Contents

1 Lecture 1

Primary Goal. To the study the foundations of arithmetic—Operations: addition, subtraction. Rules of computation; High school (easy); Numbers!

First issue: what are numbers?

1. quantity;
2. they form a set satisfying some axioms. → structure

   We want the mathematical theory to apply to as many different number systems as possible. Building this theory was hard but dead people did this for us so nice.

3. Want: ordering? Consider $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Or quaternions. Or octonions. Or p-adic numbers. Vectors. Algebraic. Transcendental. Surreal.

   What do these things all have in common that we can use to build our theory?

   Essential commonality: arithmetic operations ($+$ and $\cdot$). Ex: associative law. $(a+b)+c = a+(b+c)$. Similarly for multiplication.

   The associative law is the hardest one to implement.

   Ex: the commutativity law: $a+b=b+a$.
   Ex: the distributive law: $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$.

Definition 1.1. A **semiring** is a set R with two operations: $(+)\colon R\times R\to R$, addition, and $(\cdot)\colon R\times R\to R$, multiplication, such that the following axioms hold:

1. (Associativity) $\forall a,b,c\in R$,

$$(a+b)+c = c+(b+c),$$
$$\text{and } (a\cdot b)\cdot c = a\cdot(b\cdot c).$$

2. (Identities).
   (a) There exists $0\in R$ s.t. $\forall a\in R, a+0=0+a=a$.
   (b) There exists $1\in R$ such that $\forall a\in R, a\cdot 1 = 1\cdot a = a$.
3. (+ commutes), $\forall a,b,\in R$, $a+b=b+a$.
4. (Distributive property) $\forall a,b,c\in R$

$$a\cdot(b+c) = (a\cdot b)+(a\cdot c)$$
$$(a+b)\cdot c = (a\cdot c)+(b\cdot c).$$

This is the most important because it's the only one the says how the two operations talk to each other.

Definition 1.2. A **ring** is a semiring that satisfies the following:

5. (Additive inverses), $\forall a \in R$, $\exists b \in R$ such that $a + b = b + a = 0$. We write $-a := b$.

Definition 1.3. A **commutative ring** is a ring satisfying commutativity for multiplication:

6. ($\cdot$ commutes) $\forall a, b \in R$, $a \cdot b = b \cdot a$.

Examples 1.4.

1. The most fundamental semiring is the natural numbers, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
   Not a ring because no inverse.

2. The integers, $\mathbb{Z}$, is the most fundamental ring. $\mathbb{Z} := \{m + (-1)n \mid m, n \in \mathbb{N}\}$.

   $$m_1 + (-1)n_1 = m_2 = (-1)n_2 \in \mathbb{Z}$$

   exactly when

   $$m_1 + n_2 = m_2 + n_1 \in \mathbb{N}.$$

3. The rationals, $\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\}$.

   $$m_1/n_1 + m_2/n_2 := (m_1n_2 + m_2n_1)/n_1n_2,$$

   multiplication similarly defined.

   $$m_1/n_1 = m_2/n_2 \in \mathbb{Q} \Leftrightarrow m_1n_2 = m_2n_1 \in \mathbb{Z}.$$

   They form a field.

   Definition 1.5. A **field** F is a commutative ring such that $\forall a \neq 0 \in F$, there exists a $b \in F$ such that $a \cdot b = b \cdot a = 1$. Also, a is called a **unit** in F.

4. The reals, $\mathbb{R}$.

5. The complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$.

   $$a_1 + b_1i = a_2 + b_2i \in \mathbb{C} \Leftrightarrow a_1 = a_2, b_1 = b_2 \in \mathbb{R}.$$

   We also have

   $$(a_1 + b_1i) + (a_2 + b_2i) := (a_1 + a_2) + (b_1 + b_2),$$

   and

   $$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i.$$

2 Lecture 2

Review what we did last time: introduction to rings. What's the purpose of algebra, natural numbers, etc.

Examples 2.1.

6. The **Guassian integers** $\mathbb{Z}[i] = \{m + ni \mid n, n \in \mathbb{Z}, i^2 = -1\} \subseteq \mathbb{C}$. This is a classic example of a subring.

   Definition 2.2. If R is a ring and $S \subseteq R$ is a subset, then we say S is a **subring** if

   - $0, 1 \in S$;
   - $S + S \subseteq S$ (Closed under addition);
   - $S \cdot S \subseteq S$ (Closed under multiplication);
   - $-S \subseteq S$.

7. (Hamilton) The **quaternions** $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1 = ijk, ij = -ji\}$. This is not a commutative ring because of the last identity.

   One incredible property is that for all $a \neq 0 \in \mathbb{H}$, a is a unit. $\mathbb{H}$ is like a "non-commutative field". Actually called a **division ring**.

Let's talk about a few ways to make new rings out of old rings we have.

2.1 Construction of Rings

Let R be a commutative ring. The **polynomial ring** $R[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_dx^d \mid a_i \in R\}$.

Let R, S be rings. The **Cartesian product** $R \times S$[1] is a ring. It's not as useful for rings as it is for groups.

Let R be a ring and X a set. $R^X = \{f \colon X \to R\}$,

$$(f + g)(x) := f(x) = g(x)$$
$$(f \cdot g)(x) := f(x) \cdot g(x),$$

is a ring.

2.2 Morphisms

Whenever you make a new object you then want to study the function between objects that preserve structure (morphisms).

Definition 2.3. A function $\varphi \colon R \to S$ between rings is called a **ring homomorphism** or simply a **morphism**, if $\forall a, b \in R$,

1. $\varphi(1) = 1$;
2. $\varphi(a + b) = \varphi(a) + \varphi(b)$; and
3. $\varphi(ab) = \varphi(a)\varphi(b)$.

[1] addition and multiplication done component-wise.

The first property is not always required in some texts.

If φ is invertible as a function then we say φ is an **isomorphism** and we say R and S are isomorphic, $R \cong S$.

Isomorphic rings are essentially the same.

Example 2.4. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ naturally sit inside of each other. Natural inclusions are ring homomorphisms. We also have $Z \subseteq \mathbb{Z}[i] \subseteq \mathbb{C}$.

Example 2.5. $\varepsilon_7 \colon \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(7)$ (surjective ring homomorphism).

Broadly speaking we're trying to understand rings up to isomorphism. Certainly can't do that for all rings, but at the least the ones we care about we'd like to understand. And their ring homomorphisms!

2.3 Quotients

This is a more interesting way of constructing a new ring from an old ring.

Example 2.6. $R := \{f(x) \in \mathbb{Z}[x] \mid x^2 = -1\}$. Start with something we know and impose a relation.

We'll give a more formal definition in a bit.

Consider $3 + 5x + 2x^2 - x^3 = 3 + 5x + 2(-1) - (-1)x = 1 + 6x$.

We can write $R = \{m + nx \mid x^2 = -1\}$. In fact, $R \cong \mathbb{Z}[i]$. How would we prove this? By definition $\rho \colon \mathbb{Z}[x] \to R$. Question becomes: when $\rho(f(x)) = \rho(g(x))$? $\rho(f(x) - g(x)) = \rho(f(x)) - \rho(g(x)) = 0$. So it suffices to study $\rho(f(x)) = 0$.

Definition 2.7. If $\varphi \colon R \to S$ is a morphism, then the **kernel** of φ is $\ker \varphi := \varphi^{-1}(0)$.

Proposition 2.8. *Let $\varphi \colon R \to S$ be a morphism. Then,*

1. $a, b \in \ker \varphi$ *then* $a + b \in \ker \varphi$*;*

2. *if* $a \in \ker \varphi$*,* $b \in R$*, then* $ab \in \ker \varphi$*;*

3. $0 \in \ker \varphi$*,* $-a \in \ker \varphi$ *whenever* $a \in \ker \varphi$*. (Check the details).*

This will motivate the notion of an *ideal.*

3 Lecture 3

Goal: make rigorous and systematic the idea of "imposing relations on a ring." E.g., $S \approx \{f(x) \in \mathbb{Z}[x] \mid x^2 = -1\}$. The elements of the rings should be equivalence classes of polynomial coefficients for all things that we can prove are equal using this identity and ring axioms. But how do we formalize this notion of all ring-theoretic consequences?

Want: $\rho \colon \mathbb{Z}[x] \to S$, $f(x) \mapsto$ equiv. class to be a surjective ring homomorphism. Last time we looked at the kernel because $\varphi(a) = \varphi(b)$ iff $\varphi(a - b) = 0$ so $a - b \in \ker \varphi$.

Proof of prop 2.8.

1. If $a, b \in \ker \varphi$ then $\varphi(a + b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$. So $a + b \in \ker \varphi$;

2. if $a \in \ker\varphi, b \in R$ then $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot \varphi(b) = 0$. So $ab \in \ker\varphi$; and

3. if $a \in \ker\varphi$, $\varphi(-a) = -\varphi(a) = -0 = 0$. So $-a \in \ker\varphi$. □

Question: if we just know R and some stuff that should belong to the kernel, can we reconstruct $\rho\colon R \to S$ and S? The answer will be yes!

So how do we define a kernel without having a homomorphism?

Definition 3.1. A subset $J \subseteq R$ of a commutative ring R is called an **ideal** if

1. $J + J \subseteq J$;
2. $R \cdot J \subseteq J$;
3. $-J \subseteq J$.

The proposition implies that $\ker\varphi$ is an ideal.

Ideal comes from the idea of an idealized number, whose notion came about before it was made rigorous by Dedekind.

Theorem 3.2 (/Definition)**.** *Let R be a commutative ring and let $J \subseteq R$ be an ideal in R. If $a \in R$, then $a + J := \{a + j \mid j \in J\} \subseteq R$ is called a **coset**. Let $R/J := \{a + J \mid a \in R\}$.*

1. *If $a, b \in R$ then $a + J = b + J$ iff $a - b \in J$;*
2. *the operations:*
$$(a + J) + (b + J) := (a + b) + J$$
$$(a + J) \cdot (b + J) := (a \cdot b) + J,$$
are well defined;
3. *R/J is a commutative ring with respect to these operations. And the additive identity is $0 + J = J$. The multiplicative identity is $1 + J$.*
4. *The function $\rho_J\colon R \to R/J$, $a \mapsto a + J$ is a surjective ring homomorphism. And $\ker\rho_J = J$.*

Proof.

1. The forward direction is pretty easy. Suppose $a+J = b+J$. We have $a+0 \in a+J = a = b+j$ for some $j \in J$. Then $a = b = j \in J$.

   For the other direction suppose $j := a - b \in J$. Then $a = b + j$. Say $a + j' \in a + J$. So $b + j + j' = b + (j + j') \in b + J$ (because it's closed by definition). Therefore, $a + J \subseteq b + J$. Likewise, $b = a - j = a + (-j)$, which gives us $b + J \subseteq a + J$ by symmetry. Thus, $a + J = b + J$ and we've proven the reverse direction.

2. Claim that it suffices to show that if $a_1 + J = a_2 + J$, a_1, a_2 representatives, then
   (a) $(a_1 + J) + (b + J) = (a_2 + J) + (b + J)$;
   (b) $(a_1 + J) \cdot (b + J) = (a_2 + J) \cdot (b + J)$.

[Check why this claim is sufficient]

For (a), we have $(a_1 + J) + (b + J) = (a_1 + b) + J$ and $(a_2 + J) + (b + J) = (a_2 + b) + J$. Well, $(a_1 + b) - (a_2 + b) = a_1 - a_2 \in J$ by assumption.

For (b) we have $(a_1 + J)(b + J) = (a_1 b) + J$ and $(a_2 + J)(b + J) = (a_2 b) + J$. $a_1 b - a_2 b = (a_1 - a_2)b \in J$ (property 2 of an ideal).

3. This one is a bunch of verification. All of these properties are going to follow because similar properties hold for R. We're just going to look at one property here for brevity: distributive property.

$$\begin{aligned}(a + J)((b + J) + (c + J)) &= (a + J)((b + c) + J) \\ &= a(b + c) + J \\ &= ((ab) + (ac)) + J \\ &= (ab + J) + (ac + J) \\ &= (a + J)(b + J) + (a + J)(c + J).\end{aligned}$$

4. Our function respects addition: $\rho_J(a + b) = (a + b) + J = (a + J) + (b + J) = \rho_J(a) + \rho_J(b)$. We have $a + J = \rho_J(a)$ so ρ_J is surjective. $\rho_J^{-1}(0 + J) = J$. Therefore, $\ker \rho_J = J$. □

Corollary 3.3. *Every ideal $J \subseteq R$ is a kernel of some ring homomorphism.*

Proof. From the previous theorem, $\rho_J \colon R \to R/J$ has $\ker \rho_J = J$. □

Definition 3.4. If R is a commutative ring and $b \in R$ then the **principal ideal** generated by b is $\langle b \rangle := \{ab \mid a \in R\}$.

This is "all ring theoretical consequences of setting $b = 0$." Then in $\mathbb{Z}[x]$ we have $(x^2 + 1) =: J$. Now we have $\rho \colon \mathbb{Z}[x] \to \mathbb{Z}[x]/(x^2 + 1)$. We claim this was the exact ring we were trying to construct.

Example 3.5. $(2 + 3x + 5x^2 + x^3) + J = (-3 + 2x) + J$. $5 + x + 5x^2 + x^3 = (5 + x)(x^2 + 1) \in J$. Replace x^2 with -1. We have $2 + 3x + 5(-1) + x(-1) = -3 + 2x$.

4 Lecture 4

Useful notation: $J \subseteq R$ ideal in a commutative ring. $\rho_J \colon R \to R/J$, $a \mapsto a + J$, and $a, b \in R$.

$a \equiv b \pmod{J}$ iff $a - b \in J$ iff $a + J = b + J$ iff $\rho_J(a) = \rho_J(b)$.

Example 4.1. Suppose $J = (5) \subseteq \mathbb{Z}$. Recall that $(5) := \{5m \mid m \in \mathbb{Z}\}$. So $3 \equiv 13 \pmod{5}$ because $3 - 13 \in (5)$ because $-10 = (-2) \cdot 5$.

Example 4.2. $J = (x^1 + 1) \subseteq \mathbb{Z}[x]$. So $x^2 \equiv -1 \pmod{x^2 + 1}$ and so

$$\begin{aligned}2 + 3x + 5x^2 + x^3 &\equiv 2 + 3x + 5(-1) + (-1)x \\ &\equiv -3 + 2x \pmod{x^2 + 1}.\end{aligned}$$

This next theorem is very important. We will be using it all the time.

Theorem 4.3 (Fundamental Isomorphism Theorem)**.** *Let R be a commutative ring and suppose $J \subseteq R$ is an ideal.*

1. *If $\varphi\colon R \to S$ is a morphism, and if $\ker\varphi \supseteq J$, then there exists a unique $\tilde{\varphi}_J\colon R/J \to S$ such that $\varphi = \tilde{\varphi}_J \circ \rho_J$.*[2]

2. *If $\varphi\colon R \to S$ is a surjective morphism then $\tilde{\varphi}_{\ker\varphi}\colon R/\ker\varphi \to S$ is an isomorphism.*

Proof.

1. $\tilde{\varphi}_J(a+J) := \varphi(a)$. We're defining the function in terms of a coset representative.

   $\tilde{\varphi}_J$ well-defined $a+J = b+J$. Want to show $\varphi(a) = \varphi(b)$. We have $a - b = j \in J$ and so $\varphi(a-b) = \varphi(j) = 0$ because $J \subseteq \ker(\varphi)$. So it's well-defined.

   Ring homomorphism Not going to show all the parts. E.g, $\tilde{\varphi}_J((a+J)\cdot(b+J)) = \tilde{\varphi}_J(a\cdot b + J) = \tilde{\varphi}_J(\rho_J(a\cdot b)) = \varphi(a\cdot b) = \varphi(a)\varphi(b) = \tilde{\varphi}_J(\rho_J(a)) \cdot \tilde{\varphi}_J(\rho_J(b)) = \tilde{\varphi}_J(a+J)\cdot\tilde{\varphi}_J(b+J)$.

2. We assume $\varphi\colon R \to S$ is surjective. It suffices to show $\tilde{\varphi}$ is a bijection. Surjectivity: If $s \in S$ then $s = \varphi(a)$ for some $a \in R$ (because φ surjective). So then $\varphi(a) = \tilde{\varphi}\circ\rho(a) = \tilde{\varphi}(a + \ker(\varphi))$. Thus, $\tilde{\varphi}$ is surjective. Injectivity is also pretty easy. There's a standard trick we're going to use here: prove the kernel is the trivial ideal. Want to show $\ker(\tilde{\varphi}) = (0)$ in $R/\ker(\varphi)$. But what is the zero element in this quotient? Exactly the elements of $\ker(\varphi)$. If $a + \ker(\varphi) \in \ker(\tilde{\varphi})$ then $0 = \tilde{\varphi}(a + \ker(\varphi)) = \tilde{\varphi}(\rho(a)) = \varphi(a)$ which implies $a \in \ker(\varphi)$. Therefore $a + \ker(\varphi) = (0)$ in $R/\ker(\varphi)$. Therefore $\tilde{\varphi}$ is injective. Thus, $\tilde{\varphi}$ is an isomorphism. □

The theorem says: quotient rings R/J are essentially the same thing as surjective morphisms $\varphi\colon R \to S$.

Fact 4.4. *If $\varphi\colon R \to S$ is any homomorphism, then $\varphi(R) \subseteq S$ is a subring of S.*

$$\begin{tikzcd}
R \arrow[rr, dash, "\varphi"] \arrow[dr, dash, "\varphi_2"'] & & S \\
& \varphi(R) \arrow[ur, dash, "\varphi_1"'] &
\end{tikzcd}$$

Example 4.5 (Constructing $\mathbb{C}$)**.** $\varepsilon_i\colon \mathbb{R}[x] \to \mathbb{C}$ defined by $\varepsilon_i(f(x)) := f(i)$. So ε_i is a surjective ring homomorphism. We claim that $\ker(\varepsilon_i) = (x^2+1)$. We have $\varepsilon_i(x^2+1) = i^2+1 = 0$. Therefore $x^2+1 \in \ker(\varepsilon_i)$ and therefore $(x^2+1) \subseteq \ker(\varepsilon_i)$.

For the other direction we use division with remainder. If $f(x) \in \ker(\varepsilon_i)$ then $f(x) = g(x)(x^2+1) + a + bx$, $a, b \in R$. By definition, $0 = f(i) = a + bi$ iff $a = b = 0$ (if $b \neq 0$, $i = -a/b \in R$).

Theorem 4.6. $\tilde{\varepsilon}\colon \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$[3]

[2] This could also be seen as a commutative diagram which is of course harder to make in LaTeX.

[3] put a tilde over the arrow to show it's an isomorphism.

5 Lecture 5

Next homework is out...

Many of our favorite rings are constructed as quotients of simpler rings. Our goal is to understand properties of R/J in terms of properties of R and properties of J.

Proposition 5.1. *Let $\varphi\colon R \to S$ be a surj. morphism. The function $\varphi^{-1}\colon \mathrm{Ideal}(S) \to \{J \subseteq R\colon \ker\varphi \subseteq J\}$ with $I \mapsto \varphi^{-1}(I)$ is a bijection.*

Corollary 5.2. *Let $\rho_J\colon R \to R/J$. $\rho_J^{-1}\colon \mathrm{Ideal}(R/J) \to \{I \subseteq R\colon J \subseteq I\}$ is a bijection.*

Proof of proposition. We want to say

1. $\varphi^{-1}(I)$ is an ideal. This is a very general property (applies to any ring morphism). We'll just show one property: closed under addition. $a, b \in \varphi^{-1}(I)$ so $\varphi(a), \varphi(b) \in I$. So $\varphi(a+b) = \varphi(a) + \varphi(b) \in I$. Therefore $a + b \in \varphi^{-1}(I)$.

2. $\ker(\varphi) \subseteq \varphi^{-1}(I)$. Take $a \in \ker\varphi$. $\varphi(a) = 0 \in I$. Therefore $a \in \varphi^{-1}(I)$.

3. Define $\varphi\colon \{J \subset R\colon \ker\varphi \subseteq J, J \text{ ideal}\} \to \mathrm{Ideal}(S)$ by $J \mapsto \varphi(J)$ (yes, we are shadowing our variable).

   (a) Closed under addition. For $a, b \in J$, $\varphi(a) + \varphi(b) = \varphi(a+b)$ with $a + b \in J$ tells us $\varphi(a+b) \in \varphi(J)$.

   (b) Closed under negatives. For $a \in J$, $-\varphi(a) = \varphi(-a) \in \varphi(J)$.

   (c) Closed under scalar multiplication. For $a \in J, s \in S$. Goal is to show $s \cdot \varphi(a) \in \varphi(J)$. Since φ is surjective $s = \varphi(r)$ for some $r \in R$. Then $s \cdot \varphi(a) = \varphi(r) \cdot \varphi(a) = \varphi(ra) \in \varphi(J)$ because $ra \in J$ since J is ideal.

4. For all $I \subseteq S$, $\varphi(\varphi^{-1}(I)) = I$ (think this through). For all $J \subseteq R$, want to show for $\ker(\varphi) \subseteq J$ we have $\varphi^{-1}\varphi(J) = J$.

   If $a \in J$ then $\varphi(a) \in \varphi(J) \iff a \in \varphi^{-1}(\varphi(J))$ by definition..

   If $a \in \varphi^{-1}(\varphi(J))$ then $\varphi(a) \in \varphi(J)$. There exists $b \in J$ such that $\varphi(a) = \varphi(b)$ and $\varphi(a-b) = 0$ so $a - b \in \ker(\varphi) \subseteq J$. Therefore $a = a - b + b \in J$ by J closed under addition.

   Therefore, φ^{-1} is a bijection.

□

The main difficulty of abstract algebra is that it's abstract. But the way we gain intuition is by looking at concrete examples.

Example 5.3. What are the ideals in $\mathbb{Z}/(6)$? The proposition tells us there's a connection between $\mathbb{Z}/(6)$ and the ideals contained in (6)?

$(1) \supseteq (2), (3) \supseteq (6)$. $(6) \subseteq (m)$ iff $m \mid 6$. That's because $\mathbb{Z}$ is a PID.

Ideals let us ignore units. Which in the case of the integers, means we just have to care about the positive integers. Technically $\mathbb{Z}/(6)$ is not a PID because it's not even an integer domain: $2 \cdot 3 \equiv 0 \pmod 6$.

We could also write it as $(1 \mod 6) \supseteq (2 \mod 6), (3 \mod 6) \supseteq (6 \mod 6) = (0)$ in $\mathbb{Z}/(6)$.

Corollary 5.4. *If $I \subseteq J$ ideals, $\tilde{\rho}_I \colon R/J \twoheadrightarrow R/I$ surjective morphism defined by $a \pmod{I} \mapsto a \pmod{J}$.*

So $\mathbb{Z}/(6) \twoheadrightarrow \mathbb{Z}/(2), \mathbb{Z}/(3) \twoheadrightarrow 0$.

Definition 5.5. A **proper ideal** $J \subseteq R$ is an ideal such that $J \neq R$.

Definition 5.6. A **prime ideal** $P \subseteq R$ is a proper ideal such that if $ab \in P$ then $a \in P$ or $b \in P$.

Definition 5.7. A **maximal ideal** $M \subseteq R$ is a proper ideal such that if $M \subseteq J \subseteq R$ then either $J = M$ or $J = R$.

Proposition 5.8. *Let $J \subseteq R$ be an ideal.*

1. *J is prime iff R/J is an integral domain.*
2. *J is maximal iff R/J is a field.*

Proof. Homework. □

Recall: a nonzero element $p \in R$ is called **prime** if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proposition 5.9. *$0 \neq p \in R$ is prime iff (p) is a prime ideal.*

Proof. If $ab \in (p)$ then $p \mid ab$. So $p \mid a$ or $p \mid b$ and therefore $a \in (p)$ or $b \in (p)$. The other direction left as an exercise (it's easy). □

6 Lecture 6

Recall the propositions from the previous lecture and that non-unit, $0 \neq p \in R$ is prime if $p|ab$ implies $p|a$ or $p|b$. But why is *this* the right definition of prime. We're used to prime meaning irreducible but that's not what's happening here.

Example 6.1. $\mathbb{Z}$. What are the primes in the integers? The prime numbers (positive and negative). From these primes we get $(2), (3), (5), \dots$ which are principal ideals by 5.9. The only *prime* ideal we're missing is (0) (because $\mathbb{Z}/(0) \cong \mathbb{Z}$). So $\mathbb{Z}/(p)$ is an integral domain. That is, if $ab = 0 \mod p$ then $a = 0$ or $b = 0$. How do we know these are all the prime ideals? Well we know all the ideals of the integers are principal (we proved this previously on the homework).

For example, $\mathbb{Z}/(6)$ is not prime because $2 \cdot 3 \equiv 0 \pmod{6}$ but $2, 3 \not\equiv 0 \pmod{6}$. We call 2 and 3 **zero divisors** of $\mathbb{Z}/(6)$.

Say $p \in \mathbb{Z}$ is prime. What ideals contain (p)? Since $\mathbb{Z}$ is a PID then $(p) \subseteq (m) \iff m \mid p$. So $m = \pm 1$ or $m = \pm p$ because in the integers every prime is irreducible. If $m = \pm 1$ then $(m) = R$ and otherwise $(m) = (p)$. So (p) is maximal.

This brings us to:

Theorem 6.2. *$\mathbb{Z}/(p)$, for p prime, is a field.*

Number theorists say $\mathbb{F}_p = \mathbb{Z}/(p)$. In CS they might call it $GF(p)$ (Galois field of p). You might also see $\mathbb{Z}_p$ but this is almost exclusively reserved for undergrad textbooks.[4]

With this theorem, now we can ask $5^{-1} \overset{?}{\equiv} x \pmod{11}$. Just brute-force the 10 numbers to try.

[4] It also means something totally different in higher-level math.

Theorem 6.3 (Fermat's Little Theorem)**.** *If $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$.*

In any ring the units form a group. Because $\mathbb{F}_p$ field, every nonzero element is a unit. There are p elements in the field of which $p-1$ are non-zero.

This is an application of Lagrange's Theorem.

There's another way we can compute multiplicative inverses using gcd's. If $a \neq 0 \pmod{p}$ then $\gcd(a,p) = 1$. Then use Bezout's theorem to get $b, c \in \mathbb{Z}$ such that $ab + cp = 1$. Reduce this modulo p so then $ab \equiv 1 \pmod{p}$. So $b \equiv \frac{1}{a} \pmod{p}$. This is probably more efficient than using Fermat's Little Theorem.

Theorem 6.4 (Chinese Remainder Theorem)**.** *R a commutative ring, $I, J \subseteq R$ ideals. We have a morphism $\rho\colon R \to R/I \times R/J$ defined by $a \mapsto (a \pmod{I}, a \pmod{J})$. What is $\ker \rho$? The intersection of I and J. Using the first part of the fundamental isomorphism theorem, we know that $\rho_{I\cap J}\colon R/(I \cap J) \to R/I \times R/J$. When is this surjective? If and only if ρ is surjective. Intuitively, if it's going to be surjective then I and J need to be somewhat independent.*

Suppose it is surjective. Then there exist a, b such that $a \equiv 0 \pmod{I}$ and $a \equiv 1 \pmod{J}$ and $b \equiv 1 \pmod{I}$ and $b \equiv 1 \pmod{J}$. This tells us that $\rho(a+b) = (1 \mod I, 1 \mod J) = \rho(1)$. So $c := a + b - 1 \in \ker(\rho) = I \cap J$. Then $a + (b - c) = 1$ and $a \in I, b \in J, c \in I \cap J$, so $b - c \in J$. Therefore $I + J = (1) = R$. What does this mean?[5] We interpret this as "I and J are coprime." The CRT says $\rho_{I\cap J}\colon R/(I \cap J) \to R/I \times R/J$ is an isomorphism iff $I + J = (1)$.

Proof. So it suffices to show $I + J = (1)$ implies ρ surjective. Then there exist $a \in I$, $b \in J$ such that $a + b = 1$. To show it's surjective take an arbitrary class in the RHS and construct an element that maps to it. The trick is we use a and b as "coordinate" functions. We claim that $ac + bd \mapsto (c \mod I, d \mod J)$.

What? □

7 Lecture 7

7.1 Chinese Remainder Theorem continued

Trevor fells bad about rushing the proof last time so we're giving it some TLC today.

Theorem 7.1 (Chinese Remainder Theorem Take 2)**.** *R is a commutative ring. Ideals $I, J \subseteq R$.*

1. *$\rho\colon R \to R/I \times R/J$ surjective iff $I + J = (1) = R$. We say that I and J are **coprime**.*

2. *$I + J = (1)$ iff $\tilde{\rho}\colon R/(I \cap J) \xrightarrow{\sim} R/I \times R/J$ is an isomorphism.*

Proof.

1. We showed the necessity last time. Now we need to show the sufficiency. By assumption we have $a, b \in I, J$ respectively such that $a + b = 1$. Then $a \equiv 0 \pmod{I}$ because $a \in I$ and $a \equiv 1 \pmod{J}$. For b we have the opposite.

   Suppose we have $y = (c \mod I, d \mod J)$. We claim that $x = ad + bc$ is the element that maps to the one before. Why does this work? Well consider that $x \equiv c \pmod{I}$ and $x \equiv d \pmod{J}$. We just showed $y = \rho(x)$ which is exactly surjectivity.

[5] If $m, n \in \mathbb{Z}$ then $(m) + (n) = (\gcd(m,n))$. So think of what we're doing as sort of a generalization of this property to just ideals.

2. Recall that $\ker(\rho) = I \cap J$ because that's what need ned to map to $0 = (0,0)$. Since ρ is surjective by part (1), the fundamental isomorphism theorem tells us that there exists $\tilde{\rho}\colon R/(I \cap J) \xrightarrow{\sim} R/I \times R/J$.

□

What does this theorem mean? Example time!

Example 7.2. Consider our favorite ring, $\mathbb{Z}$. Recall that $\mathbb{Z}$ is a PID and assume $(m) + (n) = (1)$. Then the CRT tells us $\mathbb{Z}/(m) \times \mathbb{Z}/(n) \cong \mathbb{Z}/((m) \cap (n)) \equiv \mathbb{Z}/(\mathrm{lcm}(m,n))$, the last part since $(m) \cap (n) = (\mathrm{lcm}(mn))$. In general , $(m) + (n) = (\gcd(m,n))$. So we know that $\gcd(m,n) = 1$. But we've proven the identity $\mathrm{lcm}(m,n)\gcd(m,n) = mn$. So $\mathrm{lcm}(m,n) = mn$. This is what the CRT says for the integers. It might be stated classically as: $\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$.

Notice the nice properties about intersection and sum of ideals in the integers. The *intuition* in general is that $I \cap J \approx \mathrm{lcm}(I,J)$ and $I + J \approx \gcd(I,J)$.

Question 7.3. Can you find an intger n such that $n \equiv 2 \pmod 5$ and $n \equiv 3 \pmod 7$.

Answer. Yes! Because 5 and 7 are coprime. Can we actually do it better than brute-forcing? Indeed we can. We use the part where we proved surjectivity in the proof of CRT. We want to find $a \in (5)$, $b \in (7)$, such that $a + b = 1$ and $5j + 7k = 1$. Start with the bigger number and divide by 7, getting a remainder: $7 = 1 \cdot 5 + 2$ and $5 = 2 \cdot 2 + 1$. Rearrange to $2 = -5 + 7$ and $1 = -2 \cdot 2 + 5$ which is equivalent to $1 = -2 \cdot (-5 + 7) + 5 = 3 \cdot 5 + -2 \cdot 7$. So $a = 15, b = -14$. So $n = 15 \cdot 3 + -14 \cdot 2 = 17$. Check that 17 is indeed the answer.

The CRT tells us that all solution have the form $17 + 35k$. □

Remark on the second homework: nearly everyone missed something about the degree of product of polynomials. The subtlety is that we need the product of leading coefficients to be nonzero. And this is because we're in a field and every field is an integral domain. This doesn't work when you're not in an integral domain!

That does it for quotients for now. (Thank god.)

7.2 Localization and Fractions

We love to divide. Fields let us divide. Rings don't necessarily. Big rip. Why do we need to divide so much? Because we need divison to solve linear equations, the most basic type of equation. For example, consider $ax + b = c$. We can move the b over and it'd be nice to divide by a but we can't always do that.

Question 7.4. Given a commutative ring R, is there a ring $S \supseteq R$ in which every element of R has an inverse?

Example 7.5. $\mathbb{Z} \subseteq \mathbb{Q}$ would be an affirmative answer to the question above. But we can't inverse 0 still. Can we make it even bigger to divide by zero? Let's try it. Suppose $1 = 0/0 = 0 \cdot \frac{1}{0} = 0$, which means we're in the trivial ring. No killing the ring! So $\mathbb{Q}$ is the best we can hope for.

Recall how we construct the rationals. $\mathbb{Q} = \{mn \mid m, n \in \mathbb{Z}, n \neq 0\}/\sim$ where $m_1/n_1 \sim m_2/n_2$ iff $m_1 n_2 = m_2 n_1$. We of course also need to define the operations but I don't want to type that up.[6]

[6] I might've screwed up this notation for equivalence classes. Question though: are equivalence class constructions also a quotient ring or is the notion just similar?

8 Lecture 8

I missed it.

9 Lecture 9

Theorem 9.1 (Localization)**.** *Let $M \subseteq R$ be multiplicative.*

1. *The function $i_M \colon R \to M^{-1}R$ defined by $a \mapsto a/1$, is a ring homomorphism and $i_{M^{-1}}$ is injective iff M contains no zero divisors.*

2. *If $\varphi \colon R \to S$ is a morphism such that $\varphi(M) \subseteq S^\times$ then there exists a unique $\varphi_{M^{-1}} \colon M^{-1}R \to S$ such that $\varphi = \varphi_{M^{-1}} \circ i_{M^{-1}}$.*

We finished the proof of the first part last time. So we're just going to do the second part.

Proof of the second part. Let's just do the fun part. We want to first show uniqueness. So we suppose existence. The first observation is that if $a \in$ then $\varphi(a) = \varphi_{M^{-1}}(i_{M^{-1}}(a)) = \varphi_{M^{-1}}(a/1)$. The second observation is that if $m \in M$ then $1 = m/m = \frac{m}{1} \cdot \frac{1}{m}$ in $M^{-1}R$. Apply $\varphi_{M^{-1}}$ to both sides. So we have $1 = \varphi(m)\varphi_{M^{-1}}(1/m)$. We can solve this in S since we know that $\varphi(m)$ has an inverse by assumption. So $\varphi(m)^{-1} = \varphi_{M^{-1}}(1/m)$. Then $\varphi_{M^{-1}}(a/m) = \varphi_{M^{-1}}(a/1) \cdot \varphi_{M^{-1}}(1/m) = \varphi(a)\varphi(m)^{-1}$.

Existence: define $\varphi_{M^{-1}}(a/m) = \varphi(a)\varphi(m)^{-1}$. We can only make this definition because we assume $\varphi(m)$ is a unit. We have to show this function is well-defined. The issue is that we're working on equivalence classes. Suppose we have $a/m = b/n$ in $M^{-1}R$. Then there exists $c \in M$ such that $c(an - bm) = 0$. So we apply φ: $\varphi(c)(\varphi(a)\varphi(n) - \varphi(b)\varphi(m)) = 0$ in S. So $\varphi(c)$ is a unit. We can divide it out and it's gone. $\varphi(a)\varphi(n) = \varphi(b)\varphi(m)$. We also know $\varphi(n), \varphi(m)$ are unit because they're in the multiplicative set. So we can divide them out to get $\varphi_{M^{-1}}(a/m) = \varphi(a)\varphi(m)^{-1} = \varphi(b)\varphi(n)^{-1} = \varphi_{M^{-1}}(b/n)$.

Should be easy to prove it's a ring homomorphism. □

This theorem tells us the nice properties of this localization construction. We were trying to figure out when we could add fractions to a ring. This tells us as long as we avoid zero-divisors we're ok.

If R is an intregral domain then $M_{\text{TOT}} = R \setminus \{0\}$. $\text{Frac}(R) := M_{\text{TOT}}^{-1}R$ is the **field of fractions of** R. (It is a field and $R \to \text{Frac}(R)$ and $a \mapsto a/1$.)

Now we can divide. Nice.

Example 9.2. Our favorite integral domain: $\mathbb{Z}$. What is the field of fractions of $\mathbb{Z}$? The rationals, $\mathbb{Q}$, by definition.

Example 9.3. Polynomial rings over a field, $K[x]$. The field of fractions is the field of rational functions, denoted $K(x)$.

Example 9.4. $\text{Frac}(K) \cong K$ for any field K.

Question 9.5. $\mathbb{Z}/(n)$ are perefectly good rings. Not always integral domains. What is the ring of total fractions?

To recap what we've done so far in this course:

1. Introduce a ring
2. Introduce ring homomorphisms
3. Different kinds of constructions with rings (quotients, quotients by an ideal)
4. Localization

That's the main foundations of ring theory. It goes much further and is still an active area of research.

Now we're going to get into field theory. You ready? Deep math coming at ya.

We proved on the hw: If K is a field and $\varphi\colon K \to S$ a ring homomorphism then either S is trivial or φ is injective.

10 Lecture 10

Snow days are great days for math. Crunch the numbers before Spring guilt arrives.

10.1 Field Theory

Recall: a field K is a non-trivial commutative ring such that $K^\times = K \setminus \{0\}$. Notice that the non-trivial restriction forces *at least* two elements.

We discussed last time that the only interesting ring homomorphisms between fields are injective. So we're really mostly going to be studying field extensions.

Definition 10.1. If $K \subseteq L$ (a subring[7]) are fields, then we say L is a **field extension** of K and K is a subfield of L. We write L/K to says "L is an extension of K." Not confusing at all.

Example 10.2. $\mathbb{R} \subseteq \mathbb{C}$.

If L/K is an extension then L is a K-vector space. (Proved this on the homework.) The dimension of L as a K-vector space is called the **degree of the extension**. We denote it by $[L : K]$.[8]

Example 10.3. $\mathbb{C}$ is an $\mathbb{R}$-vector space. What does this say about $[\mathbb{C} : \mathbb{R}]$? The construction

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\},$$

is a 2-dimensional $\mathbb{R}$ vector space and $\{1, i\}$ is a basis.

We can also say $[\mathbb{C} : \mathbb{C}] = 1$ but that's not saying much.

What about $[\mathbb{R} : \mathbb{Q}]$? It's infinite for sure. It's uncountably infinite. Why? $\mathbb{R}$ is uncountable, $\mathbb{Q}$ is countable, and the countable union of countable sets is countable, but the countable product is not.

So you can have field extensions of any kind of degree you want.

[7] Fancy way of saying their properties are very similar.

[8] Same notation is used w.r.t. groups to represent index of a subgroup.

Example 10.4. $\mathbb{Q}(x)/\mathbb{Q}$. What is $[\mathbb{Q}(x) : \mathbb{Q}]$? Countably infinite.

We're mostly going to be interested in studying algebraic extensions.

Definition 10.5. If L/K is an extension. And $\alpha \in L$ then we say α is **algebraic** if there exists $m(x) \in K[x]$ not constant such that $m(\alpha) = 0$. We say L/K is algebraic if every $\alpha \in L$ is algebraic. If α is not algebraic then we say α is **transcendental over** K.

Example 10.6. In $\mathbb{C}/\mathbb{R}$ we claim that i is algebraic. Why? Because $x^2 + 1 \in \mathbb{R}[x]$. Now we claim $\mathbb{C}/\mathbb{R}$ is algebraic. Let's do it. We have $a + bi$. Consider $(x - (a + bi))$. This doesn't work because it's probably not a real. But we can write $(x - (a + bi))(x - (a - bi))$ and this has real coefficients if you multiply it out.

Example 10.7. $\mathbb{R}/\mathbb{Q}$ is transcendental. This was hard to prove, but you only need to find one element. It turns out that almost every element is transcendental. That's actually how it was originally proved. Good to know that π is transcendental.

In general it's hard to find the polynomial that we found in the example above.

Proposition 10.8. *If L/K is a finite extension then L/K is algebraic.*

Proof. Say $d = [L : K]$. Let $0 \neq \alpha \in L$. Consider $\{1, \alpha, \alpha^2, \dots, \alpha^d\} \subseteq L$ which has $d + 1$ elements. This set has to be linearly dependent. So there exist $b_i \in K$ (at least two non-zero because $\alpha \neq 0$) such that $b_0 \cdot 1 + b_1\alpha + \cdots + b_d\alpha^d = 0$. So $m(x) = b_0 + b_1x + \cdots + b_dx^d \in K[x]$ non-constant and which vanishes at α. So α is algebraic and we're done since α was arbitrary. [Need to fix the proof in case the set we made does not have distinct elements. See the email.] □

11 Lecture 11

Last time: field extnesions, algebraic and transcendental.

It is not true that every algebraic extension is finite.

Suppose L/K is a field extension, $\alpha \in L$ algebraic over K. What can we do with this? Well we have a ring homomorphism: $\epsilon_\alpha \colon K[x] \to L$ defined by $f(x) \mapsto f(\alpha)$. We didn't actually need that α is algebraic. What's $\ker \epsilon_\alpha$? We're in a PID so write $\ker \epsilon_\alpha = (m_\alpha(x))$. Then $m_\alpha(\alpha) = 0$ by definition. If α were not algebraic then what could we say about the degree of this polynomial? It's $-\infty$ because the polynomial must be identically 0. Otherwise, if α is algebraic then it has to have positive degree because being algebraic means you're the root of *some* non-constant polynomial. Cool.

We claim that without loss of generality we can assume $m_\alpha(x)$ is monic. This is because we're working in a field so we can just eliminate the leading coefficient. So assume $m_\alpha(x)$ is monic.

This polynomial also has a name.

Definition 11.1. $m_\alpha(x)$ is called the **minimal polynomial of** α **over** K**.**

It is the smallest positive degree monic polynomial in $K[x]$ that vanishes at α. Why? Because anything that vanishes at α is in the ideal so its degree is at least as big as $\deg m_\alpha$.

Example 11.2. $i \in \mathbb{C}$. Then $m_i(x) = x^2 + 1 \in \mathbb{R}[x]$. If it's linear and monic it could only be $x - i \notin \mathbb{R}[x]$. So the first one must be the smallest degree polynomial.

This notation makes it seem like the polynomial just depends on α but that's not true, it also depends on the base field.

What's $m_i(x)$ over $\mathbb{C}$? It must be $x - i \in \mathbb{C}[x]$.

The next proposition is related to the homework but it's important so we'll do it again.

Proposition 11.3. *If $\alpha \in L$ is algebraic over K then*

1. *$m_\alpha(x)$ is irreducible over K.*

2. *$K[x]/(m_\alpha(x)) \cong K(\alpha) =$ the smallest subfield of L containing α and K.*

3. *$[K(\alpha) : K] = \deg m_\alpha(x)$.*

Proof.

1. Suppose for the sake of contradiction that $m_\alpha(x) = f(x)g(x)$ for $f(x), g(x) \in K[x]$. So $0 = m_\alpha(\alpha) = f(\alpha)g(\alpha) \in L$, which is a field and therefore an integral domain. So without loss of generality, $f(\alpha) = 0$. So $m_\alpha(x) \mid f(x)$, or $f(x) = m_\alpha(x)h(x)$. Then $m_\alpha(x) = m_\alpha(x)g(x)h(x)$. So $1 = g(x)h(x)$ and therefore $g(x)$ is a unit. So $m_\alpha(x)$ is irreducible.

2. Claim that $m_\alpha(x)$ irreducible and $K[x]$ being a PID implies $(m_\alpha(x))$ is maximal. If $(m_\alpha(x)) \subseteq (g(x))$ then $g(x) \mid m_\alpha(x)$. But $m_\alpha(x)$ is irreducible so $(g(x)) = K[x]$ (if $g(x)$ is a unit) or $(g(x)) = (m_\alpha(x))$. So $(m_\alpha(x))$ maximal by definition. We love a maximal ideal because then the quotient by the ideal is a field. We love fields. So $K[x]/(m_\alpha(x))$ is a field. Let $F = \operatorname{im}(\epsilon_\alpha) \subseteq L$. The FIT tells us that $K[x]/(m_\alpha(x)) \cong F \subseteq L$. Therefore F is a field and not just a lame subring. We know that $K \subseteq F$ because all constants evaluated at α is just the constant. We also claim α is in the image (mapped to by x). So $K(\alpha) \subseteq F$. We'll be done with this part if we can show the inclusion the other way around.

   $K(\alpha) = \bigcap_{\alpha, K \subseteq \tilde{F} \subseteq L} \tilde{F}$. Suppose $\tilde{F} \subseteq L$ subfield such that $K, \alpha \in \tilde{F}$. If $f(x) \in K[x]$ then we claim that $f(\alpha) \in \tilde{F}$. Then $F \subseteq \tilde{F}$. It follows that $F \subseteq K(\alpha)$. Thus, we have equality.

3. We've got that $K(\alpha) \cong K[x]/(m_\alpha(x))$ is an isomorphism of rings. We claim it's also an isomorphism of K-vector spaces. What does it mean for a function to be an isomorphism of K-vector spaces? It's a bijective K-linear transformation. Recall that $f \colon V \to W$ is an isomorphism of K-vs if it's linear, scalars can be factored out, and bijective. Additive becasue ring homomorphism, satisfies scalar multiple property because the isomorphism is just evaluation,[9] and it's a bijection because it's something rings. Therefore $\dim_K K(\alpha) = \dim_K K[x]/(m_\alpha(x))$. Let $d = \deg m_\alpha$. We claim that $\{1, x, x^2, \ldots, x^{d-1}\}$ is a basis for $K[x]/(m_\alpha(x))$. Division with remainder: it's unique in this polynomial ring! So take $f(x) = q(x)m_\alpha(x) + r(x)$ with $\deg r(x) < \deg m_\alpha(x) = d$. This proves the claim. □

Some comments

1. $K(\alpha) = K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$.

2. You can do all the field arithmetic in the extension just using division with remainder. This is how these field extensions are represented in computers.

[9] $\epsilon_\alpha(c \cdot g(x)) = cg(\alpha) = c\epsilon_\alpha(g(x))$

Suppose we have $m(x) \in K[x]$ irreducible. Then is there some field extension where this is the minimal polynomial? Yes. Put another way, is there some field extension that contains a root of $m(x)$. Here's the field extension: $K \subseteq K[x]/(m(x))$. It's a field extension containing a root of $m(x)$: x. Nice.

12 Lecture 12

Midterm on Friday in class, the whole time, study guide online. No surprises except for the optional challenge problem.

Recall that last week we went over field extensions. We're particularly concerned with algebraic field extensions because they're interesting. We also defined the degree of a field extension. We also showed that every irreducible polynomial $m(x) \in K[x]$ has a field extension with $m(x)$ as the root: $K[x]/(m(x))$. The degree of this field extension in $\deg m(x)$.

Let α be a root of $m(x)$ (some irreducible polynomial) and consider $K(\alpha)/K$. What we mean is $K(\alpha) = K[x]/(m(x))$. It feels ambiguous to say this because we're saying *any* root of $m(x)$, but we proved last time this'll be isomorphic to what we defined $K(\alpha)$ as.

What about $K(\alpha, \beta)/K$ where α, β are roots of two different irreducible polynomials. But after we add α the other polynomial may not be irreducible anymore. It's still difficult if we just have two roots of the same polynomial. The polynomial must not be irreducible over the extension, so it seems like we can't add two different roots to our field extension. This is what we're going to work on.

Question 12.1. Say L/K is a field extension. What are the intermediate extensions?

Question 12.2. If $K(\alpha)/K$ is a field extension where α is a root of $m(x)$, how many of the roots of $m(x)$ live in this field?

Question 12.3. Which polynomials $f(x)$ will have roots in $K(\alpha)/K$?

Theorem 12.4 (Tower Theorem)**.** *Let $K \subseteq L \subseteq M$ be field extensions. If M/L and L/K are finite, then M/K is finite and $[M : K] = [M : L] \cdot [L : K]$.*

Proof. Let $[M : L] =: d$ and $[L : K] =: e$.[10] Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be a basis for M/L. Let $B = \{\beta_1, \beta_2, \ldots, \beta_e\}$ be a basis for L/K. We claim that $C = \{\alpha_i\beta_j \mid 1 \leq i \leq d, 1 \leq j \leq e\}$ is a basis for M/K. What does it take to prove something's a basis? It spans M as a vector space over K and it's linearly independent.

Spanning Let $\gamma \in M$. Because A spans over L, we know that $\gamma = \sum_{i=1}^{d} m_i\alpha_i$, $m_i \in L$. For each i, we can write $m_i = \sum_{j=1}^{e} n_{ij}\beta_j$ for $n_{ij} \in K$. Smoosh it together:

$$\gamma = \sum_{i=1}^{d}\sum_{j=1}^{e} n_{ij}\alpha_i\beta_j,$$

which is exactly what we intended to show.

[10] In a sense, group theory is equivalent to field theory. This theorem is analogous to Lagrange's theorem.

Linearly independent Suppose that

$$\sum_{i=1}^{d}\sum_{j=1}^{e} n_{ij}\alpha_i\beta_j = 0.$$

We can group all of the βs together:

$$0 = \sum_{i=1}^{d}\left(\sum_{j=1}^{e} n_{ij}\beta_j\right)\alpha_i.$$

Because A is independent, for each i, $\sum_{j=1}^{e} n_{ij}\beta_j = 0$. Because B is independent over K, $n_{ij} = 0$. □

Corollary 12.5. *If L/K is a degree d extension, and $\alpha \in L$, then $\deg m_\alpha(x)$ divides d.*

Proof. Oof it's a picture. My tikz skills aren't there. □

Example 12.6. Consider $\mathbb{Q}(\sqrt[3]{2})$. What is the degree of this extension? It's 3 because $m(x) = x^3 - 2$. We claim that if a degree 3 polynomial factors it must have a linear factor (this is a special case for degree 2 and degree 3). We also claim if it factors over $\mathbb{Q}$ it factors over $\mathbb{Z}$ (Gauss's Lemma). No way because 2 is prime. So we know $m(x)$ is the minimal polynomial over $\mathbb{Q}$. Ergo, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

[Another picture. L between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})$. Then $[L : \mathbb{Q}]$ is 1 or 3. So either $L = \mathbb{Q}$ or $L = \mathbb{Q}(\sqrt[3]{2})$.]

Nothing interesting in the intermediate fields. Does $x^3 - 2$ have more than one root in this extension? It's not clear. It turns out the answer is no. Why? Gotta use some tricks.[11] Suppose there are at least two distinct roots, α and β in $\mathbb{Q}(\sqrt[3]{2})$. Neither of them can be zero. So we can divide by β. Consider $\omega = \alpha/\beta \in \mathbb{Q}(\sqrt[2]{3})$. Then $\omega^3 = \alpha^3/\beta^3 = 1$. But $\omega \neq 1$ because $\alpha \neq \beta$. Factor $x^3 - 1$. Use the quadratic formula. We get a negative square root. So definitely not in the real numbers. Last observation: there is a cube root of 2 in the real numbers. So this field is embedded into the reals. But $\omega \notin \mathbb{R}$. So $\alpha = \beta$.

13 Lecture 13

Bring a calculator if you don't like doing arithmetic by hand. Do I even have a calculator?

Last time we proved the Tower Theorem (super useful). Here's a mnemonic: "$M/K = M/L \cdot L/K$."

Suppose α a root of minimial polynomial $m(x)$ for K. What polynomials $f(x)$ have roots in $K(\alpha)$ and how many? In the particular case of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ we can use the tower theorem to show there's no intermediates. It's tough to say in general.

But let's look at some fields where it's easier to answer these questions.

Example 13.1. Suppose L/K is degree 2. We call this a **quadratic extension**. We claim that if $m(x) \in K[x]$ irreducible with a root in L, then all the roots of $m(x)$ are in L.

[11] Play bridge.

Proof. Suppose α is a root of $m(x)$ in L. Then we have $K \subseteq K(\alpha) \subseteq L$. So $[K(\alpha) : K]$ is 1 or 2 by the tower theorem. If the degree is 1 then $\alpha \in K$ because the fields are equal. So the irreducible polynomial has degree 1. (Recall that we proved the degree of the extension is equal to the degree of the minimal polynomial.) Therefore all the roots of m actually live in $K \subseteq L$. Now, suppose the extension has degree 2. Then $K(\alpha) = L$ (again by the tower theorem). So m is quadratic and has a root α so we can factor it as $m(x) = (x - \alpha)(x - \beta) \in L[x]$.[12] Therefore $\beta \in L$. Thus, all the roots of m live in L. □

Definition 13.2. A finite extension L/K is said to be **normal** if whenever $m(x) \in K[x]$ irreducible has a root $\alpha_1 \in L$, then $m(x)$ **splits completely** over L:

$$m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) \in L[x].$$

The name "normal" is misleading because most field extensions are not normal. How would we go about finding a normal field extension? We just showed that ever quadratic extension is normal.

Question 13.3. How to find other normal extensions?

Hold that thought.

Nonexample 13.4. The extension $\mathbb{Q}(\sqrt[3]{2}/)\mathbb{Q}$ is not normal because we proved that $x^3 - 2$ has one root in $\mathbb{Q}(\sqrt[3]{2})$.

Definition 13.5. We say L/K is a **splitting field** if there is some $f(x) \in K[x]$ such that

1. f splits completely over L.
2. $L = K(\alpha_1, \ldots, \alpha_d)$ where α_i are the roots of f.

Example 13.6. Every quadratic extension L/K is a splitting field.

Proof. Let $\alpha \in L \setminus K$. Then we get a topic of field extensions: $K \subseteq K(\alpha) \subseteq L$ with $[L : K] = 2$. So $L = K(\alpha)$. Let $m(x)$ be the minimal polynomial of α. We just showed $m(x)$ splits completely over L. Note that we don't actually need both roots to make the full field in this case. This shows every quadratic extension is a splitting field. □

Right now we can't say that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ isn't a splitting field. But we'll do that by the end of class.

Proposition 13.7. *If $f(x) \in K[x]$, then there exists a splitting field L/K of $f(x)$.*

Proof. We want to prove $P(d)$ defined as: for all fields K and for all $f(x) \in K[x]$ with $\deg f \leq d$ has a splitting field. The idea is to use a cleverly constructed induction.[13]

Base case If $d = 1$ then if $f(x)$ has degree 1 then $f(x) = a(x - b)$. So it already splits completely over K.

[12] This factorization follows from the fact that we can write $m(x) = q(x)(x - \alpha) + r(x)$ where we know $\deg r(x) = 1$. We have $0 = m(\alpha) = r(\alpha)$ so $r(x) = 0$. Since the quotient is quadratic we must have that $q(x)$ is linear.

[13] That should be the main takeaway of this proof.

Inductive step Suppose $P(d)$ for some $d \geq 1$. Let $f(x) \in K[x]$ be degree $d+1$. Let $m(x)$ be an irreducible factor (proved in HW2) with $\deg m(x) \geq 1$. Let $K(\alpha)$ be an extension with a root of $m(x)$. So, $(x-\alpha) \in K(\alpha)[x]$. This (like before) implies $f(x) = (x-\alpha)g(x) \in K(\alpha)[x]$. We can say that $\deg g(x) = d$. By indutive hypothesis, that implies $g(x)$ has a splitting field over $K(\alpha)$, call it L. So then $L = K(\alpha)(\alpha_1, \alpha_2, \ldots, \alpha_d)$ where α_i are the roots of g. But this is the same as just $K(\alpha, \alpha_1, \alpha_2, \ldots, \alpha_d)$. Those are also the roots of f. Therefore L is a splitting field of f. □

We just proved splitting fields exist. Even better, splitting fields are essentially unique. Let's make this notion precise.

Definition 13.8. We say that L_1/K and L_2/K are **isomorphic over** K or **isomorphic extensions of** K if there exists some $\varphi\colon L_1 \to L_2$ ring isomorphism such that for all $a \in K$, $\varphi(a) = a$. We call this φ a K **isomorphism.**

Fact 13.9. *If φ is a K-isomorphism then it is a K-linear isomorphism of $L_1 \cong L_2$ as K-vector spaces.*

Recall these field extensions are playing double lives: they're fields but they're also vector spaces over K. If L_1/K and L_2/K are K-isomorphic then they have the same degree over K.

Theorem 13.10. *If $f(x) \in K[x]$ and L_1/K and L_2/K are splitting fields of $f(x)$, then $L_1 \cong L_2$ as extensions of K.*

Proof. Next homework. □

Theorem 13.11. *A finite extension L/K is normal iff L/K is a splitting field over K.*

Proof. The forward direction is easy. Suppose L/K is normal. Then because L is a finite extension it must be generated by finitely many elements: $L = K(\alpha_1, \ldots, \alpha_d)$ for some $\alpha_1, \ldots, \alpha_d \in L$. (Start building up the tower and it makes sense.) Punchline: let $m_i(x)$ be the minimal polynomial of α_i. Then the product of these all should split. □

14 Lecture 14

Let's redo (and complete) the proof of last time. Recall that

1. Definition 13.5,[14]

2. Definition 13.2.

Last time we proved splitting fields exist. On homework we'll prove they're unique. My memory feels shot today what is going on.

Proof of Theorem 13.11. For the forward direction (easier because universal quantifier implying an existential quantifier) suppose that L/K is normal. We claim $L = K(\beta_1, \beta_2, \ldots, \beta_d)$. Because L/K is finite, it's finite dimensional as a vector space over K which implies there's a basis: $\beta_1, \beta_2, \ldots, \beta_d$. This proves the claim. Let $m_i(x) \in K[x]$ be the minimal polynomial of

[14] Don't LaTeX and math, kids.

β_i. Then $f(x) = m_1(x)m_2(x)\cdots m_d(x) \in K[x]$. We claim that f splits completely in L and L is a splitting field for f. Why the first claim? $m_i(x)$ is irreducible and has a root $\beta_i \in L$. So therefore, normality implies $m_i(x)$ splits completely over L. Now we show it's the smallest extension generated by these roots. Let $\beta_1, \dots, \beta_d, \dots, \beta_e \in L$ be all the roots of $f(x)$. So $L \supseteq K(\beta_1, \beta_2, \dots, \beta_e) \supseteq K(\beta_1, \beta_2, \dots, \beta_d) = L$. Therefore L is the smallest field containing the roots of f so L/K is a splitting field.

For the reverse direction suppose L/K is a splitting field over K. Let $m(x) \in K$ be an irreducible polynomial. Let M/L be a splitting field of $m(x)$. We claim that if $\alpha, \beta \in M$ are two roots of $m(x)$, then $[L(\alpha) : L] = [L(\beta) : L]$. This is at the heart of what we want to show. Suppose the claim is true. If $\alpha \in L$ is some root of $m(x)$, then $[L(\alpha) : L] = 1$. But if the claim is true and β is another root then $[L(\beta) : L] = 1$. So $\beta \in L$. So now we prove the claim. We're making diagrams again this is fun. Wish I could LaTeX that. Tower theorem says $[L(\alpha) : L][L : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K]$. Similarly with β. We claim that $[K(\alpha) : K] = [K(\beta) : K]$. Both sides are $\deg(m(x))$. So now we need to show $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$. Turns out the two fields are isomorphic because we proved $K(\alpha) \cong K[x]/(m(x)) =: F \cong K(\beta)$. So $L(\alpha)$ and $L(\beta)$ can both be viewed as field extensions of F. Now (pay attention) claim that $L(\alpha)/F$ and $L(\beta)/F$ are splitting fields of $f(x)$. Because L/K splitting field, we know that $L = K(\gamma_1, \dots, \gamma_d)$ with $\gamma_1, \dots, \gamma_d$ the roots of $f(x)$. That tells us that $L(\alpha) = K(\gamma_1, \dots, \gamma_d, \alpha)$. So, in particular, $f(x)$ splits completely over $L(\alpha)$. The fact the identity holds tells us it's the smallest extension of F that contains all of the roots. So $K(\gamma_1, \dots, \gamma_d, \alpha) = F(\gamma_1, \dots, \gamma_d)$. This implies $L(\alpha)/F$ is a splitting field. By symmetry we can use the same argument to show $L(\beta)/F$ is a splitting field. So these are two splitting fields of the same polynomial on the same base field. Use uniqueness (this week's homework) up to isomorphism to finish the proof: $L(\alpha) \cong L(\beta)$ over F. In particular, $[L(\alpha) : K(\beta)] = [L(\alpha) : F] = [L(\beta) : F] = [L(\beta) : K(\beta)]$, which is all we had left to show. We can divide. I don't want to write it down. □

15 Lecture 15

Last time: finite normal extensions and splitting fields are the same. Splitting fields are always finite degree because a polynomial only has finitely many roots. You could also look at zeros of power series but those aren't algebraic extensions in general and you have to deal with analytic issues.

The proof from last time isn't that important, just remember the result.

15.1 Symmetric Polynomials

Definition 15.1. R is a commutative ring, $n \geq 1$. Consider $R[x_1, x_2, \dots, x_n]$. We'll use a little bit of group actions. Recall the symmetric group, denoted S_n which is permutations of $\{1, 2, \dots, n\}$ and the operation is just composition of functions. S_n acts on $R[x_1, x_2, \dots, x_n]$ on the right. If $\sigma \in S_n$ then

$$f^\sigma(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, f_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

For example, $\sigma = (12)(34) \in S_4$. If $f = x_1^2 x_2 + x_3$ then $f^\sigma = x_2^2 x_1 + x_4$.

$\sigma, \tau \in S_n$. $f^{(\sigma\tau)} = (f^\sigma)^\tau$. "Pre-composition."

Another example I don't feel like writing down.

Ha gottem. Action isn't on the right it's on the left. Define it as

$$\sigma f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, f_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

So now $(\sigma\tau)f = \sigma(\tau f)$

S_n acts by ring automorphisms. So $\sigma(f+g) = \sigma f + \sigma g$ and $\sigma(fg) = \sigma(f)\sigma(g)$. Also $\sigma(1) = 1$ and $\sigma(0) = 0$.

A polynomial $f \in R[x_1, x_2, \ldots, x_n]$ is **symmetric** if $\sigma f = f$ for all $\sigma \in S_n$. We write $R[x_1, x_2, \ldots, x_n]^{S_n}$ to denote the set of all symmetric polynomials.

Claim $R[x_1, x_2, \ldots, x_n]^{S_n}$ is a ring.

Some examples: constants, $x_1 + x_2 + x_3$, $x_1x_2x_3$.

Nonexample: $x_1x_2^2$.

Elementary Symmetric Polynomials.

$R[x_1, x_2, \ldots, x_n]$ for $1 \le k \le n$.

$$e_k := \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Proposition 15.2. *Let $n \geq 1$ and consider $(1 + x_1y)(1 + x_2y)\cdots(1 + x_ny) \in R[x_1, \ldots, x_n][y]$.*

Proof. Coefficient of y^k is sum over ways of choosing k terms with a y in it. Sum over all choices is e_k. □

Corollary 15.3. $(y - x_i)(y - x_2)\cdots(y - x_n) = y^n - e_1y^{n-1} + \cdots + (-1)^n e_n$.

Proof. Replace y with $-1/y$ in the previous expansion. Then we get $(1 - x_1/y)(1 - x_2/y)\cdots(1 - x_n/y) = 1 - e_1/y + e_2/y^2 + \cdots + (-1)^n e_n/y_n$. Now multiply both sides by y^n. We get $(y - x_1)(y - x_2)\cdots(y - x_n) = y^n - e_1y^{n-1} + e_2y^{n-2} + \cdots + (-1)^n e_n$. □

16 Lecture 16

Theorem 16.1 (Fundamental Theorem of Symmetric Functions)**.** *Let R be a commutative ring $n \geq 1$. Then*

$$R[x_1, x_2, \ldots, x_n]^{S_n} = R[e_1, e_2, \ldots, e_n].$$

"Every symmetric polynomial is a polynomial in elementary symmetric functions (in a unique way)."

Example 16.2. $n = 2$. We can pick $f = x_1^3 + x_2^3$. Then $f - e_1^3 = -3x_1x_2^2 - 3x_1^2x_2 = -3x_1x_2(x_1 + x_2) = -3e_1e_2$ first because we're trying to get rid of the leading term.

"groups acting on rings"

Corollary 16.3. *Let $f(x) \in K[x]$ by a monic polynomial. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in a splitting field L/K of $f(x)$. If $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]^{S_n}$ is a symmetric polynomial then $g(\alpha_1, \ldots, \alpha_n) \in K$.*

Proof. FTSP: $g(x_1, \ldots, x_n) = h(e_1, \ldots, e_n)$. So $g(\alpha_1, \ldots, \alpha_n) = h(e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n))$

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = x^n - e_1x^{n-1} + e_2x^{n-2} + \cdots + (-1)^n e_n \in K[x]$$

□

16.1 Separable Extensions

Definition 16.4. $f(x) \in K[x]$ is **separable** if the number of distinct roots of f in a splitting field is equal to $\deg(f)$.

Definition 16.5. Let L/K be a field extensio, $\alpha \in L$ is **separable** if $m_\alpha(x) \in K[x]$ is separable.

We say L/K is **separable** if every element $\alpha \in L$ is separable.

Definition 16.6. A field is **perfect** if every irreducible polynomial $\in K[x]$ is separable.

This includes: every field of characteristic 0 and every finite field.

Non-example: $\mathbb{F}_p(y)$

We always want to assume perfect!

These are the ingredients to a Galois extension.

Theorem 16.7 (Primitive Element Theorem)**.** *Let $L = K(\alpha_1, \dots, \alpha_n)$ be a finite extension of K such that each α_i is separable over K. Then there exists some $\beta \in L$ such that $L = K(\beta)$ and β is separable over K. We call β a **primitive element for** L/K.*

That's pretty neat.

Proof. We will asume K is infinite (the other case on your homework). Induction on N

Base case $N = 2$ and we say $L = (\alpha, \beta)$, α, β separable. Let $f(x)$ and $g(x)$ be the minimal polynomials of α and β, respectively. Let M/L be a splitting field of $f(x)g(x)$. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_m$ be the roots of f and $\beta = \beta_1, \beta_2, \dots, \beta_n$ be the roots of g.

Since K is infinite there exists $\lambda \in K$ such that $\lambda \neq \frac{\alpha_i - \alpha_j}{\beta_r - \beta_s}$ for $i \neq j$, $r \neq s$. This is equivalent to $\alpha_i + \lambda\beta_s \neq \alpha_j + \lambda\beta_r$. Let $\gamma := \alpha + \lambda\beta \in L$. We claim that $L = K(\gamma)$.

$K(\gamma) \subseteq L = K(\alpha, \beta)$. $\gamma = \alpha + \lambda\beta \in K(\alpha, \beta) = L$.

$K(\alpha, \beta) \subseteq K(\gamma)$. Suffices to show $\alpha, \beta \in K(\gamma)$. Remember that f and g are the min polynomials of α and β, respectively. Wkt β is a root of $g \in K[x] \subseteq K(\gamma)[x]$. Consider $f(\gamma - \lambda x) \in K(\gamma)[x]$. Plug in β: $f(\gamma - \lambda\beta) = f(\alpha + \lambda\beta - \lambda\beta) = f(\alpha) = 0$ so β is a root of $f(\gamma - \lambda x)$.

$h(x) = \gcd(f(\gamma - \lambda x), g(x)) \in K(\gamma)[x]$. $h(\beta) = 0$ so $\deg h \geq 1$. We claim that $\deg h = 1$. Suppose for the sake of contradiction that $\deg h > 1$. Then because $h(x) \mid g(x)$, therefore there exists β_i, $i \neq 1$ such that $h(\beta_i) = 0$. β separable implies there exists a root of $g(x) \neq \beta$. β_i is a root of $f(\gamma - \lambda x)$. So $0 = f(\gamma - \lambda\beta_i) = f(\alpha_1 + \lambda\beta_1 - \lambda b_i)$. Therefore $\alpha_1 + \lambda\beta_1\lambda\beta_i = \alpha_j$ for some j. Rearrange: $\alpha_1 + \lambda\beta_1 = \alpha_j + \lambda\beta_i$. Which contradicts the definition of λ. Therefore $\deg h = 1$. So $h(x) = (x - \beta) \in K(\gamma)[x]$ because it's the gcd. That implies $\beta \in K(\gamma)$.

Now $K(\gamma) \ni \gamma - \lambda\beta = \alpha + \lambda\beta - \lambda\beta = \alpha$. So $\alpha \in K(\gamma)$. Therefore $K(\alpha, \beta) \subseteq K(\gamma)$.

Inductive step Replace generators one pair at a time using the base case.

Now we claim γ is separable. Let $p(x) \in K[x]$ be the minimal polynomial of γ. Let $q(x) = \prod_{j=1}^n f(x - \lambda\beta_j) \in K[x]$ by the corollary (since it's symmetric). $f(x) = \prod_{i=1}^m (x - \alpha_i)$ so therefore $q(x) = \prod_{i=1}^m \prod_{j=1}^n (x - (\alpha_i + \lambda\beta_j))$. Roots all distinct by the definition of λ. q has coefficients in K and vanishes at γ. Therefore $p(x) \mid q(x)$ because $p(x)$ minimal polynomial of γ. So $q(x)$ separable implies $p(x)$ separable which implies γ separable. □

17 Lecture 17

Three weeks left.

Last time we were talking about separable extensions. We proved the Primitive Element Theorem (Theorem 16.7). The finite field case is going to be on next week's homework. One reason it's useful is we like extensions that are generated by a single element because we know they can be expressed as the quotient of a polynomial ring (in one variable).

Corollary 17.1. *Let L/K be a finite separable extension.*

1. *$L = K(\beta)$ for some $\beta \in L$.*
2. *There are finitely many intermediate extensions.*

A while back we were trying to understand how many things there were. Looks like we're doing that again.

Proof.

1. L/K finite implies $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n$. Each α_i is separable because it's a separable extension. Therefore, the primitive element theorem tells us that $L = K(\beta)$ for some $\beta \in L$.

2. Suppose $K \subseteq F \subseteq L$ subfield. Use the first part to say $L = K(\beta)$ We claim that $L = F(\beta)$. This follows because $L \supseteq F(\beta) \supseteq K(\beta) = L$. Let $m_K(x) \in K[x]$ be the minimal polynomial of β over K, and let $m_F(x) \in F[x]$ be the minimum polynomial of β over F. Recall that a minimal polynomial is the lowest positive degree polynomial that vanishes at β. We've proven some fun stuff about this polynomial. By definition, $m_K(x) \in K[x] \subseteq F[x]$ and $m_K(\beta) = 0$. So $m_F(x) \mid m_K(x)$. Key insight: $m_K(x)$ has finitely many distinct monic factors.

   Suppose $K \subseteq F_1, F_2 \subseteq L$ intermediate fields have the same minimal polynomial $m(x) = m_{F_1}(x) = m_{F_2}(x)$ for β. Goal is to show $F_1 = F_2$. We have $F_1(\beta) = L = F_2(\beta)$. We can write $m(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ where $a_i \in F_1$ *and* $a_i \in F_2$. I.e., $a_i \in F_1 \cap F_2$. This is another intermediate field. That's a hard one to draw. $L = (F_1 \cap F_2)(\beta)$. The extension from the intersection to L is the same as the intersection to F_i then to L. So those links must have degree 1 which means $F_1 = F_2$, which is what we were trying to show.

$$\begin{tikzcd}
 & L \arrow[dl, dash, "1"'] \arrow[d, dash, "1"] \arrow[dr, dash, "1"] & \\
F_1(\beta) \arrow[r, dash, "1"] \arrow[d, dash, "d"] & (F_1 \cap F_2)(\beta) \arrow[r, dash, "1"] \arrow[d, dash, "d"] & F_2(\beta) \arrow[d, dash, "d"] \\
F_1 \arrow[r, dash, "1"] \arrow[dr, dash, bend right] & F_1 \cap F_2 \arrow[r, dash, "1"] \arrow[d, dash] & F_2 \arrow[dl, dash, bend left] \\
 & K &
\end{tikzcd}$$

□

17.1 Galois Groups

Definition 17.2. Suppose L/K finite extension. Then $\mathrm{Gal}(L/K) := \{\sigma\colon L \xrightarrow{\sim} L \mid \sigma \text{ is } K\text{-isomorphism}\}$ is called the **Galois group of** L/K.

Earlier we proved for all rings R, $\mathrm{Aut}(R)$ forms a group wrt composition. $\mathrm{Gal}(L/K) \subseteq \mathrm{Aut}(L)$. Claim this is a subgroup. If $\sigma, \tau \in \mathrm{Gal}(L/K)$ then $\sigma \circ \tau$ is an automorphism of L. If $a \in K$ then $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$. So $\sigma \circ \tau \in \mathrm{Gal}(L/K)$. So $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$. So $\sigma^{-1} \in \mathrm{Gal}(L/K)$.

Example 17.3. Let $\mathbb{C}/\mathbb{R}$. Claim $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$, where τ is complex conjugation and 1 is the identity. Recall that $\tau(a + bi) = a - bi$. When you learned this last you probably weren't told this is a field automorphism that fixes the real numbers.

Proposition 17.4. *Let L/K be a finite extension.*

1. *If $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ and $\beta_1, \ldots, \beta_n \in L$, then for all $\sigma \in \mathrm{Gal}(L/K)$, we have that $\sigma(f(\beta_1, \ldots, \beta_n)) = f(\sigma(\beta_1), \ldots, \sigma(\beta_n))$.*
2. *If $\beta \in L$ is a root of $g(x) \in K[x]$, then $\sigma(\beta)$ is also a root of $g(x)$.*
3. *$L = K(\beta_1, \ldots, \beta_n)$, then σ is completely determined by $\sigma(\beta_1), \ldots, \sigma(\beta_n)$.*
4. *$|\mathrm{Gal}(L/K)| \leq \prod_{i=1}^{n} \deg m_i(x)$, where $m_i(x)$ is the minimal polynomial of β_i over K.*

Proof.

1. Let $\sigma \in \mathrm{Gal}(L/K)$. We claim it suffices to prove this for monomials: $f = cx_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ where $c \in K$. This because we can break a polynomial into a sum of monomials. This is just to keep our notation clean. So $\sigma(f(\beta_1, \ldots, \beta_n)) = \sigma(c\beta_1^{e_1}\cdots\beta_n^{e_n}) = \sigma(c)\sigma(\beta_1)^{e_1}\cdots\sigma(\beta_n)^{e_n} = f(\sigma(\beta_1), \ldots, \sigma(\beta_n))$. (In this, e_i are non-negative integers, *not* elementary symmetric polynomials.)
2. $g(x) \in K[x]$ and $0 = g(\beta)$. Apply σ to both sides, $0 = \sigma(0) = \sigma(g(\beta)) = g(\sigma(\beta))$. So $\sigma(\beta)$ is a root of $g(x)$.
3. $K(\beta_1, \ldots, \beta_n) = \{f(\beta_1, \ldots, \beta_n) \mid f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}$. Then we have that if $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$ and if $\sigma_1(\beta_i) = \sigma_1(\beta_i)$ then by part (1) we have $\sigma_1(f(\beta_1, \ldots, \beta_n)) = \sigma_2(f(\beta_1, \ldots, \beta_n))$. So $\sigma_1 = \sigma_2$. (One should write more steps between these equalities but Trevor's hand is tired.)
4. If $m_i(x)$ is the minimal polynomial of β_i over K then for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\beta_i)$ is another root of $m_i(x)$. Therefore, $|\mathrm{Gal}(L/K)| \leq \prod_{i=1}^{n} \deg m_i(x)$. □

Theorem 17.5. *If L/K is a finite, normal, and separable extension then $|\mathrm{Gal}(L/K)| = [L : K]$.*

Definition 17.6. L/K is a **galois extension** if it is finite, normal, and separable.

18 Lecture 18

18.1 Construction of Field Automorphism

Proof of Theorem. Since L/K finite and separable, $\beta \in L$ such that $L = K(\beta)$ by primitive element theorem. Let $m(x)$ be a minimal polynomial of β let $d = \deg(m(x)) = [L : K]$. We know that $|\operatorname{Gal}(L/K)| \leq d$ and if $\sigma \in (\operatorname{Gal}(L/K))$ then σ completely determined by $\sigma(\beta)$ and furthermore, $m(\sigma(\beta)) = 0$. We only have d choices.

Let $\{\beta_1, \ldots, \beta_d\}$ be the roots of $m(x)$. By L/K normal and $\beta \in L$ and $m(x)$ irreducible, $\{\beta_1, \ldots, \beta_d\} \subseteq L$.

$$L = K(\beta) \overset{\varphi_1}{\cong} \frac{K[x]}{m(x)} \overset{\varphi_i}{\cong} K(\beta_i) = L$$

but $[K(\beta_i) : K] = d$ so $[L : K(\beta)] = 1$. φ_1, φ_i are K-isomorphisms. $phi(x) = \beta$, $\varphi_i(x) = \beta_i$.

(N.B., $f(x) \in K[x]$, $\varphi(f(x)) = f(\varphi(x)) = f(\beta)$ since φ K-isomorphism, does not affect coefficients. So isomorphism determined exactly by action on β.)

$\varphi_i \circ \varphi^{-1} \colon L \overset{\sim}{\to} L$ is a K-isomorphism. And $\varphi_i \circ \varphi^{-1}(\beta) = \varphi_i(\varphi^{-1}(\beta)) = \varphi_i(x) = \beta_i$. There are d-choices for β_i hence $|\operatorname{Gal}(L/K)| \geq d$. Thus, $|\operatorname{Gal}(L/K)| = d$. □

Example 18.1. Suppose p prime. $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. $x^2 - p \in \mathbb{Q}[p]$ irreducible by Eisenstein/u f and primeness. $x^2 - p$ is separable by $\mathbb{Q}$ is perfect field (finite exptension of perfect field separable). Field is normal since $\mathbb{Q}(\sqrt{p})$ is a splitting field for $x^2 - p$.

By Theorem, $|\operatorname{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})| = 2 \cong C_2$ (only one group order 2).

Something I'm missing.

19 Lecture 19

20 Lecture 20

Proposition 20.1. *Let L/K be a Galois extension. Suppose $K \subseteq F \subseteq L$ is an intermediate field. Then L/F is also Galois. And* $\operatorname{Gal}(L/F) \subseteq \operatorname{Gal}(L/K)$.

Proof. We can write $L = K(\beta)$ because it's a finite separable extension. Say $m(x) \in K[x]$ is the minimal polynomial of β. Then L is the splitting field of $M(x)$ over K. Because L/K is finite an separable, L/F is finite and separable. Then $L = K(\beta) \subseteq F(\beta) \subseteq L$. So $L = F(\beta)$ and L is a splitting field of $m(x)$ over F. Also $m(x) \in F[x]$. Therefore L/F is Galois.

$\operatorname{Gal}(L/F) = \{\sigma \in \operatorname{Aut}(L) \mid \sigma(a) = a \forall a \in F \supseteq K\} \subseteq \operatorname{Gal}(L/K)$. □

Definition 20.2. Let L/K be Galois. We write $\operatorname{Int}(L/K) = \{F \mid K \subseteq F \subseteq L\}$ and $\operatorname{Sub}(L/K) = \{H \subseteq \operatorname{Gal}(L/K), \text{ subgroups}\}$.

We're going to show $\operatorname{Gal}(L/K) \colon \operatorname{Int}(L/K) \to \operatorname{Sub}(L/K)$ defined by $F \mapsto \operatorname{Gal}(L/F)$ is bijective.

Proposition 20.3. *Let L/K be Galois and suppose that $H \subseteq \operatorname{Gal}(L/K)$.*

1. *$L^H = \{a \in L \mid \sigma(a) = a, \sigma \in H\}$ is an intermediate field $K \subseteq L^H \subseteq L$. We call this the **fixed field of** H.*

2. *L/L^H is Galois and $\operatorname{Gal}(L/L^H) = H$. So $[L : L^H] = |H|$.*

Proof.

1. First we need to show L^H is a field. We have to show it's a ring and ever nonzero element is invertible. Why are $0, 1 \in L^H$? Because ring automorphisms have to fix 0 and 1. Now we show addition and multiplication. Suppose $a, b \in L^H$. Let $\sigma \in H$. Then $\sigma(a+b) = \sigma(a)+\sigma(b) = a+b$. And we can do the same thing for multiplication: $\sigma(ab) = \sigma(a)\sigma(b) = ab$. So $a+b, ab \in L^H$. For additive inverses, if $a \in L^H$ then $\sigma(-a) = -\sigma(a) = -a \in L^h$. Say $a \neq 0$. Then $\sigma(1/a) = 1/sigma(a) = 1/a \in L^H$. So L^H is a field.

   Why does it contain K? Because by definition K is fixed by every element of the Galois group so it's certainly fixed by a subgroup.

2. Definitely $H \subseteq \operatorname{Gal}(L/L^H)$ by definition of L^H. $d = |H| \leq |\operatorname{Gal}(L/L^H)|$. Then $L = K(\beta)$.

   $$m(x) = \prod_{\sigma \in H} (x - \sigma(\beta)) \overset{?}{\in} L^H[x].$$

   $\deg m(x) = d$.

   $[L^H(\beta) : L^H] \leq d$ because minimial polynomial of β over L^H must divide $m(x)$. But $L = K(\beta) \subseteq L^H(\beta) \subseteq L$ So $[L^H(\beta) : L^H] = [L : L^H] \leq d|H| \leq |\operatorname{Gal}(L/L^H)|$. So $H = \operatorname{Gal}(L/L^H)$. □

We just proved that a function written above is surjective. So to finish the proof that it's bijective we just need to show it's injective. We'll do this by showing these two functions are inverses. So if we start with an intermediate field we get the corresponding Galois group. Take the fixed field of that and you get the intermediate field? Let's see.

Proposition 20.4. *Let L/K be Galois and suppose we have an intermediate field: $K \subseteq F \subseteq L$. Then $L^{\operatorname{Gal}(L/F)} = F$.*

Proof. Claim that $F \subseteq L^{\operatorname{Gal}(L/F)}$. It's by definition but it's a lot to unpack.

$|\operatorname{Gal}(L/F)| = [L : F] \leq [L : L^{\operatorname{Gal}(L/F)}] = |\operatorname{Gal}(L/F)|$. Therefore $F = L^{\operatorname{Gal}(L/F)}$. □

Theorem 20.5 (Galois Correspondence I)**.** *Let L/K be Galois. Then $\operatorname{Int}(L/K) \leftrightarrow \operatorname{Sub}(L/K)$ with $F \mapsto \operatorname{Gal}(L/F)$ and $H \mapsto L^H$ are inverses.*

1. *If $F_1 \subseteq F_2$ then $\operatorname{Gal}(L/F_2) \supseteq \operatorname{Gal}(L/F_1)$.*
2. *Similarly, if $H_1 \subseteq H_2$ fixed groups then $L^{H_2} \subseteq L^{H_1}$*

"There is an inclusion reversing bijection between $\operatorname{Int}(L/K)$ and $\operatorname{Sub}(L/K)$."

$$\begin{tikzcd}
\operatorname{Int}(L/K) \arrow[r, bend left, "F \mapsto \operatorname{Gal}(L/F)"] \arrow[r, bend right, "L^P \mapsfrom"'] & \operatorname{Sub}(L/K)
\end{tikzcd}$$

Proof.

1. By definition.

2. By definition.

$\square$

Proposition 20.6. *Let L/K be Galois. Suppose $K \subseteq F \subseteq L$ such that F/K is Galois. Then for all $\sigma \in \operatorname{Gal}(L/K)$, $\sigma(F) = F$ (but not pointwise!) and $\rho\colon \operatorname{Gal}(L/K) \to \operatorname{Gal}(F/K)$ defined by $\sigma \mapsto \sigma|_F$ is a surjective group homomorphism and* $\ker(\rho) = \operatorname{Gal}(L/F)$. *So* $\frac{\operatorname{Gal}(L/K)}{\operatorname{Gal}(L/F)} \cong \operatorname{Gal}(F/K)$.

Proof. Kernels of group homomorphisms are normal so we know that $\operatorname{Gal}(L/F)$ is a normal subgroup. Want to show that $\sigma \in \operatorname{Gal}(L/F)$ sends F to itself. We can write $F = K(\beta)$ for some $\beta \in F$ and let $m(x) \in K[x]$ be the minimal polynomial. We know $m(x)$ splits completely in F so $m(x)$ has roots $\beta_1, \dots, \beta_d \in F$. Then $\sigma(F) = \sigma(K(\beta)) = K(\sigma(\beta))$ We claim that $\sigma(\beta)$ has to be one of the β_is. We proved that if you have a field automorphism that fixed K it has to send a root to another root (Recall we proved this with $\sigma(m(\beta) = 0)) = m(\sigma(\beta)) = 0$. Also $K(\beta_i) = F$. So we've shown $\sigma(F) = F$.

Now we're claiming the restriction is a group homomorphism. There's not much content to that. The surjective part though, we've got more to work with there. We'll get it surjective by proving the quotient is the right side. Say $H = \operatorname{im}(\rho)$. Then $\ker(\rho) = \{\sigma \in \operatorname{Gal}(L/K) \mid \sigma|_F = 1\}$. This means $\sigma(a) = a$ for all $a \in F$. But that's the definition of $\operatorname{Gal}(L/F)$. So $\ker(\rho) = \operatorname{Gal}(L/F)$. So by the fundamental isomorphism theorem for groups, $H \cong \frac{\operatorname{Gal}(L/K)}{\operatorname{Gal}(L/F)}$. Then $|H| = \frac{|\operatorname{Gal}(L/K)|}{|\operatorname{Gal}(L/F)|} = \frac{[L:K]}{[L:F]} = [F : K] = |\operatorname{Gal}(F/K)|$. Therefore $H = \operatorname{Gal}(F/K)$. $\square$

21 Lecture 21

Last time we proved the first Galois Correspondence. Let's review this theorem. There's a correspondence between intermediate fields in a Galois extension and the subgroups of a Galois group. More precisely the theorem says not only do the sets have the same size, but there's a natural way to go back and forth between them. So if we have an intermediate field F of L we can get a subgroup just but looking at $\operatorname{Gal}(L/F)$.

We're working up to the second part of the Galois Correspondence which will tell us somsething about intermediate extensions which are Galois over K. Look at the proposition from last time. Think of the quotient group like fractions and go "off of vibes."

Definition 21.1. Suppose we have $K \subseteq F \subseteq L$ and $\sigma \in \operatorname{Gal}(L/K)$. Then $\sigma(F)$ is a field and $K \subseteq \sigma(F) \subseteq L$. Walk through why this is the case .... We call σF a **conjugate field** of F.

Proposition 21.2. *Let L/K be Galois and $K \subseteq F \subseteq L$, and $\sigma \in \operatorname{Gal}(L/K)$. Claim* $\operatorname{Gal}(L/\sigma F) = \sigma \operatorname{Gal}(L/F)\sigma^{-1}$. *These are conjugate subgroups.*

Proof. Let $\tau \in \operatorname{Gal}(L/F)$. Want to show $(\sigma\tau\sigma^{-1})\sigma(a) = \sigma\tau a = \sigma(a)$ which is what we wanted to show. Therefore $\sigma\tau\sigma^{-1} \in \operatorname{Gal}(L/\sigma F)$. So $\sigma \operatorname{Gal}(L/F)\sigma^{-1} \subseteq \operatorname{Gal}(L/\sigma F)$.

For the other direction, $|\sigma \operatorname{Gal}(L/F)\sigma^{-1}| = |\operatorname{Gal}(L/F)| = [L : F]$. On the other hand, $|Gal(L/\sigma F)| = [L : \sigma F]$. Claim that $[F : K] = [\sigma F : K]$. Oh no another diagram. σ is a K-automorphism. σ is an isomorphism between F and σF. Why? Because reasons.

$$[L:F] = \frac{[L:K]^\sigma}{[F:K]} = \frac{L:K}{[\sigma F:K]} = [L:\sigma F.]$$

Therefore $\mathrm{Gal}(L/\sigma F) = \sigma \,\mathrm{Gal}(L/F)\sigma^{-1}$. □

Proposition 21.3. *Let L/K be a finite separable extension. Then*

1. $|\,\mathrm{Gal}(L/K)| \leq [L:K]$
2. $|\,\mathrm{Gal}(L/K)| = [L:K]$ *iff L/K Galois.*

Proof.

1. Let $L = K(\beta)$. Suppose that $m(x)$ is the minimal polynomial of β and let $d = \deg m(x) = [L:K]$. If $\sigma \in \mathrm{Gal}(L/K)$ it's completely determined by $\sigma(\beta)$. We have at most d choices. Therefore $|\,\mathrm{Gal}(L/K)| \leq [L:K]$.
2. Suppose that $\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_2, \dots, \sigma_d\}$. So $\sigma_1(\beta), \sigma_2(\beta), \sigma_d(\beta)$ are d distinct roots of $m(x)$ in L. In particular this tells us that $m(x)$ splits completely over L. Therefore L splitting field of $m(x)$. Thus L/K Galois.

□

Theorem 21.4 (Galois Correspondence II)**.** *Let L/K be Galois and suppose that $K \subseteq F \subseteq L$. Then F/K is Galois iff* $\mathrm{Gal}(L/K)$ *is normal in* $\mathrm{Gal}(L/K)$*.*

Proof. Last time we proved the forward direction. Goal is to show $\rho\colon \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ defined by $\sigma \mapsto \sigma|_F$ is well defined. We need to show the restrictionr really is an element of $\mathrm{Gal}(F/K)$. If we look at $\mathrm{Gal}(L/\sigma(F)) = \sigma \,\mathrm{Gal}(L/F)\sigma^{-1} = \mathrm{Gal}(L/F)$ (because normal subgroup—you're equal to all your conjugates). So then

$$L^{\mathrm{Gal}(L/\sigma F)} = L^{\mathrm{Gal}(L/F)} = F.$$

Image of ρ is isomorphic to

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)} \cong \mathrm{Im}(\rho) \subseteq \mathrm{Gal}(F/K).$$

But

$$\left|\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/F)}\right| = \frac{|\,\mathrm{Gal}(L/K)|}{|\,\mathrm{Gal}(L/F)|} = \frac{[L:K]}{[L:F]} = [F:K].$$

Therefore $[F:K] \leq |\,\mathrm{Gal}(F/K)| \leq [F:K]$. Therefore $|Gal(F/K)| = [F:K]$. Thus F/K Galois. □

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}) \cong \mathrm{AGL}_1(\mathbb{F}_p) = \{ax + b \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p\}.$$

$\sigma_{a,b} \leftrightarrow ax + b$

We had this extension and when we were proving things about it we were looking at a commutative diagram. What are the normal subgroups of $\mathrm{AGL}_1(\mathbb{F}_p)$? It's not obvious. But Trevor knows the answer. There's only one nontrivial normal subgroup: the entire group.

22 Lecture 22

Last time we finished the proof for the second part of the Galois correspondence.

$L_p = \mathbb{Q}(\sqrt[p]{2}, 3_p)/\mathbb{Q}$.

Galois of degree $p(p-1)$. $\mathrm{Gal}(L_p/\mathbb{Q}) \cong \mathrm{AGL}_1(\mathbb{F}_p)$

$\sigma_{a,b}(\alpha_p) = \zeta_p^b \alpha_p$.

$\sigma_{a,b}(3_p) = 3_p^a$.

To make things concrete let $p = 7$. What is degree of $L_7/\mathbb{Q}$. It's 42. So in theory we like primitive elements because they make proofs easier but in practice we use multiple generators of smaller degree. Let's take a subgroup of the Galois group and let's try to figure out its fixed field. Let $H = \langle \sigma_{2,1} \rangle \cong \langle 2x+1 \rangle \subseteq \mathrm{AGL}_1(\mathbb{F}_7)$. We claim we can figure out the degree of $L_7^H/\mathbb{Q}$. What does GC tell us about L_7/L_7^H well it's degree $|H|$. What is the order of a cyclic subgroup? You just keep composing the elements until you get the identity. $H = \{\sigma_{1,0}, \sigma_{2,1}, \sigma_{2,1}^2 = \sigma_{4,3}\}$. So $|H| = 3$. Let's find the generators of $L_7^H/\mathbb{Q}$. It has to be something fixed by H, or fixed by $\sigma_{2,1}$. What we can do is start by picking any element we want and take its orbit under the subgroup. Say ζ_7. If we apply $\sigma_{2,1}(\zeta_7) = \zeta_7^2$ we know ζ_7 is not in the fixed field. Take $\sigma_{4,3}(\zeta_7) = \zeta_7^4$. So now we have an orbit under the action. Now take a symmetric polynomial in the orbit: $\beta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. We claim that this is fixed by H. Just expand it. This means $\beta \in L_7^H$. Is β rational? It's not obvious. We're going to prove it's not rational.

$\alpha_7 = \sqrt[7]{2}$.

[Got distracted.]

We're going to show $[\mathbb{Q}(\beta, \zeta_7^{-1}\alpha_7) : \mathbb{Q}] = 14$ which is equivalent to $L_7^H = \mathbb{Q}(\beta, \zeta_7^{-1}\alpha_7)$.

Drawing some more field diagrams.

$x^7 - 2 \in \mathbb{Q}[x]$. Why is it irreducible? Because S–E criterion. So x^7-2 is the minimal polynomial. So it tells us $[\mathbb{Q}(\zeta_7^{-1}\alpha_7) : \mathbb{Q}] = 7$. Now we look at $[\mathbb{Q}(\beta) : \mathbb{Q}]$. Recall that $\beta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. Notice that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\zeta_7)$. So we have $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$. So the degree of $\mathbb{Q}(\beta)/\mathbb{Q}$ is either 1 or 2. If the degree were 1 then β would be rational. We claim β is not rational. Suppose for contradiction that $\beta \in \mathbb{Q}$. Then we can get a contradiction about the minimal polynomial of ζ_7 by considering $x^4 + x^2 + x - \beta \in \mathbb{Q}[x]$ and ζ_7 is a root. Contradiction of minimal polynomial. So the degree is 2. Thus $L_7^H = \mathbb{Q}(\zeta_7^{-1}\alpha_7, \beta)$.

That was a fun example

Observe that $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_7) \subseteq L_7$. We claim $\mathbb{Q}(\zeta_7)$ is Galois. Why? We claim that $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ is a splitting field because we can write out all the roots in terms of ζ_7. By the Galois correspondence this tells us that $\mathrm{Gal}(L_7/\mathbb{Q}(\zeta_7))$ is a normal subgroup of $\mathrm{Gal}(L_7/\mathbb{Q})$. What subgroup is it? Suppose $\sigma_{a,b}$ fixes ζ_7. Then $\zeta_7 = \sigma_{a,b}(\zeta_7) = \zeta_7^a$ iff $a \equiv 1 \pmod 7$. This implies $\mathrm{Gal}(L_7/\mathbb{Q}(\zeta_7)) = \{\sigma_{1,b} \mid b \in \mathbb{F}_2\} \cong \{x + b \mid b \in \mathbb{F}_7\}$. Why is this a normal subgroup? Let's try it out. It suffices to show that the subgroup is stable under translations and dilations separately. The translations form a commutative subgroup. You can also write it out with the dilations.

And I got very distracted by an update.

23 Lecture 23

For this last week we're going to do a big picture discussion about some important theorems in Galois Theory. We're not going to be able to prove everything. But the most important is the Galois correspondence which we already know.

23.1 Solvability by Radicals

We've known how to solve quadratic equations, $x^2+bx+c=0$, for a very long time. The quadratic formula:

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

It's a little bit of a cheat though because we've reduced one polynomial to another polynomial (the square root). Reduced to $x^2-d=0$. Solution is $\pm\sqrt{d}$. We know a lot of algorithms for estimating roots, so we consider these to be known.

In general, $x^n-d=0$ and $x=\sqrt[n]{d}$. Can we do this for $n \neq 2$?

Theorem 23.1 (Cardano–Tartaglia, ≈ 1539)**.** *Solved cubic by radicals. You probably haven't seen this formula because it's pretty complicated. First we reduce to $x^3+bx+c=0$, a depressed cubic (no quadratic term). We can get rid of this by a linear change of coordinates. Here's one root:*

$$x = \sqrt[3]{-\frac{c}{2}+\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}} + \sqrt[3]{-\frac{c}{2}-\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}.$$

This is a solution by radicals. Back then they didn't know about complex numbers so this was kinda confusing. The complex parts cancel out sometimes which made them even more confused. Why do we need imaginary numbers? This is why.

Quartic formula? Yes.

Theorem 23.2 (Ferrari, ≈ 1545)**.** *Solved general quartic by radicals.*

This is not easy.

Question 23.3. Can we solve quintics by radicals?

Question 23.4. Where do these formulas come from?

Not everybody even believed in negative numbers at this time (might be wrong). So they had entire books about how to solve equations without negative numbers. That's silly. Let's not judge them too hard tho.

Back in the day people thought math was describing something that actually had to exist. Now we're making up things left and right. Back then you had to discover stuff.

Theorem 23.5 (Abel, 1824)**.** *Not every quintic is not solvable by radicals.*

Here's an example of one that cannot be solved by radicals: $x^5+x+1=0$.

A little bit later Galois came along and translated these questions about radicals into questions about groups using the Galois correspondence. Turns out that the Galois group of a polynomial's splitting field (over $\mathbb{Q}$) completely determines if it can be solved by radicals. In practice you use gradient descent algorithms to find the roots.

How to translate this problem into a problem about field theory.

Caveat: all fields are char 0 for us!

Definition 23.6. We say that L/K finite extension is **radical** if $K=F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = L$ and $\alpha_i \in F_i$ and $m_i \in \mathbb{Z}$ such that $\alpha_i^{m_i} \in F_{n-1}$ and $F_i(\alpha_i) = F_{i+1}$.

Example 23.7. $\mathbb{Q}(\sqrt[3]{2+\sqrt{3}})/\mathbb{Q}$ is radical:

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

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{2+\sqrt{3}})$. This shows that the extension is radical.

Definition 23.8. We say L/K is **solvable** if $L \subseteq M$ where M/K is radical.

Definition 23.9. let $m(x) \in K[x]$ be irreducible and α a root of $m(x)$ in L/K. Then we say that $m(x)$ is **solvable by radicals** if $K(\alpha)/K$ is a solvable extension.

Theorem 23.10. *If $m(x) \in K[x]$ is irreducible with splitting field L/K, then $m(x)$ is solvable by radicals iff L/K is a solvable extension.*

We've reduced solvability of $m(x)$ to solvability of L/K.

We want to translate this property of solvability from fields extensions to something about subgroups.

23.2 Composition Series & Solvable Groups

Let G be a finite group.

Definition 23.11.

1. G is **simple** if the only normal subgroups of G are the trivial group and G itself.
2. A sequence of subgroups $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_k = G$ is called a **composition series** if N_{i+1}/N_i are all simple. We call N_{i+1}/N_i the **composition factors** of G.

Theorem 23.12 (Jordan-Hölder)**.** *For all finite groups G, the composition factors are unique up to isomorphism and permutation. That is, they're independent of the series.*

So potentially you could take a group and find multiple composition series, but this theorem says you'll get the same sequence of groups up to isomorphism, possibly in a different order. You can think of this like unique factorization for groups. In fact, it's a strict generalization.

Example 23.13. Let's say our group is S_3. How big is this? 6. We want find a composition series for S_3.

$$1 \triangleleft \langle (123) \rangle \triangleleft S_3.$$

We need to check that the quotients are all simple groups. In this case it's pretty easy because $S_3/\langle(123)\rangle \cong C_2$ (C_p is simple for primes p.). If we take this group modulo the trivial group we get itself, which is also simple.

$C_6 = \langle \sigma \rangle$
$1 \triangleleft \langle \sigma^2 \rangle \triangleleft C_6$.
$C_6/\langle \sigma^2 \rangle \cong C_2$
$\langle \sigma^2 \rangle / 1 \cong C_3$.
The glueing is the complicated part.

Definition 23.14. G is **solvable** if all the composition factors of G are C_p for primes p.