(E_{i-1})$

Definition 8.2. A real number α is constructible if $(\alpha, 0)$ is constructible.

Theorem 8.3. If α is constructible then it should be algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ for some r.

Proof. Set $p = (\alpha, 0)$. By definition, there is a sequence

$$p_0, \ldots, p_n = p$$

with the above properties. Say that for each i, $p_i = (\alpha_i, \beta_i)$.

Let $F_0 = \mathbb{Q}$, $F_{i+1} = F_i(\alpha_{i+1}, \beta_{i+1}) \subseteq \mathbb{R}$ for $i \geq 0$. We claim that $[F_{i+1} : F_i]$ is either 1 or 2; that is, if $F_{i+1} \supsetneq F_i$, then it is just a quadratic extension.

To prove this, we will consider the point $p_{i+1} = (\alpha_{i+1}, \beta_{i+1})$ and the set E_i of points added before this. We know that it is either (1) the intersection of two lines in $\mathcal{L}(E_i)$, (2) an intersection of a line in $\mathcal{L}(E_i)$ and a circle in $\mathcal{C}(E_i)$, or (3) an intersection of distinct circles in $\mathcal{C}(E_i)$.

Remember that the equation for a line between two points (a, b) and (a', b') is

$$(x - a)(b' - b) = (y - b)(a' - a).$$

Thus, for all lines in $\mathcal{L}(E_i)$, the equation for the line is of the form

$$\lambda x + \mu y = \nu, \quad \lambda, \mu, \nu \in F_i.$$

Moreover, the equation for a circle centered at (a, b) and with radius $r = \sqrt{(a - a')^2 + (b - b')^2}$ is

$$(x - a)^2 + (y - b)^2 = r^2,$$

so for all lines in $\mathcal{C}(E_i)$, the equation for the line is of the form

$$x^2 + y^2 + fx + gy + h = 0, \quad f, g, h \in F_i.$$

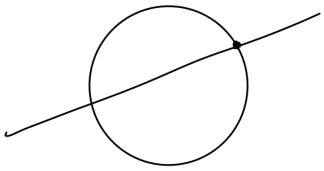
Now, we can go through our three cases for point p_{i+1}.

(1) If p_{i+1} is the intersection of two lines, then we know that $(\alpha_{i+1}, \beta_{i+1})$ is the solution to the linear equations

$$\begin{cases} \lambda_1 x + \mu_1 y &= \nu_1 \\ \lambda_2 x + \mu_2 y &= \nu_2. \end{cases}$$

But this means that we can express α_{i+1} and β_{i+1} as a linear combination of elements in F_i, which means α_{i+1} and β_{i+1} are already in F_i, and $[F_{i+1} : F_i] = 1$.

(2) If p_{i+1} is the intersection of a line and a circle

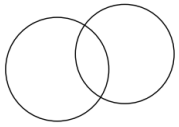


then we know that $(\alpha_{i+1}, \beta_{i+1})$ is the solution to the equations

$$\begin{cases} x^2 + y^2 + fx + gy + h &= 0 \\ \lambda x + \mu y &= \nu. \end{cases}$$

By substituting an expression for x in terms of y (or y in terms of x) into the first equation, we get a quadratic whose coefficients are in F_i and whose solution is either α_{i+1} or β_{i+1}. And once we have gotten one of the two, we have a linear equation to get the other, so $[F_{i+1} : F_i] \leq 2$ (it could be 1 in the case where our quadratic equation already has roots in F_i).

(3) If p_{i+1} is the intersection of two circles



then $(\alpha_{i+1}, \beta_{i+1})$ is the solution to the equations

$$\begin{cases} x^2 + y^2 + f_1 x + g_1 y + h_1 &= 0 \\ x^2 + y^2 + f_2 x + g_2 y + h_2 &= 0. \end{cases}$$

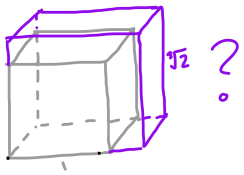
But by subtracting the second equation from the first, we can see that this is equivalent to the system of equations

$$\begin{cases} x^2 + y^2 + f_1 x + g_1 y + h_1 & = 0 \\ (f_1 - f_2)x + (g_1 - g_2)y & = (h_2 - h_1), \end{cases}$$

and this reduces to the second case, so $[F_{i+1} : F_i] \leq 2$.

Since at each step, $[F_{i+1} : F_i] = 1$ or 2, and $[F_{i+1} : \mathbb{Q}] = [F_i : \mathbb{Q}][F_{i+1} : F_i]$, we can see by induction that $[F_i : \mathbb{Q}]$ is a power of 2 for all i, and specifically that $[F_n : \mathbb{Q}]$ is a power of 2. Then, since $\alpha \in F_n$, we can see that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must be a factor of $[F_n : \mathbb{Q}]$ and therefore must also be a power of 2. □

Example 8.4. We know that $x^3 - 2$ is irreducible over $\mathbb{Q}$, by Eisenstein's criterion. So $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2, so $\sqrt[3]{2}$ cannot be constructed.
One standard problem is: given a cube, can we construct a cube with twice the volume?

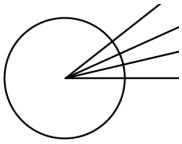


This tells us the answer is no, because we cannot construct an edge with side length $\sqrt[3]{2}$.

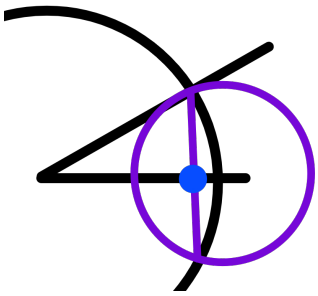
Using this, we can return to our question of trisecting an angle.

Corollary 8.5. The angle $\frac{\pi}{3}$ cannot be trisected.

Proof. Assume we can trisect $\pi/3$. So we can construct the following diagram:



Zooming in on the smallest angle, which has degree $\pi/9$, we can see that we can construct $\left(\cos\left(\frac{\pi}{9}\right), 0\right)$ as the blue point in:



By Theorem 8.3 we can see that this implies $\alpha = \cos \pi/9$ is algebraic, and if the minimal polynomial for α over $\mathbb{Q}$ has degree d, d must be a power of 2.

But the cosine sum formula tells us us that

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$$

for any angle θ. Plugging in $\theta = \pi/9$, we get that

$$\frac{1}{2} = 4\alpha^3 - 3\alpha.$$

But this means that α is a root of the polynomial

$$8x^3 - 6x - 1,$$

or that 2α is a root of

$$f(x) = x^3 - 3x - 1.$$

But $f(x)$ is irreducible in $\mathbb{Q}$; we can see this by the rational root theorem or by seeing that it has no integer roots and applying Gauss's Lemma.

So $[\mathbb{Q}(2\alpha) : \mathbb{Q}] = 3$, and since $\mathbb{Q}(2\alpha) = \mathbb{Q}(\alpha)$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. But 3 is not a power of 2, and we have reached a contradiction. Thus, we cannot trisect $\pi/3$. □

An aside on Gauss's Lemma:

Lemma 8.6 (Gauss's Lemma)**.** Let R be a UFD and F its field of fractions. Then, $f \in R[x]$ is irreducible if and only if it is irreducible in $F[x]$.

(The following proof is thanks to Victor Yin.)

Proof. First, if f is reducible in $R[x]$ then it is clearly reducible in $F[x]$, so one direction is clear.

For the other direction, suppose f is reducible in $F[x]$, so $f = gh$ where g and h have positive degree.

Let $c_1 \in R$ be the lcm of the denominators of the coefficients of $g(x)$, and let $c_2 \in R$ be the lcm of the denominators of the coefficients of $h(x)$. Then, if we define $g' = c_1 g$ and $h' = c_2 h$, we get that

$$c_1 c_2 f(x) = g'(x)h'(x),$$

where both $g'(x)$ and $h'(x)$ are elements of $R[x]$.

Note that we can assume without loss of generality that the gcd of the coefficients of $g'(x)$ is 1, since if not we can divide $g'(x)$ by this gcd and multiply $h'(x)$ by the gcd to get a product of the same form where the gcd of the coefficients of $g'(x)$ is actually 1.

Then, note that since R is a UFD, $c_1 c_2$ has a unique prime factorization. Take any prime p that is a factor of $c_1 c_2$. Since p is a factor of $g'(x)h'(x)$ it must be a factor of one of the two, and since $g'(x)$ has no constant factors, we get that

$$\left(\frac{c_1 c_2}{p}\right) f(x) = g'(x)\left(h'(x)/p\right),$$

where $h'(x)/p$ is still an element of $F[x]$. Repeating this process inductively, we get that

$$f(x) = g'(x)\left(\frac{h'(x)}{c_1 c_2}\right),$$

where $g'(x)$ and $h'(x)/(c_1 c_2)$ are both elements of $R[x]$.

Thus, if f is reducible in $F[x]$, it is also reducible in $R[x]$, and we are done. □

Lecture 9: The Splitting Field

We begin with a brief review of some previous lecture content. For any field K and irreducible polynomial $f(x) \in K[x]$, we know how to construct the field extension $K(\alpha)/K$, where α is a root of $f(x)$.

Moreover, we know that there is a bijection between the set $\mathrm{Aut}(K(\alpha)/K)$ and the distinct roots of $f(x)$ in $K(\alpha)$.

In Example 6.4, we considered the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, and found that if α is a root of $f(x)$, then $\left|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})\right| = 1$. We will see that $\mathbb{Q}(\alpha)$ is *not* a splitting field of $f(x)$ over $\mathbb{Q}$.

In Example 6.5, we considered the polynomial $f(x) = x^4 + 1 \in \mathbb{Q}[x]$, and found that if α is a root of $f(x)$, then $\left|\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})\right| = 4$. We will see that $\mathbb{Q}(\alpha)$ is a splitting field of $f(x)$ over $\mathbb{Q}$.

Definition 9.1. Let $f(x) \in K[x]$ be a (not necessarily irreducible) polynomial of degree d. Then F/K is a **splitting field** of $f(x)$ over K if

(1) $f(x)$ *splits completely* in $F[x]$; that is

$$f(x) = c\prod_{i=1}^{d}(x - \alpha_i) \in F[x]$$

and

(2) $F = K(\alpha_1, \ldots, \alpha_d)$, so the roots of $f(x)$ in F generate F/K.

Theorem 9.2. For any $f(x) \in K[x]$, we can construct its splitting field F/K. Furthermore, if $d = \deg f(x)$, then $[F : K] \leq d!$

Note that F/K tends to have many self-symmetries; we saw above that $\mathbb{Q}(\sqrt{i})/\mathbb{Q}$ has many self-symmetries.

Proof. First, we will construct this splitting field, by induction on the degree d.

If f splits completely in $K[x]$ then we can take $F = K$, so that $[F : K] = 1 \leq d!$ and we are done. (Note that this covers our base case of when $\deg f = 1$.)

Otherwise, let $g(x)$ be an irreducible factor of $f(x)$, such that $g(x)$ has degree greater than 1. Then, we know we can construct the field extension E/K, where $E = K(\alpha)$ such that $g(\alpha) = 0$. Then, in $E[x]$, we can write

$$f(x) = (x - \alpha)h(x)$$

for some polynomial $h(x) \in E[x]$. But then the degree of $h(x)$ is less than the degree of $f(x)$, so by our inductive assumption, we can find a splitting field F/E of $h(x)$.

Then, F contains α, and it contains all roots of $h(x)$, so it contains all roots of $f(x)$. Moreover,

$$F = E(\alpha_2, \ldots, \alpha_d) = K(\alpha, \alpha_2, \ldots, \alpha_d)$$

since it is a splitting field of $h(x)$ over $E = K(\alpha)$. So, F is a splitting field of $f(x)$ over K.

Moreover, $[F : K] = [F : E][E : K]$. By our inductive assumption, $[F : E] \leq (d-1)!$, and since we know that $[E : K] = \deg g(x) \leq d$, we get that $[F : K] \leq d!$
So the splitting field exists and has our desired dimension. □

Note that for $[F : K]$ to be exactly $d!$, $f(x)$ must be irreducible over K, and then $h(x)$ must be irreducible over E, and so on.

Moreover, this splitting field is unique up to isomorphism over K. We will actually prove a more general statement.

Theorem 9.3. Let $\varphi : F \tilde{\to} F'$ be a field isomorphism. Then, for any polynomial $f(x) \in F[x]$, let $f'(x)$ be the image of f with φ applied to the coefficients. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $f'(x)$ over F', φ extends to the isomorphism $\sigma : E \tilde{\to} E'$.

Pictorially, we have the diagram

$$\begin{array}{ccc} E & -\sigma \to & E' \\ | & & | \\ F & -\varphi \to & F' \end{array}$$

where φ and σ are both isomorphisms.

Proof. This means that if f splits completely in F, then f' splits completely in F', and we can have $E = F$ and $E' = F'$, and we are done.

We will show the case where f does not split completely in F via induction on the degree n of f.
At a base case, when $n = 1$, then there must be a root α of $f(x)$, then $\varphi(\alpha)$ is the root of $f'(x)$. So we have $E = F$ and $E' = F'$, so we are done.

Then, for the inductive step, we have the inductive assumption that the theorem statement is true for any field F, polynomial f, and isomorphism φ, where the degree of f is at most k. We would like to show that it holds for f of degree $k + 1$, where f does not split completely in F.

But we know that this means there is some irreducible factor $p(x)$ of f, where $p(x)$ has degree at least 2. Let $p'(x)$ be the image of $p(x)$ under our isomorphism; remember that this is also an irreducible factor of $f'(x)$. Then, we know that if α is a root of $p(x)$ and β is a root of $p'(x)$, then we have the induced isomorphism

$$\begin{array}{ccc} F(\alpha) & \longrightarrow^{\sigma_1} & F'(\beta) \\ | & & | \\ F & \longrightarrow^{\varphi} & F' \end{array}$$

where σ_1 is the map extending φ and setting $\sigma_1(\alpha) = \beta$. But then, we know that in $F(\alpha)[x]$, there exists some polynomial $h(x)$ such that $f(x) = (x - \alpha)h(x) \in F(\alpha)[x]$. Similarly, $f'(x) = (x - \beta)h'(x)$, where $h'(x) = \sigma_1(h(x))$. We can see that $E/F(\alpha)$ is a splitting field for $h(x)$ and $E'/F'(\beta)$ is a splitting field for $h'(x)$. Then, since $h(x)$ has degree at most k, we can apply our inductive assumption to induce another isomorphism:

$$\begin{array}{ccc} E & \longrightarrow^{\sigma} & E' \\ | & & | \\ F(\alpha) & \longrightarrow^{\sigma_1} & F'(\beta) \\ | & & | \\ F & \longrightarrow^{\varphi} & F' \end{array}$$

But this is exactly what we wanted, so we are done! □

Of course, by applying isomorphisms from F to itself that map $f(x)$ to itself, we can see that any way of constructing this splitting field is equivalent.

Corollary 9.4. Any two splitting fields for $f(x) \in F[x]$ are isomorphic.

Moreover, we have the following theorem, which can be proved in the same way as the above:

Theorem 9.5. For any polynomial $f(x) \in K[x]$, the splitting field F/K of $f(x)$ is the unique field with the property that, for any L/K, if $f(x)$ splits in $L[x]$ then there is a homomorphism $F \to L$ over K.

Lecture 10: Examples of Splitting Fields

Let's return to Example 6.4.

We showed that if α is a root of $f(x) = x^3 - 2$, then $\mathbb{Q}(\alpha)$ has no other roots of $f(x)$. Thus, $\mathbb{Q}(\alpha)$ is *not* the splitting field of $f(x)$. Specifically, we can see that

$$f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2) \in \mathbb{Q}(\alpha)[x].$$

Since $\mathbb{Q}(\alpha)$ has no other roots of $f(x)$, these factors must be irreducible over $\mathbb{Q}(\alpha)$.

Then, let β be a root of $x^2 + \alpha x + \alpha^2$, and define $F = \mathbb{Q}(\alpha, \beta)$. Then, F also contains the last root of this polynomial. In this case, the last root is $\alpha - \beta$, but we can also see that in general if we have one root of a quadratic, we must be able to factor it into the product of two linear polynomials, and therefore also have the second root.

Thus, F is the splitting field of $f(x)$, and

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 6.$$

We can also consider F as a subfield of $\mathbb{C}$. We know that in $\mathbb{C}$, the three roots of $x^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where ω is the primitive cube root of unity, or $e^{2i\pi}3 = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$.

We know from the definition of splitting field that $F \cong \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. In this case,

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{C}.$$

And there are multiple isomorphisms of F, such as

$$a \longmapsto \omega\sqrt[3]{2}, \qquad b \longmapsto \omega^2\sqrt[3]{2}, \text{or}$$
$$a \longmapsto \sqrt[3]{2}, \qquad b \longmapsto \omega\sqrt[3]{2}.$$

We can go back to looking at the symmetries of splitting fields.

Challenge 10.1. Convince yourself that:

(1) When F is the splitting field of $f(x) = x^4 + 1$ over $\mathbb{Q}$, $\mathrm{Aut}(F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (all automorphisms have order 2).

(2) When F is the splitting field of $f(x) = x^3 - 2$, $\mathrm{Aut}(F/\mathbb{Q}) \cong S_3$. (Note that the automorphism group of the splitting field of a cubic must be a subgroup of S_3, since it acts on the roots of $f(x)$.)

A useful observation is that:

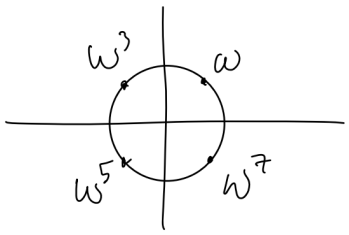
For any degree-d polynomial $f(x) \in \mathbb{Q}[x]$, f has roots $\alpha_1, \ldots \alpha_d$ in $\mathbb{C}$, by the fundamental theorem of algebra. In other words, $f(x)$ splits completely in $\mathbb{C}[x]$. So the splitting field of $f(x)$ is isomorphic to the subfield

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_d) \subseteq \mathbb{C}.$$

Example 10.2. The splitting field of $x^4 + 1$ over $\mathbb{Q}$ has degree 4.

What is the splitting field of $x^4 + 2$ over $\mathbb{Q}$?

Take a root ω of $x^4 + 1$:



Then, the roots (in $\mathbb{C}$) of x^4+2 are $\sqrt[4]{2}\omega$, $\sqrt[4]{2}\omega^3$, $\sqrt[4]{2}\omega^5$, and $\sqrt[4]{2}\omega^7$.

Thus, the splitting field is

$$F = \mathbb{Q}(\sqrt[4]{2}\omega, \sqrt[4]{2}\omega^3, \sqrt[4]{2}\omega^5, \sqrt[4]{2}\omega^7) \subseteq \mathbb{C}.$$

But since $\omega = \frac{\sqrt{2}}{2}(1+i)$, we can see that $F \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$.

Note that

$$\sqrt{2} = \frac{\left(\sqrt[4]{2}\omega\right)^3}{\sqrt[4]{2}\omega^3},$$

so $\sqrt{2} \in F$. Then,

$$i = \omega^2 = \frac{\left(\sqrt[4]{2}\omega\right)^2}{\sqrt{2}},$$

so $i \in F$, and then $\omega = \frac{\sqrt{2}}{2}(1+i) \in F$, and finally $\sqrt[4]{2} = (\sqrt[4]{2}\omega)/\omega \in F$. So, $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq F$, and $F = \mathbb{Q}(\sqrt[4]{2}, i)$.

Then, $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2})(i)$, and since the minimal polynomial of $\sqrt[4]{2}$ is x^4-2 and the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$ is x^2+1, we get that

$$\begin{aligned}[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \\ &= 2 \cdot 4 = 8.\end{aligned}$$

Example 10.3. What is the degree of $x^4 - 2$ over $\mathbb{Q}$?

The roots of $x^4 - 2$ in $\mathbb{C}$ are $\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i$.

Thus, the splitting field is $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i) \subseteq \mathbb{C}$, so the degree is 8, as we just showed.

So the splitting field of x^4+2 is the splitting field of x^4-2.

But we can see that the splitting field of x^4+1 is $\mathbb{Q}(\omega)$, while the splitting field of x^4-1 is $\mathbb{Q}(i)$, so this isn't a general pattern.

Lecture 11: The Algebraic Closure

The splitting field of x^4+2 over $\mathbb{Q}$ is the degree-8 extension $\mathbb{Q}(\sqrt[4]{2}, i)$.

The splitting field of x^4+1 over $\mathbb{Q}$ is the degree-4 extension $\mathbb{Q}(\sqrt{2}, i)$.

All of these are subfields of $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, where, as we defined before $\overline{\mathbb{Q}}$ is the set of all $\alpha \in \mathbb{C}$ such that α is algebraic over $\mathbb{Q}$.

Can we similarly construct $\overline{K}$ for any field K?

Is $\overline{K}$ uniquely determined by K?

Is there an algebraic extension of K that splits all polynomials in $K[x]$?

Proposition 11.1. For fields $K \subseteq E \subseteq F$, $F/K$is algebraic if and only if F/E and E/K is algebraic.

Proof. One direction is clear, because if every element of F is algebraic over K, then every element of F is algebraic over $E \supseteq K$, and every element of $E \subseteq F$ is algebraic over K.

For the other direction, suppose F/E and E/K are algebraic. Then, for any $\alpha \in F$, there exists some minimal polynomial

$$f(x) = x^d + e_{d-1}x^{d-1} + \cdots + e_0 \in E[x].$$

Then, we can see that

$$K \subseteq K(e_0, \ldots, e_{d-1}) \subseteq K(e_0, \ldots, e_{d-1}, \alpha).$$

The first extension is finite because it is finitely generated and algebraic (since each $e_i \in E$), and the second extension is finite because its degree is d. Thus, $K(\alpha)/K$ is also finite, so α is algebraic. □

Definition 11.2. Let F be a field. F is **algebraically closed** if every irreducible polynomial in $F[x]$ has degree 1, or, equivalently, that every non-constant polynomial $f(x) \in F[x]$ has a root in F.

Example 11.3. $\mathbb{C}$ is algebraically closed.

Is $\overline{\mathbb{Q}}$ algebraically closed?

Take any polynomial $f(x)$ which is irreducible in $\overline{\mathbb{Q}}[x]$. It has a zero $\alpha \in \mathbb{C}$. But then $\overline{\mathbb{Q}}(\alpha)$ is an algebraic extension of $\overline{\mathbb{Q}}$, which is an algebraic extension of $\mathbb{Q}$, so $\overline{\mathbb{Q}}(\alpha)/\mathbb{Q}$ is algebraic, and $\alpha \in \overline{\mathbb{Q}}$ by definition. So, $\overline{\mathbb{Q}}$ is algebraically closed.

Generalizing this idea gives us the following proposition:

Proposition 11.4. Let L be an algebraically closed field, and let K be a subfield of L. Then

$$\overline{K} = \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$$

is an algebraically closed field that is algebraic over K.

Definition 11.5. Let K be a field. Then, the **algebraic closure** of K is an algebraic extension F/K, where F is algebraically closed.

Next lecture, we will show that for any field K, an algebraic closure of K exists and is unique up to isomorphism over K. For the rest of this lecture, we will look at more properties of algebraically closed fields, which will help us prove this theorem next lecture.

Lemma 11.6. A field F is algebraically closed if and only if F has no nontrivial algebraic extensions.

Proof. Assume F is algebraically closed. Then, let L be an algebraic extension of F. For any $\alpha \in L$, we know that the minimal polynomial of α over F must be irreducible, so since F is algebraically closed, it must have degree 1. Thus $\alpha \in F$, and $L = F$.

Assume every algebraic extension of F is trivial. Then, for any irreducible polynomial $f(x) \in F[x]$, we know that the extension $F(\alpha)/F$, where $f(\alpha) = 0$, is trivial. But the degree of this extension must equal the degree of $f(x)$, so $f(x)$ must have degree 1, and F is algebraically closed. □

We will now show that any algebraically closed extension of K contains every algebraic extension of K.

Proposition 11.7. Let L be an algebraically closed field, and K be a subfield of L. Then, if F/K is an algebraic field extension, there is homomorphism $F \to L$ over K.

Note that algebraic closure is an absolute property, it isn't relative to anything else.

The idea behind this proof is: If $F = K(\alpha)$, with minimal polynomial $f(x)$ over K, then since $f(x) \in L[x]$ and L is algebraically closed, L must contain a root of $f(x)$, so $K(\alpha) \subseteq L$. Then, if $F = K(\alpha, \beta)$ we know that $K(\alpha)$ is a subfield of L, and then there is some minimal polynomial for β over $K(\alpha)$, which must have a root in L, so we can assign that root to β...
How do we know when to terminate? Using Zorn's Lemma.

Proof. Consider the collection of homomorphisms

$$\mathcal{P} = \{i_E : E \to L \text{ over } K, K \subset E \subset F\}.$$

Then, $\mathcal{P}$ is a partially ordered set, under the ordering

$$i_{E_1} \leq i_{E_2} \text{ when } E_1 \subseteq E_2 \text{ and } i_{E_2}\,|_{E_1} = i_{E_1}.$$

Then, for every chain $\mathcal{C}$ of $\mathcal{P}$, we can construct the upper bound of $\mathcal{C}$ as follows: first, define

$$E_{\mathcal{C}} = \bigcup_{i_E \in \mathcal{C}} E.$$

This is a field since it is the union of the chain $E_1 \subseteq E_2 \subseteq \cdots$. Then, the upper bound of the chain is the homomorphism

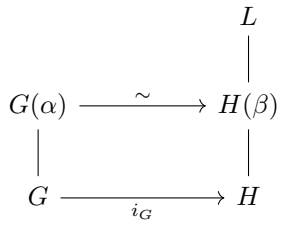
$$i_{E_{\mathcal{C}}}(x) = i_E(x) \text{ for any } i_E \in \mathcal{C} \text{ such that } x \in E.$$

This is well-defined, because if there is E_1, E_2 in the chain such that $x \in E_1 \cap E_2$, we know by definition that $i_{E_1}(x) = i_{E_2}(x)$.

Then, Zorn's Lemma tells us there is a maximal element in $\mathcal{P}$. Let us call this element $i_G : G \to L$ over K.

We claim $G = F$. To see this, assume there is some $\alpha \in F \setminus G$. Then, since F/K is algebraic, $G(\alpha)$ is algebraic over G. Then, let $f(x) \in G[x]$ be the minimal polynomial of α over G, and let H be the image of

G in L. Then, $i_G(f(x)) \in H[x]$ has some root in L, which we can call β. We get the induced isomorphism:



and we can see that $i_{G(\alpha)} > i_G$, which contradicts the fact that i_G is the maximal element.

Thus, $G = F$, and we have found a homomorphism $F \to L$ over K. □

Moreover, we can show that if an algebraic closure of K exists, it is unique up to isomorphism.

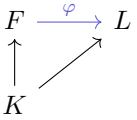
Theorem 11.8. If F_1, F_2 are algebraic closures of K, then there is an isomorphism $F_1 \to F_2$ over K.

Proof. By the above proposition, we know that there exists a homomorphism $\varphi : F_1 \to F_2$ over K. Then, $F_2/\varphi(F_1)$ is an algebraic field extension. But $\varphi(F_1) \simeq F_1$, so $\varphi(F_1)$ is algebraically closed. This means the only algebraic extensions of $\varphi(F_1)$ are trivial, so $F_2 = \varphi(F_1) \cong F_1$. □

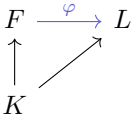
Lecture 12: Constructing the Algebraic Closure

We begin with a review of the different type of field extensions we have seen so far, and their universal properties. Assume K is a field.

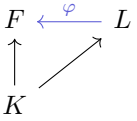
Let F be the field generated by a root of an irreducible $f(x) \in K[x]$.
$\implies$ F/K contains a root of $f(x)$ and for any L/K containing a root of $f(x)$ there is a homomorphism $F \to L$ over K.



Let F be the splitting field of a polynomial $f(x) \in K[x]$.
$\implies$ the polynomial $f(x)$ splits completely in $F[x]$ and for any L/K such that $f(x)$ splits completely in $L[x]$, there is a homomorphism $F \to L$ over K.



Let F be the algebraic closure of K.
$\implies$ F/K is algebraic and for any algebraic extension L/K there is a homomorphism $L \to F$ over K.



Theorem 12.1. For any field K, there is an algebraic extension F/K such that F is algebraically closed.

(We already showed that such an F is unique up to isomorphism.)

Proof. It is enough to show that there is an algebraically closed field L containing K. We showed last lecture that if we have such a field $L \supseteq K$, then the set of all elements in L that are algebraic over K forms a subfield of L that is algebraically closed and an algebraic extension of K.

Let $\mathcal{F}$ be the set of all monic polynomials in $K[x]$ with positive degree. Then, for each polynomial $f(x) \in F$, define the variable y_f. Then, we will consider the ring

$$S = K[y_f]_{f \in \mathcal{F}}.$$

This is similar to the polynomial ring $K[x]$, except we adjoin a new variable for each polynomial $f(x) \in F$.

Then, let $I \subseteq S$ be the ideal $(f(y_f))_{f \in \mathcal{F}}$. This is the ideal containing $f(y_f)$ for each polynomial $f \in \mathcal{F}$. We want this to be a proper ideal of S. To show this, assume it was not a proper ideal, so I contains 1. This means there is some linear combination of finitely many of the $f(y_f)$'s that equals 1:

$$g_1 f_1(y_{f_1}) + \cdots + g_n f_n(y_{f_n}) = 1,$$

where $g_1, \ldots, g_n \in S$, so they are polynomials over finitely many of the other y_f's. But then, let K' be an algebraic extension of K containing roots $\alpha_1, \ldots, \alpha_n$ of $f_1, \ldots, f_n$, respectively. We can evaluate this

polynomial over K', setting $y_{f_i} = \alpha_i$ for each i (and setting all of the other inputs for g_i arbitrarily), and we get that

$$g_1 f_1(\alpha_1) + \cdots + g_n f_n(\alpha_n) = 1$$
$$0 + \cdots + 0 = 1 \in K',$$

which is clearly a contradiction. Thus, I is a proper ideal of S.

Then, applying Zorn's lemma, there is a maximal ideal of M of S containing I. Then, we can take $K_1 = S/M$, since the quotient of a ring and a maximal ideal is a field.

Then, we can see that every non-constant $f(x) \in K[x]$ has a root in K_1, because $[y_f] \in K_1$ and $f([y_f]) = [f(y_f)] = 0 \in K_1$ since $f(y_f) \in I$ by definition.

But in order for our field to be algebraically closed, we also need all polynomials in $K_1[x]$ to have a root in the field. So we repeat the above process with K_1 as our base field, and continue indefinitely to get the chain

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots .$$

Then, we can take

$$L = \bigcup_{i=0}^{\infty} K_i,$$

and we can see that for any $f(x) \in L(x)$, since $f(x)$ has finitely many coefficients, there must be some K_i such that all coefficients of $f(x)$ are in K_i. But this means that $K_{i+1} \subseteq L$ has a root of f, so L is algebraically closed.

Then, let F be the collection of elements of L which are algebraic over K. We showed last lecture that this is a field, and it is clear F/K is algebraic. Then, every polynomial $f(x) \in K[x]$ splits completely into linear factors $(x - \alpha)$ in $L[x]$. But each such α, by definition, is the root of a polynomial in $K[x]$, which means it is an element of F, so $f(x)$ also splits completely in $F[x]$, and we have found an algebraic extension of K which is also algebraically closed. □

We know that typically $\overline{K}/K$ is infinite. But how large is $\mathrm{Aut}(\overline{K}/K)$?

Example 12.2. There are no non-identity automorphisms of $\mathbb{R}$ over $\mathbb{Q}$, so $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$. But $[\mathbb{R} : \mathbb{Q}]$ is infinite because $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$ are all linearly independent over $\mathbb{Q}$.

Proposition 12.3. Let F/K be the splitting field of $f(x)$ in $K[x]$. Then, there is a surjective group homomorphism

$$\mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}(F/K),$$

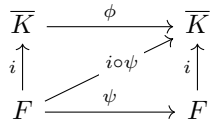
which implies that $\left|\mathrm{Aut}(\overline{K}/K)\right| \geq \left|\mathrm{Aut}(F/K)\right|$.

Proof. Let $Z(f) = \left\{\alpha \in \overline{K} \;\middle|\; f(\alpha) = 0\right\}$. We can see that $Z(f) \subseteq K$ generates the splitting field F (technically, it generates an isomorphic copy of F, as a subfield of K).

We claim that for any automorphism $\varphi \in \mathrm{Aut}(\overline{K}/K)$, $\varphi(F) \subseteq F$. This is because $\varphi(Z(f)) \subseteq Z(f)$, since for φ to be an isomorphism, it must map all roots of f to other roots of f. Moreover, since φ is an injective map, and it maps a finite-dimensional vector space F/K to itself, it must also be surjective over F, so $\varphi(F) = F$.

Thus, $\varphi|_F$ is an automorphism over F, so we get the group homomorphism $\mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}(F/K)$ by sending $\varphi \mapsto \varphi\,|_F$.

This is a surjective group homomorphism, since if $\psi \in \mathrm{Aut}(F/K)$, then we know that there is a $\phi \in \mathrm{Aut}(\overline{K}/K)$ extending ψ. This is because $\overline{F} = \overline{K}$, and applying the universal property of algebraic closure to the (top-left triangle of the) following commutative diagram



tells us that ϕ must exist.
Thus, we have found a surjective group homomorphism $\mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}(F/K)$. □

The following is still an open problem

Conjecture 12.4 (Inverse Galois Problem)**.** Given any finite group G, there is $f(x) \in \mathbb{Q}[x]$ whose splitting field F satisfies

$$\mathrm{Aut}(F/\mathbb{Q}) \cong G.$$

The proposition we just proved tells us that this would imply:

Given any finite group G, there is a surjective group homomorphism

$$\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G.$$

Later, we will describe the group $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

Lecture 13: Conjugate Elements and Normal Extensions

What is algebraic closure of K?

It is a homomorphism from K to an algebraically closed field that is algebraic over K.

We proved that for any field K, there is an algebraic closure $\overline{K}$ of K, and it is unique up to isomorphism over K.

We also proved that for any splitting field F/K, there is a surjective group homomorphism $\mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}(F/K)$. (Remember that $K \subseteq F \subseteq \overline{K}$ in this case.)

Specifically, this homomorphism was the just restriction of isomorphisms of $\overline{K}/K$ to F/K. The main idea was that if F is the splitting field of $f(x) \in K[x]$, which has n distinct roots in $\overline{K}$, then any automorphism $\varphi \in \mathrm{Aut}(\overline{K}/K)$ must permute these n roots (it cannot map a root of $f(x)$ to something that is not a root of $f(x)$, and it is injective and therefore surjective over these roots). We can view φ as a permutation of these n roots, and doing so gives us a homomorphism $\mathrm{Aut}(\overline{K}/K) \to S_n$, mapping each φ to its corresponding permutation. Then, the image of this homomorphism is isomorphic to $\mathrm{Aut}(F/K)$, since by Theorem 6.2, every automorphism of F over K is defined by the permutation of these roots.

Definition 13.1. When $K = \mathbb{F}_p$ or $K = \mathbb{Q}$, $\mathrm{Aut}(\overline{K}/K)$ is called the **absolute Galois group of** K.

Remember from Math 120 that in general, if G is a group acting on a set X, X is the disjoint union of G-orbits.

The group $\mathrm{Aut}(\overline{K}/K)$ acts on the set $\overline{K}$.

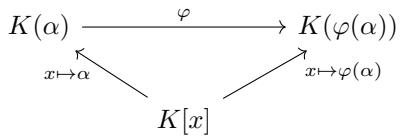
What is the corresponding orbit decomposition of $\overline{K}$?

Definition 13.2. Two elements α_1, α_2 of $\overline{K}$ are **conjugate** if the minimal polynomial of α_1 over K is the minimal polynomial of α_2 over K.

Proposition 13.3. For any $\alpha \in \overline{K}$, the orbit of α under $\mathrm{Aut}(\overline{K}/K)$ is the set of conjugates of α over K.

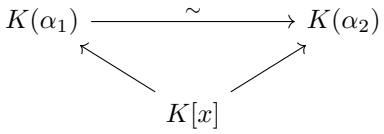
Proof. We will first prove that if two elements in $\overline{K}$ are in the same orbit under $\mathrm{Aut}(\overline{K}/K)$, they are conjugate.

For any $\alpha \in \overline{K}$ and $\varphi \in \mathrm{Aut}(\overline{K}/K)$, we want to show that α and $\varphi(\alpha)$ are conjugate. But by the universal property of field extension, we have

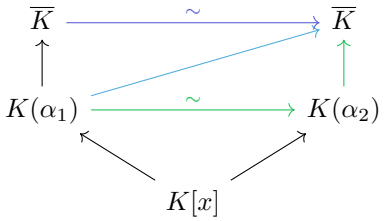


But this means that the kernels of the left and right maps must be the same. We can see that the kernel of the $K[x] \to K(\alpha)$ map is the ideal $(f_\alpha(x))$, where $f_\alpha(x)$ is the minimal polynomial of α over K, and the kernel of the $K[x] \to K(\varphi(\alpha))$ map is the ideal $(f_{\varphi(\alpha)}(x))$ where $f_{\varphi(\alpha)}$ is the minimal polynomial of $\varphi(\alpha)$ over K. But for these two kernels to be the same, the minimal polynomials must be the same, so α and $\varphi(\alpha)$ are conjugate.

Next, we will prove that if two elements of $\overline{K}$ are conjugate, they must be in the same orbit under $\mathrm{Aut}(\overline{K}/K)$. Take any α_1, α_2 in $\overline{K}$ that are conjugate. This means they have the same minimal polynomial, so $K(\alpha_1) = K(\alpha_2)$. This gives us the commutative diagram



But then, by the universal property of the algebraic closure, we get the commutative diagram



by first defining the blue arrow as the composition of the green arrows, and then applying the universal property to the top-left triangle to get the purple arrow.

But the purple arrow in this commutative diagram, which we can call φ, is an automorphism $\overline{K} \to \overline{K}$, and $\varphi(\alpha_1) = \alpha_2$, since it is an extension of the isomorphism $K(\alpha_1) \to K(\alpha_2)$. But this means that α_1 and α_2 are in the same orbit under $\mathrm{Aut}(\overline{K}/K)$, which is what we wanted to show.

Thus, the orbit of α under $\mathrm{Aut}(\overline{K}/K)$ is exactly the set of conjugates of α, for any $\alpha \in \overline{K}$. □

Informally, we can think of this as saying that the set $\overline{K}$ modulo the action of $\mathrm{Aut}(\overline{K}/K)$ is the set of all monic irreducibles in $K[x]$. This means that $\overline{K}$ is the set of all roots of all irreducibles in $K[x]$.

Let's shift back to talking about splitting fields.

Different polynomials can have the same splitting field; we saw this in Example 10.2.

A finite extension of $\mathbb{Q}$ isn't necessarily the splitting field of any polynomial in $\mathbb{Q}[x]$. We will show soon that $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$.

We will show later that every finite extension of $\mathbb{F}_p$ is the splitting field of some $f(x) \in \mathbb{F}_p[x]$.

Definition 13.4. An algebraic extension F/K is **normal** if for every irreducible polynomial $f(x) \in K[x]$, either $f(x)$ splits in $F[x]$ or $f(X)$ has no roots in F.

A useful reformulation of this definition is that F/K is normal if for every $\alpha \in F$, the minimal polynomial of α over K splits completely in $F[x]$.

Example 13.5.

(1) For any field K, K/K is a normal extension because for any $\alpha \in K$, the minimal polynomial for α is linear, so it splits completely in $K[x]$.

(2) For any field K, $\overline{K}/K$ because by definition, every polynomial splits completely over $\overline{K}$.

(3) A quadratic extension F/K is normal since for all $\alpha \in F$, either the minimal polynomial for α is linear, or it is quadratic and can be split into $(x-\alpha)$ and some other linear factor.

(4) For any field K and $f(x) \in K[x]$, the splitting field extension F/K is normal.

To show this, we know that $K \subseteq F \subseteq \overline{K}$. Then, for any $\alpha \in F$, we want to show that F contains all conjugates of α in $\overline{K}$. Proposition 13.3 tells us this is equivalent to showing that for all $\varphi \in \mathrm{Aut}(\overline{K}/K)$, $\varphi(\alpha) \in F$. But we already showed that for a splitting field F, $\varphi(F) \subseteq F$, so we are done.

Example 13.6.

(1) The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$, but its minimal polynomial x^3-2 does not split completely in $\mathbb{Q}(\sqrt[3]{2})$. Since we just showed that all splitting fields are normal, $\mathbb{Q}(\sqrt[3]{2})$ cannot be the splitting field for any polynomial in $\mathbb{Q}[x]$.

(2) Similarly, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the minimal polynomial of $\sqrt[4]{2}$ is x^4-2, and this does not split completely in $\mathbb{Q}(\sqrt[4]{2})$. Thus, it is also not the splitting field of any polynomial in $\mathbb{Q}[x]$

Theorem 13.7. The following are equivalent for any finite extension F/K:

(1) F/K is the splitting field of a polynomial over K

(2) For any homomorphisms $\psi_1 : F \to \overline{K}$, $\psi_2 : F \to \overline{K}$ over K, $\psi_1(F) = \psi_2(F)$

(3) F/K is normal

We just showed that (1) $\implies$ (3) in the previous examples. For intuition about (2), we can see that (2) does not hold for $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Consider the homomorphism $\psi_1 : \mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$ which is the inclusion map, and $\psi_2 : \mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$ defined by $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$, where $\omega = e^{2i\pi/3}$. Then, we can see that $\operatorname{im}\psi_1 \subseteq \mathbb{R}$, while $\operatorname{im}\psi_2$ contains $\omega\sqrt[3]{2}$, which is not an element of $\mathbb{R}$, so the two cannot be equal.

Proof. We first show that (1) $\implies$ (2):

Suppose F/K is the splitting field of some polynomial $f(x) \in K[x]$. Then, let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in $\overline{K}$. We know that by definition of the splitting field, F must also have n distinct roots of $f(x)$. We can see that for any $\psi : F \to \overline{K}$, since ψ is a homomorphism over K, each of the the roots of $f(x)$ in F must map to some α_i. Moreover, since field homomorphisms are injective, and there are n distinct roots in F, all of $\alpha_1, \ldots, \alpha_n$ must be in the image of ψ, and we get that $\psi(F)$ is exactly $K(\alpha_1, \ldots, \alpha_n) \subseteq \overline{K}$, for all such ψ.

Then, we will show that (2) $\implies$ (3):

Suppose F/K has a well-defined image F' in $\overline{K}$. Then, for any $\varphi \in \mathrm{Aut}(\overline{K}/K)$, we see that $\varphi(F')$ must equal F' (otherwise $\varphi \circ \psi$ would give us a distinct image of F, contradicting (2)). Then, we know from Proposition 13.3 that for any $\alpha \in F'$, F' must contain all conjugates of α, so $F'/K \cong F/K$ is normal.

Finally, we will show that (3) $\implies$ (1):

Since F/K is finite, it has some basis $\alpha_1, \ldots, \alpha_n$ over K. For each $1 \le i \le n$, let $f_i(x)$ be the minimal polynomial for α_i over K. Then,

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

splits completely in $F[x]$, and since $F = K(\alpha_1, \ldots, \alpha_n)$, F is the splitting field for $f(x)$.

Thus, the three properties are equivalent, for *finite* field extensions. □

Remark 13.8. Recall that if $K \subseteq E \subseteq F$ is a chain of field extensions, then $[F : K]$ is finite if and and only if $[E : K]$ and $[F : E]$ are finite.

Similarly, if $K \subseteq E \subseteq F$ is a chain of field extensions, then F/K is algebraic if and only if F/E and E/K are algebraic.

But neither direction of this is true for normal extensions. We have the following counterexamples:

$$\mathbb{Q} \xrightarrow{\text{normal}} \mathbb{Q}(\sqrt{2}) \xrightarrow{\text{normal}} \mathbb{Q}(\sqrt[4]{2}), \quad \mathbb{Q} \xrightarrow{\text{not normal}} \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\text{normal}} \mathbb{Q}(\sqrt[3]{2}, \omega)$$

However, we do have the following weaker proposition:

Proposition 13.9. If $K \subseteq E \subseteq F$ is a chain of field extensions, and F/K is normal, then F/E is normal.

Proof. For $\alpha \in F$, define $f_K(x)$ to be the minimal polynomial of α over K and $f_E(x)$ to be the minimal polynomial of α over E. But this means there is some $g(x) \in E[x]$ such that

$$f_K(x) = f_E(x)g(x) \in E[x].$$

So if $f_K(x)$ splits completely in $F[x]$, $f_E(x)$ must also split completely in $F[x]$, so since F is normal over K, it must also be normal over E. □

If we have a chain of field extensions $K \subseteq E \subseteq F$, where F/K and E/K are both normal, what can we say about their automorphism groups?

We know there is a group automorphism $\mathrm{Aut}(F/K) \to \mathrm{Aut}(E/K)$ defined by the restriction map $\varphi \mapsto \varphi|_E$. Moreover, since we have the following commutative diagram,

$$\begin{array}{ccc} \mathrm{Aut}(F/K) & \twoheadrightarrow & \mathrm{Aut}(E/K) \\ & \nwarrow \quad \nearrow & \\ & \mathrm{Aut}(\overline{K}/K) & \end{array}$$

and the arrows in green are surjective by Proposition 12.3, our map $\mathrm{Aut}(F/K) \to \mathrm{Aut}(E/K)$ must also be surjective. But we need $\varphi(E/K)$ to be normal for this map to exist, since we are relying on the fact that, for any automorphism $\varphi : F/K \to F/K$, $\varphi(E) = E$.

This is a preview of some of the Galois theory we will be doing towards the end of this course.

Lecture 14: Separable Polynomials

Last time, we discussed properties of finite normal extensions. But there are also infinite normal extensions.

Example 14.1. The extensions $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(i)/\mathbb{Q}$, and $\mathbb{F}_4/\mathbb{F}_2$ are all normal because they are quadratic.

Remember from last time that for a chain of field extensions $K \subseteq E \subseteq F$, it is possible for F/K to be normal but E/K to not be normal. For example:

$$\mathbb{Q} \xrightarrow{\text{not normal}} \mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\text{normal}} \mathbb{Q}(\sqrt[3]{2}, \omega)$$
$$\mathbb{Q} \xrightarrow[\text{normal}]{} \mathbb{Q}(\sqrt[3]{2}, \omega)$$

Let us say we have some $\alpha \in \overline{K}$ whose minimal polynomial over K is $f(x)$. Then, the roots of $f(x)$ are the conjugates of α over K, by definition.

Does this mean that, if $\alpha = \alpha_1, \ldots, \alpha_n$ are the conjugates of α, $f(x)$ is exactly

$$\prod_{i=1}^{n} (x - \alpha_i) \in \overline{K}[x],$$

or can some of the roots appear with multiplicity?

In general, there can be multiplicity, but when $K = \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{F}_p$ for prime p, there is no multiplicity. We will learn later that this is because $\mathbb{Q}$ and $\mathbb{R}$ and $\mathbb{F}_p$ are examples of perfect fields.

Definition 14.2. The polynomial $f(x) \in K[x]$ is **separable** if all its roots over its splitting field are distinct; it has no factors that appear multiple times.

The amazing fact is that we can easily decide if $f(x)$ is separable or not, by differentiating $f(x)$ over K.

Definition 14.3. We define the **derivative** over K to be the K-linear map $\frac{d}{dx} : K[x] \to K[x]$, defined by

$$\frac{d}{dx}(x^n) = nx^{n-1} \text{ and } \frac{d}{dx}(1) = 0.$$

Here, the exponent n is an integer, so in the term nx^{n-1}, we take n to mean $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$.

Then, we need to know that the derivative of a product is what we would expect.

Theorem 14.4. $\frac{d}{dx}(fg) = f\frac{d}{dx}(g) + g\frac{d}{dx}(f)$.

Proof. Since the derivative is a K-linear map, we just need to show that this holds for basis elements, so when $f = x^m$ and $g = x^n$ for some positive integers m and n. We can see that

$$\begin{aligned}\frac{d}{dx}(x^{m+n}) &= (m+n)x^{m+n-1} \\ &= nx^{n-1}x^m + mx^{m-1}x^n \\ &= x^m \frac{d}{dx}(x^n) + x^n \frac{d}{dx}(x^m).\end{aligned}$$

Thus, the derivative of our product is what we wanted. □

Using this, we have a condition for when $f(x) \in K[x]$ is separable.

Theorem 14.5. A polynomial $f(x) \in K[x]$ is separable if and only if $f(x)$ and $\frac{d}{dx}(f(x))$ are relatively prime in $K[x]$.

Proof. Let F be the splitting field of $f(x)$.

First, if $f(x)$ has a multiple root $\alpha \in F$, so that

$$f(x) = (x-\alpha)^m g(x) \in F[x],$$

where $m \geq 2$, the derivative is

$$\frac{d}{dx}(f(x)) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m \frac{d}{dx}g(x).$$

But then, clearly $(x-\alpha)$ is a factor of both $f(x)$ and $\frac{d}{dx}(f(x))$ in $F[x]$, which means the minimal polynomial for α must be a factor of both $f(x)$ and $\frac{d}{dx}(f(x))$ in $K[x]$, and the two cannot be relatively prime.

Then, if $f(x)$ and $\frac{d}{dx}(f(x))$ are not relatively prime in $K[x]$, they have some common factor $d(x)$ in $K[x]$. But then $d(x)$ splits in $F[x]$, so there exists some $\alpha \in F$ that is a root of both $f(x)$ and $\frac{d}{dx}(f(x))$. So, we can write

$$f(x) = (x-\alpha)h(x) \in F[x],$$

and taking the derivative gives us

$$\frac{d}{dx}(f(x)) = h(x) + (x-\alpha)\frac{d}{dx}h(x).$$

So for $\frac{d}{dx}(f)(\alpha)$ to be 0, we need $h(\alpha) = 0$. But that means that $(x-\alpha)^2$ is a factor of $f(x)$, and $f(x)$ is not separable. □

Corollary 14.6. If $\mathrm{ch}(K) = 0$ then every irreducible polynomial in $K[x]$ is separable.

Proof. If $f(x) \in K[x]$ is an irreducible polynomial of degree d, then $\frac{d}{dx}f(x)$ is a nonzero polynomial of degree $d-1$, which clearly must be relatively prime to an irreducible. So $f(x)$ is separable. □

The above proof doesn't work for a field with characteristic p, because in that case it is possible that $\frac{d}{dx}f(x) = 0$ even when $f(x)$ is non-constant, and then $f(x)$ and its derivative are not relatively prime.

Example 14.7. For an example of an irreducible polynomial that is not separable, consider the field $K = \mathbb{F}_p(t)$.

Then, take

$$f(x) = x^p - t \in K[x].$$

This is irreducible by Eisenstein's criterion applied to the prime ideal (t). But it is not separable, since $\frac{d}{dx}(x^p - 1) = 0$, and $f(x)$ and 0 are not relatively prime.

Specifically, we can see that $\alpha = t^{1/p}$ is a root of this polynomial. If we consider the field $F = K(\alpha)$, we can see that

$$(x-\alpha)^p = x^p - \alpha^p = x^p - t \in F[x],$$

so α is the only root of $f(x)$ in $\overline{K}$, and it appears with multiplicity p.

Lecture 15: Perfect Fields

Last lecture, we defined a **separable** polynomial as one whose roots are all distinct. Moreover, we showed that a polynomial $f(x) \in K[x]$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime in $K[x]$, which implies that when $\text{ch}(K) = 0$, every irreducible polynomial is separable.

Let us now consider case where $f(x) \in K[x]$ is an irreducible but *not* separable polynomial. This occurs only in the case where $\text{ch}(K)$ is some prime $p > 0$. Moreover, $\frac{d}{dx}(f(x))$ must be the constant polynomial 0, because otherwise $f(x)$ and $\frac{d}{dx}(f(x))$ are still relatively prime.

Then, if we write

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d,$$

we get that

$$\frac{d}{dx}(f(x)) = a_1 + \cdots + d a_d x^{d-1}.$$

For this derivative to equal 0, we must have $a_i = 0$ for all i not divisible by p. So $f(x)$ must be of the form

$$f(x) = a_0 + a_p x^p + \cdots + a_{dp} x^{dp}.$$

Definition 15.1. Suppose $\text{ch}(K) = p$. Then, the **Frobenius map** of K is the map $\varphi : K \to K$ defined by $\varphi(a) = a^p$.

An amazing fact is that φ is a field homomorphism, since $a^p + b^p = (a+b)^p$ and $a^p b^p = (ab)^p$ in K.

Remark 15.2. The only homomorphism from $\mathbb{F}_p$ to $\mathbb{F}_p$ is the identity map, since we must map 1 to 1, and 1 generates all of $\mathbb{F}_p$. This implies that $a^p \equiv a \mod p$ for any $a \in \mathbb{Z}$.

But for any finite field K of cardinality p^e, where $e > 1$, the Frobenius map is not the identity map. This is because $x^p - x$ cannot have more than p roots in K, but K has more than p elements, so there must be elements $a \in K$ such that $a^p \neq a$.

The Frobenius map is thus a nontrivial automorphism of a finite field - we know it is an isomorphism because all field homomorphisms are injective, and since the domain and the range are both K, which is finite, it must also be surjective.

Definition 15.3. A field K is **perfect** if $\text{ch}(K) = 0$ or $\text{ch}(K) = p$ and the Frobenius map of K is surjective.

We like perfect fields, because they have lots of nice properties that make doing Galois theory with them very clean and applicable ☺

Example 15.4.

(1) Every finite field is perfect, as we showed above.

(2) Every algebraic extension of a finite field is perfect, but there aren't many examples of infinite algebraic extensions. This is because (as we showed on homework 3) all homomorphisms over the base field extend to isomorphisms over an algebraic extension.

(3) All fields of characteristic 0 are perfect.

Theorem 15.5. In a perfect field, all irreducible polynomials in $K[x]$ are separable.

Proof. We already showed that this is true when $\text{ch}(K) = 0$, so we just need to prove the case where $\text{ch}(K) = p > 0$.
In this case, assume we can find some $f(x) \in K[x]$ that is irreducible and inseparable. We showed at the beginning of this lecture that this means

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{np} x^{np},$$

for some n. Since K is prefect, we know that each a_{ip} can be expressed as b_i^p for some $b_i \in K$. Then,

$$\begin{aligned} f(x) &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^p, \end{aligned}$$

so $f(x)$ is not irreducible, which is a contradiction. □

Definition 15.6. An algebraic extension F/K is **separable** if for every $\alpha \in F$, the minimal polynomial of α over K is separable.

Remark 15.7. Note that "the minimal polynomial of α over K is separable" is a property of α and $\overline{K}$, not K itself. Thus, if we have a chain of field extensions $K \subseteq E \subseteq F$, then if F/K is separable, so is E/K (since this is a subset of F/K) and F/E (since $\overline{E} = \overline{K}$).

Remark 15.8. If K is perfect, then every algebraic extension F/K is separable. This is because the minimal polynomial for any $\alpha \in F$ is irreducible in $K[x]$, so it must be separable.

Proposition 15.9. For a field K, the following are equivalent:

(1) K is perfect

(2) Every irreducible polynomial in $K[x]$ is separable

(3) Every algebraic extension of K is separable

Proof. We already know that (1) $\implies$ (2). We will show that (2) $\implies$ (3) and (3) $\implies$ (1), to show that the three are equivalent.

We first show that (2) $\implies$ (3). We can see that for any algebraic extension F/K, and any $\alpha \in F$, the minimal polynomial for α over K is irreducible in $K[x]$. Thus, by (2), it is separable, so our algebraic extension is separable.

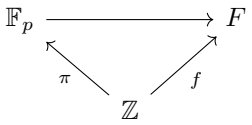
Then, we will show that (3) $\implies$ (1). Assume every algebraic extension of K is separable. If $\text{ch}(K) = 0$ then K is perfect by definition, so assume $\text{ch}(K) = p$. We need to show that the Frobenius map is surjective. That is, for every $a \in K$, we need to show that there exists $b \in K$ such that $b^p = a$. Consider the polynomial $x^p - a$. We know that this has some root $b \in \overline{K}$; we want to show that $b \in K$. Consider the minimal polynomial $f(x)$ of b over K. We know that there exists some $g(x)$ such that

$$(x^p - a) = (x - b)^p = f(x)g(x) \in \overline{K}[x].$$

But this means $f(x) = (x - b)^k \in \overline{K}[x]$, for some $k \leq p$. But we know by (3) that $K(b)$ is separable and therefore $f(x)$ is separable, which means $k = 1$, and the minimal polynomial for b over K is $x - b$, so $b \in K$. Thus, the Frobenius map is surjective, and K is perfect. □

Lecture 16: Finite Fields of Prime Power Order

Let F be a finite field, and let $p = \text{ch}(F)$. Remember that there is a natural homomorphism $f : \mathbb{Z} \to F$ determined by $f(1) = 1$. The kernel of this map is $p\mathbb{Z}$, and quotienting out this kernel gives us the injective field homomorphism $\mathbb{F}_p \to F$.



Theorem 16.1. Say that $q = p^n$, where p is a prime and $n \geq 1$. Then, there is a field F with $|F| = q$, and it is unique up to isomorphism.

We will call this field $\mathbb{F}_q$.

Proof. Let F be the splitting field of $f(x) = x^q - x$ over $\mathbb{F}_p$.

Note that $\frac{d}{dx}(f(x)) = qx^{q-1} - 1 = -1$. So it is relatively prime to $f(x)$, and $f(x)$ must therefore be a separable polynomial.

Thus, there are exactly q distinct roots of $f(x)$ in F. We will call this set of roots $R \subseteq F$, and note that $|R| = q$.

But R has all the properties of a field:

It is clear that O and 1 are both roots of $f(x)$. Moreover, for any roots a, b of $f(x)$, we know that $a^q = a$ and $b^q = b$. So $(ab)^q = a^q b^q = ab$, so this is closed under multiplication, and

$$(a+b)^q = \left((a+b)^p\right)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} = (a^{p^2} + b^{p^2})^{p^{n-2}} = \cdots = a^q + b^q = a + b,$$

so this is closed under addition. Finally, if $a^q = a$ and $a \neq 0$, we can see that

$$(a^{-1})^q = a^{-q} = (a^q)^{-1} = a^{-1},$$

so this is closed under inverses. Thus, R is a subfield of F.

But this implies that $\mathbb{F}_p \subseteq R$, since $1 \in R$ and 1 generates all of $\mathbb{F}_p$. Moreover, since R contains all roots of $f(x)$, $f(x)$ splits over R. Since $R \subseteq F$, and F is the splitting field of $f(x)$, this means that $R = F$, and we get that $|F| = |R| = q$, as we desired.

To show uniqueness, suppose F is a field $|F| = q$. Then, we can see that $F^\times$ is an abelian group, with $\left|F^\times\right| = q - 1$.

This means that for any $\alpha \in F^\times$, $\alpha^{q-1} = 1$, so for any $\alpha \in F$, $\alpha^q = \alpha$. Thus, F contains q distinct roots of the polynomial $x^q - x$, so it is the splitting field of $x^q - x$, which we know is unique up to isomorphism. □

Corollary 16.2. The field extension $\mathbb{F}_q/\mathbb{F}_p$ is normal and separable.

Proof. It is normal because we know all splitting field extensions are normal, and it is separable because $\mathbb{F}_p$ is a perfect field, so every algebraic extension is separable. □

Proposition 16.3. We can see that the algebraic closure is

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

Proof. It is sufficient to show that for any irreducible $g(x) \in \mathbb{F}_p[x]$, g splits completely in some $\mathbb{F}_{p^n}$. Let F be the splitting field of $g(x)$ over $\mathbb{F}_p$, and say $[F : \mathbb{F}_p] = n$. But then, we know that $|F| = p^n$, so F is isomorphic to $\mathbb{F}_{p^n}$, and $g(x)$ splits completely over $\mathbb{F}_{p^n}$.
Thus, for any α that is algebraic over $\mathbb{F}_p$, its minimal polynomial splits completely in some $\mathbb{F}_{p^n}$, so

$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

□

Moreover, since $\mathbb{F}_q/\mathbb{F}_p$ is normal for every q, we see that for every q, there is a unique image of $\mathbb{F}_q$ in $\overline{\mathbb{F}_p}$.

The field $\mathbb{F}_q$ that we just constructed has the property that $\mathbb{F}_q^\times$ is cyclic. To show this, we will prove a more general theorem.

Theorem 16.4. Let F be any field. Then, if $G \subseteq F^\times$ is a finite subgroup of the multiplicative group, it is cyclic.

Proof. By the fundamental theorem of finite abelian groups, we know we can express G as

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z},$$

where each d_i is greater than 1, and

$$d_1 \mid d_2 \mid \cdots \mid d_k,$$

so each d_i is a multiple of the previous ones.

Then, this implies that for any $\alpha \in G$,

$$\alpha^{d_k} = 1,$$

so G is a subset of the roots of $f(x) = x^{d_k} - 1$ in F. There are at most d_k such roots in F, so $|G| \leq d_k$.

But we know that $|G| = d_1 d_2 \cdots d_k$. So this implies that actually $k = 1$ and $G \cong \mathbb{Z}/d_1\mathbb{Z}$, so G is cyclic. □

Corollary 16.5. For all prime powers q, $\mathbb{F}_q$ is cyclic.

Proof. This follows directly from the above theorem, by taking $F = \mathbb{F}_q$ and $G = \mathbb{F}_q^\times$. □

As a reminder, a **simple extension** F/K is one in which $F = K(\alpha)$ for some $\alpha \in F$.

Corollary 16.6. $\mathbb{F}_q/\mathbb{F}_p$ is a simple extension.

Proof. We can see that since $\mathbb{F}_q^\times$ is cyclic, we can take α to be a generator of $\mathbb{F}_q^\times$, and then clearly $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. □

Corollary 16.7. For any $n \geq 1$, there is an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

This follows from the fact that $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is not a finite extension; in contrast, all irreducible polynomials over $\mathbb{R}$ have degree at most 2.

Proof. Take $q = p^n$, and consider the field extension $\mathbb{F}_q/\mathbb{F}_p$. By Corollary 16.6 we know this is a simple extension, so there exists some α so that $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. But then the minimal polynomial for α over $\mathbb{F}_p$ is an irreducible, and it has degree $[\mathbb{F}_q : \mathbb{F}_p] = n$. □

Lecture 17: The Automorphism Group of $\mathbb{F}_q/\mathbb{F}_p$

We are working with $q = p^n$, where p is prime. We showed last time that $\mathbb{F}_q/\mathbb{F}_p$ is a simple, normal, and separable extension.

What is the automorphism group $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$?

We know that it is not just $\{1\}$, because the Frobenius map

$$\begin{aligned} \varphi_F : \mathbb{F}_q &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha^p \end{aligned}$$

is a non-trivial element of the automorphism group.

Theorem 17.1. There is an isomorphism of groups $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) \to \mathbb{Z}/n\mathbb{Z}$, $\varphi_F \mapsto 1$. So $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic.

To prove this, we use the following lemma:

Lemma 17.2. If $F = K(\alpha)$, where α is algebraic over K, and F/K is normal and separable, then

$$\left|\mathrm{Aut}(F/K)\right| = [F : K].$$

Proof. Let $f(x)$ be the minimal polynomial of α over K. Then, we know there is a set bijection between $\mathrm{Aut}(F/K)$ and the roots of $f(x)$ in F. But since F/K is normal, F must contain all the roots of $f(x)$, and since F/K is separable, there are exactly $\deg f(x) = [F : K]$ distinct roots of $f(x)$.

Thus, $\left|\mathrm{Aut}(F/K)\right| = [F : K]$. □

Now that we have this lemma, we can go back to proving the main theorem.

Proof of theorem. Recall that if we take α to be a generator of $\mathbb{F}_q^\times$ (which we proved was cyclic), then $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

Moreover, we showed that since $\mathbb{F}_q/\mathbb{F}_p$ is the splitting field of $x^q - x$, it is normal, and since $\mathbb{F}_p$ is perfect, $\mathbb{F}_q$ is separable.

So we can apply the lemma to get that $\left|\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)\right| = [\mathbb{F}_q : \mathbb{F}_p] = n$.

Then, let d be the order of φ_F, as an element of this automorphism group. This means that φ_F^d is the identity, so for all $\beta \in \mathbb{F}_q$,

$$\beta = \varphi_F^d(\beta) = \beta^{p^d}.$$

So every element of $\mathbb{F}_q$ must be a root of $f(x) = x^{p^d} - x$, which means $q \le p^d$, or $n \le d$. But since d is the order of an element in the automorphism group, d must be at most n, so we get that $n = d$.

Thus, this is a cyclic group of order n that is generated by φ_F, so it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ under the isomorphism specified. □

Now, we will look at the group symmetries of a polynomial.

Remember that if we have a polynomial $f(x) \in K[x]$, and F is the splitting field of $f(x)$, then elements of $\mathrm{Aut}(F/K)$ are permutations of the roots of $f(x)$ in F. These possible permutations are what we mean by the symmetries of a polynomial.

From what we have shown earlier, if $K = \mathbb{C}$, then this group is always just $\{1\}$. If $K = \mathbb{R}$, the group is $\mathbb{Z}/n\mathbb{Z}$, where $n = [F : K]$, which is either 1 or 2, depending on whether the polynomial has imaginary roots. If $K = \mathbb{F}_p$, the group is $\mathbb{Z}/n\mathbb{Z}$, where $n = [F : K]$. In this case, n can be arbitrarily large.

Example 17.3. We know that $\mathbb{C}$ is the splitting field of $x^4 - 1$ over $\mathbb{R}$, and we can consider $\mathbb{F}_q$ to be the splitting field of $x^{q-1} - 1$ over $\mathbb{F}_p$.

Definition 17.4. The m^{th} **cyclotomic extension** of an arbitrary field K is the splitting field of $x^m - 1$ over K.

We will assume that m is not divisible by $\mathrm{ch}(K)$, since otherwise, if $\mathrm{ch}(K) = p$,

$$x^m - 1 = (x^{m/p} - 1)^p,$$

so this is just the splitting field of $x^{m/p} - 1$ (and we can repeat this process if m/p is still divisible by p).

Under this assumption, $x^m - 1$ is separable over K, since mx^{m-1} is not the zero polynomial, and the only root of mx^{m-1} is 0, so it has no roots in common with $x^m - 1$.

An easy observation is that the group of roots of $x^m - 1$ in $\overline{K}$ is a subgroup of $(\overline{K})^\times$. We will call this subgroup $\mu[m]$, since it has m elements. Moreover, by Theorem 16.4, we know that $\mu[m]$ is cyclic, so $\mu[m] \cong \mathbb{Z}/m\mathbb{Z}$.

Definition 17.5. A **primitive** m^{th} root of unity in $\overline{K}$ is a generator of $\mu[m]$.

For primitive roots of unity $\alpha \in \mu[m]$, we have the isomorphism $\mu[m] \to \mathbb{Z}/m\mathbb{Z}$ defined by $\alpha^i \mapsto i$.

Corollary 17.6. The splitting field of $x^m - 1$ over K is $K(\alpha)$, where α is any primitive m^{th} root of unity.

How many primitive m^{th} roots of unity are there in $\overline{K}$?

We know that $\mu[m] \cong \mathbb{Z}/m\mathbb{Z}$, so the question becomes: how many generators are there in $\mathbb{Z}/m\mathbb{Z}$?

An element $x \in \mathbb{Z}/m\mathbb{Z}$ is a generator if and only if x is relatively prime to m. Thus, the number of primitive m^{th} roots of unity is $\left|(\mathbb{Z}/m\mathbb{Z})^\times\right| = \varphi(m)$.

Theorem 17.7. Let K be any field, and let $F = K(\alpha)$, where α is a primitive m^{th} root of unity. Then, there is an injective group homomorphism $\mathrm{Aut}(F/K) \to (\mathbb{Z}/m\mathbb{Z})^\times$, where if $\varphi(\alpha) = \alpha^\ell$, then the homomorphism is $\varphi \mapsto \ell$.

Proof. For an automorphism $\varphi \in \mathrm{Aut}(F/K)$, what elements can $\varphi(\alpha)$ be?

We know that φ must map α to a different primitive root of unity, so if $\varphi(\alpha) = \alpha^\ell$, then $\ell \in (\mathbb{Z}/m\mathbb{Z})^\times$, as we wanted.

Since our automorphisms are determined by where they map α, this is an injective map. Moreover, we can see that if $\varphi_1(\alpha) = \alpha^{\ell_1}$ and $\varphi_2(\alpha) = \alpha^{\ell_2}$, then

$$\varphi_1\varphi_2(\alpha) = \alpha^{\ell_1\ell_2},$$

so this is a group homomorphism. □

Thus, $\mathrm{Aut}(F/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$, which means it is abelian.

The main question is: when is the map defined in the theorem an isomorphism?

Lecture 18: Cyclotomic Extensions

Let K be a field. Remember that we are looking at cyclotomic extensions of K; that is, we are looking at K adjoined with the m^{th} roots of unity.

As before, let $\mu[m]$ be the group of m^{th} roots of unity; this is a subgroup of $(\overline{K})^\times$. Let α be a primitive root of unity, so that $K(\mu[m]) = K(\alpha)$.

We left off last lecture by showing that there is an injective group homomorphism

$$\text{Aut}(K(\alpha)/K) \to (\mathbb{Z}/m\mathbb{Z})^\times.$$

When is this an isomorphism?

This happens if and only if $[K(\alpha) : K] = \varphi(m)$.

Example 18.1. Consider $\mathbb{C} = \mathbb{R}(\mu[m])$ for any $m \geq 3$. We know that the automorphism group $\text{Aut}(\mathbb{C}/\mathbb{R})$ has two elements; the identity, and complex conjugation. Then, we have that the image of our identity under our map $\text{Aut}(\mathbb{C}/\mathbb{R}) \to (\mathbb{Z}/m\mathbb{Z})^\times$ that we defined earlier is 1, and the image of complex conjugation is -1 (since for a root of unity, its inverse is its complex conjugate).

This is not an isomorphism for $m > 3$.

Example 18.2. Consider $\mathbb{F}_8 = \mathbb{F}_2(\mu[7])$.

In this case, our injective group homomorphism $\text{Aut}(\mathbb{F}_8/\mathbb{F}_2) \to (\mathbb{Z}/7\mathbb{Z})^\times$ is not an isomorphism. We can see that $\varphi_F : x \mapsto x^2$ has order 3; if α is a primitive root of $x^7 - 1$ then

$$\begin{aligned} \varphi_F^1(\alpha) &= \alpha^2, & \varphi_F^1 &\mapsto 2 \\ \varphi_F^2(\alpha) &= \alpha^4, & \varphi_F^2 &\mapsto 4 \\ \varphi_F^3(\alpha) &= \alpha^8 = \alpha, & \varphi_F^3 &\mapsto 1, \end{aligned}$$

and these are the three elements of $\text{Aut}(\mathbb{F}_8/\mathbb{F}_2)$.

In general, since $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(x^{p^n-1}-1)$, we get that our injective group homomorphism $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \to (\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ is defined by $\varphi_F \mapsto p$, and therefore this is not an isomorphism.

We will now look at one example where this *is* an isomorphism:

Example 18.3. Remember that the splitting field of $x^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$ where $\alpha = e^{i\pi/4}$. This implies that α is a primitive 8^{th} root of unity, and we can see that the automorphisms of $\mathbb{Q}(\alpha)/\mathbb{Q}$ are:

$$\begin{aligned} 1 &: \alpha \mapsto \alpha \\ \varphi_3 &: \alpha \mapsto \alpha^3 \\ \varphi_5 &: \alpha \mapsto \alpha^5 \\ \varphi_7 &: \alpha \mapsto \alpha^7, \end{aligned}$$

since they must all be permutations of the roots of $x^4 + 1$. Moreover, we can see that each map squared is the identity, so

$$\text{Aut}(\mathbb{Q}(\mu[8])/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

But $\left|(\mathbb{Z}/8\mathbb{Z})^\times\right| = 4$ as well, so in this case,

$$\mathrm{Aut}(\mathbb{Q}(\mu[8])/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$$

and the injective group homomorphism is actually an isomorphism.

Theorem 18.4. For any m,

$$\mathrm{Aut}(\mathbb{Q}(\mu[m])/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

In other words, the degree $[\mathbb{Q}(\mu[m]) : \mathbb{Q}]$ is $\varphi(m)$.

Proof. Let α be a primitive m^{th} root of unity in $\overline{\mathbb{Q}}$ and let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. We know that $f(x) \neq x^m - 1$, since $x^m - 1$ is not irreducible over $\mathbb{Q}$. Thus,

$$x^m - 1 = f(x)h(x) \in \mathbb{Q}[x],$$

for some $h(x)$. Moreover, by Gauss's lemma, this means we can factor $x^m - 1$ in the same way in $\mathbb{Z}[x]$. Then, we need the following claim:

Claim. For any prime p not dividing m, α^p is a root of $f(x)$. In other words, α and α^p are conjugates over $\mathbb{Q}$.

To prove the claim, suppose α^p is not a root of $f(x)$. Then, α^p is still an m^{th} root of unity, so it must be a root of $h(x)$. But this means α is a root of $h(x^p)$. But then $h(x^p) = f(x)g(x) \in \mathbb{Q}[x]$, for some $g(x) \in \mathbb{Q}[x]$. By Gauss's Lemma, this means that $h(x^p) = f(x)g(x) \in \mathbb{Z}[x]$ as well.

Then, since we are working with polynomials with integer coefficients, we can consider $\tilde{f}(x), \tilde{g}(x)$, and $\tilde{h}(x)$ to be the images of $f(x), g(x)$, and $h(x)$, respectively, in $\mathbb{F}_p[x]$. But in $\mathbb{F}_p[x]$,

$$\tilde{h}(x^p) = (\tilde{h}(x))^p,$$

so $(\tilde{h}(x))^p$ is a multiple of $\tilde{f}(x)$, and $\tilde{h}$ and $\tilde{f}$ are *not* relatively prime in this field.

But

$$x^m - 1 = \tilde{f}(x)\tilde{h}(x),$$

so $x^m - 1$ has a multiple root in $\overline{\mathbb{F}_p}$. But we know that since $\mathbb{F}_p$ is perfect and $(m, p) = 1$, $x^m - 1$ is separable over $\mathbb{F}_p$. This is a contradiction, and so α^p must be a root of $f(x)$.

Now that we have this claim, note that for any ℓ relatively prime to m, α^ℓ must be a root of $f(x)$, since we can write ℓ as the product of primes relatively prime to m, and then inductively imply the claim.

Thus, $f(x)$ has at least $\varphi(m)$ distinct roots, and then by Theorem 6.2, we get that $\left|\mathrm{Aut}(\mathbb{Q}(\mu[m])/\mathbb{Q})\right| \geq \varphi(m)$. But since we know there is an injective group homomorphism $\left|\mathrm{Aut}(\mathbb{Q}(\mu[m])/\mathbb{Q})\right| \to (\mathbb{Z}/m\mathbb{Z})^\times$, the size of this automorphism group must at most $\varphi(m)$, and therefore this homomorphism is actually an isomorphism. □

We can see that the above theorem actually holds for any field K that is the field of fractions for a UFD R; we replace $\mathbb{Z}[x]$ with $R[x]$ and then prove our claim in $R/(p)$, where p is actually the image of p in the homomorphism $\mathbb{Z} \to R$.

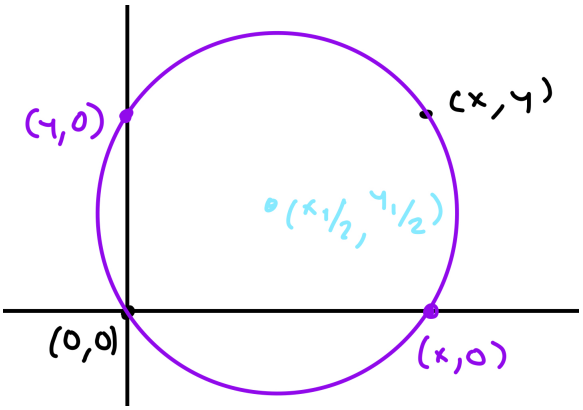
Lecture 19: Fermat Primes and Constructibility II

We now have the tools to return to the question: which regular n-gons are constructible using a straightedge and compass?

In an earlier lecture, we said that we can construct $\triangle$, $\square$, $\pentagon$, and $\hexagon$.

We can also construct octagons, since we know how to bisect an angle. We cannot construct a 9-gon, since we cannot trisect an angle, and we can also construct a 10-gon, 12-gon, 15-gon (shown by Euclid), 16-gon, and 17-gon (shown by Gauss).

Note that if a point (x, y) is constructible, then both x and y are constructible, since we have:



where we can first find the midpoint in blue, and then use that to draw the circle in purple. From Theorem 8.3 this means that x and y are both algebraic over $\mathbb{Q}$, and $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

Theorem 19.1. If a regular n-gon is constructible, then $\varphi(n)$ is a power of 2.

We will see later using Galois theory that the converse of this also holds.

Proof. Recall that if $(x, y) \in \mathbb{R}^2$ is constructible, then $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^\ell$ for some integer $\ell > 0$.

Then, consider a primitive n^{th} root of unity $\zeta_n \in \mathbb{C}$. We know that the image of ζ_n under the map $\mathbb{C} \to \mathbb{R}^2$, $x + iy \mapsto (x, y)$ is a point on our regular n-gon, so it must be constructible.

But then, if $\zeta_n = x + iy$, we get that

$$[\mathbb{Q}(x, y, i) : \mathbb{Q}] = [\mathbb{Q}(x, y, i) : \mathbb{Q}(x, y)][\mathbb{Q}(x, y) : \mathbb{Q}] = 2^{\ell+1}.$$

Since $\zeta_n \in \mathbb{Q}(x, y, i)$, we can see that

$$2^{\ell+1} = [\mathbb{Q}(x, y, i) : \mathbb{Q}] = [\mathbb{Q}(x, y, i) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}],$$

so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^k$ for some $k \leq n$.

Since by Theorem 18.4, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, we get that $\varphi(n) = 2^k$, as we wanted. □

Consider the case where we are trying to construct a p-gon, for some prime p. This theorem is saying that if a regular p-gon is constructible, then $\varphi(p) = p - 1 = 2^k$ for some integer $k \geq 0$.

Definition 19.2. A **Fermat prime** is a prime of the form $2^k + 1$.

Proposition 19.3. If p is a Fermat prime, then $p = 2^{2^\ell} + 1$ for some integer $\ell \geq 0$.

Proof. Assume p is a Fermat prime, so it is of the form $2^k + 1$, but k is not a power of 2. Then, we can write $k = 2^a b$, where $a \geq 0$ and $b > 1$ is odd.

But then, we can see that $2^{2^a} + 1$ is a factor of $2^k + 1$ (This is because $x + 1$ is a factor of $x^b + 1$ when b is odd, and we can write $2^k + 1$ as $\left(2^{2^a}\right)^b + 1$...), which contradicts the fact that $2^k + 1$ is prime.

Thus, all Fermat primes are of the form $2^{2^\ell} + 1$. □

We can consider some examples of numbers of the form $2^{2^\ell} + 1$:

$$2^{2^0} + 1 = 3$$
$$2^{2^1} + 1 = 5$$
$$2^{2^2} + 1 = 17$$
$$2^{2^3} + 1 = 257$$
$$2^{2^4} + 1 = 65537$$
$$2^{2^5} + 1 = 4294967297 = 641 * 6700417,$$

so not all numbers of this form are prime. In fact, the first five terms listed here are the only known Fermat primes, and we are not sure if any more Fermat primes exist.

Definition 19.4. The m^{th} **cyclotomic polynomial**, denoted $\Phi_m(x)$, is the minimal polynomial of a primitive m^{th} root of unity over $\mathbb{Q}$.

The degree of the m^{th} cyclotomic polynomial is $\varphi(m)$.

We can also see that for any m,

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{\substack{n|m \\ n<m}} \Phi_n(x)},$$

since any $y \in \mu[m]$ is a primitive d^{th} root of unity for some $d \mid m$; specifically, it is a primitive d^{th} root of unity, where d is the order of y in the group $\mu[m]$.

By manually computing, it has been shown that all nonzero coefficients of $\Phi_m(x)$ are ± 1, for $m < 105$. But $\Phi_{105}(x)$ has some coefficients that are ± 2, and in general we conjecture that the value of the coefficients is bounded based on the number of distinct odd prime divisors of m.

Lecture 20: The Separable Degree of a Field Extension

Recall that a field extension F/K is separable if every $\alpha \in F$ is separable over K (the minimal polynomial for α over K has no multiple roots in $\overline{K}$). We showed in Corollary 14.6 and in Theorem 15.5 that if K is finite or $\text{ch}(K)$ is 0, then F/K is separable.

Also, remember that a field extension F/K is normal if for every $\alpha \in F$, the minimal polynomial for α over K splits completely in $F[x]$. We showed in Theorem 13.7 some properties that are equivalent to a field extension being normal.

We will now show some inequalities in category theory.

Theorem 20.1. For any finite extension F/K,

$$\left|\text{Aut}(F/K)\right| \leq \left|\text{Hom}(F/K, \overline{K}/K)\right|,$$

with equality if and only if F/K is normal.

Proof. Let G be the group $\text{Aut}(F/K)$ and let X be the set $\text{Hom}(F/K, \overline{K}/K)$. Then, there is a G-action on X, where for all $\varphi : F/K \to F/K$ and $\psi : F/K \to \overline{K}/K$,

$$\varphi \cdot \psi = \psi \circ \varphi,$$

which is the map

$$F/K \xrightarrow{\quad\varphi\quad} F/K \xrightarrow{\quad\psi\quad} \overline{K}/K$$

This is true for all categories.

Remember that a free action is one in which $g \cdot x = x$ if and only if $g = 1$. But we can see that in this case, since $\psi \in X$ is a field homomorphism, it is injective, so for any $a \in F$

$$\psi(\varphi(a)) = \psi(a)$$

if and only if $\varphi(a) = a$. Thus, $\varphi \cdot \psi = \psi \circ \varphi = \psi$ only when φ is the identity, and this a free action.

Then, we know that since we have a G-action on X, X must be the disjoint union of G-orbits. Then, the orbit-stabilizer theorem tells us that the size of the orbit of $x \in X$ is $|G|$ divided by the size of the stabilizer of x. But since this is a free group, we get that the stabilizer of x is just the identity, and therefore the size of the orbit of x is just $|G|$.

Since the size of an orbit is at most $|X|$, we get $|G| \leq |X|$, or

$$\left|\text{Aut}(F/K)\right| \leq \left|\text{Hom}(F/K, \overline{K}/K)\right|,$$

as we desired.

Then, equality holds if and only if there is exactly one orbit under this group action.

Claim. Two homomorphisms $\psi_1, \psi_2 \in X$ are in the same G-orbit if and only if $\psi_1(F) = \psi_2(F)$.

The only if part is clear, because for any $\varphi \in G$, φ is an automorphism, so $\varphi \cdot \psi_1(F) = \psi_1(F)$, and if $\psi_1(F) \neq \psi_2(F)$ then clearly $\varphi \cdot \psi_1 \neq \psi_2$.

For the other direction, suppose $\psi_1(F) = \psi_2(F) = F' \subseteq \overline{K}$. By the first isomorphism theorem, $\psi_2 : F \to F'$ is an isomorphism over K, so it has an inverse ψ_2^{-1} which is also an isomorphism. Similarly, $\psi_1 : F \to F'$ is an isomorphism, so $\psi_2^{-1} \circ \psi_1 : F \to F$ is an isomorphism, and the diagram

$$F/K \xrightarrow{\psi_2^{-1}\circ\psi_1} F/K \xrightarrow{\psi_2} \overline{K}/K, \qquad F/K \xrightarrow[\psi_1]{} \overline{K}/K$$

commutes. Thus, $\psi_2^{-1} \circ \psi_1$ is an element of $\mathrm{Aut}(F/K)$ and sends ψ_2 to ψ_1.

So our claim is true, and we have that

$$\left|\mathrm{Aut}(F/K)\right| = \left|\mathrm{Hom}(F/K, \overline{K}/K)\right|$$

if and only if there is some $F' \subseteq \overline{K}$ such that $\psi(F) = F'$ for all $\psi \in \mathrm{Hom}(F/K, \overline{K}/K)$. But by Theorem 13.7, this is true if and only if F/K is normal. □

Let's take a closer look at $\mathrm{Hom}(F/K, \overline{K}/K)$.

Definition 20.2. The size of $\mathrm{Hom}(F/K, \overline{K}/K)$, or $\left|\mathrm{Hom}(F/K, \overline{K}/K)\right|$ is called the **separable degree** of F over K.

Theorem 20.3. The separable degree is multiplicative; that is, for any chain of field extensions $K \subseteq E \subseteq F$,

$$\left|\mathrm{Hom}(F/K, \overline{K}/K)\right| = \left|\mathrm{Hom}(E/K, \overline{K}/K)\right|\left|\mathrm{Hom}(F/E, \overline{E}/E)\right|.$$

Proof. There is a map between sets, called the restriction map

$$r : \mathrm{Hom}(F/K, \overline{K}/K) \to \mathrm{Hom}(E/K, \overline{K}/K)$$

defined by

$$\left(F/K \xrightarrow{\varphi} \overline{K}/K\right) \longmapsto \left(E/K \xrightarrow[\text{inclusion}]{} F/K \xrightarrow{\varphi} \overline{K}/K\right)$$

Then, we can see that for any $\psi : E/K \to \overline{K}/K$, the preimage $r^{-1}(\psi)$ is the set of all $\varphi : F/K \to \overline{K}/K$ that restrict to ψ on E. But since $\overline{K} = \overline{E}$, we get that

$$r^{-1}(\psi) \cong \mathrm{Hom}(F/E, \overline{E}/E).$$

Thus, the size of the domain is the number of options for ψ, times the size of $r^{-1}(\psi)$, and therefore

$$\left|\mathrm{Hom}(F/K, \overline{K}/K)\right| = \left|\mathrm{Hom}(F/E, \overline{E}/E)\right|\left|\mathrm{Hom}(E/K, \overline{K}/K)\right|.$$

□

Theorem 20.4. For any finite field extension F/K,

$$\left|\mathrm{Hom}(F/K, \overline{K}/K)\right| \leq [F : K],$$

with equality if and only if F/K is separable.

Proof. We will show this via induction on the degree $[F : K]$.

First, for the base case, if $[F:K]=1$, then $F=K$ and the only homomorphism that fixes K is the identity, so $\left|\mathrm{Hom}(F/K,\overline{K}/K)\right|=[F:K]=1$.

For the inductive case, assume the statement is true for all extensions of degree at most k; we will prove it for $[F:K]=k+1$. Choose some field extension $K\subsetneq E=K(\alpha)\subseteq F$, and let $f(x)$ be the minimal polynomial of α over K. Remember from the previous theorem that

$$\left|\mathrm{Hom}(F/K,\overline{K}/K)\right|=\left|\mathrm{Hom}(F/E,\overline{E}/E)\right|\left|\mathrm{Hom}(E/K,\overline{K}/K)\right|.$$

Then, we know that by the inductive assumption, $\left|\mathrm{Hom}(F/E,\overline{E}/E)\right|\leq[F:E]$ and by Theorem 6.2, $\left|\mathrm{Hom}(E/K,\overline{K}/K)\right|$ is the number of distinct roots of $f(x)$ in $\overline{K}$, so it is at most $[E:K]$. Thus, we get that

$$\left|\mathrm{Hom}(F/K,\overline{K}/K)\right|\leq[F:E][E:K]\leq[F:K].$$

Specifically, we can see that if F is separable over K, then it is separable over E, and by the inductive assumption, $\left|\mathrm{Hom}(F/E,\overline{E}/E)\right|=[F:E]$. Moreover, $f(x)$ is separable, so the number of distinct roots of $f(x)$ in $\overline{K}$ is exactly $[E:K]$, and we get

$$\left|\mathrm{Hom}(F/K,\overline{K}/K)\right|=[F:K].$$

If F is not separable over K, then either F is not separable over E and by the inductive assumption, $\left|\mathrm{Hom}(F/E,\overline{E}/E)\right|<[F:E]$, or $f(x)$ is not separable and the number of distinct roots of $f(x)$ in $\overline{K}$ is strictly less than $[E:K]$ (or both). Thus, in this case,

$$\left|\mathrm{Hom}(F/K,\overline{K}/K)\right|<[F:K].$$

Thus, by induction, the theorem statement holds. □

Corollary 20.5. A field extension $K(\alpha)/K$ is separable if and only if α is separable over K. More generally, $K(\alpha_1,\ldots,\alpha_n)/K$ is separable if and only if $\alpha_1,\ldots,\alpha_n$ are separable over K.

Proof. The "only if" direction is clear.

For the other direction, note that if α is separable then the homomorphisms in $\mathrm{Hom}(K(\alpha)/K,\overline{K}/K)$ are determined by where we map α to in $\overline{K}$, so $\left|\mathrm{Hom}(K(\alpha)/K,\overline{K}/K)\right|$ is the number of distinct roots of $f(x)$ in $\overline{K}$, which we know by separability is $[K(\alpha):K]$. But then,

$$\left|\mathrm{Hom}(K(\alpha)/K,\overline{K}/K)\right|=[K(\alpha):K],$$

so by the theorem above, $K(\alpha)$ is separable.

For the $K(\alpha_1,\ldots,\alpha_n)$ case, repeat the above step inductively. □

Corollary 20.6. For any finite F/K,

$$\left|\mathrm{Aut}(F/K)\right|\leq[F:K],$$

with equality if and only F/K is normal and separable.

Proof. This follows from combining the above two theorem statements. □

The inequalities we proved above are pretty hefty. For some intuition about them, recall that in Theorem 6.2 we showed that if $f(x)$ is the minimal polynomial for α over K, $\left|\mathrm{Aut}(K(\alpha)/K)\right|$ is the number of distinct roots of $f(x)$ in $K(\alpha)$. This gives one special case of the above corollary, because we can see that if $f(x)$ is separable and splits completely in $K(\alpha)$, then clearly

$$\left|\mathrm{Aut}(K(\alpha)/K)\right| = [K(\alpha) : K],$$

and otherwise there are some roots of $f(x)$ that are either duplicates or don't appear in $K(\alpha)$, so

$$\left|\mathrm{Aut}(K(\alpha)/K)\right| < [K(\alpha) : K].$$

Definition 20.7. A finite extension F/K is called a **Galois extension** if F/K is normal and separable.

Example 20.8. If K is a finite field, or if it has characteristic 0, then it is perfect. Thus, by Proposition 15.9, for any $f(x) \in K[x]$, the splitting field F of $f(x)$ is normal and separable over K, so F/K is Galois.

Similarly, for any F/K where F is finite, then F is separable since K must be finite and therefore perfect, and it is normal because it is the splitting field of $x^{|F|} - x$ over $\mathbb{F}_p \subseteq K$, where $p = \mathrm{ch}(K)$.

Lecture 21: Simple Extensions

Last lecture, we showed that

$$\left|\mathrm{Aut}(F/K)\right| \leq \left|\mathrm{Hom}(F/K, \overline{K}/K)\right| \leq [F:K],$$

with the first $\leq$ being an equality if and only if F/K is a normal extension, and the second $\leq$ being an equality if and only if F/K is a simple extension.

Definition 21.1. A field extension F/K is **simple** if $F = K(\alpha)$ for some $\alpha \in F$.

From our construction of $K(\alpha)$, the simple fields are all the ones of the form $K[x]/(f(x))$ for irreducible $f(x) \in K[x]$.

It is not always obvious which extensions are simple.

Example 21.2. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension of $\mathbb{Q}$, because $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Clearly, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, we can also see that

$$\sqrt{2} = (\sqrt{2} + \sqrt{3})^3 + \frac{1}{\sqrt{2} + \sqrt{3}} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

and then we can express $\sqrt{3}$ as $\left(\sqrt{2} + \sqrt{3}\right) - \sqrt{2}$, so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

So how would we prove that an extension is *not* simple?

Theorem 21.3. An algebraic extension F/K is simple if and only if the number of fields E satisfying $K \subseteq E \subseteq F$ is finite.

Proof. If F/K is simple, we can write $F = K(\alpha)$ for some α. Then, consider any $K \subseteq E \subseteq F$. If $f(x)$ is the minimal polynomial of α over K, let $f_E(x)$ be the minimal polynomial of α over E.

Claim. If

$$f_E = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n,$$

where $c_0, \ldots, c_{n-1} \in E$, then $E = K(c_0, \ldots, c_{n-1})$.

First, we can see that $K(c_0, \ldots, c_{n-1}) \subseteq E$, since each of these coefficients is an element of E by definition. Then, we can see that $f_E(x)$ is irreducible over $K(c_0, \ldots, c_{n-1})$ since it is a subset of E and $f_E(x)$ is irreducible over E. Moreover, since $F = K(\alpha)$ and $E \subseteq F$, we get that

$$F = E(\alpha), \qquad F = K(c_0, \ldots, c_{n-1})(\alpha).$$

But then f_E is the minimal polynomial for α over both, so $[F : K(c_0, \ldots, c_{n-1})] = [F : E] = \deg(f_E)$. But since

$$[F : K(c_0, \ldots, c_{n-1})] = [F : E][E : K(c_0, \ldots, c_{n-1})],$$

we get that $[E : K(c_0, \ldots, c_{n-1})] = 1$, and $E = K(c_0, \ldots, c_{n-1})$.

So we have proved our claim. This implies that the map

$$E \mapsto f_E(x)$$

is injective. The domain of this map is the set of intermediate fields. But we also have that $f_E(x) \mid f(x)$, so the number of intermediate fields E is at most the number of factors of $f(x)$ in $\overline{K}[x]$, which is finite.

To prove the other direction, suppose that the set $S = \{E \mid K \subseteq E \subseteq F\}$ is finite. First, this means that F/K is finitely generated; otherwise we have the infinite chain

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F,$$

where $\alpha_i \in F \setminus K(\alpha_1, \ldots, \alpha_{i-1})$ for $i \geq 1$. But then, each one of the fields in our chain is an element of S, so S is infinite, which is a contradiction.

Since F/K is a finitely generated algebraic extension, we can see that $[F : K]$ is finite, and therefore if K is finite, F must also be finite. But this means $F^\times$ is cyclic (since every finite field is isomorphic to some $\mathbb{F}_q$), so we can pick a generator $\alpha \in F^\times$, and then $F = K(\alpha)$.
We are left with the case where K is infinite and $F = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in F$. It is enough to prove that in this case $K(\alpha_1, \alpha_2)$ is simple, as then we can express this as $K(\alpha_1')$, and use the same logic to argue that $K(\alpha_1', \alpha_3)$ is simple, and continue on inductively to see that $F = K(\alpha_1, \ldots, \alpha_n)$ is simple.

For each $c \in K$, consider the field $E = K(c\alpha_1 + \alpha_2) \in S$. Since K is infinite, there are infinitely many c's, but since S is finite, there are only finitely many distinct E's, so there must be some $c_1 \neq c_2 \in K$ such that

$$K(c_1\alpha_1 + \alpha_2) = K(c_2\alpha_1 + \alpha_2).$$

But then we can see that $\alpha_1 \in K(c_1\alpha_1 + \alpha_2)$ since

$$\alpha_1 = \frac{(c_1\alpha_1 + \alpha_2) - (c_2\alpha_1 + \alpha_2)}{c_1 - c_2}.$$

From there, we can see that $\alpha_2 \in K(c_1\alpha_1 + \alpha_2)$, since

$$\alpha_2 = (c_1\alpha_1 + c_2) - c_1\alpha_1.$$

Moreover, it is clear that $c_1\alpha_1 + \alpha_2 \in K(\alpha_1, \alpha_2)$, so

$$K(\alpha_1, \alpha_2) = K(c_1\alpha_1 + \alpha_2).$$

Thus, $K(\alpha_1, \alpha_2)$ is simple, and repeating this step inductively, we can conclude that $F = K(\alpha_1, \ldots, \alpha_n)$ is simple.
So, when there are finitely many field extensions E such that $K \subseteq E \subseteq F$, F/K must be simple. □

This is a nice characterization of simple fields, but it is not widely applicable. Next lecture, we will prove a more applicable theorem.

Lecture 22: The Primitive Element Theorem and Fixed Fields

Theorem 22.1 (Primitive Element Theorem)**.** If F/K is finite and separable, then it is simple.

Note that this is not an "if and only if" because there are simple extensions that are not separable; see Example 14.7 for an example of this.

Proof. Remember that if F is finite, then it is a simple extension of K because $F^\times$ is cyclic, so $F = K(\alpha)$, where α is a generator of $F^\times$.

We consider the case where F, and therefore K, is infinite. Let $n = [F : K]$, since we know it is finite. Since F/K is separable, we know that

$$\left|\mathrm{Hom}(F/K, \overline{K}/K)\right| = n.$$

Let $\{\sigma_1, \ldots, \sigma_n\}$ be the elements of $\mathrm{Hom}(F/K, \overline{K}/K)$.

Then, since $[F : K] = n$, we know that $F \cong K^n$ as a vector space over K. Moreover, each σ_i is a K-linear function on F.

For each $1 \leq i < j \leq n$, set

$$S_{i,j} = \left\{\eta \in F \;\middle|\; \sigma_i(\eta) = \sigma_j(\eta)\right\}.$$

This is a proper subspace of F since $\sigma_i \neq \sigma_j$.

Then, pick any $\alpha \in F \setminus \bigcup_{i<j} S_{i,j}$. We can do this because if you have an n-dimensional space and m k-dimensional subspaces (where $k < n$), then there must exist an element α not in any of the subspaces.

But this means that $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are all distinct.

Remember that if $f(x)$ is the minimal polynomial of α over K, then since σ_i maps roots to roots, $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are all roots of $f(x)$.

Thus, the minimal polynomial of α over K has degree at least n. So we have that $K(\alpha) \subseteq F$ and $[K(\alpha) : K] = n$, so $F = K(\alpha)$, and F must be simple. □

The following corollary directly follows from the fact that all finite extensions of perfect fields are separable.

Corollary 22.2. Any finite extension F/K is simple if $\mathrm{ch}(K) = 0$, or, more generally if K is perfect.

Remember that F/K is a Galois extension if it is normal and separable.

If we are given K, how do we construct a Galois extension F/K?

We can just take the splitting field of a separable polynomial in $K[x]$.

If we are given F, how do we construct a Galois extension F/K?

Definition 22.3. Let F be a field and let G be a subgroup of $\mathrm{Aut}(F)$ (note that this is $\mathrm{Aut}(F)$ and not

$\mathrm{Aut}(F/K)$ because K isn't defined yet). Then, the **fixed field** of F in G is the subset

$$F^G = \left\{\alpha \in F \;\middle|\; \sigma(\alpha) = \alpha \text{ for all } \alpha \in G\right\}.$$

Proposition 22.4. F^G is a subfield of F.

Proof. We can see that $1 \in F^G$ because for all $\sigma \in G$, $\sigma(1) = 1$.

For all $\alpha, \beta \in F^G$, $\alpha + \beta, \alpha\beta \in F^G$ because

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$$

and

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$$

for all $\sigma \in G$.

Finally, if $\alpha \neq 0 \in F^G$ then $\alpha^{-1} \in F^G$ because

$$\sigma(\alpha^{-1}) = (\sigma(\alpha))^{-1} = \alpha^{-1}$$

for all $\sigma \in G$. □

Note that our proof holds for any G that is a sub*set* of $\mathrm{Aut}(F)$, not just a subgroup.

Theorem 22.5. For any finite subgroup $G \subseteq \mathrm{Aut}(F)$, $[F : F^G] = |G|$.

Proof. Let $K = F^G$ and $n = |G|$. Then, for nay $\alpha \in F$, consider its G-orbit as G acts on F:

$$G \cdot \alpha = \left\{\sigma(\alpha) \;\middle|\; \sigma \in G\right\}.$$

Then, let $|G \cdot \alpha| = m$. We know that this is finite, since

$$G \cdot \alpha \subseteq G \subseteq \mathrm{Aut}(F/K),$$

and applying Corollary 20.6, we get that

$$|G \cdot \alpha| \leq \left|\mathrm{Aut}(F/K)\right| \leq [F : K]$$

which is a finite extension.

Then, $m \leq n$ and $G \cdot \alpha = \left\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\right\}$. Consider the polynomial

$$f(x) = \prod_{i=1}^{m} (x - \sigma_i(\alpha)) \in F[x].$$

We can see that for any $\sigma \in G$,

$$\left\{\sigma \circ \sigma_1(\alpha), \ldots, \sigma \cdot \sigma_m(\alpha)\right\} = G \cdot \alpha,$$

since applying a group action should just permute the elements of the orbit. But this means that applying σ to the coefficients does not change $f(x)$, for any $\sigma \in G$, so $f(x) \in K[x]$.

Then, $f(x)$ is the minimal polynomial of α over K, since all $\sigma_i(\alpha)$ would have the same minimal polynomial. This means that α is separable over K and $[K(\alpha) : K] = m$.

Since α was arbitrary, the entire extension F/K is separable. Then, since F/K is finite and separable, the Primitive Element Theorem tells us that $F = K(\beta)$ for some $\beta \in F$. But then, we get the chain of inequalities

$$|G| \leq \left|\mathrm{Aut}(F/K)\right| \leq [F : K] = [K(\beta) : K] = |G \cdot \beta| \leq |G|.$$

So all of these inequalities are actually equalities, and $[F : K] = |G|$. □

Corollary 22.6. The extension F/F^G is a Galois extension and $G = \mathrm{Aut}(F/F^G)$.

Proof. We showed in the proof of the theorem that F/F^G is separable. To see that it is normal, note that when we showed the last chain of inequalities was actually an equality, we showed that

$$\left|\mathrm{Aut}(F/K)\right| = [F : K]$$

which by Corollary 20.6 means that F/K is a normal extension. Moreover, we just proved that $|G| = [F : K]$, which, combined with the above equation, means that

$$\left|\mathrm{Aut}(F/K)\right| = |G| .$$

But since $G \subseteq \mathrm{Aut}(F/K)$, and both are finite groups, the two must be equal. □

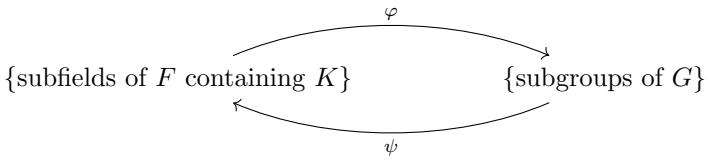
Lecture 23: The Fundamental Theorem of Galois Theory

Let $K \subseteq F$ be a finite field extension. Then,

$$\mathrm{Aut}(F/K) = \left\{\sigma \in \mathrm{Aut}(F) \;\middle|\; \sigma(a) = a \text{ for all } a \in K\right\}$$

is a subgroup of $\mathrm{Aut}(F)$.

Definition 23.1 (Galois correspondence)**.** For any $K \subseteq F$ and $G = \mathrm{Aut}(F/K)$, the functions φ and ψ are defined as follows



where $\varphi(E) = \mathrm{Aut}(F/E) \subseteq G$ and $\psi(H) = F^H$. Note that since $H \subseteq G = \mathrm{Aut}(F/K)$, $K \subseteq \psi(H)$.

Note that if $K \subseteq E_1 \subseteq E_2 \subseteq F$ then $\varphi(E_2) \subseteq \varphi(E_1)$, because if our homomorphism fixes E_2, then it fixes E_1.

Moreover, if $H_1 \subseteq H_2 \subseteq G$ then $\psi(H_2) \subseteq \psi(H_1)$ because everything fixed by all of H_2 is also fixed by H_1.

So, φ and ψ are inclusion-reversing.

Also, for any subgroup $H \subseteq G$, Theorem 22.5 tells us that $[F : \psi(H)] = |H|$.

Proposition 23.2. For any $H \subseteq G$, $\varphi \circ \psi(H) = H$.

Proof. We know that $\psi(H) = F^H$, so $\varphi \circ \psi(H) = \mathrm{Aut}(F/F^H)$. We know that any $h \in H$ fixes any $\alpha \in F^H$, so $H \subseteq \mathrm{Aut}(F/F^H)$. But by Theorem 22.5,

$$|H| \leq \left|\mathrm{Aut}(F/F^H)\right| \leq [F : F^H] = |H|,$$

so these are all equalities and $H = \mathrm{Aut}(F/F^F)$.

Thus, $\varphi \circ \psi(H) = H$. □

Corollary 23.3. φ is surjective and ψ is injective. Thus, the size of the set of intermediate fields of $K \subseteq F$ must be at least the size of the set of subgroups of G.

Let us look at some examples of these maps, on various field extensions.

Example 23.4. Consider the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, which is separable but not normal. Remember that $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$, so that all elements of this group fix all of $\mathbb{Q}(\sqrt[3]{2})$. Thus,

$$\begin{aligned}\varphi(\mathbb{Q}(\sqrt[3]{2})) &= \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \\ \varphi(\mathbb{Q}) &= \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \\ \psi(\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) &= \mathbb{Q}(\sqrt[3]{2}),\end{aligned}$$

Example 23.5. Consider the field extension $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$, which is normal but not separable. Again, the only element of $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p))$ is the identity, so we get that

$$\begin{aligned}\varphi(\mathbb{F}_p(x)) &= 1\\ \varphi(\mathbb{F}_p(x^p)) &= 1\\ \psi(1) &= \mathbb{F}_p(x),\end{aligned}$$

Example 23.6. Finally, consider the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which is normal and separable. We showed that $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, and we can see that

$$\begin{aligned}\varphi(\mathbb{Q}) &= \mathbb{Z}/2\mathbb{Z}\\ \varphi(\mathbb{Q}(\sqrt{2})) &= 1\\ \psi(\mathbb{Z}/2\mathbb{Z}) &= \mathbb{Q},\\ \psi(1) &= \mathbb{Q}(\sqrt{2}).\end{aligned}$$

We know that $\varphi \circ \psi$ is the identity. How about $\psi \circ \varphi$?

We can see from the above examples that it is not always the identity.

Proposition 23.7. For any $K \subseteq E \subseteq F$,

$$\psi \circ \varphi(E) = E$$

if and only if F/E is a Galois extension.

Proof. For any such E, let $G = \mathrm{Aut}(F/E)$. Then, we have that

$$\psi \circ \varphi(E) = \psi(G) = F^G.$$

We know that any $\alpha \in E$ is fixed by any $\sigma \in G$, by definition, so that $E \subseteq F^G$.

Then, Theorem 22.5 tells us that

$$[F : F^G] = \left|\mathrm{Aut}(F/E)\right|.$$

But then, we know that by Corollary 20.6 that if F/E is a Galois extension, then $\left|\mathrm{Aut}(F/E)\right| = [F : E]$, so we get that

$$[F : F^G] = [F : E],$$

and since $E \subseteq F^G$, this implies that $E = F^G$.

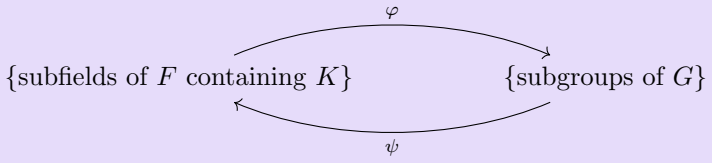
If F/E is not a Galois extension, then Corollary 20.6 tells us that $\left|\mathrm{Aut}(F/E)\right| < [F : E]$, so that

$$[F : F^G] < [F : E]$$

and this implies that $E \subsetneq F^G$, so $\psi \circ \varphi(E) \neq E$. □

Theorem 23.8 (Fundamental Theorem of Galois Theory)**.** IF $K \subseteq F$ is a finite Galois extension with

$G = \mathrm{Aut}(F/K)$ then there are bijections



which are inverses to each other.

Proof. The only step missing is that if F/K is Galois, then we know that F/E is also normal and separable for any $K \subseteq E \subseteq F$. □

Moreover, when F/K is a Galois extension, and $G = \mathrm{Aut}(F/K)$, then φ and ψ preserve indices. We know from Theorem 22.5 that for any subgroup $H \subseteq G$,

$$|H| = [F : \psi(H)],$$

which implies that $[G : H] = [\psi(H) : K]$ since $|G| = [F : K]$. Then, for any $K \subseteq E \subseteq F$, we can see that $[E : K] = [G : \varphi(E)]$, so $[F : E] = \big|\varphi(E)\big|$.

Corollary 23.9. For any finite Galois extension F/K,

$$\big|\{\text{subfields of } F \text{ containing } K\}\big| = \Big|\big\{\text{subgroups of } \mathrm{Aut}(F/K)\big\}\Big|.$$

Proof. This follows from the fact that the maps in the Fundamental Theorem are bijections. □

Example 23.10. Let us say we have a Galois extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. Then, we know that all intermediate fields $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\alpha)$ are simple, by Corollary 22.2, so they are all of the form $\mathbb{Q}(\alpha_i)$ for some $\alpha_i \in \mathbb{Q}(\alpha_i)$. Then, we have a partially-ordered set relation among all the intermediate fields, where $\mathbb{Q}(\alpha_{i_1}) \leq \mathbb{Q}(\alpha_{i_2})$ if $\alpha_{i_1} \in \mathbb{Q}(\alpha_{i_2})$.

Lecture 24: The Galois Correspondences

Definition 24.1. For any field extension, define

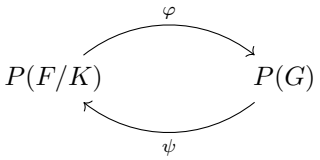
$$P(F/K) = \{\text{subfields of } F \text{ containing } K\}.$$

For any group G, define

$$P(G) = \{\text{subgroups of } G\}.$$

Then, $P(F/K)$ and $P(G)$ are partially ordered sets under inclusion.

Last time, we showed that if F/K is a finite Galois extension, there are inclusion-reversing isomorphisms of partially ordered sets:



where $G = \text{Aut}(F/K)$. These maps are defined as $\varphi(E) = \text{Aut}(F/E)$ and $\psi(H) = F^H$, so that $\varphi \circ \psi = \text{id}$ and because F/K is a Galois extension, $\psi \circ \varphi = \text{id}$.

Moreover, φ and ψ preserve indices. That is, for any $K \subseteq E \subseteq F$, we have the mapping

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

and then

$$[F : E] = [H : 1] = |H|,$$

and

$$[E : K] = [G : H] = |G| / |H|.$$

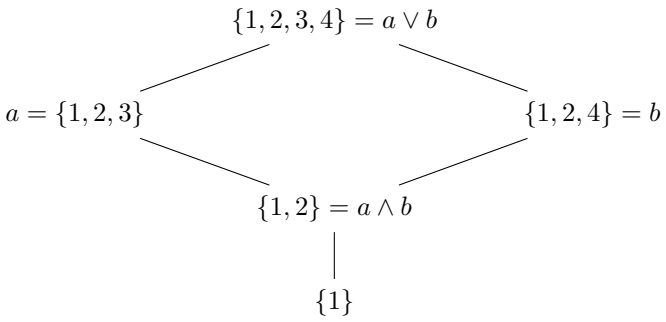
Definition 24.2. In a partially ordered set P, the **greatest lower bound** of $a, b \in P$, denoted $a \wedge b$, is an element $c \in P$ such that $c \leq a$ and $c \leq b$, but for any $c' \in P$ such that $c' \leq a$ and $c' \leq b$, $c \geq c'$.

The **least upper bound** of a and b, denoted $a \vee b$, is defined similarly.

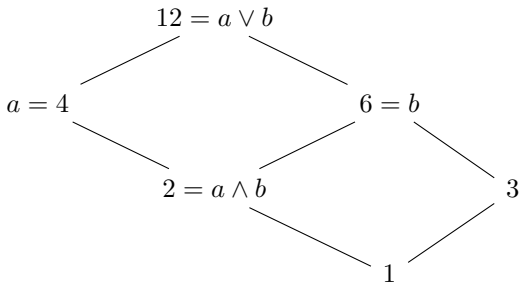
Definition 24.3. A partially ordered set P is a **lattice** if for any $a, b \in P$, the greatest lower bound of a and b and the least upper bound of a and b exist.

Example 24.4. The following partially ordered set, where a set $S \leq Q$ iff $S \subseteq Q$, is a lattice, and we

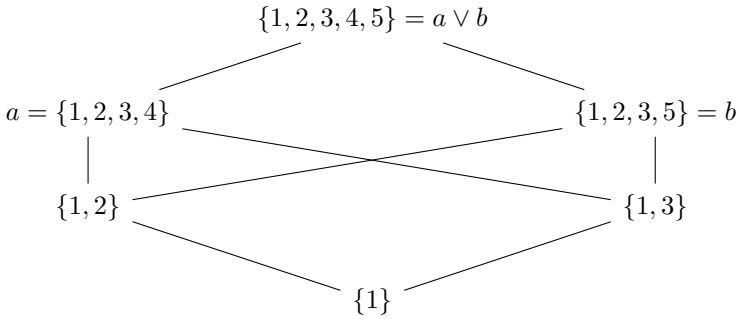
see one example of a greatest lower bound and a least upper bound.



Example 24.5. The following partially ordered set, where an integer $x \leq y$ iff $x \mid y$, is a lattice, and we see one example of a greatest lower bound and a least upper bound.



Example 24.6. In the following partially ordered set, where a set $S \leq Q$ iff $S \subseteq Q$, we see that it is not a lattice, because there is no greatest lower bound of the a and b indicated.



Note that for any group G, $P(G)$ is a lattice, since for subgroups $H_1, H_2 \subseteq G$, $H_1 \wedge H_2 = H_1 \cap H_2$ and $H_1 \vee H_2 = \langle H_1, H_2 \rangle$.

Moreover, for any field extension F/K, $P(F/K)$ is a lattice, because $E_1 \wedge E_2 = E_1 \cap E_2$, and $E_1 \vee E_2 = E_1 E_2$, where $E_1 E_2$ is defined to be $K(E_1, E_2)$, or the field generated by E_1 and E_2 over K.

Corollary 24.7. The maps φ and ψ are inclusion-reversing isomorphisms of lattices. With some com-

putation, we can see that

$$\varphi(E_1 \wedge E_2) = \varphi(E_1) \vee \varphi(E_2)$$
$$\varphi(E_1 \vee E_2) = \varphi(E_1) \wedge \varphi(E_2)$$
$$\psi(H_1 \wedge H_2) = \psi(H_1) \vee \psi(H_2)$$
$$\psi(H_1 \vee H_2) = \psi(H_1) \wedge \psi(H_2).$$

Example 24.8. We can consider the splitting field of $x^3 - 2$ over $\mathbb{Q}$; this is a Galois extension. We can see that it has degree 6 because we have the chain of extensions

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2) \\ \Big| 2 \\ \mathbb{Q}(\sqrt[3]{2}) \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

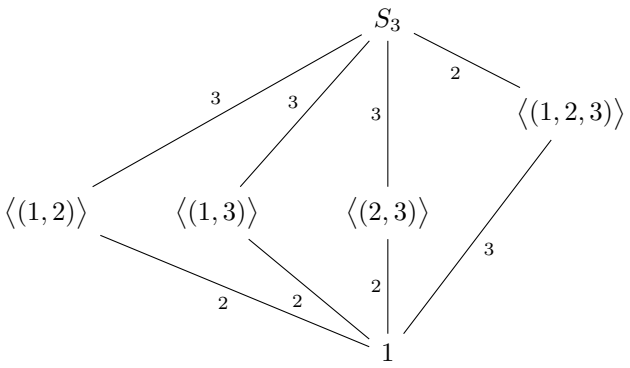
where $\eta = e^{2i\pi/3}$. Then, by Corollary 20.6, we can see that $\left|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2)/\mathbb{Q})\right| = 6$. But we also know that all automorphisms of this extension are defined by permutations of the roots, so

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2)) \subseteq S_3.$$

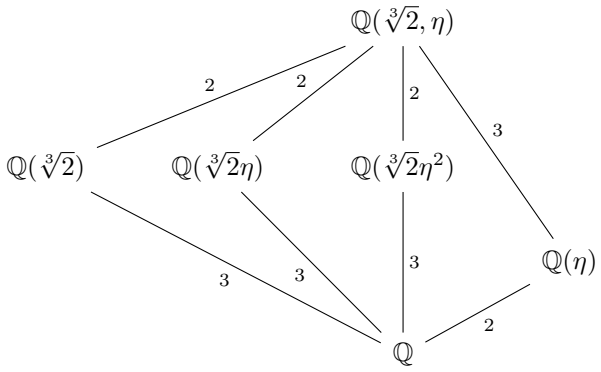
Since $|S_3| = 6$, we get that

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2)/\mathbb{Q}) \cong S_3.$$

Then, we can see that $P(S_3)$ is the following lattice:



and $P(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2)/\mathbb{Q})$ is the following lattice (note that $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\eta, \sqrt[3]{2}\eta^2) = \mathbb{Q}(\sqrt[3]{2}, \eta)$):



which we can see is an upside-down version of the previous lattice.

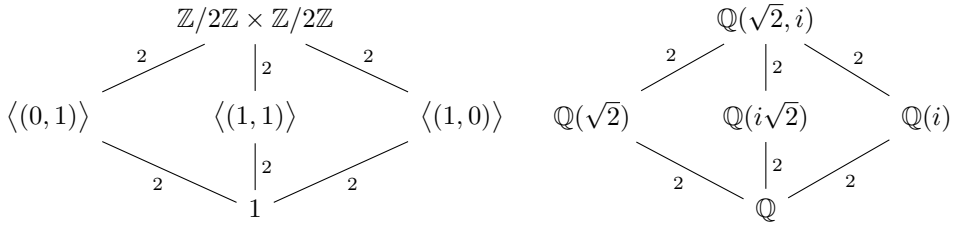
Example 24.9. We can consider the splitting field of $x^4 + 1$ over $\mathbb{Q}$, which we know is also a Galois extension. Specifically, it is the extension $\mathbb{Q}(\eta)/\mathbb{Q}$, where η is a primitive 8^{th} root of unity. We know that

$$\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

and that this automorphism group consists of the elements

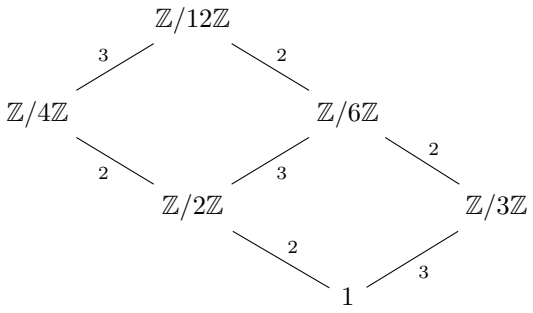
$$\eta \mapsto \eta,\ \eta \mapsto \eta^3,\ \eta \mapsto \eta^5,\ \eta \mapsto \eta^7.$$

Then, we have the following lattices, since, as we showed in Example 10.2, $\mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{2}, i)$.

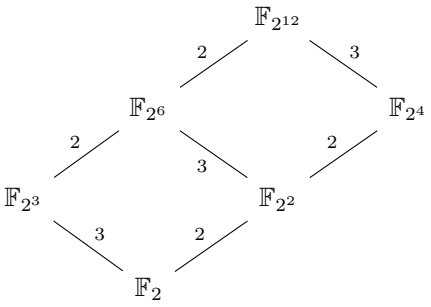


Example 24.10. Finally, remember that $\mathbb{F}_{2^{12}}/\mathbb{F}_2$ is a Galois extension, as we showed in Example 20.8. Moreover, remember that since $[\mathbb{F}_{2^{12}} : \mathbb{F}_2] = 12$, Theorem 17.1 tells us that $\text{Aut}(\mathbb{F}_{2^{12}}/\mathbb{F}_2) \cong \mathbb{Z}/12\mathbb{Z}$.

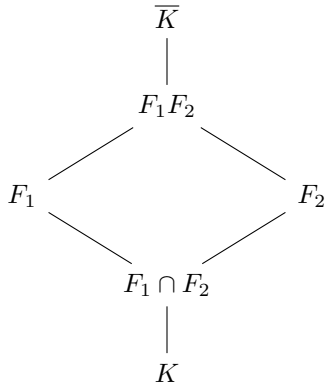
Then, we can see that $P(\mathbb{Z}/12\mathbb{Z})$ is:



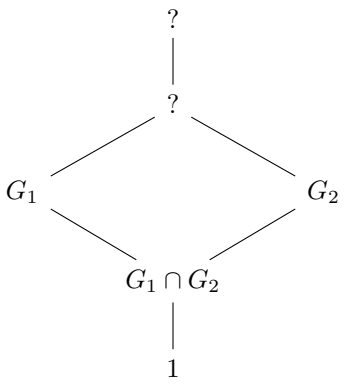
and by matching degrees to the previous diagram, we get that $P(\mathbb{F}_{2^{12}}/\mathbb{F}_2)$ is:



If we have the field extensions

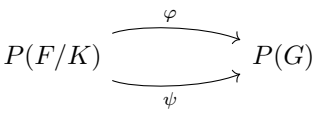


where F_1/K and F_2/K are Galois extensions, we know that the corresponding group lattice looks something like this (if G_1 is the automorphism group of F_1 and G_2 is the automoprhism group of F_2):



because $G_1 \cap G_2$ is clearly the automorphism group of F_1F_2. What goes in the question marks?

We know that we have the isomorphisms



Note that $P(G)$ admits a G-action

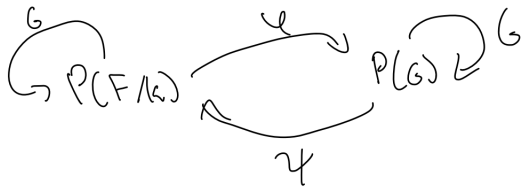
$$g \cdot H = gHg^{-1}.$$

That is, G acts by conjugation on the subgroups of G; remember from Math 120 that this leads to the Sylow theorems and the classification of finite subgroups.

The poset $P(F/K)$ also admits a G-action

$$g \cdot E = g(E)$$

since g is an automorphism of F over K. Thus, we can prove that this diagram commutes



Theorem 24.11. The Galois correspondences φ and ψ are isomorphisms of G-sets.

What we mean by this is that for any σ in G, and any $E \in P(F/K)$ and $H \in P(G)$,

$$\varphi(\sigma \cdot E) = \sigma \cdot \varphi(E)$$
$$\psi(\sigma \cdot H) = \sigma \cdot \psi(H).$$

We will prove this next lecture, but for now let's look at an example of where this theorem is applicable.

Example 24.12. Remember our field extension $\mathbb{Q}(\sqrt[3]{2}, \eta)/\mathbb{Q}$, where $G = S_3$.

Remember that since $\mathbb{Z}/3\mathbb{Z}$ is a subgroup of S_3 with index 2, it is a normal subgroup of S_3.

Moreover, note that the other three subgroups, which are all isomorphic to $\mathbb{Z}/2\mathbb{Z}$, are in the same G-orbit.

So if we look at $P(\mathbb{Q}(\sqrt[3]{2}, \eta), \mathbb{Q})$, we can see that for any $g \in G$,

$$g \cdot \mathbb{Q}(\eta) = \mathbb{Q}(\eta),$$

while the other three subfields: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\eta)$, and $\mathbb{Q}(\sqrt[3]{2}\eta^2)$ are conjugate.

We can actually see that since all the automorphisms of $\mathbb{Q}(\sqrt[3]{2}, \eta)/\mathbb{Q}$ fix $\mathbb{Q}(\eta)$, and all the automorphisms of $\overline{\mathbb{Q}}/\mathbb{Q}$ fix $\mathbb{Q}(\sqrt[3]{2}), \eta)$ (since it is a Galois extension), so $\mathbb{Q}(\eta)/\mathbb{Q}$ is a normal extension.

This logic works for any normal subgroup of a general $P(G)$, so we have found a relation between normal subgroups and normal extensions.

Lecture 25: Galois Correspondences and Normal Extensions

As promised, we will begin this lecture by proving Theorem 24.11.

Proof of Theorem 24.11. We want to show that φ and ψ are isomorphisms of G-sets. We already know that they are bijections, and we want to show that they are homomorphisms of G-sets. That is, for any $\sigma \in G$, and for any subgroup H of G and subfield $K \subseteq E \subseteq F$,

$$\mathrm{Aut}(F/\sigma(E)) = \sigma \,\mathrm{Aut}(F/E)\sigma^{-1},$$

and

$$F^{\sigma H \sigma^{-1}} = \sigma(F^H).$$

Since we already know that the two are inverses, we actually just need to prove one of the two statements, since this will imply the other. We will prove that

$$F^{\sigma H \sigma^{-1}} = \sigma(F^H)$$

for all $\sigma \in G$ and subgroups $H \subseteq G$.

Claim. $\sigma(F^H) \subseteq F^{\sigma H \sigma^{-1}}$

This is true because we can express any element in $\sigma(F^H)$ as $\sigma(\alpha)$, for some $\alpha \in H$. But then, for any element $\sigma h \sigma^{-1} \in \sigma H \sigma^{-1}$,

$$\sigma h \sigma^{-1} \cdot (\sigma \cdot \alpha) = \sigma h \cdot \alpha = \sigma \alpha$$

since we know that h fixes α. But this means that $\sigma h \sigma^{-1}$ fixes $\sigma(\alpha)$ for any $h \in H$, which means that

$$\sigma(\alpha) \in F^{\sigma H \sigma^{-1}}.$$

Since this is true for all elements $\sigma(\alpha) \in \sigma(F^H)$, we get that

$$\sigma(F^H) \subseteq F^{\sigma H \sigma^{-1}}.$$

Claim. $\sigma(F^H) = F^{\sigma H \sigma^{-1}}$

We only need to check that $[\sigma(F^H) : K] = [F^{\sigma H \sigma^{-1}} : K]$, or equivalently that

$$[F : \sigma(F^H)] = [F : F^{\sigma H \sigma^{-1}}].$$

Note that since σ is an isomorphism, $[F : \sigma(F^H)] = [F : F^H]$. But then, by Theorem 22.5, we get that

$$[F : \sigma(F^H)] = [F : F^H] = |H|.$$

Similarly, by Theorem 22.5,

$$[F : F^{\sigma H \sigma^{-1}}] = \left|\sigma H \sigma^{-1}\right|.$$

But conjugation is a bijection, so $\left|\sigma H \sigma^{-1}\right| = |H|$, and we are done. □

Now, let's think about the set of fixed points of the G-action. Recall that a fixed point under conjugation is a normal subgroup $H \trianglelefteq G$.

Which intermediate fields of F/K are fixed under the G-action?

Proposition 25.1. Let F/K be a finite Galois extension and let $G = \mathrm{Aut}(F/K)$. Let H be a subgroup of G and $E = \psi(H)$ be an intermediate field of F/K.

Then, $H \trianglelefteq G$ if and only if E is a normal extension of K.

Note that E is always separable over K, since F/K is separable. Thus, if E is a normal extension of K, then it is also a Galois extension.

Proof. Remember that H is a normal subgroup of G if and only if it is fixed under conjugation, which is equivalent to

$$\sigma(E) = E$$

for all $\sigma \in G$.

Thus, we will prove that E/K is normal if and only if $\sigma(E) = E$ for all $\sigma \in G$.

For the first direction, note that if E/K is normal, then by Theorem 13.7, $f(E) = E$ for all automorphisms $f : \overline{K}/K \to \overline{K}K$. But this implies that $\sigma(E) = E$ for all automorphisms $\sigma : F/K \to F/K$, which is what we wanted to show.

For the second direction, if $\sigma(E) = E$ for all $\sigma \in G$, then the restriction map

$$\begin{aligned} r : \mathrm{Aut}(F/K) &\to \mathrm{Aut}(E/K) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

is a group homomorphism. Observe that $\ker(r) = \mathrm{Aut}(F/E)$. Moreover, we know that $r : G/\ker(r) \to \mathrm{Aut}(E/K)$ is an injective map. So,

$$\big|\mathrm{Aut}(F/K)\big| \,/ \big|\mathrm{Aut}(F/E)\big| \leq \big|\mathrm{Aut}(E/K)\big| \leq [E : K].$$

But since F/K is Galois, and this implies F/E is Galois, the left-hand side equals $[F : K]/[F : E] = [E : K]$. So we get that

$$[E : K] \leq \big|\mathrm{Aut}(E/K)\big| \leq [E : K],$$

so these must be equalities, and therefore by Corollary 20.6, E/K is Galois and therefore normal. □

Corollary 25.2. Note that the last part of this proof implies that r is also surjective, so any automorphism in $\mathrm{Aut}(E/K)$ can be extended to an automorphism of F/K.

Proposition 25.3. Suppose E/K is Galois and $H \trianglelefteq G$ is a normal subgroup of G, with $\varphi(E) = H$ and $\psi(H) = E$. Then, $\mathrm{Aut}(E/K) \cong G/H$.

Proof. Remember from the proof of the theorem above that we have

$$\begin{array}{ccc} G & & \\ {\scriptstyle \pi}\downarrow & & \\ G/\ker(r) & \xrightarrow[r]{} & \mathrm{Aut}(E/K) \end{array}$$

where r is an isomorphism. But we also showed that $\ker(r) = \mathrm{Aut}(F/E) = H$. So we get that $G/H \cong \mathrm{Aut}(E/K)$, as we desired. □

Corollary 25.4. Any subfield of the cyclotomic extension $\mathbb{Q}(\mu[m])/\mathbb{Q}$ is the splitting field of a polynomial in $\mathbb{Q}[x]$. (Moreover, we can replace $\mathbb{Q}$ with a general field K, and the statement still holds.)

Proof. Remember that $\mathrm{Aut}(\mathbb{Q}(\mu[m])/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$, which is abelian. Thus, all intermediate fields of $\mathbb{Q}(\mu[m])/\mathbb{Q}$ correspond to subgroups of an abelian group, which are normal, and therefore these intermediate fields must all be normal extensions. □

A further conclusion is that $\sqrt[3]{2}$ is not contained in any $\mathbb{Q}(\mu[m])$, because then $\mathbb{Q}(\sqrt[3]{2})$ would be a subgroup of $\mathbb{Q}(\mu[m])$ and we know that $\sqrt[3]{2}$ is not normal.

Theorem 25.5. For any finite abelian group G, there is a polynomial in $\mathbb{Q}[x]$ whose Galois group is isomorphic to G.

Proof. Note that G appears as a quotient of the group

$$\mathbb{Z}/(p_1-1)\mathbb{Z} \times \mathbb{Z}/(p_2-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_n-1)\mathbb{Z}$$

for some list of distinct primes $p_1, \ldots, p_n$.

Let $m = p_1 \cdots p_n$. Then, we know that

$$(\mathbb{Z}/m\mathbb{Z})^\times = \mathbb{Z}/(p_1-1)\mathbb{Z} \times \mathbb{Z}/(p_2-1)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_n-1)\mathbb{Z}$$

and there exists some subgroup $H \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ such that $(\mathbb{Z}/m\mathbb{Z})^\times/H \cong G$.

Now, consider the field $\mathbb{Q}(\mu[m])$. We have the diagram

$$\begin{array}{ccc} \mathbb{Q}(\mu[m]) & \longleftrightarrow & 1 \\ | & & | \\ \mathbb{Q}(\mu[m])^H & \longleftrightarrow & H \\ | & & | \\ \mathbb{Q} & \longleftrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \end{array}$$

Moreover, since H is a subgroup of an abelian group, it is a normal subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$, which means that $E = \mathbb{Q}(\mu[m])^H$ is a normal extension of $\mathbb{Q}$, so E is the splitting field of some polynomial $f(x) \in \mathbb{Q}[x]$.

Moreover, we know that by Proposition 25.3,

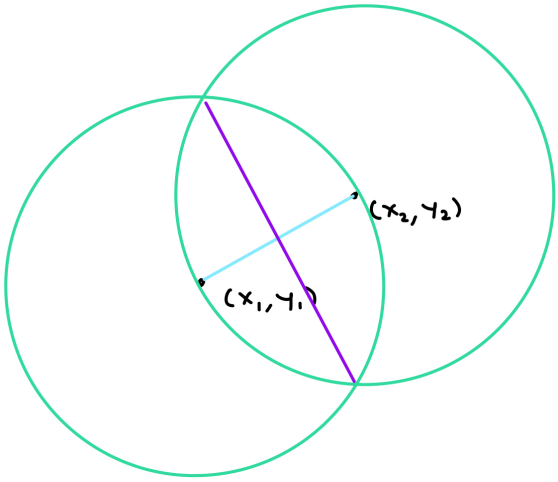
$$\mathrm{Aut}(E/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times/H \cong G,$$

so the Galois group of $f(x)$ is isomorphic to G. □

Lecture 26: Constructability III and Extensions by Radicals

We return to looking at straightedge and compass constructions.

First, note that if we have any two points (x_1, y_1) and (x_2, y_2), we can construct their midpoint by drawing the blue line, then drawing the green circles, and finally drawing the purple line and looking at its intersection with the blue line:



We will use this fact in various places in this lecture.

Recall that Theorem 8.3 tells us that if α is contstructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ for some nonnegative integer r. In essence, this is because we are creating at most a quadratic extension at each step of the construction.

In fact, the following converse holds:

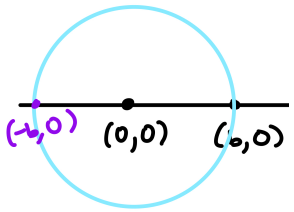
Theorem 26.1. For any sequence of field extensions

$$\mathbb{R} \supseteq F_n \supseteq \cdots \supseteq F_0 = \mathbb{Q},$$

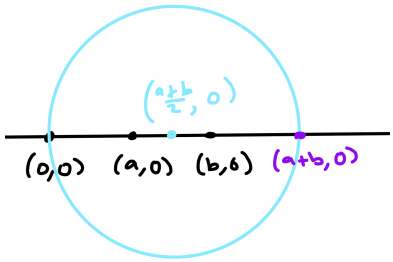
where $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq n$, any $\alpha \in F_n$ is constructible.

Proof. First, we will show that if the basis of our field is constructible, then any element of our field is constructible. To do so, we need to show that all the field operations are constructible; if we have two points a, b that are constructible, we can construct $a + b$, $-b$, ab, and b^{-1}. We will go through each of these operations:

- To construct $-b$, we draw the circle centered at $(b, 0)$ and containing $(0, 0)$. This next intersects the axis at $(-b, 0)$.

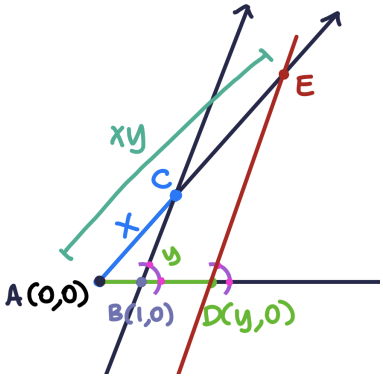


- To construct $a+b$, we first find the midpoint of $(a,0)$ and $(b,0)$ as mentioned above. Then, we can draw the circle centered at $\left(\frac{a+b}{2},0\right)$ and containing the point $(0,0)$, and this circle next intersects the x-axis at the point $(a+b,0)$.



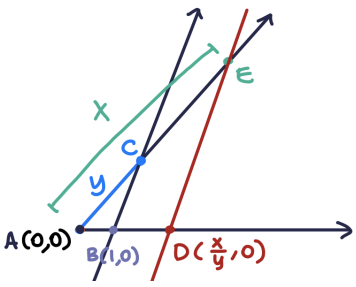
(the following two constructions are from Adam Inamasu)

- To construct the product of two elements x and y, we first draw lines at a given angle from $(1,0)$ and $(y,0)$. (Remember that we can construct, e.g, a $60°$ angle by drawing an equilateral triangle.) Then, mark off the point where the line through $(1,0)$ meets the circle passing through $(x,0)$ and centered at $(0,0)$; this is a line segment $\overline{AC}$ of length x. We can extend this line segment to pass through our line though $(y,0)$; this gives us a line segment $\overline{AE}$ which by similar triangles must have length xy.



If we want the point $(xy,0)$ from here, we can simply draw the circle centered at A and passing through E.

- We construct x/y in a similar way. First, draw a line at an arbritary angle from $(1,0)$, and mark off the point C where this line intersects the circle centered at $(0,0)$ with radius y. Then, extend the line $\overline{AC}$ to intersect the circle centered at $(0,0)$ with radius x. We will call this intersection point E. Then, draw a line passing through E but parallel to BC, and this intersects the axis at $(x/y,0)$, as we wanted.

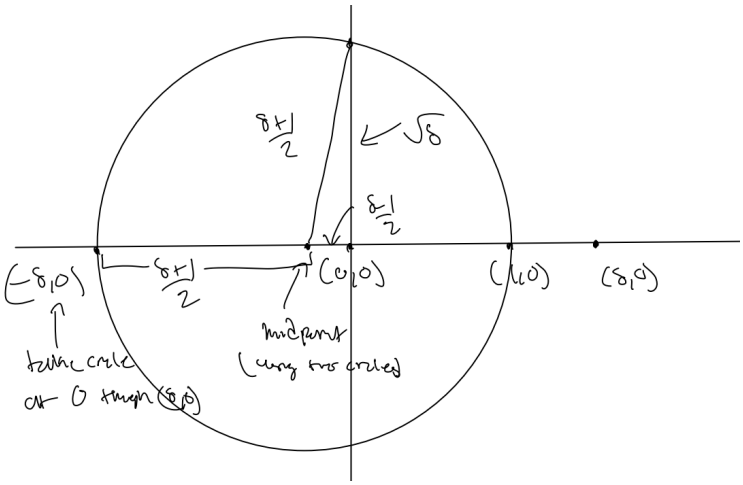


This implies that all of $\mathbb{Q}$ is constructible, because we know we can obtain any element in $\mathbb{Q}$ by applying these operations to 1 and 0. Moreover, we can see that for any i, if $F_i = F_{i-1}(\alpha)$, then if α and all of F_{i-1} are constructible, then all of F_i is constructible. So all we need to show now is that we can construct our field extensions; specifically, we need to find such an α for each i, and show that α is constructible.

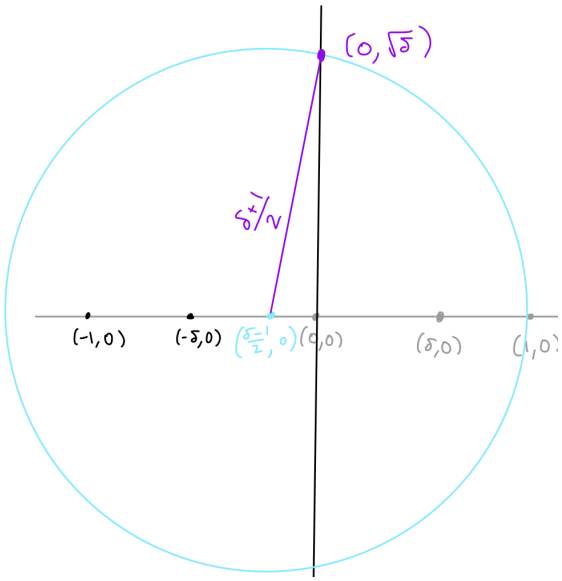
First, note that since it is a quadratic extension, we can say that $F_i = F_{i-1}(\alpha)$ for any $\alpha \in F_i \setminus F_{i-1}$. Then, let $x^2 + bx + c$ be the minimal polynomial of α over F_{i-1}. Then, if we set $\delta = b^2 - 4c$, the quadratic formula tells us that

$$F_{i-1}(\alpha) = F_{i-1}(\sqrt{\delta}) = F_i.$$

So we can always write F_i as $F_{i-1}(\sqrt{\delta})$, where $\delta \in F_{i-1}$. It is enough to show that if δ is constructible, $\sqrt{\delta}$ is also constructible. If $\delta > 1$, we can construct $\sqrt{\delta}$ as follows:



Similarly, if $\delta < 1$ (the case where $\delta = 1$ is obvious), we can construct $\sqrt{\delta}$ by first constructing the black points and the vertical line in the below diagram, and then constructing the blue point as the midpoint between $(1, 0)$ and $(-\delta, 0)$ and the blue circle as the circle centered at the blue point and containing $(1, 0)$, and finally we can see by the Pythagorean Theorem that the purple point is exactly $(0, \sqrt{\delta})$.



Thus, $\sqrt{\delta}$ is constructible, and it follows that any point in this chain is constructible. □

Theorem 26.2. The regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2.

Proof. We showed the "only if" part in Theorem 19.1.

Now, we will show the converse. Remember that the regular n-gon is constructible if and only if (x_n, y_n) is constructible, where $\eta_n = x_n + iy_n$ is a primitive n^{th} root of unity.

Suppose $\varphi(n) = 2^\ell$ for some ℓ. We have that

$$\mathbb{Q}(\eta_n) \supseteq \mathbb{Q}(x_n) \supseteq \mathbb{Q}(\eta_n + \eta_n^{-1}).$$

Note that

$$\eta_n^2 - 2x_n\eta_n + 1 = 0,$$

so the degree of $\mathbb{Q}(\eta_n)$ over $\mathbb{Q}(x_n)$ is at most 2. Since $i \in \mathbb{Q}(\eta_n)$ but $i \notin \mathbb{Q}(x_n)$, we have that $[\mathbb{Q}(\eta_n) : \mathbb{Q}(x_n)] = 2$.

Remember that $\text{Aut}(\mathbb{Q}(\eta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so it is an abelian group of order 2^ℓ.

This means that all subgroups of this autormophism group are normal, so, specifically, $\text{Aut}(\mathbb{Q}(\eta_n)/\mathbb{Q}(x_n))$ is normal and therefore $\mathbb{Q}(x_n)/\mathbb{Q}$ is a Galois extension. Additionally, $\text{Aut}(\mathbb{Q}(x_n)/\mathbb{Q}) = 2^\ell/2 = 2^\ell - 1$.

Then, the Fundamental Theorem of Finitely Generated Abelian Groups tells us that

$$\text{Aut}(\mathbb{Q}(x_n)/\mathbb{Q}) \cong (\mathbb{Z}/2^{k_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^{k_n}\mathbb{Z}),$$

for some $k_1, \ldots, k_n$.

But since our group has this structure, we can find a chain of subgroups

$$1 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_t = \text{Aut}(\mathbb{Q}(x_n)/\mathbb{Q}),$$

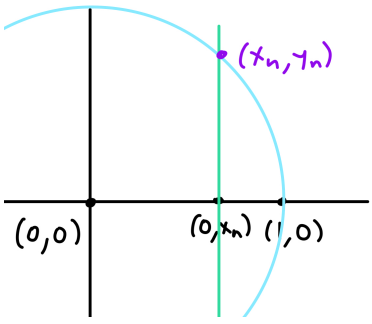
where $[G_i : G_{i-1}] = 2$ for each i.

But this means there are subsets

$$\mathbb{Q}(x_n) = F_t \supseteq \cdots \supseteq F_2 \supseteq F_1 \supseteq F_0 = \mathbb{Q},$$

where $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq t$.

But from Theorem 26.1, we get that x_n is constructible. But then, we can see that if we have the point $(x_n, 0)$, then by drawing the blue circle and then the vertical green line, we can construct the point (x_n, y_n):



Thus, we have constructed the n-gon. □

Note that the chain of subgroups we used is related to and is actually a demonstration of the solvability of the abelian group.

Corollary 26.3. If p is a prime, then a regular p-gon is constructible if and only if p is a Fermat prime.

(You could theoretically extract a specific construction of the regular p-gon using the chain of subgroups.)

Definition 26.4. Let F/K be a field extension. Then, $\alpha \in F$ is **radical** over K if $\alpha^n \in K$ for some n.

Definition 26.5. We say that F/K is an **extension by radicals** if there are intermediate fields

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = F$$

such that for each $1 \leq i \leq r$, $F_i = F_{i-1}(\alpha)$ for some α that is radical over F_{i-1}.

Definition 26.6. We say $f(x) \in K[x]$ is **solvable by radicals** if there is an extension by radicals F/K that contains all the roots of $f(x)$.

Example 26.7. Every quadratic $f(x) \in K[x]$ is solvable by radicals if $\text{ch}(K) \neq 2$. This is because if we let $f(x) = x^2 + bx + c$, then we know that the splitting field of $f(x)$ over K is a subfield of $K(\sqrt{b^2 - 4c})$, so this contains all the roots of $f(x)$ and it is clearly an extension by radicals.

Theorem 26.8. For any field K such that $\text{ch}(K) \neq 2, 3$, every cubic $f(x) \in K[x]$ is solvable by radicals.

Proof. First, note that $f(x)$ is solvable by radicals if and only if $f(x + b)$ is solvable by radicals, for some $b \in K$. So by using this linear shift, we can write every cubic as

$$x^3 + px + q = 0$$

for some $p, q \in K$.
But then, we can see that

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

and

$$\beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

are both roots of this polynomial, and clearly α and β are both solvable by radicals. Moreover, we can see that

$$\alpha\beta = \sqrt[3]{\frac{q^2}{4} - \frac{q^2}{4} - \frac{p^3}{27}} = -\frac{p}{3},$$

so by Vieta's, the remaining root of the cubic is $-\alpha - \beta$, which would already be an element of $K(\alpha, \beta)$.

Thus, this polynomial is solvable by radicals. □

The following is also known to be true, though we will not prove it in this class:

Theorem 26.9. Every quartic $f(x) \in K[x]$ is solvable by radicals.

Lecture 27: Solvable Groups and Solvability by Radicals

When is a polynomial $f(x) \in K[x]$ solvable by radicals?

We have the following theorem.

Theorem 27.1. Suppose $\text{ch}(K) = 0$. Then, a polynomial $f(x) \in K[x]$ is solvable by radicals if and only if the Galois group of $f(x)$ over K is solvable.

In a sense, for a polynomial to be solvable, we want its Galois group to be nearly abelian.

We will prove this theorem in the next lecture, but for now we will look at some examples.

What is the Galois group of $x^n - b \in K[x]$?

(Assume $\text{ch}(K) \not| n$, so that $x^n - b$ is separable.)

Proposition 27.2. For any field K, the Galois group of $x^n - b$ over $K[x]$ is solvable.

Proof. We will divide this proof into two cases.

Case 1: K contains a primitive n^{th} root of unity.
Let η be this primitive n^{th} root, so that $\eta^n = 1$. Then, if α is a zero of $f(x) = x^n - b$, then the set of roots of $f(x)$ is

$$\left\{\alpha, \alpha\eta, \ldots, \alpha\eta^{n-1}\right\}.$$

Thus, $F = K(\alpha)$ is the splitting field of $f(x)$. Then,

$$\text{Aut}(F/K) = \{\sigma_0, \ldots, \sigma_{n-1}\},$$

where $\sigma_i(\alpha) = \alpha\eta^i$ for each i. We can see that for any i, j,

$$\begin{aligned}\sigma_i\sigma_j(\alpha) &= \sigma_i(\alpha\eta^j) \\ &= \sigma_i(\alpha)\sigma_i(\eta)^j \\ &= \alpha\eta^{i+j},\end{aligned}$$

since $\eta \in K$, so $\sigma_i(\eta) = \eta$. Thus, this group is $\mathbb{Z}/n\mathbb{Z}$ and therefore abelian.

Case 2: K does not contain a primitive n^{th} root of unity.
If α is a root of $f(x)$, then the set of roots of $f(x)$ are

$$\left\{\alpha, \alpha\eta, \ldots, \alpha\eta^{n-1}\right\}.$$

Then, we have the diagram

$$\begin{array}{ccc} F = K(\alpha, \eta) & \longleftrightarrow & 1 \\ | & & | \\ K(\eta) & \longleftrightarrow & H = \text{Aut}(F/K(\eta)) \\ | & & | \\ K & \longleftrightarrow & G = \text{Aut}(F/K) \end{array}$$

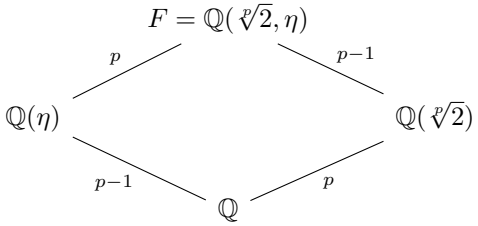
It should be clear that all of these are normal extensions. Moreover, we can see that $\mathrm{Aut}(F/K(\eta)) = H$ is abelian by Case 1, and $\mathrm{Aut}(K(\eta)/K) \cong G/H$ is abelian since it is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. But this means that G is a solvable group, since we can decompose it into

$$1 \trianglelefteq H \trianglelefteq G,$$

and each composition factor is normal.

So, either way, the Galois group is solvable. □

Example 27.3. Consider the polynomial $x^p - 2 \in \mathbb{Q}[x]$, where p is prime. We have the following decomposition:



where we can solve for the top two degrees by the fact that $[F : \mathbb{Q}] \leq p(p-1)$, since $\sqrt[p]{2}$ has a minimal polynomial of degree p over $\mathbb{Q}$ and η has a minimal polynomial of degree $p-1$ over $\mathbb{Q}$.

Then, we know by Corollary 20.6 that $G = \mathrm{Gal}(F/\mathbb{Q})$ has $|G| \leq p(p=1)$.

For $0 < a < p$ and $0 \leq b < p$, define $\sigma_b^a \in G$ to be the automorphism over $\mathbb{Q}$ defined by

$$\sigma_b^a(\sqrt[p]{2}) = \sqrt[p]{2}\eta^b, \qquad \sigma_b^a(\eta) = \eta^a.$$

Note that we have the short exact sequence

$$1 \longrightarrow \mathbb{F}_p \longrightarrow G \longrightarrow \mathbb{F}_p^\times \longrightarrow 1.$$

But G is not abelian, since

$$\begin{aligned}\sigma_{b_1}^{a_1}\sigma_{b_2}^{a_2}(\sqrt[p]{2}) &= \sigma_{b_1}^{a_1}(\sqrt[p]{2})\sigma_{b_1}^{a_1}(\eta)^{b_2} \\ &= \sqrt[p]{2}\eta^{b_1}\eta^{a_1 b_2} \\ &= \sqrt[p]{2}\eta^{a_1 b_2 + b_1},\end{aligned}$$

and

$$\sigma_{b_1}^{a_1}\sigma_{b_2}^{a_2}(\eta) = \sigma_{b_1}^{a_1}(\eta^{a_2}) = \eta^{a_1 a_2}.$$

This means that $\sigma_{b_1}^{a_1}\sigma_{b_2}^{a_2} = \sigma_{a_1 b_2 + b_1}^{a_1 a_2}$, and clearly this is not abelian since $a_1 b_2 + b_1 \neq a_2 b_1 + b_2$ in general.

We can think of this as the group of affine transformations over $\mathbb{F}_p$ since we can map each σ_a^b to a map $\mathbb{F}_p \to \mathbb{F}_p$ defined by $x \mapsto ax + b$ (where $a \neq 0$). In terms of matrices, this is the group of invertible matrices over $\mathbb{F}_p$ of the form

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix},$$

and it has a normal subgroup H, which is the group of triangulations over $\mathbb{F}_p$, of the form

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}.$$

This group is isomorphic to $\mathbb{F}_p$, since we are restricted to choosing $b \in \mathbb{F}_p$.

Then, $G/H \cong \mathbb{F}_p^\times$, because it corresponds to the set of possible options for a, and it is abelian.

We turn to talking about solvable groups - this is a review of Math 120.

Let G be a finite group.

Definition 27.4. A **composition series** of G is a sequence of subgroups

$$H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq G$$

so that H_{i-1} is normal in H_i. It is the sequence of this form with the maximum length.

The maximality condition is equivalent to the condition that H_i/H_{i-1} is a simple group; this is because H_i/H_{i-1} has no normal subgroups if and only if there is no H such that $H_{i-1} \trianglelefteq H \trianglelefteq H_i$.

Definition 27.5. The simple groups H_i/H_{i-1} are called the **composition factors** of G.

Theorem 27.6 (Jordan-Hölder)**.** The isomorphism classes of the composition factors and their multiplicities only depend on G and not the chosen composition series.

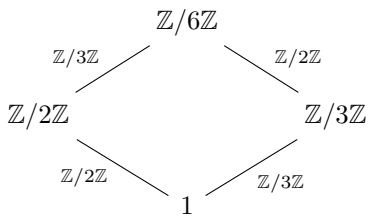
We can look at some examples of dividing a group into its composition series:

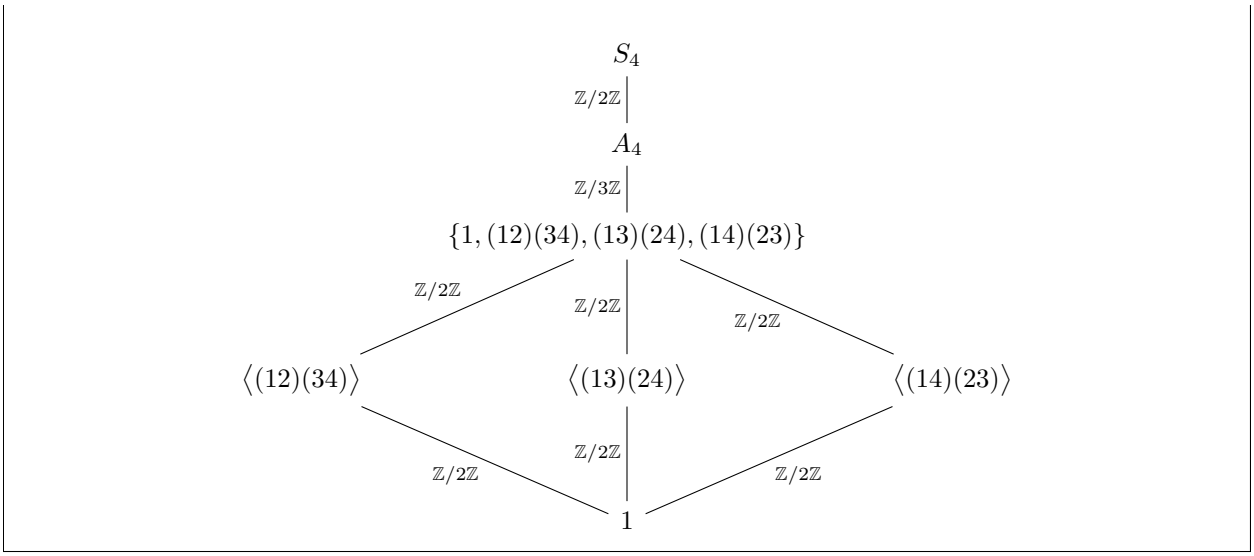
Example 27.7. When $G = S_3$, we have the composition series

$$1 \trianglelefteq A_3 \trianglelefteq S_3.$$

But $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ and $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Example 27.8. We have a few more examples, in the form of diagrams:





We see that many times, the composition factors are $\mathbb{Z}/p\mathbb{Z}$.

Definition 27.9. A finite group G is **solvable** if all of its composition factors are cyclic.

Since we know the composition factors are all simple groups, we can see that if G is solvable, all of its composition factors are $\mathbb{Z}/p\mathbb{Z}$ for prime p.

We already showed that the Galois groups $\mathrm{Gal}(F/K)$, where F is the splitting field of $x^n - b$ over K, are all solvable groups.

We now return to proving our actual theorem.

Proof of Jordan-Hölder. First, we need to show that such a composition series exists. To do so, we use induction on the size of G.

The base case is when G is the trivial group, and then the composition series is just G itself.

For the inductive case, for any G, let N be the largest normal subgroup of G. We know that N exists because there is at least one normal subgoup of G, $\{1\}$, and since G is finite this means there must be a largest one. But then, we can see that G/N is simple because if $H \trianglelefteq G/N$ then the fourth isomorphism theorem would tell us that there exists some H' such that $H'/N = H$ and $N \trianglelefteq H' \trianglelefteq G$. Thus, G/N is simple, and we know by induction that N has a composition series, so we have a composition series for G.

For the uniqueness of composition factors, we will again use induction.

For a base case, if G is simple then clearly

$$1 \trianglelefteq G$$

is the only composition series.

For the inductive case, assume we have two composition series for G:

$$1 \trianglelefteq H_1 \trianglelefteq H_2 \cdots \trianglelefteq H_r \trianglelefteq G$$
$$1 \trianglelefteq K_1 \trianglelefteq K_2 \cdots \trianglelefteq K_s \trianglelefteq G.$$

First, if $H_r = K_s$ then we know that $G/K_s = G/H_r$ and we know by the inductive assumption that the composition factors leading up to H_r are some permutation of the composition factors leading up to K_s.

Otherwise, define $H = H_r$, $K = K_s$, and $L = H \cap K$. The second isomorphism theorem tells us that $L \trianglelefteq H$ and $L \trianglelefteq K$, and $G/H \cong K/L$ and $G/K \cong H/L$.

Then, note that L must have some composition series

$$1 \trianglelefteq L \trianglelefteq \cdots \trianglelefteq L_t \trianglelefteq L.$$

But this means that

$$1 \trianglelefteq L \trianglelefteq \cdots \trianglelefteq L_t \trianglelefteq L \trianglelefteq H$$
$$1 \trianglelefteq L \trianglelefteq \cdots \trianglelefteq L_t \trianglelefteq L \trianglelefteq K$$

are composition series. But by the inductive assumption, we know that the composition factors of H are unique up to permutation, so that $r = t + 1$ and the composition factors of H are some permutation of

$$\left(H/L, L_t/L_{t-1}, \ldots, L_1/1\right)$$

and similarly, the composition factors of K are unique up to isomorphism, so $s = t + 1$ and the composition factors of K must be some permutation of

$$\left(K/L, L_t/L_{t-1}, \ldots, L_1/1\right).$$

Then, we can return to our two composition series

$$1 \trianglelefteq H_1 \trianglelefteq H_2 \cdots \trianglelefteq H \trianglelefteq G$$
$$1 \trianglelefteq K_1 \trianglelefteq K_2 \cdots \trianglelefteq K \trianglelefteq G.$$

We can see that the composition factors for the first series are some permutation of

$$\left(G/H, H/L, L_t/L_{t-1}, \ldots, L_1/1\right)$$

and the composition factors for the second series are some permutation of

$$\left(G/K, K/L, L_t/L_{t-1}, \ldots, L_1/1\right).$$

But since $G/H \cong K/L$ and $G/K \cong H/L$, these two are permutations of each other, and since this is true for any two composition series for G, we get that the composition factors for G are unique up to permutation. $\square$

Lecture 28: Galois Groups and Solvability by Radicals

Let K be a field, such that $\mathrm{ch}(K) = 0$.

Last time, we stated Theorem 27.1, which says that a polynomial $f(x) \in K[x]$ is solvable by radicals if and only if the Galois group of the polynomial is solvable.

We will only prove one direction of this statement: that if $f(x) \in K[x]$ is solvable by radicals, then the Galois group is solvable.

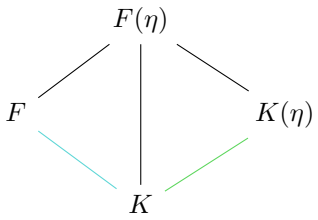
Proof. Let F/K be an extension by radicals containing the splitting field of $f(x) \in K[x]$. This means we have some chain of field extensions

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F,$$

with $F_i = F_{i-1}(\alpha_i)$ such that there is some natural number n_i such that $\alpha_i^{n_i} \in F_{i-1}$.
We want to show that the Galois group of $f(x)$ is solvable.

If F/K is a Galois extension, we proceed as follows.

First, set $m = \prod_i n_i$ and let η be a primitive m^{th} root of unity over K. Then, consider the extensions



We can see that the green extension is Galois because it is the splitting field of a perfect field, and the blue extension is Galois by assumption.

Then, note that in general, if A/K and B/K are Galois with $\mathrm{ch}(K) = 0$, then A/K corresponds to $\mathrm{Aut}(F/A)$ and B/K corresponds to $\mathrm{Aut}(F/B)$, which are both normal subgroups of $\mathrm{Aut}(F/K)$. But this means that $\mathrm{Aut}(F/A) \cap \mathrm{Aut}(F/B)$ is a normal subgroup of $\mathrm{Aut}(F/K)$, which means that AB/K is a normal extension, and since K is perfect, it must also be separable.

This implies that $F(\eta) = FK(\eta)$ is also a Galois extension of K.

We then have the extension by radicals

$$K \subseteq K(\eta) = F_0(\eta) \subseteq F_1 \subseteq \cdots \subseteq F_n = F \subseteq F_{n+1} = F(\eta),$$

so we have extended our previous sequence by 1.

Note that $F_i(\eta)$ is the splitting field of $x^{n_i} - \alpha_i^{n_i}$ over $F_{i-1}(\eta)[x]$. Since these are splitting field extensions over perfect fields, each $F_i(\eta)/F_{i-1}(\eta)$ is a Galois extension. This implies that $F(\eta)/K$ is also a Galois extension.

Let E be the splitting field of $f(x)$ over K, so that we have $E \subseteq F \subseteq F(\eta)$.

For each i, let H_i be the corresponding group for $F_i(\eta)$, so that

$$H_i = \text{Aut}(F_n(\eta)/F_i(\eta)).$$

Moreover, let H be the corresponding group for E, so

$$H = \text{Aut}(F_n(\eta)/E)$$

and then the Galois group of E is $G = \text{Aut}(F(\eta)/K)/H$.

Note that since each $F_i(\eta)/F_{i-1}(\eta)$ is a normal extension, $H_i \trianglelefteq H_{i-1}$ for each i. Moreover, for each i, we can see that

$$H_i/H_{i-1} = \text{Aut}(F_i(\eta)/F_{i-1}(\eta))$$

is the Galois group for $x^{n_i} - \alpha_i^{n_i}$ over $F_{i-1}(\eta)$; we showed in Proposition 27.2 that this group is solvable.

But then since we have expressed $\text{Aut}(F_n(\eta)/K)$ as a chain of normal subgroups whose quotients are solvable, we get that $\text{Aut}(F_n(\eta)/K)$ is solvable as well.

Then, since G is the quotient group of a solvable group, a fact in group theory tells us that G is also solvable, and we are done. □

In this proof, why can we assume that F/K is Galois?

We can always construct something called the *Galois closure* of F, which is a field containing F which is Galois over K. We can show that when F/K is an extension by radicals, there exists a Galois closure of F which is also an extension by radicals.

Let

$$\text{Hom}(F/K, \overline{K}/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_d\}$$

where $d = [F : K]$. Note that we know all the roots are distinct because K is a perfect field, so F/K is separable. Now, consider the extension

$$L = \prod_{j=1}^{d} \sigma_j(F)$$

over K; this is the smallest field containing $\sigma_i(F)$ for all $1 \leq i \leq d$. If F was normal then each of these would equal F, and $L = F$.

Note that L/K is Galois as L is a normal extension. Specifically, we can see that for any $\sigma \in \text{Hom}(F/K, \overline{K}/K)$,

$$\sigma(L) = \prod_{j=1}^{d} \sigma\sigma_j(F) = \prod_{j=1}^{d} \sigma_j(F).$$

If $F = K(\alpha)$, then L is the splitting field of the minimal polynomial of α over K.

Moreover, L is an extension by radicals over K. That is, we know

$$F = K(\alpha_1, \ldots, \alpha_m)$$

where for each $1 \leq i \leq m$, there exists some natural number n_i such that $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. Then,

$$L = \prod_{j=1}^{d} = K\left(\sigma_1(\alpha_1), \sigma_2(\alpha_2), \ldots, \sigma_1(\alpha_m), \sigma_2(\alpha_1), \ldots, \sigma_d(\alpha_m)\right).$$

But then, note that

$$\sigma_1(\alpha_1)^{n_1} = \sigma_1(\alpha_1^{n_1}) = \alpha_1^{n_1}$$

since $\alpha_1^{n_1} \in K$, and then

$$\sigma_1(\alpha_2)^{n_2} = \sigma_1(\alpha_2^{n_2}) \in \sigma_1(K(\alpha_1)) = K(\sigma_1(\alpha_1)),$$

and we can continue inductively, noting that for each i,

$$\sigma_i(\alpha_1)^{n_1} = \sigma_i(\alpha_1^{n_1}) = \alpha_1^{n_1} \in K \subseteq K\left(\sigma_1(\alpha_1), \sigma_2(\alpha_2), \ldots, \sigma_1(\alpha_m), \sigma_2(\alpha_1), \ldots, \sigma_{i-1}(\alpha_m)\right).$$

Thus, we get that L/K is an extension by radicals.

Thus, for each field F which is an extension by radicals containing the splitting field of $f(x)$, there is a Galois closure L of F which is still an extension by radicals, so we can make our assumption in the proof that F is Galois by replacing it with its Galois closure if it is not.

Another group theoretic fact:

Many groups are not soluble.

Example 28.1. The alternating subgroup $A_5 \trianglelefteq S_5$ is simple, which means it has no nontrivial normal subgroup. By Jordan-Hölder, if we find one composition series that doesn't follow the properties of solvability, our group is not solvable. Consider the composition series

$$S_5 \text{ —— } A_5 \text{ —— } 1$$

We can see that $A_5 = A_5/1$ is not abelian, so S_5 is not solvable.

Note that the nontrivial proper subgroups of A_5 are

$\mathbb{Z}/2\mathbb{Z}$,	$\langle (12)(34) \rangle$	15
$(\mathbb{Z}/2\mathbb{Z})^2$,	$\langle (12)(34), (13)(24) \rangle$	5
$\mathbb{Z}/3\mathbb{Z}$,	$\langle (123) \rangle$	10
$\mathbb{Z}/5\mathbb{Z}$,	$\langle (12345) \rangle$	6
S_3,	$\langle (123), (12)(45) \rangle$	10
D_{10},	$\langle (12345), (12)(34) \rangle$	6
A_4,	$\langle (123), (12)(34) \rangle$	5

None of these are fixed under conjugation, so A_5 is simple.

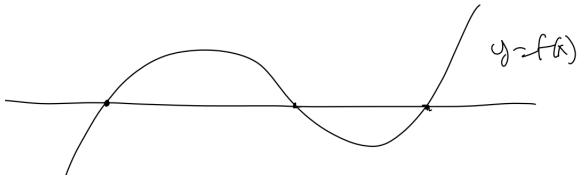
Corollary 28.2. Any polynomial with Galois group A_5 or S_5 is not solvable by radicals.

Example 28.3. Most polynomials of degree 5 have symmetry group S_5. Consider the polynomial

$$f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x].$$

It is irreducible by Eisenstein's criterion. Thus, $5 \mid |G|$ since we start constructing the splitting field of $f(x)$ by adjoining any of its roots to $\mathbb{Q}$, and this is a degree-5 extension.

This means that G must contain a 5-cycle when viewed as a subgroup of S_5. Note that $f'(x) = 5x^4 - 6$ contains exactly two real roots: $\pm\sqrt[4]{\frac{6}{5}}$. Neither of these are critical points, so the graph of $f(x)$ looks something like



and there are 3 real roots of $f(x)$.

Then, if F is the splitting field over $\mathbb{Q}$, complex conjugation acts on F by permuting the two complex roots.

This means that G contains a transposition and a 5-cycle, so it must be the entirety of S_5. (This is because, for any prime p, S_p is generated by a transposition and a p-cycle.)

Thus, $x^5 - 6x + 3$ is not solvable by radicals.