Math 123: Algebra II

Course Taught by Sebastien Vasey
Notes Taken by Forrest Flesher

Spring 2020

Welcome to Math 123: Algebra II. Here's some important information:

- The course webpage is:
  http://people.math.harvard.edu/~sebv/123-spring-2020/
- The syllabus is located at:
  http://people.math.harvard.edu/~sebv/123-spring-2020/syllabus.pdf
  Office hours are at the following times over Zoom:
  - Tuesday, Thursday, 4-5pm ET.
- Your CAs will also hold office hours at the following times over Zoom:
  - Garrett: Sunday 10-11am ET, Monday 8-10pm ET,
  - Forrest: Tuesday 9:30-11:59pm, Friday 3-4pm.
- The text for the course is Dummit and Foote "Abstract Algebra, 3rd edition." If you don't have a copy, don't worry: all the problem sets will include copies of the problems, and the course notes will contain all the course material.
- Relevant emails are sebv@math.harvard.edu , forrestflesher@college.harvard.edu, garrettbrown@college.harvard.edu, Email with any questions, comments, or concerns, especially if you find a mistake in these notes.
- We will use the Canvas site for submitting/grading problem sets.
- It is okay if your psets are legibly non-latexed, but latex is much preferred.
- The prerequisites are math 122 or math 55a. If you haven't taken either of these but are comfortable enough with algebra, that is also okay.

Contents

§1 January 29, 2020

§1.1 Review

Over the next few classes, we'll be doing a quick review of the prerequisites for the course. A **binary operation** on a set X is a function $\cdot : X \times X \to X$, typically written $a \cdot b$ instead of $\cdot(a, b)$. The familiar operations of addition, multiplication, subtraction, etc. on $\mathbf{Z}, \mathbf{R}$, etc. are examples of binary operations.

A binary operation $\cdot$ is **associative** if for all a, b, c then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. An **identity** for a binary operation on a set X is an element e such that for all $a \in X$, then $a \cdot e = e \cdot a = a$. The identity is always unique, since if e and e' are identities, then $e = e \cdot e' = e' \cdot e = e'$. An **inverse** for an element a is an element b such that $a \cdot b = e$, the identity.

A **group** is a set together with an operation that is associative, has an identity, and has inverses. Some examples are $(\mathbf{Z}, +), (\mathbf{R} - \{0\}, \cdot)$, and S_n, the set of functions from $\{1, \dots, n\}$ to itself, with the operation of addition. These first two examples are **abelian** (or **commutative**) groups, meaning $a \cdot b = b \cdot a$ for all a, b, and the symmetric group S_n is not.

We now define the primary objects of study for this course.

Definition 1.1 — A **ring** is a set R with two operations, $+, \cdot$, such that $(R, +)$ is an abelian group with identity 0, and $(R, \cdot)$ is associative with identity 1. The two operations must also satisfy **distributivity**, meaning $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a, b, c in the ring. If the operation $\cdot$ is commutative, then the ring is called a **commutative ring**. NB: we will always assume rings have a multiplicative identity.

Example 1.2

- The zero ring $(\{0\}, +, \cdot)$, with $1 = 0$.
- The familiar $\mathbf{R}, \mathbf{C}, \mathbf{Q}, \mathbf{Z}$ with addition and multiplication.
- The set of $n \times n$ matrices with entries in $\mathbf{R}$, with matrix addition and multiplication (note this ring is not commutative unless $n = 1$).
- The **quaternions** $a + ib + jc + kd$, with $a, b, c, d \in \mathbf{R}$. Addition is component by component, and multiplication is defined by the relations $i^2 = j^2 = k^2 = -1, ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$. You should check that these actually form a ring. Notice that this ring is not commutative, but it is an example of a **division ring** (or skew field), where $1 \neq 0$ and every nonzero element has a multiplicative inverse:
$$(a + ib + jc + kd)^{-1} = \frac{a - ib - jc - kd}{a^2 + b^2 + c^2 + d^2}.$$
- The ring $\mathbf{Z}/n\mathbf{Z}$, integers modulo n, defined as the set $\{0, \dots, n-1\}$ together with the operations of addition and multiplication modulo n. You should check that this is indeed a ring.

Definition 1.3 — A **field** is a commutative division ring ($1 \neq 0$). The sets $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields, but $\mathbf{Z}$ is not.

If we are working in a general ring R, a **unit** is an element $a \in R$ such that a has a multiplicative inverse. We write $R^\times$ for the set of unites. As an exercise, you should prove that $R^\times$ is always a group with the operation of multiplication. Note that 0 is never a unit.

Example 1.4

- $\mathbf{Z}^\times = \{1, -1\}$, since the only integers with integer inverses are 1 and -1.
- $\mathbf{Q}^\times = \mathbf{Z} - \{0\}$, since the only non-unit is 0.

A **zero divisor** a in a ring R is a nonzero element such that there exists some $b \neq 0$ with $ab = 0$ or $ba = 0$. Note, zero divisors are never units, since zero is not a unit. However, units aren't always nonzerodivisors, for example there are no zerodivisors in $\mathbf{Z}$, but many non-units.

Definition 1.5 — A **integral domain** is a commutative ring with $0 \neq 1$ and with no zero divisors. Note that any field is an integral domain.

The ring $\mathbf{Z}/n\mathbf{Z}$ is an integral domain if and only if n is prime. More generally, if $a \neq 0$ is an element of $\mathbf{Z}/n\mathbf{Z}$, then a is a zero divisor if and only if $\gcd(a, n) \neq 1$. Note that in this case, $\mathbf{Z}/n\mathbf{Z}$ is also a field if n is prime. In fact, we have the following theorem.

Theorem 1.6

Any finite integral domain R is a field.

Proof. Let $a \in R$ nonzero. Consider the function $f : R \to R$ defined as $x \mapsto ax$. The function f is injective, since in an integral domain $ab = ac$ implies $b = c$, for $a \neq 0$ (check this). Since f is an injective map from a finite set to itself, it is also surjective. Then there exists some $r \in R$ such that $f(r) = 1$, so $ar = 1$ and thus a is invertible. Since the arbitrary nonzero element a is invertible, then R is a field. □

§1.2 Course Overview

There are many applications of rings and fields in math. For example it is very useful for algebraic geometry (Math 137) and number theory (Math 129). There are also many applications outside of pure math in physics, computer science, and other fields.

One famous problem we will cover in this class is the problem of a formula for roots of 5th degree polynomials. There is the familiar quadratic formula for finding all the roots of 2nd degree polynomials, and also a less-familiar formula for 3rd and 4th degree polynomials. However, there is no such formula for 5th degree polynomials. We will prove that such a formula cannot exist using Galois theory in class. Although we don't have a formula to find roots of such polynomials, we can prove that roots exist, which is the content of the Fundamental Theorem of Algebra.

Another application of abstract algebra is to ruler and compass constructions (you might have done these in high school geometry). The Greeks were very into ruler and

compass constructions, and were able to construct many lengths and shapes. For example, although $\sqrt{2}$ is irrational, it can be constructed as the diagonal of a 1×1 square. However, talented the Greeks were at these constructions, they were never able to solve certain problems. For example, they could not "square the circle": given a circle of radius 1, can we construct a square with the same area? We will solve this ancient problem in this class and prove that it is not possible to do this. What does this have to do with algebra? Well, a real number x is called **constructible** if given a segment of unit length, we can construct a segment of length x using the unit segment. It turns out that if x and y are constructible, then so are $x+y$, $x\dot{y}$, $1/x$ and $\sqrt{x}$. It turns out that the constructible numbers form a field, so we can use our theory of fields to study geometric constructions. The circle squaring problem for example, boils down to showing that $\sqrt{\pi}$ is not constructible, which boils down to showing that π is transcendental. Some of the other problems of this nature we will solve are "doubling the cube," "trisecting the angle," constructing regular n-gons, and other problems. As a spoiler, we'll see that trisecting an arbitrary angle is impossible, doubling the cube is impossible, and the constructible regular n-gons are those with $n=2^r\cdot p_1\cdots p_k$, where the p_i are distinct Fermat primes and r is a nonnegative integer. Fermat primes are those of the form $2^{(2^m)}+1$. If you ever find yourself extremely bored, try constructing the regular 17-gon ($17=2^{2^2}+1$).

§2 February 5, 2020

§2.1 Ring Homomorphisms and Ideals

Today we will discuss how to construct new rings from old rings, which will give us more objects of study. The first such constructions are polynomial rings.

Given a ring R (usually commutative), let $R[x]$ denote the ring of polynomials with coefficients in R, which are formal sums of the form

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0.$$

The ring $R[x]$ is called the **polynomial ring** with coefficients in R.

NB: We do not regard these polynomials as functions. Instead, we think of them as *formal sums*. For example, consider $R=\mathbf{Z}/2\mathbf{Z}$, and the polynomials $p(x)=x^2$ and $q(x)=x$. Then $p(0)=0, p(1)=1, q(0)=0, q(1)=1$, so *as functions*, p and q are equal, but *as polynomials* they are not.

Although we usually like to think of polynomials as lists of coefficients, we can regard them as functions: if S is the ring of all functions from R to R, then the map $\varphi: R[x]\to S$ sending $p(x)\mapsto p(x)$, where the first $p(x)$ is a polynomial and the second is a function. You can check that $\varphi(p+q)=\varphi(p)+\varphi(q)$ and $\varphi(pq)=\varphi(p)\varphi(q)$. Notice that this map is not injective.

This leads us to the important definition of a ring homomorphism. Given a ring R and a ring S, a **ring homomorphism** is a function $\varphi: R\to S$ such that

$$\begin{aligned}\varphi(a+b)&=\varphi(a)+\varphi(b)\\ \varphi(ab)&=\varphi(a)\varphi(b)\\ \varphi(1_R)&=1_S.\end{aligned}$$

That is, the homomorphism must respect addition and multiplication and send the identities to the identities.

Note that the third condition in our definition of ring homomorphism doesn't follow from the first two. Consider $\varphi:\mathbf{Z}\to\mathbf{Z}$ defined by $\varphi: x\mapsto 0$ for all x. This satisfies the

first two properties, but $\varphi(1) = 0 \neq 1$. However, if we instead consider the zero map into the zero ring, $\varphi : \mathbf{Z} \to \{0\}$ defined by $\varphi : x \mapsto 0$, this *is* a ring homomorphism. In fact, for any ring R, there is a unique homomorphism $R \to \{0\}$.

Example 2.1

- The map $\varphi : \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$n \mapsto \begin{cases} 0, & n \text{ even} \\ 1, & n \text{ odd} \end{cases}$$

  is a ring homomorphism.

- For any ring S, there is a *unique* map $\varphi : \mathbf{Z} \to S$ given by $\varphi(1) = 1_S$, and $\varphi(n) = \underbrace{1_S + \cdots + 1_S}_{n\text{-times}}$.

- The evaluation at zero map, $\mathbf{Z}[x] \to \mathbf{Z}$, $p \mapsto p(0)$, is a ring homomorphism.

We say that a ring homomorphism is an **isomorphism** if it is bijective. If $\varphi : R \to S$ is a ring homomorphism, then the **kernel** of φ is

$$\ker(\varphi) := \{r \in R : \varphi(r) = 0\}.$$

The **image** of φ is

$$\operatorname{im}(\varphi) := \{s \in S : \varphi(r) = s, \text{ for some } S\}.$$

Observe that the image $\operatorname{im}(\varphi) \subseteq S$ of any ring homomorphism is a subring of S. Note however that the kernel is *not* always a subring, since it does not always contain 1. However, the kernel does have many interesting properties. It is closed under addition: if $a, b \in \ker(\varphi)$, then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$. It is also closed under multiplication by *any* element of the ring: if $r \in R$, and $a \in \ker(\varphi)$, then $\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$. These properties make the kernel into an ideal, which we now defined.

Definition 2.2 — An **ideal** in a ring R is a subset $I \subseteq R$ such that

- $0 \in I$,
- if $a, b \in I$ then $a + b \in I$,
- and if $a \in I$, and $r \in R$ (any element of the ring), then $ra \in I$.

Example 2.3

- The kernel $\ker(\varphi)$ is always an ideal, as discussed above.
- If R is a ring, then $\{0\}$ is an ideal.
- What are the ideals of $\mathbf{Q}$? Certainly $\{0\}$ and $\mathbf{Q}$ are ideals inside $\mathbf{Q}$. In fact, these are the only ideals. Since $\mathbf{Q}$, and any ideal is closed under multiplication by arbitrary elements of the ring, then the multiplicative identity 1 must be in the ideal. This implies that every element of $\mathbf{Q}$ is in the ideal. So in $\mathbf{Q}$, the only ideals are $\{0\}$ and $\mathbf{Q}$. In fact, if R is any division ring, then the only

ideals are $\{0\}$ and R.

- What are the ideals of $\mathbf{Z}$? The ideals must be additive subgroups, so we should first find these. The additive subgroups of $\mathbf{Z}$ are those of the form $n\mathbf{Z} = (n)$, the set of multiples of $n \in \mathbf{Z}$. Any additive subgroup is of this form, and additionally all these subgroups are ideals: if we multiply any $r \in \mathbf{Z}$ by $x \in (n)$, then $rx \in (n)$, since it is still a multiple of n.
- In the polynomial ring, the set of polynomials with zero constant and linear coefficient
$$I = \{a_n x^n + \cdots + a_0 : a_0 = a_1 = 0\}$$
is an ideal of $\mathbf{Z}[x]$.

§2.2 Quotients, Isomorphism Theorems, and Ideals

Now, if R is a ring and I is an ideal, then I is a normal subgroup of the group $(R, +)$, so it makes sense to define a quotient. The quotient group R/I with elements being equivalence classes of the form $r+I$, with multiplication defined by $(a+I)\cdot(b+I) := a\cdot b+I$. This makes R/I into a ring, which is called the **quotient ring**. In your homework, you will show that in order for this to be a ring, we do need that I is an ideal and not just some arbitrary additive subgroup.

The definition of the quotient ring R/I leads us to the definition of an important ring homomorphism. For any ring R and any ideal I, there is a homomorphism

$$\varphi : R \to R/I$$
$$\varphi : r \mapsto r + I.$$

This map is surjective, with kernel I. It is often called the *quotient map*.

Now that we have defined quotients, there are several theorems, similar to those for groups, about isomorphisms between quotient rings, called the **isomorphism theorems**.

Theorem 2.4 (First Isomorphism Theorem)
If $\varphi : R \to S$ is a ring homomorphism, then $R/\ker(\varphi) \simeq \mathrm{im}(\varphi)$.

Proof. By the first isomorphism theorem for groups, it is enough to check that the map

$$R/\ker(\varphi) \to \mathrm{im}(\varphi)$$
$$a + \ker(\varphi) \mapsto \varphi(a)$$

preserves multiplication. You should verify this as an exercise. □

There are more 'isomorphism theorems' for rings, but the first is the most important.

Example 2.5
Let $R = \mathbf{Z}[x]$, and
$$I = \{a_n x^n + \cdots + a_1 x + a_0 : a_0 = a_1 = 0\}.$$
In R/I, the $[x^3 + 5x + 2] = [x^3 + x^2 + 5x + 2] = [5x + 2] \neq [5x + 3]$, where the $[]$ denotes the equivalence class in R/I. That is, in R/I, we can think of $x^2, x^3, \ldots$ as being

zero. You can think of "modding out by an ideal" roughly as setting everything in the ideal equal to zero.

Since ideals are very useful for constructing quotients and other purposes, we would like to know how to construct ideals. For a ring R, and $A \subseteq R$, then the **ideal generated by** A is

$$J = \bigcap_{\text{ideals } I \supseteq A} I.$$

This is the smallest ideal which contains the set A. More concretely, this is equal to the set

$$\{\sum_i r_i a_i s_i : s_i \in A, r_i \in R, s_i \in R\}.$$

(We have to multiply by R on the left and right since our ring might not be commutative.) In the above, the sum is finite, which will typically be true for sums in this class. If the ring R is commutative, then this is just

$$\{\sum_i r_i a_i : r_i \in R, a_i \in A\}.$$

Some of the simplest ideals are those generated by one element. An ideal is called **principal** if it is generated by one element. We denote the ideal generated by an element a by (a). If R is commutative, then $(a) = \{ra : r \in R\}$.

Notice that in $\mathbf{Z}$, all the ideals are of the form $n\mathbf{Z} = (n)$. That is, all ideals are principal.

Example 2.6

Let $R = \mathbf{Z}[x]$, and let I be the set of polynomials with no constant or linear term $I = \{a_n x^n + \cdots + a_0 : a_0 = a_1 = 0\}$. The ideal I is generated by (x^2). For example, $x^3 + 5x^2 = (x+5)x^2$, so $x^3 + 5x^2 \in (x^2)$. As an exercise, you should prove that all the elements of I are in (x^2).

Also, notice that in $\mathbf{Z}[x]$, *not* all ideals are principal. For example, $(2, x)$ is not a principal ideal. For contradiction, suppose that $(2, x)$ is principal. Then $(2, x) = (a(x))$, for some $a(x)$, so $2 = p(x)a(x)$ for some polynomial $p(x)$, which means p and a are constant. This implies $a(x) = 1, -1, 2, -2$. But $a(x) \neq \pm 1$, since otherwise the ideal would be the entire ring. But $a(x) \neq \pm 2$, since $x \in (2, x)$ and $x \notin (\pm 2)$. This is a contradiction, and thus the ideal $(2, x)$ is not principal.

§3 February 7, 2020

§3.1 Types of Ideals

Last time we saw the example of $\mathbf{Q}$, a ring in which the only ideals are $\{0\}$ and $\mathbf{Q}$. Continuing this, we have the following proposition.

Proposition 3.1

If R is a commutative ring, with $0 \neq 1$, then R is a field if and only if the only ideals of R are $\{0\}$ and R.

Proof. We proved last time that if R is a field, then the only ideals of R are $\{0\}$ and R. For the other direction, let $0 \neq a \in R$, and let $I = (a)$. By assumption, $I = R$, so $1 \in (a)$. This means that there exists some $r \in R$ with $ra = 1$, so a is a unit. □

NB: the assumption that R is commutative is essential, as you can see in the following exercise.

Exercise 3.2. The ring $M_n(\mathbf{R})$ of $n \times n$ real-valued matrices has only $\{0\}$ and $M_n(\mathbf{R})$ as its ideals.

Corollary 3.3

If $\varphi : F \to S$ is a homomorphism from a field F to any set S is either constantly zero or injective.

Proof. The kernel $\ker(\varphi)$ is an ideal of F, so it is either $\{0\}$ or F. If it is F, then the map φ is the zero map, and if it is $\{0\}$, then φ is injective. □

Now we'll cover some important types of ideals. An ideal M is a **maximal ideal** if $M \neq R$, and $M \subseteq I \subseteq R$ implies $I = M$ or $I = R$ for any ideal I. That is, an ideal is maximal if it is not properly contained in any other ideal aside from the ideal R.

NB: The ring R is *not* a maximal ideal.

Example 3.4

- In $\mathbf{Z}$, the ideal (a) is maximal if and only if a is prime
- In a field, $\{0\}$ is a maximal ideal.
- The zero ring has no maximal ideal.

The following theorem is very useful for proving that rings are fields, or for proving that ideals are maximal.

Theorem 3.5

In a commutative ring R, an ideal M is maximal if and only if R/M is a field.

Proof. First we note the following fact: the ideals containing an ideal I in a ring R are in bijection with the ideals of R/I. This follows from one of the isomorphism theorems, and a proof can be found here. Using this, suppose that M is maximal. Then there are only two ideals containing M, namely M itself and R. Since the ideals of R containing M are in bijection with the ideals of R/M, this tells us that there are only two ideals in R/M, which must be $\{0\}$ and R/M. By proposition 3.1, this implies R/M is a field. The other direction of the proof uses the same fact and is similar. □

Remember that this only works for commutative rings. For noncommutative rings, all we can say is that if M is maximal, then R/M has no proper nontrivial two sided ideals (R/M is a simple ring).

Example 3.6

Consider the ring $\mathbf{Z}[x]$, and the ideal $(2, x)$. Then $\mathbf{Z}[x]/(2, x) \simeq \mathbf{Z}/2\mathbf{Z}$ is a field, so $(2, x)$ is maximal.

Another important type of ideal is the prime ideal. An ideal $P \subset R$ is a **prime ideal** if $a \cdot b \in P$ implies $a \in P$ or $b \in P$. In the integers $\mathbf{Z}$, the prime ideals are (p) for p prime or zero. For example, (4) is not prime, since $2 \cdot 2 \in I$, but $2 \notin I$.

Proposition 3.7

In a commutative ring R, an ideal P is prime if and only if R/P is an integral domain.

The proof is left as an exercise to the reader. As an example application, note that (x) in $\mathbf{Z}[x]$ is prime, since $\mathbf{Z}[x]/(x) \simeq \mathbf{Z}$, and $\mathbf{Z}$ is an integral domain. However, $\mathbf{Z}$ is not a field, so (x) is not maximal.

Since fields are integral domains, we have the following corollary.

Corollary 3.8

Any maximal ideal is prime.

Proof. If M is maximal, then R/M is a field. Since fields are integral domains, then R/M is an integral domain, so M is prime. □

§3.2 Fields of Fractions and Operations on Ideals

We now define another object which is useful in the study of rings: the field of fractions of a ring. This construction turn a ring into a field by adding inverses, as equivalence classes of elements of the ring.

Definition 3.9 — Given any integral domain R, the **field of fractions** of R is defined as follows. Let

$$F = \{(a, b) | a \in R, b \in R, b \neq 0\}.$$

Define an equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$ (intuitively $a/b = c/d$). Then the field of fractions is $Q = F/\sim$. Usually, for the equivalence class $[(a, b)]_\sim$ of the element (a, b), we just write $\frac{a}{b}$. We define addition and multiplication as

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

You can check that this is well defined, and that Q is a field. In addition, R embeds into Q via the map $r \mapsto \frac{r}{1}$.

The field of fractions of a ring R is the smallest field containing R. A slightly more general construction than the field of fractions is localization. We will not define localizations in this class, but you can read about them here.

Example 3.10

- The field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$.

- The field of fractions of $\mathbf{Z}[x]$ is the field of rational functions. That is, the set of objects of the form
$$\frac{p(x)}{q(x)},$$
where $p(x)$ and $q(x)$ are polynomials with coefficients in $\mathbf{Z}$.

Another important ring construction is the direct product. If R and S are rings, the **direct product** $R \times S$ is the set of pairs (r, s), where $r \in R$ and $s \in S$, and addition and multiplication are done componentwise.

We can also look at operations on ideals. The intersection $I \cap J$ of two ideals I and J is again an ideal. The **ideal sum** of two ideals I and J is defined as

$$I + J := \{a + b : a \in I, b \in J\},$$

and is an ideal. The **ideal product** of two ideals I and J is the ideal

$$I \cdot J := \{\sum_i a_i b_i : a \in I, b \in J\},$$

where as always, the sum is finite. An important thing to remember is that the ideal product is made up of *sums* of elements of the form $a \cdot b$, not just the products themselves. For example, the ideal $(a) \cdot (b)$ is the ideal $(a \cdot b)$, the ideal generated by $a \cdot b$. Recall that $(a \cdot b)$ contains more elements than just (element of (a))·(element of (b)).

Note that while the intersection of two ideals is again an ideal, the union of two ideals is not always an ideal.

It is easy to show that for any ideals I and J, the product is a subset of the intersection: $I \cdot J \subseteq I \cap J$. We can ask the question, when is $I \cdot J = I \cap J$? In $\mathbf{Z}$, if $I = (a)$ and $J = (b)$, then $(a) \cap (b) = (a) \cdot (b)$ if a and b are coprime. To generalize this, we need the following definition. Two ideals I and J in R are **comaximal** if $I + J = R$. In the integers for example, a and b are coprime if and only if there exist r, s with $ra + sb = 1$, which is true if and only if (a) and (b) are comaximal.

Theorem 3.11

If I and J are comaximal, then $I \cap J = I \cdot J$.

§3.3 Chinese Remainder Theorem

Instead of proving theorem 3.11, we prove the more general Chinese Remainder Theorem, from which the above fact follows.

Theorem 3.12 (Chinese Remainder Theorem)

Let R be a commutative ring with $0 \neq 1$, and let $A_1, \ldots, A_k$ be ideals. The map

$$\begin{aligned} \varphi : R &\to R/A_1 \times \cdots \times R/A_k \\ : r &\mapsto (r + A_1, \ldots, r + A_k), \end{aligned}$$

is a homomorphism with kernel $A_1 \cap \cdots \cap A_k$. Moreover, if A_i and A_j are comaximal, for all $i \neq j$, then φ is surjective, and $A_1 \cap \cdots \cap A_k = A_1 \cdots A_k$, so

$$R/A_1 \cdots A_k \simeq R/A_1 \times \cdots \times R/A_k.$$

As a consequence, let $R = \mathbf{Z}$, and let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. By the above, we have

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/p_1^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_k^{\alpha_k}\mathbf{Z}.$$

Then

$$(\mathbf{Z}/n\mathbf{Z})^\times = (\mathbf{Z}/p_1^{\alpha_1})^\times \mathbf{Z} \times \cdots \times (\mathbf{Z}/p_k^{\alpha_k}\mathbf{Z})^\times,$$

where the superscript $\times$ denotes the group of units. We also have $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$, where φ is the Euler Totient Function.

Proof. We proceed by induction on k, where $A_1, \ldots, A_k$ are comaximal. Suppose $k = 2$. Since A_1 and A_2 are comaximal, there exist $x \in A_1$ and $y \in A_2$ with $x + y = 1$, so $\varphi(x) = (0,1), \varphi(y) = (1,0)$. So given $(r,s) \in R/A_1 \times R/A_2$, then

$$\varphi(sx + ry) = (r,s),$$

so φ is surjective, as desired. Also, if $c \in A_1 \cap A_2$, then we have $c = c \cdot 1 = c(x+y) = xc + cy \in A_2A_1 + A_1A_2$, so $c \in A_1 \cdot A_2$ (the ring is commutative), thus $A_1 \cap A_2 \subseteq A_1 \cdot A_2$. Since $A_1 \cdot A_2 \subseteq A_1 \cap A_2$ for any ideals, then we have $A_1 \cdot A_2 = A_1 \cap A_2$, as desired.

The induction step is straightforward. □

February 12, 2020

§3.4 Integral Domains and PIDs

Last time we discussed different types of ideals, quotients, and integral domains. Recall that a maximal ideal is a proper ideal not contained in any other proper ideal. We now show that these actually exists

Proposition 3.13

For any ideal $I \subsetneq R$, there is a maximal ideal M such that $I \subseteq M \subsetneq R$.

Proof. If I is maximal, we are done. If I is not maximal, then there exists some $I_2 \supsetneq I$, with $I_2 \neq R$. If I_2 is maximal, we are done. Else, we can take $I_3 \supsetneq I_2$ with $I_3 \neq R$, and continue. Let $I_{\mathbf{N}} = \cup I_n$, which is an ideal. We can continue this process, and use Zorn's lemma to prove the proposition. □

Recall that in $\mathbf{Z}$, all ideals are of the form (a), for some $a \in \mathbf{Z}$. That is, all the ideals are principal. The integers are an example of a special type of ring which has this property.

Definition 3.14 — An integral domain in which all ideals are principal is called a **principal ideal domain (PID)**.

Definition 3.15 — A **Euclidean domain** is an integral domain R, together with a norm $N : R \to \mathbf{Z}_{\geq 0}$, where

- $N(0) = 0$, and
- $q = qb + r$ for some q, r with $r = 0$ or $N(r) < N(b)$. Note that the codomain of N is $\mathbf{Z}_{\geq 0}$, so norm are nonnegative.

Example 3.16

- The ring of integers $\mathbf{Z}$ is a Euclidean domain, with $N(a) = |a|$, the ordinary absolute value.
- Let F be a field. There are multiple ways to choose a norm to make F into a Euclidean domain. In fact, any norm N with $N(0) = 0$ works, since every element a is invertible and thus can be written $a = qb + r$, with $r = 0$. If F is a field, then $F[x]$, the polynomial ring with coefficients in F, is also a field. Take

$$N(p) = \begin{cases} \deg(p), & p \neq 0 \\ 0, & p = 0 \end{cases}.$$

  You can use polynomial division to verify that any element a can be written in the desired $a = qb + r$ form. Note, we need F to be a field in order that $F[x]$ be a Euclidean domain.
- The Gaussian integers $\mathbf{Z}[i] = \{a + bi : a, b, \in \mathbf{Z}\}$ are a Euclidean domain. Take $N(a + bi) = a^2 + b^2$.

Theorem 3.17

Any Euclidean domain is a PID.

Proof. Let I be an ideal, and $0 \neq b \in I$ have least norm. If $a \in I$, then $a = qb + r$. By minimality of the norm of b, then $N(a) = 0$, and thus $a = qb$. That is, any element of the ideal is a multiple of b, so $I = (b)$. Thus, every ideal is principal. □

Proposition 3.18

In a PID, any nonzero prime ideal is maximal.

Proof. Let (p) be a prime ideal, with $p \neq 0$. Let $(p) \subseteq I \subseteq R$, some ideal I. Then $I = (m)$ for some $m \in R$. Thus, $p = rm$ for some $r \in R$. Since (p) is prime, one of r or m must be in (p). If $m \in (p)$, then $(p) = (m)$, since $(p) \subseteq (m)$ and $(m) \subseteq (p)$, and thus (p) is maximal. If $r \in (p)$, then $r = sp$ for some s. Then $p = rm = spm$. Since R is an integral domain, then $sm = 1$, so m is a unit (has an inverse). Thus $I = (m) = (1)$ is the entire ring, so (p) is maximal. □

Corollary 3.19

For R a commutative ring, then $R[x]$ is a PID if and only if R is a field.

Proof. We've already shown that if R is a field, then $R[x]$ is an integral domain. For the other direction, suppose $R[x]$ is a PID. Since $R[x]$ is an integral domain and $R \subset R[x]$, then R is an integral domain. Since $R[x]/(x) \simeq R$ and R is an integral domain, then (x) is prime. Since every prime ideal in a PID is maximal, then (x) is maximal, and $R[x]/(x) \simeq R$ is a field, as desired. □

In the above proof, we used the fact that a subring of an integral domain is an integral domain. It's important to remember that this is *not* true for PIDs. For example, $\mathbf{R}[z]$ is PID, and $\mathbf{Z}[x] \subset \mathbf{R}[x]$ is a subring, but $\mathbf{Z}[x]$ is not a PID.

§3.5 Factorization

Let R be an integral domain. We say that $r \in R$ is **irreducible** if $r \neq 0$, r is not a unit, and if $r = ab$, then a or b must be a unit. We say that r is **prime** if (r) is prime. Concretely this means that if r divides ab, then r divides a or b.

Proposition 3.20
In an integral domain, all prime elements are irreducible.

Proof. Suppose that p is prime, and that $p = ab$ for some a, b. Then p divides a or p divides b. Without loss, say p divides a. Then $a = rp$ for some r. Then $p = rbp$, so $1 = rb$, so b is a unit, so p is irreducible. □

Consider the ring $R = \mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b, \in \mathbf{Z}\}$. In this ring, the element 3 is irreducible. To see this, suppose $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Then $3 = ac - 5bd$ and $ad + bc = 0$. The rest of the proof is casework. While 3 is irreducible, it is not prime, since 3 divides $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, but does not divide $2 + \sqrt{-5}$ or $2 - \sqrt{-5}$, so 3 is not prime. Thus, irreducible does not imply prime in general. However, in the case of PIDs, it does.

Proposition 3.21
In a PID R, an element is irreducible if and only if it is prime.

Proof. We already know that prime implies irreducible. Suppose that p is irreducible. Let $R \supseteq I \supseteq (p)$. Since R is a PID, then $I = (m)$, so $p = rm$ for some r. Since p is irreducible, then r or m is a unit. If m is a unit, then $(m) = I = R$. If r is a unit then $m = r^{-1}p$, so $(m) = (p)$, so (p) is maximal, and thus prime, so p is prime. □

Definition 3.22 — Two elements $a, b \in R$ are **associates** if $a = ub$ for some unit u.

From your homework, we know that a and b are associates if and only if $(a) = (b)$. Thus being associates is an equivalence relation. In $\mathbf{Z}$, the elements -2 and 2 are associates. In $\mathbf{Z}[i]$, the elements $5i$ and -5 are associates. In $\mathbf{R}[x]$, the elements x^2 and $\sqrt{2}x^2$ are associates.

Note that in general, factorization in a ring is not unique. For example, in $\mathbf{Z}[\sqrt{-5}]$, then $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Since factorization is important, we give a name to rings that do have unique factorization.

Definition 3.23 — A **unique factorization domain (UFD)** is an integral domain where every $r \neq 0$ with r not a unit satisfies:

- r is a product of irreducible elements,

- this product is unique up to associates. That is, if $r = p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and after reordering, then p_i and q_i are associates.

Exercise 3.24. In a UFD, an element is prime if and only if it is irreducible.

Theorem 3.25

Any principal ideal domain is a unique factorization domain.

Proof. We use that in a PID, and element is prime if and only if it is irreducible. We first prove uniqueness of factorization. Suppose $p_1 \cdots p_n = q_1 \cdots q_m$, for irreducibles p_i, q_i. Then the p_i, q_i are prime, so p_1 must divides some q_j, and without loss, say it divides q_1. Since q_1 is irreducible, then $q_1 = up_1$ for some unit u. Continue this reasoning for $p_2 \cdots p_n = q_2 \cdots q_m$.

To prove existence of factorization, suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a chain of ideals in a PID. Then for some n, $I_n = I_m$ for all $m \geq n$. To see why this is true, consider $I = \bigcup_n I_n$. Since we are in a PID, then $I = (a)$ for some a. But $a \in I_n$ for some $n \in \mathbf{N}$, by definition of I. Then for each $m \geq n$, $I_m \supseteq I_n$, so $a \in I_m$, and thus $I_m = I_n$.

Now, let r be an element of our PID. We show that $r = r_1 b$, for some irreducible r_1. If not, then $r = s_1 t_1$, and $s_1 = s_2 t_2$, and $s_2 = s_3 t_3$, etc. Consider the chain of primes $(r) \subsetneq (s_1) \subsetneq (s_2) \subsetneq \cdots$. This contradicts the fact about chains of prime ideals discussed above. Continue this reasoning for b, and we obtain that r is a product of irreducibles. □

§4 February 14, 2020 ♡

§4.1 Factorization in Polynomial Rings

Throughout the class today, all rings are commutative, and $0 \neq 1$. We begin with some definitions. The degree of a polynomial $p(x) = a_n x^n + \cdots + a_0 \in R[x]$ is the largest m such that $a_m \neq 0$. If $p = 0$, then the degree is not defined. A polynomial p is monic if $a_{\deg(p)} = 1$. You have probably used the following proposition before, and indeed it is very important.

Proposition 4.1

- If $p(x), q(x) \in R[x]$ are nonzero, then
$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)).$$
- The units of $R[x]$ are the units of R.
- The ring $R[x]$ is an integral domain
- If I is an ideal in R, then $(I) \subseteq R[x]$ is an ideal of $R[x]$, and is the set of polynomials with coefficients from I. Also, $R[x]/I \simeq (R/I)[x]$. In particular, if I is prime, then (I) is prime.

Exercise 4.2. Prove proposition 4.1.

We will prove later that R is a unique factorization domain if and only if $R[x]$ is. One direction is easy, and you should do it as an exercise.

Example 4.3

The polynomial ring $\mathbf{Z}[x]$ is a UFD. For example, $x^2 - 1 = (x-1)(x+1)$. But $\mathbf{Q}[x]$ is not a UFD, since for example $x^2 - 1 = (x-1)(x+1) = (\frac{1}{2}x - \frac{1}{2})(2x+2)$.

In the above example, we were able to factor a polynomial in $\mathbf{Q}[x]$ and in the ring $\mathbf{Z}[x]$. We can ask the question in general: if R is a UFD, F its field of fractions, and $p(x)$ is a polynomial which is reducible in $F[x]$, is it also reducible in $R[x]$. The answer to this is the content of Gauss' Lemma.

Lemma 4.4 (Gauss' Lemma)

Let R be a UFD, and F the field of fractions of R. Let $p(x)$ be a polynomial which is reducible in $F[x]$. Then $p(x)$ is also reducible in $R[x]$. Moreover, if $p(x) = A(x)B(x)$, where $A, B \in F[x]$, then $p(x) = a(x)b(x)$, where $a, b \in R[x]$ and $A(x) = ra(x), B(x) = sb(x)$, for some constants r, s. That is, the factorization in $R[x]$ is the same as the factorization in $F[x]$, except for possibly multiplication by some constant factors.

It might be helpful in the proof below (and in general when dealing with polynomial rings) to keep in mind the example of $R = \mathbf{Z}$ and $F = \mathbf{Q}$.

Proof. Say $p(x) = A(x)B(x)$, where $A, B \in F(x)$. Let $d \in R$ be a common denominator of all the coefficients of A and B. Then $dp(x) = a_1(x)b_1(x)$, where now $a_1, b_1 \in R[x]$. We are not quite done yet, since the left hand side, $dp(x)$, contains a factor of d, and we want just $p(x)$.

To accomplish this, we use the fact that we are working in a unique factorization domain to write $d = p_1 \cdots p_n$ (assuming d is not a unit). Let's divide both sides of $dp(x) = a_1(x)b_1(x)$ by p_1. That is, we reduce this expression modulo the ideal (p_1), to get

$$0 = \bar{a_1}(x)\bar{b_1}(x).$$

Since (p_1) is prime, then $R[x]/(p_1)$ is an integral domain, which means either $a_1 = 0$ or $b_1 = 0$. Thus, p_1 divides a_1 or b_1. Thus, after dividing both sides of $dp(x) = a_1(x)b_1(x)$ by p_1, the right hand side will still have coefficients in R. Continuing similarly for $p_2, \ldots, p_n$, we end up with $p(x) = a_n(x)b_n(x)$, where a_n and b_n have coefficients in R, as desired. □

For the converse, we can ask: if p is reducible in $R[x]$, is it also reducible in $F[x]$? This might seem to be obviously true because $R \subseteq F$, but it's actually not true, due to a subtlety in the definitions. As an example, $7x \in \mathbf{Z}[x]$ is reducible, since $7x = 7 \cdot x$. However, in $\mathbf{Q}[x]$, it is irreducible, since 7 is a unit in $\mathbf{Q}$. So the converse of the above is not true. However, if we impose some additional hypotheses, we can get a useful converses.

Corollary 4.5

If R is a UFD, F its field of fractions, and $p(x) \in R[x]$ a polynomial such that the gcd of the coefficients is 1, then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$.

Proof. The forward direction of the proof is Gauss' Lemma, which we proved above. For the other direction, suppose that $p(x)$ is reducible in $R[x]$. Then the factors have lower degree than p, so $p(x)$ is reducible in $F[x]$. □

Corollary 4.6

A ring R is a unique factorization domain if and only if $R[x]$ is.

Exercise 4.7. Prove corollary 4.6. Hint: use Gauss' Lemma.

The above discussion is very theoretical and abstract. What if we actually want to determine if a polynomial, like $x^4 + 1$ is irreducible in $\mathbf{Z}[x]$? To do this, we need some tools for computing things like this. An important thing to remember when factoring anything is that reducibility very much depends on the ring we're working in, as the examples below demonstrate.

Example 4.8

- The polynomial $x^2 + 1$ is irreducible in $\mathbf{R}[x]$, but reducible in $\mathbf{C}[x]$, as
$$(x + i)(x - i).$$
- The polynomial $x^2 - 2$ is irreducible in $\mathbf{Q}[x]$, but reducible in $\mathbf{R}[x]$, as
$$(x + \sqrt{2})(x - \sqrt{2}).$$

Proposition 4.9

If F is a field, then $p(x) \in F[x]$ has a root in F if and only if $p(x)$ has a linear (degree 1) factor.

Proof. First, if $p(x)$ has a linear factor, then we can write it as $p(x) = (x - \alpha)q(x)$, for $\alpha \in F$, so $p(\alpha) = 0$, so α is a root.

For the other direction, suppose $\alpha \in F$ is a root of p, so that $p(\alpha) = 0$. By polynomial division in $F[x]$, then $p(x) = (x - \alpha)q(x) + r(x)$, for some $r(x), q(x)$, and either $r = 0$ or $\deg(r) < \deg(x - \alpha)$. Thus, $r(x)$ must be a constant polynomial, but since$p(\alpha) = 0 = r(\alpha) = 0$, then $r(x)$ is the constantly zero polynomial. □

Corollary 4.10

A polynomial of degree n in $F[x]$ has at most n distinct roots.

Corollary 4.11 (Small degree reducibility check)
If $p(x) \in F[x]$ has degree 2 or 3, then $p(x)$ is reducible if and only if p has a root in F.

Proof. We know $p(x)$ is reducible if and only if p has a linear factor. Then apply corollary 4.10. □

Example 4.12
In $\mathbf{Q}[x]$, then $(x^2+1)(x^2+1) = x^4+2x^2+1$. Since x^2+1 is irreducible, this tells us that x^4+2x^2+1 has no roots in $\mathbf{Q}$.

Proposition 4.13 (Rational Roots Theorem)
If $p(x) = a_n x^n + \cdots + a_0 \in \mathbf{Z}[x]$ is a polynomial with a root of the form $\frac{r}{s} \in \mathbf{Q}$, and $\gcd(r,s) = 1$, then s divides a_n and r divides a_0.

Proof. Since $p(\frac{r}{s}) = 0$, then $a_n(\frac{r}{s})^n + \cdots + a_0 = 0$, which implies

$$a_n r^n + a_{n-1} s r^{n-1} + \cdots + s^n a_0 = 0,$$

by multiplying both sides by s^n. So

$$-a_n r^n = s(a_{n-1} r^{n-1} + \cdots + s^{n-1} a_0),$$

and similarly,

$$-a_0 s^n = r(a_n r^{n-1} + \cdots + a_1).$$

Because s and r have no common factors, then s divides a_n, and r divides a_0. □

Example 4.14
Let $p(x) = x^2 - 2$, and suppose that $\frac{r}{s}$ is a root. Then we must have $s = \pm 1$ and $r = \pm 1, \pm 2$. Checking each of these, we see that none of these are a root, and therefore $x^2 - 2$ has no roots in the rationals. Since $\sqrt{2}$ is a root of $x^2 - 2$, we have another proof that $\sqrt{2}$ is irrational.

More generally, $x^2 - p, x^3 - p$ are irreducible in $\mathbf{Q}[x]$ for any prime p. Now, for higher degree polynomials, Eisenstein's criterion will be very useful.

Proposition 4.15 (Eisenstein's Criterion)
let R be a UFD, and let P be a prime ideal in R. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $n > 0$ be a polynomial such that $a_{n-1}, a_{n-2}, \ldots, a_0 \in P$, but $a_0 \notin P^2$ and $a_n \notin P$. Then f is irreducible in $R[x]$.

Proof. Suppose that f is reducible. By Gauss lemma, there exists a factorization $f(x) = A(x)B(x)$ in $R[x]$. Since the leading coefficient of f is not in P, then reducing modulo P, we have

$$a_n x^n = \bar{A}(x)\bar{B}(x).$$

Since P is prime, then R/P is an integral domain. The only way that two polynomials over an integral domain can multiply to $a_n x^n$ is if each of the polynomials $\bar{A}(x)$ and $\bar{B}(x)$ is in fact a monomial. However, the degrees $\bar{A}$ and $\bar{B}$ must be positive, which means the constant terms of $\bar{A}$ and $\bar{B}$ are zero (in $(R/P)[x]$). The only way for this to be true is if the constant coefficients of A and B are both in P to begin with. But this implies that the constant term of $A(x)B(x) = f(x)$ is in P^2, a contradiction. Thus, f is irreducible. □

Exercise 4.16. In the above proof of Eisenstein's criterion, where did we use the fact that R is a UFD?

Eisenstein's criterion is very useful for showing that polynomials are irreducible, as the following example shows.

Example 4.17

The polynomial x^4+1 is irreducible in $\mathbf{Q}[x]$. To show this, first note that by making the change of variable $x \to x+1$, it is equivalent to show that $(x+1)^4+1$ is irreducible. But

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

which satisfies Eisenstein's criterion, with $P = (2)$, and is therefore irreducible. So x^4+1 is irreducible. This same trick can be used to show that cyclotomic polynomials of prime degree are irreducible. Note: $P = (2)$ is in $\mathbf{Z}$, not in $\mathbf{Q}$, and then the fact that the polynomial is irreducible in $\mathbf{Z}[x]$ implies it is irreducible in $\mathbf{Q}[x]$, by the contrapositive to Gauss' Lemma.

§5 February 19, 2020

§5.1 Modules

You are likely familiar with vector spaces over a field. The structure of a module over a ring is very similar, except that the field is replaced with a ring, and there are some slight changes in the definitions.

Definition 5.1 — Let R be a ring. A (left) **R-module** is an Abelian group $(M,+)$, together with a map $\psi : R \times M \to M$, which satisfies the following properties (where we write rm of $r \cdot m$ for $\psi(r,m)$):

- $(r_1 + r_2)m = (r_1 m) + (r_2 m)$, where $r_1, r_2 \in R$ and $m \in M$,
- $r(m+n) = rm + rn$, where $r \in R$ and $m, n \in M$,
- $r(sm) = (rs)m$, for $r, s \in R$ and $m \in M$, and
- $1m = m$, for any $m \in M$.

Example 5.2

If $R = F$ is a field, then an F-module is the same as a vector space over F.

Definition 5.3 — If M is an R-module, then an **R-submodule** of an R-module is a subset $N \subseteq M$ that is an Abelian subgroup closed under the ring action, i.e. if $r \in R$ and $n \in N$, then $rn \in N$.

Example 5.4

- Let R be a ring. It is an R module over itself, by left multiplication. If R is commutative, then the submodules of R are exactly the ideals of R. This is since ideals have to be closed by multiplication on both sides, and modules only have to be closed under multiplication on the left. If the ring is commutative, this distinction doesn't matter.
- For any $n \geq 1$, then $R^n := \underbrace{R \times \cdots \times R}_{n \text{ times}}$ is an R-module, with
$$r \cdot (a_1, \ldots, a_n) = (ra_1, \ldots, ra_n).$$
This is called the **free module over R** of rank n.
- We can also define the **direct product** or **direct sum** of two modules M_1 and M_2, written $M_1 \times M_2$ or $M_1 \oplus M_2$, with addition componentwise.

Now let's look at some of the rings we know, and see what modules look like over these rings. For example, what are the modules over $\mathbf{Z}$? Well, given any Abelian group $(A, +)$, we can make it into a $\mathbf{Z}$-module as follows. For $n \in \mathbf{Z}$, define

$$n \cdot a = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & n > 0 \\ 0, & n = 0 \\ \underbrace{-a - a - \cdots - a}_{n \text{ times}}, & n < 0 \end{cases}.$$

Now, to go the other way, if A is any $\mathbf{Z}$-module, then

$$n \cdot a = \underbrace{a + \cdots + a}_{n \text{ times}},$$

by the distributivity axiom and the fact that $n = \underbrace{1 + \cdots + 1}_{n \text{ times}}$ in $\mathbf{Z}$. Thus, any $\mathbf{Z}$-module is an Abelian group. That is, we have a correspondence:

$$\{\mathbf{Z} - \text{modules}\} \Leftrightarrow \{\text{Abelian Groups}\}$$
$$\{\mathbf{Z} - \text{submodules}\} \Leftrightarrow \{\text{Subgroups}\}.$$

Now, what are the $F[x]$-modules, where F is a field? Well, suppose we have an $F[x]$-module M. Then the action of F on $F[x]$ gives M the structure of an F-vector space V (since modules over fields are vector spaces). In addition, if we consider the action of *polynomials* on the vector space M, we get a linear transformation T, given by

$$T : V \to V$$
$$T : v \mapsto x \cdot v,$$

where here x is the polynomial in $F[x]$. You should check that this is a linear transformation of vector spaces (respects addition and scalar multiplication by elements of F). Now, what is x^2v? This is

$$\begin{aligned} x^2 \cdot v &= x \cdot (x \cdot v) \\ &= x \cdot (T(v)) \\ &= T(T(v)) \\ &= T^2(v). \end{aligned}$$

Generally, $x^n v = T^n(v)$, where $T^n = \underbrace{T \circ \cdots \circ T}_{n \text{ times}}$.

In summary, for any $F[x]$-module M, we get a vector space $V \sim M$ (from the action of F on M), and a linear transformation $T : V \to V$ (from the action of x on M).

Conversely, if V is a vector space over F, and $T : V \to V$ is a linear transformation, then we get an $F[x]$-module structure on V, by letting x act as $x \cdot v := T(v)$. Thus, we have a correspondence

$$\begin{aligned} &\{F[x] - \text{module}\} \Leftrightarrow \{F - \text{vector space } V \text{ and lienar map } T : V \to V\} \\ &\{F[x] - \text{submodules}\} \Leftrightarrow \{T - \text{invariant subspaces}\}. \end{aligned}$$

Now that we know about modules, we can understand our next major goal in this class: to study finitely generated R-modules over principal ideal domains, and prove a structure theorem about them.

§5.2 Module Homomorphisms and Quotients

Definition 5.5 — If M and N are R-modules, then an **R-module homomorphism** is a map $\varphi : M \to N$ such that

- $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ for $m_1, m_2 \in M$, and
- $\varphi(rm) = r \cdot \varphi(m)$ for $r \in R$ and $m \in M$.

Define isomorphism , kernel, image.

Now, suppose we have an R-module M, and an R-submodule N. Then we can define an R-submodule structure on the quotient group M/N by

$$r(m + N) := (rm) + N,$$

for $r \in R$. This is well defined: if $m + N = m' + N$, then $m - m' \in N$, by the definition of *group* quotient. So $r(m - m') \in N$, by closure of modules, and thus $(rm) + N = (rm') + N$. You should also check that the quotient gives an R-module.

The map $\varphi : M \to M/N$ defined by $m \mapsto m + N$ is a surjective module homomorphism with kernel N. Then similarly to what we did for rings, it is possible to prove the isomorphism theorems for modules.

Exercise 5.6. Prove the isomorphism theorems for modules.

Definition 5.7 — Let M be an R-module, and I be an ideal of R. We say that I **annihilates** M if $am = 0$ for all $a \in I$ and $m \in M$.

the concept of annihilation gives us another way to quotient. Suppose that M is an R-module and I is an ideal of R which annihilates M. Then M is an R/I-module, with structure given by

$$(r+I)\cdot m := r\cdot m,$$

where $(r+I) \in R/I$ and $m \in M$. You should check that this is well-defined.

Example 5.8

- Let $M = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, as a $\mathbf{Z}$-module. Let $I = (6) \subset \mathbf{Z}$. Then I annihilates M, so M is also a $\mathbf{Z}/(6\mathbf{Z})$-module.
- In the $\mathbf{Z}$-module $\mathbf{Z}/4\mathbf{Z}$, then $2\cdot 2 = 0$, where the first 2 is in $\mathbf{Z}$ and the second 2 is in $\mathbf{Z}/4\mathbf{Z}$. This *never* happens in vector spaces over fields, which gives us an example of an important way in which modules are really different from fields.

Definition 5.9 —

- Let M be an R-module. If N_1, N_2 are submodules, define the **module sum** as

$$N_1 + N_2 := \{n_1 + n_2 | n_1 \in N_1, n_2 \in N_2\}.$$

  Note that this is similar to the ideal sum (in fact, it's the same if the modules in question are ideals).

- Let $A \subseteq M$. Define the submodule **generated by** A as

$$RA := \{r_1a_1 + \cdots + r_na_n | a_1, \ldots, a_n \in A, r_1 \ldots, r_n \in R\}.$$

Definition 5.10 —

- A submodule N is **finitely generated** if $N = RA$ for some finite $A \subseteq N$.
- A submodule N is **cyclic** if $N = Ra := R\{a\}$, where $a \in N$ is some element.

Example 5.11

- If R is commutative, then an ideal of R is finitely generated as an ideal if and only if it is finitely generated as a module. Similarly, and ideal is principal as an ideal if and only if it is cyclic as a module.
- If $R = \mathbf{Z}$, then a subgroup is cyclic if and only if it is cyclic as a $\mathbf{Z}$-module.

Note that an F vector space is cyclic as a module if and only if it is one/zero-dimensional as a vector space. To see this, remember that one dimensional vector spaces are "generated" by one basis element.

Recall from above that we can treat a vector space V over F with a linear transformation T as an $F[x]$-module M. Then M is generated by $v \in V$ if and only if $v, T(v), T^2(v), \ldots$ spans V as a vector space.

Example 5.12

Now, suppose that $V = F^n$, and $T : V \to V$ is a "shift," given by

$$T(a_1, \ldots, a_n) = (a_2, \ldots, a_n, 0).$$

Then $T^k(e_n) = e_{n-k}$, for $0 < k < n$, where $\{e_i\}$ is the standard basis. So the module M over $F[x]$ given by V and T is cyclic, generated by e_n.

Theorem 5.13 (Structure Theorem, Weak Version)

Let M be a finitely generated R-module, where R is a principal ideal domain. Then M is a product of cyclic modules.

We will prove this structure theorem later.

Example 5.14

Suppose M is a cyclic R-module, generated by m. Examine the homomorphism $\varphi : R \to M$, defined by $r \mapsto rm$. This is surjective, since M is generated by m. By the isomorphism theorem, we have

$$R/\ker(\varphi) \simeq M = \operatorname{im}(\varphi).$$

Exercise 5.15. What is the kernel of the map $\varphi : r \mapsto rm$ in example 5.14 above?

§6 February 21, 2020

§6.1 Structure Theorem for Modules

Our goal is to prove that if R is a principal ideal domain, then any finitely generated R-module is a direct sum of cyclic modules. Recall from last lecture that if M_1, M_2 are R-modules, then the **direct product** is the module $M_1 \times M_2$, and is also called the (external) **direct sum**, written $M_1 \oplus M_2$. Recall from linear algebra that to simplify problems, we often like to write a vector space as a direct sum of subspaces. Similarly, we can ask: when is a module the direct sum of some submodules?

Proposition 6.1

Let M be an R-module, and $N_1, \dots, N_k$ submodules. Then the following are equivalent:

1. The map
$$\varphi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$$
$$\varphi : (a_1, \dots, a_k) \mapsto a_1 + \cdots + a_k,$$
is an isomorphism.
2. For all j, then
$$N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = \{0\}.$$
3. Any $x \in N_1 + \cdots + N_k$ can be written uniquely as $n_1 + \cdots + n_k$, for $n_i \in N_i$.

If $M = N_1 + \cdots + N_k$ and the conditions above hold, then we say that M is the **internal direct sum** of $N_1, \dots, N_k$, and write $M = N_1 \oplus \cdots \oplus N_k$. In this course, direct sums are direct sums, and you don't need to worry about interval/external.

Proof.

- (1) $\Rightarrow$ (2): Suppose that the map φ is an isomorphism, and that $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \neq \{0\}$. Then for some $a_j \in N_j$,
$$a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k,$$
where $a_i \in N_i$. So
$$a_1 + \cdots + a_{j-1} - a_j + a_{j+1} + \cdots + a_i = 0.$$
But this gives us a nonzero element in the kernel of φ, which means φ is not injective, a contradiction.

- (2) $\Rightarrow$ (3): Suppose that
$$x = n_1 + \cdots + n_k = n_1' + \cdots + n_k',$$
where $n_i, n_i' \in N_i$. Then we have
$$n_j - n_j' = (n_1' - n_1) + \cdots + (n_{j-1}' - n_{j-1}) + (n_{j+1}' - n_{j+1}) + \cdots + (n_k' - n_k).$$
But $(n_i - n_i') \in N_i$ for each i. But then we have an equation of the form
$$m_j = m_1 + \cdots + m_k,$$
where $m_i \in N_i$, which means $m_i = 0$ for each i by the zero intersection of property 2. Thus, $n_i - n_i' = 0$ for each i, and thus the representation of x is unique.

- (3) $\Rightarrow$ (1): Property 3 tells us that φ is injective, by uniqueness, and φ is always a surjective homomorphism.

□

Note, if $M = N_1 \oplus N_2$, then $M/N_1 \simeq N_2$.

Definition 6.2 — An R-module M is **free** on $A \subseteq M$ if for every $x \in M$, there exists a unique $a_1, \dots, a_n \in A$ and $r_1, \dots, r_n \in R$ such that $x = r_1 a_1 + \cdots + r_n a_n$. In the case that M is free, we call A a **basis** for M.

Now, M is free on $\{x_1, \dots, x_n\}$ if and only if $M = Rx_1 \oplus \cdots \oplus Rx_n$ and $x_1, \dots, x_n$ are non-torsion. Non-torsion means that $rx_i \neq 0$ if $r \neq 0$. Notice that $R \simeq Rx_i$, via the isomorphism $r \mapsto rx_i$ for each i. Then $M \simeq R^n$, by applying the isomorphism componentwise.

Now, we are starting to see that certain types of rings are very similar to vector spaces. Let us explore some more similarities between modules and vector spaces. Be very careful when comparing modules to vector spaces that you note the conditions on the rings. For example, in the below proposition, R is an integral domain.

Proposition 6.3

Let R be an integral domain, let $M = R^n$, and let $y_1, \dots, y_{n+1} \in M$. Then the y_i are linearly dependent, i.e. there exist $r_1, \dots, r_{n+1} \in R$ not all zero such that $r_1 y_1 + \cdots + r_{n+1} y_{n+1} = 0$.

Proof. Let F be the field of fractions of R. Then $M \subseteq F^n$, so by linear algebra, there exist

$$\frac{a_1}{b_1}, \dots, \frac{a_{n+1}}{b_{n+1}} \in F,$$

not all zero, with $a_i, b_i \in R$, such that

$$\frac{a_1}{b_1} y_1 + \cdots + \frac{a_{n+1}}{b_{n+1}} y_{n+1} = 0.$$

Now multiply by $b_1 \cdots b_{n+1}$, and the result follows. □

Definition 6.4 — For R an integral domain, the **rank** of a module is the largest n such that there are n linearly independent elements in M. If such n does not exist, then the rank is infinite. For example, R^n has rank n, and any submodule has rank $\leq n$.

In general, submodules of free modules are not always free. For example, let $R = \mathbf{Z}[x] = M$. Then M is free of rank 1, since the ring R is the same as the module. Let $N = (2, x)$, which is a submodule, and also has rank 1. However, N is not free. If N were free, then it would be isomorphic to R, which it is not, since it is not cyclic. However, if our ring R is a PID, then submodules are free, as we will now show.

Proposition 6.5

IF M is a free R-module of rank n, and R is an integral domain, then $M \simeq R^n$.

Proof. For some A, M is free on A. Since the rank is $n\infty$, then A is finite. Then $A = \{x_1, \dots, x_k\}$, so $M = Rx_1 \oplus \cdots \oplus Rx_k$ for some k, which means $M = R^k$. Since the rank of M is n then $k = n$. □

Theorem 6.6

Let R be a principal ideal domain, M a free R-module of rank n, and N a submodule. Then:

- The submodule N is free of rank $m \leq n$.
- There is a basis $y_1, \dots, y_m$ for M, and $a_1, \dots, a_m \in R$ not all zero, such that $a_1 y_1, \dots, a_m y_m$ is a basis for N and $a_1 | a_2 | \cdots | a_m$.

Example 6.7

- Let $R = \mathbf{Z}$, $M = \mathbf{Z} \times \mathbf{Z}$, and $N = 2\mathbf{Z} \times 3\mathbf{Z} \simeq \mathbf{Z} \times \mathbf{Z}$. Then N is free with basis $\{(2,0),(0,3)\}$.
- Let $M = \mathbf{Z} \times \mathbf{Z}$, and $N = \{(a,a) : a \in \mathbf{Z}\} \simeq \mathbf{Z}$. Then $N \neq N_1 \times N_2$ for any submodules N_1, N_2 of $\mathbf{Z}$.

Now we have all the tools we need for our main result. We first prove existence.

Theorem 6.8 (Structure Theorem, Existence)

Let R be a principal ideal domain, and M a finitely generated R-module. Then

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$

with $a_1 | a_2 | \cdots | a_m$, nonzero and non-unit.

In the above, we call r the **free rank** or **Betti number**, and $a_1, \dots, a_m$ are called the **invariant factors**.

Proof. Fix $x_1, \dots, x_n$ generators of M. Let $\varphi_i : R^n \to M$ be defined by $\varphi(e_i) = x_i$, where e_i is the i'th standard basis vector (1 in the i'th slot and zeros elsewhere). This is a surjective homomorphism, since the x_i generate M. By the first isomorphism theorem, $R^n/\ker(\varphi) \simeq M$. Apply theorem 6.6 to R^n and $\ker(\varphi)$ to get a basis $y_1, \dots, y_n$ of R^n and $a_1 | \cdots | a_m$ such that $a_1 y_1, \dots, a_m y_m$ is a basis of $\ker(\varphi)$. By definition, we have

$$R^n = Ry_1 \oplus \cdots \oplus Ry_n.$$

Then

$$\ker(\varphi) = Ra_1 y_1 \oplus \cdots \oplus Ra_m y_m \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-m}.$$

Note that $Ry_i/Ra_i y_i \simeq R/(a_i)$, for $i \leq m$, and $Ry_i/\{0\} \simeq R$ for $i > m$. Thus,

$$R^n/\ker(\varphi) \simeq R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

That finishes the proof. We now use the CRT to show that there is another form in which we can write the above theorem. If a_i is a unit, then $R/(a_i) = \{0\}$, so we can remove that module from the direct sum. Since a PID is a UFD, then each a_i can be written as a product of primes. Say $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the p_i are distinct. Then

$$R/(a) = R/(p_1^{\alpha})\cdots(p_k^{\alpha_k}) \simeq R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(P_k^{\alpha_k}),$$

where the second isomorphism holds by the Chinese remainder theorem. The $p_i^{\alpha_i}$ in the above equation are called the **invariant factors**. □

Exercise 6.9. Show that $Ry_i/Ra_iy_i \simeq R/(a_i)$, as stated in the above proof of theorem 6.8.

§7 February 26, 2020

§7.1 More Structure Theorem

Recall the structure theorem for finitely generated modules over PIDs. This says that if R is a PID, and M is a finitely generated R-module, then

(i)
$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m),$$
with $a_1 \mid a_2 \mid \cdots \mid a_m$ in R, nonzero, and nonunits. The a_i are called **invariant factors**.

(ii)
$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_k^{\alpha_k}).$$
The $p_i^{\alpha_i}$ are called **elementary divisors**.

Note that in the second case, with $p_1, \dots, p_k$ prime (not necessarily distinct), then they are unique. That is, two R-modules with are isomorphic if and only if they have the same free rank and invariant factors/elementary divisors.

Example 7.1

- We have
$$M = \mathbf{Z}_6 \simeq \mathbf{Z}^0 \oplus \mathbf{Z}_6 \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_3.$$
Then 2 and 3 are the elementary divisors (in invariant factor form).
- We have
$$M = \mathbf{Z}_6 \oplus \mathbf{Z}_{12} \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_3.$$
The elementary divisors are again $2, 4, 3, 3$.
- We have
$$M = \mathbf{Z}_6 \oplus \mathbf{Z}_{12} \simeq \mathbf{Z}_{2^3} \oplus \mathbf{Z}_{2^2} \oplus \mathbf{Z}_3,$$
so the elementary divisors are $2^2, 2^3, 3$. Now consider
$$\mathbf{Z}_{96} \simeq \mathbf{Z}_{2^5} \oplus \mathbf{Z}_3,$$
which has elementary divisors $2^5, 3$. This tells us that $\mathbf{Z}_6 \oplus \mathbf{Z}_{12} \not\simeq \mathbf{Z}_{96}$.

To summarize:

- To get the elementary divisors from the invariant factors, write the invariant factors as products of prime powers.
- To get the invariant factors from the elementary divisors, multiply the highest prime powers to get the highest invariant factor, and continue.

Example 7.2

Suppose the elementary divisors are $2, 2^2, 2^3, 5, 5^2$. The highest invariant factor is then $2^3 \cdot 5^2$. The next invariant factor is $2^2 \cdot 5$, etc.

We will not prove the uniqueness part of the Structure Theorem, because it is boring and just involves a lot of induction. Instead, we will talk about Tor and Ann

§7.2 Tor and Ann

Recall that $m \in M$ is called a **torsion** element if $rm = 0$ for some $r \neq 0$. Note that $m = 0$ *is* considered a torsion element. Then we define $\operatorname{Tor}(M)$ as the set of all torsion elements. A module M is said to be **torsion** if $\operatorname{Tor}(M) = M$, and is **torsion-free** if $\operatorname{Tor}(M) = \{0\}$.

Exercise 7.3. If R is an integral domain, show that $\operatorname{Tor}(M)$ is a submodule of M.

Now, let's apply the structure theorem: $M = R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. Then $\operatorname{Tor}(M) \simeq R/(a_1) \oplus \cdots \oplus R/(a_m)$, and $M/\operatorname{Tor}(M) \simeq R^r$. Intuitively, this follows from the fact that R^r has no zero divisors (the structure theorem applies when R is a PID), and a_i is zero in $R/(a_i)$.

Corollary 7.4

If R is a PID, and M is finitely generated, then M is torsion-free if and only if M is free.

Definition 7.5 — The **annihilator** of M is

$$\operatorname{Ann}(M) := \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Intuitively, it is the set of elements in R which "annihilate" all of M. The annihilator is an ideal of R.

Exercise 7.6. Prove that the annihilator, $\operatorname{Ann}(M)$, is an ideal of R.

Note, if M is not torsion, then $\operatorname{Ann}(M) = \{0\}$. If $M = R/(a_1) \oplus \cdots \oplus R/(a_m)$, then $\operatorname{Ann}(M) = (a_m)$. This is because $a_1 \mid \cdots \mid a_m$.

That is all that we will say about torsion and annihilators for now. We will now go back and prove the "key theorem" which we left out earlier.

§7.3 Key Theorem and Noetherian Modules

Our goal now will be to prove the "Key Theorem" from earlier that we skipped. In order to do so, we will make use of the following definition.

Definition 7.7 — Let R be a ring. An R-module M is said to be **Noetherian** if whenever $M_1 \subseteq M_2 \subseteq \cdots$ is an ascending chain of submodules, there is n such that for all $k \geq n$, then $M_k = M_n$. That is, any strictly increasing chain of submodules must eventually stop.

Exercise 7.8. Prove that all PIDs are Noetherian.

Theorem 7.9

The following are equivalent:

(i) M is Noetherian;

(ii) Any non-empty set Σ of submodules of M has a $\subseteq$-maximal element in Σ;

(iii) Any submodule of M is finitely generated.

Proof.

- ((i)⇒(ii)): Let $M_1 \in \Sigma$. If it is not maximal, take $M_1 \subsetneq M_2$. If M_2 is not maximal, take $M_2 \subsetneq M_3$. This has to stop at some point, since M is Noetherian. This tells us that Σ has some $\subseteq$-maximal element.
- ((ii)⇒(iii)): Let N be a submodule, and let Σ be the set of all finitely generated submodules of N. Note that $\Sigma \neq \varnothing$, since at least $\{0\} \in \Sigma$. So let $N' \in Sigma$ be maximal (with respect to set inclusion). If $N = N'$, then we are done, since then N is finitely generated. If $N \neq N'$, then pick $x \in N \setminus N'$. Let $A \subseteq N'$ generate N'. Then $A \cup \{x\}$ generates a proper extension of N' in Σ, which is a contradiction to the maximality assumption of N'.
- ((iii)⇒(i)): Let $M_1 \subseteq M_2 \subseteq \cdots$, and let

  $$N = \cup_{i=1}^{\infty} M_i.$$

  We know that N is generated by some finite $A \subseteq N$, by assumption. Pick n such that $A \subseteq M_n$. Then $M_k = N$ for all $k \geq n$, since it is also generated by A. Thus, the ascending chain condition is satisfied.

□

Now, we are ready to prove the key theorem. The proof involves a few steps, and is fairly technical. The general ideal is that we will take some arbitrary basis, and use projection maps and some clever homomorphisms to construct a basis that has the form in the theorem. To reiterate:

Theorem 7.10

Let R be a PID, M a free R-module of rank n, and N a submodule of M. Then N is free of rank $m \leq n$, and there is a basis $y_1, \ldots, y_n$ for M and $a_1 \mid \cdots \mid a_m$ in R such that $a_1 y_1, \ldots, a_m y_m$ is a basis for N.

Proof. Without loss of generality, we assume that $M = R^n$ and that $N \neq 0$. So there exists some basis $\{e_1, \ldots, e_n\}$ for M (not necessarily the desired one). Now let

$$\Sigma = \{\phi(N) \mid \phi : M \to R \text{ is a homomorphism}\}.$$

That is, Σ is the set of subsets of R which are images of N under some homomorphism. For each ϕ, then $\phi(N)$ is an R-submodule of R and thus an ideal. Thus, Σ is a subset of ideals of R, and nonempty, since we can choose ϕ to be a projection or the zero map. Then Σ is a nonempty set of ideals of R, which contains a maximal element, I, since R

is Noetherian. By the definition of Σ there exists some homomorphism $\nu : M \to R$ such that $I = \nu(N)$. Since R is a PID, then $I = \nu(N) = (a_1)$ for some a_1. Since $a_1 \in I$, there exists some $y \in N$ such that $\nu(y) = a_1$. Note that a_1 is nonzero.

Now, let ϕ be any homomorphism $M \to R$. We show that a_1 divides $\phi(y)$. Then consider the ideal $(a_1, \phi(y))$. Since R is a PID, this is equal to $(a_1, \phi(y)) = (d)$ for some element $d \in R$. Note in particular that $(a_1) \subseteq (d)$. Then by the definition of $(a_1, \phi(y))$, there exists some $r_1, r_2 \in R$ such that $r_1 a_1 + r_2 \phi(y) = d$.

We now define a homomorphism ψ by $\psi(x) := r_1 \nu(x) + r_2 \phi(x)$. As noted above, we then have $\psi(y) = d$, so that $d \in \psi(N)$, and thus $(d) \subseteq \psi(N)$. Then we have $(a_1) \subseteq (d) \subseteq \psi(N)$. By the definition of $I = (a_1)$ as maximal in Σ, then $(d) = (a_1)$, so a_1 divides $\phi(y)$, since (d) divides $\phi(y)$.

Now, we have shown that for $a_1 = \nu(y)$, then for any homomorphism $\phi : M \to R$, then a_1 divides $\phi(y)$. Now, define $\pi_i : R^n \to R$ be the map which sends an element $(x_1, \dots, x_n)$ to its i'th component (the i'th component being the component multiplied by e_i, the basis vector). Then a_1 divides $\pi_i(y)$ for each i, so we can write $\pi_i(y) = a_1 b_i$ for some $b_i \in R$. Then we can write $y = (a_1 b_1, a_1 b_2, \dots, a_1 b_n)$, by the definition of the π_i and the fact that $\pi_i(y) = a_1 b_i$. We can factor this to write $y = a_1(b_1, \dots, b_n)$. Define $y_1 = (b_1, \dots, b_n)$, so that $y = a_1 y_1$. Recalling ν from above, we have $a_1 = \nu(y) = \nu(a_1 y_1) = a_1 \nu(y_1)$. Since R is a PID and thus an integral domain, then $a_1 = a_1 \nu(y_1)$ implies $\nu(y_1) = 1$.

To proceed, we need to show the following:

$$M = Ry_1 \oplus \ker \nu$$
$$N = Ra_1 y_1 \oplus N \cap \ker \nu.$$

That is, we need to show that y_1 can be taken as a basis vector for M, and $a_1 y_1$ can be taken as a basis vector for N. To do this, suppose $m \in M$. Write

$$m = \nu(m) y_1 + (m - y_1 \nu(m)).$$

Then $\nu(m) y_1 \in Ry_1$, and $(m - y_1 \nu(m)) \in \ker \nu$, since

$$\nu(m - y_1 \nu(m)) = \nu(m) - \nu(y_1)\nu(m) = 0,$$

because $\nu(y_1) = 1$. So we have $M = Ry_1 + \ker \nu$. To verify that the sum is direct, we need to show that $Ry_1 \cap \ker \nu = \{0\}$. If $ry_1 \in \ker \nu$, then $\nu(ry_1) = \nu(r)\nu(y_1) = 0$, which implies $\nu(r) = r = 0$. Thus, the intersection is trivial. The verification that $N = Ra_1 y_1 \oplus N \cap \ker \nu$ is similar.

We now proceed by induction on n. That is, assume the result of the theorem is true up to $n - 1$. We write $M = Ry_1 \oplus \ker \nu$, and note that $\ker \nu$ has free rank less than n, which implies it is a free module with rank $n - 1$. By the induction hypothesis, then $\ker \nu$ has a basis $\{y_2, \dots, y_n\}$, where $\{a_2 y_2, \dots, a_m y_m\}$ is a basis for $N \cap \ker \nu$. With $a_2 \mid \cdots \mid a_n$. Then $\{y_1, \dots, y_n\}$ is a basis for M, and $\{a_1 y_1, \dots, a_m y_m\}$ is a basis for N.

All that remains is to verify that $a_1 \mid a_2$. This is left as an exercise to the reader. □

Exercise 7.11. Verify that $a_1 \mid a_2$ in the above proof of the key theorem. Hint: let $\phi : M \to R$ be a homomorphism such that if $(x_1, \dots, x_n) \in M$, then $\phi(x_1) = \phi(x_2) = 1$ and $\phi(x_i) = 0$ for $i \geq 2$. Then examine $\phi(a_i y_i)$, and show that $(a_1) \supseteq (a_2)$.

§8 February 28, 2020

§8.1 Structure Theorem and Linear Algebra

Today, we will apply the structure theorem for finitely generated modules over a PID in the special case where $R = F[x]$. Recall that polynomial rings over fields are PIDs, even though general polynomial rings are not.

The setup is the following. Fix a field F, a vector space V, and a transformation $T : V \to V$. Think of V as an $F[x]$ module, as we discussed earlier (with the action $x \cdot v := T(v)$). Assume that V is finite dimensional, $\dim(V) = n \geq 2$. Since V is finite dimensional, it is finitely generated as an F-module, and thus also finitely generated as an $F[x]$-module. So we can apply the structure theorem.

The free rank of V is 0. That is, V is torsion. To see this, we need to show that for any $v \in V$, there is an element of $F[x]$ which kills v. Look at the sequence $v, T(v), T^2(v), \dots, T^n(v)$. This gives us $n+1$ vectors in V, which must be linearly dependent. So there are $a_0, \dots, a_n$, such that

$$r_0 v + r_1 T(v) + \cdots + r_n T^n(v) = 0.$$

But this tells us that

$$(r_0 + r_1 x + \cdots + r_n x^n)v = 0,$$

by how we defined the action of x^i on the vector space. This gives us an element of the ring $R = F[x]$ which kills v, which implies V has free rank 0.

Using this, we can write

$$V \simeq F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_m(x)).$$

We want to understand what each of the $F[x]/(a_i(x))$ look like. So let's consider $F[x]/(a(x))$, for some arbitrary polynomial $a(x)$ of degree $k \geq 1$. We can assume that $a(x)$ is monic, and write $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0$. Thus, $F[x]/(a(x))$ is an $F[x]$-module, and also an F-module of dimension k. A basis is $1, \bar{x}, \dots, \bar{x}^{k-1}$. The linear transformation $v \mapsto x \cdot v$ acts on this new module as

$$\begin{aligned} 1 &\mapsto \bar{x} \\ \bar{x} &\mapsto \bar{x}^2 \\ &\vdots \\ \bar{x}^{k-1} &\mapsto \bar{x}^k = -b_{k-1}\bar{x}^{k-1} - \cdots - b_0. \end{aligned}$$

Using this, we can write the matrix of this map as

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & -b_0 \\ 1 & 0 & 0 & \cdots & -b_1 \\ 0 & 1 & 0 & \cdots & -b_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -b_{k-1} \end{pmatrix}.$$

This matrix is written $C_{a(x)}$, and is called the **companion matrix** of $a(x)$. For the a_i in the decomposition above, let $C_{a_i(x)}$ be the companion matrix of $a_i(x)$ with corresponding basis $\mathcal{B}_i$. Then we can concatenate the $\mathcal{B}_i$ into a basis $\mathcal{B}$ for V, and write the matrix for T in block form

$$\begin{pmatrix} C_{a_1(x)} & 0 & \cdots & 0 \\ 0 & C_{a_2(x)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_{a_m(x)} \end{pmatrix}.$$

This matrix is called the **rational canonical form** of T.

Now, let's go over some connections to eigenvalues from linear algebra. We begin with a definition which might be familiar.

Definition 8.1 — The **characteristic polynomial** of T is $c_T(x) = \det(xI - A)$, where A is any matrix for T. Recall that λ is an eigenvalue for T if and only if $c_T(\lambda) = 0$, and that $c_T(x)$ has degree n (the dimension of the vector space), and is monic.

For the companion matrix above, the characteristic polynomial is

$$b_0 + b_1 x + \cdots + x^k.$$

Exercise 8.2. Use expansion by cofactors to show that the characteristic polynomial for $C_{a(x)}$ is $b_0 + b_1 x + \cdots + x^k$.

That is, $c_{C_{a(x)}} = a(x)$. Since the determinant of a block matrix is the product of the determinants of the blocks, then the characteristic polynomial of T is

$$a_1(x)a_2(x)\cdots a_m(x),$$

the product of the invariant factors. In particular, $a_m(x)$ divides $c_T(x)$. Since $a_m(x)$ generates the annihilator of V, then $a_m(T) = 0$, and thus $c_T(T) = 0$. (This is the **Cayley-Hamilton** theorem for vector space linear transformations).

Now, suppose that each $a_i(x)$ factors as a product of linear polynomials (as is the case if $F = \mathbf{C}$). Then the elementary divisors look like $(x - \lambda)^k$. The product of the elementary divisors is the characteristic polynomial, which tells us that the λ are roots of the characteristic polynomial, and thus an eigenvalue.

Now, look at $F[x]/((x - \lambda)^k)$. Consider $\{1, \bar{x} - \lambda, \ldots, (\bar{x} - \lambda)^{k-1}$. This is a basis for $F[x]/((x - \lambda)^k)$, which you can check by defining a bijective map to the basis $\{1, \bar{x}, \ldots, \bar{x}^{k-1}\}$.

What does T do to the basis? We have

$$\begin{aligned} T : (\bar{x} - \lambda)^{k-1} &\mapsto x(\bar{x} - \lambda)^{k-1} = \lambda(\bar{x} - \lambda)^{k-1} \\ (\bar{x} - \lambda)^{k-2} &\mapsto (\bar{x} - \lambda)^{k-1} + \lambda(\bar{x} - \lambda)^{k-2}, \end{aligned}$$

and similarly for the rest of the terms. Thus, we can write out the matrix for T in this basis:

$$J_\lambda = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

This is called a **Jordan block**, J_λ. Now, remember that

$$V \simeq F[x]/(x - \lambda_1)^{k_1} \oplus \cdots \oplus F[x]/(x - \lambda_t)^{k_t},$$

so we can write the matrix of T on the concatenated basis $\mathcal{B}$ as

$$\begin{pmatrix} J_{\lambda_1} & 0 & 0 & \cdots & 0 \\ 0 & J_{\lambda_2} & 0 & \cdots & 0 \\ 0 & 0 & J_{\lambda_3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & J_{\lambda_t} \end{pmatrix},$$

which is known as the **Jordan Normal Form** for the transformation T. Notice that T diagonalizable if and only if $K_1 = 1$ for all i, which is true if and only if the elementary divisors are irreducible.

Also, note that we assumed earlier that each $a_i(x)$ factors as a product of linear polynomials. This is not always possible if our field is not algebraically closed: we need the characteristic polynomial to split into linear factors. If we are working over $\mathbf{R}$, we can get close to Jordan normal form, but not always exactly. If you are interested, see the Wikipedia page for Jordan Normal Form.

§9 March 4, 2020

§9.1 Field Theory

Recall that a **field** is a commutative ring with $0 \neq 1$ such that every nonzero element is a unit. The **characteristic** of a field F, written $\operatorname{char}(F)$, is the least $n \geq 1$ such that $\underbrace{1_F + \cdots + 1_F}_{n} = 0$, or $n = 0$ if this never happens. The reals $\mathbf{R}$, rationals $\mathbf{Q}$, and complexes $\mathbf{C}$ have characteristic zero. The characteristic of $\mathbf{Z}/p\mathbf{Z}$ is p.

Recall that there is a unique homomorphism $\varphi : \mathbf{Z} \to F$, and $\operatorname{char}(F)$ is the unique $n \geq 0$ such that $\ker(\varphi) = (n)$, the ideal generated by n. The following definition should be familiar from your homework.

Definition 9.1 — The **prime subfield** of a field F is the intersection of all subfields of F. This is "the smallest subfield of F."

Exercise 9.2. The prime subfield is isomorphic to either $\mathbf{Q}$ or $\mathbf{Z}/p\mathbf{Z}$ if $\operatorname{char}(F) = 0$ or $p \neq 0$, respectively.

Exercise 9.3. If $\operatorname{char}(F) \neq 0$, then $\operatorname{char}(F)$ is prime.

Example 9.4

The prime subfield of $\mathbf{Q}$ is $\mathbf{Q}$. The prime subfield of $\mathbf{R}$ is $\mathbf{Q}$. The prime subfield of $\mathbf{C}$ is $\mathbf{Q}$. Let $\mathbf{F}_p(x)$ be $\mathbf{F}_p$ adjoined x, the field of fractions of $\mathbf{F}_p[x]$ (note the square vs curved braces). The elements of $\mathbf{F}_p(x)$ are of the form $p(x)/q(x)$, where p, q are polynomials with $q \neq 0$. The prime subfield is the ring of constant polynomials in $\mathbf{F}_p[x]$.

Definition 9.5 — If K is a field and F is a subfield of K (so that $F \subset K$), then we say that K is an **extension** of F. We write this as K/F, and it is pronounced "K over F." NB: this notation does *not* mean that we are quotienting. Sometimes we call F the **base** of the extension.

Note that an extension K/F is a vector space over F. The **degree** of K/F, written $[K : F]$ (or sometimes $\deg_F K$) is the dimension of K as an F-vector space. We say that K/F is **infinite** if $[K : F]$ is infinite, and **finite** otherwise.

Exercise 9.6. Show that

- $[\mathbf{C} : \mathbf{R}] = 2$,
- $[\mathbf{R} : \mathbf{Q}]$ is infinite,
- $[\mathbf{F}_p(x) : \mathbf{F}_p]$ is infinite. Note that this is $\mathbf{F}_p(x)$ and not $\mathbf{F}_p[x]$. The latter is not a field.

For most of this class and today, we will be dealing with finite field extensions. The setup for today is the following: suppose we have a field F and a polynomial $p(x) \in F[x]$ of degree ≥ 1. We want to find a field extension of F with a root for $p(x)$. For example, if our field is $\mathbf{R}$, and our polynomial is $p(x) = x^2 + 1$, then $\mathbf{C}$ is a field extension with a root for $p(x)$ (namely i).

We assume without loss that $p(x)$ is irreducible. The following theorem shows us that this we can always find this root containing field extension.

Theorem 9.7 (Existence of Extensions)

If F is a field, and $p(x) \in F[x]$ is irreducible of degree $n \geq 1$, then there exists a field extension K of F, and $\alpha \in K$ such that $p(\alpha) = 0$.

Proof. Consider $F[x]/(p(x))$, and let $\alpha = x \mod (p(x))$. Note that because $p(x)$ is irreducible, then $F[x]/(p(x))$ is a field. That is, α is the image of x under $F[x] \to F[x]/(p(x))$. Then $p(\alpha) = 0$. Consider the composite homomorphism

$$\varphi : F \xrightarrow{\iota} F[x] \xrightarrow{q} F[x]/(p(x)).$$

We want to show that φ is injective, so that it embeds into $F[x]/(p(x))$ ("embeds" means that there's a copy of F sitting inside of $F[x]/(p(x))$, i.e. the image of φ is a field). To see that φ is injective, note that $\varphi(1) = 1 \mod p(x) \neq 0$, so $\ker(\varphi) \neq F$. Since $\ker(\varphi)$ is an ideal, then $\ker(\varphi) = \{0\}$. Thus, φ is injective.

We have that F embeds into $F[x]/(p(x))$. Then identify $\varphi(F)$ with F, so $F[x]/(p(x))$ is indeed an extension of F, and has a root for $p(x)$. □

Theorem 9.8

If $p(x)$ is irreducible in $F[x]$, with degree $n \geq 1$, then

$$[F[x]/(p(x)) : F] = n.$$

Exercise 9.9. Prove theorem 9.8. Hint: a basis for $F[x]/(p(x))$ as a vector space is $\{1, \bar{x}, \ldots, \bar{x}^{n-1}\}$.

Example 9.10

Let $F = \mathbf{Q}$, and $p(x) = x^3 - 2$. Then a basis for $F[x]/(x^3 - 2)$ over F is $1, \bar{x}, \bar{x}^2$.

If K/F is a field extension, and $A \subseteq K$, the the intersection of all fields containing both A and F is called the **field generated by A over F**, and is denoted $F(A)$ (note that A doesn't have to be a field - in fact usually it isn't). If A has one element a, we write $F(a)$ instead of $F(\{a\})$, and often say that $F(a)$ is "F adjoined a." Extensions of this form are called **simple extensions**.

Example 9.11

Let $K = \mathbf{C}$ or $\mathbf{R}$. Then

$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}.$$

You should check that this is in fact a field.

Using this notation, we now show that the root containing extension from above is in fact unique (i.e. we can talk about "the smallest field" that contains roots).

Theorem 9.12 (Uniqueness of Extensions)

Let F be a field, and $p(x) \in F[x]$ an irreducible polynomial of degree $n \geq 1$. Let K/F be a field extension with a root α for $p(x)$. Then

$$F(\alpha) \simeq F[x]/(p(x)).$$

Proof. Define $\varphi : F[x] \to F(\alpha)$ by $\varphi(x) = \alpha$, and $\varphi(1) = 1$. This is a homomorphism which we will use to construct an isomorphism between the two fields. Note that $\varphi(p(x)) = p(\alpha) = 0$, so $p(x) \in \ker(\varphi)$, so that $(p(x)) \subseteq \ker(\varphi)$. Thus, the map

$$\varphi' : F[x]/(p(x)) \to F(\alpha)$$

given by $\varphi'(q(\alpha) \mod p(x)) = \varphi(q(x))$ is a well defined map of fields. Since $\varphi' \neq 0$, then $\ker(\varphi') \neq F[x]/(p(x))$, so $\ker(\varphi') = \{0\}$ since it is an ideal in a field, and thus φ' is injective.

Now to see that φ' is surjective, consider $\mathrm{im}(\varphi')$. This is a subfield of $F(\alpha)$, $\mathrm{im}(\varphi) \subseteq F(\alpha)$. In addition, $F \subseteq \mathrm{im}(\varphi')$, since $\varphi'(\bar{a}) = a$, so $a \in \mathrm{im}(\varphi')$ for any $a \in F$. Since $\varphi'(\bar{x}) = \alpha$, then $\mathrm{im}(\varphi')$ is a subfield of $F(\alpha)$ which contains F and α. By definition of $F(\alpha)$ as the minimal such field extension, this tells us that $\mathrm{im}(\varphi')$ must contain $F(\alpha)$. Then $F(\alpha) \subseteq \mathrm{im}(\varphi') \subseteq F(\alpha)$, and $\mathrm{im}(\varphi') = F(\alpha)$, so φ' is the desired isomorphism. □

Example 9.13

Let $F = \mathbf{Q}$ and $K = \mathbf{C}$. Let $p(x) = x^2 - 2$. Then $\sqrt{2}$ and $\sqrt{-2}$ are roots of $p(x)$ in $\mathbf{C}$. By the theorem, then $\mathbf{Q}(\sqrt{2}) \simeq \mathbf{Q}[x]/(p(x)) \simeq \mathbf{Q}(-\sqrt{2})$, via the maps $a + b\sqrt{2} \mapsto a + b\bar{x} \mapsto a - b\sqrt{2}$.

Note especially that $\mathbf{Q}(\sqrt{2}) \simeq \mathbf{Q}(-\sqrt{2})$. Then $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbf{Q}(\sqrt{2})$, which leaves $\mathbf{Q}$ fixed. We'll see this sort of thing come up later in Galois theory.

Example 9.14

Let $F = \mathbf{Q}$, $K = \mathbf{C}$, and $p(x) = x^3 - 2$. The roots are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}e^{2\pi i/3}$, and $\alpha_3 = \sqrt[3]{2}e^{4\pi i/3}$. By the theorem, then $\mathbf{Q}(\alpha_1) \simeq \mathbf{Q}(\alpha_2) \simeq \mathbf{Q}(\alpha_3)$. But note that these aren't necessarily equal. In particular, $\mathbf{Q}(\alpha_1) \subseteq \mathbf{R}$, but $\mathbf{Q}(\alpha_2) \not\subseteq \mathbf{R}$.

§10 March 6, 2020

For those of you who are reading these lecture notes because you didn't come to class, please see: here, here, and here. This still applies to zoom lectures.

§10.1 Field Theory

Let us return to the example from last time, where $F = \mathbf{Q}, K = \mathbf{C}$, and $p(x) = x^3 - 2$. The roots are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}e^{2\pi i/3}$, and $\alpha_3 = \sqrt[3]{2}e^{4\pi i/3}$. Note that $\mathbf{Q}(\alpha_1) \simeq \mathbf{Q}(\alpha_2) \simeq \mathbf{Q}(\alpha_3))$. However, $\mathbf{Q}(\alpha_1) \neq \mathbf{Q}(\alpha_2)$, since $\mathbf{Q}(\alpha_1) \subseteq \mathbf{R}$ and $\mathbf{Q}(\alpha_2)$ contains elements with imaginary components.

In addition, $\mathbf{Q}(\alpha_2) \neq \mathbf{Q}(\alpha_3)$. To see why this is true, suppose that they are equal, so that $\mathbf{Q}(\alpha_2) = \mathbf{Q}(\alpha_3) = L$. Then $\alpha_2\alpha_3 = \sqrt[3]{4} \in L$. So $\sqrt[3]{4}\alpha_2 = 2e^{2\pi i/3} \in L$ and thus $e^{2\pi i/3} \in L$. This implies $\alpha_2/(e^{2\pi i/3}) = \sqrt[3]{2} \in L$. This implies that $\mathbf{Q}(\alpha_1) \subsetneq \mathbf{Q}(\alpha_2) = L$. But this is false, since $\mathbf{Q}(\alpha_1)$ and L both have degree 3 over $\mathbf{Q}$, and this would mean that we have a three dimensional vector space which is a strict subset of another three dimensional vector space.

For another proof that $\mathbf{Q}(\alpha_2) \neq \mathbf{Q}(\alpha_3)$, again suppose that $\mathbf{Q}(\alpha_2) = \mathbf{Q}(\alpha_3)$. Let $\varphi : \mathbf{Q}(\alpha_2) \to \mathbf{Q}(\alpha_1)$ be an isomorphism, with $\varphi(\alpha_2) = \alpha_1$, which is possible since they are isomorphic. Then examine $\varphi(\alpha_3)$. For any $r \in \mathbf{Q}$, then $\varphi(r) = r$. Since $p(\alpha_3) = p(\varphi(\alpha_3)) = p(\alpha_1) = 0$, then either $\varphi(\alpha_3) = \alpha_1$ and φ is not injective, or $\varphi(\alpha_3) = \alpha_2 \notin \mathbf{Q}(\alpha_1)$. In either case, we have a contradiction.

Notice that in the first proof, we actually showed that $\mathbf{Q}(\alpha_2, \alpha_3) = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$. The field $\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$ is known as the *splitting field* of p. We will discuss splitting fields more later.

Definition 10.1 — Let K be a field extension of F. We say that $\alpha \in K$ is **algebraic over** F if α is the root of some nonzero polynomial $p \in F[x]$. We say that K/F is **algebraic** if all $\alpha \in K$ are algebraic over F. If α is not algebraic over F, it is called **transcendental**.

Example 10.2

Let $K = \mathbf{C}$ and $F = \mathbf{Q}$. Then $i, \sqrt{2}, \sqrt[3]{2}$ are algebraic. The numbers e and π are transcendental, which follows from the Lindemann Weierstrass Theorem.

The field $\mathbf{C}$ is algebraic over $\mathbf{R}$, and is equal to $\mathbf{C} = \mathbf{R}(i)$.

Lemma 10.3

Let K/F be an extension, and $\alpha \in K$ be algebraic. Then there is a unique monic polynomial $m(x) = m_{\alpha,F}(x) \in F[x]$ of least degree such that α is a root of m. Moreover, if α is a root of any $f \in F[x]$, then m divides f. The polynomial $m(x)$ is known as the **minimal polynomial of** α **over** F. This polynomial is irreducible.

Proof. Let $g(x) \in F[x]$ have least degree such that $g(\alpha) = 0$. Dividing by a unit, we can assume that g is monic. Suppose that $f \in F[x]$ also satisfies $f(\alpha) = 0$. We can write $f(x) = g(x)q(x)+r(x)$, with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Then $0 = f(\alpha) = 0+r(\alpha)$, so $r(\alpha) = 0$. If $\deg(r(x)) = 0$, then it must be constantly zero. If $\deg(r(x)) > 0$, then $\deg(r(x)) < \deg(g(x))$, so $r(x)$ is a polynomial with α as a root which has degree lower than the degree of $g(x)$, which is a contradiction to the minimality assumption on the

degree of $g(x)$. Thus, g divides f. If f is monic and of the same degree as f, then inverting the above argument shows that f divides g. □

Note that the minimal polynomial depends on the base field. For example the minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{Q}$ is $x^3 - 2$. However, the minimal polynomial of $\sqrt[3]{2}$ over $\mathbf{R}$ is just $x - \sqrt[3]{2}$. In general, it we have a minimal polynomial for some α over a bigger field, then it must divide the minimal polynomial for the same α over the smaller field.

§10.2 Algebraic Extensions

We now turn our attention to algebraic extensions, which will typically be the only types of extensions we'll consider in this course.

Proposition 10.4

The extension $F(\alpha)/F$ is finite if and only if α is algebraic over F. Recall that $F(\alpha)/F$ being finite means that $[F(\alpha) : F]$ is finite.

As an example, $\mathbf{C} = \mathbf{R}(i)$ is finite, since i is algbraic over $\mathbf{R}$.

Proof.

- ($\Rightarrow$): Suppose that $F(\alpha)/F$ is finite, and that $1, \alpha, \ldots, \alpha^n$ are linearly dependent. Then $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ for $a_i \in F$, not all zero. Then let $p(x) = a_0 + \cdots + a_n x^n$. This polynomial has α as a root, so α is algebraic over F.
- ($\Leftarrow$): We know that $F(\alpha)/F$ has degree equal to the degree of the minimal polynomial of α.

□

Corollary 10.5

If K/F is a finite extension, then it is algebraic.

Proof. Apply proposition 10.4 to every $\alpha \in K$. □

Example 10.6

- The extension $\mathbf{C}/\mathbf{R}$ is algebraic.
- The extension $\mathbf{R}/\mathbf{Q}$ is *not* algebraic, using the fact that e, π are transcendental, so $\mathbf{R}/\mathbf{Q}$ is an infinite extension.
- The extension $\mathbf{F}_p(x)/\mathbf{F}_p$ is not algebraic, since x is transcendental. Thus the extension is infinite.

We will mostly be concerned with algebraic extensions in this class. The simplest algebraic extensions are obtained by adjoining one element. We can also adjoin two elements, three elements, etc. It is useful to know how the degree of the extensions changes as we consider extensions of extensions.

Theorem 10.7

Let $F \subseteq K \subseteq L$ be field extensions. Then $[L : F] = [L : K][K : F]$. That is, the degree is multiplicative.

Proof. Suppose that $[L, K] = m$ and $[K : F] = n$ are finite. Fix a basis $\alpha_1, \ldots, \alpha_m$ for L/K and a basis $\beta_1, \ldots, \beta_n$ for K/F. Let $a \in L$, and use the basis for L/K to write $a = a_1\alpha_1 + \cdots + a_m\alpha_m$, where $a_i \in K$. Now for each i, using the basis for K/F to write $a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{in}\beta_n$, or $b_{ij} \in F$. So we have

$$a = \sum_{i=1,\ldots,m, j=1,\ldots,n} b_{ij}\alpha_i\beta_j.$$

Since we can write arbitrary $a \in L$ as a linear combination of $\{(\alpha_i\beta_j)\}_{i,j}$, then this set spans L. They are also linearly independent, since if

$$a = 0 = \sum b_{ij}\alpha_i\beta_j,$$

the defining a_i as before, then $0 = a = \alpha_1 a_1 + \cdots + \alpha_m a_m$. Since $\{\alpha_i\}$ is a basis, then $a_1 = \cdots = a_m = 0$. Since $\beta_1, \ldots, \beta_n$ is a basis, then $b_{i1} = \cdots = b_{in} = 0$. Thus the $(\alpha_i\beta_j)$ are linearly independent. □

Exercise 10.8. Show that if either $[L : K]$ or $[K : F]$ are infinite, then $[L : F]$ is also infinite.

Corollary 10.9

Suppose that $F \subseteq K \subseteq L$, and L/F is finite. Then $[K : F]$ divides $[L : F]$.

We'll now discuss some applications. First, can we tell if $\sqrt{2} \in \mathbf{Q}(\sqrt[3]{2})$? If it were, then we would have field extensions $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt[3]{2})$. The degree of $\mathbf{Q}(\sqrt{2})$ is 2 and the degree of $\mathbf{Q}(\sqrt[3]{2})$ is 3. By corollary 10.9, this is not possible. Thus, $\sqrt{2} \notin \mathbf{Q}(\sqrt[3]{2})$.

More generally, if θ is a root of any irreducible cubic over $\mathbf{Q}$, then $\sqrt{2} \notin \mathbf{Q}(\theta))$, by the same degree argument.

Now, consider $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt[6]{2})$. This is finite, since the degree of $\mathbf{Q}(\sqrt[6]{2})/\mathbf{Q}$ is 6, which follows from the fact that the minimal polynomial is $x^6 - 2$, irreducible by Eisenstein's criterion. Note that $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ and $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}] = 6$. By corollary 10.9, then $[\mathbf{Q}(\sqrt[6]{2} : \mathbf{Q}(\sqrt{2})]$ is 3, so the minimal polynomial of $\sqrt[6]{2}$ over $\mathbf{Q}(\sqrt{2})$ is $x^3 - \sqrt{2}$. It is difficult to prove directly that $x^3 - \sqrt{2}$ is irreducible in $\mathbf{Q}(\sqrt{2})[x]$. However, since we know the degree of the extension $\mathbf{Q}(\sqrt[6]{2})/\mathbf{Q}(\sqrt{2})$ is 3, then we know that the minimal polynomial has degree 3, and it must be $x^3 - \sqrt{2}$.

We can also adjoint two elements to a field. Consider $\mathbf{Q}(\sqrt{2}, \sqrt{3})$. Then we have $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Each of these extensions has degree 2, since $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$. Thus, the degree of the extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$ is 4. This is hard to show directly without using degree arguments.

Exercise 10.10. Show that $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$. Hint: write $\sqrt{3} = a + b\sqrt{2}$, with $a, b \in \mathbf{Q}$, and play around until you get a contradiction.

§11 March 11, 2020

Welcome to the future, your lectures are now on zoom, with slides instead of a blackboard. Use the zoom chat if you need to. There is no midterm. The take-home final is now a home final, since you are already home and there is nowhere to take it. Your two worst assignment scores will be dropped, and the grading is now 35% final, 64% assignments. Feel free to email me or Garrett with any questions. We will also be having office hours over zoom. The lectures will be recorded so you can watch them at any time (esp. if you live in the West). Many of the full formal proofs will not be covered in the lectures. I'll try my best to include the full proofs in the notes.

§11.1 Finitely Generated Field Extensions

Recall that the **degree** of a field extension K/F, written $[K : F]$ is the dimension of K as an F-vector space, and that an extension is called **finite** if the degree is finite. Finite extensions are **algebraic** meaning every element α in the extension is the root of some polynomial in $F[x]$. If $\alpha \in K$, then the field obtained by adjoining α to F, denoted $F(\alpha)$, is called a **simple** field, and its degree is the degree of the minimal polynomial for α.

Example 11.1

Let $K = \mathbf{C}$, and $F = \mathbf{Q}$. The extension K/F is *not* finite. The extension $F(\sqrt[3]{2})/F$ is simple and has degree 3, since the minimal polynomial is $x^3 - 2$.

Now, let's look at some more complicated extensions, such as $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$. Extensions of the form $F(A)$, where A is a finite set, are called **finitely generated** extensions.

Exercise 11.2. Show that $F(\alpha, \beta)$, the field obtained from F by adjoining α, β, is equal to $(F(\alpha))(\beta)$, the field obtained by adjoining β to the field obtained by adjoining α to F.

Now, if $K = F(\alpha_1, \ldots, \alpha_k)$, then letting $F_0 = F$, and $F_{i+1} = F_i(\alpha_{i+1})$ for each $0 \le i \le k$, then we get a chain of extensions

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = K.$$

We proved last time that the degree of field extensions is multiplicative, i.e. if L is an extension of K and K is an extension of F, then $[L : F] = [L : K][K : F]$. As a consequence of this, for the chain of extensions above, we have $[K : F] = [F_k : F_{k-1}] \cdots [F_1 : F_0]$. Thus, if $[F(\alpha_i) : F] = n_i$ for each i, then the degree $[K : F]$ is at most $n_1 \cdots n_k$. Note, this is an upper bound, and it could be strictly less.

Example 11.3

Let $F = \mathbf{Q}$, $\alpha_1 = \sqrt{2}, \alpha_2 = \sqrt[6]{2}$. Then $n_1 = 2, n_2 = 6$, but $\mathbf{Q}(\alpha_1, \alpha_2) = \mathbf{Q}(\alpha_2)$ has degree $6 < 6 \cdot 2$.

Also, recall that we deduced last time that $[\mathbf{Q}(\sqrt[6]{2}) : \mathbf{Q}(\sqrt{2})] = 3$, which is difficult to do directly, since you would have to show that $\sqrt[6]{2} \notin \mathbf{Q}(\sqrt{2})$.

We can now cover some important conclusions about field extensions.

Proposition 11.4

An extension K/F is finite if and only if K is generated by finitely-many algebraic elements. (Note however, that algebraic does *not* imply finite.)

Proof. We saw before that a finite extension is algebraic, so we can take a basis, which gives a generating set for K over F. For the other directions, if $K = F(\alpha_1, \ldots, \alpha_k)$, with each α_i algebraic of degree n_i, then K/F has degree at most the product $n_1 \cdots n_k$, which is finite. □

Proposition 11.5

If K/F, then the numbers in K which are algebraic over F form a field.

Proof. We need to show that if α, β are algebraic, then so are $\alpha + \beta$, $\alpha \cdot \beta$, $-\alpha$, and α^{-1}. This is true since they are all contained in $F(\alpha, \beta)$, which is finite by the previous proposition and thus algebraic. □

Proposition 11.6

If L is algebraic over K and K is algebraic over F, then L is algebraic over F.

Proof. Let $\alpha \in L$. Since α is algebraic over K, by assumption, then α is the root of some polynomial $a_0 + a_1 x + \cdots + a_n x^n$, with each $a_i \in K$. Since K is algebraic over F, then each a_i is algebraic over F. Thus, the extensions $F(a_0, \ldots, a_n)$ is finite over F. The extension $F(a_0, \ldots, a_n)(\alpha)$ is finite over $F(a_0, \ldots, a_n)$, since α satisfies the polynomial $a_0 + \cdots + a_n x^n$. By 11.2, this implies that $F(a_1, \ldots, a_n, \alpha)$ is finite over F, and thus α is algebraic over F. □

Example 11.7

Let $F = \mathbf{Q}$, and $K = \mathbf{C}$. Let $\bar{\mathbf{Q}}$ denote *all* the complex numbers which are algebraic over $\mathbf{Q}$, the **algebraic closure** of $\mathbf{Q}$. What is $[\bar{\mathbf{Q}} : \mathbf{Q}]$? For each n, then $\sqrt[n]{2}$ is algebraic with minimal polynomial $x^n - 2$. So $[\bar{\mathbf{Q}} : \mathbf{Q}] \geq n$ for each n, and is therefore infinite. However, this extension is algebraic! We saw that finite implies algebraic, but the converse is not true.

Exercise 11.8. Prove that $\bar{\mathbf{Q}}$ is countable. Hint: consider the number of polynomials of degree n with coefficients in $\mathbf{Q}$, and recall that an infinite cardinal raised to a finite power is itself.

Since $\mathbf{C}$ and $\mathbf{R}$ are uncountable, this fact proves the existence of transcendental numbers. Showing that specific numbers are transcendental is much more difficult. I will write a short paper on the course site with proofs of transcendence of some common numbers.

§11.2 Composite fields

Definition 11.9 — For K_1, K_2 subfields of a field K, let K_1K_2 be the smallest subfield of K containing both K_1 and K_2, called the **composite field** of K_1 and K_2.

Example 11.10

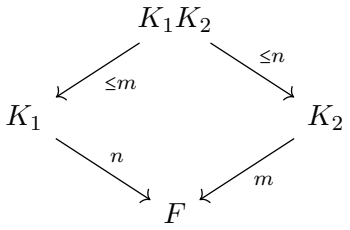
Consider the composite field $\mathbf{Q}(\sqrt{2})\mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbf{Q}(\sqrt[6]{2})$. To see why the last equality is true, first note that $\sqrt{2} \in \mathbf{Q}(\sqrt[6]{2})$, since $\sqrt{2} = \sqrt[6]{2}^3$, so $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[6]{2})$. Then $\sqrt[6]{2} = 2^{1/6} = 2^{1/2-1/3} = \sqrt{2}/\sqrt[3]{2} \in \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$, so that $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[6]{2}$.

Now, suppose that K_1, K_2 are finite extensions of F with bases $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_m$ respectively. Then the composite field is equal to

$$K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m).$$

That is, K_1K_2 is generated by products and sums of α_i's and β_j's with repetition, i.e. all elements of the form $\alpha_1\beta_1, \alpha_1^2\beta_1, \alpha_1^2\beta_1^2, \alpha_1^3\beta_1, \alpha_2\beta_1, \dots$. But most of these products are redundant. Products of α_i's are F-linear combinations of α_i's, since these products are in K_1 and $\{\alpha_i\}$ forms a basis for K_1 over F, and similarly for the β_j's. Thus, we see that $(\alpha_i\beta_j)_{1\le i\le n, 1\le j\le m}$ spans K_1K_2, which means that $[K_1K_2 : F] \le nm = [K_1 : F][K_2 : F]$. Note that this set is not necessarily a basis for K_1K_2.

We can express this relationship diagrammatically as



Recall that the degree of each of the extensions K_1, K_2 has to divide the degree of the composite K_1K_2, since it is an extension of both. If $\gcd(n, m) = 1$, then the equality $[K_1K_2 : F] = nm$ holds, since n and m must divide the degree of K_1K_2.

§12 March 13, 2020

§12.1 Ruler and Compass constructions

Today we will study some problems of the ancient Greeks, namely ruler and compass constructions. These are really "straightedge" and compass constructions, since we aren't allowed to use the markings on the ruler. In fact, these problems are different if you are allowed to use the markings on a ruler.

- Doubling the cube: starting with a line segment L, construct another line segment L' so that a cube with side L' has exactly twice the volume of a cube with side L.
- Trisecting an angle: Given an angle θ, construct the angle $\theta/3$.
- Squaring the circle: Given a circle, construct a square with the same area.

Definition 12.1 — Let S be a set of points in the plane. A line is **S-constructed** if it contains two distinct points of S. A circle is vocab$S$-constructed if it contains a point in S and its center is also in S.

Definition 12.2 — The set of **constructible points of the plane** is the smallest subset S of $\mathbf{R}^2$ with the following properties:

(a) $(0,0) \in S$ and $(1,0) \in S$.

(b) If two non-parallel S-constructed lines intersect at the point P, then $P \in S$.

(c) If C_1 and C_2 are distinct S-constructed circles which intersect at a point P, then $P \in S$.

(d) if C is an S-constructed circle and L is and S-constructed line which intersects C at a point P, then $P \in S$.

Intuitively, a point in the plane is **constructible** if it can be obtained from $(0,0)$ and $(1,0)$ using only the following straightedge and compass operations:

1. Drawing a line between already constructed points.
2. Drawing a circle with the center at a constructed point and also passing through a constructed point.
3. Mark the point at which two straight lines intersect.
4. Mark the points at which a straight line and a circle intersect.
5. Mark the points at which two circles intersect.

Example 12.3

The point $(2,0)$ is constructible: draw the line L between $(0,0)$ and $(1,0)$, draw a circle with center $(1,0)$ and passing through $(0,0)$, and find the intersection of this circle with the line L. This also allows us to construct any integer point on the x-axis.

A line is called **constructible** if it passes through two distinct constructible points, and a circle is **constructible** if its center is constructible and it passes through a constructible point.

Lemma 12.4

Suppose that L is a constructible line and P is a constructible point. Then

- The line perpendicular to L and passing through P is constructible.
- The line parallel to L and passing through P is constructible.

You might have done many of these ruler and compass constructions in a high school geometry class. We have seen the definition of constructible point, constructible line, and constructible circle. The definition we want is a constructible *number*.

Definition 12.5 — A real number r is **constructible** if $|r|$ is the length a segment between two constructible points.

Lemma 12.6

- A real number r is constructible if and only if the point $(r, 0)$ is a constructible point.
- A point (x, y) is constructible if and only if both x and y are constructible numbers.
- A circle is constructible if and only if its center is a constructible point and its radius is a constructible number.

The proof is left as an exercise.

Lemma 12.7

If a and b are constructible numbers, then $a+b$, $-a$, $a \cdot b$, a^{-1}, and $\sqrt{a}$ are constructible. In particular, the constructible numbers form a field.

Proof. First, $a = |-a|$ is constructible, and since both a and b are constructible, then the points $(b, 0)$ and $(-a, 0)$ are constructible. Then $a + b$ is the distance between $(b, 0)$ and $(-a, 0)$. To construct products and inverses, use similar triangles.

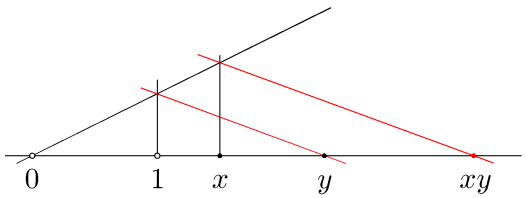


Figure 1: Construction of products

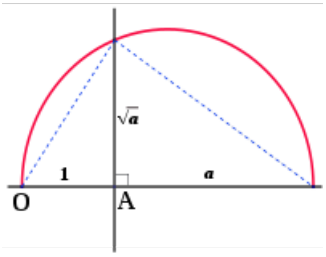


Figure 2: Construction of square roots

□

Note, since we can construct square roots using the above, e.g. $\sqrt{2}$, then we can also construct fourth roots, e.g. $\sqrt[4]{2}$, and so on.

Now, we will use algebra to solve problems of constructibility. We now show that a number is constructible if and only if it can be obtained from 0 and 1 using the field

operations and square roots. Recall that a **quadratic** extension is a field extension of degree 2.

Theorem 12.8

A real number is constructible if and only if it is contained in an extension K of $\mathbf{Q}$ which is an iteration of quadratic extensions. This means that there are subfields

$$\mathbf{Q} = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = K,$$

where for all $i < k$, we have $F_{i+1} = F_i(\sqrt{\alpha_i})$, for α_i a non-negative real number in F_i.

I include a full proof below. Most of it is just writing out the equations of lines and circle and some casework, but it's good to review just to see the sort of argument used.

Proof. First, we show that any element of K is constructible. Suppose that $x \in K$. Since $F_2 = \mathbf{Q}(\sqrt{\alpha_1})$ for some α_1, then every element of F_2 is an element of $\mathbf{Q}$ or some square root, and thus constructible. Since all the elements of F_2 are constructible, and $F_3 = F_2(\sqrt{\alpha_2})$, then all the elements of F_3 can be constructed using square roots. Continuing inductively, then $x \in K$ is constructible.

For the other direction, suppose that γ is constructible. Then γ is the coordinate of some constructible point, which is constructed using a finite number of ruler and compass operations. After each of these operations, some number of constructible numbers will have been used. We prove that γ is constructible by induction on the number of constructible numbers used to obtain γ.

Suppose that $\{x_1, \ldots, x_k\}$ is a set of numbers which have been constructed. It suffices to show that if γ is constructed from the elements of this set, then $[\mathbf{Q}(x, x_1, \ldots, x_k) : \mathbf{Q}(x_1, \ldots, x_k)]$ is 2 or 1. We need to check that this is the case for each of the 5 ruler and compass constructions given above. We do this by first checking that the coefficients of a line or circle constructed using points in $BQ(x_1, \ldots, x_k)$ are still in $\mathbf{Q}(x_1, \ldots, x_k)$, and then verifying what points we can constructed from these lines and circles.

First, consider a line drawn through two points. If the two points are (α_1, β_1) and (α_2, β_2), where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are in $\mathbf{Q}(x_1, \ldots, x_k)$, then the equation of the line through the two points is $y = (\beta_2 - \beta_1)(x - \alpha_1)/(\alpha_2 - \alpha_1) + \beta_1$. The coefficients in this equation all lie in $\mathbf{Q}(x_1, \ldots, x_k)$.

Now consider a circle with its center at a constructed point and radius equal to the distance between two constructed points. If the center of the circle is (α_1, β_1) and the radius is equal to r, then the equation of the circle is $(x - \alpha_1)^2 + (y - \beta_1)^2 = r^2$, and all the coefficients in this equation are in $\mathbf{Q}(x_1, \ldots, x_k)$.

Suppose now that γ is constructed by taking the intersection of two lines. We know that all the constructed lines have coefficients in $\mathbf{Q}(x_1, \ldots, x_k)$. Suppose that we draw the point of intersection of two of these lines. The lines are given by

$$\alpha_{11}x + \alpha_{12}y = \beta_1$$
$$\alpha_{21}x + \alpha_{22}y = \beta_2,$$

where $\alpha_{ij}, \beta_\ell \in \mathbf{Q}(x_1, \ldots, x_k)$. These two lines meet at the point (x_1, y_1), where

$$x_1 = \frac{\beta_1\alpha_{22} - \beta_2\alpha_{12}}{\alpha_{11}\alpha_{22} - \alpha_{21}\alpha_{12}}$$
$$y_1 = \frac{\alpha_{11}\beta_2 - \beta_1\alpha_{21}}{\alpha_{11}\alpha_{22} - \alpha_{21}\alpha_{12}}.$$

Since all the coefficients are in $\mathbf{Q}(x_1, \ldots, x_k)$, then the constructed points x_1, y_1 are also in $\mathbf{Q}(x_1, \ldots, x_k)$. Thus, any γ constructed in this way is in $\mathbf{Q}(x_1, \ldots, x_k)$

Now suppose γ is constructed by taking a point of intersection of a circle and a line, where the coefficients of the circle and line are in $\mathbf{Q}(x_1, \ldots, x_k)$. If (x, y) are the points of intersection, then x must satisfy an equation of the form

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

with $a, b, c \in \mathbf{Q}(x_1, \ldots, x_k)$. You can show this by writing the equations of a line and a circle and eliminating y, for example see here. The circle and line will intersect only if $b^2 - 4ac \geq 0$. Then we have

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

which are either in $\mathbf{Q}(x_1, \ldots, x_k)$ or in $\mathbf{Q}(x_1, \ldots, x_k, \sqrt{b^2 - 4ac})$, a quadratic extension. A similar result holds for the y coordinates, so any γ constructed in this way is in either $\mathbf{Q}(x_1, \ldots, x_k)$ or a quadratic extension of it, as desired.

Now suppose that γ is constructed by taking a point of intersection of two circles. Suppose the equations of the circles are

$$x^2 + y^2 + a_1 x + b_1 y + c_1 = 0$$
$$x^2 + y^2 + a_2 x + b_2 y + c_2 = 0.$$

The points of intersection are the intersection of one of them with the line

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0.$$

Since all the coefficients are in $\mathbf{Q}(x_1, \ldots, x_k)$, then γ constructed in this way is in either $\mathbf{Q}(x_1, \ldots, x_k)$ or a quadratic extension of it, by the argument for the intersection of a line and a circle.

Now, to finish the induction, consider the base case where $k = 2$. Then $\mathbf{Q}(x_1, x_2) = \mathbf{Q}(0, 1) = \mathbf{Q}$. Thus, the result follows by induction, so

$$\gamma \in \mathbf{Q}(x_1, \ldots, x_n),$$

for some n. Since each $\mathbf{Q}(x_1, \ldots, x_{n-1})(x_n)$ is a quadratic extension then it follows that

$$\gamma \in K \supseteq \cdots \supseteq F_1 = \mathbf{Q},$$

where each extension is quadratic, as desired. □

Corollary 12.9

If x is constructible, then $[\mathbf{Q}(x) : \mathbf{Q}] = 2^k$ for some k.

Proof. This follows from the fact that $x \in F_k \supseteq \cdots \supseteq F_1 = \mathbf{Q}$ for some k and each extension is degree 2. □

We can now prove some results about the Ancient Greek problems.

Theorem 12.10 (Doubling the Cube)

Given a cube, it is not possible to construct a cube with twice the volume. That is, if we are given the length of an edge of a cube, it is not possible to construct the length of the edge of the cube with twice the volume.

Proof. suppose that the cube has side length 1, and thus volume 1, without loss of generality. A cube that doubles its volume would have side length $\sqrt[3]{2}$, which is not constructible since $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$. □

Theorem 12.11 (Squaring the Circle)

Given a circle, it is not possible to construct a square with the same area.

Proof. A unit circle (radius 1), has area π. Thus, to construct such a square, we would need to construct the number $\sqrt{\pi}$, which is not possible since $\mathbf{Q}(\sqrt{\pi})$ has infinite degree. □

For trisecting angles, we'll first need the following fact.

Exercise 12.12. An angle θ can be constructed (that is, two lines with the angle between them θ can be constructed) if and only if $\cos(\theta)$ is a constructible real number.

The question of trisecting an angle thus boils down to the following question: if $\cos(\theta)$ is constructible, is $\cos(\theta/3)$ also constructible? Note that $\cos(\theta) = 2\cos^2(\theta/2) - 1$, so we can construct $\cos(\theta/2)$ by solving a quadratic. Thus, angle bisection is possible. But trisection is not in general possible.

Theorem 12.13 (Trisecting an Angle)

An angle θ can be trisected if and only if $4x^3 - 3x - \cos(\theta)$ is reducible over $\mathbf{Q}(\cos(\theta))$.

Proof. De Moivre's formula tells us that

$$\begin{aligned}\cos(\theta) &= (\cos(\theta/3) + i\sin(\theta/3))^3 - i\sin(\theta) \\ &= \cos^3(\theta/3) + 3i\cos^2(\theta/3)\sin(\theta/3) - 3\cos(\theta/3)\sin^2(\theta/3) - i\sin^3(\theta/3) - isin(\theta) \\ &= 4\cos^3(\theta/3) - 3\cos(\theta/3).\end{aligned}$$

Thus, $\cos(\theta/3)$ satisfies the equation $4x^3 - 3x - \cos(\theta)$.

Now, if the polynomial $4x^3 - 3x - \cos(\theta)$ is reducible over $\mathbf{Q}(\cos(\theta))$, then $\cos(\theta/3)$ is the root of a degree one or two polynomial over $\mathbf{Q}(\cos(\theta))$, and therefore $\cos(\theta/3)$ is constructible from $\mathbf{Q}(\cos(\theta))$, which means that $\cos(\theta/3)$ is constructible, and therefore the angle $\theta/3$ is constructible.

Now, if the polynomial $4x^3 - 3x - \cos(\theta)$ is irreducible over $\mathbf{Q}(\cos(\theta))$, then $[\mathbf{Q}(\cos(\theta)) : \mathbf{Q}(\cos(\theta/3))] = 3$, which implies $\cos(\theta/3)$ is not constructible and thus $\cos/3$ is not constructible. □

§12.2 More Field Theory

Recall that if F is a field, and $p(x) \in F[x]$, then it is always possible to find an extension of F which contains a root of p, and if p is irreducible, then there is a minimal such extension. We now generalize this to consider more than one root of p.

Definition 12.14 — For a field F and a polynomial $p \in F[x]$, an extension K is called a **splitting field** for p if $p(x)$ factors into linear factors in $K[x]$, and does not factor into linear factors over any subfield of $K[x]$. In the case that $p(x)$ factors into linear factors in $K[x]$, we say that p **splits completely** in $K[x]$.

We now show the existence of splitting fields.

Theorem 12.15 (Existence of Splitting Fields)
Let F be a field, and $p(x) \in F[x]$ a nonconstant polynomial. Then there exists a splitting field K of F.

Proof. By 9.7, there exists an extension F_1 of F such that F_1 contains a root for p. Then p factors in $F_1[x]$ to have at least one linear factor. Remove the linear factors to get a polynomial $p_1(x)$. Then there exists an extension F_2 of F_1 which contains a root for p_1. Continue inductively, and eventually we obtain the desired field K. □

Exercise 12.16. Show that splitting fields are unique up to isomorphism.

Example 12.17

- The splitting field of $x^2 - 2$ over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{2})$.
- The splitting field of $(x^2-2)(x^2-3)$ is $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.
- The splitting field of $x^3 - 2$ is *not* $\mathbf{Q}(\sqrt[3]{2})$. Remember that $x^3 - 2$ has the complex roots $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2}e^{2\pi i/3}, \alpha_3 = \sqrt[3]{2}e^{4\pi i/3}$. The splitting field of $x^3 - 2$ is the smallest field containing all of these roots, which is $K = \mathbf{Q}(\alpha_1, \alpha_2)$.
- Observe that $\alpha_2/\alpha_1 = e^{2\pi i/3}$ is in the splitting field, where α_1, α_2 are from above. We can write $e^{2\pi i/3}$ as $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, so $\sqrt{3}i = \sqrt{-3}$ is in the splitting field. But $\sqrt{-3}$ is a root of $x^2 + 3$, which has degree 2. This tells us that the splitting field $K = \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$, which is the same K as above, has degree 6.

What can we say in general about the degree of a splitting field of a polynomial of degree n? The following lemma gives us an upper bound on the degree of such a splitting field.

Lemma 12.18
The splitting field of a polynomial $p(x)$ of degree n has degree at most $n!$.

Proof. Add a root α of p to F, to get an extension of degree at most n. Divide p by $(x - \alpha)$, and get a polynomial of degree $n - 1$. Add a root of this to the extension to get

another extension of at most degree $n-1$. The composite extension has degree at most $n(n-1)$. Continuing inductively, we see that the maximal possible degree of the splitting field is $n!$. □

We could have used the above lemma to see that the degree of the splitting field of x^3-2 has degree $d=6$. We know that $d \le 3! = 6$. Since the field strictly contains $\mathbf{Q}(\sqrt[3]{2})$, which has degree 3, then we have $3 < d \le 6$. Since $d \mid 6$, then we must have $d = 6$.

Example 12.19

Splitting field can be smaller than expected. Consider the polynomial x^4+4. You might expect that the splitting field has degree at least 4, but this is not true! The polynomial factors as $(x^2+2x+2)(x^2-2x+2)$. The roots are $\pm 1 \pm i$. Thus, the splitting field is actually $\mathbf{Q}(i)$, which has degree 2.

§13 March 25, 2020

There was one question from last class about whether we can prove impossibility of geometric constructions without using field theory. For trisecting the angle we can, for example see here.

§13.1 Splitting Fields

Recall the definition of a *splitting field* of a field F and a polynomial $p \in F[x]$ from last time: the smallest field K containing F such that K contains *all* the roots of p. Today we continue our study of splitting fields, first by showing that they are unique.

Lemma 13.1 (Uniqueness of Simple Extensions)

Let $\phi : F \to F'$ be a field isomorphism. Let $p(x) \in F[x]$ be an irreducible polynomial, and $p'(x) \in F'[x]$ be the corresponding polynomial under ϕ, i.e. the polynomial obtained by applying ϕ to the coefficients of $p(x)$. Let α be a root of $p(x)$ in some extension of F, and let α' be some root of $p'(x)$. Then there is an isomorphism $\sigma : F(\alpha) \to F'(\alpha')$ such that σ restricted to F is the map ϕ, $\sigma|_F = \phi$, and $\sigma(\alpha) = \alpha'$. This is summarized in the following commutative diagram.

$$\begin{array}{ccc} F(\alpha) & \overset{\exists \sigma}{\dashrightarrow} & F'(\alpha') \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

Proof. The consider the isomorphism $\Phi : F[x] \to F'[x]$ induced by ϕ. This maps the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$, by definition of the induced map. Then note that $F(\alpha) \simeq F[x]/(p(x))$, and $F'(\alpha') \simeq F'[x]/(p'(x))$, and these fields are isomorphic by quotienting the map Φ. □

Exercise 13.2. In the proof of lemma 13.1, check that the induced isomorphism actually restricts to ϕ, and that it maps α to α'.

Theorem 13.3 (Uniqueness of Splitting Fields)

Let $\phi : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be a polynomial, and let $p'(x) \in F'[x]$ be the corresponding polynomial induced by ϕ. Let K be a splitting field for $p(x)$ over F, and let K' be a splitting field for $p'(x)$ over F'. Then ϕ extends to a an isomorphism $\sigma : K \to K'$, summarized by the following diagram:

$$\begin{array}{ccc} K & \overset{\exists \sigma}{\dashrightarrow} & K' \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

Proof. Proceed by induction on the degree n of $p(x)$. If $n = 1$, then $F = K$, and $F' = K'$, so let $\sigma = \phi$ and we are done. If $n \geq 2$, then suppose that the result holds for polynomials of degree less than or equal to $n-1$. Let $f(x)$ an irreducible factor of $p(x)$. Add a root $\alpha \in K$ for f to the field F, and add a root $\alpha' \in K'$ for f' to the field F'. By lemma 13.1, we get an isomorphism $\phi_1 : F(\alpha) \to F'(\alpha')$. Then apply the induction hypothesis to the polynomial $p(x)/(x-\alpha)$, which is of degree $n-1$. This is summarized in the following commutative diagram:

$$\begin{array}{ccc} K & \overset{\exists \sigma (\text{induction})}{\dashrightarrow} & K' \\ \downarrow & & \downarrow \\ F(\alpha) & \overset{\exists \phi' (13.1)}{\dashrightarrow} & F'(\alpha') \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

In particular, if $F = F'$ and ϕ is the identity, then we get that any two splitting fields of $p(x)$ over F are isomorphic. □

Example 13.4

The roots of the polynomial $x^n - 1 \in \mathbf{Q}[x]$ are called the **n'th roots of unity**. The n'th roots of unity are of the form $2^{\pi ik/n}$, for $k = 1, \ldots, n$. For fixed n, the n'th roots of unity form a group. We show below that this group is cyclic.

Lemma 13.5

If F is a field, and $F^\times$ is its group of units, then any finite subgroup of $F^\times$ is cyclic.

Proof. First, note that $F^\times$ is abelian, since F is a field, and so $G \subseteq F^\times$ is also abelian. By the structure theorem for finitely generated $\mathbf{Z}$-modules (abelian groups), then G is isomorphism to $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$, where $2 \leq n_1 \mid n_2 \mid \cdots \mid n_k$. We want to show that G is cyclic, which here just means $k = 1$. To do this, note that any $\alpha \in G$ is a root of the polynomial $x^{n_k} - 1$, and $x^{n_k} - 1$ has at most n_k roots, which means $|G| \leq n_k$. But using the degrees from the structure theorem, we also have $n_1 \cdots n_k = |G|$, which means $n_1 \cdots n_k \leq n_k$, which implies $k = 1$. (Note, we used the fact that in a field, polynomials of degree n have at most n roots). □

The above lemma tells us that the group of roots of unity is cyclic. In particular, this group has generators, which are called the **primitive roots of unity**. For example $e^{2\pi i/n}$ *is* a primitive n'th root of unity, but $1 = e^{2\pi in/n}$ is *not* a primitive root of unity (for $n \geq 2$). In general $e^{2\pi ik/n}$ is a primitive root of unity if and only if k is coprime to n, so there are $\phi(n)$ primitive n'th roots of unity, where ϕ here is the Euler Totient function. We write ζ_n for $e^{2\pi i/n}$. The splitting field of $x^n - 1$ is then $\mathbf{Q}(\zeta_n)$, from example 13.4.

Later we will see that $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \phi(n)$. For $n = p$ a prime, we can show this already. We have

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1).$$

Since $\zeta_p \neq 1$, then it is a root of $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. We need to show that $f(x)$ is irreducible, so that ζ_p has degree $p - 1 = \phi(p)$. To show that $f(x)$ is irreducible, observe that

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Then replace x by $x + 1$. By the binomial theorem, then

$$\frac{1}{x}\left(\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x\right) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}.$$

Since p divides all the non leading coefficients, and the last coefficient is p, then we can apply Eisenstein's criterion to show that the polynomial is irreducible.

Example 13.6

Let's look at the splitting field of $x^p - 2$, where p is prime. The roots of $x^p - 2$ are $\zeta\sqrt[p]{2}$, where ζ is any p'th root of unity. Since $\zeta_p = (\zeta_p\sqrt[p]{2})/(\sqrt[p]{2})$, then $\mathbf{Q}(\sqrt[p]{2}, \zeta_p)$ is contained in the splitting field. On the other hand, if ζ is any p'th root of unity, then $\zeta\sqrt[p]{2} = \zeta_p^k\sqrt[p]{2}$ for some k, so $\zeta\sqrt[p]{2} \in \mathbf{Q}(\sqrt[p]{2}, \zeta_p)$, so that $\mathbf{Q}(\sqrt[p]{2}, \zeta_p)$ is the entire splitting field.

What is the degree of this splitting field? Well, $\mathbf{Q}(\sqrt[p]{2}, \zeta_p)$ is the composite of $\mathbf{Q}(\sqrt[p]{2})$ which has degree p, and $\mathbf{Q}(\zeta_p)$ which has degree $p - 1$. Since p and $p - 1$ are relatively prime, then the degree of the composite field is the product $p(p-1)$.

§13.2 Algebraic Closure

Recall, a simple algebraic extension adds *one* root of *one* polynomial. The splitting field adds *all* the roots of *one* polynomial. Let's add *all* the roots of *all* the polynomials.

Definition 13.7 — The field $\bar{F}$ is called an **algebraic closure** of F if $\bar{F}$ is an algebraic extension of F and *every* polynomial $p(x) \in F[x]$ splits completely over $\bar{F}$. A field K is called **algebraically closed** if every polynomial in $K[x]$ has a root in K.

Proposition 13.8

A field K is algebraically closed if and only if $\bar{K} = K$.

Exercise 13.9. Prove that an algebraic closure $\bar{F}$ of F is algebraically closed. Hint: let

$p(x) \in \bar{F}[x]$, with a root α. Consider $\bar{F}(\alpha)$, and use the fact that algebraicness is transitive.

Theorem 13.10

Any field has an algebraic closure, and any two algebraic closures of a given field are isomorphic.

Exercise 13.11. Prove theorem 13.10. Hint: for existence, you need Zorn's lemma. For uniqueness, use an argument similar to the uniqueness of the splitting field.

Example 13.12

The complex numbers $\mathbf{C}$ are algebraically closed (we'll prove this later). The rational numbers $\mathbf{Q}$ are not algebraically closed. The algebraic closure of $\mathbf{Q}$ is *not* $\mathbf{C}$.

§13.3 Multiplicity of Roots

Let F be a field, and $f(x) \in F[x]$ be a polynomial with leading coefficient $a_n \neq 0$. In the splitting field K of $f(x)$ over F, we can write

$$f(x) = a_n(x-\alpha_1)^{n_1}\cdots(x-\alpha_k)^{n_k},$$

where $\alpha_1, \ldots, \alpha_k \in K$ are distinct, and $n_i \geq 1$ for all i. The number n_i is called the **multiplicity** of the root α_i. If $n_i = 1$, then α_i is called a **simple root**, else it is called a **multiple root**. The polynomial $f(x)$ is called **separable** if it has no multiple roots, else it is called **inseparable**.

Example 13.13

- The polynomial $x^2 - 2 \in \mathbf{Q}[x]$ is separable. It has distinct roots $\sqrt{2}$ and $-\sqrt{2}$.
- The polynomial $(x^2-2)^3$ is inseparable, since $\sqrt{2}$ and $-\sqrt{2}$ each have multiplicity 3.
- Let $F = \mathbf{Z}/2\mathbf{Z}(t)$, the field of rational functions in t over the field $\mathbf{Z}/2\mathbf{Z}$. Consider $x^2 - t \in F[x]$. This polynomial is irreducible by Eisenstein's criterion. Let $\sqrt{t}$ be a root of the polynomial, in some extension. Then $(x-\sqrt{t})^2 = x^2+t = x^2t$, since $2 = 0$ in F. Then $x^2 - t$ is inseparable, since $\sqrt{t}$ has multiplicity 2.

We want to develop a systematic way of testing for multiple roots. To do this, we define the **derivative** of a polynomial. To us, the derivative is a strictly *algebraic* construction: there is no analysis/calculus involved, rather is it purely symbolic (even though it turns out to be the same as the derivative in calculus).

Definition 13.14 — If

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x],$$

then the **derivative** of $f(x)$ is the polynomial

$$D_x f(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

Exercise 13.15. Verify that the sum and product rules hold for this definition of the derivative. That is, show that $D_x(f(x)+g(x)) = (D_x f(x)) + (D_x g(x))$ and that $D_x(f(x)\cdot g(x)) = f(x)(D_x g(x)) + (D_x f(x))g(x)$. Don't use any calculus.

We'll now prove the theorem that allows us to check whether a polynomial has multiple roots.

Theorem 13.16

A polynomial $f(x)$ has a multiple root α if and only if α is a root of both $f(x)$ and $D_x f(x)$.

Proof. Suppose that α is a root of $f(x)$ with multiplicity $n \geq 1$. Then $f(x) = (x-\alpha)^n g(x)$ for some polynomial $g(x)$ in some splitting field. Taking derivatives and using the product rule, then

$$D_x f(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n D_x g(x).$$

If $n \geq 2$, then $n-1 \geq 1$ and α is a root of $D_x f(x)$. So if α is a multiple root of $f(x)$, then it is also a root of the derivative $D_x f(x)$.

On the other hand, if $n = 1$, then $D_x f(x) = g(x) + (x-\alpha)^n D_x g(x)$, so $(D_x f(x))(\alpha) = g(\alpha)$. But $g(\alpha) \neq 0$ by definition, so α is not a root of $D_x f(x)$. Thus, if α is not a simple root of f, then it is not a root of the derivative. □

Corollary 13.17

A polynomial $f(x)$ has a multiple root α if and only if $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial of α. In particular, $f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

Corollary 13.18

A polynomial $f(x)$ is separable if and only if it is coprime to $D_x f(x)$.

The proofs of the above two corollaries are immediate from the theorem.

Corollary 13.19

Every irreducible polynomial $f(x)$ over a field of characteristic 0 is separable.

Proof. If f has degree $n \geq 1$, then $D_x f(x)$ has degree $n-1$. In particular, since the characteristic of the field zero, then the derivative is nonzero. Since f was assumed to be irreducible, then the only divisors of f are $f(x)$ and 1. Since the degree of $D_x f(x)$ is less than the degree of $f(x)$, then $f(x)$ does not divide $D_x f(x)$. Thus f is coprime to its derivative, and the polynomial is separable. □

Note that in characteristic p, the derivative might be zero, so the above proof doesn't quite work. We'll examine this situation more next time.

§14 March 27, 2020

§14.1 Separability and Finite Fields

Recall from last time that we proved that if $f(x) \in F[x]$, then a root α of $f(x)$ is a multiple root if and only if α is also a root of the derivative $f'(x)$. We also stated several corollaries about the separability of polynomials. In particular, we saw that every irreducible polynomial over a field of characteristic 0 is separable. The proof fails in the case of characteristic p, but we would still like to know when polynomials are separable in characteristic p fields.

Example 14.1

Let F be a field of prime characteristic p. Let $f(x) = x^n - 1$. Then the derivative of f is nx^{n-1}. But if $p \mid n$, this is equal to zero in F. In particular, any p'th root of unity is a multiple root. If n does not divide p, then nx^{n-1} is nonzero, and the only root is 0. Thus, f is separable, since all the roots of unity are distinct.

We can fix the corollary to work for all characteristics, zero or nonzero. The proof is almost exactly the same as the proof of corollary 13.19.

Corollary 14.2

An irreducible polynomial with nonzero derivative is separable.

Now that we know any irreducible polynomial with nonzero derivative is separable, we need to know when the derivative of a polynomial is zero. If F is a field of characteristic $p \neq 0$, and $f(x) = a_n x^n + \cdots + a_0$, then the derivative of $f(x)$ is zero if and only if p divides i for each nonzero coefficient a_i.

So if the derivative of a polynomial f is zero, then we can write f as a polynomial in x^p:

$$f(x) = b_m x^{pm} + b_{m-1} x^{p(m-1)} + \cdots + b_0.$$

That is, we have $f(x) = f_1(x^p)$, where $f_1(x) = b_m x^m + \cdots + b_0$. Note that if f is irreducible, then so is f_1.

If f_1 is itself not separable, then we can write it as as polynomial in x^p again: $f_1(x) = f_2(x^p)$, and so $f(x) = f_2(x^{p^2})$. Continuing, we will eventually reach a separable polynomial for some $k \geq 0$, so $f(x) = f_k(x^{p^k})$. In this case we write $f_k = f_{\text{sep}}$.

The degree of f_{sep} for which this happens is called the **separable degree**, and is denoted $\deg_s f(x)$. The number p^k is called the **inseparability degree** of $f(x)$, denoted $\deg_i f(x)$. Note, the separable degree is the degree of the *polynomial* $f_{\text{sep}}(x)$, and the inseparability degree is the *power* of x that we plug into the polynomial $f_{\text{sep}}(x)$ to get the polynomial $f(x)$. Note that $\deg f(x) = \deg_s f(x) \cdot \deg_i f(x)$.

Example 14.3

- Let p be a prime and $f(x) = x^p - t$, as a polynomial in $(\mathbf{F}_p(t))[x]$, the field of rational functions over the field $\mathbf{F}_p$. This polynomial is irreducible, but its derivative is zero. Then we have $f_p(x) = x - t$, so $f_p(x^p) = x^p - t$, and so $f_{\text{sep}}(x) = x - t$. So the separable degree of f is 1, and its inseparability degree is p.

- More generally, $f(x) = x^{p^n} - t$ has $f_{\text{sep}} = x - t$, and inseparability degree p^n.

Exercise 14.4. For $f(x) = x^p - t \in (\mathbf{F}_p(t))[x]$, show that $f(x)$ has a single root of multiplicity p.

We now define a special field homomorphism called the *Frobenius map*. The map also works in the setting of rings, but for this class we'll only work with the field case.

Theorem 14.5

Let F be a field of characteristic $p \neq 0$. For any $a, b \in F$, then $(a+b)^p = a^p + b^p$, and $(ab)^p = a^p b^p$. The map $a \mapsto a^p$ is an injective homomorphism from F to F. The map $a \mapsto a^p$ is called the **Frobenius map**.

Proof. That $(ab)^p = a^p b^p$ is straightforward. To see that $(a+b)^p = a^p + b^p$, use the binomial theorem and expand

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Note that p divides all the coefficients except for the a^p and b^p. So $(a+b)^p = a^p + b^p$. For injectivity of the map, note that $a \mapsto a^p = 0$ implies $a = 0$, since fields do not have nilpotent elements. □

Note however that the Froebenius map is not always surjective. Fields for which the Frobenius map *is* surjective are called *perfect* fields. That is, a field is **perfect** field if either $p = 0$ or if any element in the field is a p'th power: for all $a \in F$, then $a = b^p$ for some $b \in F$.

Example 14.6

- Recall that any injective map of finite fields is also surjective. Thus, every finite field is perfect.
- The field $\mathbf{F}_p(t)$ of rational functions over $\mathbf{F}_p$ is *not* perfect. This gives some motivation for the next theorem.

Theorem 14.7

Irreducible polynomials over perfect fields are separable.

Proof. Let F be a perfect field, and let $f(x) \in F[x]$. If it is inseparable, then its derivative is zero, so $f(x) = g(x^p)$ for some polynomial g. Since the field is perfect, we can write $g(x) = b_m^p x^m + \cdots + b_0^p$, for some b_i. But then $f(x) = b_m^p x^{pm} + \cdots + b_0^p$, which means $f(x) = (b_m x^m + \cdots + b_0)^p$, contradicting the irreducibility of f. Thus, f is separable. □

We now prove the existence and uniqueness of finite fields of any prime power order.

Theorem 14.8

For any prime p and any $n \geq 1$ in $\mathbf{Z}$, there exists a unique field with p^n elements.

Proof. Let $f(x) \in \mathbf{F}_p[x]$ be the polynomial $f(x) = x^{p^n} - x$. Since the derivative is -1, then f is separable, and has p^n distinct roots in its splitting field. Let F be the set of all these distinct roots, so there are p^n elements in F. We now show that F is a field. Suppose $a, b \in F$. Then $a^{p^n} = a$, and $b^{p^n} = b$. So

$$f(a+b) = a^{p^n} + b^{p^n} - a - b = a + b - a - b = 0.$$

Thus, $a+b$ is one of the distinct roots of f, and is thus in F. Similarly,

$$f(ab) = (ab)^{p^n} - ab = ab - ab = 0.$$

Also, $a^{-1} \in F$, and $0, 1 \in F$, so F is a finite field with p^n elements. It is the splitting field of f, by construction.

We now show that this field is unique. Suppose F is any finite field characteristic p. The prime subfield is $\mathbf{F}_p$. Let n be the degree of F over $\mathbf{F}_p$ (as a vector space). Such an n exists since F was assumed to be finite. Basic counting gives that F has p^n elements. Denote by $F^\times$ be the group of units of F. It contains $p^n - 1$ elements, so Lagrange's theorem tells us that for all $a \in F^\times$, $a^{p^n} = a$, so a is a root of $f(x) = x^{p^n} - x$. Since 0 is also a root, and $F^\times = F \setminus \{0\}$, then every element of F is a root of $f(x)$. So F is the splitting field of $f(x)$ over $\mathbf{F}_p$. We proved earlier that splitting fields are unique, so any two finite fields with p^n elements are isomorphic. □

§14.2 Cyclotomic Extensions

Recall the notation $\zeta_n = e^{2\pi i/n}$. The extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ the **cyclotomic extensions** of the n'th root of unity. It is by definition the splitting field of $x^n - 1$. It is an extension of degree $\phi(n)$ (we'll show this soon), where ϕ is the Euler totient function: $\phi(n)$ is the number of elements in $\{1, \dots, n\}$ coprime to n.

The roots of unity are elements of the form ζ_n^k. The n'th roots of unity form a cyclic group under multiplication, generated by ζ_n. We denote this group by μ_n.

Lemma 14.9

A number d divides n if and only if μ_d is a subgroup of μ_n, where μ_i is the cyclic group of i'th roots of unity.

Proof. If d divides n, then we can write $n = kd$ for some k. If ζ is a d'th root of unity, then $\zeta^n = \zeta^{kd} = (\zeta^d)^k = 1$, so it is also an n'th root of unity.

If $\mu_d \subseteq \mu_n$ is a subgroup, then $\zeta_d \in \mu_n$, and has order d. By Lagrange's theorem, then the order of any element must divide the order of the group. Since the order of the group μ_n is n, then d divides n. □

Recall that an n'th root of unity is called **primitive** if it is a generator of μ_n, so ζ_n^k is primitive if and only if k and n are coprime. We now define cyclotomic polynomials.

Definition 14.10 — The ***n*'th cyclotomic polynomial**, denoted $\Phi_n(x)$, is the polynomial whose roots are the primitive n'th roots of unity:

$$\Phi_n(x) = \prod_{1 \le k \le n, \gcd(k,n)=1} (x - \zeta_n^k).$$

This is a monic polynomial of degree $\phi(n)$, having ζ_n as a root. Our goal is to show that this is in fact the *minimal* polynomial of ζ_n over $\mathbf{Q}$.

Notice that we can write the polynomial $x^n - 1$ as

$$x^n - 1 = \prod_{1 \le k \le n} (x - \zeta_n^k).$$

Note that we have dropped the gcd condition. Now, suppose that ζ is some element of μ_n with order d. Then ζ is a primitive d'th root of unity (note d not n). Then we can write

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \left(\prod_{\zeta \in \mu_d, \zeta \text{ primitive}} (x - \zeta) \right) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned}$$

By examining degrees, we recover the formula from number theory $n = \sum_{d|n} \phi(d)$. For some examples of cyclotomic polynomials, see the Wikipedia page.

Lemma 14.11

Cyclotomic polynomials have integer coefficients. That is, $\Phi_n(x) \in \mathbf{Z}[x]$.

Proof. Proceed by induction on n. For $n = 1$, then $\Phi_n(x) = x - 1$.

For $n \ge 2$, suppose that the result holds up to $n - 1$. Then

$$x^n - 1 = \Phi_n(x) f(x) = \Phi_n(x) \prod_{d|n, d \ne n} \Phi_d(x).$$

Then $f(x) \in \mathbf{Z}[x]$ by the induction hypothesis. In $\mathbf{Q}(\zeta_n)[x]$, then $f(x)$ divides $x^n - 1$. Since $x^n - 1$ and $f(x)$ have rational coefficients, then $\phi_n(x)$ also has rational coefficients, by the division algorithm. By Gauss' lemma, the factorization of $x^n - 1$ into monic irreducibles in $\mathbf{Z}[x]$ and $\mathbf{Q}[x]$ must be the same. Since $f(x)$ divides $x^n - 1$ in $\mathbf{Q}[x]$, then it must divides $x^n - 1$ in $\mathbf{Z}[x]$, which means $\Phi_n(x) \in \mathbf{Z}[x]$. □

Theorem 14.12

The cyclotomic polynomial $\Phi_n(x)$ is irreducible in $\mathbf{Z}[x]$, so the degree of $\mathbf{Q}(\zeta_n)$ over $\mathbf{Q}$ is $\phi(n)$.

Proof. Suppose that $\Phi_n(x)$ is reducible, and write $\Phi_n(x) = f(x)g(x)$, for $f, g \in \mathbf{Z}[x]$ monic, where f is irreducible and has some primitive n'th root of unity ζ as a root: $f(\zeta) = 0$.

Let p be a prime which doesn't divide n. Then ζ^p is a primitive n'th root of unity. Since $\Phi_n(\zeta^p) = 0$, then either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$.

If $g(\zeta^p) = 0$, then ζ is a root of $g(x^p)$, so $f(x)$ divides $g(x^p)$ in $\mathbf{Z}[x]$, and we can write $g(x^p) = f(x)h(x)$ for some h. Reducing modulo p, we find that $\bar{g}(x^p) = (\bar{g}(x))^p = \bar{f}(x)\bar{g}(x)$. (The first equality follows from the "Freshman's dream" identity and from Fermat's little theorem.) This means that inside $\mathbf{F}_p[x]$, the polynomials $\bar{f}$ and $\bar{g}$ share an irreducible factor. Also, $\bar{f}\bar{g} = \overline{\Phi_n}$. Since $\bar{f}$ and $\bar{g}$ share a factor, then $\overline{\Phi_n}$ has a multiple root inside $\mathbf{F}_p[x]$.

Recalling the formula in the proof of lemma 14.11, this tells us that $x^n - 1$ also has a multiple root in $\mathbf{F}_p[x]$. But since p doesn't divide n, then $x^n - 1$ is separable, which is a contradiction. Thus, we cannot have $g(\zeta^p) = 0$.

Observe: this tells us that for any root ρ of f and for any prime p not dividing n, then $f(\rho^p) = 0$. If ζ is a root of f, then any other primitive root of unity is of the form ζ^k, for k coprime to n, which means $k = p_1 \cdots p_m$, where the p_i's do not divide n.

We know that $f(\zeta^{p_1}) = 0$. Then in our observation, let $\rho = \zeta^{p_1}$ and $p = p_2$. Then $f(\zeta^{p_1 p_2}) = 0$. Continuing, then $f(\zeta^k) = 0$. This means that f has *every* primitive root of unity as a root, which means $f = \Phi_n$. Since we assumed f is irreducible, this completes the proof. □

§15 April 1, 2020

Today we prove the Riemann Hypothesis. Haha, April Fools! Instead we will talk about Galois theory. The idea behind Galois theory is to study the automorphisms of fields, and how they permute the roots of polynomials. It provides a connection between field theory and group theory. It is named after the mathematician Evariste Galois, who at the age of 18 solved the problem of solving polynomials by radicals, a problem which had remained unsolved for over 300 years. He was also very active in the French politics (and spent 6 months in jail). Sadly though, he died in a duel two years later at the age of 20 (no one knows what the duel was about, but apparently there is some evidence that it was over a romantic interest). There were also riots at his funeral. Very interesting person.

§15.1 Galois Theory

We start with some definitions.

Definition 15.1 — An isomorphism σ from a field K to itself is called an **automorphism** of K. The set of automorphisms of a field K is denoted $\mathrm{Aut}(K)$. We say that an automorphism **fixes** an element $a \in K$ if $\sigma(a) = a$, and that it fixes a set A if it fixes all $a \in A$.

If K/F is a field extensions, then we write $\mathrm{Aut}(K/F)$ for the set of all automorphisms of K which fix F. NB: by definition, these automorphisms fix *each element* of F: we're *not* saying that F is just mapped to itself.

Note that $\mathrm{Aut}(K)$ is a group under composition. If $\sigma_1, \sigma_2 \in \mathrm{Aut}(K/F)$, and $a \in F$ then

$$(\sigma_1 \circ \sigma_2)(a) = \sigma_1(\sigma_2(a)) = \sigma_1(a) = a,$$

and if $\sigma : a \mapsto a$, then $\sigma^{-1} : a \mapsto a$ as well, so $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.

Also, suppose that $f(x) \in F[x]$, and $\alpha \in K$ is a root of f. Then we can write

$$0 = f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0.$$

Applying σ to the above gives

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(a_n \alpha^n + \cdots + a_1 \alpha + a_0) \\ &= a_n \sigma(\alpha)^n + \cdots + a_1 \sigma(\alpha) + a_0 \\ &= f(\sigma(\alpha)), \end{aligned}$$

where we've used the fact that σ fixes F and the fact that σ is a field homomorphism. Thus $\sigma(\alpha)$ is also a root of f: the group $\mathrm{Aut}(K/F)$ permutes the roots of a given polynomial.

Let's look at some examples to see how this works in practice.

Example 15.2

The group $\mathrm{Aut}(\mathbf{Q})$ is the trivial group, since any automorphism must fix 1, and preserve sums and quotients. We write 1 for the identity map, so $\mathrm{Aut}(\mathbf{Q}) = \{1\}$. Similarly, $\mathrm{Aut}(\mathbf{F}_p) = \{1\}$

Example 15.3

Let $F = \mathbf{Q}$, and let $K = \mathbf{Q}(\sqrt{2})$. Then $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K)$. Since $\sqrt{2}$ is a root of $x^2 - 2 \in F[x]$, then $\sigma(\sqrt{2})$ must also be a root. Thus, $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Since we can write any element in $\mathbf{Q}(\sqrt{2})$ as $a + b\sqrt{2}$, where $a, b \in \mathbf{Q}$, then σ is completely determined by its action on $\sqrt{2}$. So there are precisely two automorphisms of $\mathbf{Q}(\sqrt{2})$, so $\mathrm{Aut}(K/F) = \{1, \sigma\}$, the cyclic group of order 2.

Example 15.4

Let $F = \mathbf{Q}$, and $K = \mathbf{Q}(\sqrt[3]{2})$. As above, any automorphism is determined by its action on $\sqrt[3]{2}$. Suppose $\sigma \in \mathrm{Aut}(K/F)$, so $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2$. But the only other roots of $\sqrt[3]{2}$ are imaginary, so we must have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, and thus $\mathrm{Aut}(K/F) = \{1\}$.

We've seen that if we have a given field K and a subfield F, then we get a group $\mathrm{Aut}(K/F)$. We can also go the other way. Suppose we have a field K, and a subgroup H of $\mathrm{Aut}(K)$. Then we can get a subfield of K. We define the **fixed field** of $H \subseteq \mathrm{Aut}(K)$ as the set of all elements of K fixed by every automorphism in H.

Exercise 15.5. Check that the fixed field of a subgroup $H \subseteq \mathrm{Aut}(K)$ is actually a field.

The operations of going back-and-forth from field to group are *inclusion-reversing*. This means that if $F_1 \subseteq F_2 \subseteq K$, then $\mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$. Intuitively, "the fewer things we have to fix, the automorphisms there are." On the other hand, if $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K)$ have fixed fields F_1 and F_2 respectively, then $F_2 \subseteq F_1$. Intuitively, "fewer automorphisms fix more things."

Example 15.6

Let $K = \mathbf{Q}(\sqrt{2})$, and $F = \mathbf{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is the set of $a + b\sqrt{2}$ fixed by all the automorphisms, which is just $\mathbf{Q}$, since there is an automorphism which takes $\sqrt{2} \mapsto -\sqrt{2}$. The fixed field of $\{1\} \subseteq \mathrm{Aut}(K/F)$ is $\mathbf{Q}(\sqrt{2})$.

Example 15.7

Let $K = \mathbf{Q}(\sqrt[3]{2})$, and $F = \mathbf{Q}$. The fixed field of $\mathrm{Aut}(K/F)$ is $\mathbf{Q}(\sqrt[3]{2})$, since there is only one automorphism, the identity.

We'll now study some more properties of the automorphism groups of field extensions. First we'll put a natural bound on the size of $\mathrm{Aut}(K/F)$ if K is the splitting field of a polynomial.

Theorem 15.8

Let K be the splitting field of a polynomial $f(x) \in F[x]$. Then $\mathrm{Aut}(K/F)$ has at most $[K : F]$ elements, with equality if f is separable.

Proof. We'll actually prove something more general. Namely, if ϕ is an isomorphism $\phi : F \to F'$, where K is a splitting field of $f(x)$ and K' is a splitting field of the corresponding $f' = \phi(f)$, then how many isomorphisms $\sigma : K \to K'$ does the map ϕ extend to? This is visualized in the diagram

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K' \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

The special case $F = F'$ and $K = K'$ is the statement of the theorem.

We'll prove this by induction on the degree of the extension, $n = [K : F]$. If $n = 1$, then $\sigma = \phi$ is the only extension. For $n \geq 2$, suppose that the result holds up to $n - 1$. Let $p(x)$ be an irreducible factor of $f(x)$, and $p'(x)$ the corresponding irreducible factor of $f'(x)$. Adjoin one of the roots, α, of $p(x)$ to the field F. Then for any root α' of $p'(x)$, we have an isomorphism $\phi'(\alpha) = \alpha'$. There are as many ways to do this as the number of roots of $p(x)$, which is at most the degree of $p(x)$, with equality if $p(x)$ is separable. This extension is visualized in the following diagram.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\phi'} & F'(\alpha') \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F'. \end{array}$$

Now, by the induction hypothesis, there are at most $[K : F(\alpha)]$ ways to extend each of these ϕ' to an automorphism σ, with equality if $f(x)/(x - \alpha)$ is separable. So the total number of ways to extend the map ϕ is at most $[K : F(\alpha)] \cdot [F(\alpha) : F] = [K : F]$, with equality if $f(x)$ is separable. This is visualized in the following diagram, where the bottom layer is the diagram from above, and the top layer is the induction step.

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K' \\ \downarrow & & \downarrow \\ F(\alpha) & \xrightarrow{\phi'} & F'(\alpha') \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F'. \end{array}$$

□

Exercise 15.9. Prove that if K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K:F]$.

Definition 15.10 — A finite extension K/F is **Galois** if $|\mathrm{Aut}(K/F)| = [K:F]$. If K/F is Galois, then $\mathrm{Aut}(K/F)$ is called the **Galois group** of K/F.

What we showed above can be rephrased in the following theorem.

Theorem 15.11

If K is the splitting field of a separable polynomial in $F[x]$, then K/F is Galois. (The converse is also true, to be proven later.)

Example 15.12

The extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is Galois, but the extension $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is *not*. Over $\mathbf{Q}[x]$, the splitting field of any polynomial is Galois over $\mathbf{Q}$.

Example 15.13

Let $F = \mathbf{Q}$, and $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Since K is the splitting field of $(x^2-2)(x^2-3)$, it is Galois. To determine the Galois group, note that any automorphism sends

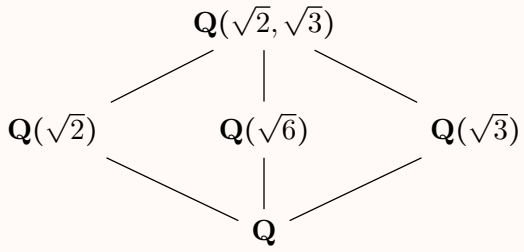
$$\sqrt{2} \mapsto \pm\sqrt{2}$$
$$\sqrt{3} \mapsto \pm\sqrt{3}.$$

Thus there are $2 \cdot 2 = 4$ candidates for automorphisms. Since $|\mathrm{Aut}(K/F)| = [K:F] = 4$, then all four of these are indeed automorphisms. Since all the automorphisms are order 2, then the Galois group is the Klein 4 group. Now, remember that for each subgroup of $\mathrm{Aut}(K/F)$, there is a fixed field. Define the automorphisms as follows

$$1 : \sqrt{2}, \sqrt{3} \mapsto \sqrt{2}, \sqrt{3}$$
$$\sigma : \sqrt{2}, \sqrt{3} \mapsto -\sqrt{2}, \sqrt{3}$$
$$\tau : \sqrt{2}, \sqrt{3} \mapsto \sqrt{2}, -\sqrt{3}.$$

The extension is degree 4, and has basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. The fixed field of $\{1\}$ is $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, the fixed field of $\{1, \sigma\}$ is $\mathbf{Q}(\sqrt{3})$, since $\sigma : \sqrt{3} \mapsto \sqrt{3}$, and similarly the fixed field of $\{1, \tau\}$ is $\mathbf{Q}(\sqrt{2})$. Neither of these fix $\sqrt{6}$, since each takes $\sqrt{6} = \sqrt{2}\sqrt{3} \mapsto -\sqrt{2}\sqrt{3} = -\sqrt{6}$. The fixed field of $\{1, \sigma\tau\}$ is $\mathbf{Q}(\sqrt{6})$, since $\sigma\tau(\sqrt{6}) = \sqrt{2}\sqrt{3}$.

This can all be visualized in the following diagram.



The best way to learn Galois theory (or anything really) is by doing lots of examples. Thus, we will do more examples.

Example 15.14

Let $F = \mathbf{Q}$, and K be the splitting field of $x^3 - 2$, which is $\mathbf{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Any automorphism of K/F must permute the roots of $x^3 - 2$, and there are $3! = 6$ such permutations. Since $|\mathrm{Aut}(K/F)| = [K : F] = 6$, then any permutation of the roots is an automorphism, and $\mathrm{Aut}(K/F) \simeq S_3$.

Example 15.15

Let's do something with a finite field. Let $F = \mathbf{F}_p$, and $K = \mathbf{F}_{p^n}$. We showed already that K is the splitting field of $x^{p^n} - x$, a separable polynomial. Thus K/F is Galois and $|\mathrm{Aut}(K/F)| = [K : F] = n$. One of the automorphisms in this group is the Frobenius map $\sigma : a \mapsto a^p$, and in fact the map $\sigma^k : a \mapsto a^{p^k}$ is also an automorphism for any $k \geq 1$. Note that $\sigma^n = \mathrm{id}$, and for each $k < n$, $x^{p^k} = x$ has at most p^k solutions, so σ^k is not the identity for $k < n$. Since $[K : F] = n$ and σ has order n, the Galois group is cyclic of order n, generated by the Frobenius map.

§16 April 3, 2020

§16.1 The Fundamental Theorem of Galois Theory, Part I

Today we will state and prove the Fundamental Theorem of Galois Theory.

Theorem 16.1 (Fundamental Theorem of Galois Theory)

If K/F is a Galois extension, then there is a bijective correspondence between subgroups of $\mathrm{Aut}(K/F)$ and intermediate fields L, with $F \subseteq L \subseteq K$. The correspondence is given by taking fixed fields.

We'll prove this using the following key theorem.

Theorem 16.2 (Key Theorem)

If K is a field and G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| = [K : F]$.

In order to prove these, we need a few more definitions and results. The **character** χ of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$. Note that any automorphism of a field K gives a character of the multiplicative group $K^\times$.

Theorem 16.3

If $\chi_1, \dots, \chi_n$ are distinct characters of a group G with values in L, then they are L-linearly independent, i.e. if $a_1\chi_1 + \cdots + a_n\chi_n = 0$, then $a_1 = \cdots = a_n = 0$.

Proof. Suppose that $\chi_1, \dots, \chi_n$ are distinct and linearly dependent. Choose n minimal such that this is true, i.e. n is the smallest number such that there are n distinct linearly dependent characters. Pick $a_1, \dots, a_n$ not all zero such that $a_1\chi_1 + \cdots + a_n\chi_n = 0$.

Now, since the χ_i are distinct we can find $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_n(g_0)$. For any $g \in G$, then

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \cdots + a_n\chi_n(g_0g) = 0.$$

Since the χ_i are homomorphisms, then

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0. \tag{16.1}$$

Now, multiplying $\chi_n(g_0)$ times $a_1\chi_1 + \cdots + a_n\chi_n = 0$ and evaluating at g, we have

$$a_1\chi_n(g_0)\chi_1(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0. \tag{16.2}$$

Subtracting equation (16.2) from (16.1), we have

$$a_1(\chi_1(g_0) - \chi_n(g_0))\chi_1(g) + \cdots + a_{n-1}(\chi_{n-1}(g_0) - \chi_n(g_0))\chi_{n-1}(g) = 0,$$

since the χ_n terms are the same. Because we had $\chi_1(g_0) \neq \chi_n(g_0)$, then we know at least $a_1(\chi_1(g_0) - \chi_n(g_0) \neq 0$, so we have written 0 as a linear combination of the χ_i with not all zero coefficients. But this contradicts the minimality assumption on n. □

We'll now work towards proving the key theorem above. We do this in two steps, proving both inequalities.

Lemma 16.4

Let K be a field, and let G be a finite subgroup of $\mathrm{Aut}(K)$, and F the fixed field of G. Then $|G| \leq [K : F]$.

Proof. Suppose for contradiction that $n = |G| > [K : F] = m$. Write the elements of G as $G = \{\sigma_1, \dots, \sigma_n\}$. Let $\omega_1, \dots, \omega_m$ be a basis of for K over F (as a vector space). We'll examine the actions of the σ_i on this basis to get a contradiction to independence of characters.

Consider the following system of equations:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \cdots + \sigma_n(\omega_m)x_n &= 0. \end{aligned}$$

This is a system of m equations in n unknowns, with $n > m$, so there is a nonzero solution, which we denote $\beta_1, \dots, \beta_n \in K$. We can write

$$\begin{aligned} \sigma_1(\omega_1)\beta_1 + \sigma_2(\omega_1)\beta_2 + \cdots + \sigma_n(\omega_1)\beta_n &= 0 \\ &\vdots \\ \sigma_1(\omega_m)\beta_1 + \sigma_2(\omega_m)\beta_2 + \cdots + \sigma_n(\omega_m)\beta_n &= 0. \end{aligned}$$

Let $\alpha \in K$ be arbitrary. Since $\{\omega_i\}$ is a basis, we can write $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$, with $a_i \in F$. Since F is the fixed field, then $\sigma_i(a_k\omega_j) = a_k\sigma_i(\omega_j)$ for each i, j, k. Multiplying the i'th equation above by a_i, and then adding together all the equations, we get

$$\sigma_1(\sum a_i\omega_i)\beta_1 + \sigma_2(\sum a_i\omega_i)\beta_2 + \cdots + \sigma_n(\sum a_i\omega_i)\beta_n = 0,$$

which can be rewritten as

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0.$$

Since α was arbitrary, this means that $\sigma_1\beta_1 + \cdots + \sigma_n\beta_n = 0$. Since the σ_i are distinct characters, and $\beta_i \in K$, this contradicts independence of characters. □

We now prove the other inequality.

Lemma 16.5

Let $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$ with fixed field F. Then $|G| \geq [K : F]$.

Proof. Suppose for contradiction that $n = |G| < [K : F]$, so there exist $n + 1$ F-linearly independent elements in K, which we denote $\alpha_1, \dots, \alpha_{n+1}$. Consider the system of linear equations

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0. \end{aligned}$$

This is a system of n equations in $n + 1$ unknowns, so there is a solution $\beta_1, \dots, \beta_{n+1} \in K$ with not all β_i zero. Choose a solutions set $\beta_1, \dots, \beta_{n+1}$ with the minimal number of nonzero β_i. Without loss of generality, we can assume $\beta_{n+1} \neq 0$. Dividing by β_{n+1}, we can assume $\beta_{n+1} = 1 \in F$. If we show that all the β_i are in F, then plugging this into the first equation, we obtain an expression $\alpha_1\beta_1 + \cdots + \alpha_{n+1}\beta_{n+1} = 0$ with $\beta_i \in F$, which contradicts the linear independence of α_i, which is our desired contradiction. Thus, we need to show that all the β_i are in F.

To this end, suppose that $\beta_j \notin F$ for some j, and without loss of generality, assume $j = 1$. By the definition of F as the fixed field of G, then since $\beta_1 \notin F$ there is an automorphism $\sigma_{k_0} \in G$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$. Apply σ_{k_0} to the i'th equation in the system above to get

$$\sigma_{k_0}\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_{k_0}\sigma_i(\alpha_{n+1})\sigma_{k_0}(\beta_{n+1}) = 0.$$

We know that $\beta_{n+1} \in F$, so $\sigma_{k_0}(\beta_{n+1}) = \beta_{n+1}$ since $\sigma_{k_0} \in G$.

Since $\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \dots, \sigma_{k_0}\sigma_n$ is just a permutation of $\sigma_1, \dots, \sigma_n$, then we can assume without loss of generality that

$$\sigma_1(\alpha_1)\sigma_{k_0}(\beta_1) + \cdots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0. \tag{16.3}$$

Recalling the definition of the β_i, we have

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{n+1})\beta_{n+1} = 0, \tag{16.4}$$

for each i. Subtracting 16.4 from 16.3, we have

$$(\beta_1 - \sigma_{k_0}(\beta_1))\sigma_i(\alpha_1) + \cdots + (\beta_n - \sigma_{k_0}(\beta_n))\sigma_i(\alpha_n) = 0.$$

But then $\beta_1 - \sigma_{k_0}(\beta_1), \ldots, \beta_n - \sigma_{k_0}(\beta_n)$ is a solution to our system of equations with fewer nonzero elements than $\beta_1, \ldots, \beta_n$, which contradicts our minimality assumption. □

Combining the inequalities in the two lemmas above give the key theorem.

Theorem 16.6 (Key Theorem)
If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $|G| = [K : F]$.

We'll now work towards proving the fundamental theorem of Galois theory.

Corollary 16.7
If K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$, with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$. So K/F is Galois if and only if F is the fixed field of $\mathrm{Aut}(K/F)$.

Proof. Let F_1 be the fixed field of $G = \mathrm{Aut}(K/F)$. By definition, G fixes F, so $F \subseteq F_1 \subseteq K$. By the key theorem, $[K : F_1] = |\mathrm{Aut}(K/F)|$, so

$$[K : F] = [K : F_1][F_1 : F] = |\mathrm{Aut}(K/F)|\,[F_1 : F].$$

So $|\mathrm{Aut}(K/F)| \leq [K : F]$, with equality if and only if $F_1 = F$ (i.e. $[F_1 : F] = 1$). □

Lemma 16.8
If K/F is a Galois extension, then every irreducible $p(x) \in F[x]$ which has a root in K is separable and splits completely in K.

Proof. Let $G = \mathrm{Aut}(K/F)$, and write $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Let $p(x)$ be irreducible, and let $\alpha \in K$ be a root of $p(x)$. We need to show that $p(x)$ is separable and splits completely. Consider $\{\alpha = \sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$. These are all roots of $p(x)$ since G permutes roots. Suppose that r of them are distinct, and label them $\alpha = \alpha_1, \ldots, \alpha_r$. Consider the polynomial $f(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_r)$. The coefficients are all products of the α_i, and so they are fixed by elements of G. That is, the coefficients lie in the fixed field of G. By corollary 16.7, the fixed field of g is F, and so $f(x) \in F[x]$.

Since $p(x)$ is irreducible it is the minimal polynomial with its roots, so $p(x) \mid f(x)$. Since $f(x)$ has fewer roots than $p(x)$, then $f(x) \mid p(x)$. So $f(x)$ and $p(x)$ are the same up to a unit, which means $p(x) = (x - \alpha)\cdots(x - \alpha_r)$, and is therefore separable and splits completely. □

Corollary 16.9

An extension K/F is Galois if and only if it is the splitting field of a separable polynomial over F.

Proof. We already proved the fact that the splitting field of a separable polynomial is a Galois in the last section. So suppose that K/F is Galois, and let $\omega_1, \ldots, \omega_n$ be a basis for K/F, and let $p_1, \ldots, p_n$ be the minimal polynomials for $\omega_1, \ldots, \omega_n$ respectively. By lemma 16.8, each of the p_i is separable and splits completely. Let $q_1(x), \ldots, q_r(x)$ be the *distinct* p_i's. Let $g(x) = q_1(x) \cdots q_r(x)$. Then K is the splitting field of $g(x)$. □

Corollary 16.10

If K/F is Galois, and $F \subseteq E \subseteq K$, then K/E is Galois.

Proof. Since K/F is Galois, then K is the splitting field of some polynomial $p(x) \in F[x]$. Since $F \subseteq E$, then $p(x) \in E[x]$ as well, so K is also the splitting field of $p(x)$ as a polynomial in E, so K/E is Galois. □

Corollary 16.11

If G is a finite subgroup of $\mathrm{Aut}(K)$ with fixed field F, then $G = \mathrm{Aut}(K/F)$.

Proof. Since G has fixed field F, then any element of G is in $\mathrm{Aut}(K/F)$, so $|G| \leq |\mathrm{Aut}(K/F)|$. By the key theorem, $|G| = [K : F]$, so K/F is finite, since G is finite. By corollary 16.7, then $|\mathrm{Aut}(K/F)| \leq [K : F]$, so $|\mathrm{Aut}(K/F)|\,|G| \leq |\mathrm{Aut}(K/F)|$. Since G is a subset of $\mathrm{Aut}(K)$ and $|G| = |\mathrm{Aut}(K/F)|$, then $G = \mathrm{Aut}(K/F)$. □

Corollary 16.12

If $G_1 \neq G_2$ are distinct finite subgroups of $\mathrm{Aut}(K)$, then their fixed fields are distinct.

Proof. By the corollary above, if the fixed fields of G_1, G_2 are F_1, F_2 respectively, then we have $G_1 = \mathrm{Aut}(K/F_1)$ and $G_2 = \mathrm{Aut}(K/F_2)$. Thus $F_1 = F_2$ implies $G_1 = G_2$, and the contrapositive is the desired result. □

We now state the first part of the fundamental theorem.

Theorem 16.13 (Fundamental Theorem of Galois Theory, Part I)

Let K/F be a Galois extension, and let $G = \mathrm{Aut}(K/F)$ be the Galois group.

There is a bijection between the subfields E of K containing F, and the subgroups H of G.

The bijection is given by sending a field E to the subgroup of elements of G which fix E, and sending a subgroup H to the fixed field of H. Moreover, this correspondence is inclusion reversing.

1. If E_1 and E_2 correspond to H_1 and H_2 respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \subseteq H_1$.
2. If H corresponds to E, then $[K : E] = |H|$, and $[E : F] = |G : H|$.
3. The extension K/E is Galois, with Galois group $\mathrm{Aut}(K/E) = H$.

We visualize the fundamental theorem in the following two pictures.
Increasing size of subgroup to get smaller subfields:

$$\begin{array}{c} K = \text{fixed field of } 1 \\ \Big| {\scriptstyle |H|} \\ E = \text{fixed field of } H \\ \Big| {\scriptstyle |G:H|} \\ F = \text{fixed field of } G \end{array}$$

Fixing more elements of K to get smaller subgroups:

$$\begin{array}{c} G = \mathrm{Aut}(K/F) = \text{automorphisms fixing } F \\ \Big| {\scriptstyle [E:F]} \\ H = \text{automorphisms fixing } E \\ \Big| {\scriptstyle [K:E]} \\ 1 = \text{automorphisms fixing } K \end{array}$$

Proof. Corollary 16.12 shows that the map sending a group to its fixed field is injective. Corollary 16.10 shows that K/E is Galois for intermediate fields E, so E is the fixed field of $\mathrm{Aut}(K/E)$, and thus the correspondence is surjective.

If E is the fixed field of H then by corollary 16.11, $\mathrm{Aut}(K/E) = H$, so $|H| = \mathrm{Aut}(K/E) = [K : E]$. Since the extension K is Galois, by definition $[K : F] = |G|$. Multiplicativity of degrees and taking quotients gives $|G : H| = |G/H| = |G|/|H| = [E : F]$. □

§17 April 8, 2020

§17.1 The Fundamental Theorem of Galois Theory, Part II

Last time, we covered the first part of the fundamental theorem of Galois theory, which said that if K/F is Galois, and $G = \mathrm{Aut}(K/F)$, then there is a bijection between subfields E of K containing F and the subgroups H of G. The second part will give us more information about the intermediate fields E.

Theorem 17.1 (Fundamental Theorem of Galois Theory, Part II)

Let K/F be a Galois extension with Galois group $G = \mathrm{Aut}(K/F)$, and E an intermediate field (i.e. $F \subseteq E \subseteq K$), which by the first part of the theorem corresponds to a subgroup $H \subseteq G = \mathrm{Aut}(K/E)$. Then the field E is Galois over F if and only if H is a normal subgroup of G, in which case $\mathrm{Aut}(E/F) \simeq G/H$:

$$\begin{array}{ccc} K & & 1 \\ \Big| \text{(always Galois)} & & \Big| \text{(always normal)} \\ E & & H \\ \Big| \text{(Galois)} & & \Big| \text{(normal)} \\ F & & G \end{array}$$

Before we prove the theorem, let's examine in more detail how the automorphisms in $\mathrm{Aut}(E/F)$ relate to the automorphisms in $\mathrm{Aut}(K/F)$. If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma|_E$ isn't necessarily in $\mathrm{Aut}(E/F)$, since there's no guarantee that the image of E under sigma is equal to E. That is, we don't necessarily have $\sigma(E) = E$. All we know is that $\sigma|_E$ is an injective map $\sigma|_E : E \to K$, which fixed F. An injective homomorphism is called an **embedding**. We denote the set of embeddings of E into K which fix F by $\mathrm{Emb}(E/F)$. If $\tau : E \to K$ is an injective map fixing F, then its restriction is an isomorhpism of E onto its image. Since K/F is Galois, then K is the splitting field of some separable $f(x) \in F[x]$, and since τ fixes F, then $\tau(f(x)) = f(x) \in \tau(E)[x]$, and τ extends to an automorphism $\sigma \in \mathrm{Aut}(K/F)$. So the map $\sigma : \mathrm{Aut}(K/F) \to \mathrm{Emb}(E/F)$ given by $\sigma \mapsto \sigma|_E$ is a surjection. Now we prove the theorem.

Proof. We first show that E/F is Galois if and only if $\sigma(E) = E$ for all $\sigma \in G = \mathrm{Aut}(K/F)$. We then show that $\sigma(E) = E$ for all $\sigma \in G$ if and only if H is normal.

Suppose $\sigma, \sigma' \in G$, and consider $\sigma|_E$ and $\sigma'|_E$. These restrictions are equal if and only if $(\sigma^{-1}\sigma')|_E$ is the identity, which is equivalent to saying $\sigma^{-1}\sigma'$ must fix E, which means it must be in $\mathrm{Aut}(K/E) = H$, which means $\sigma \in \sigma' H$. So $\sigma|_E = \sigma'|_E$ if and only if $\sigma' H = \sigma H$. So for each distinct σ, there is exactly one coset of H in G. That is, the embeddings of E which fix F are in one to one correspondence with the cosets of H in G, so $|\mathrm{Emb}(E/F)| = [G : H] = [E : F]$. The extension E/F is Galois by definition if and only if $[E : F] = |\mathrm{Aut}(E/F)|$, which means E/F is Galois if and only if $|\mathrm{Emb}(E/F)| = [E : F] = |\mathrm{Aut}(E/F)|$, which happens if and only if $\sigma(E) = E$ for all $\sigma \in G$.

Now, when is $\sigma(E) = E$ for all $\sigma \in G$? By the one-to-one correspondence in the first part of the fundamental theorem, this happens exactly when $\mathrm{Aut}(K/E) = \mathrm{Aut}(K/\sigma(E))$. We now claim that $\mathrm{Aut}(K/\sigma(E)) = \sigma H \sigma^{-1}$, where $H = \mathrm{Aut}(K/E)$. To this end suppose that $\tau \in \mathrm{Aut}(K/\sigma(E))$, and let $\tau' = \sigma^{-1}\tau\sigma$. Then for all $a \in E$, we have

$$\tau'(a) = \sigma^{-1}\tau\sigma(a) = \sigma^{-1}\sigma(a) = a,$$

since τ fixes $\sigma(E)$. Thus $\tau' \in H$, which means $\mathrm{Aut}(K/\sigma(E)) \subseteq \sigma H \sigma^{-1}$. For the other direction, note that

$$|\mathrm{Aut}(K/\sigma(E))| = |\mathrm{Aut}(K/E)| = [K : E] = |H| = \left|\sigma H \sigma^{-1}\right|.$$

So we have $\mathrm{Aut}(K/\sigma(E)) = \sigma H \sigma^{-1}$.

We've shown E/F is Galois if and only if $\sigma(E) = E$ for all $\sigma \in G$, which happens if and only if $H = \sigma H \sigma^{-1}$ for all $\sigma \in G$, which by definition means that H is normal. Our proof also gave a construction of a bijection between $\mathrm{Aut}(E/F)$ and the cosets of H in $\mathrm{Aut}(K/F)$ which respects composition. This, $\mathrm{Aut}(E/F) \simeq G/H$, which concludes the proof. □

As an application of the second part of the fundamental theorem of Galois theory, consider the splitting field of $x^3 - 2$, which we showed was $\mathbf{Q}(\sqrt[3]{2}, \rho)$, where $\rho = e^{2\pi i/3}$. We have the following intermediate fields between $\mathbf{Q}(\sqrt[3]{2}, \rho)$ and $\mathbf{Q}$.

$$\begin{aligned}
\mathbf{Q} \subseteq \mathbf{Q}(\rho) \subseteq \mathbf{Q}(\sqrt[3]{2}, \rho) \\
\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[3]{2}, \rho) \\
\mathbf{Q} \subseteq \mathbf{Q}(\rho\sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[3]{2}, \rho) \\
\mathbf{Q} \subseteq \mathbf{Q}(\rho^2\sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[3]{2}, \rho).
\end{aligned}$$

The first of these extensions, $\mathbf{Q}(\rho)/\mathbf{Q}$, is Galois and the last three are not. These intermediate fields correspond respectively to the group subgroup inclusions

$$\begin{aligned}
1 \subseteq \langle \sigma \rangle \subseteq S_3 \\
1 \subseteq \langle \tau \rangle \subseteq S_3 \\
1 \subseteq \langle \tau\sigma \rangle \subseteq S_3 \\
1 \subseteq \langle \tau\sigma^2 \rangle \subseteq S_3.
\end{aligned}$$

The first subgroup $\langle \sigma \rangle \subseteq S_3$ is normal, and the last three are not.

§17.2 The Fundamental Theorem of Galois Theory, Part III

We now state the third part of the fundamental theorem of Galois theory, which you can prove for yourself as an exercise.

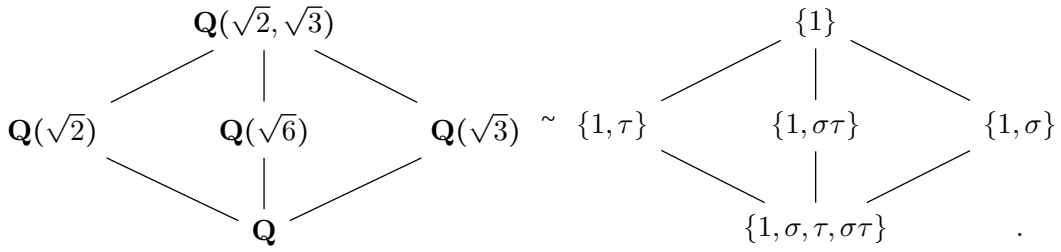
Theorem 17.2 (Fundamental Theorem of Galois Theory, Part III)
If intermediate fields $F \subseteq E_1, E_2 \subseteq K$ correspond to subgroups $H_1, H_2 \subseteq G = \mathrm{Aut}(K/F)$, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$, and E_1E_2 corresponds to $H_1 \cap H_2$.

Proof. See exercise 17.3. □

Exercise 17.3. Prove theorem 17.2.

As an application of this, consider the field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$. This has intermediate subfields $\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{6}), \mathbf{Q}(\sqrt{3})$, corresponding to $\{1, \tau\}, \{1, \sigma\tau\}, \{1, \sigma\}$ respectively. The field $\mathbf{Q}$ corresponds to $\{1, \sigma, \tau, \sigma\tau\}$, and $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ corresponds to $\{1\}$. The intersection $\mathbf{Q}(\sqrt{2}) \cap \mathbf{Q}(\sqrt{3})$ is $\mathbf{Q}$, which is the field corresponding to $\langle \{1, \tau\}, \{1, \sigma\} \rangle$. The composite is $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, which corresponds to $\{1, \tau\} \cap \{1, \sigma\} = \{1\}$. This is visualized in the

following diagram:



§17.3 Examples

We just did a lot of abstract Galois theory. Let's compute some examples to see how it all works out in real life. One definition before we begin: if K/F is an extension, and α is an algebraic element, and $f(x)$ is the minimal polynomial for α, then the roots of $f(x)$ are called the **Galois conjugates**, or just conjugates, of α. Recall that any $\sigma \in \mathrm{Aut}(K/F)$ permutes the roots of a polynomial.

Example 17.4 ($\mathbf{Q}(\sqrt{2}+\sqrt{3})$)

We compute the minimal polynomial of $\sqrt{2}+\sqrt{3}$ using Galois theory. The extension $\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}$ is Galois of degree 4, since it's the splitting field of $(x^2-2)(x^2-3)$. Since $\sqrt{2}+\sqrt{3} = 1\cdot\sqrt{2}+1\cdot\sqrt{3}$, then $\mathbf{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2},\sqrt{3})$. The roots of the minimal polynomial $f(x)$ are the conjugates of $\sqrt{2}+\sqrt{3}$ under $\mathrm{Aut}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$. So the roots of $f(x)$ are $\pm\sqrt{2}\pm\sqrt{3}$, which are all distinct. Then the minimal $f(x)$ is

$$f(x) = (x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})).$$

Expanding and simplifying, this is $f(x) = x^4 - 10x^2 + 1$. This is irreducible and $\mathbf{Q}(\sqrt{2}+\sqrt{3})$ has degree 4, and thus $\mathbf{Q}(\sqrt{2}+\sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$.

Example 17.5 (Splitting field of x^8-2)

Denote the splitting field of x^8-2 by K, which is generated by $\theta = \sqrt[8]{2}$ and $\zeta = e^{2\pi i/8}$, a primitive 8th root of unity, so $K = \mathbf{Q}(\sqrt[8]{2},\zeta)$.

An automorphism of K is completely determined by what it does to $\sqrt[8]{2}$ and ζ. There are 8 options for the action on $\theta = \sqrt[8]{2}$, since it's minimal polynomial is x^8-2, and there are 4 options for the action of ζ, since the 8'th cyclotomic polynomial, the minimal polynomial of ζ, has degree $\phi(8) = 4$. This *doesn't* mean that there are $4\cdot 8 = 32$ automorphisms. There are relations that do not allow for certain automorphisms. For example, $\theta^4 = \sqrt{2} = \zeta+\zeta^7$. So we can't send $\zeta \mapsto \zeta^3$ and $\theta \mapsto \theta$, since this breaks the relation: $\zeta^3+\zeta^{21} = -\sqrt{2}$.

Examining relations like this can get very complicated very quickly. It's easier to just check the degree of the field extension first. Observe $\zeta = \frac{\sqrt{2}}{2}(1+i)$, and one can show that $K = \mathbf{Q}(\sqrt[8]{2},\zeta) = \mathbf{Q}(\sqrt[8]{2},i)$. The degree of this extension is at most $2\cdot 8 = 16$, but strictly greater than 8, since $\mathbf{Q}(\sqrt[8]{2})$ has degree 8 and $\sqrt[8]{2}$ is real and i is imaginary. Thus it must have degree exactly 16, since 8 must divide the degree (it contains $\mathbf{Q}(\sqrt[8]{2})$).

The extension is also Galois (the splitting field of a separable polynomial), so $G = \mathrm{Aut}(K/\mathbf{Q})$ has 16 elements (the same as the degree), which are determined by

their action on $\theta = \sqrt[8]{2}$ and i. Since i is a root of x^2+1, we must have $i \mapsto \pm i$, and $\sqrt[8]{2}$ is a root of x^8-2, so we must have $\sqrt[8]{2} \mapsto \zeta^n \sqrt[8]{2}$, for $n = 0, 1, \ldots, 7$. There are $2 \cdot 8 = 16$ of these total, so they're all automorphisms. Letting

$$\sigma : \theta \mapsto \zeta\theta$$
$$\sigma : i \mapsto i,$$

and

$$\tau : \theta \mapsto \theta$$
$$\tau : i \mapsto -i,$$

then $G = \langle \sigma, \theta \rangle$ with the relations $\sigma^2 = 1$, $\theta^8 = 1$, and $\sigma\tau = \tau\sigma^3$. This completely determines the group, which is the "quasidihedral group" of order 16.

Example 17.6 (Galois Group of Finite Fields)

Let $F = \mathbf{F}_p$ and $K = \mathbf{F}_{p^n}$. We showed that K is the splitting field of $x^{p^n} - x$, a separable polynomial. Thus, K/F is Galois, and $|\mathrm{Aut}(K/F)| = [K : F] = n$. One of the automorphisms is the Frobenius map $\sigma : a \mapsto a^p$ for $a \in K$. For each $k \geq 1$, then $\sigma^k : a \mapsto a^{p^k}$ is also an automorphism. The order of σ is n, since σ^n is the identity, and σ^k is not the identity for $k < n$, since $x^{p^k} = x$ has at most p^k solutions (if σ^k were the identity, it would have n solutions).

Since σ has order n, the Galois group of K/F is cyclic of order n, generated by σ. By the one-to-one correspondence from the fundamental theorem, then the subfields of $\mathbf{F}_{p^n}$ and the subgroups of $\mathbf{Z}/n\mathbf{Z}$ are in one-to-one correspondence. The subgroups of $\mathbf{Z}/n\mathbf{Z}$ are the subgroups generated by d, where $d|n$. So for each divisor $d|n$, there is a unique subfield E of $\mathbf{F}_{p^n}$, and no other subfields.

That is, for each $d \mid n$, and H the subgroup generated by σ^d, then $|H| = n/d$, so if E is the fixed field of σ^d, then $[K : E] = n/d$ and $[E : F] = d$. Since finite fields of finite degree are all unique, then $E = \mathbf{F}_{p^d}$. So the subfields of $\mathbf{F}_{p^n}$ are the fields $\mathbf{F}_{p^d}$ where $d \mid n$, and since cyclic groups are abelian, all the subgroups are normal, and thus all the E/F are Galois.

In one of your homework assignments, you built finite fields by writing irreducible elements of $\mathbf{F}_p[x]$ of certain degrees. But these polynomials can be hard to find. How do we know for example that there even is an irreducible polynomial of degree n in $\mathbf{F}_p[x]$? We show now that this is true.

Theorem 17.7

The extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ is simple, meaning $\mathbf{F}_{p^n} = \mathbf{F}_p(\theta)$ for some θ. In particular, the minimal polynomial of θ is irreducible in $\mathbf{F}_p[x]$, and of degree n.

Proof. By lemma 13.5, any finite subgroup of the group of units of a field is cyclic, so $\mathbf{F}_{p^n}^\times$ is cyclic. Let θ be the generator of this group. □

Corollary 17.8

For each prime p and each n, there are irreducible polynomials in $\mathbf{F}_p[x]$ of degree n.

How do we find these irreducible polynomials? Well, writing $\mathbf{F}_{p^n} = \mathbf{F}_p(\theta)$, since $\mathbf{F}_{p^n}$ is the set of roots of the polynomial $x^{p^n} - x$, then θ is a root, so its minimal polynomial divides $x^{p^n} - x$. Conversely, if we take any polynomial $p(x) \in \mathbf{F}_p[x]$, irreducible of degree d which divides $x^{p^n} - x$ with $p(\alpha) = 0$, then $\mathbf{F}_p(\alpha)$ is a subfield of $\mathbf{F}_{p^n}$ of degree d. We have $\mathbf{F}_p(\alpha) = \mathbf{F}_{p^d}$, and in particular $d \mid n$. Since $\mathbf{F}_p(\alpha)$ is Galois, it contains *all* the roots of $p(x)$, which means $x^{p^n} - x$ is a product of factors $(x - \beta)$, for β a root having a minimal polynomial of degree $d \mid n$. And any irreducible polynomial with degree $d \mid n$ must generate $\mathbf{F}_{p^d}$, and divides $x^{p^n} - x$. This leads us to the following proposition, which can be used to recursively produce irreducible polynomials.

Proposition 17.9

The polynomial $x^{p^n} - x$ is the product of all the distinct irreducible polynomials in $\mathbf{F}_p[x]$ of degree d, where d runs through all the divisors of n.

We finish up with a fun result.

Proposition 17.10

The polynomial $x^4 + 1$, which is irreducible in $\mathbf{Z}[x]$, is reducible modulo every prime.

Proof. If $p = 2$, then $x^4 + 1 = (x + 1)^4$. So suppose p is odd.

Modulo 8, any odd prime p is either $1, 3, 5$, or 7, so 8 divides $p^2 - 1$. So $x^8 - 1$ divides $x^{p^2-1} - 1$, since any root of $x^8 - 1$ is also a root of $x^{p^2-1} - 1$, since $x^8 = 1$ implies $x^{8n} = 1$ for any n. We then have

$$(x^4 + 1) \mid (x^8 - 1) \mid (x^{p^2-1} - 1) \mid (x^{p^2} - x).$$

So all the roots of $x^4 + 1$ are also roots of $x^{p^2} - x$, and are therefore in $\mathbf{F}_{p^2}$.

For contradiction, suppose that $x^4 + 1$ is irreducible over $\mathbf{F}_p[x]$. This would mean that there's an extension K of degree 4 with $\mathbf{F}_p \subseteq K \subseteq \mathbf{F}_{p^2}$. But $\mathbf{F}_{p^2}/\mathbf{F}_p$ is degree 2, which is a contradiction. □

§18 April 10, 2020

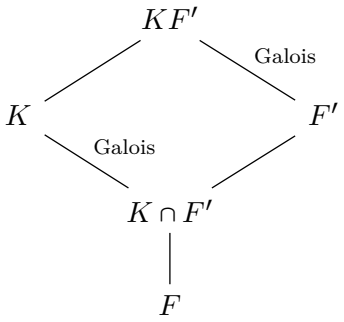
§18.1 Composite Extensions

Today we study composite extensions. Recall that if K_1 and K_2 are subfields of some field K, the the **composite** of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2.

Proposition 18.1

Suppose K/F is a Galois extension, and F'/F is *any* extension. Then the composite extension KF'/F' is Galois, with Galois group $\mathrm{Aut}(KF'/F') \simeq \mathrm{Aut}(K/(K \cap F'))$. (Note that it is KF'/F', *not* KF'/F).

The above proposition can be visualized by the following diagram:



Proof. Since K/F is Galois, it is the splitting field of a separable polynomial $f(x) \in F[x]$. Since $F' \supseteq F$, we can regard $f(x)$ as a polynomial $f'(x) \in F'[x]$, and KF'/F' is the splitting field of $f'(x)$. This implies KF'/F' is Galois.

Now, define a map

$$\begin{aligned}\phi &: \mathrm{Aut}(KF'/F') \to \mathrm{Aut}(K/F)\\ \phi &: \sigma \mapsto \sigma|_K.\end{aligned}$$

Since K/F is Galois, this map is well-defined (we saw this last time: any embedding of K which fixes F is an automorphism of K). If $\tau \in \ker(\phi)$, then τ must fix F', by definition of $\mathrm{Aut}(KF'/F')$, and also K, since it is in the kernel. Thus, anything in the kernel must fix KF', and is thus trivial, so the map ϕ is injective.

Write $H = \mathrm{im}(\phi) \subseteq \mathrm{Aut}(K/F)$, and K_H the fixed field of H in K/F. Since every element in H fixed F', then $F' \cap K \subseteq K_H$. In addition, the composite $K_H F'$ is fixed by $\mathrm{Aut}(KF'/F')$, since if $\sigma \in \mathrm{Aut}(KF'/F')$, then σ fixes F', and $\sigma|_K \in \mathrm{im}(\phi) = H$, so σ fixes K_H by definition. Then $K_H F'$ corresponds to $1 \in \mathrm{Aut}(KF'/F')$ via the correspondence in the fundamental theorem of Galois theory, and by one-to-oneness of the correspondence, this means $K_H F' = F'$. So $K_H \subseteq F'$, which means $K_H = K \cap F'$. By the fundamental theorem of Galois theory, then $H = \mathrm{Aut}(K/K_H) = \mathrm{Aut}(K/K \cap F')$. □

Corollary 18.2

If K/F is Galois, and F'/F is any finite extension, then

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proof. Using proposition 18.1, we have

$$\begin{aligned}[KF' : F] &= [KF' : F'][F' : F]\\ &= \left|\mathrm{Aut}(KF'/F')\right| [F' : F]\\ &= \left|\mathrm{Aut}(K/K \cap F')\right| [F' : F]\\ &= [K : K \cap F'][F' : F]\\ &= \frac{[K : F][F' : F]}{[K \cap F' : F]}.\end{aligned}$$

□

Note that in the above, we need at least one of the extensions to be Galois.

Exercise 18.3. Give a counterexample to 18.1 in the case where neither K nor F' are Galois.

Proposition 18.4

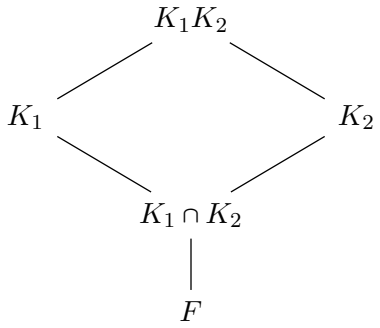
Suppose K_1/F and K_2/F are Galois. Then

(i) $(K_1 \cap K_2)/F$ is Galois, and

(ii) K_1K_2/F is Galois. The Galois group H is the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ defined by

$$H = \{(\sigma_1, \sigma_2) : \sigma_1|_{K_1 \cap K_2} = \sigma_2|_{K_1 \cap K_2}\}.$$

We can visualize this in the following diagram:



Proof. (i) Let $p(x) \in F[x]$ be an irreducible polynomial with a root α in $K_1 \cap K_2$. Then all the roots of p must lie in both K_1 and K_2, and thus in $K_1 \cap K_2$. So $K_1 \cap K_2$ is the splitting field of p, and thus Galois.

(ii) Say K_1/F is the splitting field of a separable polynomial $f_1(x)$, and K_2/F is the splitting field of a separable polynomial $f_2(x)$. Then K_1K_2 is the splitting field of $f_1(x)f_2(x)$. Removing repeated factors, then K_1K_2 is the splitting field of a separable polynomial.

Now, consider the map

$$\phi : \mathrm{Aut}(K_1K_2/F) \to \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$$
$$\phi : \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2}).$$

The kernel is the set of elements which are the identity on both K_1 and K_2, and is thus trivial, so the map is injective. Let H be the same as in the statement of the proposition: the subgroup of $\mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F)$ of all (σ_1, σ_2) which agree on $K_1 \cap K_2$. The image of ϕ is contained in H, since for any σ,

$$(\sigma|_{K_1})|_{K_1 \cap K_2} = \sigma|_{K_1 \cap K_2} = (\sigma|_{K_2})|_{K_1 \cap K_2}.$$

We now show that $|H| = |\mathrm{Aut}(K_1K_2/F)|$, so that the image is in fact all of H.

Let $\sigma_1 \in \mathrm{Aut}(K_1/F)$. Then there exactly $|\mathrm{Aut}(K_2/K_1 \cap K_2)|$ automorphisms $\sigma_2 \in \mathrm{Aut}(K_2/F)$ which which satisfy $(\sigma_1, \sigma_2) \in H$. So

$$|H| = |\mathrm{Aut}(K_1/F)||\mathrm{Aut}(K_2/K_1 \cap K_2)| = |\mathrm{Aut}(K_1/F)| \frac{|\mathrm{Aut}(K_2/F)|}{|\mathrm{Aut}(K_1 \cap K_2/f)|}.$$

By the previous corollary then $H = [K_1K_2 : F]$, as desired.

□

Exercise 18.5. In the above proof, why are there exactly $|\mathrm{Aut}(K_2/K_1 \cap K_2)|$ values of σ_2 which satisfy $(\sigma_1, \sigma_2) \in H$?

Corollary 18.6

Let K_1/F and K_2/F be Galois extensions. If $K_1 \cap K_2 = F$, then

$$\mathrm{Aut}(K_1K_2/F) \simeq \mathrm{Aut}(K_1/F) \times \mathrm{Aut}(K_2/F).$$

Example 18.7

Let $F = \mathbf{Q}$, $K_1 = \mathbf{Q}(\sqrt{2})$, and $K_2 = \mathbf{Q}(\sqrt{3})$. Each of these extensions is Galois, with Galois group $\mathbf{Z}_2$. Since $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$, then $K_1 \neq K_2$. So $F \subsetneq K_1 \cap K_2 \subsetneq K_1$, and by Galois correspondence or a degree argument, then $F = K_1 \cap K_2$. Thus,

$$\mathrm{Aut}(K_1K_2/F) = \mathrm{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3}/\mathbf{Q}) \simeq \mathbf{Z}_2 \times \mathbf{Z}_2.$$

§18.2 Separable Extensions

Recall that an extension is **separable** if every element in E is the root of a separable polynomial in $F[x]$. If a field has characteristic zero or is perfect, then any irreducible polynomial is separable. So any algebraic extension of a perfect field is separable. We now show that any finite separable extension (and thus any finite algebraic extension of a perfect field) is contained in a Galois extension.

Corollary 18.8

If E/F is a finite separable field extension, then E is contained in an extension K/F which is Galois over F and is minimal, meaning no proper subfield of K containing E is Galois over F.

Proof. Since E/F is finite it has a basis, so let $f_1(x), f_2(x), \ldots, f_n(x)$ be the minimal polynomials for each element in the basis, and let $K_1/F, K_2/F, \ldots, K_n/F$ be the splitting fields of $f_1(x), \ldots, f_n(x)$ respectively. These are Galois extensions. Then $K_1K_2 \cdots K_n/F$ is a Galois extension containing E. Since it has finite degree, the Galois group is finite, and thus it only has finitely many subfields. Let K be the intersection of all the subfields containing E which are Galois over F. Then K is Galois and minimal. □

The field K from the above corollary is called the **Galois closure** of the E over F. Since Galois closures always exist, we can often use them to simplify computations for non-Galois extensions.

§19 April 15, 2020

§19.1 Simple Extensions and the Primitive Element Theorem

Recall that an extension K of a field F is called **simple** if $K = F(\theta)$ for some θ. The element $\theta \in K$ is called a **primitive element**. For example, the extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is simple, and $\sqrt{2}$ is a primitive element. Another simple extension is $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, with primitive element $\sqrt{2} + \sqrt{3}$. Note that primitive elements are not unique: we can write $\mathbf{Q}(\sqrt{2}) = \mathbf{Q}(1 + \sqrt{2})$ for example.

Our goal for today will be to prove the primitive element theorem, which says that if K/F is finite and separable, then K/F is simple. Recall that an extension K/F is *separable* if every element of K is the root of some separable polynomial in $F[x]$. For perfect fields, any finite extension is separable (this includes all characteristic zero fields). To prove this, we'll use the following lemma.

Lemma 19.1

Let K/F be a finite extension. Then K/F is simple if and only if there exist only finitely many subfields of K containing F.

Proof. For the forward direction, suppose that K/F is simple, so $K = F(\theta)$ for some θ. Let E be a subfield of K containing F, so we have $F \subseteq E \subseteq K$. Let $f(x) \in F[x]$ be the minimal polynomial of θ over F, and $g(x) \in E[x]$ be the minimal polynomial of θ over E. Then inside $E[x]$, we have that g divides f. Let $E' \subseteq E$ be the subfield of E generated by the coefficients of $g(x)$. The minimal polynomial for θ is the same in E' as it is in E, since the coefficients are in E'. So $[K : E] = [K : E'] = \deg g$. This means that $E = E'$.

Since E was arbitrary, then this means that any subfield of K is generated by the coefficients of some monic polynomial g dividing f. There are only finitely many such polynomials, and thus K has only finitely-many subfields.

For the other direction, suppose that K has only finitely many subfields containing F. If F is finite, then K is a simple extension by theorem 17.7.

So suppose that F is infinite. Let $\alpha, \beta \in K$, and consider $F(\alpha, \beta)/F$. It is enough to show that this extension is simple, since the main result follows by induction. Consider all the subfields $F(\alpha + c\beta) \subseteq F(\alpha, \beta)$ for $c \in F$. There are infinitely many choices for c, and by assumption only finitely many subfields of $F(\alpha, \beta)$. Thus there exist $c \neq c' \in F$ such that $F(\alpha + c\beta) = F(\alpha + c'\beta)$. Then $\alpha + c\beta - (\alpha +' \beta) \in F(\alpha + c\beta)$, which means $(c - c')\beta \in F(\alpha + c\beta)$, which means $\beta \in F(\alpha + c\beta)$, and thus also $\alpha \in F(\alpha + c\beta)$. This means that $F(\alpha + c\beta) = F(\alpha, \beta)$, so $F(\alpha, \beta)$ is simple, as desired. □

We now state and prove the primitive element theorem, which is extremely useful in many contexts.

Theorem 19.2 (Primitive Element Theorem)

If K/F is finite and separable, then K/F is simple.

Proof. Let L/F be the Galois closure of K/F, the smallest extension of F containing K, which exists by corollary 18.8. Since L/F is finite, then $\mathrm{Aut}(L/F)$ is finite. So by Galois correspondence, L/F has finitely many intermediate fields. Since $K \subseteq L$, then K also has only finitely many intermediate fields. Applying the above lemma, we are done. □

Let's do an example to see how the primitive element theorem can be extremely useful.

Example 19.3

Let $F = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. By the primitive element theorem, K/F is a simple extension. Examining the proof of the above lemma, we see that there is a generator of the form $\alpha_c = \sqrt[3]{2} + ce^{2\pi i/3}$, for some $c \in \mathbf{Q}$. We need to find a value of c that works.

Let's look at what the elements of the Galois group do to α_c. The Galois group has order 6. It has generators

$$\begin{aligned}
\sigma &: \sqrt[3]{2} \mapsto e^{2\pi i 3}\sqrt[3]{2} \\
\sigma &: e^{2\pi i/3} \mapsto e^{2\pi i/3} \\
\tau &: \sqrt[3]{2} \mapsto \sqrt[3]{2} \\
\tau &: e^{2\pi i/3} \mapsto e^{4\pi i/3}.
\end{aligned}$$

Then

$$\begin{aligned}
\sigma(\alpha_c) &= e^{2\pi i/3}\sqrt[3]{2} + ce^{2\pi i/3} \\
\tau(\alpha_c) &= \sqrt[3]{2} + ce^{4\pi i/3}.
\end{aligned}$$

so $\sigma(\alpha_c) \neq \alpha_c$ for all c, and $\tau(\alpha_c) \neq \alpha_c$ for $c \neq 0$.

So if $c \neq 0$, then α_c is not fixed by any non-identity automorphism, which means that the field $\mathbf{Q}(\alpha_c)$ corresponds to the group $\{1\}$, which has fixed field K. So α_c is a primitive element for any $c \neq 0$.

§19.2 Cyclotomic Extensions

Write $\zeta_n = e^{2\pi i/n}$. We've already shown that $\mathbf{Q}(\zeta_n)$ is a degree $\phi(n)$ Galois extension. Let's compute the Galois group.

Theorem 19.4

The Galois group of $\mathbf{Q}(\zeta_n)$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^\times$, the group of units of $\mathbf{Z}/n\mathbf{Z}$ under multiplication.

Proof. Any automorphism must send ζ_n to a primitive root of unity. Since there are $\phi(n)$ automorphisms (the order of the Galois group), then each mapping of ζ_n to a root of unity gives an automorphism. For a coprime to n, write $\sigma_a \in \mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ for the map

$$\sigma_a : \zeta_n \mapsto \zeta_n^a.$$

Then the map

$$\begin{aligned}
\phi &: (\mathbf{Z}/n\mathbf{Z})^\times \to \mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \\
\phi &: a \mapsto \sigma_a
\end{aligned}$$

is an isomorphism, which finishes the proof. □

Corollary 19.5

Let $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, where p_i are distinct primes. Then the extensions $\mathbf{Q}(\zeta_{p_i^{a_i}})$ intersect only in $\mathbf{Q}$, and their composite is $\mathbf{Q}(\zeta_n)$.

Proof. Since $p_i^{a_i}$ divides n, then $\mathbf{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbf{Q}(\zeta_n)$. The composite of all the $\mathbf{Q}(\zeta_{p_i^{a_i}})$'s contains the product $\prod_i \zeta_{p_i^{a_i}}$, which is a primitive n'th root of unity. Since the composite contains a primitive n'th root of unity, then it is equal to $\mathbf{Q}(\zeta_n)$.

Now, we have $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k})$. Since the number of automorphisms of $\mathbf{Q}(\zeta_n)$ is $\phi(n)$, and the number of automorphisms of each of the $\mathbf{Q}(\zeta_{p_i^{a_i}})$ is $\phi(p_i^{a_i})$, and since $\phi(n) = \prod_i \phi(p_i^{a_i})$, then the intersection must be $\mathbf{Q}$. □

Example 19.6

We compute the subfields of $\mathbf{Q}(\zeta_5)$. The field $\mathbf{Q}(\zeta_5)$ is Galois over $\mathbf{Q}$ with automorphism group $(\mathbf{Z}/5\mathbf{Z})^\times = \mathbf{Z}/4\mathbf{Z}$. This is a Galois extension of $\mathbf{Q}$ of degree 4 with a cyclic Galois group. A generator of this group is the automorphism $\sigma : \zeta_5 \mapsto \zeta_5^2$. Since $\mathbf{Z}_4$ has only one nontrivial subgroup, $\{1, \sigma^2\}$, then there is one nontrivial subfield of $\mathbf{Q}(\zeta_5)$, which is the fixed field of $\{1, \sigma^2\}$. Note that $\sigma^2 : \zeta_5 \mapsto \zeta_5^4 = \zeta_5^{-1}$. Then $\alpha = \zeta_5 + \zeta_5^{-1}$ is in the fixed field, since

$$\sigma(\zeta_5 + \zeta_5^{-1}) = \sigma(\zeta_5) + \sigma(\zeta_5^{-1}) = \zeta_5^{-1} + \zeta_5.$$

By the fundamental theorem, α must generated the fixed field, meaning the fixed field is equal to $\mathbf{Q}(\alpha)$, which is a quadratic extension. Notice that $\alpha = 2\cos(2\pi/5)$. The minimal polynomial of ζ_5 is

$$x^4 + x^3 + x^2 + x + 1.$$

Then

$$\begin{aligned}\alpha^2 + \alpha - 1 &= (\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1\\ &= (\zeta_5^2 + \zeta_5^3 + 2) + (\zeta_5 + \zeta_5^4) - 1\\ &= 0.\end{aligned}$$

So the minimal polynomial of α is $x^2 + x - 1$, and solving, we find that

$$\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{5}).$$

Let's look at $\mathbf{Q}(\zeta_p)$ for any prime p, any try to construct primitive elements for the subfields, like we did for $\mathbf{Q}(\zeta_5)$. The set $\{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ is a basis for $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$. Since these are just the primitive p'th roots of unity (everything less than p is coprime to it), then $\mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ permutes theses between themselves.

Suppose H is a subgroup of $\mathrm{Aut}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Define

$$\alpha_H = \sum_{\sigma\in H} \sigma(\zeta_p),$$

as the sum of all the conjugates of ζ_p by automorphisms in H. If $\tau \in H$, then as σ runs over all the elements of H, so will $\tau\sigma$, which means $\tau\alpha_H = \alpha_H$. So α_H is in the fixed field for H.

Suppose $\tau \notin H$, and suppose $\tau\alpha_H = \alpha_H$. Since τ permutes the ζ_p, then this means that $\tau(\zeta_p) = \sigma(\zeta_p)$ for some $\sigma(\zeta_p)$. But then $\tau\sigma^{-1} = 1$, and so $\tau = \sigma \in H$. So we must have $\tau\alpha_H \neq \alpha_H$, which means α_H is not fixed by any $\tau \notin H$ and thus the fixed field of H is exactly $\mathbf{Q}(\alpha)$.

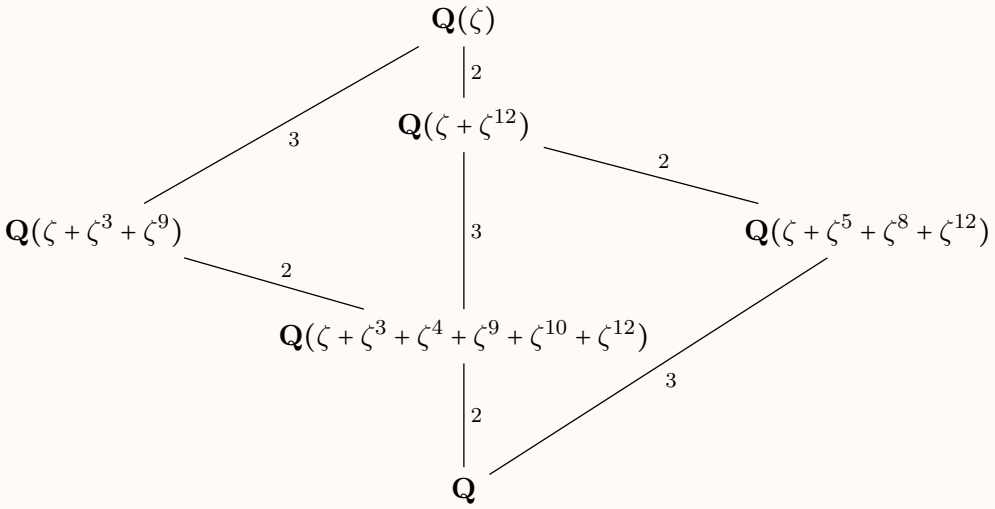
Example 19.7

Let's compute the subfields of $\mathbf{Q}(\zeta_{13})$, which correspond to the subgroups of $\mathbf{Z}/12\mathbf{Z}$, a cyclic group, with generator $\sigma : \zeta_{13} \mapsto \zeta_{13}^2$. There are four nontrivial subgroups, of orders $2, 3, 4, 6$, which have generators $\sigma^6, \sigma^4, \sigma^3, \sigma^2$ respectively. The fields corresponding to these subgroups have orders $6, 4, 3, 2$ respectively.

The field of degree 4 corresponds to the subgroup of order 4, which is $\{1, \sigma^4, \sigma^8\}$. By the above discussion, we can find the primitive element for the subfield by summing over the conjugates of ζ_{13} by $1, \sigma^4, \sigma^8$, which is

$$\zeta_{13} + \sigma^4(\zeta_{13}) + \sigma^8(\zeta_{13}) = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9.$$

You can similarly compute the primitive elements for the other subfields. Writing $\zeta = \zeta_{13}$, we can write out the diagram for the subfields as



Now for another useful and natural definition, which gives a name to the "nicest" types of extensions. A field extension K/F is an **abelian extension** if K/F is Galois and the Galois group is abelian. Note: it's the *Galois group* which abelian, not the field (fields are always abelian). Abelian extensions have nice properties:

Exercise 19.8. Show that if K/F is an abelian extension, then every subfield of K containing F is an abelian extension. Show that the composite of abelian extensions is abelian.

Proposition 19.9

Any finite abelian group is the Galois group of an extension of $\mathbf{Q}$.

Proof. Let G be an abelian group. Then

$$G \simeq \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_k}$$

for some $n_1, \dots, n_k$. If $n_i = p_i - 1$ for $p_1, \dots, p_k$ all distinct primes, then we'd be done, since we could use $\mathbf{Q}(\zeta_{p_1 \cdots p_k})$.

We use the fact that for any natural number n, there are infinitely many primes p with $p \equiv 1 \mod n$. For a discussion of this: see this paper by Keith Conrad. For a full proof of the result, see here.

Using this, we can find distinct primes $p_1, \dots, p_k$ such that $p_i \equiv 1 \mod n_i$. Let $n = p_1 p_2 \cdots p_k$. The Galois group of $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}/p_1 \cdots p_k \mathbf{Z} = \mathbf{Z}_{p_1 - 1} \times \cdots \times \mathbf{Z}_{p_k - 1}$. Since n_i divides $p_i - 1$, there is a subgroup H_i of $\mathbf{Z}_{p_i - 1}$ of index n_i. Then the extension $H_1 \times \cdots \times H_k$ has G as its Galois group. □

Exercise 19.10. Above, we showed that any finite abelian group is the Galois group of an extension of $\mathbf{Q}$. If G is *any* finite group, is G the Galois group of an extension of $\mathbf{Q}$. Hint: ....

§20 April 17, 2020

§20.1 Constructibility of Polygons

In this section we will answer another question of the ancient Greeks: which polygons are constructible? The Greeks knew that the 2-gon, 3-gon (triangle), 4-gon (square), and 5-gon (pentagon) are constructible, and that if it is possible to construct an n-gon, then it is also possible to construct a $2n$-gon. The Greeks did not know how to construct $7, 9, 11, 13$...-gons. When he was 19, Gauss showed how to construct the regular 17-gon (by actually constructing it). He wanted it inscribed on his tomb, but alas this did not happen. When he was 24, he proved a sufficient condition for constructibility, and it was later proved that this condition is necessary. It is not possible to construct the 7-gon, 9-gon, 11-gon, or 13-gon. It is possible to construct the 257-gon. What is the condition?

First let's recall what it means for a polygon to be constructible. Recall that a *point* is constructible if it can be constructed (using ruler and compass constructions) starting with the points $(0, 0)$ and $(0, 1)$ only. A *real number* α is constructible if $|\alpha|$ is the length of a straight line between two points.

Recall also the following theorem on constructibility of real numbers.

Theorem 20.1

A real number α is constructible if and only if there exists a chain of extensions

$$\mathbf{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m \subseteq \mathbf{R},$$

such that $[K_{i+1} : K_i] = 2$ for all $i \leq m$. In particular, we must have that $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is a power of 2 for any α.

An *angle* is constructible if it is angle between two lines which go through constructible points, and which intersect in a constructible point. Recall also that an angle θ is constructible if and only if $\cos(\theta)$ is constructible.

With that, we're ready to discuss constructibility of n-gons. We say that a regular n-gon is constructible if the angle $2\pi/n$ is constructible. To see how this relates to polygons, note that if $2\pi/n$ is constructible, then the points $(\cos(2k\pi/n), \sin(2k\pi/n))$ for $k = 1, \dots, n$ are constructible, which are the vertices of a regular n-gon. By the half angle formula, if $\cos(\pi/n)$ is constructible, then so is $\cos(\pi/(2n))$, which tells us that if

an n-gon can be constructed, then so can a $2n$-gon. Using this and what we've already discussed about constructibility.

We'll now discuss the sufficient condition for the constructibility of the n-gon. Let $\zeta_n = e^{2\pi i/n}$ be the primitive n'th root of unity. Since $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$, then the regular n-gon is constructible if and only if $\alpha = \zeta_n + \zeta_n^{-1}$. So let's look at $\mathbf{Q}(\alpha)$, which is a proper subfield of $\mathbf{Q}(\zeta_n)$. Since $[\mathbf{Q}(\zeta_n) : \mathbf{Q}(\alpha)] = 2$, and $\mathbf{Q}(\zeta_n)$ has degree $\phi(n)$, then $\mathbf{Q}(\alpha)$ has degree $\phi(n)/2$ over the rationals. If α is constructible, then $\phi(n)/2$ is a power of 2, which means $\phi(n)$ is also a power of 2. This proves the following theorem, due to Gauss.

Theorem 20.2

If the regular n-gon is constructible, then $\phi(n)$ is a power of 2.

The converse is also true.

Theorem 20.3

If $\phi(n)$ is a power of 2, then the regular n-gon is constructible.

Proof. Suppose $\phi(n) = 2^m$. Then $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ has degree 2^m, and $\mathbf{Q}(\alpha)$ has degree 2^{m-1}, as noted above. The Galois group $\mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^\times$, and thus abelian. Thus, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois, with abelian Galois group of order 2^{m-1}. By group theory (Sylow theorems), there exists a chain of abelian subgroups

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{m-1} = G,$$

with $[G_{i+1} : G_i] = 2$ for all i.

By the fundamental theorem of Galois theory, there is a corresponding chain of subfields of $\mathbf{Q}(\alpha)$:

$$\mathbf{Q} = F_{m-1} \subseteq F_{m-2} \subseteq \cdots \subseteq F_0 = \mathbf{Q}(\alpha),$$

with $[F_{i+1} : F_i] = 2$ for all i.

Since there exists such a chain of field extensions of $\mathbf{Q}$ to $\mathbf{Q}(\alpha)$, then α is constructible. □

Since $\phi(17) = 16$, then the regular 17-gon is constructible.

For any n, we can determine when $\phi(n)$ is a power of 2 using the prime factorization of n. Suppose that $n = p_1^{k_1} \cdots p_m^{k_m}$, with $p_1, \ldots, p_m$ distinct primes. The Euler totient function is multiplicative, so $\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_m^{k_m})$. This means that $\phi(n)$ is a power of 2 if and only if $\phi(p_i^{k_i})$ is a power of 2 for all i.

Exercise 20.4. Show that $\phi(p^k) = p^{k-1}(p-1)$ if p is prime.

Using the above exercise, we see that if p is an odd prime, then $\phi(p^k) = p^{k-1}(p-1)$ is a power of 2 if and only if $k = 1$ and $p-1$ is a power of 2. So $p - 1 = 2^\ell$ for some ℓ, thus $2^\ell \equiv 1 \mod p$, so $2^{2\ell} \equiv 1 \mod p$. By Lagrange's theorem, 2ℓ must divide $p-1$. Since $p-1$ is a power of 2, then ℓ is a power of 2. So p must be a prime of the form $2^{2^s} + 1$. Primes of the form $2^{2^2} + 1$ are called **Fermat primes**. This leads us to the following theorem.

Theorem 20.5

A regular n-gon can be constructed if and only if n is the product of a power of 2 and distinct Fermat primes.

We now now exactly which regular n-gons are constructible. It should be noted that there are only 5 known Fermat primes: 3,5,17, 257, 65537.

§20.2 Fundamental Theorem of Algebra

We'll now study another result which was proved by Gauss: the Fundamental Theorem of Algebra. There are many proofs of this theorem, all of which use some sort of analysis (we need the properties of $\mathbf{R}$). The theorem is also not really necessary, since we can prove existence of algebraically closed fields. So it's not actually that fundamental or algebraic. But we will prove it, because the name sounds important and because people will always ask you to prove it because you are a math major (it's also showed up on quantitative finance interviews).

We begin with two facts from analysis:

1. Any odd degree polynomial with real coefficients has a real root. This follows from the intermediate value theorem.
2. Any equation $ax^2 + bx + c = 0$, with $a, b, c \in \mathbf{C}$ and $a \neq 0$ has a solution in $\mathbf{C}$. This follows from the quadratic formula.

We now translate these facts into algebra:

1. The only extension of $\mathbf{R}$ with odd degree is $\mathbf{R}$. This follows from the primitive element theorem. The extension must be generated by some primitive element, which has minimal polynomial of odd degree. Then factor the minimal polynomial.
2. There are no extensions of $\mathbf{C}$ of degree 2.

We'll now prove the fundamental theorem of algebra.

Theorem 20.6

The field $\mathbf{C}$ is algebraically closed.

Proof. Let $f(x) \in \mathbf{C}[x]$ of degree $n \geq 1$. We need to show that $f(x)$ has a root in $\mathbf{C}$. Suppose that it has no roots in $\mathbf{C}$. Then the conjugate polynomial $\tau(f)(x)$ also has no roots in $\mathbf{C}$ (here τ is the automorphism of complex conjugation). Thus, the product $f(x)\tau(f)(x)$ has no roots in $\mathbf{C}$. Since this polynomial is fixed by τ, $\tau(f(x)\tau(f)(x)) = \tau(f)(x)f(x)$, then it has real coefficients. We have found some polynomial with real coefficients and no roots in $\mathbf{C}$, so we can assume without loss of generality that $f(x) \in \mathbf{R}[x]$. We'll do two proofs:

1. Let $K/\mathbf{R}$ be the splitting field of $f(x)$. Then $K(i)$ is a Galois extension of $\mathbf{R}$, since it's the composite field of $\mathbf{C}$ and K over $\mathbf{R}$. Let $G = \mathrm{Aut}(K(i)/\mathbf{R})$. Since the degree of $\mathbf{C}$ over $\mathbf{R}$ is 2, then we have $|G| = 2^k m$ for some $k \geq 1$ and some odd m. By the Sylow theorems, there exists a subgroup $P_2 \subseteq G$ of order 2^k. Since P_2 is a subgroup with index m, then its fixed field has degree m, by Galois theory.

But there are no nontrivial odd degree extensions of $\mathbf{R}$, which means we must have $m = 1$.

So the order of G is a power of 2, so G is a 2-group, $|G| = 2^k$. Then $G' = \mathrm{Aut}(K(i)/\mathbf{C})$ has order 2^{k-1}. Using the fact that p-groups have subgroups of all orders for p prime, then as long as $k \neq 1$, G' must have some subgroup of index 2, which we call H.

The fixed field of H is a degree 2 extension of $\mathbf{C}$. But such an extension does not exist. Thus, we must have $k = m = 1$, and $K(i) = \mathbf{C}$.

2. Let n be the degree of $f(x) \in \mathbf{R}[x]$, where $f(x)$ has no roots in $\mathbf{C}$. Write $n = 2^k m$, for $k \geq 0$ and m odd. We proceed by induction on k. If $k = 0$, then f has a root by the intermediate value theorem, so assume $k \geq 1$, and that the result holds up to $k - 1$.

   Let $K/\mathbf{R}$ be the splitting field of $f(x)$. Then $K(i)/\mathbf{R}$ is Galois, as in proof 1. Write $K(i) = \mathbf{R}(\alpha_1, \ldots, \alpha_n, i)$, where α_j are the roots of $f(x)$. For each $t \in \mathbf{R}$, define the polynomial

$$L_t(x) = \prod_{1 \leq i < j \leq n} (x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)).$$

   This polynomial $L_t(x)$ is fixed by any automorphism of $K(i)$, since automorphisms permute Galois conjugates, and thus $L_t(x)$ is in $\mathbf{R}[x]$. The degree of $L_t(x)$ is $n(n-1)/2$, which we can write as $2^{k-1}m'$ for some odd m'. By the induction hypothesis, $L_t(x)$ has a root in $\mathbf{C}$. Since $L_t(x)$ is a product of factors of the form $x - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$, then one of these factors must have a root, meaning $\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbf{C}$ for some i, j.

   Since this is true for every $t \in \mathbf{R}$. Since there are infinitely many such t, and only finitely many choices for $i < j$, then there exists some $s \neq t$ for which

$$\alpha_i + \alpha_j + t\alpha_i\alpha_j \in \mathbf{C}$$
$$\alpha_i + \alpha_j + s\alpha_i\alpha_j \in \mathbf{C}.$$

   Subtracting, we have $(t - s)\alpha_i\alpha_j \in \mathbf{C}$, which means $\alpha_i\alpha_j \in \mathbf{C}$, and also $\alpha_i + \alpha_j \in \mathbf{C}$. But then α_i, α_j are roots of the polynomial

$$x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j \in \mathbf{C}[x].$$

   This is a quadratic, so its roots, α_i and α_j, are in $\mathbf{C}$, which contradicts the assumption that $f(x)$ has no roots in $\mathbf{C}$, so we are done.

□

§21 April 21, 2020

§21.1 Galois Groups of Polynomials

Recall that we defined the Galois group of a separable *polynomial* as the Galois group of the splitting field of $f(x)$. For example, the Galois group of $(x^2 - 2)(x^2 - 3)$ is $\mathrm{Aut}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}) \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$. Today we will discuss techniques for the computation of Galois groups of polynomials.

First, suppose that $\alpha_1, \ldots, \alpha_n$ are the roots of some polynomial $f(x) \in F[x]$, which sit inside the splitting field K. If $\sigma \in \mathrm{Aut}(K/F)$, then σ permutes the elements $\{\alpha_1, \ldots, \alpha_n\}$,

and we can regard this as a permutation on $\{1, \dots, n\}$. So we have an injective homomorphism from $\mathrm{Aut}(K/F)$ so S_n, the symmetric group, which sends $\sigma : \alpha_i \mapsto \alpha_j$ in $\mathrm{Aut}(K/F)$ to the element $i \mapsto j$ in S_n. So the Galois group of a polynomial of order n is a subgroup of S_n. This gives us a group theoretical proof that splitting fields have order at most $n!$.

Suppoose that $f(x) = f_1(x) \cdots f_k(x)$ is a separable polynomial of degree n, with each f_i irreducible of degree n_i. Since the automorphisms permute the roots of the individual f_i's, then the Galois group of $f(x)$ is a subgroup of $S_{n_1} \times \cdots \times S_{n_k}$. Since the f_i are irreducible, then the Galois group is transitive on the roots of $f_i(x)$, meaning there exists an automorphism sending any root of $f_i(x)$ to any other root of $f_i(x)$.

Example 21.1

Let $f(x) = (x^2 - 2)(x^2 - 3)$. Let

$$\begin{aligned} \alpha_1 &= \sqrt{2} \\ \alpha_2 &= -\sqrt{2} \\ \alpha_3 &= \sqrt{3} \\ \alpha_4 &= -\sqrt{3}. \end{aligned}$$

Since $f(x)$ is degree 4, the Galois group of $f(x)$ is a subgroup of S_4. Furthermore, any permutation must permute α_1 with α_2, and α_3 with α_4. We know that

$$\begin{aligned} \sigma : \sqrt{3} &\mapsto \sqrt{3} \\ \sigma : \sqrt{2} &\mapsto -\sqrt{2} \end{aligned}$$

is an automorphism. This σ corresponds to $(12) \in S_4$. Similarly,

$$\begin{aligned} \tau : \sqrt{2} &\mapsto \sqrt{2} \\ \tau : \sqrt{3} &\mapsto -\sqrt{3} \end{aligned}$$

corresponds to $(34) \in S_4$. The Galois group is generated by these two, and is isomorphic the the Klein 4-group.

Example 21.2

Let $f(x) = x^3 - 2$, and

$$\begin{aligned} \alpha_1 &= \sqrt[3]{2} \\ \alpha_2 &= e^{2\pi i/3} \sqrt[3]{2} \\ \alpha_3 &= e^{4\pi i/3} \sqrt[3]{2}. \end{aligned}$$

Since $f(x)$ is of degree 3, the Galois group is a subgroup of S_3. Sending $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ and $e^{2\pi i/3} \mapsto e^{4\pi i/3}$ is an automorphism. This corresponds to $(23) \in S_3$. Sending $\sqrt[3]{2} \mapsto e^{2\pi i/3} \sqrt[3]{2}$ and fixing $e^{2\pi i/3}$ is an automorphism. These generate all of S_3, so the Galois group is S_3.

We can ask the following question: for any n, is there a polynomial of degree n with S_n as its Galois group? The answer is yes. Polynomials with this property are in a sense "generic," meaning there are no relations between their roots. (It also turns out that an arbitrary polynomial over $\mathbf{Q}$ has a very high probability of the Galois group being all of S_n, see here.) To answer this question more fully, we'll need some more theory about polynomials. We'll study symmetric polynomials.

Definition 21.3 — Let $x_1, \dots, x_n$ be indeterminates (variables). The **elementary symmetric functions** $s_1, \dots, s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n = \sum_{i<j\le n} x_ix_j \\ &\vdots \\ s_n &= x_1x_2\cdots x_n. \end{aligned}$$

In general, we have the following formula for the polynomials:

$$s_k = \sum_{S\subseteq\{1,\dots,n\},|S|=k} \prod_{i\in S} x_i.$$

We generally think of these functions as members of $F(x_1, \dots, x_n)$, the field of rational functions in $x_1, \dots, x_n$. The **general polynomial** of degree n is defined as

$$(x - x_1)(x - x_2)\cdots(x - x_n) \in F(x_1, \dots, x_n)[x].$$

Exercise 21.4. Show that

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

Also, show that if $\sigma \in S_n$, then σ fixes each s_i.

According to the above exercise, the general polynomial of degree n, $f(x)$, is an element of $F(s_1, \dots, s_n)[x]$. So $F(x_1, \dots, x_n)$ is the splitting field of $f(x)$ over $F(s_1, \dots, s_n)$.

What is the Galois group of $F(x_1, \dots, x_n)$ over $F(s_1, \dots, s_n)$? By the discussion above, it must be a subgroup of S_n, and moreover any $\sigma \in S_n$ gives an automorphism of $F(x_1, \dots, x_n)/F$ by permuting the x_i's. By the exercise above, σ fixes each s_i, and thus $\sigma \in \mathrm{Aut}(F(x_1, \dots, X_n)/F(s_1, \dots, s_n))$. So the Galois group is all of S_n:

$$\mathrm{Aut}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)) \simeq S_n.$$

A rational function $f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ is a **symmetric function** if it is not changed by permuting the x_i's. Note these are *rational functions*, so $\frac{x_1+x_2}{x_1x_2}$ is valid. Note also that symmetric functions are *not* all *elementary* symmetric functions. However, the fundamental theorem of symmetric functions tells us that there is a relationship between the two.

Corollary 21.5 (Fundamental Theorem of Symmetric Functions)
Any symmetric function $f(x_1, \dots, x_n)$ is a rational function in the elementary symmetric functions $s_1, \dots, s_n$:

$$f(x_1, \dots, x_n) \in F(s_1, \dots, s_n).$$

Proof. Since $f(x)$ is a symmetric function, it is by definition in the field which is fixed by all $\sigma \in \mathrm{Aut}(F(x_1,\dots,x_n)/F(s_1,\dots,s_n))$ where σ is given by permuting the x_i's. But we just showed above that this is in fact the entire Galois group. So by the fundamental theorem of Galois theory, the fixed field is $F(s_1,\dots,s_n)$. □

It is also true that symmetric *polynomials* are *polynomials* in the elementary symmetric functions

Example 21.6

- Consider the function $(x_1-x_2)^2$. We have
$$\begin{aligned}(x_1-x_2)^2 &= x_1^2 - 2x_1x_2 + x_2^2\\ &= (x_1+x_2)^2 - 4x_1x_2\\ &= s_1^2 - 4s_2.\end{aligned}$$
- Consider the function $x_1^2+x_2^2+x_3^2$. We have
$$\begin{aligned}x_1^2+x_2^2+x_3^2 &= (x_1+x_2+x_3)^2 - 2(x_1x_2+x_1x_3+x_2x_3)\\ &= s_1^2 - 2s_2.\end{aligned}$$

Now, consider again the polynomial

$$(x-x_1)\cdots(x-x_n) = x^n - s_1^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n.$$

Let's consider this as a function over $F(s_1,\dots,s_n)$, so now the s_i's are variables (no longer assumed to be symmetric functions). If we add the roots, $\{x_1,\dots,x_n\}$, of the polynomial $x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$, then the s_i are the elementary symmetric functions in $x_1,\dots,x_n$. For example, look at $f(x) = x^2+bx+c$. If we know the roots $f(x) = (x-\alpha_1)(x-\alpha_2)$ of this polynomial, then $b = -(\alpha_1+\alpha_2)$ and $x = \alpha_1\alpha_2$. Let's now return to the generic polynomial, and prove a useful corollary.

Corollary 21.7

If $s_1,\dots,s_n$ are indeterminates, then the general polynomial

$$x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in F(s_1,\dots,s_n)$$

is a separable polynomial with Galois group S_n.

Proof. Add the roots $x_1,\dots,x_n$ to the field $F(s_1,\dots,s_n)$. We show that there are no polynomial relations between the $x_1,\dots,x_n$, so there are no restrictions on the automorphisms and thus the Galois group is all of S_n.

Suppose for contradiction that there are polynomial relations between the $x_1,\dots,x_n$. That is, suppose $p(t_1,\dots,t_n)$ satisfies $p(x_1,\dots,x_n) = 0$. Then

$$p^* = \prod_{\sigma\in S_n} p(t_{\sigma(1)}, t_{\sigma(2)}, \dots, t_{\sigma(n)})$$

is a *symmetric* polynomial in indeterminates $t_1,\dots,t_n$, with roots $x_1,\dots,x_n$. By the fundamental theorem of symmetric polynomials, this gives a polynomial relation between the s_i, which is not possible. □

As an application, let $F = \mathbf{Q}$. Let $e_1 \in \mathbf{C}$ be transcendental over $\mathbf{Q}$, let $e_2 \in \mathbf{C}$ be transcendental over $\mathbf{Q}(e_1)$, and similarly up to e_n. The above corollary shows that

$$x^n - e_1 x^{n-1} + e_2 x^{n-2} + \cdots + (-1)^n e_n$$

is a separable polynomial, with Galois group S_n.

Remark 21.8. (i) Over $\mathbf{Q}$, the "generic" polynomials have Galois group S_n. This is over $\mathbf{Q}$, and it does *not* mean that any field has an extension with Galois group S_n. For example $\mathbf{C}$ has no nontrivial finite extensions at all. Also, all the Galois groups of finite extensions of $\mathbf{F}_p$ are cyclic.

(ii) Any group of order n is a subgroup of S_n, and S_n is the Galois group of an extension of $\mathbf{Q}$. This does *not* mean that any group is realized as a Galois extension of $\mathbf{Q}$. Recall that the correspondence is inclusion reversing: if $K/\mathbf{Q}$ has Galois group S_n, and if H is some subgroup of S_n, then the fixed field E of H satisfies $\mathrm{Aut}(E/\mathbf{Q}) \simeq G/H$, not H itself. However, $\mathrm{Aut}(K/E) \simeq H$, so any finite group is realized as a Galois group over a *finite extension of* $\mathbf{Q}$.

We now continue in our study of $F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)$. This is a Galois extension with Galois group S_n. We can ask: are there any intermediate Galois extensions? Well, if $n \geq 5$, then S_n has only one normal subgroup: the alternating group A_n, with $|S_n/A_n| = 2$. What is the fixed field of A_n? To answer this, we define the *discriminant*.

Definition 21.9 — The **discriminant** D of $x_1, \ldots, x_n$ is

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

The discriminant of a polynomial is the discriminant of the roots of the polynomial.

The discriminant is a symmetric function, thus it is an element of $F(s_1, \ldots, s_n)$. How is the discriminant related to the alternating group? A permutation $\sigma \in S_n$ is in the alternating group A_n if and only if σ fixes the square root of the discriminant, $\sqrt{D} \in \mathbf{Z}[x_1, \ldots, x_n]$. We leave this as an exercise to the reader.

Exercise 21.10. Show that a permutation $\sigma \in S_n$ is in the alternating group A_n if and only if σ fixes

$$\sqrt{D} = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbf{Z}[x_1, \ldots, x_n].$$

This tells us that the fixed field of A_n is generated by $\sqrt{D}$, and is equal to $F(s_1, \ldots, s_n)(\sqrt{D})$. We'll next examine more about how the discriminant relates to the Galois group of polynomials.

Now, let $f(x) \in \mathbf{Q}[x]$, of degree at least 1, and let $\alpha_1, \ldots, \alpha_n$ be its roots, counted with multiplicity. The discriminant of $f(x)$ is $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$, which is nonzero if and only if $f(x)$ is separable. If $f(x)$ isn't separable, then we can examine the product of the distinct irreducible factors of $f(x)$, and the splitting field is the same. So without loss of generality, assume $f(x)$ is separable. Since D is symmetric in the roots of $f(x)$, then by the above it is fixed by all the members of the Galois group, and is therefore in $\mathbf{Q}$.

Theorem 21.11

If $f(x) \in F[x]$, then the Galois group of $f(x)$ is a subgroup of A_n if and only if the discriminant D is the square of a member of F.

Proof. As mentioned above, the Galois group is contained in A_n if and only if every automorphism fixes $\sqrt{D}$, which means $\sqrt{D} \in F$. □

Example 21.12

We will compute the Galois group of an arbitrary quadratic polynomial over $\mathbf{Q}$. Consider $x^2 + bx + c \in \mathbf{Q}[x]$, with roots α, β. We can regard $x^2 + bx + c$ as a "general" polynomial $x^2 - s_1 x + s_2$ in the indeterminates s_1, s_2, so $b = -s_1$, and $c = s_2$.

By the above, the indeterminates s_1, s_2 are symmetric functions in the roots, so

$$s_1 = \alpha + \beta$$
$$s_2 = \alpha\beta.$$

The discriminant is $(\alpha - \beta)^2$. This can be written as a polynomial in the symmetric functions

$$(\alpha + \beta)^2 - 4\alpha\beta = s_1^2 - 4s_2 = (-b)^2 - 4c,$$

which is the familiar discriminant of a quadratic from "high school" algebra! The polynomial is separable if and only if $D = b^2 - 4c \neq 0$. The Galois group is a subgroup of $S_2 = \mathbf{Z}_2$, and is trivial if and only if D is the square of a rational, meaning $\sqrt{D} \in \mathbf{Q}$.

§22 April 24, 2020

You might have been thinking: when are we finally going to prove the insolvability of the quintic? The day has come.

§22.1 The insolvability of the Quintic

We will discuss the following: if $f(x) \in \mathbf{Q}[x]$, when is there a formula for the roots of $f(x)$ using only addition, multiplication, and roots? To answer this, we first study adjunctions of n'th roots.

Definition 22.1 — An extension K/F is a **simple radical extension** if it is obtained by adjoining the n'th root of an element a of F, for some n. That is, K is a simple radical extension if $K = F(b)$, where $b^n = a$. We'll also write $K = F(\sqrt[n]{a})$.

Such an extension K/F is Galois if and only if it contains *all* the roots of $x^n - a$, if and only if F contains all the n'th roots of unity. This is because then K is the splitting field of $x^n - a$. For example $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ is Galois, but $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is not.

An extension K/F is a **cyclic extension** if it is Galois with cyclic Galois group (similarly to how we defined an abelian extension). When is an extension cyclic? To answer this, we first define the *Lagrange resolvent*.

Definition 22.2 — Let K/F be a cyclic field extension of degree n, and suppose the characteristic of F does not divide n, and that F contains all the n'th roots of unity. Let $\sigma \in \mathrm{Aut}(K/F)$ be a generator for the Galois group, and let ζ be any n'th root of unity. Then the **Lagrange resolvent** of α and ζ is

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

Proposition 22.3

Let F be a field of characteristic not dividing n, and containing all the n'th roots of unity. An extension K/F of degree n is cyclic if and only if $K = F(\sqrt[n]{a})$ for some $a \in F$.

Proposition 22.4

(i) ($\Leftarrow$): Suppose that $K = F(\sqrt[n]{a})$ for some $a \in F$. Since the characteristic of F doesn't divide n, then the polynomial $x^n - a$ is separable. The field K/F is the splitting field, and thus a Galois extension, since F contains all the n'th roots of unity. If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\sqrt[n]{a})$ is also a root of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some n'th root of unity ζ_σ. So $\sigma \mapsto \zeta_\sigma$ gives an injective homomorphism $\mathrm{Aut}(K/F) \to \mu_n$, where μ_n is the group of n'th roots of unity. Since the map is injective, and μ_n is cyclic, then the Galois group is cyclic and thus K is a cyclic extension

(ii) ($\Rightarrow$): Suppose that K is a cyclic extension. Let $\sigma \in \mathrm{Aut}(K/F)$ be a generator, and let ζ be an n'th root of unity. Since $\zeta \in F$, then it is fixed by σ. So, if (α, ζ) is the Lagrange resolvent of α and ζ (defined above), then

$$\sigma((\alpha,\zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha) + \zeta^{n-1}\alpha.$$

This tells us that $\sigma((\alpha,\zeta)) = \zeta^{-1}(\alpha,\zeta)$, and thus

$$\sigma((\alpha,\zeta)^n) = \zeta^{-n}(\alpha,\zeta)^n = (\alpha,\zeta)^n.$$

So $(\alpha,\zeta)^n \in F$, since it is fixed by σ.

Now, let ζ be a *primitive* n'th root of unity. We show now that $K = F((\alpha,\zeta))$, for some $\alpha \in K$. This will complete the proof, since then $K = F(\sqrt[n]{(\alpha,\zeta)^n})$. To this end, recall that $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent characters (from the proof of the fundamental theorem of Galois theory). So there exists some $\alpha \in K$ such that $(\alpha,\zeta) \neq 0$.

Since ζ is a primitive n'th root of unity, then $\zeta^{-i}(\alpha,\zeta) \neq (\alpha,\zeta)$ for any $1 \leq i < n$, which means σ^i does not fix (α,ζ) for any $1 \leq i < n$. By the fundamental theorem of Galois theory, $F((\alpha,\zeta))$ cannot be a proper subfield of K (else it would be fixed by one of the σ^i, $i < n$). So $F((\alpha,\zeta)) = K$, which completes the proof.

From now on, F will be a field of characteristic zero.

Definition 22.5 — An extension K/F is a **root extension** if there exists a chain of subfields

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K,$$

such that for all $i < s$, the field K_{i+1} is a simple radical extension of K_i. That is, $K_{i+1} = K_i(\sqrt[n]{a_i})$ for some $a_i \in K_i$, for all i.

We say that an element α, in any extension of F, can be **expressed by radicals** if α is in some root extension of F.

We say that a polynomial $f(x) \in F[x]$ can be **solved by radicals** if all its roots can be expressed by radicals.

These definitions make a lot more sense after a couple of examples.

Example 22.6

- The element $\sqrt[171]{\sqrt{2}+\sqrt{5}}$ can be expressed by radicals over $\mathbf{Q}$. Let
$$K_0 = \mathbf{Q}, K_1 = \mathbf{Q}(\sqrt{2}), K_2 = K_1(\sqrt{5}), K_3 = K_2(\sqrt[171]{\sqrt{2}+\sqrt{5}}.$$
- Any constructible number can be expressed by radicals over $\mathbf{Q}$. Recall that the constructible numbers must be inside a chain of degree 2 extensions.
- The element $\sqrt[3]{2}$ can be expressed by radicals over $\mathbf{Q}$. However, it's not constructible.

We'll now cover a few useful lemmas about root extensions before we prove the insolvability of the quintic.

Lemma 22.7 (i) The composite of a simple radical extension with a root extension is a root extension.

(ii) The composite of two root extensions is a root extension.

Proof. (i) Let K/F with
$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K$$
be a root extension, and let K'/F be a simple radical extension, so $K' = F(\sqrt[n]{a})$, for some a. Since each K_{i+1} is a simple radical extension over K_i, then we can write $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. Then
$$K'K_{i+1} = (K'K_i)(\sqrt[n_i]{a_i}),$$
and thus
$$F \subseteq K' = K_0K' \subseteq K_1K' \subseteq \cdots \subseteq K_sK' = KK'.$$
This implies that KK' is a root extension.

(ii) Write
$$F = K_0 \subseteq \cdots \subseteq K_s = K$$
for the root extensions K. Suppose that K' is another root extension. Then
$$F \subseteq K_0K' \subseteq \cdots \subseteq K_sK'$$
is an iteration of root extensions, so the composite K_sK' is a root extension, as desired.

□

Lemma 22.8

If K/F is a root extension, then its Galois closure L/F is a root extension.

Proof. Since K/F is a root extension, then we can write

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K.$$

If $\sigma \in \mathrm{Aut}(L/F)$, then we can write the following chain of subfields of $\sigma(K)$:

$$F = K_0 = \sigma(K_0) \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_s) = \sigma(K).$$

Since each $\sigma(K_{i+1})/\sigma(K_i)$ is a simple radical extensions, then $\sigma(K)/F$ is a root extension. Since L is the composite of all the $\sigma(K)/F$'s for $\sigma \in \mathrm{Aut}(K/F)$, and the composite of root extensions is a root extension, then L is a root extension. □

Lemma 22.9

If K/F is a Galois root extension, then there exist subfields

$$F = K_0' \subseteq K_1' \subseteq \cdots \subseteq K_s' \subseteq K,$$

such that K_{i+1}'/K_i' is cyclic.

Proof. Since K is a root extension, then we can write

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K.$$

Write $K_{i+1} = \sqrt[n_i]{a_i}$ with $a_i \in K_i$, for each i.

Since K/F is Galois, then K/K_i is Galois for each i, which means that *all* the n_i'th roots of a_i are in K (not just $\sqrt[n_i]{a_i}$), which means the n_i'th roots of unity are in K for each i. Let F' be the smallest extension of F containing all of the n_i'th roots of unity for each i. This is a root extension, and we get a chain

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_s = K.$$

For each i, then $F'K_{i+1}/F'K_i$ is a simple radical extension, with $F'K_i$ containing all the n_i'th roots of unity. So by lemma 22.3, $F'K_{i+1}/F'K_i$ is a cyclic extension. To finish, we need F'/F to be an iteration of cyclic extensions. This follows from the fact that F'/F is a composite of cyclotomic extensions (by its definition). This finishes the proof. □

We've shown the following theorem.

Theorem 22.10

If K/F is a root extension, then there exists an extension L/K such that

- L/F is Galois, and
- there exist subfields
$$F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L,$$
such that L_{i+1}/L_i is a cyclic extension for each i.

We'll now define the notion of a solvable group, and use this to characterize when a polynomial can be solved by radicals. This will tell us that certain polynomials with degree $n \geq 5$ cannot be solved by radicals.

Definition 22.11 — A finite group G is a **solvable group** if there exists a chain of subgroups

$$1 = G_s \subseteq G_{s-1} \subseteq \cdots \subseteq G_0 = G$$

such that G_i/G_{i+1} is cyclic for all i.

Note the similarity of this notion to that of root extensions from above. We'll leave it to you to show some of the important facts about solvable groups in the below exercises.

Exercise 22.12. Show that if H is a normal subgroup of G, then G is solvable if and only if G/H and H are both solvable

Exercise 22.13. Show that "cyclic" can be replaced by "abelian" in the above definition.

Exercise 22.14. Show that the alternating group A_n and the symmetric group S_n are solvable if and only if $n \leq 4$. Hint: use the fact that A_n is simple for $n \geq 5$.

For the following theorem, recall that we are working over a field F with characteristic 0.

Theorem 22.15

A polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

Proof. (i) ($\Rightarrow$): Suppose that $f(x)$ can be solved by radicals. Then each root of $f(x)$ is contained in a root extension, by definition. By the above lemmas, then each root of $f(x)$ is contained in a *Galois* root extension. Let L/F be the composite of all these extensions for the roots of $f(x)$. Then L/F is a Galois root extension, so we can write

$$L_0 = F \subseteq L_1 \subseteq \cdots \subseteq L_s = L,$$

where L_i are intermediate fields so that L_{i+1}/L_i is a cyclic extension for each $i < s$.

Let G_i be the subgroup of the Galois group $\mathrm{Aut}(L/F)$ corresponding under the fundamental theorem to the subfield L_i. By the fundamental theorem, then G_i/G_{i+1} is a cyclic group. This implies that $\mathrm{Aut}(L/F) = G_0$ is a solvable group. Sine the splitting field of $f(x)$ is a subfield of L, its Galois group is a quotient of G_0, which is also solvable.

(ii) $(Leftarrow)$: Suppose that the Galois group G of $f(x)$ is solvable. Let K/F be the splitting field of $f(x)$, so that we can write

$$1 = G_s \subseteq G_{s-1} \subseteq \cdots \subseteq G_0 = G.$$

For each i, let K_i be the fixed field of G_i. Then we can write the chain

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = K,$$

where K_i are subfields with K_{i+1}/K_i cyclic extensions for each $i < s$.

Define $n_i = [K_{i+1}, K_i]$, and let $F' \subseteq K$ be the field obtained by adjoining all the n_i'th roots of unity, for each i. Consider the chain

$$F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \cdots \subseteq F'K_s = K.$$

We then have that $\mathrm{Aut}(F'K_{i+1}/F'K_i) \simeq \mathrm{Aut}(K_{i+1}/K_{i+1} \cap F')$ is a subgroup of $\mathrm{Aut}(K_{i+1}/K_i)$, and is therefore cyclic (you should work through the definitions and prove this as an exercise). This means that $F'K_{i+1}/F'K_i$ is a cyclic extension.

Since F' contains all the relevant roots of unity, then by lemma 22.3, $F'K_{i+1}/F'K_i$ is a simple radical extension for each i. Since F'/F is a root extension, then K/F is a root extension. Thus, the polynomial $f(x)$ can be solved by radicals.

□

As a corollary (and using Exercise 22.14), we get the insolvability of the quintic.

Corollary 22.16

If a polynomial in $\mathbf{Q}[x]$ has Galois group S_n for $n \geq 5$, then it cannot be solved by radicals.

Example 22.17

Let $f(x) = x^5 - 6x + 3$. Using Eisenstein's criterion, $f(x)$ is irreducible. Plugging in

$$\begin{aligned} f(-2) &= -17 \\ f(0) &= 3 \\ f(1) &= -2 \\ f(2) &= 23, \end{aligned}$$

we see that $f(x)$ has at least 3 real roots. The derivative $f'(x) = 5x^4 - 6$ has only two real roots. If $f(x)$ had more than 3 roots, then $f'(x)$ would have more real roots. So $f(x)$ has three real roots, and two complex roots. The two complex roots must be conjugates.

Now, let K be the splitting field of $f(x)$. Adjoining one root of $f(x)$ gives a degree 5 extension, so the degree of K is divisible by 5. So the Galois group G of $K/\mathbf{Q}$ is a subgroup of S_5, with order divisible by 5. This means that G contains an element of order 5. Since this element sits inside S_5, it must be a 5-cycle.

The Galois group G also contains a transposition, since restriction the complex conjugation map $\mathbf{C} \to \mathbf{C}$ to K gives an automorphism which permutes the two complex roots of $f(x)$, and which fixes the three real roots.

The group S_5 is generated any transposition together with any 5-cycle. Thus, the Galois group of $f(x)$ is S_5. But S_5 is not solvable. So $f(x)$ cannot be solved by radicals.

§23 April 29, 2020

§23.1 Solving the Cubic

Today we will work on solving the cubic. Historically, there were contributions to this problem from the Babylonians, Egyptians, Greeks, Chinese, Indians, Persians, and Italian.

In the early 16th century, Del Ferro solved $x^3 - mx = n$. This is the general case, if you allow m and n to be negative numbers. But Del Ferro didn't know about negative numbers (because negative numbers don't exist). He kept his solution secret until his death, when he passed it on to his student Antonio Fior. In 1530, Tartaglia announced that he can solve some cubics. This lead to a contest between Fior and Tartaglia. Tartaglia is asked to solve $x^3 + mx = n$, and he can do this. Fior is asked to solve $x^3 + mx^2 = n$. In 1539, Cardano persuaded Tartaglia to reveal his method, in the form of a poem (math was different back then). Cardano had to promise not to reveal it. Cardano got around this by publishing this result as the work of Del Ferro. Then Tartaglia challenged Cardano to a competition. At the end of the day, the solution was known as Cardano's formula. For more, see here.

Now, let's look at how to solve the cubic. Consider

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

Substitute $x = y - a/3$. We get

$$\begin{aligned} g(y) &= y^3 + py + q \\ p &= \frac{1}{3}(3b - a^2) \\ q &= \frac{1}{27}(2a^3 - 9ab + 27c). \end{aligned}$$

The splitting field for f and g is the same. Now, recall the *discriminant* of a polynomial,

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

for roots $\alpha_1, \ldots, \alpha_n$. In our case, you can check that the difference between any of the roots of $f(x)$ and $g(x)$ is the same, so the discriminant is the same.

Let α, β, γ be the roots of $g(y)$. Let's try to compute an expression for D in terms of p and q. Since $g(y) = (y - \alpha)(y - \beta)(y - \gamma)$, then

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

So $D = -g'(\alpha)g'(\beta)g'(\gamma)$. We can compute $g'(\alpha), g'(\beta), g'(\gamma)$, using $g(y) = y^3 + py + q$, and we get

$$-D = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p).$$

Recall from our discussion of symmetric functions, if we consider a general polynomial

$$(x - \alpha)(x - \beta)(x - \gamma) = x^3 - s_1 x^2 + s_2 x - s_3,$$

then

$$\begin{aligned} s_1 &= \alpha + \beta + \gamma \\ s_2 &= \alpha\beta + \alpha\gamma + \beta\gamma \\ s_3 &= \alpha\beta\gamma. \end{aligned}$$

In our case, $s_1 = 0, s_2 = p, s_3 = -q$. Expanding D, we get

$$-D = 27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3.$$

You can check that in terms of s_1, s_2, s_3, this simplifies to

$$-D = 27(-q)^2 + 9p(p^2) + 3p^2(-2p) + p^3,$$

so $D = -4p^3 - 27q^2$. We now have an expression for the discriminant, which allows us to examine the behavior of the roots: recall that for quadratics, if the discriminant is negative, there are no real roots, etc. In summary we have

$$D = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$$
$$D = -4p^3 - 27q^2.$$

We know that $g(y)$ has at least one real root (intermediate value theorem). Say that this root is α. Let's examine the other two roots, β and γ.

If β and γ are not real, then they are conjugates. This means that $\alpha-\beta$ and $\alpha-\gamma$ are conjugates as well, and so $(\alpha-\beta)^2(\alpha-\gamma)^2$ is real, and $\beta-\gamma$ is purely imaginary. Thus $D < 0$.

Conversely, if $D < 0$, then $g(y)$ has non-real roots. So the roots are real if and only if $D \geq 0$. If $D = 0$, then some roots repeat, and if $D > 0$ then they are all distinct.

Example 23.1

We can check that $x^3 + x^2 - 2x - 1$ has discriminant 35721, which is greater than zero, and thus $x^3 + x^2 - 2x - 1$ has three distinct real roots.

To solve cubics, let's look at the Galois group of a cubic. Let $g(y) = y^3 + py + q \in \mathbf{Q}[x]$. If $g(y)$ is reducible, the it factors as either a linear term times a quadratic, or as the product of three linear factors. So the Galois group is either $\mathbf{Z}_2$ or 1. If $g(y)$ is irreducible, then the Galois group is a subgroup of S_3 of order divisible by 3, and is therefore either $A_3 = \mathbf{Z}_3$ or S_3.

If the Galois group is $\mathbf{Z}_3$, then the splitting field has degree 3 and is obtained by adding any root. If it is S_3, we saw that $\sqrt{D} \notin \mathbf{Q}$. The splitting field in this case has degree 6, and is obtained by adding any root and $\sqrt{D}$.

This gives us a method to solve cubics. We will not derive Cardano's actual formula, but we will state it here. Define

$$A = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}$$
$$B = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$$
$$\rho = e^{2\pi i/3}.$$

Then the roots of $g(y) = y^3 + py + q$ are given by

$$\alpha = \frac{A+B}{3}$$
$$\beta = \frac{\rho^2 A + \rho B}{3}$$
$$\gamma = \frac{\rho A + \rho^2 B}{3}.$$

Note that we have to be a little bit careful about taking cube roots in A and B, since A and B might not be real. This formula works for any D, but remember that Cardano didn't know what imaginary numbers are (he never could have *imagined* them), so he was puzzled by the case $D > 0$, and this case was named "Casus irreducibilis."

Exercise 23.2. Express Cardano's formula in the form of a poem.

If $D > 0$, then there are three distinct real roots, for example with $x^3 + x^2 - 2x - 1$, and Cardano's formula requires going through complex numbers. Can we avoid complex numbers? The answer is no! We'll now prove that any formula for the cubic must go through the complex numbers, even if all the roots are real.

Suppose for contradiction that we had an irreducible polynomial $f(x) \in \mathbf{Q}[x]$ with three distinct real roots, and that we could express one of these roots by radicals involving *only* the reals. Then the splitting field of $f(x)$ is contained in a root extension

$$\mathbf{Q} = K_0 \subseteq K_1 = \mathbf{Q}(\sqrt{D}) \subseteq \cdots \subseteq K_s = K \subseteq \mathbf{R},$$

where K_{i+1}/K_i is a simple radical extension, $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, with $a_i \in K_i$. Note that $s \geq 2$, since the degree of the splitting field of $f(x)$ is divisible by 2, and $\mathbf{Q}(\sqrt{D})$ is degree 2.

Without loss of generality, take $n_i = p_i$ prime (since otherwise $n_i = m_i k_i$, and $\sqrt[n_i]{a_i} = \sqrt[m_i]{\sqrt[k_i]{a_i}}$). It follows that the degree is 1 or p_i, via the following lemma.

Lemma 23.3

If F is a subfield of $\mathbf{R}$, $a \in F$, and p is prime, then $d = [F(\sqrt[p]{a}) : F]$ is either 1 or p.

Proof. The minimal polynomial for $\alpha = \sqrt[p]{a}$ is

$$\prod_{\sigma \in \mathrm{Aut}(L/F)} (x - \sigma(\alpha)),$$

where L is the Galois closure of $F(\sqrt[p]{a})/F$. Since $\sigma(\alpha) = \alpha\zeta$, then multiplying the $\sigma(\alpha)$ together, we see that the constant term of the minimal polynomial is $\alpha^d\zeta$, where ζ is some p'th root of unity. Since $\alpha \in \mathbf{R}$, and $\alpha^d\zeta \in F$ is also real, then $\zeta \in \mathbf{R}$. This means that $\zeta = \pm 1$.

So $\alpha^d \in F$, and $\alpha^p = a \in F$. If $d \neq p$, then we can write $1 = ad + bp$ and we get $\alpha \in F$. Thus $d = 1$. □

Recall we saw that any extension containing $\sqrt{D}$ and a root of $f(x)$ must contain the entire splitting field. So without loss of generality, assume K_{s-1} does not contain a root of $f(x)$. In particular $f(x)$ is irreducible over K_{s-1}, so K_s/K_{s-1} has degree divisible by 3 Since the degree is prime, it must be exactly 3.

But K_s is the splitting field of $f(x)$ over K_{s-1} so it is Galois. Since $K_s = K_{s-1}(\sqrt[3]{a_{s-1}})$, then it contains the other cube roots of a_{s-1}, which means that K_s contains the cube roots of unity, so cannot be contained in the reals. So it's not possible to solve the cubic without using complex numbers! This is one of the ways the complex numbers were first seen to be useful.

Index