Lecture Notes

These are the daily lecture notes for MATH 322: Introductory Abstract Algebra, taught in Spring 2020 at the University of Northern Colorado.

Week 1: Jan 13-17
Monday, January 13

Today we introduce the course, including both logistics of how the course will run, and the content of the course through an activity about extension fields.

First, some notes on the syllabus:

- Textbook: a modified version of my Judson's abstract algebra book. The book is free online (link in Canvas).
- Quizzes, homework, exams, and project.
  - There will be in-class quizzes (occasional) and online reading quizzes, through Canvas.
  - Daily homework (1-2 problems). Expect to try them and resubmit for full credit.
    I encourage you to type homework using LaTeX or markdown. See link to blog post.
  - The exams will have a take-home and in-class portion. Announce tentative dates listed on syllabus. The final is cummulative, but a take-home
  - There is a group project: 2-3 students per group. We will work throughout the semester on it; you will present during the final exam meeting and submit a short paper on the topic.
- Classroom policies: participation, attendance, makeups, don't be rude, don't cheat, disability resources, other resources.

Introduction to Field Theory.

The goal today is to work through a problem typical of what we will try to do this semester. A lot of this should be review, but it is not easy review.

Work in groups on (((Unresolved xref, reference "ws_fields-intro"; check spelling or use "provisional" attribute))) .

For next class, read section 1.1. Next time you will work together to remind each other what you learned last semester.

Wednesday, January 15

Today you will work on an (((Unresolved xref, reference "ws_rings-review1"; check spelling or use "provisional" attribute)))activity to review rings, ideals, and quoteint rings.

Friday, January 17

We continue our review with an (((Unresolved xref, reference "ws_rings-review2"; check spelling or use "provisional" attribute)))activity to review the Euclidean algorithm and Bezout's lemma.

Week 2: Jan 20-24

No class on Monday, January 20th in observance of Marthin Luther King, Jr. Day.

Wednesday, January 22

Today we will bring together the review from last week to see how it helps us understand extension fields built to contain particular roots of polynomials.

Extension Fields as Quotient Rings.

To set the stage: we are considering a field E that extends a field F (which we often take to be $\mathbb{Q}$).

- We want E to be the smallest field in which a particular polynomial irreducible $p(x)$, with coefficients from the **base field** F, can factor.
- Let α be a root of $p(x)$. We consider $F(\alpha) = \{a + b\alpha + c\alpha^2 + \cdots : a, b, c, \ldots \in F\}$ (the powers of α go up to one less than the degree of $p(x)$).
- This is certainly a ring, but we want to make sure it is a field.
- Consider $F[x]$, the set of all polynomials with coefficients from F. Consider the **evaluation homomorphism** $\sigma_\alpha : F[x] \to F(\alpha)$ given by $\sigma_\alpha(p(x)) = p(\alpha)$. That is, just plug in α for x.
- We can easily see that σ_α is a *surjective* homomorphism. What's more, the *kernel* K of σ_α is an ideal that contains $p(x)$.
- In fact, K must contain exactly the polynomials that have α as a root. By the division algorithm, we can show that all these polynomials have $p(x)$ as a factor (since $p(x)$ is irreducible). That is, $K = \langle p(x) \rangle$.
- Thus by the Fundamental Homomorphism Theorem, $F[x]/\langle p(x) \rangle \cong F(c)$.
- The reason this is helpful: if we can prove that $F[x]/\langle p(x) \rangle$ is a field, then $F(c)$ must also be a field.
- The only thing we need to check is that every non-zero element of that quoteint ring $F[x]/\langle p(x) \rangle$ has a multiplicative inverse.

Friday, January 24

The goal today is to connect the work we have done with the Euclidean algorithm and Bezout's lemma to the idea of extension fields as quotient rings. Do the activity and discuss.

Week 3: Jan 27-31
Algebraic Numbers and Minimal Polynomials (Monday, January 27)

We have seen that if $p(x)$ is an irriducible polynomial in $F[x]$,with root α, that there is field extension $F(\alpha)$ of F. In fact, we can take this field extension to be $F[x]/\langle p(x)\rangle$.

Today we think about whether we can start with $c \in E$, an extension of F, instead of starting with a polynomial.

- First we need to agree what it means for a number α in a field E to be **algebraic** over another field F. It means that α is the root of some polynomial in $F[x]$.
- When $F = \mathbb{Q}$, then we say that α is an **algebraic number**.
- If α is *not* the root of a polynomial in $F[x]$, then it is called **transcendental** over F (and if $F = \mathbb{Q}$, simply a **transcendental number**).
- Now if E is a field extension of F and contains a number α algebraic over F, we can consider the smallest field containing F and α, which we write $F(\alpha)$. Note we have not said anything about a polynomial yet.
- Is $F(\alpha)$ isomorphic to $F[x]/\langle p(x)\rangle$ for some $p(x) \in F[x]$? If so, how much choice do we have for $p(x)$?
- Since α is algebraic, there is some polynomial it is the root of. In fact, there are infinitely many polynomials it is the root of.
- However, we can prove that there is a unique irreducible monic polynomial $p(x) \in F[x]$ of smallest degree such that $p(\alpha) = 0$. Further, any polynomial $f(x)$ for which α is a root is a multiple of $p(x)$.
    - Why is this true? We consider the evaluation homomorphism!
    - The easy way: the kernel of the homomorphism contains all polynomials for which α is a root. Since $F[x]$ is a principle ideal domain, there is a single generator for this ideal.
    - Here is a better way to understand this (which really just repeats the proof that $F[x]$ is a principle ideal domain). Let $p(x)$ be any polynomial of least degree that has α as a root. We can easily make $p(x)$ monic by dividing through by the leading coefficient.
    - Now suppose $f(x)$ is any other polynomial for which α is a root. Divide! That is, by the division algorithm there are $q(x)$ and $r(x)$ such that $f(x) = q(x)p(x) + r(x)$. Plug in α: $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha)$. But this says that $r(\alpha) = 0$, so $r(x)$ has α as a root. This says that $r = 0$ (since otherwise its degree wouls be less than $p(x)$).
    - This says that $f(x)$ is a multiple of $p(x)$.
- We call this smallest degree, irreducible monic polynomial the **minimal polynomial** for α over F. We will say that the **degree of α over F** is the degree of $p(x)$.
- For example, let $\alpha = \sqrt{2+\sqrt{3}}$. What does $F(\alpha)$ look like? First find that the minimal polynomial for this α is $p(x) = x^4 - 4x^2 + 1$. (Why is this irreducible? We will save that for another day.)
- We can now say that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle p(x)\rangle$. But this means that $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3\}$.
- Here is something strange: what if β was another root of $p(x)$? Then $\mathbb{Q}(\beta) \cong \mathbb{Q}[x]/\langle p(x)\rangle$ as well. So $\mathbb{Q}(\beta) \cong \mathbb{Q}(\alpha)$.

- For example, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3}$, since these are both roots of $x^3 - 2$.
- In general, we will want to explore how field extensions relate to each other. How are $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}+1)$ related? What about $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$?

Vector Space Review (Wednesday, January 29)

Let's review some basic ideas from linear algebra.

- When you first thought about vectors, you worked with a specific example: vectors in $\mathbb{R}^n$. These were columns of numbers which we could add together, as well as multiply by constants.
- In general, a vector space is a collection of objects called *vectors* together with some field of *scalars* and two operations: addition on the vectors and scalar multiplication (allowing vectors to be multiplied by scalars).
- Just like with groups and rings, there are some axioms that a vector space must adhere to which say how addition and scalar multiplication work. For one, the vectors under addition form an abelian group. Also, scalar multiplication works like you expect (in terms of distributive properties and associativity).
- We are particularly interested to two concepts: linear independence and span.
- A set of vectors is linearly *dependent* if one of them is a linear combination of the others (in other words, you can get one by adding scalar multiples of the others). Another way to say this is that you can get the zero vector as a non-trivial linear combination of the others. That is
$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$
with not all of $a_1, a_2, \ldots, a_n$ equal to 0.
- Thus a set of vectors is linearly independent if the only way to get 0 as a linear combination is for all the scalars to be 0.
- If we can get a vector $\mathbf{v}_0$ as a linear combination of, say $\mathbf{v}_1$ and $\mathbf{v}_2$, then we say that $\mathbf{v}_0$ is in the *span* of $\mathbf{v}_1$ and $\mathbf{v}_2$.
- If we have a set of vectors so that every vector in the vector space is in their span, we say the set of vectors *spans* the vector space.
- Now think of starting with a single vector and building the largest possible set of linearly independent vectors. Eventually, you will get to a point where you can't add any more. This is because every vector not in your set is in the span of the set. This maximal set of linearly independent vectors must span the vector space.
- Alternatively, start with a large set of vectors which span the vector space. If any of these are in the span of the remaining vectors, we can get rid of it (we don't need it to span the vector space). So trim down the set until we get a minimal spanning set. This set must be linearly independent (otherwise we could get rid of the vector which was a linear combination of the others).
- The number of vectors in any maximal independent set will be equal to the number of vectors in all minimal spanning sets. Such sets are called *bases* for the vector space, and the number of vectors in the set is called the *dimension* of the vector space.

Degrees of Field Extensions (Friday, Jan 31)

Why do we care about vector spaces? It turns out you can view a field extension as a vector space. This is useful because we can borrow the concept of linear independence, span and dimension and apply them to better understand field extensions.

- Let F be a field and K and extension field. We can view the elements of K as vectors, and the elements of F as scalars. This makes K into a vector space.
- Vector spaces have dimension (the number of vectors in any basis). We are most interested in when that dimension is finite, say n. In this case we say that K is an **extension of degree** n or that the **degree of K over F** is n and write
$$[K : F] = n.$$
- Now consider our favorite field extension $F(c)$ over F. Recall this is the smallest field containing both F and c. What is the degree of $F(c)$ over F?
- Suppose c is *algebraic* over F (that is, it is the root to some polynomial $p(x)$ in $F[x]$). Well let $p(x)$ be the minimum polynomial of c over F, say of degree n. Then we can write every element of $F(c)$ as
$$a_0 + a_1c + a_2c^2 + \cdots + a_{n-1}c^{n-1}$$
where the a_i are in F. In other words, the set $\{1, c, c^2, \ldots, c^{n-1}\}$ span $F(c)$.
- Actually, how do we know this? Well let $a(c)$ be any element of $F(c)$. We know for sure that $a(x)$ is some polynomial (possibly of degree larger than n) because $F(c)$ contains c and is closed under addition and multiplication.
- Now use the division algorithm on $a(x)$ and $p(x)$. We get
$$a(x) = q(x)p(x) + r(x)$$
where $\deg(r(x)) \leqslant n - 1$. So plug in c: we get $a(c) = r(c)$. Thus we only need to go up to a c^{n-1} term.
- So $\{1, c, c^2, \ldots, c^{n-1}\}$ spans $F(c)$. Is the set linearly independent? Well consider a linear combination equal to 0:
$$a_0 + a_1c + a_2c^2 + \cdots + a_{n-1}c^{n-1} = 0$$
If any of the coefficients a_i were non-zero, we would have a polynomial of degree $n - 1$ for which c was a root. But $p(x)$ of degree n was the minimum polynomial, so this is impossible. Thus the set is indeed linearly independent.
- Putting these together, we see that $\{1, c, c^2, \ldots, c^{n-1}\}$ is a basis for $F(c)$, and thus $F(c)$ is a degree n extension of F.

What is the degree of $\mathbb{C}$ over $\mathbb{R}$?

What is the degree of $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$? Well the minimum polynomial for $\sqrt{5}$ is $x^2 - 5$ (why is this minimal?). Thus $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Notice this confirms our suspicion that every element of $\mathbb{Q}(\sqrt{5})$ can be written as $a + b\sqrt{5}$ for rational a and b.

What is the degree of $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ over $\mathbb{Q}(\sqrt{5})$? What about over $\mathbb{Q}$? Well if we start with $\mathbb{Q}(\sqrt{5})$ as our base field, we must find the minimum polynomial for $\sqrt{7}$. First, could $\sqrt{7}$ be in $\mathbb{Q}(\sqrt{5})$? If it were, then $\sqrt{7} = a + b\sqrt{5}$. Square both sides and rearrange to get that $\sqrt{5}$ is rational (it is not). Notice that $\sqrt{7}$ is a root of $x^2 - 7$. This is irreducible over $\mathbb{Q}$, but because $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$, it is also irreducible in $\mathbb{Q}(\sqrt{5})$. Thus $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ has degree 2 over $\mathbb{Q}(\sqrt{5})$. Similarly, it has degree 2 over $\mathbb{Q}(\sqrt{7})$. What about over $\mathbb{Q}$? It turns out it has degree 4 over $\mathbb{Q}$. Why?

Week 4: February 3-7
Monday: Summary of Extension Fields

Let's summarize what we have said about field extensions so far.

- Given any field F and any number α algebraic over F, we can form $E = F(\alpha)$, an algebraic extension of F.
- This is the smallest field containing F and α, by definition.
- Since α is algebraic, it is the root of a polynomial in $F[x]$. In fact, there must be some irreducible monic polynomial $p(x)$ that has α as a root. We call this the **minimal polynomial** for α.
- If the degree of $p(x)$ is n, then we know that every element in $F(\alpha)$ can be written in the form $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$. The reason we know this is because $F(\alpha) \cong F[x]/\langle p(x)\rangle$, and we know that the quotient ring is a field.
- That we can write everything in that form says that as a *vector space*, $F(\alpha)$ has dimension n. That is, there is a basis containing n elements, specifically, $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.
- We also saw that we can extend an extension field further by adding another algebraic element: $F(\alpha, \beta)$ is an extension of $F(\alpha)$.
- We can look for the degree of this field extension over $F(\alpha)$, again by looking for the size of a basis (with the field of scalars now being $F(\alpha)$), or by looking for an irreducible polynomial in $F(\alpha)[x]$ that has β as a root.
- If $[F(\alpha, \beta) : F(\alpha)] = m$ (our notation for the degree of the extension), then we can multiply to find $[F(\alpha, \beta) : F] = n \cdot m$. We call this the tower rule.

Let's work through an example.

- Explore $\mathbb{Q}(\sqrt[5]{7}, \sqrt{2}i)$. Can we compare this to $\mathbb{Q}(\sqrt[5]{7} + \sqrt{2}i)$ (which is a simple extension, rather than an iterated extension)?

We have seen that if we adjoin an algebraic element to a field, we get a finite extension (an extension of finite degree). What if I told you I had a finite degree extension. Is every element algebraic?

- Yes! Let $\alpha \in E$ be any element of the field E with $[E : F] = n$.
- We know then that $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly *dependent*, since it is a set that contains $n+1$ elements.
- This means that there are scalars $c_0, \ldots, c_n$, not all zero, such that $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$.
- But then $p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ has α as a root.
- Careful: this does not say that $E = F(\alpha)$, since we don't know that $p(x)$ is irreducible here. In fact, we could take $\alpha \in F$. Then the minimal polynomial is degree 1.

For next time: do the constructions preview activity.

Wednesday: Constructible Numbers

The activity you did to prepare for class today shows that some geometric objects are constructible, while others might not be. But how can we be sure that it is *impossible* to "double the cube," for example?

We need to algebratize constructions. We will define a set of **constructible numbers** and then use abstract algebra to analyze this set.

Complete the activity (((Unresolved xref, reference "ws_fields-constructable-numbers"; check spelling or use "provisional" attribute)))Constructible Numbers .

Friday: Constructible Extensions

Last class we saw that the set of constructible numbers is a *field*, extending $\mathbb{Q}$ and closed under taking square roots of positive elements. Today we will consider the converse: are there any other constructible numbers other than those you can get from $\mathbb{Q}$ using field operations and square roots.

- Let's think about constructible points (a, b) in the plane $\mathbb{R}^2$. Certainly if a and b are constructible numbers (as defined previously) then (a, b) a constructible point (by using perpendicular lines).
- Also, if (a, b) is constructible, so is $(0, b)$ and $(a, 0)$.
- We already know that all rational numbers are constructible, so we now have all points in $\mathbb{Q} \times \mathbb{Q}$ constructible.
- Consider the field $K_1 = \mathbb{Q}(a, b)$ where the point (a, b) was constructed in one step from $\mathbb{Q} \times \mathbb{Q}$. Then $K_2 = K_1(c, d)$ where the point (c, d) was constructed in one step from points in $K_1 \times K_1$. And so on.
- If a point is to be constructible, then it will need to be constructed in some finite number of steps starting from $\mathbb{Q} \times \mathbb{Q}$.
- Recall that a point is constructible provided it is at the intersection of lines and circles, each of which are constructible.
- Consider the case for the intersection of two lines. Let L_1 pass through (a_1, b_1), and (c_1, d_1) and L_2 pass through (a_2, b_2) and (c_2, d_2). Can we find the coordinates of the intersection of these two lines?
- Yes, doing so requires solving a system of two linear equation. In particular, the new x coordinate is a linear combination of $a_1, a_2, b_1, \ldots, d_2$.
- So x is the root of a degree 1 polynomial over K_i, so $[K_{i+1} : K_i] = 1$. Similarly for y.
- What about the intersection of a line and a circle? Recall that we can write the equation of a circle as $(x - a)^2 + (y - b)^2 = k^2$. Substitute in the equation for the line to get a quadratic polynomial in x (or y).
- Finally, the intersection of two circles. Use the equation for a circle in the form

  $$x^2 + y^2 + dx + ey + f = 0$$

  and take the difference of the two equations to get a linear expression involving x and y which can be substituted into one of the equations for the circle as above.

- What does all this tell us? Well, if we extend $\mathbb{Q}$ to get a field containing the coordinates of a constructible point, then we must have extended *only* by taking square roots of elements. Of course, not necessarily elements in $\mathbb{Q}$, but definitely elements in some extension field we got along the way.

- More specifically, we have that if F is some field containing constructible numbers, then the points determined by the intersections of lines and circles in F lie in the field $F(\sqrt{\alpha})$ for some $\alpha \in F$.

- Since this is recursive, we can say that a real number α is constructible if and only if there exists a sequence of fields
$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_k$$
such that $F_i = F_{i-1}(\sqrt{\alpha_i})$ with $\alpha_i \in F_i$ and $\alpha \in F_k$.

- This tells us exactly what sort of field extension any constructible number belongs to. It also says that the field of *all* constructible numbers is an infinite algebraic extension of $\mathbb{Q}$.

- But what about doubling the cube? Note that if we started with a cube of side length 1, we would get a cube of volume 2, so side length $\sqrt[3]{2}$. Is this a constructible number? If it is, then it is in a field extension of $\mathbb{Q}$ like those described above. So is it? Not obviously so, since it is not the square root of a number. But perhaps we can get the $\sqrt[3]{2}$ in a field extension you make by just adding square roots.

- What does all this tell us? Well, if we extend $\mathbb{Q}$ to get a field containing the coordinates of a constructible point, then we can be sure that the degree of the field extension is a power of 2.

- So what? Well what if we could double the cube? This would mean we could start with a cube of side length 1, and get a cube with volume 2. But the side length of such a cube would be $\sqrt[3]{2}$, and $\sqrt[3]{2}$ belongs to a degree 3 field extension, so any field containing $\sqrt[3]{2}$ would need to have degree a multiple of 3.

- Trisecting the angle? Consider an attempt to trisect 60°. We would be able to construct 20° then, so surely we could also get $\cos(20^\circ)$ as a constructible number (how?). But
$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$$
and since $\cos(60^\circ) = 1/2$, this says that $\cos(20^\circ)$ is a root of the polynomial $8x^3 - 6x - 1$ or that $2\cos(20^\circ)$ is the root of $x^3 - 3x - 1$. We can show this is irreducible using the rational roots theorem. So again, any extension containing a trisected 60° would have a degree that was a multiple of 3.

- Finally, if we could square the circle, then we would be able to construct a square whose side length was $\sqrt{\pi}$. But this is transcendental, so definitely would not give an extension whose degree was a power of 2.

Week 5: February 10-14
Galois Theory

We have been investigating fields for the last few weeks. One application of this was to see that certain numbers (and shapes) are not *constructible*. It is surprising that we can make such a concrete connection between geometry and algebra (although *analytic* geometry is just this: describing geometric objects with equations and numbers).

This was not our primary reason to study fields though. So why are we doing all this in an algebra class? Why does UNC think you should learn this before teaching high school algebra? Well basic algebra is largely about solving equations, and when those equations involve polynomials of degree greater than 2, this becomes very challenging.

Our goal for the next few classes is to better understand the relationship between polynomials and field extensions. This will lead us to our final application: deciding when you can solve a polynomial using radicals.

Monday: Derivatives and Roots.

- Recall what we know about extension fields and their relationship to minimum polynomials.
- If a polynomial $p(x)$ has degree n, what can you say about the number of roots it has (in a large enough extension field)?
- We know it must have at most n roots, but these might not be distinct. But what if $p(x)$ is irreducible?

  Let $p(x) \in F[x]$ be irreducible, and assume that F has characteristic 0. Then $p(x)$ does not have any repeated roots.

  The cool thing about this proof is that it uses derivatives. But we define these purely formally. But still the usual way.

  Suppose $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ does have a repeated root (in some extension field), call it c. Then $p(x) = (x-c)^2q(x)$ for some polynomial $q(x)$. Now consider $p'(x)$:

  $$p'(x) = 2(x-c)q(x) + (x-c)^2q'(x) = (x-c)(2q(x0 + (x-c)q'(x))$$

  So $x - c$ is a factor of $p'(x)$ so c is a root.

  Since $p(x)$ is irreducible and has c as a root, $p(x)$ must be the minimum polynomial for c. This says that every polynomial which has c as a root is a multiple of $p(x)$. In other words, $p'(x)$ is a multiple of $p(x)$. But unless $p'(x) = 0$, this is impossible because $p'(x)$ has smaller degree than $p(x)$.

  So $p'(x) = na_nx^{n-1} + \cdots + a_1 = 0$ would imply that $na_n = 0$. This cannot happen in a field of characteristic 0 (although if we were in $\mathbb{Z}_5[x]$ this would be problematic).
- From here on out, let's consider fields of characteristic 0 only (that is, extensions of $\mathbb{Q}$). Now irreducible polynomials have only distinct roots.
- Now do the field extension thing for these roots. What can happen?
- We can adjoin a root, and then in that bigger field, the polynomial factors. But does it factor into linear terms? Maybe, maybe not. If not, then we could find a root to one of the factors and adjoin that as well. Eventually, we will adjoin enough roots to get an extension field in which the polynomial factors completely (into linear factors).

- This extension field is call the *root field* or *splitting field* of the polynomial (because in that field, the polynomial "splits" into linear factors).

  What is the splitting field of $p(x) = x^3 + 2$? What is its degree over $\mathbb{Q}$?

  What is the degree of the splitting field of $p(x) = x^4 - 10x^2 + 25x - 5$? Well, $p(x)$ is irreducible, so there is at least one root α which we can adjoin to $\mathbb{Q}$ to get the degree 4 field extension $\mathbb{Q}(\alpha)$. Now what? From the polynomial's graph, we know that there are 2 real roots, so 2 complex roots. If α was one of the real roots, then we are not yet in the splitting field. So we need to add another root β. This might be of degree 2 or 3, depending on how $p(x)$ factored in $\mathbb{Q}(\alpha)$. It get's messy.

- Notice that if c and d are two distinct roots of $p(x)$, then $F(c) \cong F(d)$. Why?

- In fact, what can we say about isomorphisms between field extensions?

Wednesday and Friday: Isomorphisms and Automorphisms of Extension Fields

To understand splitting fields better, and to understand how the roots of polynomials relate to each other, we want to consider isomorphisms between extension fields.

- Suppose you have two extensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ of $\mathbb{Q}$. How might these be related to each other?

- Specifically, what if α and β are both roots of the same polynomial? Then each are isomorphic to $\mathbb{Q}[x]/\langle p(x)\rangle$, so isomorphic to each other.

- What does that isomorphism look like? Where can it send elements from $\mathbb{Q}$? Where does it send α?

- Since the 0 and 1 need to be sent to themselves, all of $\mathbb{Q}$ must be sent to itself!

- Elements in $\mathbb{Q}(\alpha)$ look like $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^n$. Apply the isomorphism to this! If we send α to β, this works.

- More in general, if you have an isomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\beta)$, consider what happens to polynomials in $\mathbb{Q}[x]$ under this isomorphism. In particular, consider the minimum polynomial for α and β.

- Let's consider the set of all automorphisms of a field, call it $\mathrm{Aut}(F)$. It is easy to see that $\mathrm{Aut}(F)$ is a group (under composition).

- Now consider a field extension E of F and the elements of $\mathrm{Aut}(E)$. Instead of looking at all the automorphisms, look only at the automorphisms that *fix* F. That is, $\sigma(a) = a$ for all $a \in F$.

- Call the set of these automorphisms $\mathrm{Gal}(E : F)$. This is called the *Galois group* of E over F. It is called a group because it is! Show this.

  Consider $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. This is an extension of $\mathbb{Q}$, but also of $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$. Describe $G(E/\mathbb{Q})$. What group is this? (It is $\mathbb{Z}_2 \times \mathbb{Z}_2$.)

- So what does this have to do with polynomials?

- Well if $p(x)$ is a polynomial in $F[x]$, and suppose E is an extension of F containing (some of the) roots of $p(x)$. Then any automorphism in $G(E/F)$ defines a permutation of the roots of $p(x)$ that lie in E, since roots are sent to roots.

- The converse of the above is also true. That is, if a and b are roots of the same polynomial, then there is an isomorphism $\varphi : F(a) \to F(b)$ that fixes F.

- Now we are ready to think about how large the Galois group can be. Say $p(x)$ is a polynomial in $F[x]$ and E is the splitting field for $p(x)$ over F. As long as f has no repeated roots, then $|G(E/F)| = [E : F]$.

  Proceed by induction on the degree of $p(x)$. If the degree is 1, then $E = F$ and we are done. Assume the result holds for all polynomials of degree $k < n$ and that $p(x)$ has degree n.

  Now let $q(x)$ be an irreducible factor of $p(x)$ (maybe $q(x) = p(x)$), with degree m. The roots of $q(x)$ lie in E, so pick one of them, call it a. We have

  $$[E : F(a)] = n/m \quad \text{and} \quad [F(a) : F] = m$$

  Now $q(x)$ has exactly m roots, all of them in E. For each root b we have an isomorphism from $F(a)$ to $F(b)$ which fixes F. So there are m such isomorphisms.

  Consider $G(E/F(a))$. This is the set of all automorphisms of E that fix $F(a)$. By our inductive hypothesis, we have $|G(E/F(a))| = [E : F(a)] = n/m$. Each of these composed with an isomorphism between $F(a)$ and $F(b)$ gives an element of $G(E/F)$.

- Find the Galois group of $p(x) = x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$. Note this is irreducible over $\mathbb{Q}$ by Eisenstein (and substitution of $x + 1$ for x). To find the roots, first multiply by $(x - 1)$ to get $x^5 - 1$. Let a be a fifth root of unity. Then $\mathbb{Q}(a)$ is the splitting field and has degree 4 over $\mathbb{Q}$. What are the automorphisms? Well, send a to a^i for $i = 1, 2, 3, 4$. The automorphism σ_2 which sends a to a^2 generates $G(\mathbb{Q}(a)/\mathbb{Q})$, so the group is $\mathbb{Z}_4$.

Week 6: February 17-21
Monday: Galois Correspondence

Recall that the Galois group of a splitting field K over a base field F is the group of all automorphisms of K that leave F fixed. These automorphisms are determined by where they send the roots of a (really any) polynomial $p(x) \in F[x]$ that has K as its splitting field: roots of an irreducible polynomial must be sent to other roots of the same irreducible polynomial. So we can determine quite a bit about the splitting field, polynomials that split in the field, and the Galois group using the other two of these to say something about the third.

Today, let's look at what can happen in *subgroups* of the Galois group.

- Start with a familiar example. $K = \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$ has Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2$. We can list out the automorphisms exactly, but let's call them ε, α, β and γ.
- We can think of $\varepsilon = (0,0)$, $\alpha = (1,0)$, etc. where a zero means we send $\sqrt{3}$ or $\sqrt{5}$ to itself, a 1 means we sent it to its negative.
- What do the subgroups look like? There are 5 subgroups: the two trivial subgroups and the subgroups $\{\varepsilon, \alpha\}$, $\{\varepsilon, \beta\}$, and $\{\varepsilon, \gamma\}$. Draw the lattice of subgroups.
- Look at $H = \{\varepsilon, \alpha\}$, where α sends $\sqrt{3}$ to $-\sqrt{3}$ and $\sqrt{5} \mapsto \sqrt{5}$. Note that all (both) the automorphism of K here fix every element in $\mathbb{Q}(\sqrt{5})$.
- We call $\mathbb{Q}(\sqrt{5})$ the fixed field of the subgroup H. For short, call it the *fixfield* of H. Will every subgroup of $G = G(K/\mathbb{Q})$ have a fixfield?
- What about the other direction? Suppose you have a subfield E of K contained in $\mathbb{Q}$ (an *intermediate field*). Of course we can consider the Galois group $G(K/E)$, the set of all automorphisms of K that fix E. Try this with $\mathbb{Q}(\sqrt{3})$. You get a subgroup of G, which will will call the *fixer* of E. Does every intermediate field have a fixer?
- There is a very strong relationship between the fixfields of subgroups of G and fixers of intermeidate fields. Every subgroup has a fixfield, and the fixer of the fixfield is the subgroup. Every intermdiate field has a fixer, and the fixfield of the fixer is the intermediate field!
- Note that so far we have thought of the intermediate fields in our example as just $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$. But since there are three intermediate subgroups, there must be three intermediate fields. Can we find the last fixfield? It's $\mathbb{Q}(\sqrt{15})$.
- There is more! What can we say about the degree of extensions in the field lattice and the size of the subgroups? Well, the size of a subgroup H of G will be equal to $[K : I]$, where I is the fixfield of H. Note that this really shows that the lattice of subgroups matches up with the lattice of intermediate fields, just flipped upside down.

Week 7: February 24-28

Monday is the in-class half of exam 1.

Wednesday: Cayley's Theorem

Main question: What do the roots of $x^5 - 5x - 2$ look like? Is there something analogous to the quadratic formula that will tell us the roots?

Approach: Describe the splitting field E, and consider $G(E/\mathbb{Q})$ and its subgroups. Use properties of groups to say something interesting about the subgroups. Translate this back to say something interesting about the splitting field (and its subfields). Translate that to say something about the polynomial.

But before we can do that, we need to remind ourselves about groups and learn some more advanced tolambdacs in group theory. Let us begin.

- Remember the definition of a group. There are three axioms.
- Some examples to keep in mind: D_4, S_3, $\mathbb{Z}_n$ (infinite groups like $\mathbb{Z}$, $\mathbb{Q}$, etc will be of less interest).
- How should we *represent* our groups? Remember that there are lots of groups that look different but end up being the same (isomorphic). So we should think a bit about how to present groups in some standard way.
- Do the activity: Cayley Permutations.
- One example of a group from last semester was S_n, the group of permutations on n elements. The symmetric groups, and subgroups of them, are nice to work with, since it is relatively easy to say how to multiply elements.
- You might wonder if there are any other groups. In some sense the answer is yes: D_4, $\mathbb{Z}_7$, $\mathbb{Z}$, $\mathbb{R}^*$, etc. But some of these turned out to be isomorphic to a symmetric group or at least a subgroup of a symmetric group. Is this always the case?
- Surprisingly YES! Cayley's theorem says that every group is isomorphic to a group of permutations. That is, to a subgroup of some symmetric group. In fact, if $|G| = n$ (that is, G has exactly n elements) then G is isomorphic to a subgroup of S_n.
- Example: Find a group of permutations isomorphic to $G = \{a, b, c, d\}$ whose table is given below

  Table 1

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

  There are many answers. We will give what is called the (left) regular representation of G. We will show that G is a subgroup of S_4. The idea is that we think of the elements as 1, 2, 3, and 4, and assign to each element $g \in G$ the permutation which moves each element to the result of multiplying it by g on the left.

So we will have 4 permutations: λ_a, λ_b, λ_c, and λ_d. λ_a says where each element goes when you multiply it by a. Well, the elements stay put, since a is the identity. So $\lambda_a = (1)$. Now λ_b is the permutation: "multiply by b on the left." So $\lambda_b = (12)(34)$. This is because multiplying by b causes the first and second elements to swap places, and the 3rd and 4th as well: $ba = b$, $bb = a$, $bc = d$ and $bd = c$. Next $\lambda_c = (13)(24)$ and finally $\lambda_d = (14)(23)$.

Proof of Cayley's Theorem.

- Cayley's theorem says that every group is isomorphic to a group of permutations.
- Let's prove this. Now remember, to show G is isomorphic to H, we must find an isomorphism $\varphi : G \to H$. We want H to be a subgroup of S_A. So for each $a \in G$, we want $\varphi(a)$ to be a permutation of the elements in A. What should A be?
- How about...THE ELEMENTS OF G!?!?!? Yes, take A to be the set G.
- Consider the permutation $\lambda_a : G \to G$ defined by $\lambda_a(x) = ax$. That is, the permutation takes an element in G and sends it to the result of multiplying that element by a (on the left).
- Now, what do we need to prove?
  1. It better be that λ_a is a bijection (so that it is an element of S_G). So each λ_a must be injective (one-to-one) and surjective (onto).
  2. We must show that $\bar{G} = \{\lambda_a : a \in G\}$ really is a subgroup of S_G. So we need to show that $\bar{G}$ has the identity, is closed under the operation (composition) and is closed under inverses.
  3. It's not enough that $\bar{G}$ is a subgroup of S_G: it must be the right one. That is, we must show that $\bar{G} \cong G$. Let $\varphi : G \to \bar{G}$ be defined by $\varphi(a) = \lambda_a$. Now prove this is an isomorphism: φ is injective, surjective, and satisfies the homomorphism property.

Even and Odd Permutations

- Here is a bar bet. Suppose you have 5 playing cards (all with different numbers) laid out in a row. You and a friend take turns, swapping the position of any two cards at a time. You must work together to get the cards in the correct order and must do so after both of you have had an equal number of turns.
- The bet: you won't be able to do it, no matter what you try. That is, if I start with the correct arrangement. So how can I pick arrangements which will prevent you from completing the task?
- Notice that what we are really doing is starting with a permutation of the set $\{1, 2, 3, 4, 5\}$ and writing it as a product of transpositions. Actually, we are finding the inverse permutation, as a product of transpositions, but it should be clear that by reversing it (whatever that means) we get the original permutation as a product of transpositions. The requirement that both players move the same number of times asks for there to be an *even* number of transpositions.
- If there are some initial configurations which can not be "solved" that means that the (inverse of the) permutation *cannot* be written as the product of an even number of transpositions. There are permutations like this.

- In fact, a permutation can be written as an even number of transpositions if and only if it cannot be written as a product of an odd number of permutations. Given this fact, it makes sense to call a permutation itself either even or odd - doing so is well defined.
- Let's prove: No permutation can be written as both an even number and an odd number of transpositions.
- Consider first how you might write the identity ε as a product of transpositions. We can prove that the number of transpositions must be even. We do this by rewriting the product using 2 fewer transpositions. This is enough, because it is obvious that ε can't be written as one transposition.
- The idea: fix some number x and find the last time x occurs (the right-most x). We move this x to the left until the transposition it is in is next to a copy of itself, in which case you can remove both copies.
- Show this process with an example: $\varepsilon = (45)(23)(13)(25)(14)(24)(35)(15)$ Use $x = 3$.
- More precisely, what are the possibilities for the transposition directly to the left of (xa). If it is (xa), remove both. If it is (bc), we can swap them, since disjoint cycles commute. If it is (xb), then write $(xb)(xa) = (xa)(ab)$. If it is (ab), then write $(ab)(xa) = (xb)(ab)$.
- Once we know that ε is even, suppose π is both even and odd. Then so would be π^{-1}. But then $\pi \circ \pi^{-1} = \varepsilon$ would be odd.
- Neat. It now makes sense to call a permutation *even* if it can be written as an even number of permutations, and *odd* otherwise. That is, the *parity* of a permutation is a property of the permutation, not just the way we happen to write it.
- We will let A_n denote the set of all even permutations in S_n. What would it take to prove that A_n is a subgroup of S_n?
- How many elements are in A_n? That is, how many of the $n!$ elements of S_n are even?
- To prove that $|A_n| = \frac{1}{2}|S_n|$, we can define a bijection from the set of even permutations to the set of odd permutations. Do this by picking any transposition σ and sending τ to $\sigma\tau$ (that is, compose the even transposition τ with σ, but this really just means writing σ at the start of the transposition τ). We can prove this is injective and surjective. Thus the set of even permtuations will be the same size as the set of odd permutations.

Week 8: March 2-6
Monday: Even and Odd Permutations, again

On Friday we started to prove that the identity is an even permutation (i.e., that no matter how you write it as a product of transpositions, you will always use an even number of them). This would be enough to prove that every permutation is either always even or always odd. Let's start by completing that proof.

- Let's prove: No permutation can be written as both an even number and an odd number of transpositions.
- Consider first how you might write the identity ε as a product of transpositions. We can prove that the number of transpositions must be even. We do this by rewriting the product using 2 fewer transpositions. This is enough, because it is obvious that ε can't be written as one transposition.
- The idea: fix some number x and find the last time x occurs (the right-most x). We move this x to the left until the transposition it is in is next to a copy of itself, in which case you can remove both copies.
- Show this process with an example: $\varepsilon = (45)(23)(13)(25)(14)(24)(35)(15)$ Use $x = 3$.
- More precisely, what are the possibilities for the transposition directly to the left of (xa). If it is (xa), remove both. If it is (bc), we can swap them, since disjoint cycles commute. If it is (xb), then write $(xb)(xa) = (xa)(ab)$. If it is (ab), then write $(ab)(xa) = (xb)(ab)$.
- Once we know that ε is even, suppose π is both even and odd. Then so would be π^{-1}. But then $\pi \circ \pi^{-1} = \varepsilon$ would be odd.
- Neat. It now makes sense to call a permutation *even* if it can be written as an even number of permutations, and *odd* otherwise. That is, the *parity* of a permutation is a property of the permutation, not just the way we happen to write it.
- We will let A_n denote the set of all even permutations in S_n. What would it take to prove that A_n is a subgroup of S_n?
- How many elements are in A_n? That is, how many of the $n!$ elements of S_n are even?
- To prove that $|A_n| = \frac{1}{2}|S_n|$, we can define a bijection from the set of even permutations to the set of odd permutations. Do this by picking any transposition σ and sending τ to $\sigma\tau$ (that is, compose the even transposition τ with σ, but this really just means writing σ at the start of the transposition τ). We can prove this is injective and surjective. Thus the set of even permutations will be the same size as the set of odd permutations.

Monday: Solvable Groups

The goal today is to gain familiarity with the definitions of subnormal and normal series, and to understand what a composition or principle series is. This will lead to the definition of a solvable group.

One preliminary is the notion of a *simple group*. These are groups that have no non-trivial normal subgroups. One of the great accomplishments of algebra recently is the complete classification of all finite simple groups in 2008. It turns out that the simple groups are only

- $\mathbb{Z}_p$ for prime p,

- A_n for $n \geqslant 5$,
- Belong to one of 16 families of groups of Lie type.
- One of 26 exceptions (called the sporadic groups, 20 of which are subquotients of the *Monster group* of order $2^{46}3^{20}5^{9}7^{6}11^{2}13^{3}17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \times 10^{53}$, the other 6 known as *p*ariahs).

For us: $\mathbb{Z}_p$ or A_n.
Now do the activity to remind ourselves how subgroups and quotient groups interact.

Wednesday: Normal Series

- Motivating question: Let G be a group with normal subgroup H. Suppose G/H is not simple (that is, it has a normal subgroup). What does that tell us about the relationship between G and H?
- Perhaps consider the example $G = \mathbb{Z}_{60}$ and $H = \langle 6 \rangle$. What is $\mathbb{Z}_{60}/\langle 6 \rangle$? It looks like $\mathbb{Z}_6$. Now $\mathbb{Z}_6$ has a normal subgroup $\{0, 3\}$. Which subgroup of G/H is this? Can we recognize this as a quotient group itself?
- Finish up the activity from last time.
- The Jordan-Hölder Theorem: Any two composition series of G are isomorphic. By isomorphic, we mean there is a 1-1 correspondence between the quotient groups in the composition series.
- This is really remarkable. It says that however you decompose a group using a subnormal series, you will essentially get the same series (in as much as the quotient groups will match up). In particular, the *length* of composition series is well defined.
- Another useful definition is this: A group G is *solvable* if it has a subnormal series $\{H_i\}$ such that all the quotient groups H_{i+1}/H_i are abelian. Next week we will see why calling such groups "solvable" makes sense.

Friday: Simplicity of the Alternating Group

Today we will work through an activity that proves that S_5 is not solvable, by showing that A_5 is simple: it contains no non-trivial normal subgroups.

Week 9: March 9-13
Monday and Wednesday: Solvability by Radicals

Here is the main question we asked after the last exam: What do the roots of $x^5 - 5x - 2$ look like? Is there something analogous to the quadratic formula that will tell us the roots?

Approach: Describe the splitting field E, and consider $\text{Gal}(E : \mathbb{Q})$ and its subgroups. Use properties of groups to say something interesting about the subgroups. Translate this back to say something interesting about the splitting field (and its subfields). Translate that to say something about the polynomial.

Today, let's remind ourselves about what we know from Galois theory.

- Given a polynomial $p(x)$, we can find its *splitting field* E, the smallest extension field in which the polynomial factors into linear terms (splits).
- We can look at automorphisms of the splitting field that *fix* the base field (usually $\mathbb{Q}$, which has to be fixed anyway).
- These automorphisms must send roots of irreducible polynomials to roots of the same irreducible polynomial. If $p(x)$ is not irreducible, then we need to look at its irreducible factors to see what the automorphisms look like.
- The set of all $\mathbb{Q}$-fixing automorphisms of E forms a group (under composition) called the *Galois group of E over $\mathbb{Q}$*, written $\text{Gal}(E : \mathbb{Q})$.
- There is a strong connection between the field extension and the Galois group, which is the content of the *Fundamental Theorem of Galois Theory*.
- One of these is that the size of the Galois group is equal to the degree of the field extension. But there is more.
- If we look at a subgroup H of $\text{Gal}(E : \mathbb{Q})$, we get a subset of the automorphisms of E that fix $\mathbb{Q}$. We consider the set of elements in E that are fixed by all the automorphisms in H. This is a field F, and thus an *intermediate field* between $\mathbb{Q}$ and E. We call it the *fixed field* of H.
- On the other hand, if we take an intermediate field I (so $\mathbb{Q} \subset I \subset E$) we can consider $\text{Gal}(E : I)$, the group of all automorphisms of E that fix I. We call this group the *fixer* of I.
- These match up exactly! We could prove: If H is the fixer of I, then I is the fixed field of H, and if I is the fixed field of H, then H is the fixer of I.
- And it gets even better. Suppose that I is not just an intermediate field, but is itself a splitting field from some polynomial. In this case it makes sense to consider $\text{Gal}(I : \mathbb{Q})$ as well.
- These are automorphisms of I that fix $\mathbb{Q}$. Now technically none of these automorphisms belong to $\text{Gal}(E : \mathbb{Q})$, but they are related. By a homomorphism!
- Given an automorphism in $\text{Gal}(E : \mathbb{Q})$, consider its restriction to I. That is, simply restrict the domain to only include elements from I. It turns out that the function that takes a automorphism to its restriction is a homomorphism. And where there's a homomorphism, there is a kernel. These will be the automorphisms of $\text{Gal}(E : \mathbb{Q})$ which are the identity on I. That is, exactly the elements of $\text{Gal}(E : I)$.

- So by the Fundamental Homomorphism Theorem,

$$\mathrm{Gal}(I : \mathbb{Q}) \cong [\mathrm{Gal}(E : \mathbb{Q})]/[\mathrm{Gal}(E : I)]$$

In particular, we see that the fixer of a splitting field is a normal subgroup.

Show the Galois correspondence for the whole diagram of intermediate fields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{7})$ has Galois group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Consider the two subnormal series

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \supset \langle (1,0,0), (0,1,0) \rangle \supset \{(0,0,0)\}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \supset \langle (0,0,1) \rangle \supset \{(0,0,0)\}$$

What intermediate fields do these match up with?

Let's try to understand why there is nothing like the quadratic formula for polynomials in general. Specifically, there is no quintic (or higher) formula.

- What do we mean by something like the quadratic formula? We mean solvability by radicals. That is, is there some way to express the roots of a polynomial in terms of field operations and nth roots?
- This question can be framed in the language of extension fields. Remember, we know that every polynomial has roots in some extension field. Asking what the roots look like is asking what the extension field looks like.
- In particular, we need to see if the roots lie in a field extension obtained by taking nth roots of elements in lower fields.
- We say that an extension E of a field F is an *extension by radicals* if there is a chain of subfields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = E$$

such that for $i = 1, 2, \ldots, 3$ we have $F_i = F_{k-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$.

- Then a polynomial $f(x)$ is *solvable by radicals* over F if the splitting field K of $f(x)$ over F is contained in an extension of F by radicals.
- An easy example of a polynomial that is solvable by radicals is $x^n - a$ (for any $a \in \mathbb{Q}$). We can say exactly what the roots look like. Let ω be a primitive nth root of unity (what does this mean?), so the roots are $\sqrt[n]{a}\omega^k$ for $k \in \{0, 1, \ldots, n-1\}$.
- We wish to make a connection to groups. We do so using Galois theory. Let the splitting field for $x^n - a$ over $\mathbb{Q}$ be E. What does $\mathrm{Gal}(E : \mathbb{Q})$ look like?
- First extend $\mathbb{Q}$ by ω. We can check that $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q})$ is abelian, and thus solvable. Then extend again to get E (we know $E \supseteq \mathbb{Q}(\omega)$). We can argue that $\mathrm{Gal}(E : \mathbb{Q}(\omega))$ is also abelian, and thus solvable. Then put it together (look at the two series).
- What this says is that at least in this special case, since the polynomial is solvable by radicals, the splitting field's Galois group is solvable. This holds in general. Essentially, just repeat the process for each extension (putting in the primitive roots of unity as required).
- The converse happens to also be true. So a polynomial is solvable by radicals if and only if the Galois group of its splitting field is a solvable group.

- Now consider the polynomial $p(x) = x^5 - 6x^3 - 27x - 3$. This is irreducible by Eisenstein. Thus there are 5 distinct roots in some splitting field E.
- What do the roots look like? By either graphing or doing some calculus, we can verify that there are exactly three real roots (there are only two critical points). Thus there are exactly two complex roots.
- The automorphisms of the splitting field are determined by what they do to the five roots. So each automorphism can be viewed as an element of S_5.
- One automorphism is complex conjugation. This leaves the three real roots fixed, and permutes the other two. So in S_5, this is a transposition.
- We also know that $\text{Gal}(E : \mathbb{Q})$ has order that is a multiple of 5. We get this by considering the tower of extensions of $\mathbb{Q}$ in E: the first extension must be of degree 5, so the degree $[E : \mathbb{Q}]$ is a multiple of 5, and this is the same as the order of $\text{Gal}(E : \mathbb{Q})$. By Cauchy's theorem, $\text{Gal}(E : \mathbb{Q})$ must have an element of order 5. In S_5 this is necessarily a 5-cycle.
- So $\text{Gal}(E : \mathbb{Q})$ is a subgroup of S_5 that contains a 2-cycle and a 5-cycle. We can show that this means that $\text{Gal}(E : \mathbb{Q}) \cong S_5$. In fact, S_5 is generated by any 2-cycle and any 5-cycle.
- Now consider the composition series for S_5:

  $$S_5 \supset A_5 \supset \{0\}$$

  Since A_5 is simple, we get that S_5 is not solvable. And this means that $p(x)$ is not solvable by radicals. Ta Daa.

Friday: Project work

Today you have the option of working with your group on your final project, either in class or from home.

Week 10: March 23-27

No class on Monday, March 23.

Wednesday: Powers mod powers

Start with the activity. That is, what is the remainder when you divide a^p by p?

- This will depend on a and p. But if p is prime, we should realize that $a^p \equiv p \pmod{p}$.
- Another way to say this is that $a^{p-1} \equiv 1 \pmod{p}$.
- What if p isn't prime? Is there a power of all a which is equivruent to 1 mod p? That is, for a given number n, will there be some m such that $a^m \equiv 1 \pmod{n}$ (no matter what a is)? We will come back to this later.
- Returning to the p prime case: Why might this be true? Let's use group theory.
- Which group should we look at if we are taking powers and working mod p? Yup, $\mathbb{Z}_p^* = U(p)$.
- Asking what power of an element gives us 1 is asking for the **order** of the element. That is, how many times do you need to "multiply" an element by itself to get the identity?
- In $U(7)$, find the order of each element. Note that different elements might have different orders. But what do you notice about all the orders?
- In any group G, for any $g \in G$, we know that the order of g is a divisor of the *order* of G (the number of elements in G).
- This is a consequence of Lagrange's theorem. If you look at the powers of g, you will get the cyclic subgroup $\langle g \rangle$, which will have exactly as many elements as the order of g. But Lagrange's theorem says that the order of a subgroup must divide the order of a group.
- So that means that whatever the order of a is in $U(p)$, it must divide the size of $U(p)$, which is $p-1$.
- But further, if $a^t = e$, then $a^{kt} = e$ as well. So $a^{p-1} = 1$ in $U(p)$ (since $p-1$ is a multiple of the order of each element).

Friday: More order and Euler's Theorem

Last time we considered what powers of numbers are equivalent to 1 mod particular numbers. We conjectured that if p is prime, then for any $a < p$ we have $a^{p-1} \equiv 1 \pmod{p}$. This led to a discussion of the order of elements. Here is a summary of what we have so far:

- For any finite group G and any element $g \in G$, we say the **order** of g is the least k such that $a^k = e$ (the identity).
- We also noted that if $\text{ord}(g) = k$ then $g, g^2, g^3, \ldots, g^k$ are distinct elements. Why is this?
- Suppose $g^a = g^b$ with $1 \leqslant a < b < k$. Then $g^{a-a} = g^{b-a}$, but $g^{a-a} = e$. So that would mean that $g^{b-a} = e$. This is impossible since $b-a$ is less than k, and k was the least positive power of g that gives the identity.
- Since there are k distinct powers of g, we have that the cyclic subgroup generated by g, that is, $\langle g \rangle$ contains exactly k elements.

- That is, the order of the element g is equal to the order of the cyclic subgroup generated by g.
- But Lagrange's theorem tells us that the order of a subgroup must divide the order of the group.
- Thus the order of any element $g \in G$ must divide the order of G.

Now let's continue where we left off.

- Suppose $\text{ord}(g) = k$. What is g^{nk} for any n?
- We have $g^{nk} = (g^k)^n = e^n = e$.
- That is, if m is a multiple of $\text{ord}(g)$, then $g^m = e$. Since the $|G|$ is a multiple of $\text{ord}(g)$, we have $g^{|G|} = e$.
- Is the converse true? That is, if $g^m = e$ does that mean that m is a multiple of $\text{ord}(g)$? Yes! Homework!
- Now consider the group $U(p)$ where p is prime. This is the group of *units* mod p, which means $\{1, 2, 3, \ldots, p-1\}$ (which is a consequence of Bezout's lemma).
- Thus in $U(p)$ we have $g^{p-1} = 1$ for all $g \in U(p)$.
- Therefore $a^{p-1} \equiv 1 \pmod{p}$. This result is called *Fermat's Little Theorem*.

Now what about the non-prime case? Given n, is there a number m such that $a^m \equiv 1 \pmod{n}$ for all a?

- The answer is no, since if a and n have a common factor, then no power of a will be 1 mod n.
- Working in groups again, we can consider $U(n)$. The elements of this group are precisely the *units* of Z_n, which means those elements relatively prime to n.
- We will let $\varphi(n)$ denote the *number* of numbers less than n that are relatively prime to n. This is called the **Euler φ function**.
- Then repeating the same argument as we did for Fermat's Little Theorem, we get that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for any a relatively prime to n. This is known as Euler's Theorem.

For Euler's theorem to be useful, we need to understand how the φ function behaves.

- We know that $\varphi(p) = p - 1$ for any prime p. We also will define $\varphi(1) = 1$ (because it will be useful to do so).
- The definition of $\varphi(n)$ is: the number of positive integers less than n that are relatively prime to n. Find $\varphi(n)$ by brute force for some non-prime values of n.
- In particular, find $\varphi(6)$, $\varphi(10)$, $\varphi(14)$, $\varphi(15)$, and $\varphi(21)$. Note that each of these is the product of two primes.
- $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(8) =$

Week 11: March 30 - April 3
Monday: RSA Cryptography

Here is the idea: we want to publicly publish an encryption key that can be used to encode data, that cannot be decrypted unless you know the private decryption key.

- How do we encode the message? First, suppose you have some standard method to make the message into a number (or sequence of numbers). Call such a number x.
- Now we want to transform x into a encrypted number y. We do this by computing $x^E \pmod n$ for some numbers E and n. Then y can be sent.
- For this to work, we need a way to transform y back into x. We will do this by computing $y^D \pmod n$. This would only be secure if D was completely private (so we better not be able to find D from E and n). It would only work if this really did give x back.
- So we want $(x^E)^D \cong x \pmod n$. How can we make sure this happens?
- What if $DE = \varphi(n) + 1$? Or even $DE = k\varphi(n) + 1$? Well, if it happens that x is relatively prime to n, we would have

$$(x^E)^D = x^{DE} = x^{k\varphi(n)}x \equiv 1^k x \pmod n$$

- If x is not relatively prime to n, then we will also be okay, because of how we will pick n.
  - We will have $n = pq$ for primes p and q. Say x is a multiple of p (but not of q).
  - So $x = rp$ for some $r < q$. Then

$$x^{km} = x^{k\varphi(pq)} = (x^{\varphi}(q))^{k\varphi(p)} \equiv 1 \pmod q$$

  - This means that $x^{k\varphi(pq)} = 1 + tq$ for some t. We get

$$(x^E)^D = x^{k\varphi(pq)}x = (1 + tq)x = x + tq(rp) = x + trn \equiv x \pmod n$$

- Great. So we want $DE = k\varphi(n) + 1$ which is the same as saying $DE \equiv 1 \pmod{\varphi(n)}$.
- We also want $n = pq$, so $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. Use $m = \varphi(n)$.
- So here is what we want to do:
  - Pick two really big prime number p and q; find $n = pq$ and $m = (p-1)(q-1)$ (these are easy if we start with p and q).
  - Find a number E that is relatively prime to m. Just guess and check until you find something.
  - Find D such that $DE \equiv 1 \pmod m$. You can do this using the Euclidean algorithm. You will be successful because $\gcd(E, m) = 1$
  - Don't tell anyone what p, q, m or D are. Tell everyone what n and E are.
  - Note: we want E to be fairly large. Taking $E = 2$ would always work, but then you could undo the encryption by searching for a square root perhaps. Other considerations are whether it is efficient to compute x^E, which is easier if in binary E doesn't have too many 1's.
- Work through an example with small primes. Have a student write down their favorite number x (in secret) and then compute $x^E \pmod n$ (in secret). Then as a class, decrypt the result.

- One concern is how to compute the power mod n in any sort of reasonable way. We can use the method of repeated squares:
  - First, write E as a sum of powers of 2 (like the Egyptians would).
  - So now we just need to compute $x^{2^{k_1}+2^{k_2}+\cdots+2^{k_n}}$. This becomes a product of terms for the form x^{2^k} for different k.
  - Notice though that $x^{2^k} = (x^2)^{2^{k-1}}$. In other words, we can keep squaring x, k times.
  - This doesn't seem to help, except that we can reduce mod n at each step. So as long as we can square a number less than n, we are good.

Wednesday: RSA Lab

Today we did the RSA Cryptography "lab" activity.

Friday: Direct Products

Today we will work through the Direct Products activity.

Week 12: April 6-10
Monday: Fundamental Theorem of Finite Abelian Groups

The goal today is to understand how to classify all finite abelian groups.

- Some abelian groups are cyclic. And if they are, we know exactly what they look like. They are isomorphic to $\mathbb{Z}_n$ for some n (and this happens precisely when there is an element of order n in the group).
- But not all abelian groups are cyclic. In fact, even $\mathbb{Z}_2 \times \mathbb{Z}_2$ is an example of this. So what does an abelian group look like in general?
- Note that if a group is not cyclic, then it is not generated by a single element. But it will be generated by some number of elements. There are groups that are *finitely generated* and others that are not (require an infinite set of generators). Of course finite groups are finitely generated.
- If g_1, g_2, ...g_n is a set of generators, that means that every element of the group can be written as a product of powers of these elements. If the group is abelian, then we can say each element $g \in G$ is $g = g_1^{k_1} g_2^{k_2} \dots g_n^{k_n}$. Some of the k_i might be negative or zero.
- Now the powers of g_1 are exactly the elements of the cyclic subgroup $\langle g_1 \rangle$, and similarly for all g_i. So this says that $G = \langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_n \rangle$. So perhaps you would think that G could be written as an *internal* direct product of cyclic groups.
- To make sure that were true, we would also need $\langle a_i \rangle \cap \langle a_j \rangle = \{e\}$ (the other requirement, that the subgroups are normal, we get for free since we are in an abelian group).
- This will not always be true. In $\mathbb{Z}_{12}$, if we picked $a_1 = 3$ and $a_2 = 6$, then we are done for.
- So we must pick the generators carefully. We pick them based on what their orders are.
- Given any abelian group G, let $G(p)$ be the set of all elements whose orders are a power of p. For prime p, we call such groups *p-groups*. Our first step is to break G down as the direct product of p-groups.
- Specifically, say $|G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$. We can show that G is the internal direct product of $G(p_1)$, $G(p_2)$,...$G(p_n)$.
- It is easy to verify that $G(p_i)$ is really a subgroup. Thus we must only argue that $G(p_i) \cap G(p_j) = \{e\}$ for all $i \neq j$ and that $G = G(p_1)G(p_2) \cdots G(p_n)$.
- The first is obvious, since the only power of one prime equal to a power of another prime is 1, the order of the identity.
- The other must be true because we know that the product of these subgroups is at very least a subgroup of G, but it must have the same size, and therefore be equal to G.
- So now we have the G is a direct product of p-groups. These p-groups might or might not be cyclic (consider the two examples we had on the activity from last time).
- We need to understand the structure of p-groups. It would be nice to pick generators so that the p-group could be expressed as the direct product of cyclic groups (all of which will also be p-groups).

- Again, do so by considering the order of elements. Say we have a p-group G_p. Let g be any one of the elements in G_p of maximal order. So $\text{ord}(g) = p^m$ for some m. We will show that $G_p = \langle g \rangle \times H$ for some subgroup H of G_p.
- This will be enough, because then we can proceed by induction to break down H (also a p-group, but of smaller order) similarly. Eventually we will be left with a second group that is cyclic (or trivial).
- Here is the basic idea. The proof is by induction. We take g to be of largest order in G_p. Let h be of smallest order of all elements not in $\langle g \rangle$. Then shift to the quotient group $G/\langle h \rangle$ and look at the element $\langle h \rangle g$. Argue that this has maximal order in $G/\langle h \rangle$ and by induction conclude that $G/\langle h \rangle \cong \langle \langle h \rangle g \rangle \times H/\langle h \rangle$ for some subgroup H of G containing $\langle h \rangle$. Then argue that this H makes $G_p \cong \langle g \rangle \times H$.
- The takeaway: The Fundamental Theorem of Finite Abelian groups tells us that any finite abelian group G is isomorphic to the direct product of cyclic groups, each of order a power of a prime. That is,
$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$$
(the p_i need not be distinct).
- As an example, let's classify all finite abelian groups of order $540 = 2^2 3^3 5$. One of these is $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5$. Another is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5$. Or we can break down the 3^3 in two different ways. All together there will be 6 groups with this order.

Friday: Application to Counting

Note: Wednesday was group project work day.

Let's end the year with an example of how understanding group structure can help solve problems in other areas of mathematics. Consider questions of combinatorics. In Discrete you learned a variety of methods for quickly counting the number of outcomes (this is also useful in probability of course).

How many ways are there for King Arthur and his 9 knights of the round table to sit around the round table? Why is the answer not just 10 factorial?

- One way to think about the above problem is to say that there are 10 seats, with 10 choices for who sits in the first, 9 choices for who sits in the second, and so on. But this is too many, since we just care who sits next to whom, not which chairs they sit in. So divide by 10 to account for the 10 different seating arrangements that should really count as one outcome.
- We have a similar way of correcting when we think of counting *combinations* instead of permutations.
- What about this problem: You want to put out place mats for Arthur and his knights. The mats come in two colors: blue and gold. How many ways can you arrange the place mats around the table?
- This is harder. We could start by saying there are 2^{10} arrangements (each spot has 2 choices). But how do we divide out by the duplicates?
- The problem is that the number of duplicates depends on the number of each color. For example, we have only counted 1 outcome where all the mats are gold. But we have counted 10 with 1 blue and 9 gold, and they are all "the same". We have counted 45 with 2 blue and 8 gold. How many of those should we have counted?

- This is getting complicated fast. It seems like while this way of dividing up the outcomes could work, it is certainly no easy task.
- So here is an alternative suggestion. Instead of creating cases based on how many of each color we have, break up the set of distributions by the type of duplication.
- For example, we wanted to group together the 1 blue/9 gold placements because each could be achieved by rotating the table from another. So maybe lets group together all placements that are equivalent under this symmetry.
- The advantage: we understand symmetries fairly well: they give us a group structure. Here, the group of all rotations of a 10-gon, which is a subgroup of D_{10}.
- To make this precise, we will talk about the group *acting* on the set of outcomes (colorings). So let's see what we can say about "group actions."

Week 13: April 13-17
Group Actions

- Consider a group G and a set X. An *action* of G on X is a function that sends pairs in $G \times X$ to things in X. We write $(g, x) \mapsto gx$, satisfying

  1. $ex = x$ for all $x \in X$
  2. $(g_1 g_2)x = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

  We call X a *G-set*.

- Two elements $x, y \in X$ are *G-equivalent* (written $x \sim y$) provided there is some $g \in G$ such that $gx = y$.

- The *orbit* of an element $x \in X$ (written $\mathcal{O}_x$) is the set of all elements $y \in X$ that are G-equivalent to x.

- The *fixed point set* of an element $g \in G$ (written X_g) is the set of all $x \in X$ such that $gx = x$.

- The *stabilizer subgroup* of an element $x \in X$ (written G_x) is the set of all $g \in G$ such that $gx = x$.

Do an example with D_4 acting on the vertices (or edges) of a square.

We would like to make some observations about how G, X, $\mathcal{O}_x$, G_x and X_g are related, in terms of sizes. We start with the *Orbit-Stabilizer Theorem*:

Let G be a finite group acting on a set X. Then for any $x \in X$,

$$|G| = |\mathcal{O}_x| \cdot |G_x|$$

Fix $x \in X$ and consider the elements of $\mathcal{O}_x$. These are the elements $y \in X$ such that $gx = y$ for some $g \in G$. But of course there might be more than one element in G which moves x to y. Say $g_1 x = y$ and $g_2 x = y$. Then $g_1 x = g_2 x$ so $g_2^{-1} g_1 x = x$. In other words, $g_2^{-1} g_1 \in G_x$.

Consider the cosets G/G_x (remember G_x is a subgroup of G, so this makes sense). Each coset has the form gG_x for some $g \in G$. But look at what we said above: $g_2^{-1} g_1 \in G_x$ precisely when g_1 and g_2 both move x to the same element in $\mathcal{O}_x$, and now we are saying that this happens exactly when g_1 and g_2 are in the same coset. So each different element of $\mathcal{O}_x$ corresponds exactly to a coset of G/G_x. In other words:

$$|\mathcal{O}_x| = |G/G_x| = [G : G_x] = |G|/|G_x|$$

where the last equality is by Lagrange's theorem.

Let the *fixed point set* of an element $g \in G$ (written X_g) be the set of all $x \in X$ such that $gx = x$. Note here we are indexing by elements from G, instead of from X (as in $\mathcal{O}_x$ or G_x).

Now we can prove Burnside's lemma:

Let k be the number of distinct orbits defined by the action of G on X. Then

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

In other words, the number of orbits is the average number of points fixed by the elements in G.

Let's count $\sum_{g \in G} |X_g|$. This counts all the pairs (g, x) such that g fixes x. What if we break this down by x instead of g. We get

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$$

Now break it down even further: divide up the sum by orbits. For any single orbit $\mathcal{O}_x$ we want to find $\sum_{y\in\mathcal{O}_x} |G_y|$. But if x and y are in the same orbit, then $|G_x| = |G_y|$[1] so

$$\sum_{y\in\mathcal{O}_x} |G_y| = |\mathcal{O}_x| \cdot |G_x| = |G|$$

If we do this for all k orbits, we get

$$\sum_{x\in X} |G_x| = k \cdot |G|$$

but the left hand side is really $\sum_{g\in G} |X_g|$, as we need.

Here are some examples.

How many place mat placements are possible around Arthur's 10 seat round table using blue and gold place mats? We count the number of orbits of elements in X under a group action of G. What are X and G? Let X be the set of all "colorings" (place mat placements) and let G be the group of rotations of a 10-gon (a subgroup of D_{10}). We need to find $|X_g|$ for each element $g \in G$ and then average them. How many colorings are fixed by the identity? All of them. What about by a rotation by 36 degrees? Just 2. Same for rotations by 3, 7, 9. Other rotations? We get:

$$\frac{1}{|G|}\sum_{g\in G} |X_g| = \frac{1}{10}(2^{10} + 4\cdot 2^1 + 4\cdot 2^2 + 2^5) = 108$$

How many 6-bead bracelets can you make using 3 colors of beads? Note we need all of D_6 here.

$$\frac{1}{|G|}\sum_{g\in G} |X_g| = \frac{1}{12}(3^6 + 2\cdot 3^1 + 2\cdot 3^2 + 3^3 + 3\cdot 3^4 + 3\cdot 3^3 = 92$$

How many ways can you color the faces of a cube using 4 colors? We need to decide on the group of symmetries of a cube. This will be homework.

[1] How do we know this? Define $\varphi : G_x \to G_y$ by $\varphi(a) = gag^{-1}$ where g is the element which gives $gx = y$. You can show that $gag^{-1}y = y$. This is a isomorphism.