MAT347

Groups, Rings, and Fields

Class Lecture Notes

Notes by:

Emerald (Emmy) Gu

September 4, 2024

Last Updated:

November 6, 2025

Primary source material:

Class Lectures

Prof. Joe Repka

Contents

Preface

These notes were created during class lectures. As such, they may be incomplete or lacking in some detail at parts, and may contain confusing typos due to time-sensitivity. Additionally, these notes may not be comprehensive. Most statements in this document which are not Theorems, Problems, Lemmas, Corollaries, or similar, are likely paraphrased to a certain degree. Please do not treat any material in this document as the exact words of the original lecturer.

If you are viewing this document in Obsidian, you may notice that the links in the pdf document do not work. This is intentional behaviour, as I currently do not have or know of a decent solution which allows them to behave well with the setup in Obsidian. However, below certain pages, there may be links to other documents - these are usually context-relevant links between notes of different areas of study. I created these links to point out potential similarities, or in case one area of study is borrowing a concept, definition, or theorem from another area of study, and you wish to see the full, original definition/derivation/proof or whatever it may be.

I Groups

1 Actions

Lec 3 - Sept 11 (Week 2)

Definition 1.1

A group G is said "to have an action on X" or "to act on X", and X is said "to be acted on by G", if there is a map $\varphi : G \times X \to X$ which satisfies:

- $\varphi(e, x) = x$
- $\varphi(gh, x) = \varphi(g, hx)$

for all $x \in X$, $g, h \in G$.

Note that the left action maps $(g, x) \to gx$.

Example

- $\mathrm{GL}_3(\mathbb{R})$ acts on $\mathbb{R}^3$
- $\mathrm{SL}_3(\mathbb{R})$ acts on $\mathbb{R}^3$ by rotations and reflections
- $\mathrm{SO}_3(\mathbb{R})$ acts on $\mathbb{R}^3$ by rotations, but also acts on the sphere of radius r about the origin

Source: Primary Source Material

Note the definition above is specifically for *left* actions - right group actions *do not work*. This is because it fails the associativity axiom! We can fix it by mapping $(g, x) \to xg^{-1}$ instead.

Example

We can think of $\mathrm{SO}_2 < \mathrm{SO}_3$ as rotations around the earth's poles.

Indeed, if you pick a point and draw it after being acted on, you get the latitude lines. The two exceptions are the points at the poles themselves.

Source: Primary Source Material

Definition 1.2

The **orbit** of $x \in X$ under G is $Gx = \mathrm{orb}(x) = \{gx : g \in G\}$.

Lec 4 - Sept 13 (Week 2)

“get rotated” me to a square today

Corollary

Suppose G is a group. Then G acts on itself if $X = G$.
The group action then becomes a function $G \times G \to G$.

If the action is a left action, it is called a **left translation**, sometimes denoted as

$$L_g x = L_g(x) = gx$$

For fixed g, we get a map $G \to G$ as $x \to gx$. We can denote a **right translation** similarly.

We consider one more action:

$$C_g(x) = L_g R_g = R_g L_g(x) = gxg^{-1}$$

This is called *conjugation* by g.

Definition 1.3

Suppose G acts on X. For fixed $x \in X$, the **stabilizer** of x is:

$$\text{stab}_G(x) = \{g \in G : gx = x\}$$

Note that $\text{stab}(x) \leq G$.

Consider the left coset of $\text{stab}(x)$. Then $g \cdot \text{stab}(x)$ consists of all $k \in G$ such that $kx = gx$.

Lec 5 - Sept 18 (Week 3)

Suppose that σ_g represents conjugation by g. Then, $\sigma(ab) = \sigma(a)\sigma(b)$, but note that this doesn't hold for left/right group actions in general. Also note that for any subgroup H, we have that gHg^{-1} is also a subgroup of G.

Now, consider the stabilizer of some element $h \in G$. Clearly, $g \in \text{stab}(h) \iff ghg^{-1} = h \iff gh = hg$. In other words, the stabilizer of the conjugation action is called the centralizer.

Some examples of centers:

- The center of D_3 is trivial, but the center of $D_4 = \left\{e, \rho^2\right\}$.
- The center of Q_8 is given as $\{1, -1\}$.
- The center of $\text{GL}_n(\mathbb{F}) = \{cI\} \, \forall \, c \in \mathbb{F}$.
- The center of $\text{SL}_n(\mathbb{C}) = \{cI : c^n = 1\} \, \forall \, c \in \mathbb{C}$. Notice that c is given by the n-th roots of unity.

Clearly, centers can be subtle.

yaaaay quotient groups :)

okay heres something i should try and prove cause its just. weird to me

Lemma

Suppose $H \leq G$, and $x, y \in G$.

Show that $xH = yH$ if and only if $y \in xH$.

Proof.

($\Longleftarrow$) Suppose that $y \in xH$. We want to show that $yH = xH$.

Since $y \in xH$, then $y = xh$ for some $h \in H$. Notice that $yH = xhH$. We see that:

$$\begin{aligned} & a \in xhH \\ \implies & a = xhh' \\ \implies & a \in xH \end{aligned}$$

So we see that $yH \subseteq xH$. We also see that $y = xh \implies yh^{-1} = x \implies x \in yH$. So by a similar argument, we also have that $xH \subseteq yH$, so they indeed must be equal.

($\implies$) Suppose $yH = xH$. To see that $y \in xH$, notice that for some $h, h' \in H$:

$$\begin{aligned} & yh = xh' \\ \implies & y = xh'h^{-1} \\ \implies & y \in xH \end{aligned}$$

So clearly $y \in xH$ as needed. ■

2 Homomorphisms

Lec 6 - Sept 20 (Week 3)

some definitions include homomorphism, kernel, image, etc. some proofs that theyre subgroups. etc etc. inj iff trivial kernel. the works. no FIT tho lol

Example

Suppose $H = \mathrm{GL}_n(\mathbb{F}), G = \mathbb{F}^\times$. Consider $\varphi : H \to G$ as $g \to \det(g)$.

Then, $\mathrm{im}(\varphi) = \mathbb{F}^\times$, and $\ker(\varphi) = \mathrm{SL}_n(\mathbb{F})$. The group $H/\ker(\varphi) = \mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F})$ is a quotient group, where each class is given by a possible value of the determinant. A representative of an equivalence class looks like:

$$\det \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = t \in \mathbb{F}^\times$$

Source: Primary Source Material

Example

Consider $H = D_3$. Then $\varphi : H \to \mathbb{Z}/2\mathbb{Z}$ given by:

$$\begin{aligned} \text{rotation } &\to 0 \\ \text{reflection } &\to 1 \end{aligned}$$

Here, $\text{im}(\varphi) = G$, and $\ker(\varphi) = \text{rotations}$.

Source: Primary Source Material

Lec 7 - Sept 25 (Week 4)

Given a symmetry φ, it must take vertex 1 to some vertex k. Then, 2 must go to $k-1$ or $k+1$. The positions of two adjacent points determine φ uniquely. So, there are exactly $2n$ symmetries (including e).

Let ρ be the rotation through $\frac{2\pi}{n}$, and σ be the reflection that fixes 1. Then the symmetry group is:

$$\left\{e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \ldots, \rho^{n-1}\sigma\right\}$$

We call this group D_{2n}. yk, the **bad** convention.

Definition 2.1

Suppose G is a group and $A \subseteq G$ is a subset. We define the **normalizer** of A in G as:

$$N_G(A) = \left\{g \in G : gAg^{-1} = A\right\}$$

If G is finite, then this is equivalent to:

$$N_G(A) = \left\{g \in G : gag^{-1} \in A, a \in A\right\}$$

Furthermore, if G is finite, then the normalizer is closed under inverses.

Consider the group:

$$G = \left\{\begin{pmatrix} 1 & x \\ 0 & r \end{pmatrix}\right\} : x \in \mathbb{C}, r \in \mathbb{Q}^\times$$

We see that:

$$\begin{pmatrix} 1 & x \\ 0 & r \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & s \end{pmatrix} = \begin{pmatrix} 1 & y + xs \\ 0 & rs \end{pmatrix}$$

$$\begin{pmatrix} 1 & x \\ 0 & r \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \frac{-x}{r} \\ 0 & r^{-1} \end{pmatrix}$$

So it is indeed a group. Now, consider the subgroup:

$$A = \left\{\begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\} < G$$

We see that:

$$g = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad g^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

$$g \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

So then $gAg^{-1} \not\subseteq A$. However:

$$h = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \quad h^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

$$h \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} h^{-1} = \begin{pmatrix} 1 & 4n \\ 0 & 1 \end{pmatrix}$$

So we see that h satisfies $hAh^{-1} \subseteq A$, but it does not satisfy $hAh^{-1} = A$. We don't want h to be in the normalizer, since it would not be a group. Specifically, $h = g^{-1}$. So we would have h in the normalizer, but not h^{-1}, thereby not allowing it to be a group.

Exercise 2.1

Show that with the correct definition, $N_G(A)$ is a subgroup of G.

Source: Primary Source Material

Let $N \trianglelefteq G$. Consider the map $p : G \to G/N$ given by $P(x) = xN$. We see that:

$$p(xy) = xyN = xNyN = p(x)p(y)$$

$$p(x^{-1}) = x^{-1}N = (xN)^{-1} = (p(x))^{-1}$$

Therefore, p is a homomorphism. Furthermore, p is clearly surjective, since any coset xN is the image of some x. We also see that:

$$\ker(p) = \left\{x : p(x) = e_{G/N}\right\} = \{x : p(x) = eN = N\} = N$$

So we have a surjective map $p : G \to G/N$, and has kernel N. We call p the **projection** of G onto G/N.

Consider a homomorphism $\varphi : G \to H$, and write $K = \operatorname{im}(\varphi)$. We can write $\varphi : G \to K \leq H$. We claim that there is a map $\overline{\varphi} : G/\ker(\varphi) \to \operatorname{im}(\varphi)$. We define:

$$\overline{\varphi}(g \cdot \ker\varphi) = \varphi(g)$$

We show that $\overline{\varphi}$ is well-defined. Suppose $g \cdot \ker(\varphi) = g' \cdot \ker(\varphi)$. Then $g' = gk$ for some $k \in \ker(\varphi)$. So, it follows that $\varphi(g') = \varphi(gk) = \varphi(g)\,\varphi(k) = \varphi(g)e = \varphi(g)$. Next, we verify that $\varphi(g) = \overline{\varphi}(p(g))$. Indeed:

$$\overline{\varphi}(p(g)) = \overline{(\varphi)}(g \cdot \ker\varphi) = \varphi(g)$$

Notice that $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$. The kernel is given by:

$$\ker(\overline{\varphi}) = \{g \cdot \ker(\varphi) : \varphi(g) = e\} = \ker(\varphi)$$

Since $\overline{\varphi}$ is defined on $G/\ker(\varphi)$, then we see that $\ker(\varphi) = e \cdot \ker(\varphi)$ is the identity element. Therefore, $\overline{\varphi}$ has trivial kernel, and thus is injective.

Since $\overline{\varphi}$ is both injective and surjective, it is thus an isomorphism.

Theorem 2.1: First Isomorphism Theorem

Suppose $\varphi : G \to K$ is a group homomorphism.

Then, there exists an isomorphism $\overline{\varphi} : G/\ker(\varphi) \to \operatorname{im}(\varphi)$, given by $\overline{\varphi}(g \cdot \ker(\varphi)) = \varphi(g)$.

We often write $G/\ker(\varphi) \cong \operatorname{im}(\varphi)$ or $G/\ker(\varphi) \simeq \operatorname{im}(\varphi)$.

Example

Suppose $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Clearly, $\ker(\varphi) = m\mathbb{Z}$, and $\operatorname{im}(\varphi) = \mathbb{Z}/m\mathbb{Z}$. Then, the theorem in this case says that:

$$\begin{aligned} &\mathbb{Z}/\ker(\varphi) \simeq \mathbb{Z}/m\mathbb{Z} \\ \implies\quad &\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

This isn't stupid. Promise.

Source: Primary Source Material

Example

Let G be the triangle group. Define $\chi : G \to \{1, -1\}$, where:

$$\begin{aligned} \chi(\text{rotation}) &= 1 \\ \chi(\text{reflection}) &= -1 \end{aligned}$$

It can be verified that χ is indeed a homomorphism. Here, $\ker(\chi) = \{\text{rotations}\}$. Then, $G/\text{rotations} \simeq \{1, -1\}$. In particular, χ distinguishes rotations from reflections.

Source: Primary Source Material

Example

Another silly example is the trivial homomorphism $\psi : G \to G$, given by $\psi(g) = e$.

Here, $\ker(\psi) = G$, so $G/G \simeq \{e\}$. Okay, this one is pretty stupid.

Source: Primary Source Material

Example

Consider $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\times$. Here, $\ker(\det) = \mathrm{SL}_n\,\mathbb{F}$, and so $\mathrm{GL}_n\,\mathbb{F}/\mathrm{SL}_n\,\mathbb{F} \simeq \mathbb{F}^\times$.

If $g \in \mathrm{GL}_n\,\mathbb{F}$, then we can define h as:

$$h = \begin{pmatrix} \frac{1}{\det(g)} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ddots & 1 \end{pmatrix}$$

Then, $hg \in \mathrm{SL}_n\,\mathbb{F}$. In this case, we can think of h as the representation of an element of $\mathbb{F}^\times$.

Source: Primary Source Material

Lec 9 - Sept 27 (Week 5)

We call a homomorphism $\varphi : G \to G$ which is bijective an automorphism. Is it obvious that the inverse is a homomorphism? Yes. Yes it is.

We call conjugation an "inner automorphism". Denote aut as grp of automorphisms, inn similarly.

Example

If $G = \mathrm{GL}_n(\mathbb{F})$, define a homomorphism $\varphi(g) = (g^t)^{-1}$. We see that:

$$\det(\varphi(g)) = \det\left(g^t\right)^{-1} = \det(g)^{-1}$$

But:

$$\det\left(xgx^{-1}\right) = \det(x)\det(g)\det\left(x^{-1}\right) = \det(g)$$

So φ cannot be an inner automorphism. As an exercise, is φ an inner automorphism of $\mathrm{SL}_n \mathbb{F}$?

Source: Primary Source Material

Let $H, N \leq G$, and $H \leq N_G(N)$, then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G. A proposition is as follows: $N \trianglelefteq HN$.

Indeed, let $n_1 \in N$, $h \in H, n_2 \in N$. Then:

$$hn_2n_1n_2^{-1}h^{-1} = hn_3h^{-1} \in N$$

Another proposition: $H \cap N \trianglelefteq H$. To see this, suppose that $x \in H \cap N, h \in H$. Then:

$$hxh^{-1} \in H \quad hxh^{-1} \in N$$

So, since these are normal subgroups, we can take their quotients!

Theorem 2.2: Second Isomorphism Theorem (Diamond Isomorphism Theorem)

Let G be a group, and $H, N \leq G$ such that $H \leq N_G(N)$. Then:

$$HN/N \simeq H/H \cap N$$

Proof.

Try mapping $H \to HN/N$ as $h \to hN$. If we want to use the First Isomorphism Theorem, we should find its kernel and image. Indeed, $\ker(\varphi) = H \cap N$, and the image of φ is:

$$\mathrm{im}(\varphi) = \{\varphi(h) : h \in H\} = \{hN : h \in H\}$$

But notice that:

$$HN/N = \{hnN : h \in H, n \in N\} = \{hN : h \in H\}$$

Therefore, by the First Isomorphism Theorem, we have that:

$$H/\ker(\varphi) \simeq \mathrm{im}(\varphi) = HN/N$$

■

Source: Primary Source Material

We include a picture of the Second Isomorphism Theorem to help visualize it:

[picture here]

In the case that $N \leq N_G(H)$, then the other diagonals are true! In the event that both subgroups are normal, then both pairs hold, but they are not necessarily pairwise isomorphic.

Lec 9 - Oct 2

Theorem 2.3: Third Isomorphism Theorem

Suppose $H \leq G, K \leq H, K(H?) \trianglelefteq G$. Then, $K \trianglelefteq H$, and $H/K \trianglelefteq G/K$. Furthermore:

$$(G/K)/(H/K) \simeq G/H$$

If we write $\overline{G} = G/K, \overline{H} = H/K$, then $\overline{G}/\overline{H} \simeq G/H$.

Example

Let $G = \mathbb{Z}, H = 3\mathbb{Z}, K = 12\mathbb{Z}$. Then, $\overline{G} = \mathbb{Z}/12\mathbb{Z}, \overline{H} = 3\mathbb{Z}/12\mathbb{Z}$, and $\overline{G}/\overline{H} \simeq \mathbb{Z}/3\mathbb{Z}$.

To see this more clearly, note that:

$$\begin{gathered}\mathbb{Z}/12\mathbb{Z} = \{0,1,2,3,4,5,6,7,8,9,10,11\}\\ \mathbb{Z}/3\mathbb{Z} = \{0,1,2\}\\ 3\mathbb{Z}/12\mathbb{Z} = \{0,3,6,9\}\\ (\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) = \{0,1,2\}\end{gathered}$$

Source: Primary Source Material

Proof.

Define a homomorphism $\varphi : G/K \to G/H$, by:

$$gK \to gH$$

We first show that φ is well-defined. Suppose $gK = g'K$. Then:

$$\begin{aligned} & g = g'k && \text{for some } k \in K \\ \implies & \varphi(gK) = gH = g'kH && \\ & \varphi(g'K) = g'H && \\ \implies & \varphi(gK) = \varphi(g'K) && \text{since } k \in K \leq H \end{aligned}$$

We see that $\text{im}(\varphi) = G/H$, since any gH comes from gK. Furthermore, the kernel is given by:

$$\ker(\varphi) = \{gK : \varphi(gK) = e = eH\} = \{gK : g \in H\} = H/K$$

Therefore, by the first isomorphism theorem, we are done. ■

Source: Primary Source Material

Theorem 2.4: Fourth Isomorphism Theorem

Suppose $N \trianglelefteq G$. Suppose $H_1, H_2, \ldots, H_n \leq G$ are subgroups such that $N \leq H_i$. Then:

- $H_i \leq H_j \iff H_i/N \leq H_j/N$
- $H_i \trianglelefteq H_j \iff H_i/N \trianglelefteq H_j/N$
- $H_i \cap J_j \longleftrightarrow H_i/N \cap H_j/N$
- $\langle H_i, H_j \rangle \longleftrightarrow \langle H_i/N, H_j/N \rangle$
- If $H_i \trianglelefteq H_j$, then $(H_j/H_i)/N = (H_j/N)/(H_i/N)$

In other words, the subgroup lattice of G of only subgroups containing N is isomorphic (as a lattice) to the subgroup lattice of G/N.

Proof.

exercise :) ■

Something we missed: If H, G are groups, then the product group is given as:

$$H \times G = \{(h, g) : h \in H, g \in G\}$$

where:

$$(h, g)(h', g') = (hh', gg')$$

$$(h, g)^{-1} = (h^{-1}, g^{-1})$$

and the identity is given as $(e, e) = (e_H, e_G)$. Obviously, $|H \times G| = |H||G|$.

Example

Suppose $H = G = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. Then:

$$H \times G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(x, y) : x, y \in \mathbb{Z}/2\mathbb{Z}\}$$

Note that $|H \times G| = 4$. Is this isomorphic to $\mathbb{Z}/4\mathbb{Z}$?

In $H \times G$, we see that $(x, y)^2 = (2x, 2y) = (0, 0)$. So clearly, every element has order 1 or 2.

However, in $\mathbb{Z}/4\mathbb{Z}$, there are two elements of order 4. Therefore, they aren't isomorphic.

Source: Primary Source Material

The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is special, and is named the **"Klein 4-group"** after its discoverer, Felix Klein.

For product groups, we say we perform the operation **component-wise**.

3 Symmetric Group

Definition 3.1

Consider permutations of n objects, such as $1, 2, \ldots, n$.

One way to write them is as:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

where each element is permuted to the one below it. We can also write it explicitly:

$$1 \to 2 \quad 2 \to 3 \quad 3 \to 4 \quad 4 \to 1 \quad 5 \to 5$$

The set of all permutations of n objects is a group under composition, called the **symmetric group** S_n of n objects. The order is given by $|S_n| = n!$.

Another way to write permutations relies on cycles: the permutation (27145) takes 2 to 7, 7 to 1, 1 to 4, 4 to 5, and 5 to 2.

$$(27145) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 5 & 2 & 6 & 1 \end{pmatrix}$$

As in function composition, we apply permutations from right-to-left.

$$\begin{aligned} (1243)(215) &= (1543) \\ (215)(1243) &= (2435) \end{aligned}$$

Some conventions:

- Since a cycle can be written in different ways, we usually start with the smallest number.
- We call a cycle with 2 elements a "transposition".

Note that not every permutation can be written in a single cycle, such as (123)(45). We see that these cycles don't have any elements in common, so we call them *disjoint* cycles.

Corollary

Any permutation can be written as a product of disjoint cycles.

Our example from earlier shows us that in general, permutations do not commute. However, *disjoint* cycles do commute.

Clearly, the inverse of a cycle is the reverse cycle. The inverse of a product of disjoint cycles is the product of the inverses, and the order of the cycles does not matter.

Consider (1234). Notice that $(1234) = (14)(13)(12)$. This generalizes; any cycle can be written as a product of transpositions.

Corollary

Any permutation can be written as a product of transpositions, in infinitely many ways.

We want to consider the parity of a permutation, i.e. the parity of the number of transpositions.

Consider the following polynomials in n variables $x_1, \ldots, x_n$:

$$\Delta = \prod_{i>j}(x_i - x_j)$$

Given a permutation σ, we let σ act on the variables $x_i \mapsto x_{\sigma(i)}$:

$$\sigma\Delta = \prod_{i>j}(x_{\sigma(i)} - x_{\sigma(j)})$$

Then each factor is either $x_k - x_\ell$ with $k > \ell$, or $x_k - x_\ell$ with $k < \ell$. Therefore, the factors of $\sigma\Delta$ are each ± 1 of the factors of Δ, and so $\sigma\Delta = \pm\Delta$. How many pairs of indices does σ turn around - that is, $i > j$ and $\sigma(i) < \sigma(j)$?

The parity of this number determines the sign in $\sigma\Delta = \pm\Delta$, so it is well-defined. Note that this is entirely determined by σ, with no reference to the number of transpositions.

Lec 10 - Oct 4 (Week 5)

First consider $\sigma = (ij), i > j$. The factor $(x_i - x_j)$ is reversed by $\sigma = (ij)$. Any other factor $(x_k - x_\ell)$ is preserved if $k \neq i, j$ and $\ell \neq i, j$.

Now consider $k < j$. Then, the factors $(x_j - x_k)$ and $(x_i - x_k)$ are swapped by $\sigma = (ij)$ for $k < j < i$. However, neither is changed to its negative.

If $k > i$, then $(x_k - x_j)$ and $(x_k - x_i)$ are swapped, but again the signs don't change.

Finally, consider $j < k < i$. Then, when the factors $(x_i - x_k)$ and $(x_k - x_j)$ are swapped, $\sigma = (ij)$ changes each into its negative. In this case, we get a term of $(-1)^2$. So, any transposition σ takes:

$$\Delta + \sigma\Delta = -\Delta$$

Recall that any n-cycle $(a_1 a_2 \cdots a_n)$ can be written as a product of transpositions:

$$(a_1 a_2 \cdots a_n) = \underbrace{(a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2)}_{n-1 \text{ transpositions}}$$

So if σ is an n-cycle, it changes the sign of Δ by $(-1)^{n-1}$.

Definition 3.2

Any arbitrary permutation σ can be written as a product of cycles. If

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$$

and σ_i is a cycle of length ℓ_i, then σ_i changes the sign of Δ by $(-1)^i$, and σ changes the sign of Δ by:

$$\prod_{i=1}^{r}(-1)^{\ell_i - 1}$$

This factor is called the **sign** of σ, often written $\text{sgn}(\sigma)$ or $\Sigma(\sigma)$.

Note that $\text{sgn}(\sigma)$ is well-defined in that it is independent of the choice of cycles.

Corollary

We describe the parity of σ by the parity of its sign.

In particular, (ij) is odd, and (ijk) is even.

Furthermore, the function $\Sigma : S_n \to \{-1, 1\}$ is a homomorphism.

If we have a homomorphism Σ, then we can apply the first isomorphism theorem. Indeed, $\ker(\Sigma)$ is given as the subgroup of all even permutations.

Definition 3.3

We denote by A_n the **alternating group**, which is the subgroup of S_n consisting of all even permutations.

The order is given by $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$.

Example

Consider S_5.

$$|S_5| = 120 \qquad |A_5| = 60$$

$$\begin{array}{rl}
\{e\} & 1 \\
(ab) & \binom{5}{2} = 10 \\
(abc) & \binom{5}{3} \cdot 2 = 20 \\
(abcd) & \binom{5}{4} \cdot 3 \cdot 2 = 30 \\
(abcdf) & 4! = 24 \\
(ab)(cd) & \frac{1}{2}\binom{5}{2}\binom{3}{2} = 15 \\
(abc)(df) & \binom{5}{3} \cdot 2 = 20
\end{array}$$

Indeed, we see that the sum is 120. Of these permutations, the rows $1, 3, 5$, and 6 are even permutations. Indeed, these rows sum to 60 as expected.

Source: Primary Source Material

Suppose $\sigma, \tau \in S_n$. What is $\tau\sigma\tau^{-1}$?

$$\begin{array}{ccc}
\tau & \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau_1 & \tau_2 & \cdots & \tau_n \end{pmatrix} & \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau_1 & \tau_2 & \cdots & \tau_n \end{pmatrix} \\
\sigma & \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} & \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau_1) & \sigma(\tau_2) & \cdots & \sigma(\tau_n) \end{pmatrix} \\
\tau^{-1} & \begin{pmatrix} \tau_1 & \tau_2 & \cdots & \tau_n \\ 1 & 2 & \cdots & n \end{pmatrix} & \begin{pmatrix} \sigma(\tau_1) & \sigma(\tau_2) & \cdots & \sigma(\tau_n) \\ ? & ? & \cdots & ? \end{pmatrix}
\end{array}$$

Lec 11 - Oct 9 (Week 6)

are we trying this again?

$$\begin{array}{cc}
\tau & \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau_1 & \tau_2 & \cdots & \tau_n \end{pmatrix} \\
\sigma & \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} \\
\sigma\tau^{-1} & \begin{pmatrix} \tau_1 & \tau_2 & \cdots & \tau_n \\ 1 & 2 & \cdots & n \end{pmatrix} \\
 & \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix} \\
\tau\sigma\tau^{-1} & \begin{pmatrix} \tau_1 & \tau_2 & \cdots & \tau_n \\ \tau_{\sigma_1} & \tau_{\sigma_2} & \cdots & \tau_{\sigma_n} \end{pmatrix}
\end{array}$$

In other words, $\tau\sigma\tau^{-1}$ takes τ_i to τ_{σ_i}. So H acts on $(\tau_1, \ldots, \tau_n)$ the way σ acts on $(1, \ldots, n)$. Thus, we can think of $\tau\sigma\tau^{-1}$ as "relabelling" the numbers $1, \ldots, n$ according to τ.

Example

Let $\tau = (12), \sigma = (123)$.

$$\tau\sigma\tau^{-1} = (12)(123)(12) = (12)(13) = (132) = (213)$$

So effectively, $1, 2$ is changed to $2, 1$ in σ.

Source: Primary Source Material

Example

Let $\tau = (1234), \sigma = (123)$.

$$\tau\sigma\tau^{-1} = (1234)(123)(1432) = (1234)(14) = (234)$$

Here, τ shifts all the numbers by one, and indeed σ has its cycle shifted by one.

Source: Primary Source Material

So if $\sigma = (abc \cdots m)$ is a cycle, then $\tau\sigma\tau^{-1} = (\tau(a)\tau(b)\tau(c) \cdots \tau(m))$.

This is what we mean by "relabelling" according to τ.

Observe that $\tau\sigma\tau^{-1}$ has the same cycle type as σ. So the conjugacy class of σ consists of elements that have the same cycle type

Conversely, two elements with the same cycle type are conjugate in S_n, as we can find a suitable τ to "relabel" our cycles.

Theorem 3.1

The conjugacy classes in S_n correspond to cycle types.

What about A_n, the alternating group?

Example

We have that $A_3 = \{e, (123), (132)\}$. Notice that $A_3 \lhd S_3$.

We see that $(123), (132)$ are in the same conjugacy class in S_3, but *not* in A_3 - A_3 is a cyclic, and therefore abelian, subgroup.

Source: Primary Source Material

So in general, A_n conjugacy classes are not always S_n conjugacy classes.

Returning to group actions, suppose G acts on X, both finite and $|X| = n$. Label X as $\{1, 2, 3, \ldots, n\}$. Then, the action of G on X permutes the numbers $\{1, 2, \ldots, n\}$. Therefore, there exists a homomorphism $P : G \to S_n$:

$$P_g \in S_n \qquad P_g(i) = j \iff g \cdot x_i = x_j$$

What is the kernel?

$$\ker(P) = \{g \in G : \forall x \in X, gx = x\}$$

Now, fix $x \in G$. Recall $\text{stab}_G(x) = \{g : gx = x\}$. Suppose $H \le G$, not necessarily normal. Then G acts on $X = G/H$, the coset space, by $g \cdot xH = gxH$. The map $P : G \to S_{[G:H]}$ maps g to its induced permutation on G/H. What is the kernel?

Take $x \in G$, and consider $\text{stab}_G(xH)$.

$$\begin{aligned}
\text{stab}_G(xH) &= \{g \in G : gxH = xH\} \\
&= \{g \in G : gx = xh \text{ for some } h \in H\} \\
&= \left\{g \in G : x^{-1}gx \in H\right\} \\
&= \left\{g \in G : g \in xHx^{-1}\right\}
\end{aligned}$$

This holds for any $x \in G$. And if $g \in \ker(P)$, then g must be in $\text{stab}_G(x)$ for all x. Therefore, $g \in \bigcap_{x \in X} xHx^{-1}$. Therefore:

$$\ker(P) \le \bigcap_{x \in X} xHx^{-1} \unlhd G$$

We claim that the first inequality is, in fact, an equality. This is because we can reverse the previous calculation we did to get that:

$$g \in xHx^{-1} \iff gxH = xH$$

In other words, $g \in xHx^{-1}$ for all x if and only if g acts trivially on $X = G/H$.

Example

Let $H = \{e\}$, and G acts on G. Then:

$$P : G \to S_{[G:H]}$$
$$\ker(P) = \{e\}$$

Now, applying the First Isomorphism Theorem, we have that:

$$\operatorname{im}(P) \simeq G/\ker(P) = G/\{e\} = G$$
$$\operatorname{im}(P) \leq S_{[G:H]}$$

In other words, G is isomorphic to a subgroup of the symmetric group.

Source: Primary Source Material

Theorem 3.2: Cayley's Theorem

Any group G of order n is isomorphic to a subgroup of the symmetric group S_n.

Note that $n = |G|$, and $|S_n| = n!$. So S_n is *vastly* bigger. Can we find $m < n$ such that G is isomorphic to a subgroup of S_m?

Now, suppose G acts on X. Let $x \in X, H = stab_G(x)$. Then if $h \in H$, then $hx = x$. If $u, v \in G, u = vh$, then $ux = vhx = vx$. So:

$$ux = vx \implies \forall\, u \in vH, ux = vx$$

So the action of G on X amounts to a map $G \to G/H$, and the action of G on X factors through to projection $G \to G/H$. If $uH \neq vH$, then $ux \neq vx$.

In other words, two elements of G act on $x \in X$ in the same way if and only if they are in the same coset of H. So as sets, G/H corresponds to the orbit Gx. Note that G/H is not necessarily a group.

Theorem 3.3: Orbit-Stabilizer Theorem

If G acts on X, then the orbit Gx corresponds bijectively to $G/\operatorname{stab}_G(x)$.

The map $G/\operatorname{stab}_G(x) \to Gx$ respects the action of G:

$$gu \cdot \operatorname{stab}_G(x) = g \cdot u \cdot x$$

If G is finite, then applying Lagrange's Thereom tells us that:

$$|G| = |\operatorname{orb}(x)||\operatorname{stab}_G(x)|$$

The most interesting case is the action of G on itself by conjugation. Note that the orbits of this action are precisely the conjugacy classes.

$$Gx = \left\{gxg^{-1} : g \in G\right\}$$

We want to apply the orbit-stabilizer theorem; to do this, we need to find $\operatorname{stab}_G(x)$.

$$\operatorname{stab}_G(x) = \{g \in G : gx = x\} = \left\{g \in G : gxg^{-1} = x\right\} = C_G(x)$$

So by the orbit-stabilizer theorem, the size of the conjugacy class of x is $[G : C_G(x)]$.

If $z \in Z(G)$, then $C_G(z) = G$. So the conjugacy class of x, or the orbit of x under conjugation, has size equal to $[G : G] = 1$. That is, its conjugacy class is $\{z\}$.

Suppose G is a finite group. Then, G is a union of conjugacy classes:

$$G = \bigcup_{x \in G} \left\{gxg^{-1} : g \in G\right\}$$

Clearly, if G is abelian, then this is just the union of each individual element. More generally, we have:

$$\begin{aligned} G &= \left(\bigcup_{z \in Z(G)} \{z\}\right) \cup \left(\bigcup_{x \notin Z(G)} \left\{gxg^{-1} : g \in G\right\}\right) \\ &\overset{*}{=} \left(\bigcup_{z \in Z(G)} \{z\}\right) \cup \left(\bigcup_{x \notin Z(G)} G/C_G(x)\right) \end{aligned}$$

But note that the rightmost union has many repeated sets, since multiple x's correspond to the same conjugacy class. Therefore, pick a set of representatives $x_1, \ldots, x_k$ of the non-central conjugacy classes. That is, every $x \notin Z(G)$ is conjugate to x_i for a unique i.

$$G = \left(\bigsqcup_{z \in Z(G)} \{z\} \right) \cup \left(\bigsqcup_{i=1}^{k} \{g x_i g^{-1} : ginG\} \right)$$

Since these are all disjoint unions, then:

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$$

This is known as the **Class Equation**.

Example

Let p be prime, and sps $|G| = p^m$ for some $m > 0$. Then $Z(G) \leq G$, so $|Z(G)| = p^k$ for some $k \leq m$. If $k < m$, then:

$$C_G(x_i) \neq G \quad \forall x_i$$

So each $[G : C_G(x_i)]$ is divisible by p.

Source: Primary Source Material

A group G with $|G| = p^m$ is called a ***p*-group**. These groups are fundamental to the understanding of the structure of groups.

So every term in the class equation except possibly $|Z(G)|$ is divisible by p, so $p \mid |Z(G)|$. Therefore, we conclude that $Z(G) \neq \{e\}$ for any p-group G.

4 Sylow Theorems

Lec 12 - Oct 11 (Week 6)

These are fundamental theorems, by Peter Sylow (Norwegian).

Consider S_5. We know that $|S_5| = 120 = 8 \cdot 15 = 2^3 \cdot 3 \cdot 5$.

A notational quirk: if p is prime, we say that p^a **exactly divides** n if:

- $p^a \mid n$
- $p^{a+1} \nmid n$

We write $p^a \mid\mid n$ in this case.

Theorem 4.1: First Sylow Theorem

If p is prime and $p^a \mid\mid |G|$, that is, p^a "exactly" divides $|G|$, then there is a subgroup $P \leq G$ of order p^a.

Example

Conisder $G = S_5$. We see that:

- $5 \mid 120$, and indeed $P = \langle (12345) \rangle$ is a subgroup of order 5.
- $3 \mid 120$, and indeed $P = \langle (123) \rangle$ is a subgroup of order 3.
- $2^3 \mid 120$, and indeed there is a subgroup of order 8 (find it!).

Source: Primary Source Material

Definition 4.1

If $p^a \mid\mid |G|$, then a subgroup of order p^a is called a $p-$**Sylow subgroup of** G.
We write $\text{Syl}_p(G)$ as the set of all p-Sylow subgroups, and $n_p(G) = \left|\text{Syl}_p(G)\right|$.

Theorem 4.2: Second(?) Sylow Theorem

Any p-subgroup of G is contained in a (maximal) p-Sylow subgroup.

Theorem 4.3: Third(?) Sylow Theorem

For any p, all the p-Sylow subgroups of G are conjugate, and therefore isomorphic.

Theorem 4.4: Fourth(?) Sylow Theorem

For any p, $n_p(G) \equiv 1 \bmod p$.

Example

In S_5, we see that:

$$\begin{gathered} n_2(S_5) \text{ is odd} \\ n_3(S_5) = 10 \equiv 1 \bmod 3 \\ n_5(S_5) = 6 \equiv 1 \bmod 5 \end{gathered}$$

Source: Primary Source Material

Week 7 - Missed (Midterms)

Theorem 4.5: Cauchy's Theorem on Abelian Groups

If G is abelian and $p \mid |G|$ where p prime, then G contains an element of order p.

Proof.

Note that G is clearly not the trivial group. Therefore, there exists $x \in G$ such that $x \neq e$.

If $p \mid |x|$, we can write $|x| = pk$. Consider x^k. Note that $x^k \neq e$ since $k < |x|$. Furthermore, since $(x^k)^p = x^{kp} = e$, then $\left|x^k\right| = p$ as needed.

Now suppose $p \nmid |x|$. Then $\langle\, x \,\rangle \lneq G$. Since $\langle\, x \,\rangle$ is abelian, then $G/\langle\, x \,\rangle$ is well-defined, and by Sylow's First Theorem, its order is divisible by p.

Now, we induct: Assume the result holds for all groups of order less than $|G|$. In particular, $G/\langle\, x \,\rangle$ contains an element y' of order p. That is:

$$y' = y\,\langle\, x \,\rangle$$

has order p, where $y \in G$. Therefore:

$$y'^p = e' \implies y^p \in \langle\, x \,\rangle$$

where e' is the identity coset.

Since $\langle\, y' \,\rangle > \langle\, x \,\rangle$ (as y' has order p), then $y^p = x^m$ for some m. Now notice that if $p \nmid |y|$, then $|y^p| = |y| > |x^m|$. This is a contradiction, so $p \mid |y|$. If $|y| = pr$, then y^r has order p. ■

Source: Primary Source Material

Theorem 4.6

Let G be a group with a p-Sylow subgroup P of order p^α and any other p-subgroup Q. Then:

$$Q \cap N_G(P) = Q \cap P$$

Proof.

Note that $P \leq N_G(P)$, so $Q \cap P \leq Q \cap N_G(P)$. So we prove the other direction.

Let $H = Q \cap N_G(P)$, and consider HP. Since $H \leq N_G(P)$, then we know that $HP \leq N_G(P)$. So we have that:

$$|HP| = \frac{|H| \cdot |P|}{|H \cap P|}$$

Therefore, we see that $|HP|$ is a power of p. But $HP \geq P$, so $|HP| \geq p^\alpha$. But p^α is the largest possible power of p, so $|HP| = p^\alpha$. But $|P| = p^\alpha$, so $|HP| = |P|$. Therefore, $H = Q \cap N_G(P) \leq P$, so we conclude that $H \leq P \cap Q$. ■

Source: Primary Source Material

We now prove Sylow's Theorems. First, we show existence of p-Sylow subgroups.

Proof.

We have that $|G| = p^\alpha k$, where $p \nmid k$.

We proceed by induction. Assume all smaller groups have a p-Sylow subgroup. If $p \mid |Z(G)|$, then since $Z(G)$ is abelian, our first result shows that there is an element of order p in $Z(G)$.

Now, suppose $p \nmid |Z(G)|$. Let $g_1, \dots, g_r$ be the representatives of the non-central conjugacy classes in G. Then, by the Class Equation:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

By assumption, since $p \mid |G|$, if $p \mid [G : C_G(g_i)]$ for all i, then $p \mid |Z(G)|$, a contradiction. Thus, there is at least one non-central conjugacy class with order *not* divisible by p, say g_i.

Let $H = C_G(g_i)$, so $p \nmid [G : H]$. Therefore, $p^\alpha \mid |C_G(g_i)|$, say $|C_G(g_i)| = p^\alpha m$. Since $g_i \notin Z(G)$ and $H < G$, by hypothesis, H has a p-Sylow subgroup of order p^α, which is thus a p-Sylow subgroup of G.

Now, return to assuming that $p \mid |Z(G)|$. We know that $Z(G)$ has an element of order p, so consider $G/\langle\, w \,\rangle$. We have that $|G/\langle\, w \,\rangle| = p^{\alpha-1}k$, so by hypothesis, $G/\langle\, w \,\rangle$ has a p-Sylow subgroup P of order $p^{\alpha-1}$. Furthermore, $|P \cdot \langle\, w \,\rangle| = p^\alpha$, and $P \cdot \langle\, w \,\rangle$ is a subgroup of G of order p^α, i.e. a p-Sylow subgroup. ■

Source: Primary Source Material

So now we know that all groups G such that $|G| = p^\alpha k$ have a p-Sylow subgroup.

Suppose P_1 is a p-Sylow subgroup of G. Let $S = \{P_1, \dots, P_r\}$ be the sets of conjugates of P_1. Now, let Q be any p-subgroup of G. Then, Q acts on S by conjugation. S is a singe G-orbit, but may be multiple Q-orbits. We write:

$$S = O_1 \cup O_2 \cup \cdots \cup O_s$$

where O_i is a Q-orbit. We also have that:

$$|S| = r = \sum_{i=1}^{s} |O_i|$$

Now, renumber $P_1, \dots, P_r$ such that $P_i \in O_i$ for $i \in \{1, \dots, s\}$. By the orbit-stabilizer theorem:

$$|O_i| = [Q : N_Q(P_i)]$$

From our above result, we know that:

$$N_Q(P_i) = N_G(P_i) \cap Q = P_i \cap Q$$

Since this holds for arbitrary Q, it holds for $Q = P_1$. That is:

$$N_G(P_1) = N_{P_1}(P_1) = P_1$$

So:

$$|O_1| = [P_1 : P_1] = 1$$

But for other values of i, we have that $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$ and:

$$|O_i| = [P_1 : P_1 \cap P_i] > 1$$

Recall that for all p-groups $p \mid |O_i|$. Furthermore, we have that:

$$r = \sum |O_i| = |O_1| + \sum_{i=2}^{s} |O_i| = 1 + \sum_{i=2}^{s} |O_i|$$

Therefore, $r \equiv 1 \bmod p$. Here, r is the number of *conjugates* of P_1, not necessarily the number of p-Sylow subgroups. Unless...?

Let $Q \leq G$ be any p-subgroup. We claim that Q is in P_i for some i.

Assume not. Then $Q \cap P_i < Q$. In addition,

$$|O_i| = [Q : Q \cap P_i] > 1$$

So $p \mid |O_i|$ for all i, meaning $p \mid \sum |O_i| = r$. That is, $p \mid r$, which contradicts the fact that $r \equiv 1 \bmod p$.

So $Q \leq P_i$ for some i. Hence, Q is contained in gP_1g^{-1} for some g. If Q is any p-Sylow subgroup, then $Q \leq gP_1g^{-1}$ for some g. They have the same order, so this means that all p-Sylow subgroups are conjugate, and so any p-subgroup is contained in a conjugate of P_1.

In particular, $\mathrm{Syl}_p(G) = S$, the conjugates of P_1, and:

$$n_p(G) = \left|\mathrm{Syl}_p(G)\right| = r \equiv 1 \bmod p$$

Furthermore, because all p-Sylow subgroups are conjugate:

$$n_p(G) = [G : N_G(P)]$$

for any $P \in \mathrm{Syl}_p(G)$.

This completes the proof of all the Sylow theorems. At this point, it's worth noting that the proofs aren't that important; the theorems themselves are more valuable.

Example

Consider $G = S_3$. Note $|G| = 6 = 2 \cdot 3$. So, there are three 2-Sylow subgroups:

$$\langle (12) \rangle \qquad \langle (13) \rangle \qquad \langle (23) \rangle$$

Note that these are all order 2 and conjugate. We also notice that $n_2(S_3) = 3 \equiv 1 \bmod 2$, and:

$$[S_3 : N_{S_3}((12))] = [S_3 : \langle (12) \rangle] = 3 \implies n_2(S_3) = 3 \mid [S_3 : N_{S_3}((12))] = 3$$

We also have a 3-Sylow subgroup: A_3, the group of rotations.

$$n_3(S_3) = 1 \equiv 1 \bmod 3$$
$$n_3(S_3) \mid [S_3 : A_3] = 2$$

Source: Primary Source Material

The next theorem will not be proven for a while, but it's nice to know for now.

Theorem 4.7: Fundamental Theorem of Finitely Generated Abelian Groups

Any finitely generated abelian group is isomorphic to a product:

$$\mathbb{Z}^r \times C_{m_1} \times \cdots \times C_{m_k}$$

where $r \geq 0, m_i \geq 0, C_{m_i} = \mathbb{Z}/m\mathbb{Z}$, and $m_k \mid m_{k-1} \mid \cdots \mid m_2 \mid m_1$.

We call r the **rank / Betti number**, and it, along with the m_i's, determine the isomorphism class of the group completely.

Notice that if $r = 0$, then the group is *finite*. Calling $\mathbb{Z}$ an infinite group simply means that every finite abelian group is a product of cyclic groups.

Example

- The Klein 4-group is $C_2 \times C_2 \not\simeq C_4$.
- Consider any abelian group of order 8. For example:
  - C_8
  - $C_4 \times C_2$
  - $C_2 \times C_2 \times C_2$

  In fact, any abelian group of order 8 is isomorphic to one of the above three.
- Consider groups of order 8 that are not necessarily abelian. We've dealt with abelian groups; for non-abelian groups, if $|G| = 8$, then by the class equation, $Z(G) \neq \{e\}$.

  If $Z(G) = G$, then G is abelian. So, suppose that $|Z(G)| \neq 8$. Then:
  - $|Z(G)| = 4$, so $|G/Z(G)| = 2$. Note that conjugation by G will produce an automorphism of the center. We know that $Z(G) = C_4$ or $C_2 \times C_2$. Automorphisms of C_4 are given as:

    $$\begin{aligned} \{0,1,2,3\} &\to \{0,1,2,3\} & \text{identity} \\ \{0,1,2,3\} &\to \{0,3,2,3\} & \text{“minus” identity} \end{aligned}$$

    From here, one can determine all groups of order 8.
  - If $|Z(G)| = 2, Z(G) = \{0, 1\}$, so any automorphism must be the identity automorphism.

Source: Primary Source Material

Side tangent time - what are the automorphisms of C_k?

Automorphisms φ are determined by **what happens to** 1. For φ to be injective, $\varphi(1)$ must be *coprime* to k; if $\varphi(1) = u$, then $\varphi(2) = 2u$, and so on. Hence φ is just multiplication by u, and φ^{-1} is multiplication by u^{-1}, which only exists in $\mathbb{Z}/k\mathbb{Z}$ if and only if $\gcd(u, k) = 1$. Therefore, the number of automorphisms of C_k is the number of $u \in \{1, \ldots, k-1\}$ which are coprime with k - in other words, $\phi(k)$, where ϕ is the Euler totient function. Note that there is also another type of automorphism given by:

$$C_\ell \times C_\ell : (a, b) \to (b, a)$$

Okay, side tangent done!

Suppose $|G| = 44 = 4 \cdot 11$. By Sylow, $n_4(G) \equiv 1 \bmod 11$. So there might be 1, or 12. 12 seems like a lot given $|G| = 44$, but it might work if they overlap. Do they?

Corollary

If $|P| = |Q| = 11$, and $P \neq G$, then $P \cap Q = \{e\}$.

Proof.

If $e \neq x \in P \cap Q$, then $\langle\, x \,\rangle = P$ and $\langle\, x \,\rangle = Q$, so $P = Q$. ■

Source: Primary Source Material

So if $n_4(G) = 12$, then $|G| > 12(11 - 1) + 1 = 121 > 44$. So there is only 1. Denote this unique 11-Sylow subgroup by P. Then any conjugate of P is itself, so P is *normal*. We can thus take G/P, and $|G/P| = 4$, therefore we have that:

$$G/P = C_4 \text{ or } C_2 \times C_2$$

If $G/P = C_4$, then conjugation by G gives automorphisms of P, yielding a map:

$$C_4 \to \mathrm{Aut}(P)$$

Note that P is cyclic since 11 is prime, so $P = \{0, 1, \ldots, 10\}$ and $\phi(11) = 10$.

Lec 15 - Oct 23 (Week 8)

Suppose p is prime, and $|P| = p$. What is $\mathrm{Aut}(P)$?

If $P = \langle\, a \,\rangle$, then any $\sigma \in \mathrm{Aut}(P)$ maps $a \to a^r$ for some r. Therefore, for any element, we see that:

$$\sigma(a^k) = (\sigma(a))^k = (a^r)^k = a^{kr} = (a^k)^r$$

So σ is the r-th power map. Notice that:

$$(a^r)^s = a^{rs} = (a^s)^r$$

This tells us that $\mathrm{Aut}(P)$ is abelian. Furthermore, it's cyclic of order $p - 1$. If $\gcd(r, p-1) = 1$, then it is a generator.

Example

Consider the Klein 4-group, $G = \{e, a_1, a_2, a_3\}$. Here, if $i \neq j$, then $a_i a_j = a_k, k \neq i, j$.

We can let S_3 act on G by $\sigma(a_i) = a_{\sigma(i)}$. Note that:

$$\sigma(a_i a_j) = \sigma(a_k) = a_{\sigma(k)}$$

If σ is an automorphism, then it must take a_1, a_2, a_3 to themselves, in a possibly different order.

$$a_{\sigma(k)} = a_{\sigma(i)} a_{\sigma(j)}$$

So the permutation action of S_3 commutes with the group multiplication operation.

Therefore, we have that $S_3 \leq \mathrm{Aut}(G)$. In fact, we see that $S_3 = \mathrm{Aut}(G)$.

Source: Primary Source Material

Last time, we considered a group of order $44 = 2^2 \cdot 11$.

$$n_{11}(G) \equiv 1 \bmod 11$$

Note that it can't be 12, as this would mean we had $12 \cdot (11 - 1) = 120$ elements.

So $n_{11}(G) = 1 \implies P_4 \lhd G, \mathrm{Syl}_{11}(G) = P_{11}$. Furthermore, $|G/P_{11}| = 4$, and the only possibilities are $\mathbb{Z}/4\mathbb{Z}$ or the Klein 4-group.

The action of G by conjugation on P_{11} restricts to the trivial representation on P. So we really have an action of G/P_{11} on P_{11}. This gives us a map:

$$G/P_{11} \to \mathrm{Aut}(P_{11})$$

where $|G/P_{11}| = 4$, and $|\mathrm{Aut}(P_{11})| = 10$ and is cyclic.

If G/P_{11} is cyclic, we could have the trivial homomorphism. This corresponds to an abelian group of order 44. So by the Fundamental Theorem of Abelian Groups, an abelian group of order 44 is either $C_4 \times C_{11}$ or $C_2^2 \times C_{11}$. Since G/P_{11} is assumed to be cyclic, then our abelian group is $C_4 \times C_{11}$.

If the map $G/P_{11} \to \mathrm{Aut}(P_{11})$ is not trivial, then we can't have an injective homomorphism. However, we can take the quotient by the (unique) element of order 2 to get:

$$\frac{G/P_{11}}{\langle 2 \rangle / P_{11}} = \{1, -1\} = C_2 \to \mathrm{Aut}(P_{11})$$

In the corresponding group, there is a non-trivial conjugation, so G is not abelian. This gives us a second group of order 44.

What if G/P_{11} is the Klein 4-group?

$$K_4 \to \mathrm{Aut}(P_{11}) \simeq C_{10}$$
$$1 \to 5 \in \mathbb{Z}/10\mathbb{Z} \simeq \mathrm{Aut}(P_{11})$$

Note that K_4 can be written as $C_2 \times C_2$ in three different ways:

$$\langle a \rangle \times \langle b \rangle \qquad \langle a \rangle \times \langle c \rangle \qquad \langle b \rangle \times \langle c \rangle$$

Note that the three groups obtained this way are all isomorphic, because they are permuted by the action of S_3. We also could have had K_4 and the trivial homomorphism into $\mathrm{Aut}(P_{11})$ - this corresponds to $C_2 \times C_2 \times C_{11}$.

All in all, we have two abelian groups of order 44

$$C_4 \times C_{11} \qquad C_2^2 \times C_{11}$$

as well as two non-abelian:

$$G/P_{11} \simeq C_4 \qquad G/P_{11} \simeq C_2^2$$

Definition 4.2

We say a group G is **simple** if it has no normal subgroups.

Corollary

A_5 is simple.

Proof.

Consider the cycle types in A_5:

$$\begin{array}{cc} \{e\} & 1 \\ \\ (abc) & \binom{5}{3}2 = 20 \\ \\ (ab)(cd) & \dfrac{\binom{5}{2}\binom{3}{2}}{2} = 15 \\ \\ (abcdf) & 4! = 24 \end{array}$$

Observe that a normal subgroup is a union of conjugacy classes (in this case, cycle types). Additionally, notice that:

$$(12)(34) \cdot (23)(45) = (12453)$$

So if a subgroup contains all double transpositions, then it must also contain all 5-cycles. In this case, it would have $15 + 24 = 39$ elements, so it can't be a proper subgroup.

Similarly, if we have 3-cycles, we have 5-cycles:

$$(123)(345) = (12345)$$

Again, it would have 44 elements, so it also cannot be a proper subgroup.

All that's left, then, are the 5-cycles. Note that this includes the identity, so it would have $24 + 1 = 25$ elements - no dice.

Therefore, we indeed see that A_5 is simple. In fact, A_5 is the smallest simple subgroup. ■

Source: Primary Source Material

The above proof is actually wrong, because in A_n, conjugacy classes are *not* the same as cycle types - that only holds in S_n.

In (abc), two elements are conjugate in S_5: given $(abc)(\alpha\beta\gamma)$, there exists $\sigma \in S_5$ such that:

$$(abc) = \sigma(\alpha\beta\gamma)\sigma^{-1}$$

But suppose $\sigma \notin A_5$. In this case, we can fix it. Suppose $(\alpha\beta\gamma\rho\tau) = (12345)$. We can replace σ with $\sigma(\rho\tau)$, which is even, and:

$$\sigma(\rho\tau)(\alpha\beta\gamma)(\rho\tau)^{-1}\sigma^{-1}$$

so we see that:

$$(abc) = \sigma(\alpha\beta\gamma)\sigma^{-1}$$

So if $(abc), (\alpha\beta\gamma)$ are conjugate in S_5, then they are conjugate in A_5.

In S_5, what is the centralizer of $(ab)(cd)$? We can see that it includes:

$$e, (ab), (cd), (ab)(cd)$$

But notice that it also includes $(ac)(bd)$. Therefore, the centralizer has order 8.

Of these, notice that the single transpositions are not in A_5, nor does it contain the product of $(ac)(bd)$ with either single transposition. But it does have:

$$e, (ab)(cd), (ac)(bd), (ad)(bc)$$

Notice that:

$$(12)(12345)(12) = (13452)$$

We get two A_5 conjugacy classes, each of size 12.

So our proof still works: if N contains any double transpositions, it contains all of them, and hence all 3-cycles, which is impossible. Likewise, all 3-cycles gives all 5-cycles - impossible. And we have either 12 or 245-cycles, giving us a group of order 13 or 25 - doesn't work.

Sidenote: simple sometimes includes non-abelian.

5 Series of Subgroups

Lec 16 - Oct 25 (Week 8)

Note: for the purposes of this course, simple groups are *non-abelian*.

Recall that we used the class equation to show that any p-group has a non-trivial center.

Theorem 5.1

If p is prime and $|P| = p^2$, then P is abelian.

Corollary

With $p = 2$, we see that there are non non-abelian groups of order 4.

Indeed, from the fundamental theorem of finitely generated abelian groups, the only possibilities are C_4 and $C_2 \times C_2$.

Proof.

We know P must have a non-trivial center. Since $|P| = p^2$, the only possible orders for a subgroup are $1, p, p^2$.

The center is non-trivial, it has order p or p^2. In particular, we want to show that it is not p.

Suppose $|Z_p| = p$. Then $|G/Z_p| = p^2/p = p$, so G/Z_p is cyclic. Suppose xZ_p is a generator. Then, every element of G/Z_p is of the form $x^k Z_p$.

In particular, every element is of the form $x^k z$ for some $z \in Z_p$. Then the product of two elements is:

$$(x^k z)(x^m z') = x^{k+m} zz'$$
$$(x^m z')(x^k z) = x^{m+k} zz'$$

Clearly, these two are equal, so G must be abelian. In particular, this means that
$|Z_p| = |G| = p^2 \neq p$. ■

Source: Primary Source Material

Joe thinks: If $p < q$ both prime, then $|G| = pq$ implies that G is abelian unless $p \mid (q-1)$. With $p = 2$, $|Q_8| = 8 = 2^3$, but is *not* abelian. Anyway.

We've hinted that looking at normal subgroups and their quotients can give us a lot of information about a group. This information isn't quite enough to show that two groups are isomorphic.

Definition 5.1

Let G be a finite group. A sequence of subgroups

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{m-1} \lhd G_m = G$$

is called a **composition series** for G if G_{i+1}/G_i is prime, cyclic, or simple.

Note that $G_i \lhd G_{i+1}$, but G_i is not necessarily normal in G.

Theorem 5.2: Jordan-Holder Theorem

Any finite group G has a composition series. Furthermore, if G has two composition series:

$$G_0 \lhd \cdots \lhd G_m$$
$$G'_0 \lhd \cdots \lhd G'_{m'}$$

then $m = m'$, and:

$$\{G_1/G_0, G_2/G_1, \ldots, G_m/G_{m-1}\} \;=\; \{G'_1/G'_0, G'_2/G'_1, \ldots, G'_m/G'_{m-1}\}$$

The quotients are called the **composition factors** of G, and different composition series have the same composition factors, although they need not be in the same order.

Example

Let $G = D_{12}$. Then, consider:

$$\{e\} \lhd \langle\, r^3 \,\rangle \lhd \langle\, r \,\rangle \lhd D_{12}$$

Note that:

$$\left|\langle\, r^3 \,\rangle \,/\, \{e\}\right| = 2$$
$$\left|\langle\, r \,\rangle \,/\, \langle\, r^3 \,\rangle\right| = 3$$
$$|D_{12}/\,\langle\, r \,\rangle| = 2$$

Here, the composition factors are C_2, C_3, C_2. But we can also write the following composition series:

$$\{e\} \lhd \langle\, r^2 \,\rangle \lhd \langle\, r \,\rangle \lhd D_{12}$$

Note that:

$$\left|\langle\, r^2 \,\rangle \,/\, \{e\}\right| = 3$$
$$\left|\langle\, r \,\rangle \,/\, \langle\, r^2 \,\rangle\right| = 2$$
$$|D_{12}/\,\langle\, r \,\rangle| = 2$$

Here, the composition factors are C_3, C_2, C_2.

So we see that composition series are not quite enough to categorize groups. However, observe that $C_2 \times C_2 \times C_3$ has the same composition factors.

Source: Primary Source Material

Lec 17 - Nov 6 (Week 9)

Definition 5.2

A group G is **solvable** if it has a composition series with abelian composition factors.

He totally didn't forget to define this, and only defined it after defining a derived series because someone brought it up. Definitely not.

Definition 5.3

A normal subgroup $N \trianglelefteq G$ is called **characteristic** if:

$$\forall\, \varphi \in \mathrm{Aut}(G), \quad \varphi(N) = N$$

We denote a characteristic subgroup as $N \overset{c}{\trianglelefteq} G$.

A simple example of a characteristic subgroup is the center, $Z(G)$.

Example

In $G \times G$, we have that $N = G \times \{e\} \trianglelefteq G \times G$. However, N is *not* characteristic, because it is not invariant under:

$$\varphi(a, b) = (b, a) \qquad \varphi \in \mathrm{Aut}(G \times G)$$

Source: Primary Source Material

Definition 5.4

Given a finite group G, the **upper central series** is:

$$\begin{gathered} G_0 = \{e\} \\ G_1 = Z(G) \\ \vdots \\ G_i = \pi_{i-1}^{-1}(Z(G/G_{i-1})) \end{gathered}$$

Here, $\pi_{i-1} : G \to G/G_{i-1}$ is the natural projection.

An easy thing to show is that for each i, we have that $G_i \trianglelefteq G$. Slightly harder to show is that $G_i \overset{c}{\trianglelefteq} G$.

So we have a sequence of subgroups:

$$G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_i \trianglelefteq \cdots$$

A remark: note that G_i/G_{i-1} is abelian. Since G is finite, this sequence must eventually terminate. When it does, does it end at all of G?

Definition 5.5

If there exists some k such that $G_k = G$ in the above, then G is said to be **nilpotent**.

The smallest such k is called the **index of nilpotence** of G. We might also say that G is a k-step nilpotent group.

Corollary

Any p-group is nilpotent.

Corollary

If $p_1, \dots, p_r$ are distinct primes, and P_i is a p_i-group, then

$$G = \prod P_i$$

is a nilpotent group.

Recall that for $H, K \leq G$, the commutator is $[H, K]$ where:

$$[H, K] = \langle\, hkh^{-1}k^{-1} : h \in H, k \in K \,\rangle$$

Definition 5.6

Given a finite group G, the **lower central series** is:

$$\begin{aligned} G^0 &= G \\ G^1 &= [G, G] \\ G^2 &= [G, G^1] \\ &\vdots \\ G^i &= [G, G^{i-1}] \end{aligned}$$

Again, we have a sequence of groups:

$$G = G^0 \trianglerighteq G^1 \trianglerighteq \cdots \trianglerighteq G^i \trianglerighteq \cdots$$

In fact, each $G^i \overset{c}{\trianglelefteq} G$.

Again, since G is finite, this terminates. But does it terminate at the trivial subgroup?

Lemma

If there exists k such that $G^k = \{e\}$, then G is nilpotent. Furthermore, k is the index of nilpotence of G.

Definition 5.7

For a finite group G, the **derived series** is:

$$\begin{gathered} G^{(0)} = G \\ G^{(1)} = [G, G] \\ \vdots \\ G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \end{gathered}$$

Once again, we have a series of characteristic subgroups:

$$G = G^{(0)} \overset{c}{\trianglelefteq} G^{(1)} \overset{c}{\trianglelefteq} \cdots \overset{c}{\trianglelefteq} G^{(i)} \overset{c}{\trianglelefteq} \cdots$$

Lemma

If there exists k such that $G^k = \{e\}$, then G is solvable.

The converse also happens to be true, but it is much harder to prove.

Note that $G^{(i)} < G^i$ for all i. Because of this, we also get the following:

Corollary

Any nilpotent group is solvable.

(The converse of this one is not true).

Example

Fix $n \in \mathbb{N}$, and define G as:

$$G = \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}) \right\}$$

for some finite field $\mathbb{F}$. We show that G is nilpotent.

Using the upper central series, we see that:

$$G_1 = Z(G) = \left\{ \begin{pmatrix} 1 & 0 & * & \cdots & * \\ 0 & 1 & 0 & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$$

In other words, the center is the set of such matrices with a diagonal of zeroes above the main diagonal. The quotient is then:

$$G/Z(G) = \left\{ \begin{pmatrix} 1 & * & 0 & \cdots & 0 \\ 0 & 1 & * & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\}$$

And so $G_2 = \pi^{-1}(Z(G/Z(G))) = G$, so G is 2-step nilpotent. In general, G is n-step nilpotent.

Source: Primary Source Material

Fix the above...

There's somewhat of a linearity or hierarchy to groups:

$$\begin{gathered} \text{Abelian} \subsetneq \text{nilpotent} \\ p\text{-group} \subsetneq \text{nilpotent} \\ \text{nilpotent} \subsetneq \text{solvable} \subsetneq \text{all groups} \end{gathered}$$

For instance, it can be verified (do it) that the set of upper triangular matrices over a finite field is solvable, but not nilpotent.

Q_8, D_8 are 2-groups, and are thus nilpotent. In fact, D_{2k} is nilpotent if and only if $k = 2^n$ for some n.

Theorem 5.3

A group G is nilpotent if and only if $\mathrm{Syl}_{p_i}(G)$ contains a single p_i-group, where $|G| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. This is equivalent to the claim that:

$$G = P_1 \times \cdots \times P_k \qquad P_i \in \mathrm{Syl}_{p_i}(G)$$

Recall that in a direct product $G \times G'$, the subgroups

$$\overline{G} = G \times \{e\} \qquad \overline{G'} = \{e\} \times G'$$

commute with each other. Of course, in general, this doesn't always happen.

Consider the rigid motions of $\mathbb{R}^n$. We have:

$$\begin{gathered} O(n) = \left\{A \in \mathrm{GL}_n(\mathbb{R}) : A^T = A\right\} \\ \mathrm{SO}_n = \{A \in O(n) : \det A = 1\} \end{gathered}$$

Note that $\mathrm{SO}_n \subsetneq O(n)$ is precisely the set of rotations. But we also have translations:

$$T_a(x) = x + a \qquad T = \{T_a : a \in \mathbb{R}\}$$

So what happens when we combine them?

Suppose $A \in \mathrm{SO}_n, T_a \in T$. Then:

$$\begin{gathered} AT_a(x) = A(x+a) = Ax + Aa \\ T_aA(x) = T_a(Ax) = Ax + a \end{gathered}$$

So in general, they are not equal. But what if we tried this? Taking $A, B \in \mathrm{SO}_n, T_a, T_b \in T$:

$$\begin{aligned}(AT_a \cdot BT_b)(x) &= AT_aB(x+b) \\ &= AT_a(Bx+Bb) \\ &= A(Bx+Bb+a) \\ &= ABx+ABb+Aa\end{aligned}$$

The key problem here is that translations are affected by the rotations. In other words, the subgroup SO_n acts on T by:

$$AT_a(x) = T_{Aa}(Ax)$$

This leads us to the definition of a "semidirect product" of two groups.

Suppose $H \leq G, N \trianglelefteq G, H \cap N = \{e\}$. Then, HN is a group, and $HN \leq G$.

Here, H acts on N by conjugation:

$$\varphi_h(n) = h^{-1}nh$$

Then, the operation looks like:

$$hn \cdot h'n' = hh'h'^{-1}nh'n' = hh'\,\varphi_{h'^{-1}}(n)n'$$

This is a semidirect product...?

6 Semidirect Product

Lec 18 - Nov 8 (Week 9)

Let's try semidirects properly this time.

Suppose $N \trianglelefteq G, H < G$ such that $H \cap N = \{e\}$. Then, we know that HN is a subgroup of G. Consider the set:

$$\{(n,h) : n \in N, h \in H\}$$

Then, this is a group under the following operation:

$$(n,h)\cdot(n',h') = nhn'h' = nhn'h^{-1}hh' = n\,\varphi_h(n')hh'$$

where $\varphi_h(n') = hn'h^{-1}$ is conjugation by h.

Clearly, the identity is given by (e,e). What is the inverse?

$$\begin{aligned}&(n,h)(\overline{n},h^{-1}) = (e,e) \\ \implies\ &(n\,\varphi_h(\overline{n}), hh^{-1}) = (e,e) \\ \implies\ &n\,\varphi_h(\overline{n}) = e \\ \implies\ &\varphi_h(\overline{n}) = n^{-1} \\ \implies\ &\overline{n} = h^{-1}n^{-1}h \\ \implies\ &\overline{n} = \varphi_{h^{-1}}(n^{-1})\end{aligned}$$

The group we just constructed is called the semi-direct product of N and H.

Definition 6.1

Suppose $N \trianglelefteq G$ and $H < G$ such that $H \cap N = \{e\}$. Then, the **semi-direct product** of N and H is:

$$\{(n,h) : n \in N, h \in H\}$$

defined with the following operation:

$$(n,h)\cdot(n',h') = nhn'h' = nhn'h^{-1}hh' = n\,\varphi_h(n')hh'$$

where $\varphi_h(n') = hn'h^{-1}$ is conjugation by h.

The identity is given by (e,e), and the inverse is given by:

$$(n,h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$$

We denote the semi-direct product of N and H as $N \rtimes_\varphi H$, or simply $N \rtimes H$.

We can also start with the groups N and H and a homomorphism $\varphi : H \to \mathrm{Aut}(N)$.

The same formulas construct a group which we denote the same way. In this manner, we can define semidirect products between more general groups.

Note that if $\varphi(h) = \mathrm{id} \in \mathrm{Aut}(N)$ for all h, then $N \rtimes H \cong N \times H$.

In general, $N \rtimes H$ contains:

$$\overline{N} = \{(n,e) : n \in N\} \cong N$$

$$\overline{H} = \{(e,h) : h \in H\} \cong H$$

We also allow ourselves to call them N and H respectively. Note that:

$$N \cap H = \{e\} \qquad N \trianglelefteq N \rtimes H \qquad N \rtimes H = NH$$

Example

Consider the following two groups:

- $\mathrm{SO}_3 \rtimes \mathbb{R}^3$ - the special Euclidean group
- $\mathrm{O}_3 \rtimes \mathbb{R}^3$ - the Euclidean group

These groups "preserve" Euclidean geometry - the first represents rotations and translations in $\mathbb{R}^3$, and the second represents rotations, reflections, and translations in $\mathbb{R}^3$.

Source: Primary Source Material

Example: Lorentz and Poincare group

Relativity operates in $\mathbb{R}^4$.

The Lorentz group is the group of matrices that preserve the non-positive-definite inner product, $\mathrm{SO}(3,1)$. There are also translations, given by $\mathbb{R}^4$.

So, the group $\mathbb{R}^4 \rtimes \mathrm{SO}(3,1)$ is called the Poincaré group. It is the group of things that "preserve" special relativity.

Source: Primary Source Material

Example

Consider the set of 4×4 matrices of the form:

$$\begin{array}{ccc|c} & & & x \\ & \Omega & & y \\ & & & z \\ \hline 0 & 0 & 0 & 1 \end{array}$$

where $\Omega \in \mathrm{SO}_3$. This is isomorphic to $\mathbb{R}^3 \rtimes \mathrm{SO}_3$.

Analogously for the Poincaré group, we have that:

$$\begin{array}{cccc|c} & & & & x \\ & & & & y \\ & & \Omega & & z \\ & & & & t \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}$$

Source: Primary Source Material

Midterm - Nov 13 (Week 10)

Lec 19 - Nov 15 (Week 10)

If you have a direct product $G = H \times K$, then each copy of H and K is normal:

$$H \simeq H \times \{e\} \qquad K \simeq \{e\} \times K$$

Furthermore, H and K commute with each other.

In particular, the maps $H \to \mathrm{Aut}(K)$ and $K \to \mathrm{Aut}(H)$, given by conjugation, are both trivial.

For a semi-direct product $G = N \rtimes H$, we only have that $N \trianglelefteq G$. In this case, the conjugate map $H \to \mathrm{Aut}(N)$ is non-trivial.

Again we write $N = N \times \{e\}$ and $H = \{e\} \times H$. Note that $N \cap H = \{e\}$.

So each element $g \in G$ can be written as $g = (n, h)$ for some $n \in N, h \in H$, such that n and h are uniquely determined by g.

Example

Let $G = \mathbb{Z}$, and $N = 2\mathbb{Z} \trianglelefteq G$. Note N has no complement.

Source: Primary Source Material

Example

Consider $G = S_3$, with $A_3 \trianglelefteq S_3$. Since $|G| = 6$ and $|A_3| = 3$, our complement must have order 2.

Indeed, we see that $H = \langle (12) \rangle$ is a group of order 2. Clearly, $H \cap A_3 = \{e\}$. Note that $H' = \langle (13) \rangle$ and $H'' = \langle (23) \rangle$ also work.

Source: Primary Source Material

II Ring Theory

7 Basics

Definition 7.1

A **ring** is a set with two operations, denoted addition $(+)$ and multiplication $(\cdot)$.

A ring R is an abelian group under addition with additive identity called 0. The multiplication satisfies:

- Associative: $(ab)c = a(bc)$
- Distributive: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

If multiplication is commutative, we say R is a **commutative ring**.

Furthermore, R *may or may not* have a multiplicative identity, which we call 1. If it does, we call it a **ring with unit**, or a **unital ring**.

Clearly, if R is unital, then it is unique.

Also note that multiplicative inverses need not exist; if they do, they satisfy the usual properties. Of course, inverses cannot exist without a unit. Note that 0 never has a multiplicative inverse, and:

$$0 \cdot r = r \cdot 0 = 0 \text{ for all } r \in R$$

(There is a silly exception to the above, which is the zero ring, but it is silly.)

Definition 7.2

If R is a ring with unit, then we say $r \in R$ is a unit iff r has an inverse.

Try not to get confused. I dare you.

Theorem 7.1

The set of all units in R (if any) is a group, called the group of units and denoted by $R^\times$.

Still not confused?

Example

- The integers $\mathbb{Z}$ is a commutative ring, and $\mathbb{Z}^\times = \{\pm 1\}$.
- A field $\mathbb{F}$ is a commutative ring, and $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.
- Given a field $\mathbb{F}$, the set of polynomials over $\mathbb{F}$, denoted $\mathbb{F}[x]$, has an identity 1, the constant polynomial. Here, we see that:

$$\mathbb{F}^\times[x] = \text{non-zero constant polynomials} \simeq \mathbb{F}^\times$$

- Given a field $\mathbb{F}$, then $R = M_{n\times n}(\mathbb{F})$ is a non-commutative ring (unless $n = 1$). Here:

$$M_{n\times n}^{\times}(\mathbb{F}) = \mathrm{GL}_n(\mathbb{F})$$

- If R is any ring, then $R[x]$ and $M_{n\times n}(R)$ are also rings.

Source: Primary Source Material

Lec 20 - Nov 20 (Week 11)

Quick note on examples of complements from last week:

Consider $G = C_6 = C_2 \times C_3$. The subgroup ± 1 has a complement in C_6, however has no complement in C_4. This is because both $\pm i$ generate all of C_4.

Anyway, back to (examples of) rings.

Example

- If X is a Hausdorff topological space, then $R = C(X)$, the space of continuous functions on X (real or complex-valued) forms a ring with "pointwise" operations.

  The identity is the constant function 1, and is not a field as the 0 map has no inverse. (?? this is always true joe. what)

- If X is locally compact (e.g. $\mathbb{R}^n$, $\mathbb{C}^n$, etc.), then consider the set of continuous functions of compact support, $C_c(X)$. This set has a unit iff X is compact.

Source: Primary Source Material

The following example is known as a **group ring**.

Suppose G is a finite group and $\mathbb{F}$ a field. Define $\mathbb{F}[G]$ as:

$$\mathbb{F}[G] = \left\{ \sum_{g\in G} c_g g : c_g \in \mathbb{F} \right\}$$

These are known as *formal sums*, where the product should not be interpreted literally. This forms a vector space, with dimension $|G|$ and basis given by $\{g : g \in G\}$. We define multiplication as follows:

$$f = \sum_{g\in G} c_g g \quad , \quad h = \sum_{k\in G} d_k k$$

$$f \cdot h \;=\; \left(\sum_{g} c_g g\right)\left(\sum_{k} d_k k\right) \;=\; \sum_{g,k\in G} c_g d_k gk \;=\; \sum_{x\in G} b_x x$$

What is the coefficient b_x? Well, when does $gk = x$ for some $x \in G$? Certainly, we can write $g = xk^{-1}$:

$$c_g d_k = c_{xk^{-1}} d_k$$

Therefore, we can write the multiplication as:

$$f \cdot g = \sum_{x,k\in G} c_{xk^{-1}} d_k x$$

Note that the above multiplication can be written in different ways. (joe what did u mean by this)

Notice that $\mathbb{F}[G]$ is commutative iff G is abelian. The identity is given by $1 \cdot e$:

$$(1 \cdot e)\left(\sum_g c_g g\right) = \sum_g 1 \cdot c_g e g$$

Given $g \in G$ with $g \neq e$, consider the cyclic subgroup generated by g with order m:

$$\langle\, g\, \rangle = \left\{e, g, g^2, \ldots, g^{m-1}\right\}$$

Clearly, these elements are all distinct. Taking their sum as an element of $\mathbb{F}[G]$, we get:

$$e + g + g^2 + \cdots + g^{m-1} \neq 0$$

is non-zero. (Really we should write $1 \cdot e + 1 \cdot g + \ldots$ and so on, but whatever.) Also note that $e - g = 1 \cdot e - 1 \cdot g$ is non-zero in $\mathbb{F}(G)$. Note that:

$$\begin{aligned}&(e-g)(e+g+g^2+\cdots+g^{m-1})\\ &= e+g+g^2+\cdots+g^{m-1}-g-g^2-\cdots-g^{m-1}-g^m\\ &= e\end{aligned}$$

We see that we can multiply two non-zero elements and get 0.

Definition 7.3

In a ring R, a non-zero element $d \in R$ is called a **zero divisor** if there exists $k \in R, k \neq 0$ such that $dk = 0$.

Corollary

For any nontrivial finite group G, any field $\mathbb{F}$, $\mathbb{F}[G]$ has zero divisors.

Example

In $R = \mathbb{Z}/12\mathbb{Z}$, we have that $3 \cdot 4 = 0$.

Source: Primary Source Material

Corollary

In $\mathbb{Z}/m\mathbb{Z}$, there are zero divisors iff m is *not* prime.

Example

In $\mathrm{GL}_n(\mathbb{F})$, notice that:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

So if $n > 1$, then $\mathrm{GL}_n(\mathbb{F})$ has zero divisors.

Source: Primary Source Material

Example

Consider $C(X)$. In $\mathbb{R}$, we can have the following:
[two bump functions, disjoint support]
So the product of two functions is zero if each is zero on the support of the other.

By contrast, in the ring of holomorphic functions on an open subset of $\mathbb{C}$, there are zero divisors iff the domain is disconnected.
[picture]

Source: Primary Source Material

Note that we needed G to be finite to define $\mathbb{F}[G]$ as we defined it with a *sum* over G. If G is infinite, you could consider the same sums but restricted to finitely many non-zero terms:

$$\left\{ \sum_{g \in G} c_g g : \text{finitely many coefficients } c_g \text{ are non-zero} \right\}$$

This is also a ring, but misses out on certain properties. (like what man. cmon.)

If G is finite, we have:

$$f = \sum_{g \in G} c_g g \in \mathbb{F}[G]$$

What really matters here is the c_g's. We can think of these elements as a function:

$$\begin{aligned} f : G &\to \mathbb{F} \\ g &\mapsto c_g \end{aligned}$$

In other words, $\mathbb{F}[G]$ can be identified with the set of functions on G, with multiplication defined as:

$$(f \cdot h)(x) = \sum_{k \in G} f(xk^{-1})h(k)$$

Now, suppose we'd like to extend this to $G = \mathbb{R}$. Here, elements of the ring will be functions on $\mathbb{R}$. But we can't sum over elements of $\mathbb{R}$; so instead, let's replace the sum with an integral.

$$(f \cdot h)(x) = \int_{t \in \mathbb{R}} f(x-t)h(t)\mathrm{d}t$$

Note that for this to make sense, we need:

- f, h to be measurable
- an integrability condition

It turns out that everything works if we restrict f, h to be integrable.

So, our candidate for an analogue of $\mathbb{C}[R]$ is $L^1(\mathbb{R})$. The product is called the **convolution**:

$$(f * h)(x) = \int f(x-t)h(t)\mathrm{d}t$$

uhh... he mentioned Haar measure? not sure why. he started talking abt the hair salon after.

Definition 7.4

A ring R is a **domain** iff it has no zero divisors.

If R is additionally commutative and has a unit, we call it an **integral domain**.

Example

- $\mathbb{Z}$ is an integral domain.
- Any field is an integral domain.
- For a field $\mathbb{F}$, consider $\mathbb{F}[x]$. Let $f, g \in \mathbb{F}[x]$, where:

  $$f(x) = \sum_{n=0}^{N} a_n x^n \qquad g(x) = \sum_{m=0}^{M} b_m x^m$$

  Then clearly:

  $$(f \cdot g)(x) = a_N b_M x^{N+M} + \text{lower order terms}$$

  WLOG, we assume a_N and b_N are non-zero. Since they are elements of $\mathbb{F}$, then their product is also non-zero. But this means that there are no zero divisors. Therefore, $\mathbb{F}[x]$ is an integral domain.
- In the example above, we only use the fact that fields are integral domains. So in fact, the ring $R[x]$ is an integral domain if R is an integral domain.

Source: Primary Source Material

Notice that one way we can think of multivariate polynomials $R[x, y]$ is to treat the coefficients of x as polynomials of y. That is:

$$R[x, y] \;=\; R[x][y]$$

From our above example, we see that:

$$R \text{ is an int. domain} \implies R[x] \text{ is an int. domain} \implies R[x,y] \text{ is an int. domain}$$

Corollary

If R is an integral domain, then $R[x_1, x_2, \dots x_n]$ is as well.

Consider $\mathbb{Z}/12\mathbb{Z}$. Notice:

$$3 \cdot 1 = 3 \cdot 5 = 15 = 3 \qquad 3 \cdot 1 = 3 \cdot 5 \quad 1 \neq 5$$

In other words, cancellation does not hold. In particular:

$$3 \cdot 1 - 3 \cdot 5 \ = \ 3(1-5) \ = \ 0$$

Since this is not an integral domain, $1 - 5$ does not have to be zero.

Lemma

In a domain R, cancellation holds.

Proof.

Suppose $ab = ac$ and $a \neq 0$.

Then $a(b-c) = 0$. Since R is a domain and $a \neq 0$, then we must have that:

$$a(b-c) = 0 \implies b - c = 0 \implies b = c$$

as needed. The argument for right-cancellation is analogous. ■

Source: Primary Source Material

Theorem 7.2

If R is a finite integral domain, then it is a field.

Proof.

It suffices to show that $a \in R, 0 \neq a \neq 1$ has a multiplicative inverse. Consider the elements:

$$a \quad a^2 \quad \cdots \quad a^k = a \text{ for the smallest such } k$$

Then:

$$a^k - a = 0 \implies a(a^{k-1} - 1) = 0 \implies a^{k-1} = 1$$

In other words, $a^k = a^{-1}$... bruh. just do the aluffi one ■

Source: Primary Source Material

Definition 7.5

If R is a ring, then a **subring** $S \subseteq R$ is a ring using the same operations it inherits from R.

Definition 7.6

If R, R' are rings, then define:

$$R \times R' = \{(r, r') : r \in R, r' \in R'\}$$

with component-wise operations.

Notice that if $1_R, 1_{R'}$ are units, then $\overline{R} = R \times \{0\}$ has unit $(1_R, 0)$, *not* $(1_R, 1_{R'})$, the unit of $R \times R'$.

In particular R' has a unit but R does not, then $\overline{R}$ does and $\overline{R'}$ does not.

Lec 21 - Nov 22 (Week 11)

Recall $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Let's try to make a ring out of it. To do so, define:

$$\mathbb{H} = \{a1 + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

We'll define multiplication by extending the Q_8 product linearly.

Indeed, $\mathbb{H}$ is called the **Hamiltonian quaternions**. Interestingly, H is *not* the group ring $\mathbb{R}[Q_8]$. To see this, recall that the dimension of the group ring would be 8, however $\mathbb{H}$ is clearly 4-dimensional.

Notice that every non-zero element is a unit:

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

However, it is not commutative, and thus not a field.

Definition 7.7

Let R be a ring. If R is not commutative and every non-zero element has an inverse, then the ring is called a **division ring**.

Clearly, if a division ring is commutative, then it is a field (*not* a division ring).

Theorem 7.3: Wedderburn

Any finite division ring is commutative, and therefore a field (and not a division ring).

Proof.

The proof is done in the book's exercises. ■

Observe that:

$$\{a + bi\} = \mathbb{C} \subsetneq \mathbb{H} \qquad \{a + cj\} = \mathbb{C} \subsetneq \mathbb{H} \qquad \{a + dk\} = \mathbb{C} \subsetneq \mathbb{H}$$

wow its fucking gauss again.

8 Quadratic Number Fields

Definition 8.1

The **Gaussian integers** is a subset of $\mathbb{C}$ defined as:

$$\mathbb{Z}[\sqrt{-1}] = \left\{a + b\sqrt{-1} : a, b \in \mathbb{Z}\right\} \simeq \{a + bi : a, b \in \mathbb{Z}\}$$

The Gaussian integers form a commutative ring, with inverse given as:

$$(a + b\sqrt{-1})^{-1} = \frac{a - b\sqrt{-1}}{a^2 + b^2}$$

Note that this is not a field, as the elements

$$x = \frac{a}{a^2 + b^2} \qquad y = \frac{b}{a^2 + b^2}$$

need not be integers. So $\mathbb{Z}[\sqrt{-1}]$ is a commutative ring but not a field - quite like ordinary integers.

We can think of this set as:

$$\mathbb{Z}[\sqrt{-1}] \subsetneq \mathbb{Q}[\sqrt{-1}] \subsetneq \mathbb{R}[\sqrt{-1}] = \mathbb{C}$$

The middle one, $\mathbb{Q}[\sqrt{-1}]$ happens to be a field, and we'll study it at a later time.

Can we do something analogous in $\mathbb{H}$?

$$\mathbb{Z}[i, j, k] = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$$

This forms a non-commutative ring, and hence it is not a division ring.

Definition 8.2

In $\mathbb{Z}[\sqrt{-1}]$, we shall call $a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1})$ as the **norm** of $a + b\sqrt{-1}$ (or $a - b\sqrt{-1}$). We write:

$$N(a + b\sqrt{-1}) = a^2 + b^2$$

We'll also call $a - b\sqrt{-1}$ the **complex conjugate** of $a + b\sqrt{-1}$, and write:

$$\overline{a + b\sqrt{-1}} = a - b\sqrt{-1}$$

Note that this is different from calling $\sqrt{a^2 + b^2}$ the norm of $a + bi$.

Easy to see is that $a + b\sqrt{-1}$ is a unit iff $N(a + b\sqrt{-1}) = 1$.

In $\mathbb{H}$, we see that:

$$\overline{a + bi + cj + dk} = a - bi - cj - dk$$

$$N(a + bi + cj + dk) = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

Notice:

$$N\left(\frac{1 + i + j + k}{2}\right) = N\left(\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k\right) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$$

In $\mathbb{Z}[\sqrt{-1}]$, we get that $N(a+b\sqrt{-1})=1$ iff $a=0, b=\pm 1$ *or* $a=\pm 1, b=0$. This leaves us with a choice: To find a subring of $\mathbb{H}$ that is analogous to $\mathbb{Z}$, we could take either of:

$$\mathbb{Z}[i,j,k]=\{a+bi+cj+dk : a,b,c,d\in\mathbb{Z}\} \qquad \mathbb{Z}\left[i,j,k,\frac{1+i+j+k}{2}\right]$$

The first are called the **naive integers**, and the second are called the **Harwitz integers**.

Suppose $D\in\mathbb{Q}^\times$. Consider $\mathbb{Q}[\sqrt{D}]$ given by:

$$\mathbb{Q}[\sqrt{D}]=\left\{a+b\sqrt{D} : a,b\in\mathbb{Q}\right\}$$

It is easy to see that, using the same definitions:

$$N(a+b\sqrt{D})=a^2-Db^2 \qquad (a+b\sqrt{D})^{-1}=\frac{a-b\sqrt{D}}{N(a+b\sqrt{D})}$$

Furthermore, since $N(a+b\sqrt{D})=0$ iff $a=b=0$, then:

$$a^2-Db^2=0 \implies D=\frac{a^2}{b^2}$$

So, we will assume D is non-square.

Notice that taking $D=\sqrt{2}$ creates a field. However, setting $D=\sqrt{18}$ gets that:

$$D=\sqrt{18}=\sqrt{2\cdot 9}=3\sqrt{2}$$

So when we construct the field, it turns out to be the same field. Because of this, we will also assume D is square-free; that is, not divisible by p^2 for any prime p.

Lec 22 - Nov 27 (Week 12)

Consider the set given by $\left\{a+b\sqrt{2} : a,b\in\mathbb{Q}\right\}$. This is a field, as:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+2bd)+(ad+bc)\sqrt{2} \qquad (a+b\sqrt{2})(c+d\sqrt{2})=a^2-2b^2$$

Furthermore, we see that

$$(a+b\sqrt{2})^{-1}=\frac{a-b\sqrt{2}}{a^2-2b^2}$$

and $a^2-2b^2=0 \iff a=b=0$.

A similar construction works for $\mathbb{Q}(\sqrt{3})$, however it does *not* work for $\mathbb{Q}(\sqrt{9})=\mathbb{Q}(3)$. In essence, for any non-zero D which is not a square, we have that $\mathbb{Q}(\sqrt{D})$ is a field. Note that:

$$D'=n^2D \implies \sqrt{D'}=n\sqrt{D} \implies \mathbb{Q}(\sqrt{D'})=\mathbb{Q}(\sqrt{D})$$

For instance, $\mathbb{Q}\left(\sqrt{\frac{3}{5}}\right)=\mathbb{Q}\left(5\sqrt{\frac{3}{5}}\right)=\mathbb{Q}(\sqrt{15})$. In particular, adjoining by $\sqrt{\frac{p}{q}}$ yields the same field as adjoining by $\sqrt{pq}$. Therefore, we can assume $D\in\mathbb{Z}$ is non-zero and not a square.

Furthermore, consider $D=18=2\cdot 3^2$, so $\mathbb{Q}(\sqrt{18})=\mathbb{Q}(\sqrt{2})$. Thus, it suffices to take $D\in\mathbb{Z}$ with $D\neq 0$ to be square-free.

Exercise 8.1

If D, D' are as above, then $\mathbb{Q}(\sqrt{D})$ is not isomorphic to $\mathbb{Q}(\sqrt{D'})$.

Source: Primary Source Material

These are known as the **Quadratic (Number) Fields**.

Definition 8.3

Fix some D as above. The **norm** is a map $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ given by:

$$a + b\sqrt{D} \quad \longmapsto \quad (a + b\sqrt{D})(a - b\sqrt{D}) \;=\; a^2 - b^2 D$$

Some properties:

- N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.
- N is *sub*additive: $N(\alpha + \beta) \leq N(\alpha) + N(\beta)$.
- If $D = -1, \mathbb{Q}(\sqrt{-1}) = \{a + bi : a, b \in \mathbb{Q}\}$ is the Gaussian field. Here, $N(a + bi) = a^2 + b^2$.
- Obviously, if $a, b \in \mathbb{Z}$, then $N(a + b\sqrt{D}) = a^2 - b^2 D \in \mathbb{Z}$. Are these the only such a, b that do this?

Consider $\alpha = \frac{a+b\sqrt{D}}{2}$. Then:

$$N(\alpha) = \left(\frac{a}{2} + \frac{b\sqrt{D}}{2}\right)\left(\frac{a}{2} - \frac{b\sqrt{D}}{2}\right) = \frac{a^2}{4} - \frac{b^2 D}{4} \in \mathbb{Z} \iff 4 \mid a^2 - b^2 D$$

If $D = 2$, then notice that $a^2 - 2b^2 \equiv 0$ if and only if $a, b \equiv 0$ or $2 \bmod 4$. So $N(\alpha)$ will only have integer values if $\frac{a}{2}, \frac{b}{2} \in \mathbb{Z}$. The same happens when $D \equiv 2 \bmod 4$ or $D \equiv 3 \bmod 4$.

Suppose $D \equiv 1 \bmod 4$, for instance if $D = 5$. Then:

$$N\left(\frac{a + b\sqrt{5}}{2}\right) = \frac{a^2 - 5b^2}{4} \qquad a^2 \equiv 0 \bmod 4 \text{ if even} \qquad a^2 \equiv 1 \bmod 4 \text{ if odd}$$

$$a^2 - 5b^2 \equiv \begin{cases} 0 & a, b \text{ both even or odd} \\ 1 & a \text{ odd}, b \text{ even} \\ -1 & a \text{ even}, b \text{ odd} \end{cases}$$

For instance, $N(\frac{1+\sqrt{5}}{2}) \in \mathbb{Z}$.

Turns out, if $D \equiv 1 \bmod 4$, then $N(\alpha) \in \mathbb{Z}$ if and only if α is of the form:

$$\alpha = a + b\sqrt{D} + c\frac{1 + \sqrt{5}}{2} \quad , \quad a, b, c \in \mathbb{Z}$$

Theorem 8.1

For non-zero square-free $D \in \mathbb{Z}$, take ω as:

$$\omega = \begin{cases} \sqrt{D} & D \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \bmod 4 \end{cases}$$

Then, in $\mathbb{Q}(\sqrt{D})$, the elements α such that $N(\alpha) \in \mathbb{Z}$ are exactly $\mathbb{Z}[\omega] = \{a + b\omega\}$, called the ring of integers in $\mathbb{Q}(\sqrt{D})$.

Note $\mathbb{Z}[\omega] \subseteq \mathbb{Q}(\sqrt{D})$.

9 Ring Homomorphisms and Ideals

Lec 23 - Nov 29 (Week 12) or somewhere here at least

A ring homomorphism is exactly what we expect: $\varphi : R \to S$ preserving $+, \cdot$. If R, S are unital, then we often assume $\varphi(1_R) = 1_S$. In particular, a ring homomorphism is a group homomorphism of the additive group of R into the additive group of S. Thus, $\ker(\varphi)$ is the kernel of this group homomorphism.

Next, we want to define quotients. Suppose $I \subseteq R$. Note $I \trianglelefteq R$ as additive groups. Thus, we can take R/I as an additive group.

We want multiplication to be well-defined on the quotient. In particular, we want multiplication to behave as expected, specifically that $(r+I)(r'+I) = (rr'+I)$. However, to be well-defined, we also need it to be irrespective of representation:

$$((r+i)+I)((r'+i')+I) = (r+i)(r'+i')+I = rr'+ri'+ir'+ii'+I$$

Clearly, $ii' \in I$ and $rr' \in R$. Thus, we would want that $ri', ir' \in I$.

Definition 9.1

Let $I \subseteq R$ be a subring. Then, we say that:

- I is called a **left ideal** if $ri \in I$ for all $i \in I$ and $r \in R$.
- I is called a **right ideal** if $ir \in I$ for all $i \in I$ and $r \in R$.
- I is called an **ideal** if it is both a left and right ideal.

Now, it is easy to see that multiplication on I is well-defined iff I is an ideal.

Example

- $n\mathbb{Z}$ are ideals in $\mathbb{Z}$.
- Let $R = \mathbb{F}[x]$ for some field $\mathbb{F}$. Then, the following are ideals:

$$\begin{aligned} (x) &= \{xf(x) : f \in \mathbb{F}\} = \text{polynomials with constant term } 0 \\ (x-a), a \in \mathbb{F} &= \{(x-a)f(x) : f \in \mathbb{F}\}\,\{f(x) : f(a) = 0\} \end{aligned}$$

  The second is of particular importance in algebraic geometry.
- In $R = \mathbb{F}[G]$, the group ring, $\{\alpha = \sum c_g g \in R : \sum c_g = 0\}$ is an ideal.
- In $R = M_n(\mathbb{F})$, the set of matrices with all 0's in the first j columns form a *left* ideal.

Source: Primary Source Material

Theorem 9.1: First Isomorphism for Rings

Suppose $\varphi : R \to S$ is a ring homomorphism. Then, $\ker(\varphi)$ is an ideal, and there exists an isomorphism $\overline{\varphi} : R/\ker(\varphi) \to \operatorname{im}(\varphi)$.

Proof.

We only need to show it holds for multiplication. This is easy. ■

Example

Consider $\psi : \mathbb{F}[x] \to \mathbb{F}$ for some field $\mathbb{F}$, given as the "evaluation map" at a, for some $a \in \mathbb{F}$.

Then, we notice that:

$$\ker(\psi) = \{f : f(a) = 0\} = \{(x-a)f(x) : f \in \mathbb{F}[x]\}$$

Thus, we conclude that $\mathbb{F}[x]/\{(x-a)f(x)\} \simeq \mathbb{F}$.

Source: Primary Source Material

In an extension field $\mathbb{F}$ of $\mathbb{Q}$, we find an analogue $O_{\mathbb{F}}$ of the integers $\mathbb{Z}$ in $\mathbb{Q}$. We would like to extend the idea of a prime number to rings of integers like $O_{\mathbb{F}}$. We'd like to define prime numbers in $O_{\mathbb{F}}$. It is possible, but for some unique fields $\mathbb{F}$, unique factorization doesn't always work. Thus, we work with ideals (ideal numbers) instead.

Definition 9.2

In a commutative unital ring R, an ideal P is a **prime ideal** if and only if for any $x, y \in R$ such that $xy \in P$, then $x \in P$ or $y \in P$.

Clearly in $R = \mathbb{Z}$, ideals are of the form $(n) = n\mathbb{Z}$.

Theorem 9.2

In $R = \mathbb{Z}$, the prime ideals are precisely (p) where p is prime.

Proof.

Suppose $x, y \in (p)$. Then $xy = pk \in (p)$. Clearly:

$$(p_1^{\alpha_1} \cdots p_r^{\alpha_r})(q_1^{\beta_1} \cdots q_s^{\beta_s}) = pk \implies p \mid (p_1^{\alpha_1} \cdots p_r^{\alpha_r}) \text{ or } p \mid (q_1^{\beta_1} \cdots q_s^{\beta_s})$$

Now, suppose n is not prime and (n) is a prime ideal. Then:

$$n = (p_1^{\alpha_1} \cdots p_r^{\alpha_r})$$

for distinct primes p_i. Notice that $r \geq 2$ *or* $\alpha_1 > 1$. But then:

$$n = p_1 \cdot (p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r})$$

This is a contradiction, as neither factor is in (n). ■

Source: Primary Source Material

Theorem 9.3

Let R be commutative and unital, with P a prime ideal. Then, R/P is an integral domain.

Proof.

Note $\overline{xy} = \overline{0} = 0 + p = p$, so $xy \in P$. Then, since P is prime, $x \in P$ or $y \in P$, which implies that $\overline{x} = 0$ or $\overline{y} = 0$ as needed. ■

Source: Primary Source Material

Theorem 9.4

If R/P is an integral domain, then P is a prime ideal.

Proof.

Suppose $xy \in P$. Then:

$$\overline{xy} = \overline{0} \implies \overline{x}\overline{y} = \overline{0} \implies \overline{x} = \overline{0} \text{ or } \overline{y} = \overline{0} \implies x \in P \text{ or } y \in P$$

as needed. ■

Source: Primary Source Material

Lec 24 - Jan 08 (Week 13)

why are there repeats. For today (at least), we will denote by R a ring with unit $1 \neq 0$.

Definition 9.3

Suppose $A \subseteq R$. Then $\langle A \rangle$ is the smallest ideal of R containing A.

Note that the set given by

$$RA = \left\{ \sum r_i a_i : r_i \in R, a_i \in A, \text{ finite sum} \right\}$$

is in fact a left ideal. Analagously, AR is a right ideal, and RAR is an ideal. Clearly, if R is commutative, then these are all the same.

Definition 9.4

If $A = \{a\}$ such that $\langle A \rangle = \langle a \rangle$ is an ideal, then $\langle a \rangle$ is called the **principal ideal** generated by a, more often written as (a).

Example

In $R = \mathbb{Z}$, every ideal is principal; i.e., $(n) = n\mathbb{Z}$.

However, in $R = \mathbb{Z}[x]$, polynomials with integer coefficients, $I = \langle 5, x \rangle$ is a non-principal ideal. This ideal represents all polynomials whose constant term is a multiple of 5.

In particular, this ideal contains 5, and so we have that $5 = f(x)g(x)$. The constant term of fg is the product of the two constant terms, and so the constant term of f must be 5; similarly, the constant term of g must be 1.

On the otherhand, the highest order term of fg is the product of the highest order terms. In this case, the highest order terms of f and g must thus be constants, and so $f = 5$ and $g = 1$.

But if $f = 5$, then we can't write $x \in I$ as $5h(x)$ for any h. Thus, I does not have a singular generator, and is therefore *not* principal.

Source: Primary Source Material

Given $\mathbb{F}[x_1, \dots, x_n]$ (for $n > 1$, a field $\mathbb{F}$), any ideal $I = (x_{i_1}, x_{i_2}, \dots, x_{i_k})$ is not principal when $k > 1$.

Strangely, in $\mathbb{F}[x]$, *every* ideal is principal. We will prove this later. (Note that this was false in $\mathbb{Z}[x]$!)

For example, consider R as the ring of all functions on $\mathbb{R}$. Fix $a \in \mathbb{R}$, and let $I = I_a = \{f(x) : f(a) = 0\}$. This is in fact a principal ideal.

To see this, let $d(x) = \begin{cases} 0 & x = a \\ 1 & \text{otw} \end{cases}$ and see that for any $f \in I$, we have $f(x) = f(x)d(x)$, and so $I = \langle d(x) \rangle$.

In the analogous ring of continuous functions over $\mathbb{R}$, the corresponding ideal $I_a = \{f : f(a) = 0\}$ is not principal. Even worse: it is not generated by any finite set!

Theorem 9.5

If I is an ideal in R, then $I = R$ iff I contains a unit (the invertible one).

Definition 9.5

In a unital ring, an ideal P is a **prime ideal** if:

$$xy \in P \implies x \in P \text{ or } y \in P$$

As a trivial example, with $R = \mathbb{Z}$, take any prime p. Then (p) is clearly a prime ideal. Clearly this holds iff p is prime: if we instead take p^2, we see that (p^2) is not a prime ideal (consider $x = y = p$).

Another example: take $\mathbb{F}[x_1, \dots, x_n]$. Then $(x_{i_1}, \dots, x_{i_k})$ is a prime ideal for any $k \geq 1$.

Definition 9.6

In a unital ring, an ideal M is a **maximal ideal** if there is no larger proper ideal. That is, if I is an ideal such that $M \subseteq I \subsetneq R$, then $I = M$.

Theorem 9.6

If M is a maximal ideal of R, then R/M has no ideals, and so every element is invertible.

In particular, if R is commutative, then R/M is a field iff M is maximal.

Theorem 9.7

If R is commutative, then R/P is an integral domain iff P is a prime ideal.

Corollary

If R is a unital commutative ring, then any maximal ideal is prime.

For example, in $\mathbb{F}[x_1, \dots, x_n]$, $M = (x_1, \dots, x_n)$ is maximal. Then, we have that $\mathbb{F}[x_1, \dots, x_n]/M \simeq \mathbb{F}$, given by $f \mapsto f(0, \dots, 0) \in \mathbb{F}$.

10 Division Rings and Domains

If we start with $\mathbb{Z}$, we can't divide, so we'd like to "enlarge" $\mathbb{Z}$ into something with division. We construct $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ and define addition and multiplication.

Problem: $\dfrac{a}{b}$ is not unique. Thus, we need to check that $+, \cdot$ are well-defined.

Doing the same construction with any ring R instead of $\mathbb{Z}$ yields what we call the **Ring of Fractions**.

Given a commutative unital ring R, consider ordered pairs (a, b) where $a, b \in R$ and b is not a zero divisor. We want to define addition and multiplication on this set.

$$(a, b) \cdot (c, d) = (ac, bd) \qquad (a, b) + (c, d) = (ad + bc, bd)$$

Note that the product of two non zero divisors is a non zero divisor.

Next, we define an equivalence relation:

$$(a, b) \sim (c, d) \iff ad = bc$$

Of course, we need to check this is preserved by $+, \cdot$.

Suppose $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$; that is $ab' = a'b$ and $cd' = c'd$. We want to check if $(a, b) \cdot (c, d) \sim (a', b') \cdot (c', d')$. Indeed:

$$(a, b) \cdot (c, d) = (ac, bd) \quad (a', b') \cdot (c', d') = (a'c', b'd') \qquad acb'd' = a'c'bd = ac'b'd = acb'd'$$

Addition is similar, but worse, so we skip it for now. This gives us the definition (construction) of the ring of fractions.

Definition 10.1

Given a commutative unital ring, the **ring of fractions** is the set given by $R^2/\sim$ equipped with addition and multiplication, where $\sim, +, \cdot$ are defined as above.

Clearly for $\mathbb{Z}$, we get $\mathbb{Q}$. For $R = \mathbb{F}[x]$, then we get what is known as the rational functions:

$$\left\{ \frac{f(x)}{g(x)} : f, g \in R \right\}$$

Note that strictly speaking, these are not functions on $\mathbb{F}$, as g is undefined on at least 0. Restricting the domain does turn these into functions.

Note, however, that the points at which g is 0 might be different for an equivalent representation.

Lec 25 - Jan 10 (Week 13)

Suppose R is a commutative, not necessarily unital ring. Suppose D is a subset of R that does not contain any zero divisors, and which is closed under multiplication. The elements of D are thus allowed to be denominators in the ring of fractions. If R has no zero divisors, then an obvious choice is $D = R \setminus \{0\}$.

Observe that there is a ring Q which contains an isomorphic copy of R such that every element of D in R has an inverse in Q. Moreover, Q is the smallest ring with these properties.

If R has no zero divisors and we choose the obvious choice of D, then Q is a field, called the **field of fractions**, or sometimes the **quotient field**.

Example

Let $R = \mathbb{Z}$. Choose a prime number p, and let D be defined as:

$$D = \{d \in R : p \nmid d\} = \{d \in R : \gcd(p, d) = 1\}$$

The ordered pairs we consider are (n, d), where $p \nmid d$. In particular, every prime $q \neq p$ is in D, and so $\frac{1}{q} \in D$. So in the ring of fractions Q, every prime other than p is invertible.

Source: Primary Source Material

Exercise 10.1

Not too difficult: Show that in the above, (p) is the unique prime ideal in Q.

Source: Primary Source Material

Definition 10.2

A ring with a single prime ideal is called a **local ring**.

In $\mathbb{C}[x_1, \ldots, x_n]$, the maximal ideals are of the form

$$I_a = \{f : f(a) = 0\} \qquad a \in \mathbb{C}$$

In particular, they are the *only* maximal ideals. Thus, we observe that maximal ideals represent points in $\mathbb{C}^n$. Vaguely: a local ring focuses attention on what happens “near” a point a, ignoring the global behaviour. (This is the start of algebraic geometry.)

Lemma

Suppose $\gcd(M, N) = 1$ for $M, N \in \mathbb{Z}^{>0}$, and suppose $a, b \in \mathbb{Z}$. Then there exists a unique $n \in \mathbb{Z}_{MN}$ such that:

$$n \equiv a \bmod M \qquad n \equiv b \bmod N$$

This is a familiar theorem that's not hard to show. We expand this now to our rings.

Definition 10.3

Let R be a commutative unital ring. Two ideals $A, B \subseteq R$ are **comaximal** if:

$$A + B = R \quad \text{i.e.} \quad A + B = (1)$$

This generalizes the idea of coprimality in $\mathbb{Z}$.

Suppose $A_1, \dots, A_k$ are pairwise comaximal ideals in R. Consider the map $\varphi : R \to R/A_1 \times \cdots \times R/A_k$ given by:

$$\varphi(r) = (r + A_1, \dots, r + A_k)$$

Note that $\ker(\varphi) = A_1 \cap \cdots \cap A_k$. Furthermore, the reverse inclusion ($\supseteq$) is always true.

Theorem 10.1: Chinese Remainder Theorem(?)

In the above scenario, we have that:

$$A_1 \cap \cdots \cap A_k = A_1 \cdots A_k$$

Recall that the product of ideals I, J is defined as:

$$IJ = \{i_1 j_1 + i_2 j_2 + \cdots + i_t j_t : i_k \in I, j_k \in J\}$$

Proof.

We prove $A \cap B = AB$ if $A + B = R$, as the rest follows from induction.

The key is that:

$$\varphi(a + b) = \varphi(1) = 1 \quad \varphi(a) = (1, 0) \in R/A + R/B \quad \varphi(b) = (0, 1)$$

■

Source: Primary Source Material

Lec 26 - Jan 15 (Week 14)

Consider 26180 and 80262. What is their gcd? We can use the Euclidean algorithm to find it:

$$80262 = 26180 \cdot 3 + 1722$$

Notice that if $d \mid 26180$ and $d \mid 1722$, then $d \mid 80262$. So:

$$\gcd(80262, 26180) = \gcd(26180, 1722)$$

We can repeat this process to deduce that $\gcd(80262, 26180) = 14$.

Definition 10.4

An integral domain R is called a **Euclidean domain** if it has a “norm” N such that:

- $N : R \to \mathbb{Z}^{\geq 0}$
- $N(0) = 0$
- Given $a, b \in R$, we can write a = bq + r with $N(a) < N(b)$, unless $r = 0$.

Note that a given ring R may have many norms, and some may even have a Euclidean algorithm, but the gcd you end up with will be the same.

Definition 10.5

An integral domain R is called a **Principal Integral Domain (PID)** if every ideal is a principal ideal.

Theorem 10.2

Every Euclidean domain is a PID.

Proof.

Sps R is Euclidean with I as some ideal. Choose $d \in I$ such that $N(d)$ is minimal.

Then, given any $a \in I$, we have that $a = dq + r$. Since $a, dq \in I$, then we must have $r \in I$ and $N(r) < N(d)$. This gives a contradiction, so we must have that $a = dq$. ■

Source: Primary Source Material

Example

$\mathbb{F}[x]$ is a Euclidean domain with norm given by the degree. Thus, it is a PID.

Source: Primary Source Material

Beware:

- $\mathbb{Z}[x]$ is *not* a PID; consider $(x, 5)$.
- $\mathbb{F}[x, y]$ is *not* a PID; consider (x, y).
- Similarly, $\mathbb{F}[x_1, \ldots, x_n]$ is *not* a PID.

Theorem 10.3

If R is an integral domain and $R[x]$ is a PID, then R is a field.

Proof.

Take $R[x]/(x) \simeq R$ by FIT. Since R is an integral domain, (x) is prime. Is (x) maximal?

Suppose not, and suppose $(x) \subsetneq (f(x))$ for some $f(x)$. In particular, $x \in (f(x))$, and so $x = f(x)g(x)$. Thus, f, g must be of degrees 1 and 0.

If f has degree 0, it must be constant and non-zero. Thus:

$$g(x) = a + bx \implies f(x)g(x) = c(a + bx) \implies ca + cbx$$

Thus, we must have that $a = 0, cb = 1$, and so $f(x) = 1$. But then it follows that $(f(x)) = (1) = R[x]$, which is not a proper subset.

Now suppose $g(x)$ has degree 0, the degree of $f(x)$ is 1. Then, $g(x) = c \neq 0$ and $f = a + bx$. Similarly as before:

$$f(x)g(x) \implies f(x)g(x) = x \implies ca + cbx \implies a = 0, c \text{ unit} \implies (f(x)) = (bx) \implies x$$

Hence (x) is indeed maximal, and so $R[x]/(x)$ is a field. ■

Source: Primary Source Material

Definition 10.6

An integral domain R is a **Dedekind domain (DD)** if, given any ideal I, it is possible to find prime ideals $p_1, \dots, p_k$ and natural numbers $r_1, \dots, r_k$ such that each p_i is distinct (non-isomorphic), and:

$$I = p_1^{r_1} \dots p_k^{r_k}$$

Furthermore, this decomposition is unique up to order.

Definition 10.7

An integral domain R is a **Unique Factorization domain (UFD)** if, given $a \in R$ such that $a \neq 0$, it can be written as:

$$a = p_1^{r_1} \dots p_k^{r_k}$$

where the p_i's are irreducible elements, and each p_i, p_j are distinct even up to multiplication by units. This decomposition is also unique up to ordering.

Between the different domains, we can describe them as such:

$$\text{Euclidean domain} \subseteq \text{Principal Ideal domain} \subseteq \text{Unique Factorization domain} \subseteq \text{Integral domain}$$

Also note that D&F discusses Hasse norms. Having a Hasse norm is equivalent to being a PID.

Example: Lagrange Interpolation

Given points $a_1, \dots, a_n, b_1, \dots, b_n$, with each a_i distinct, is it possible to find a polynomial f with degree less than n such that $f(a_i) = b_i$ for each i?

In $\mathbb{F}[x], I_i = (x - a_i)$ is the ideal of all polynomials vanishing at a_i. Set:

$$I = I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$$

Then, a polynomial with the specified values amounts to a point in $\mathbb{F}[x]/I$. CRT says that this is determined uniquely by a point in each $\mathbb{F}[x]/I_i$.

Source: Primary Source Material

Lec 27 - Jan 17 (Week 14)

Recall that in an integral domain, an element r being prime means that:

$$r \mid ab \implies r \mid a \text{ or } r \mid b$$

Definition 10.8

An element r is **irreducible** if whenever $r = ab$, either a or b is a unit.

Notice that in $\mathbb{Z}$, p is prime iff p is irreducible.

Example

Let $R = \mathbb{Z}[\sqrt{-5}]$. Then, there is a norm on R given by:

$$N(a + b\sqrt{-5}) \ = \ a^2 + 5b^2 \ = \ (a + b\sqrt{-5})(a - b\sqrt{-5})$$

It is easy to see that N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Consider $3 \in R$. Notice:

$$(2 + \sqrt{-5})(2 - \sqrt{-5}) \ = \ 4 + 5 \ = \ 9$$

In particular:

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}) \qquad 3 \nmid (2 \pm \sqrt{-5}) \qquad 3(x + y\sqrt{-5}) = 3x + 3y\sqrt{-5}$$

So we see that in this case, 3 is not prime. However, we claim that 3 is irreducible.

Indeed, suppose that $3 = \alpha(a + b\sqrt{-5})$. Then:

$$9 = N(\alpha)(a^2 + 5b^2)$$

Since $N(\alpha) \in \mathbb{Z}$, then $a^2 + 5b^2$ must divide 9, so it must be $1, 3$, or 9.

- If $a^2 + 5b^2 = 1$, then $b = 0, a = \pm 1$, so $a + b\sqrt{-5}$ is a unit.
- Similarly, if $a^2 + 5b^2 = 9$, then $N(\alpha) = 1$, so α is a unit.
- Suppose $a^2 + 5b^2 = 3$. Then, $b = 0$ and $a^2 = 3$, which isn't possible. Indeed, if $3 = \alpha\beta$, we can't have $N(\alpha) = 3$, so must have either $N(\alpha) = 1$ or $N(\beta) = 1$. Thus, one factor is a unit.

Source: Primary Source Material

Theorem 10.4

In an integral domain, r prime $\implies$ r irreducible.

Proof.

Suppose p is prime. If $p = ab$, then (wlog) $p \mid a$. Thus, $a = px$ for some x. Thus:

$$p = ab = pxb \implies 1 = xb$$

So b is a unit. ■

Source: Primary Source Material

Theorem 10.5

If R is a PID, then r prime $\iff$ r irreducible.

Proof.

Suppose p is irreducible. We show that (p) is maximal.

Suppose $(p) \subseteq I = (q)$. Then $p \in I \implies p = qr$, so r is a unit. Thus, $q = pr^{-1}$, so $(p) = (q)$. ■

Source: Primary Source Material

So for PID's, prime is equivalent to irreducible. How nice!

Suppose R is a UFD, with:

$$x = up_1^{r_1} \cdots p_k^{r_k} \qquad y = u' q_1^{s_1} \cdots q_\ell^{s_\ell}$$

What is $\gcd(x, y)$? We can reorganize the p's and q's such that:

$$p_1 = q_1 \quad p_2 = q_2 \quad \ldots \quad p_j = q_j$$

But the remaining p_i's are not among the q_i's and vice versa. Then:

$$\gcd(x, y) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_j^{\min(r_j, s_j)}$$

Theorem 10.6

In a UFD, primes are equivalent to irreducibles.

The proof is long; see D&F.

Lec 29 - Jan 22 (Week 15)

Recall quadradic fields $\mathbb{Q}(\sqrt{D})$, where D is a square-free integer. The ring of integers O in $\mathbb{Q}(\sqrt{D})$ is given by:

$$O = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \bmod 4 \end{cases}$$

We write $\omega = \sqrt{D}$ or $\frac{1+\sqrt{D}}{2}$ accordingly, so:

$$O = \{a + b\omega : a, b \in \mathbb{Z}\}$$

Here, we have a (field) norm $N : O \to \mathbb{Z}$ given as:

$$N(a + b\omega) = (a + b\omega)(a - b\overline{\omega})$$

where $\overline{\omega} = -\sqrt{D}$ or $\frac{1-\sqrt{D}}{2}$. When $\omega = \sqrt{D}$, we have that:

$$N(a + b\omega) = N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$$

If α is a unit, then there exists $\beta \in O$ such that $\alpha\beta = 1$. Since $N(\alpha\beta) = N(\alpha)N(\beta)$, then $N(1) = 1$. Since $N(\alpha), N(\beta) \in \mathbb{Z}$, then we must have that $N(\alpha) = N(\beta) = \pm 1$.

The converse also happens to be true; if $N(\alpha) = \pm 1$, then α is a unit:

$$1 = N(\alpha) = \alpha\overline{\alpha} \in O \implies \overline{\alpha} = \alpha^{-1}$$

So $\alpha \in O$ is a unit iff $N(\alpha) = \pm 1$.

Theorem 10.7

Suppose $\pi \in O$ is a prime element, so (π) is a prime ideal. Then, $(\pi) \cap \mathbb{Z}$ is a prime ideal.

Proof.

Let $a, b \in \mathbb{Z}$ such that $ab \in (\pi) \cap \mathbb{Z}$. Then, a, b can be regarded as elements of O, and $ab \in (\pi)$, so $a \in (\pi)$ or $b \in (\pi)$. Hence $a \in (\pi) \cap \mathbb{Z}$ or $b \in (\pi) \cap \mathbb{Z}$, and thus it is a prime ideal. We'll write $(\pi) \cap \mathbb{Z} = (p)$. ■

Source: Primary Source Material

Suppose $p = \pi_1\pi_2 \in O$. Then $N(p) = N(\pi_1)N(\pi_2) = p^2$. Then, we must have one of the following:

$$N(\pi_1) = \pm 1 \quad , \quad N(\pi_2) = \pm p^2$$
$$N(\pi_1) = N(\pi_2) = \pm p$$

If $N(\pi_1) = \pm 1$, then π_1 is a unit, and so p is irreducible as an element of O. However, if we have that $N(\pi_1) = N(\pi_2) = \pm p$, then $p = \pi_1\pi_2$ factors as the product of two irreducibles in O.

Special case: in the Gaussian integers $(D = -1)$, we have that $O = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. Here:

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

It's easy to see that this works as a "norm" for the Euclidean algorithm, and so $\mathbb{Z}[i]$ is a PID.

In $\mathbb{Z}[i]$, notice that not every norm is achievable:

$$\begin{array}{cccc}
1 = 1^2 + 0^2 & 2 = 1^2 + 1^2 & 3 = \varnothing & 4 = 2^2 + 0^2 \\
5 = 2^2 + 1^2 & 6 = \varnothing & 7 = \varnothing & 8 = 2^2 + 2^2 \\
 & 9 = 3^2 + 0^2 & 10 = 3^2 + 1^2 &
\end{array}$$

Which integers can be written as a sum of two squares? This was actually proven by Fermat. As a hint, start with the following: which primes p can be written as the sum of two squares?

11 Polynomial Rings over Fields

Recall that $\mathbb{F}[x]$ is a PID, and $\mathbb{F}[x_1, \ldots, x_n]$ is a UFD.

In $\mathbb{F}[x]$, $(x - a)$ is a maximal ideal for any $a \in \mathbb{F}$. The evaluation map $E_a : \mathbb{F}[x] \to \mathbb{F}$ is a homomorphism given by $E_a : f(x) \to f(a)$. This is clearly surjective (due to constant polynomials), and the kernel is $(x - a)$.

Lemma

Factor theorem: if $f(a) = 0$, then $(x - a) \mid f(x)$. In particular, there exists $g(x)$ such that $f(x) = (x - a)g(x)$, so $f(x) \in (x - a)$.

Therefore, we have that:

$$\mathbb{F}[x]/(x-a) \simeq \{f(a) + (x-a) : f \in \mathbb{F}[x]\} = \{c + (x-a) : c \in \mathbb{F}\} = \{c : c \in \mathbb{F}\} = \mathbb{F}$$

In $\mathbb{C}[x]$, these are the only maximal ideals (this holds for any algebraically closed field). Any maximal ideal is principal, say $(g(x))$. Over any algebraically closed field, $g(x)$ can be factored completely:

$$g(x) = (x - a_1)(x - a_2) \cdots (x - a_d)$$

Note that if $d > 1$, then:

$$((x - a_1) \cdot \cdots \cdot (x - a_d)) \subsetneq (x - a_i)$$

In $\mathbb{C}[x_1, \ldots, x_n]$ for $n > 1$, the maximal ideals are all of the form

$$((x - a_1), (x_2 - a_2), \ldots, (x_n - a_n))$$

for some $a_i \in \mathbb{C}$.

Example

Consider $\mathbb{F}_3[x]/x^2 + 1$. Does $x^2 + 1$ factor over $\mathbb{F}_3$? If so, it has a root. But:

$$f(0) = 1 \qquad f(1) = 2 \qquad f(2) = 5 = 2$$

So $x^2 + 1$ is irreducible. Modding out by $x^2 + 1$ "means" we set $x^2 + 1 = 0$, so:

$$x^2 + 1 = 0 \implies x^2 = -1 \implies x = \sqrt{-1}$$

So we compromise: $x = i$, with $i^2 = -1$. Then, $\mathbb{F}_3[x]/x^2 + 1$ is:

$$\mathbb{F}_3[x]/x^2 + 1 = \begin{array}{ccc} 0 & 1 & 2 \\ x & x+1 & x+2 \\ 2x & 2x+1 & 2x+2 \end{array}$$

In any polynomial of degree more than 1, we replace $x^2 = 2 = -1$. This yields precisely $\mathbb{F}_9$, the finite field of 9 elements.

Of course, we should check this is indeed a field. For instance, what is $(2x + 1)^{-1}$?

$$(2x+1)(ax+b) = 1 \implies 2ax^2 + (2b+a)x + b = 1 \implies 4a + (2b+a)x + b = 1$$
$$2b + a = 0 \quad , \quad 4a + b = 1 \implies a = b = 2$$

So $(2x + 1)^{-1} = (2x + 2)$.

Source: Primary Source Material

Given a prime p, there is, up to isomorphism, exactly one field of order p^m for each $m \in \mathbb{N}$. We denote this field $\mathbb{F}_{p^m}$. This field can be constructed as $\mathbb{F}_p[x]/f(x)$, where $f(x)$ is an irreducible polynomial of degree m over $\mathbb{F}_p$.

Lec 30 - Jan 24 (Week 15)

Which primes p can be written as a sum of two squares? Which naturals can be written as such?

Recall quadratic fields: $\mathbb{Q}[\sqrt{D}]$, for non-zero square-free D. Consider the ring of integers O in $\mathbb{Q}[\sqrt{D}]$. Note that if $\pi \in O$ such that $N(\pi)$ is prime, then π is irreducible. Suppose $N(\pi) = p$ for some prime $p \in \mathbb{Z} \subsetneq O$. Since $p = N(\pi) = \pi\overline{\pi}$, then $\pi \mid p$ in O. Since $N(p) = p^2$, we have a few possibilites:

- $N(\pi) = 1, N(\overline{\pi}) = p^2$
- $N(\pi) = N(\overline{\pi}) = p$
- $N(\pi) = p^2, N(\overline{\pi}) = 1$

The first is impossible since π is prime, and thus *not* a unit. The second is possible if both are irreducible, and the third is possible if $\overline{\pi}$ is a unit, thus making p prime.

So, either p is prime in O or $p = \pi\overline{\pi}$, so it "splits" into two irreducibles in O.

Example

In $\mathbb{Z}[i]$, notice that:

$$5 = 4^2 + 1^2 = (2+i)(2-i)$$

So the integer prime 5 splits into two primes in $\mathbb{Z}[i]$. By contrast, 3 is already prime in $\mathbb{Z}[i]$:

$$3 \neq a^2 + b^2 \quad \forall\, a, b \in \mathbb{Z}$$

Source: Primary Source Material

Special case: $2 = 1^2 + 1^2$.

Now, assume p is odd. Consider $\mathbb{F}_p^\times$ with order $p-1$. Then $F_p^\times$ is an abelian group with order $p-1$. Notice the element -1 has order 2. We claim that it is the *only* such element.

Indeed, any such element must satisfy:

$$x^2 - 1 = 0 \implies (x+1)(x-1) = 0 \implies x = \pm 1$$

Clearly 1 does not have order 2, and so we must have $x = -1$.

If $p \equiv 1 \bmod 4$, then $4 \mid p - 1 = \left|\mathbb{F}_p^\times\right|$.

Lemma

If $p \equiv 1 \bmod 4$, then $\mathbb{F}_p^\times$ has an element of order 4.

Proof.

Note that $\left|\mathbb{F}_p^\times / \{\pm 1\}\right|$ is even.

Any group of even order has an element of order 2, say $\overline{x}$. The element $x \in \mathbb{F}_p^\times$ must have order 2 or 4.

It can't have order 2, because we already modded out by ± 1, and -1 is the unique element of order 2. ■

Source: Primary Source Material

Lemma

If p is an odd prime, then $p \mid (n^2+1)$ for some $n \in \mathbb{Z}$ iff $p \equiv 1 \bmod 4$.

Proof.

Note that:

$$p \mid (n^2+1) \iff n^2+1 \equiv 0 \bmod p \iff n^2 \equiv -1 \bmod p$$

In other words, this amounts to saying that -1 is a square. But if $p \equiv 3 \bmod 4$, then $4 \nmid p-1 \equiv 2 \bmod 4$, so there is no element of order 4. Thus, -1 cannot be a square.

On the other hand, if $p \equiv 1 \bmod 4$, then $4 \mid p-1$, and -1 is the square of an element of order 4:

$$n^2 \equiv -1 \bmod p \implies n^2+1 \equiv 0 \bmod p$$

■

Source: Primary Source Material

If $p \equiv 1 \bmod 4$, then $p \mid (n^2+1)$, i.e. $p \mid (n+i)(n-i)$. So p must divide $n+i$ or $n-i$. But p must divide *both* complex conjugates, so $p \mid (n+i)$ and $p \mid (n-i)$, so $p \mid 2i$. “That’s bullshit.” -Joe

This shows that p is not prime in O, that is, there exists some a, b such that:

$$p = (a+bi)(a-bi) \implies p = a^2+b^2$$

Note this does not tell us how to *find* such primes.

Exercise 11.1

Show that $(a^2+b^2)(c^2+d^2)$ is a sum of two squares for all $a, b, c, d \in \mathbb{Z}$.

Source: Primary Source Material

Theorem 11.1

Suppose $n = 2^a p_1^{r_1} \cdots p_k^{r_k} q_1^{s_1} \cdots q_\ell^{s_\ell}$, where $p_i \equiv 1 \bmod 4$ and $q_i \equiv 3 \bmod 4$. Then n is a sum of two squares iff each s_i is even.

Proof.

See book - it’s “not hard”, says Joe. ■

Source: Primary Source Material

Lec 31 - Jan 29 (Week 16)

Recall that given $\mathbb{F}[x]$, PID $\implies$ UFD when $\mathbb{F}$ is a field. We also know that $\mathbb{F}[x_1, \ldots, x_n]$ is never a PID. What else can we say? We can actually show that $\mathbb{F}[x_1, \ldots, x_n]$ is a UFD. Furthermore, if $R[x_1, \ldots, x_n]$ is a UFD, then R is too!

Definition 11.1

Let R be a UFD, and consider $R[x_1, \dots, x_n]$. If $I \subseteq R$ is an ideal, we write $(I) = R[x_1, \dots, x_n]I$ as the ideal in $R[x_1, \dots, x_n]$ generated by I.

Lemma

$R[x_1, \dots, x_n]/(I) \simeq (R/I)[x_1, \dots, x_n]$

(I) is polynomials with coefficients in I. Modding out by them removes all polynomials with said coefficients; thus, the coefficients are in R/I.

Example

Let $R = \mathbb{Z}, I = (p)$ for some prime p. Then:

$$\mathbb{Z}[x_1, \dots, x_n]/(p) \simeq (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n] = \mathbb{F}_p[x_1, \dots, x_n]$$

Source: Primary Source Material

Theorem 11.2

If I is a prime ideal in R, then

$$(I) \subseteq R[x_1, \dots, x_n]$$

is a prime ideal.

Proof.

Note $R[x_1, \dots, x_n]/(I) \simeq (R/I)[x_1, \dots, x_n]$. Since I is prime, R/I is an integral domain, so $(R/I)[x_1, \dots, x_n]$ is an integral domain. Thus $R[x_1, \dots, x_n]/(I)$ is an integral domain, and so (I) must be prime. ■

Source: Primary Source Material

This leads to a very important result in the field.

Theorem 11.3: Gauss' Lemma

Suppose R is a UFD. Let F be its field of fractions, so $R \subseteq F$ (Gauss says $\mathbb{Z} \subseteq \mathbb{Q}$). Suppose $f(x) \in R[x] \subseteq F[x]$.

If f is reducible in $F[x]$, then it is reducible in $R[x]$. In particular, if:

$$f(x) = A(x)B(x) \quad , \quad A(x), B(x) \in F[x]$$

then there exist $p(x), q(x) \in F[x]$ such that:

$$a(x) = p(x)A(x) \in R[x] \qquad b(x) = q(x)B(x) \in R[x] \qquad f(x) = a(x)b(x)$$

In other words, f factors over $R[x]$ as well.

Proof.

Suppose $f(x) = A(x)B(x) \in F[x]$. Let $d =$ lcm of denominators of A, and similarly define $d' =$ lcm of denominators of B. Then, $dd'f(x) = dA(x)d'B(x)$.

If dd' is a unit in R then we can multiply by $(dd')^{-1}$ and we're done. Otherwise, since R is a UFD, we can factor into primes:

$$dd' = up_1 \cdots p_m$$

Thus each $p_i \mid d$ or d'. But as an element of $R[x]$, we know that it divides $dA(x)d'B(x)$.

Thus, p_i divides either $dA(x)$ or $d'B(x)$. Thus, we can cancel p_i from $dd'f(x) = dA(x)d'B(x)$. Note that they are still in $R[x]$ after such a cancellation.

Repeating this cancellation for each p_i, we end up with:

$$f(x) = p(x)A(x)q(x)B(x)$$

where p, q are whatever is leftover after repeated cancellation. ■

Source: Primary Source Material

Theorem 11.4

R is a UFD iff $R[x]$ is a UFD.

Proof.

First, suppose $R[x]$ is a UFD. Then, any constant polynomial r can be factored into primes in $R[x]$:

$$r = p_1 \cdots p_m$$

where each p_i is constant. Moreover, (p_i) is prime in $R[x]$, so p_i is prime in R. Thus, r factors into primes in R, and so R is a UFD.

Suppose R is a UFD. (Outline) Let $f(x) \in R[x] \subseteq F[x]$. F is a field, hence a PID and thus a UFD, so then:

$$f(x) = up_1 \cdots p_m \in F[x]$$

where each p_i is a prime unit in $F[x]$. Again, we clear denominators to get a factorization in $R[x]$. For each p_i choose $d_i =$ lcm of coefficients of p_i, and thus $d_ip_i \in R[x]$. Then:

$$\prod_i (d_i)f(x) = ud_1p_1 \cdots d_mp_m$$

To save time, use Gauss' Lemma, giving us:

$$f(x) = q_1q_2 \cdots q_n$$

factors in $R[x]$. (joe what the hell) ■

Source: Primary Source Material

Thus, R is a UFD iff $R[x]$ is a UFD. Note we can do this for any number of variables by doing induction. This tells us that in $R[x_1, \ldots, x_n]$ and $\mathbb{F}[x_1, \ldots, x_n]$, primes are the *same* as irreducibles.

In $R[x_1, \ldots, x_n]$, how do we check if a polynomial is irreducible? Starting with $\mathbb{F}[x]$, clearly linear polynomials are always irreducible. Constants are units. For quadratics ax^2+bx+c, they can only factor into two linears.

Thus a quadratic is reducible iff it has a root in $\mathbb{F}$.

Example

Over $\mathbb{R}$, the quadratic $x^2 + 1$ is irreducible. However, in $\mathbb{C}$, we know that:

$$x^2 + 1 = (x + i)(x - i)$$

Source: Primary Source Material

In an algebraically closed field like $\mathbb{C}$, all polynomials factor into linear terms. Thus, the only primes are linear.

Cubics either split into linears or a linear times a quadratic, so they're prime iff they have a root. Over $\mathbb{R}$, IVT tells us that every cubic has a root.

Quartics are different. Over $\mathbb{Q}$, we have that $x^4 - 4 = (x^2 + 2)(x^2 - 2)$. And yet, it has no roots in $\mathbb{Q}$. (Note each quadratic is irreducible here.)

There's a nice tool to help us determine when a polynomial is irreducible.

Example

Consider $x^{12} - 3x^7 + 6x^4 - 9x^3 + 3$. If it factors, then it must look like:

$$(x^? \pm \cdots \pm 3)(x^? \pm \cdots \pm 1)$$

Note these terms may or may not be divisible by 3.

Source: Primary Source Material

Lemma: Eisenstein's Criterion

Suppose p is prime and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $p \mid a_i$ and $p \mid\mid a_0$. Then, $f(x)$ is irreducible.

In the above example, notice 3 divides each term, but $9 \nmid a_0$.

Example

Suppose $n > 1$. Then $x^n - a$ is irreducible if there is any prime p such that $p \mid\mid a$. For instance:

- $x^{12} - 12 \quad (3 \mid\mid 12)$
- $x^4 - 10 \quad (5 \mid\mid 10)$

Source: Primary Source Material

The *cyclotomic polynomial* $x^n - 1$ has roots being the n roots of unity. It is *not* irreducible since 1 is a root. Instead, consider:

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

Suppose n is prime ($n = p > 2$). Then:

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

However, consider:

$$\begin{aligned} f(x+1) &= (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1)^2 + (x+1) + 1 \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{1}{1}x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{1}x + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + \binom{p}{1} \end{aligned}$$

So by Eisenstein's Criterion, it is irreducible, and so $f(x)$ is also irreducible.

Proof: Eisenstein's Criterion.

Over $\mathbb{Z}$, suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where $p \mid a_i, p \mid\mid a_0$.

Suppose that f is reducible, that is:

$$f(x) = (x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0)(x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0)$$

Then $p \mid\mid a_0 \implies p \mid b_0$ or $p \mid c_0$. WLOG, suppose $p \mid b_0$ and $p \nmid c_0$. Then, we have that the coefficient of x_k is:

$$a_k = c_0 + c_1b_k + c_2b_{k-2} + \cdots + c_kb_0 (?)$$

Note c_0 is the only term above that is not divisible by p^2. Thus, a_k is *not* divisible by p, a contradiction. (??) ■

Source: Primary Source Material

ok joe. idgi but whatever man.

Lec 32 - Jan 31 (Week 16)

Suppose $f(x) \in \mathbb{Z}[x]$, where $f(x) = a_nx^n + \cdots + a_1x + a_0$, and suppose that $\frac{r}{s}$ is a root of f, with $r, s \in \mathbb{Z}, \gcd(r, s) = 1$:

$$a_n\frac{r^n}{s^n} + a_{n-1}\frac{r^{n-1}}{s^{n-1}} + \cdots + a_1\frac{r}{s} + a_0 = 0$$

Then:

$$a_nr^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n = 0$$

In particular, $s \mid a_nr^n \implies s \mid a_n$, and $r \mid a_0s^n \implies r \mid a_0$.

Theorem 11.5: Rational Root Test

If $\frac{r}{s} \in \mathbb{Q}$ as above is a root of $f(x) = a_nx^n + \cdots + a_1x + a_0$, then $r \mid a_0$ and $s \mid a_n$.

Note that this does not give all the roots; a polynomial may not have any rational roots, such as in the case of $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Furthermore, a polynomial may split without having any rational roots, such as with $x^4 - 4 = (x^2 - 2)(x^2 + 2)$. If $f(x) = x^{2n} + 3x^4 + 2x + 4$ is monic, then any rational root must be in $\mathbb{Z}$, as the denominator must divide 1. (2n?)

Recall the Eisenstein Criterion: if $f(x)$ is monic such that $p \mid a_i, p^2 \nmid a_0$, then $f(x)$ is irreducible.

Proof.

Suppose $f(x) = g(x)h(x)$. WLOG, assume g, h are both monic. We write:

$$g(x) = x^k b_{k-1}x^{k-1} + \cdots + b_0$$
$$h(x) = x^\ell + c_{\ell-1}x^{\ell-1} + \cdots + c_0$$

Book says reduce the polynomials mod p; i.e. look at them in $\mathbb{Z}/p\mathbb{Z}[x]$. Then:

$$f(x) = x^n \qquad g(x) = x^k + \dots \qquad h(x) = x^\ell + \dots$$

Since p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, and so the constant terms of both g and h must be 0... but this is not necessarily true? Only one of them needs to be zero...

this turns out to be true as if either of the constant terms are nonzero, then in the polynomial gh you will have terms with nonzero coefficient; however, $f = x^n$. ■

Source: Primary Source Material

Note that (as in the book), Eisenstein's Criterion works over any integral domain.

Another trick: if $f(x) \in \mathbb{Z}[x]$, if there exists p such that $f(x)$ is irreducible mod p, then f has to be irreducible. Proof: if not, i.e. $f = gh$, then $\overline{f} = \overline{g}\overline{h}$ mod p.

Lec 33 - Feb 5 (Week 17)

Let $\mathbb{F}$ be a field. Recall that $\mathbb{F}[x]$ is a PID, and so all prime ideals are maximal. Also, $p(x)$ is prime iff it is irreducible. Thus, if $p(x)$ is irreducible, then $(p(x))$ is maximal, so $\mathbb{F}[x]/(p(x))$ is a field.

If $f(x) \in \mathbb{F}[x]$ and $f(a) = 0$, then the factor theorem says that:

$$f(x) = (x - a)g(x)$$

for some $g(x) \in \mathbb{F}[x]$.

If $a_1, \dots, a_n$ are not necessarily distinct roots, then $f(x)$ is divisible by:

$$(x - a_1) \cdots (x - a_n)$$

Note that if some a_i's are repeated, then it means that they are "multiple" roots. Thus, $n \leq \deg f(x)$. That is, the number of roots is at most the degree of $f(x)$.

Definition 11.2

An integral domain R is **Noetherian** if every ideal I is finitely generated:

$$I = (a_1, \dots, a_k) \qquad a_i \in R$$

for all ideals I.

Note that every PID is Notherian.

Lemma: Hilbert's Lemma

If R is Noetherian, then $R[x]$ is Noetherian.

Proof.

Suppose R is Noetherian, I an ideal in $R[x]$. Define the ideal J as:

$$J = \{a_m : \exists\, a_m x^m + \cdots + a_0 \in I\}$$

In other words, this is the set of leading coefficients of elements in I.

We first show that J is indeed an ideal. Indeed, if $a \in J, r \in R$, then $ra \in I$ since I is an ideal. Now, suppose $a, b \in J$. Set:

$$f(x) = ax^r + \cdots \in I \qquad g(x) = bx^s + \cdots \in I$$

If $r = s$, then $f + g = (a+b)x^r + \ldots$ and we're done. Otherwise, sps WLOG $r < s$. Then:

$$x^{s-r} f(x) + g(x) = (a+b)x^s + \ldots$$

Thus, $J \subseteq R$ is an ideal, and is finitely generated.

Write $J = (a_1, \ldots, a_n)$. Choose $f_i \in I$ of lowest degree such that the leading coefficient is a_i. Set $d_i = \deg(f_i)$, and let $N = \max(d_i)$.

Given $f(x) \in I$, sps the leading coefficient is a. Then:

$$a \in J \implies a = c_1 a_1 + c_2 a_2 + \cdots + c_n a_n \quad c_i \in R$$

If $\deg(f) \geq N$, then let $D = \deg(f)$. Consider:

$$c_1 x^{D-d_1} f_1(x) + \cdots + c_n x^{D-d_n} f_n(x) \;=\; c_1 a_1 x^D + \cdots + c_n a_n x^D \;=\; a x^D$$

Notice that this has the same leading term as f.

By repeating, we can replace f by a polynomial of lower degree, still in I. Thus, we only need to worry about polynomials of degree $< N$.

We use an analogous strategy for these polynomials, finding a finite set of polynomials of degree less than N in terms of which we can write these polynomials in I of degree $< N$. See book for details. (it's a mess though, should try it on your own first -joe) ■

Source: Primary Source Material

If R is Noetherian, then $R[x]$ is Noetherian. Thus, $R[x][y]$ is Noetherian, and thus by induction, $R[x_1, \ldots, x_n]$ is Noetherian.

Suppose $\mathbb{F}$ is a finite field. Then $\mathbb{F}^\times$ form a multiplicative abelian group.

Theorem 11.6

In the above, $\mathbb{F}^\times$ is cyclic.

Example

Consider $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then:

$$\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\} \qquad \left|\mathbb{F}_p^\times\right| = p - 1$$

As a more precise example, consider $\mathbb{F}_7$. Then:

$$\mathbb{F}_7^\times = \{1, 2, 3, 4, 5, 6\}$$

- 1 is clearly not a generator.
- 2 generates $2 \mapsto 4 \mapsto 8 = 1$, so not a generator.
- 3 generates $3 \mapsto 9 = 2 \mapsto 6 \mapsto 18 = 4 \mapsto 12 = 5 \mapsto 15 = 1$, so 3 is a generator.

Source: Primary Source Material

The proof relies on the classification of finite abelian groups, which tells us that:

$$\mathbb{F}^\times = C_{n_1} \times \cdots \times C_{n_k} \qquad n_k \mid n_{k-1} \mid \cdots \mid n_1$$

Digress?: in a cyclic group of order m, there are some elements of order m. The order of any element must divide m. If $d \mid m$, how many elements... i wasnt looking. In a cyclic group of order m, the elements whose order divides d number exactly d. To see this, raise a generator to all powers that are multiples of $\frac{m}{d}$, of which there are exactly d.

In $\mathbb{F}^\times = C_{n_1} \times \cdots \times C_{n_k}$, looking at C_{n_k}, we thus find n_k elements whose order divides n_k. So, there are n_k roots of $x^{n_k} - 1$ in C_{n_k}.

Similarly, since $n_k \mid n_{k-1}$, there are n_k roots of $x^{n_k} - 1$ in $C_{n_{k-1}}$. Thus, there are n_k roots of $x^{n_k} - 1$ in C_{n_i} for all i. Note that $\deg(x^{n_k} - 1) = n_k$, so it can have at most n_k roots. In particular, it can't have more than one factor. (huh. what. thats confusing)

The book defines something called Gröbner Bases. Consider polynomials over fields; these form a vector space over the field, and as such has a basis of monomials. Unfortunately, there is no canonical ordering of the basis, but Gr obner Bases are an option which are effective for computational applications (computing ideals, etc.).

III Modules

12 Basics

Suppose R is a ring. We want to generalize the idea of a vector space over a field, replacing the field with our ring R.

Definition 12.1

A **left R-module** is an abelian group M with operation $+$, together with a left action of R on M satisfying:

- $r(m+m') = rm + rm'$ for all $r \in R, m, m' \in M$
- $(r+s)m = rm + sm$ for all $r, s \in R, m \in M$
- $(rsm) = r(sm)$ for all $r, s \in R, m \in M$

Usually R has a unit, and if so, we also require that $1m = m$ for all m.

Corollary

If R is a field, then this is a vector space. :)

Example

Any ring R is a left R-module:

$$r \cdot r' = rr'$$

Similarly, R^n is a left R-module with componentwise operations.

Source: Primary Source Material

If M is any abelian group and $r \in \mathbb{Z}$, we write:

$$r \cdot m \;=\; \underbrace{m + m + \cdots + m}_{r \text{ times}} \qquad (-r)m = r(-m)$$

Thus, any abelian group is a $\mathbb{Z}$-module. In fact, $\mathbb{Z}$-modules are the same things as abelian groups.

Lec 35 - Feb 14 (Week 18)

How are modules different from vector spaces? A main difference is that we can't always find a basis.

If R is a ring and $M_1, \ldots, M_k$ are (left) R-modules, then we have already discussed the direct product:

$$M_1 \times \cdots \times M_k = \{(m_1, \ldots, m_k) : m_i \in M_i\}$$

with component-wise operation. Note this definition also works with infiniteley many factors $M_i, i \in I$.

For R-modules A, B, we also defined $A + B$ as:

$$A + B = \{a + b : a \in A, b \in B\}$$

This is also an R-submodule of M. We can similarly extend the definition to finitely many summands.

Given R-submodules $A_1, \dots, A_k \subseteq M$, we can define a map:

$$A_1 \times \cdots \times A_k \to A_1 + \cdots + A_k$$
$$(a_1, \dots, a_k) \to a_1 + \cdots + a_k$$

Theorem 12.1

The following are equivalent:

- $A_i \cap (A_1 + \cdots + \hat{A}_i + \cdots + A_k) = \{0\}$ for all i. (The hat means exclude that summand.)
- For any $a \in A_1 + \cdots + A_k$, there exists a unique $a_i \in A_i$ such that $a = a_1 + \cdots + a_k$.

Proof.

easy to prove ■

In the above situation, we'll say $A_1 + \cdots + A_k$ is a **direct sum**, notated by $A_1 \oplus \cdots \oplus A_k$. It follows that $A_1 \oplus \cdots \oplus A_k \simeq A_1 \times \cdots \times A_k$.

Note that if there are infinitely many A_i's, the above will still work, but the direct sum are *not* isomorphic to the direct product.

If $G \subseteq M$ is a subset of an R-module M, we write:

$$RG = \left\{ \sum_{i=1}^{k} r_i g_i : k \in \mathbb{N}, r_i \in R, g_i \in G \right\}$$

We say that RG is the R-submodule generated by G, and G is a set of generators for RG. Note that there may be many different sets of generators. If $G = \{g\}$, then we write Rg for RG, and Rg is called a **cyclic module**.

Example

Let $R = 2\mathbb{Z}$. Clearly this is a nonunital ring.

Notice that $M = \mathbb{Z}$ is an R-module, and:

$$R1 = \{2m \cdot 1 : m \in \mathbb{Z}\} = 2\mathbb{Z}$$

So $R1$ is a submodule of M, which does not contain 1, its generator. This happened because R has no unit, so *usually* we will work with unital rings.

Source: Primary Source Material

Suppose an R-module M satisfies:

$$M = R_{m_1} + \cdots + R_{m_k}$$

Need some notion of independence of the m_i's to get an analogue of a basis in a vector space. How about:

$$M = R_{m_1} \oplus \cdots \oplus R_{m_k}$$

This comes closer, but is still not good enough.

Example

Consider $R = \mathbb{Z}, M = \mathbb{Z}/3\mathbb{Z}$.

Clearly, M is a cyclic module, and so it is just one summand. But $3 \cdot \overline{1} = 0$. Furthermore:

$$2 \cdot \overline{1} \;=\; 5 \cdot \overline{1} \;=\; 8 \cdot \overline{1} \;=\; \ldots$$

So we see two different reasons why the above will not work.

Source: Primary Source Material

As a group, we can think of the above being represented with a relation $x^3 = 1$, or in additive notation, $3x = 0$. Thus, we want to avoid having relations amongst the generators.

Definition 12.2

We say an R-module M is a **free module on a set of generators** A iff every $m \in M$ can be written as:

$$a = r_1 a_1 + \cdots + r_k a_k$$

for finitely many $a_i \in A$, such that the nonzero a_i's and corresponding r_i's are uniquely determined.

The number of generators of a free module M is called the **rank** of M.

Free modules are a lot like vector spaces, but special. In the proof that all vector spaces have bases, we require that we can divide by our field elements; we can't expect to do the same in an arbitrary ring.

Theorem 12.2

Given a set A and a ring R, there is a module $F(A)$ (the free module on A) which has the following defining property:

Suppose M is an R-module, and there is a map $\varphi : A \to M$. Then, A is a subset of $F(A)$ and there exists $\Phi : F(A) \to M$ such that $\varphi = \Phi \circ \iota$. In other words, the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, dashed, "\Phi"] \\
 & M
\end{tikzcd}$$

Proof.

Sketch of proof:

$$F(A) = \{f : A \to R : f(a) \neq 0 \text{ for finitely many } a \in A\}$$

This is an R-module by multiplication by R.

If $f(a_i) = r_i$ for $i = 1, \ldots, k$ and $f(a) = 0$ otherwise, then $\Phi(f) = \sum_{i=1}^{k} r_i \, \varphi(a_i)$. ■

Source: Primary Source Material

13 Tensor Products

Lec 36 - Feb 26 (Week 19)

It's time for tensor products.

Recall that if M, N are R-modules, then:

$$M \oplus N \simeq M \times N = \{(m,n) : m \in M, n \in N\}$$

If $\varphi : M \times N \to K$ is a homomorphism, that is, an R-linear map, then:

$$\varphi((a,b)+(c,d)) = \varphi(a,b) + \varphi(c,d)$$
$$\varphi((ra,rb)) = \varphi(r(a,b)) = r\,\varphi(a,b)$$

We're going to discuss a *different* kind of map.

Definition 13.1

An R**-bilinear map** is a map φ which is linear on each component, separately:

$$\varphi((ra,b)) = \varphi(r(a,b)) = \varphi((a,rb)) = r\,\varphi(a,b)$$
$$\varphi((a+b),c) = \varphi(a,c) + \varphi(b,c)$$
$$\varphi(a,(b+c)) = \varphi(a,b) + \varphi(a,c)$$

Notice that in this case, we have that:

$$\varphi((ra,rb)) = r\,\varphi((a,rb)) = r^2\,\varphi(a,b)$$

A *tensor product* is a convenient way of keeping track of bilinear maps.

Let R be a commutative unital ring. Suppose $\varphi : M \times N \to K$ is an R-bilinear map. Thus:

$$\varphi((ra,b)) = r\,\varphi(a,b)$$

We can't just take any map, we need to define things carefully.

Start with $M \times N$ as an R-module. Take all the elements that correspond to the above relations:

$$(ra,b) - r(a,b)$$
$$(a,rb) - r(a,b)$$
$$(a+b,c) - (a,c) - (b,c)$$
$$(a,b+c) - (a,b) - (a,c)$$

Clearly, these are all taken to 0 by φ. Take the submodule generated by these relations; call it L. We consider $(M \times N)/L$, an R-module, denoted $M \otimes_R N$; this is the tensor product.

Note that φ gives a well-defined map on $M \otimes_R N$ since it kills everything in L; for this map, we'll use the following function:

$$\Phi : M \otimes_R N \to K$$

We now get the following diagram:

[diagram]

This is kind of like FIT; we quotient out by a certian thing and get a map from the quotient space to K. Notice that the same quotient $M \otimes_R N$ will work for *any* bilinear map φ; they must "factor through" $M \otimes_R N$.

Digression: D&F *doesn't* assume that R is commutative. So instead, they have to assume that M is a *right* R-module, and that N is a *left* R-module. A bilinear map φ now satisfies:

$$\varphi((mr, n)) = \varphi((m, rn))$$

as well. Then, everything else is defined similarly, though very complicated.

Theorem 13.1

The construction above defines an R-module $M \otimes_R N$.

Given any R-bilinear map $\varphi : M \times N \to K$, there is a unique R-module map, given by:

$$\Phi : M \otimes_R N \to K$$

such that the below diagram commutes:
[diagram]
Furthermore, if T is another R-module with the same property, then:
[diagram]
In this case, $T \simeq M \otimes_R N$, and Φ' corresponds to Φ.

Note that this tells us that tensor products count bilinear maps.

In linear algebra, let $\mathbb{F}$ be a field and U, V, W vector spaces. Then, we can think about $U \otimes_{\mathbb{F}} V$.

As it turns out, a basis for $U \otimes_{\mathbb{F}} V$ is given by:

$$\{e_i \otimes f_j\}$$

where $e_i \otimes f_j$ is the image of (e_i, f_j) in $U \otimes_{\mathbb{F}} V$, with $\{e_i\}, \{f_j\}$ as bases for U and V respectively. Thus, we see that:

$$\dim(U \otimes_{\mathbb{F}} V) = \dim(U) \cdot \dim(V)$$

This is similar to how $\dim(U \times V) = \dim(U) + \dim(V)$. A typical element of $U \otimes_{\mathbb{F}} V$ is given by:

$$\sum c_{ij} e_i \otimes f_j$$

and an element of the form $a \otimes b$ is known as a **simple tensor**. NOTE: Not all tensors are simple!

Example

Consider bilinear maps of the form $\varphi : \mathbb{F}^m \times \mathbb{F}^n \to \mathbb{F}$. What are the linear maps?

Recall that $\mathbb{F}^m \times \mathbb{F}^n \simeq \mathbb{F}^{m+n}$. Then, an element $\mathbb{F}^{m+n} \to \mathbb{F}$ is an element of the dual space:

$$\widehat{\mathbb{F}^{m+n}} \simeq \mathbb{F}^{m+n}$$

A good way of visualizing bilinear maps is as such:

$$\varphi(u, v) \quad = \quad \begin{pmatrix} \quad \mathbf{u} \quad \end{pmatrix} \left[\begin{array}{c} \text{something determined} \\ \text{by } \varphi \end{array} \right] \begin{pmatrix} \mathbf{v} \end{pmatrix}$$

So in this case, $\mathbb{F}^m \otimes_{\mathbb{F}} \mathbb{F}^n \simeq M_{m \times n}(\mathbb{F})$, and so it has dimension mn. Here the basis element $e_i \otimes f_j$ corresponds to the matrix $E_{ij} \in M_{m \times n}(\mathbb{F})$.

Source: Primary Source Material

Example

Consider $R = \mathbb{Z}$. Let $M = \mathbb{Z}/3\mathbb{Z}, N = \mathbb{Z}/5\mathbb{Z}$. What is $M \otimes_R N = \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/5\mathbb{Z}$?

Consider $\overline{(1,0)} \in M \otimes_R N$. Then, we have:

$$\overline{(1,0)} = \overline{(1, 3\cdot 0)} = \overline{(3\cdot 1, 0)} = \overline{(0,0)}$$

Similarly, $\overline{(0,1)} = 0$. So, we see that $\mathbb{Z}/3\mathbb{Z} \otimes_R \mathbb{Z}/5\mathbb{Z} = 0$, and thus there are no maps. Indeed:

$$\begin{aligned}\overline{(a,b)} = \overline{(10a,b)} &= \overline{(5\cdot 2a, b)}\\ &= \overline{(2a, 5b)}\\ &= \overline{(2a, 0)}\\ &= \overline{(2a, 3\cdot 0)}\\ &= \overline{(6a, 0)}\\ &= \overline{(0,0)}\end{aligned}$$

Thus, there are no bilinear maps $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to M$ for any $\mathbb{Z}$-module M.

Source: Primary Source Material

Lec 37 - Feb 28 (Week 19)

Given an $n \times n$ matrix over $\mathbb{C}$ (although any field works):

$$\begin{pmatrix} \\ \mathbf{v_1} & \mathbf{v_2} & \cdots & \mathbf{v_{n-1}} & \mathbf{v_n} \\ \\ \end{pmatrix} \in \underbrace{\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n}_{n \text{ times}}$$

where each $\mathbb{C}^n$ represents the columns. S_n *acts* on this tensor product by permuting the "columns". Let's look for a subspace on which the action of S_n is *odd* (switching two columns will result in a $-$ sign). Surprisingly, it turns out that only *one* subspace that satisfies this; it has dimension 1. Up to scalars, it is in fact given by the **determinant**.

Bilinear maps helped define the tensor product. We can extend this to *multi-linear maps*, which gives us:

$$M_1 \otimes \cdots \otimes M_n$$

14 Modules over PIDs

Definition 14.1

If R is a unital ring and M is an R-module, we say M is a **Noetherian module** if it satisfies the "ascending chain condition" (ACC):

Given any chain of submodules such that:

$$M_1 \subseteq M_2 \subseteq \cdots M_n \subseteq \cdots M$$

then there exists n such that $M_n = M_{n+1} = \cdots = M + k$ for all $k \geq 0$.

In other words, the chain stabilizes; there are *no* strictly infinite chains.

We say that R is **Noetherian** if it is a Noetherian module over itself.

Example

The integers $\mathbb{Z}$ are Noetherian.

Source: Primary Source Material

Theorem 14.1

Let M be an R-module. Then, the following are equivalent:

1. Any collection $\mathcal{A}$ of submodules has a maximal element.
2. M is Noetherian (satisfies ACC).
3. Any submodule of M is finitely generated.

Item 3 provides an explanation for why $\mathbb{Z}$ is Noetherian.

Proof.

($1 \implies 2$) Any infinite chain of submodules has a maximal element M_N by 1.

($2 \implies 3$) Suppose $N \subseteq M$ is a submodule. Define the following chain:

$$\begin{aligned} n_1 &\in N & N_1 &= \langle n_1 \rangle \\ n_2 &\neq n_1 & N_2 &= \langle n_1, n_2 \rangle \\ &\vdots & &\vdots \end{aligned}$$

This collection must have a maximal element, so the chain stops at some $N_M = N$. Therefore, we have that:

$$N = \langle n_1, n_2, \ldots, n_M \rangle$$

as needed.

($3 \implies 1$) Suppose $\mathcal{A}$ has no maximal ideal. Then, there is a chain of infinitely many strictly increasing submodules:

$$M_1 \subsetneq M_2 \subsetneq \cdots$$

Let $M = \bigcup_{i=1}^{\infty} M_i$. This module is finitely generated:

$$M = \langle m_1, m_2, \ldots, m_k \rangle$$

This set of generators lies in some set in the chain, say M_r. But then $M_r = M$, and is therefore a maximal element, a contradiction. ■

Source: Primary Source Material

Definition 14.2

If M is an R-module, we call $m \in M$ a **torsion element** if $rm = 0$ for some non-zero $r \in R$. We say that $r \in R$ **annihilates** $m \in M$ if $rm = 0$.

We denote by $\operatorname{Tor}(M)$ the set of torsion elements of M, and we define:

$$\operatorname{Ann}(M) = \{r \in R : rm = 0 \; \forall \, m \in M\}$$

Example

In $R = \mathbb{Z}/m\mathbb{Z}$, everything is a torsion element since $mn = 0$ for all n.

$$\operatorname{Tor}(M) = \mathbb{Z}/m\mathbb{Z}$$

Furthermore, we also have that:

$$\operatorname{Ann}(M) = m\mathbb{Z}$$

Source: Primary Source Material

Lec 38 - Mar 05 (Week 20)

If M, N are R-modules, we write $\operatorname{Hom}_R(M, N)$ for the set of all R-module homomorphisms $\varphi : M \to N$.

Theorem 14.2

Suppose R is a PID and M a free R-module of finite rank.

If $N \subseteq M$ is an R-submodule, then:

1. N is a free R-module.
2. It is possible to find a basis $y_1, \ldots, y_n$ of M and elements $a_1, \ldots, a_n \in R$ such that:

$$a_1 \mid a_2 \mid \cdots \mid a_n$$

and $a_1 y_1, \ldots, a_k y_k$ is a basis of N, and $a_{k+1}, \ldots, a_n = 0$.

Consider $\operatorname{Hom}_R(M, R)$. Note that this is analogous to the dual of a vector space. Define the set:

$$I = \{\varphi(n) : \varphi \in \operatorname{Hom}_R(M, R), n \in N\}$$

This is an ideal in R, and since R is a PID, I is thus principal, and we write $I = (a_1)$ for some $a_1 \in R$. Of course, if $N = \{0\}$, then $I = (0), a_1 = 0$, which is “just silly”. So we’ll assume $N \neq \{0\}$.

$$M = R \oplus \cdots \oplus R$$

Let π_i be the projection of the ith component:

$$\pi_i(m_1, \ldots, m_n) = m_i \qquad \pi_i \in \operatorname{Hom}_R(M, R)$$

If $N \neq \{0\}$, there will be a nonzero $n \in N$, and therefore an i such that $\pi_i(n) \neq 0$. So $I \neq \{0\}$, and $a_1 \neq 0$. Since $a_1 \in I$, there exists $\nu \in \operatorname{Hom}_R(M, R)$ and $y \in N$ such that $a_1 = \nu(y)$.

Lemma

For any $\varphi \in \operatorname{Hom}(M, R)$, we have that $a_1 \mid \varphi(y)$. That is, $(\varphi(y)) \subseteq (a_1)$.

Proof.

Let $J = \{a_1, \varphi(y)\} = (d)$ for some $d \in R$. Then $d = r_1 a_1 + r_2\, \varphi(y)$ for some $r_1, r_2 \in R$.

Let $\psi = r_1 \nu + r_2\, \varphi \in \mathrm{Hom}_R(M, R)$. It follows that $\psi(y) = r_1 \nu(y) + r_2\, \varphi(y)$. So $(d) \subseteq (a_1)$, in particular $a_1 \mid d$.

We want $a_1 \mid \varphi(y)$ (this is obvious because $(a_1) = d$ and $\varphi(y) \in (d)$ or sth. joe what) ■

Source: Primary Source Material

We apply this with $\varphi = \pi_i$. Then, $a_1 \mid \pi_i(y)$. Write $\pi_i(y) = a_1 \cdot b_i$ for all i. Take the basis $x_1, \dots, x_n$ for M, and let $y_1 = \sum_i b_i x_i$. Then:

$$a_1 y_1 = \sum_i a_1 b_i x_i = y$$

To make this work, we need (1) that $M = R_{y_1} \oplus \ker(\nu)$. Given $m \in M, m = \nu(m) y_1 + (m - \nu(m) y_1)$:

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

The above is equal to 0, provided we can show that $\nu(y_1) = 1$. We see that:

$$a_1 = \nu(y) = \nu(a_1 y_1) = a_1 \nu(y_1)$$

So $a_1 - a_1 y_1 = 0$. Thus, R being a PID means $\nu(y_1) = 1$.

Next, we also need to show (2) that $N = R a_1 y_1 \oplus (\ker(\nu) \sqcap N)$. Indeed, given $n \in N$:

$$n = \nu(n) y_1 + (n - \nu(n) y_1)$$

Since $\nu(n) \in (a_1)$, then:

$$\begin{aligned} \nu(n) y_1 + (n - \nu(n) y_1) &= c a_1 y_1 + (n - \nu(n) y_1) \\ \nu(n - \nu(n) y_1) &= \nu(n) - \nu(n)\nu(y_1) \\ &= \nu(n) - \nu(n) = 0 \end{aligned}$$

Also, $n - \nu(n) y_1 = n - c a_1 y_1 \in N$.

We then apply induction, working on the module $\ker(\nu)$ and its submodule $\ker(\nu) \cap N$.

The critical step is to observe that when we find a_2:

$$(a_2) = \{\varphi(n) : \varphi \in \mathrm{Hom}_R(\ker(\nu), R), n \in \ker(\nu) \cap N\}$$

We need $a_1 \mid a_2$. But this is easy, because the above ideal is contained in $I = (a_1)$.

Suppose we have a finitely generated abelian group G, with generators $g_1, \dots, g_n$. Define a map:

$$\Phi : \mathbb{Z}^n \to G \qquad \Phi(e_i) = g_i$$

where $\{e_1, \dots, e_n\}$ is the standard basis of $\mathbb{Z}^n$, and extending to all of $\mathbb{Z}^n$:

$$\Phi(a_1, \dots, a_n) = g_1^{a_1} g_2^{a_2} \dots g_n^{a_n}$$

Note that Φ is surjective, and $\ker(\Phi)$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$. By FIT, $G \simeq \mathbb{Z}^n / \ker(\Phi)$, and we can use the previous theorem to find a base $y_1, \dots, y_n$ of $\mathbb{Z}^n$ and $a_1 \mid \cdots \mid a_n$ such that:

$$\ker(\Phi) = \langle\, a_1 y_1 \,\rangle \oplus \cdots \oplus \langle\, a_n y_n \,\rangle$$

So, we have that:

$$G = \mathbb{Z}^n / \ker(\Phi) = \langle\, y_1 \,\rangle \oplus \cdots \oplus \langle\, y_n \,\rangle / \langle\, a_1 y_1 \,\rangle \oplus \cdots \oplus \langle\, a_n y_n \,\rangle \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}$$

If $a_i = 0$, then $\mathbb{Z}/a_i\mathbb{Z}$ is $\mathbb{Z}$. Thus, we get that:

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_k\mathbb{Z} \oplus \mathbb{Z}^{n-k} \qquad a_1 \mid \cdots \mid a_k$$

The number $n-k$ is called the **rank of** G, also called the **Betti number**. The numbers $a_1, \ldots, a_k$, usually all +ve, are the **invariant factors** of G. These determine G up to isomorphism.

If $G = \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_k\mathbb{Z}$, then $\text{Ann}(G) = a_k\mathbb{Z}$.

Example

Consider $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$. This is isomorphic to:

$$(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$$

$$(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z}$$

Our original decomposition is the invariant factor decomposition, and the third decomposition is the primary decomposition.

Source: Primary Source Material

15 Back to Linear Algebra

Recalling some linear algebra:

Given a transformation $T : V \to W$ over a field $\mathbb{F}$, We can associate with T a matrix that depends on the choice of basis for V, W. In the special case that $V = W$ with the same basis, we get a square matrix.

im not writing all this. we know what eigenvalues are lol

jcf mention?!?!?!?!

next time: rational canonical form

Lec 39 - Mar 12 (Week 21)

(last friday was cancelled since joe got sick)

Consider $R = \mathbb{F}[x]$ for some field $\mathbb{F}$; R is a PID. If A is an $n \times n$ matrix, then there is a natural action of R on $\mathbb{F}^n$ by letting x act as multiplication by A.

If $\mathfrak{a}$ is an ideal in R, then there exist ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ such that the action of R on $\mathbb{F}^n$ is isomorphic to:

$$\mathbb{F}[x]/\mathfrak{a}_1 \oplus \cdots \oplus \mathbb{F}[x]/\mathfrak{a}_k \oplus R^r$$

and $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_k$. The $\mathfrak{a}_i$'s are the **invariant factors**.

Definition 15.1

Suppose B is a square matrix with characteristic polynomial given by:

$$c_B(x) = \det(xI - B) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

Then the **companion matrix** to this polynomial is given by:

$$C_{c_B} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & 0 & \dots & 0 & -b_2 \\ 0 & 0 & 1 & \dots & 0 & -b_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -b_{m-1} \end{pmatrix}$$

Note that this has the same characteristic polynomial as B, but in general may not be similar to B:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

The rational canonical form (RCF) will be a sum of blocks, each of which is a companion matrix with characteristic equal to a generator of one of the invariant factors. To make it unique, we assume these generators are monic polynomials. But, this will only work if we can find the invariant factors.

There is a procedure for finding (monic) generators for the invariant factors: given a matrix A, write out $xI - A$:

$$xI - A = \begin{pmatrix} x - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & x - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & x - a_{nn} \end{pmatrix}$$

We will apply a kind of row and column reduction, with the goal of changing $xI - A$ to something that looks like:

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1(x) & & \\ & & & & \ddots & \\ & & & & & f_k(x) \end{pmatrix}$$

where $f_1, \dots, f_k$ are monic generators of $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ respectively. Allowed operations are:

- Multiplying a row or column by a unit c, i.e. a nonzero scalar.
- Switch two rows or columns.
- If $g(x) \in \mathbb{F}[x]$, add $g(x) \cdot R_i$ to R_j.

where R_i, R_j are any two rows (this holds analogously for columns).

Example

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Then:

$$\begin{pmatrix} x-1 & 0 \\ 0 & x-2 \end{pmatrix} \xrightarrow{R_1+R_2} \begin{pmatrix} x-1 & x-2 \\ 0 & x-2 \end{pmatrix}$$

$$\xrightarrow{C_2-C_1} \begin{pmatrix} x-1 & -1 \\ 0 & x-2 \end{pmatrix} \xrightarrow{C_1\leftrightarrow C_2} \begin{pmatrix} -1 & x-1 \\ x-2 & 0 \end{pmatrix}$$

$$\xrightarrow{-1\cdot R_1} \begin{pmatrix} 1 & 1-x \\ x-2 & 0 \end{pmatrix} \xrightarrow{R_2-(x-2)R_1} \begin{pmatrix} 1 & 1-x \\ 0 & (x-1)(x-2) \end{pmatrix}$$

$$\xrightarrow{C_2-(1-x)C_1} \begin{pmatrix} 1 & 0 \\ 0 & (x-1)(x-2) \end{pmatrix}$$

So for $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, there is only one invariant factor, and it is $(x-1)(x-2) = x^2 - 3x + 2$. So:

$$\text{RCF}(A) \;=\; \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$$

Source: Primary Source Material

Example

time to put my latex skills to the test.

Suppose $A = \begin{pmatrix} -4 & 2 & 1 \\ -7 & 5 & 1 \\ -11 & 2 & 4 \end{pmatrix}$. Then, $xI - A = \begin{pmatrix} x+4 & -2 & -1 \\ 7 & x-5 & -1 \\ 11 & -2 & x-4 \end{pmatrix}$, and:

$$\xrightarrow{-1\cdot C_3} \begin{pmatrix} x+4 & -2 & 1 \\ 7 & x-5 & 1 \\ 11 & -2 & 4-x \end{pmatrix} \xrightarrow{C_1\leftrightarrow C_3} \begin{pmatrix} 1 & -2 & x+4 \\ 1 & x-5 & 7 \\ 4-x & -2 & 11 \end{pmatrix}$$

$$\xrightarrow{R_2-R_1} \begin{pmatrix} 1 & -2 & x+4 \\ 0 & x-3 & 3-x \\ 4-x & -2 & 11 \end{pmatrix} \xrightarrow{C_2+2C_1} \begin{pmatrix} 1 & 0 & x+4 \\ 0 & x-3 & 3-x \\ 4-x & 6-2x & 11 \end{pmatrix}$$

$$\xrightarrow{C_3-(x+4)C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 3-x \\ 4-x & 6-2x & x^2-5 \end{pmatrix} \xrightarrow{R_3-(4-x)R_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 3-x \\ 0 & 6-2x & x^2-5 \end{pmatrix}$$

$$\xrightarrow{C_3+C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 0 \\ 0 & 6-2x & x^2-2x+1 \end{pmatrix} \xrightarrow{R_3+2R_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x-3 & 0 \\ 0 & 0 & x^2-2x+1 \end{pmatrix}$$

This looks like the answer, however $x-3$ does not divide x^2-2x+1, so we're not done. How can we get a 1 into the centre position?

We *could* do it - it's not impossible. But, observing that the final result has to be of the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c_A \end{pmatrix}$ and $c_A = (x-3)(x-1)^2$, we can just write down the final result:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x-3)(x-1)^2 \end{pmatrix} \qquad (x-3)(x-1)^2 = x^3 - 5x^2 + 7x - 3$$

So the RCF is given by:

$$\text{RCF}_A = \begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & -7 \\ 0 & 1 & 3 \end{pmatrix}$$

Source: Primary Source Material

In the above example, suppose we got: $\begin{pmatrix} 1 & & \\ & x-1 & \\ & & (x-1)(x-3) \end{pmatrix}$ where $(x-1)(x-3) = x^2 - 4x + 4$.

Then:

$$\text{RCF}_A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -3 \\ 0 & 1 & 4 \end{bmatrix}$$

Clearly, these are not conjugate. What are the JCFs corresponding to each?

In the second case, the corresponding JCF is in fact diagonal, and is given by $\begin{pmatrix} 1 & & \\ & 1 & \\ & & 3 \end{pmatrix}$. For the original one, however, we have a cubic, and so the JCF is given by: $\begin{pmatrix} 3 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}$. This has two blocks in JCF, and one block in RCF.

We can ask ourselves about the annihilators. Notice that:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$$

So $x-1$ doesn't kill it, but $(x-1)^2$ does. If you have a Jordan block of size $k \times k$, it needs $(x-\lambda)^k$ in the annihilator.

Theorem 15.1

Two matrices A and B are similar if and only if they have the same RCF.

Proof.

essentially follows from uniqueness of invariant factors ..... ■

Source: Primary Source Material

Exercise 15.1

Find a quiet place and convince yourself that the procedure works.

Source: Primary Source Material

Example

Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Note $c_A(x) = x^2 + 1$, so A has eigenvalues $\pm i$.

Over $\mathbb{R}$, we see that A does not have a JCF. However, over $\mathbb{C}$, it is indeed diagonalizable:

$$\text{JCF}_{\mathbb{C}} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

But notice that:

$$\text{RCF} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Interestingly, this is the RCF over $\mathbb{R}$ *or* $\mathbb{C}$ - or any field of characteristic 0, for that matter.

Source: Primary Source Material

fun fact: if you go through the entire process we just did, but isolate only the column operations (ignoring the row ops), write them as elementary matrices, and multiply them together, then multiply the resulting matrix by the original, you get the RCF. however, this is "much worse", which is why joe didn't mention it beforehand. oh okay its Storytime With Joe™ now

IV Fields and Galois Theory

16 Preliminaries

Lec 40 - Mar 14 (Week 21)

Fields and Galois theory ultimately boil down to solving polynomials. Recall that $f(x) = x^2 + 2 \in \mathbb{Q}[x]$ has no rational roots. However, it *does* have roots, $\pm\sqrt{2} \in \mathbb{R}$. More precisely, these roots actually live in:

$$\mathbb{Q}[\sqrt{2}] \;=\; \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$$

which is a field containing $\mathbb{Q}$.

Definition 16.1

If R is an integral domain (often a field), the **characteristic** of R is the smallest positive integer c such that $c \cdot r = 0$ for some $0 \neq r \in R$.

If no such c exists, we say that $\operatorname{char}(R) = 0$.

One can easily show that if $\operatorname{char}(R) = 0$, then c is prime. Note this is not necessarily true if R is *not* an integral domain. Furthermore, if $p = \operatorname{char}(R) \neq 0$, then $pr = 0$ for all $r \in R$.

Example

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p. So does $\mathbb{F}_p[x]$ and its quotient field $\mathbb{F}_p(x)$, the field of rational functions.

Source: Primary Source Material

If $\mathbb{E}, \mathbb{F}$ are fields such that $\mathbb{F} \subseteq \mathbb{E}$, we say that $\mathbb{F}$ is a **subfield** of $\mathbb{E}$, and that $\mathbb{E}$ is an **extension field** of $\mathbb{F}$. Diagrammatically:

$$\begin{tikzcd}
\mathbb{E} \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

In $\mathbb{E}$, we can multiply by elements in $\mathbb{F}$, so $\mathbb{E}$ is in fact a *vector space* over $\mathbb{F}$. If $\dim_{\mathbb{F}}(\mathbb{E}) < \infty$, then we say $\mathbb{E}/\mathbb{F}$ is a **finite extension**. We also say that $\mathbb{E}/\mathbb{F}$ is **finite**, but note that this is *not* a quotient. We write:

$$[\mathbb{E} : \mathbb{F}] = \dim_{\mathbb{F}}(\mathbb{E})$$

This is also known as the **degree of** $\mathbb{E}/\mathbb{F}$.

Example

Consider $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$. Note that 1 and $\sqrt{2}$ form a basis for $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. Thus, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, and we write:

$$\begin{tikzcd}\mathbb{Q}[\sqrt{2}] \arrow[d, dash, "2"] \\ \mathbb{Q}\end{tikzcd}$$

We can also think of $\mathbb{C}$ as a vector space over $\mathbb{R}$ with basis given by $\{1, i\}$. Thus, $[\mathbb{C} : \mathbb{R}] = 2$. In other words, we can think of $\mathbb{C}$ as $\mathbb{R}[\sqrt{-1}]$.

A third example; we can think of $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Since $\mathbb{Q}$ is countable, any vector space over $\mathbb{Q}$ must also be countable, and so we necessarily have that $[\mathbb{R} : \mathbb{Q}] = \infty$.

Source: Primary Source Material

Given a polynomial $f \in \mathbb{F}[x]$, can we find an extension field $\mathbb{E}/\mathbb{F}$ such that f has a root in $\mathbb{E}$? Yes, and it's in fact not that complicated to do so.

Assume WLOG that f is irreducible. Consider $\mathbb{F}[x]/(f(x))$. Since f is irreducible, $(f(x))$ is maximal, so this quotient is a field. Let $\mathbb{E} = \mathbb{F}[x]/(f(x))$. Note that $\mathbb{E}$ contains (an isomorphic copy of) $\mathbb{F}$ in the form of the *constant polynomials*. Thus, we can think of $\mathbb{E}$ as an extension of $\mathbb{F}$:

$$\begin{tikzcd}\mathbb{E} \arrow[d, dash] \\ \mathbb{F}\end{tikzcd}$$

Let $\overline{x} = x + (f(x)) \in \mathbb{F}[x]/(f(x)) = \mathbb{E}$. Consider an arbitrary element of $\mathbb{E}$:

$$(a_n x^n + \cdots + a_1 x + a_0) + (f(x)) \ = \ a_n \overline{x}^n + \cdots + a_1 \overline{x} + a_0$$

We can do better than that. We divide:

$$\frac{a_n x^n + \cdots + a_1 x + a_0}{f(x)} \ = \ q(x) f(x) + r(x)$$

where $\deg(r(x)) < \deg(f(x))$. Thus, modulo $(f(x))$, we have that:

$$a_n \overline{x}^n + \cdots + a_1 \overline{x} + a_0 \ = \ r(x)$$

Thus, in $\mathbb{E} = \mathbb{F}[x]/(f(x))$, arbitrary elements can be written as:

$$c_{k-1} \overline{x}^{k-1} + \cdots + c_1 \overline{x} + c_0 \overline{1}$$

with $k = \deg(f(x)), c_i \in \mathbb{F}$. Thus, $\left\{\overline{1}, \overline{x}, \ldots, \overline{x}^{k-1}\right\}$ span $\mathbb{E}/\mathbb{F}$.

To see that they are linearly independent, suppose otherwise. Then:

$$d(x) = d_0 \overline{1} + d_1 \overline{x} + \cdots + d_{k-1} \overline{x}^{k-1} = \overline{0}$$

So $d(x) \in (f(x))$. Therefore, we write $d(x) = g(x) f(x)$. However, notice that $\deg(d(x)) = k - 1 < \deg(g(x) f(x))$. Thus, we have a basis, and in particular, $[\mathbb{E} : \mathbb{F}] = k = \deg(f(x))$, so $\mathbb{E}/\mathbb{F}$ is finite.

Note that we could assume f is irreducible since $\mathbb{F}[x]$ is a UFD, and a root of f must be a root of one of its irreducible factors.

Going back to the above, consider $f(\overline{x})$, where $f \in \mathbb{F}[x] \subseteq \mathbb{E}[x]$. Evaluating $f \in \mathbb{E}[x]$ at $\overline{x} \in \mathbb{E}$ yields the following:

$$f(\overline{x}) \;=\; f(x) + (f(x)) \;=\; (f(x)) \;=\; \overline{0}$$

Thus, $\overline{x}$ is a root of f in $\mathbb{E}$.

Example

Let $\mathbb{F} = \mathbb{Q}$, and $f(x) = x^2 - 2$. Then, we have:

$$\begin{tikzcd} \mathbb{E} \arrow[d, dash, "2"] \\ \mathbb{F} \end{tikzcd}$$

We know $\overline{x} \in \mathbb{E}$ looks like $x + (f(x))$. Thus:

$$\overline{x}^2 - 2 \;=\; x^2 - 2 + (f(x)) \;=\; (f(x)) \;=\; \overline{0}$$

In addition, $\overline{x}^2 = 2$, so it actually is a square root (and so is $-\overline{x}$).

Source: Primary Source Material

Lec 41 - Mar 19 (Week 22)

Definition 16.2

Suppose $\mathbb{K}$ extends $\mathbb{F}$, and $\alpha \in \mathbb{K}$. Then $\mathbb{F}[\alpha]$ means the smallest field containing $\mathbb{F} + \alpha$.

We say $\mathbb{F}[\alpha]$ is the field generated by $\alpha/\mathbb{F}$.

Example

Let $\mathbb{F} = \mathbb{Q}, K = \mathbb{R}, \alpha = \sqrt{2}$. Then:

$$\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$$

Another familiar example is that of $\mathbb{R}[\sqrt{-1}] = \mathbb{C}$.

Source: Primary Source Material

The above definition holds analogously for $\mathbb{F}[\alpha_1, \ldots, \alpha_n], \alpha_i \in \mathbb{K}$.

Suppose $p(x) \in \mathbb{F}[x]$ is irreducible, and α is a root of p. Then:

$$\mathbb{F}[\alpha] \simeq \mathbb{F}[x]/(p(x))$$

This has a basis given by:

$$\overline{1}, \overline{x}, \ldots, \overline{x}^{m-1} \qquad m = \deg(p)$$

In particular, $[\mathbb{F}[\alpha] : \mathbb{F}] = m$.

Lemma

Suppose $\varphi : \mathbb{F} \to \mathbb{F}'$ is a field homomorphism. Then either $\varphi \equiv 0$ or φ is injective.

Proof.

Note $\ker(\varphi)$ is an ideal of $\mathbb{F}$ as a ring, and the only ideals of a field are 0 and $\mathbb{F}$ itself. ■

Source: Primary Source Material

Theorem 16.1

If $\varphi : \mathbb{F} \to \mathbb{F}'$ is an isomorphism, then it induces an isomorphism:

$$\mathbb{F}[x] \to \mathbb{F}'[x] \qquad p(x) \mapsto p'(x)$$

by acting on the coefficients.

If p is irreducible and $p(\alpha) = 0$, then φ induces a map:

$$\mathbb{F}[\alpha] = \mathbb{F}[x]/(p(x)) \to \mathbb{F}'[x]/(p'(x)) = \mathbb{F}'[\alpha'] \qquad \overline{x} = x + (p(x)) \mapsto x + (p'(x))$$

where α' is the image of α.

More simply, if $\varphi : \mathbb{F} \to \mathbb{F}'$ is an isomorphism and $p(\alpha) = 0$ for some irreducible $p \in \mathbb{F}[x]$, and β is some root of the corresponding $p'(x) \in \mathbb{F}'[x]$. Then:

$$\begin{tikzcd}
\mathbb{F}[\alpha] \arrow[r, phantom, "\simeq"] \arrow[d, dash] & \mathbb{F}'[\beta] \arrow[d, dash] \\
\mathbb{F} \arrow[r, "\varphi"] & \mathbb{F}
\end{tikzcd}$$

In other words, we can extend φ.

Example

Let $\mathbb{F} = \mathbb{R} = \mathbb{F}'$, and $\varphi = \text{id}$ (This is a particularly silly case). Let $p(x) = p'(x) = x^2 + 1$, and $\alpha = i, \beta = -i$. The theorem tells us that there exists an isomorphism such that:

$$\begin{tikzcd}
\mathbb{R}[i] = \mathbb{C} \arrow[r, "i \mapsto -i"'] \arrow[d, dash] & \mathbb{C} = \mathbb{R}[-i] \arrow[d, dash] \\
\mathbb{R} \arrow[r, "\text{id}"] & \mathbb{R}
\end{tikzcd}$$

In other words, it maps $x + iy \mapsto x - iy$. This is the complex conjugation map $z \mapsto \overline{z}$.

Source: Primary Source Material

Another way of interpreting the above example is to say that polynomials over $\mathbb{R}$ cannot distinguish between i and $-i$; anything that i can do, $-i$ can also do. Thus, in general, it may not make sense to talk about polynomials determining its roots; instead, we might have to settle for determining the set of all its roots (? kinda missed this end part).

Definition 16.3

Let $\mathbb{K}$ be some extension of $\mathbb{F}$.

An element $\alpha \in \mathbb{K}$ is called **algebraic over** $\mathbb{F}$ if it is a root of some nonzero polynomial $p(x) \in \mathbb{F}[x]$.

If α is *not* algebraic over $\mathbb{F}$, then it is instead called **transcendental over** $\mathbb{F}$.

The extension $\mathbb{K}/\mathbb{F}$ is an **algebraic extension** if every element $\alpha \in \mathbb{K}$ is algebraic over $\mathbb{F}$.

Suppose $\mathbb{K}$ is an extension of $\mathbb{F}$, and $\alpha \in \mathbb{K}$ is algebraic.

Then $\{f(x) \in \mathbb{F}[x] : f(\alpha) = 0\}$ is an ideal in $\mathbb{F}[x]$, a PID. There is a uniquely determined generator of this ideal that is monic. Moreover, it is irreducible.

Indeed, suppose the monic generator is $m(x) = g(x)h(x)$. Then:

$$0 = m(\alpha) = g(\alpha)h(\alpha)$$

so either $g(\alpha) = 0$ or $h(\alpha) = 0$, which contradicts m being a generator.

Definition 16.4

If $\alpha \in \mathbb{K}$ is algebraic over $\mathbb{F}$, then there exists a unique monic irreducible polynomial $m_{\alpha,\mathbb{F}}(x)$ of which α is a root, and $\deg(m_{\alpha,\mathbb{F}})$ is minimal. We call $m_{\alpha,\mathbb{F}}(x)$ the **minimal polynomial of** $\alpha/\mathbb{F}$.

As a simple example:

$$m_{\sqrt{2},\mathbb{Q}}(x) \ = \ x^2 - 2 \ = \ m_{-\sqrt{2},\mathbb{Q}}(x)$$

Theorem 16.2

Suppose $\alpha \in \mathbb{L}$ is algebraic over $\mathbb{K}$, an extension of $\mathbb{F}$. Then α has two minimal polynomials:

$$m_{\alpha,\mathbb{K}}(x) \qquad m_{\alpha,\mathbb{F}}(x)$$

In general, these are not equal. However:

$$m_{\alpha,\mathbb{K}}(x) \mid m_{\alpha,\mathbb{F}}(x)$$

Proof.

Note $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x] \subseteq \mathbb{K}[x]$. So $m_{\alpha,\mathbb{F}}(x)$ as an element of $\mathbb{K}[x]$ is in the ideal $(m_{\alpha,\mathbb{K}}(x))$. ■

Source: Primary Source Material

Definition 16.5

If α is algebraic over $\mathbb{F}$, then the **degree of** α is:

$$\deg(\alpha) \ = \ \deg_{\mathbb{F}}(\alpha) \ = \ \deg(m_{\alpha,\mathbb{F}}(x))$$

Recall that if α is algebraic over $\mathbb{F}$, then $\mathbb{F}[\alpha] \simeq \mathbb{F}[x]/(m_{\alpha,\mathbb{F}}(x))$.

Theorem 16.3

If α is algebraic over $\mathbb{F}$, then $\mathbb{F}[\alpha]/\mathbb{F}$ is finite.

Last week we found a basis given by $\overline{1}, \overline{x}, \ldots, \overline{x}^{d-1}$, where $d = \deg(\alpha)$.

Example

Consider quadratic extensions $\mathbb{F}[\sqrt{D}]/\mathbb{F}$. We'll assume $\operatorname{char}(\mathbb{F}) \neq 2$.

Then the roots of a quadratic polynomial are given by:

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

Note this doesn't work if char $= 2$, since the denominator would be 0.

For instance, in $\mathbb{F}_2[x]$, the monic quadratics are:

$$x^2 \qquad x^2+1 \qquad x^2+x \qquad x^2+x+1$$

Note that all except the last one factor. In particular, the second polynomial has a root 0, but we know it has no roots in $\mathbb{R}$. So these are "just different".

However, if $\operatorname{char}(\mathbb{F}) \neq 2$, then the formula does indeed work. In particular:

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

So $\left\{1, \sqrt{D}\right\}$ is a basis (where $D = b^2 - 4ac$), provided that D is not square.

Source: Primary Source Material

In other words, any nontrivial quadratic extension is $\mathbb{F}[\sqrt{D}]$ for some nonsquare D.

Suppose $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ is a tower of fields, and that they are all finite extensions. We can find a basis for $\mathbb{L}/\mathbb{K}, \{L_1, \ldots, L_r\}$.

Any arbitrary $\alpha \in \mathbb{L}$ can be written as:

$$\alpha = b_1 L_1 + \cdots + b_r L_r = \sum_{i=1}^{r} b_i L_i \qquad b_i \in \mathbb{K}$$

We can also find a basis for $\mathbb{K}/\mathbb{F}, \{K_1, \ldots, K_s\}$. Any $\beta \in K$ can similarly be written as:

$$\beta = \sum_{j=1}^{s} a_j K_j$$

In particular, $b_i \in \mathbb{K}$, so we can write:

$$b_i = \sum_{j=1}^{s} a_j^i K_j$$

for each $i, a^i_j \in \mathbb{F}$. Then, putting it all together, we have:

$$\alpha \;=\; \sum_{i=1}^{r} b_i L_i \;=\; \sum_{i=1}^{r}\left(\sum_{j=1}^{s} a^i_j K_j\right) L_i \;=\; \sum_{i=1}^{r}\sum_{j=1}^{s} a^i_j (K_j L_i)$$

So the set $\{K_j L_i\}$ spans $\mathbb{L}/\mathbb{F}$. Is it linearly independent? (Yes.) Suppose there exists $a^i_j \in \mathbb{F}$ such that:

$$\begin{aligned} \sum_{i=1}^{r}\sum_{j=1}^{s} a^i_j (K_j L_i) \;&=\; 0 \\ \implies \sum_{i=1}^{r}\left(\sum_{j=1}^{s} a^i_j K_J\right) L_i \;&=\; \sum_{i=1}^{r} b_i L_i \;=\; 0 \end{aligned}$$

Since L_i is a basis for $\mathbb{L}/\mathbb{K}$, we have that $b_i = 0$. But then since K_j is a basis for $\mathbb{K}/\mathbb{F}$, it follows that each $a^i_j = 0$, so $\{K_j L_i\}$ is indeed a basis for $\mathbb{L}/\mathbb{F}$.

Theorem 16.4

Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be finite field extensions. Then:

$$[\mathbb{L} : \mathbb{F}] \;=\; [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]$$

This is analogous to the result about the indices of subgroups.

This also holds for infinite extensions: if either side is infinite, the other must be as well.

Corollary

Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be finite field extensions. Then:

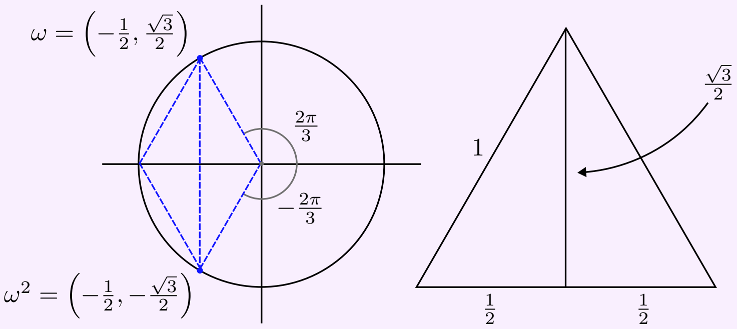
$$[\mathbb{K} : \mathbb{F}] \mid [\mathbb{L} : \mathbb{F}] \qquad [\mathbb{L} : \mathbb{K}] \mid [\mathbb{L} : \mathbb{F}]$$

Example

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. This is irreducible by Eisenstein. One root of f is $\sqrt[3]{2} \in \mathbb{R}$. Notice:

$$\left(i\sqrt[3]{2}\right)^3 \;=\; i^3\left(\sqrt[3]{2}\right)^3 \;=\; (-i)2 \qquad \text{“oops”}$$

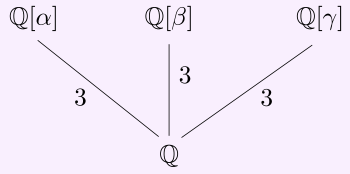
We can see that:


$\omega = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$
$\frac{2\pi}{3}$
$-\frac{2\pi}{3}$
$\omega^2 = \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$
1
$\frac{\sqrt{3}}{2}$
$\frac{1}{2}$
$\frac{1}{2}$

So, we have that:

$$x^3 - 2 \ = \ \left(x - \sqrt[3]{2}\right)\left(x - \omega\sqrt[3]{2}\right)\left(x - \omega^2\sqrt[3]{2}\right)$$

Denoting the roots as α, β, γ respectively, we can start with $\mathbb{Q}$ and adjoin each of them:



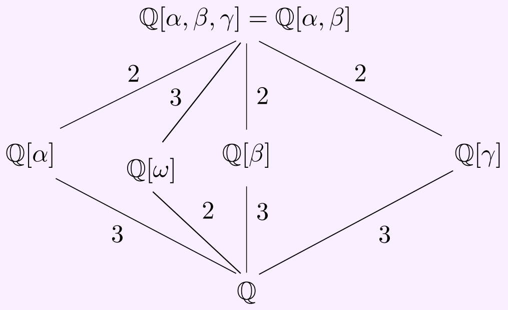
Do $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\beta]$ have an intersection $\mathbb{F}$ bigger than $\mathbb{Q}$? If so, then:

$$[\mathbb{F} : \mathbb{Q}] \mid 3 \implies [\mathbb{F} : \mathbb{Q}] = 1, 3$$

So we see it is not possible:

- $\mathbb{Q}[\alpha] \cap \mathbb{Q}[\beta] = \mathbb{Q}$
- $\mathbb{Q}[\alpha] \cap \mathbb{Q}[\gamma] = \mathbb{Q}$
- $\mathbb{Q}[\beta] \cap \mathbb{Q}[\gamma] = \mathbb{Q}$

In $\mathbb{Q}[\alpha, \beta]$, we have $\sqrt[3]{2}, \omega\sqrt[3]{2}$, so $\omega \in \mathbb{Q}[\alpha, \beta]$. But $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}$, thus:



So $[\mathbb{Q}[\alpha, \beta, \gamma] : \mathbb{Q}] = 6$.

Source: Primary Source Material

that was probably meant to be the 6th root not the 3rd, joe messed sth up here

Definition 16.6

An extension $\mathbb{K}/\mathbb{F}$ is **finitely generated** if:

$$\mathbb{K} = \mathbb{F}[\alpha_1, \dots, \alpha_n]$$

for some α_i's.

Lemma

We see that $\mathbb{F}[\alpha, \beta] = \mathbb{F}[\alpha][\beta] = \mathbb{F}[\beta][\alpha]$.

Proof.

If $\mathbb{F}[\alpha, \beta]$ is the smallest field containing $\mathbb{F}, \alpha, \beta$, then $\mathbb{F}[\alpha, \beta] \subseteq \mathbb{F}[\alpha][\beta] \subseteq \mathbb{F}[\alpha, \beta]$. A similar argument holds for $\mathbb{F}[\beta][\alpha]$. ok joe ■

Source: Primary Source Material

Theorem 16.5

An extension $\mathbb{K}/\mathbb{F}$ is finite if and only if $\mathbb{K}$ is finitely generated by algebraic elements.

Proof.

Previous result, repeated many times. ok joe 2 ■

Source: Primary Source Material

Theorem 16.6

If $\deg(a_i) = n_i$, then:

$$[\mathbb{F}[\alpha_1, \dots, \alpha_r] : \mathbb{F}] \leq n_1 \cdots n_r$$

Corollary

If α, β are algebraic over $\mathbb{F}$, then so are:

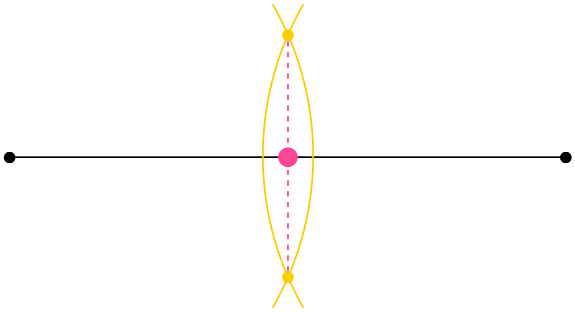
$$\alpha \pm \beta \qquad \alpha\beta \qquad \frac{\alpha}{\beta}\ (\beta \neq 0) \qquad \frac{1}{\alpha}\ (\alpha \neq 0)$$

on friday: straightedge and compass constructions :) (which i will miss due to 257 midterm)

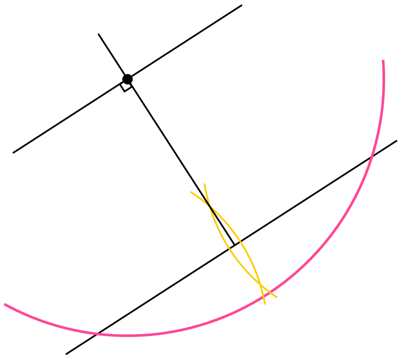
17 Straightedge and Compass Constructions

Lec 42 - Mar 21 (Week 23)

Back in Ancient Greece, mathematicians only used straight edges and compasses to draw lines and curves. Using a straightedge and compass, we can find the midpoint between any 2 points in the plane:

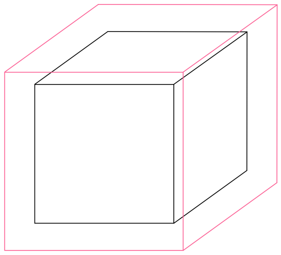


Similarly, given a line and a point not on it, we can draw a line parallel to the line which passes through the point:

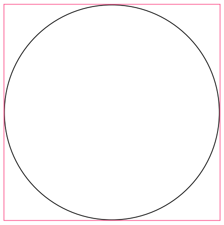


We're concerned with three particularly famous problems related to such counstructions:

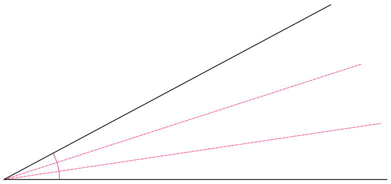
Doubling the cube (Find $\sqrt[3]{2}$):



Squaring the circle (Find $\sqrt{\pi}$):



Trisecting the angle (Find $\cos(\theta/3)$):

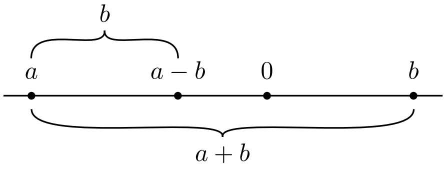


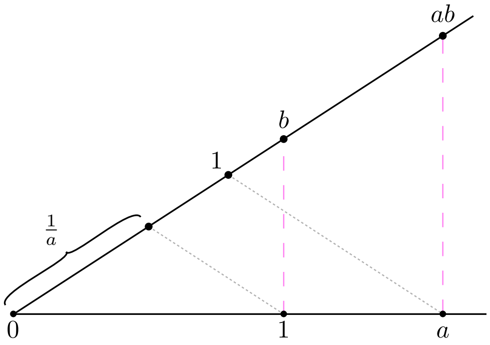
We will work in the plane $\mathbb{R}^2$ writing points as (x, y). We assert a line to be of **unit length** from $(0, 0)$ to $(1, 0)$. When we find points of intersection of 2 lines, circles or a line and circle, we get new points whose coordinates can be described.

Definition 17.1

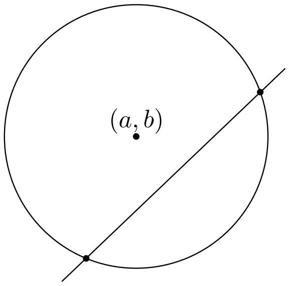
A number is called a **constructible number** if it is possible to construct a line segment of the corresponding length using only a straightedge and compass in $\mathbb{R}^2$.

The set of constructible numbers are closed under addition, subtraction, multiplication, and inverses:



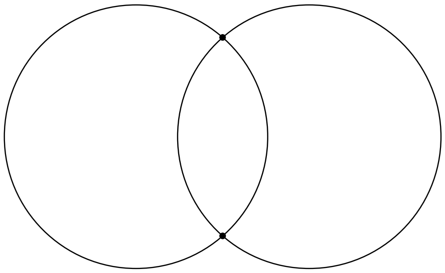


Thus, the set of constructible numbers is in fact a *field*. The point of intersection of two lines is also constructible, and:



$$(x-a)^2+(y-b)^2=r^2 \quad (1)$$
$$Ax+By=C \quad (2)$$

Can use (2) to eliminate y, making (1)
a quadratic in one variable. The coordinates
of the intersection pts might have square roots



$$x^2+y^2+\mathcal{O}(n)$$
$$x^2+y^2+\mathcal{O}(m)$$

subtracting yields a linear equation

So what does this all mean?

Any of these basic steps can produce coordinates which are either in the same field as the original diagram, *or* in a quadratic extension. A sequence of such basic steps that guarantee a field of degree 2^k over $\mathbb{Q}$:

$$\begin{tikzcd}
\mathbb{Q}[\sqrt{d_1},\ldots,\sqrt{d_k}] \arrow[dddd, dash, bend left=60, "2^k"] \\
\vdots \\
\mathbb{Q}[\sqrt{d_1},\sqrt{d_2}] \arrow[d, dash, "2"] \\
\mathbb{Q}[\sqrt{d_1}] \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

But this tells us something: Say we could double a cube. Then, the sides of this new cube would be length $\sqrt[3]{2}$, meaning some coordinates would be in $\mathbb{Q}[\sqrt[3]{2}]$. By Eisenstein, x^3-2 is irreducible, so we get:

$$\begin{tikzcd}
 & \mathbb{F} \arrow[dddd, dash, bend left=60, "2^k"] \\
 & \vdots \\
 & \mathbb{F}_2 \arrow[d, dash] \\
\mathbb{Q}[\sqrt[3]{2}] \arrow[dr, dash, "3"'] & \mathbb{F}_1 \arrow[d, dash] \\
 & \mathbb{Q}
\end{tikzcd} \qquad \implies \quad [\mathbb{Q}[\sqrt[3]{2}:\mathbb{Q}]=3\nmid 2^k$$

So we see $\mathbb{Q}[\sqrt[3]{2}]$ *cannot* be in any field created by basic steps. Thus, we conclude that doubling the cube is in fact *impossible* with a straightedge and compass. (brandon note: "what crack was the guy who solved this smoking when realized this?? i need some")

Another result is that since π is transcendental, so is $\sqrt{\pi}$, so we have that $[\mathbb{Q}[\pi]:\mathbb{Q}] = \infty$, which is even worse than before. Okay, what about trisecting angles? Can we construct $\cos(\theta/3)$?

Turns out, the answer is “sometimes”, but not in general. For example, it happens that $\cos(20°/3)$ satisfies an irreducible cubic, so this can’t be constructed. However, any angle which is a multiple of $3°$ *can* be trisected.

Lec 43 - Mar 26 (Week 24)

Pierre Waltsen solved the constructibility problems.

Definition 17.2

Suppose $f(x) \in \mathbb{F}[x]$. An extension $\mathbb{E}/\mathbb{F}$ is a **splitting field** for f if f “splits completely”, i.e.:

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

and $f(x)$ does *not* split for any subfield of $\mathbb{E}$.

Example

For $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, its splitting field is $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. Note that both $\pm\sqrt{2} \in \mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.

For $g(x) = x^2 + 1 \in \mathbb{C}[x]$, it already splits, so $\mathbb{C}$ is its splitting field. For $g(x) \in \mathbb{R}[x]$, its splitting field is $\mathbb{C}/\mathbb{R}$.

For $x^3 - 2 \in \mathbb{Q}[x]$, its splitting field is $\mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$, an extension of $\mathbb{Q}$ with degree 6.

For $h(x) = x^4 + 4 \in \mathbb{Q}[x]$, it has roots $1 \pm i, -1 \pm i$. Thus, its splitting field is $\mathbb{Q}[i]/\mathbb{Q}$.

Source: Primary Source Material

Theorem 17.1

Given $f(x) \in \mathbb{F}[x]$, there exists a splitting field for f.

Proof.

If $\deg(f) = 1$, then $\mathbb{F}$ is clearly the splitting field. Furthermore, $\mathbb{F}$ is the splitting field for any polynomial that splits in $\mathbb{F}$.

Assume by induction that the result holds for polynomials g where $\deg(g) < n = \deg(f)$. We know we can construct $\mathbb{E}/\mathbb{F}$ such that if $\alpha \in \mathbb{E}$ and $f(\alpha) = 0$, then $f(x) = (x-\alpha)g(x)$ for some g. Furthermore, $\deg(g) < n$, so let $\mathbb{E}$ be the splitting field of g.

Let $\mathbb{K} = \mathbb{E}[\alpha]$. Then, we see that f splits in $\mathbb{K}$. To take a minimal field, take the intersection of all fields in which f split. ■

Source: Primary Source Material

Definition 17.3

An extension $\mathbb{E}/\mathbb{F}$ is **normal** if $\mathbb{E}$ is a splitting field for some $f(x) \in \mathbb{F}[x]$; that is, it is generated by the roots of f.

Example

The field $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is *not* normal.

Note $\sqrt[3]{2}$ is a root of x^3-2, but the *other* roots $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are not in $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$.

The normal extension is $\mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$.

Source: Primary Source Material

Question: if $f(x) \in \mathbb{F}[x]$, can it have two different splitting fields? (should really ask - can it have two *non-isomorphic* splitting fields?) Answer: unsurprisingly, no.

Suppose $\varphi : \mathbb{F} \longrightarrow \mathbb{F}'$ is an isomorphism, and $f(x) \in \mathbb{F}[x]$. It induces a map $\mathbb{F}[x] \longrightarrow \mathbb{F}'[x]$.

If $\mathbb{E}/\mathbb{F}, \mathbb{E}'/\mathbb{F}'$ are splitting fields for f, f' respectively, then φ extends to an isomorphism $\mathbb{E} \longrightarrow \mathbb{E}'$. The proof from here follows by a similar induction argument as above.

Thus, we can indeed talk about *the* splitting field of f over $\mathbb{F}$.

Observe that the splitting field of f is $\mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$, where the α_i's are the roots of f. Since $\mathbb{F}[\alpha_1, \ldots, \alpha_n] = \mathbb{F}[\alpha_1][\alpha_2]\ldots[\alpha_n]$, note that:

$$[\mathbb{F}[\alpha_1] : \mathbb{F}] \leq n = \deg(f)$$

In this field, $f(x) = (x-\alpha_1)f_1(x)$, where $\deg(f_1) = n-1$. Then:

$$[\mathbb{F}[\alpha_2] : \mathbb{F}[\alpha_1]] \leq n-1$$

As we keep going, we see that:

$$\begin{aligned}[\mathbb{F}[\alpha_1, \ldots, \alpha_n] : \mathbb{F}] &= [\mathbb{F}[\alpha_1] : \mathbb{F}] \cdot [\mathbb{F}[\alpha_1 \alpha_2] : \mathbb{F}[\alpha_1]] \cdots [\mathbb{F}[\alpha_1, \ldots, \alpha_n] : \mathbb{F}[\alpha_1, \ldots, \alpha_{n-1}]] \\ &\leq n(n-1)(n-2)\ldots 2 \cdot 1 = n!\end{aligned}$$

Example

Notice $[\mathbb{F}[\sqrt{\alpha}] : \mathbb{F}]$ is equal to: $\begin{cases} 2 & d \text{ not a square} \\ 1 & d \text{ square} \end{cases}$. And indeed, $2 = 2! = \deg(x^2 - \alpha)$.

Notice $[\mathbb{Q}[\sqrt[3]{2}], \sqrt{-3}] = 6 = 3! = \deg(x^3 - 2)$.

For $x^4 - 4, 4! = 24$. Then:

$$[\text{splitting field} : \mathbb{Q}] \;=\; [\mathbb{Q}[i] : \mathbb{Q}] = 2 \neq 24$$

So "most" irreducible polynomials have splitting fields of degree $= (\deg(f))!$.

Source: Primary Source Material

18 Cyclotomic Fields (Roots of Unity)

Consider $x^n - 1 \in \mathbb{Q}[x]$. Clearly:

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

As complex numbers, we know what these roots look like:

[roots]

If $n = p$ is prime, we have previously shown that $x^{p-1} + \cdots + x + 1$ is irreducible, meaning:

$$[\mathbb{Q}[e^{2\pi i/p}] : \mathbb{Q}] = p - 1$$

Note: $\mathbb{Q}[e^{2\pi i/p}]$ contains every power $e^{2\pi ik/p}$, so it is the splitting field of $x^p - 1$. In particular:

$$[\mathbb{Q}[e^{2\pi i/p}] : \mathbb{Q}] = p - 1 < (p-1)! \qquad \text{(unless } p = 2, 3\text{)}$$

[doubleroots]

When we add $n = 6$, we get the mirror image. Notice that the $\sqrt{3}$ is the same in the expression. When adding the 6th roots of unity, the splitting field does not increase.

Definition 18.1

A root ζ of $x^n - 1$ is a **primitive nth root of unity** if it generates the multiplicative group of all nth roots of unity.

As it turns out, the number of primitive roots is $\varphi(n)$. A little less obvious is that this is also the degree of the splitting field.

Example

For $n = 4$, we have for $x^4 - 1$:
[runningoutofnames]
Notice -1 is a root of $x^2 - 1$ (and so is 1). In particular:

$$x^2 - 1 \mid x^4 - 1 \qquad x^4 - 1 = (x^2 - 1)(x^2 + 1)$$

By factoring, we get the primitive roots of unity.

Let's try this with $n = 6$:

$$x^6 - 1 \;=\; (x^3 - 1)(x^3 + 1) \;=\; (x^3 - 1)(x + 1)(x^2 - x + 1)$$

Indeed, $x^2 + x + 1$ gives the primitive 6th roots.

Source: Primary Source Material

It's common to write ζ_n for a primitive nth root of unity. We tend to think of $\zeta_n = e^{2\pi i/n}$, but it could be any primitive root.

If $\varphi : \mathbb{Q}[\zeta_p] \longrightarrow \mathbb{Q}[\zeta_p]$ is an automorphism, it fixes the elements of $\mathbb{Q}$. What does it do to ζ_p? Note $\varphi(\zeta_p)$ has to be a pth root of unity, and not 1. That is: $\varphi(\zeta_p) = \zeta_p^a$, for some $a = 1, \ldots, p - 1$. So:

$$\varphi(\zeta_p^k) = (\zeta_p^a)^k = (\zeta_p^k)^a$$

The automorphisms of $\mathbb{Q}[\zeta_p]$ take each non-trivial pth root of unity to a power of itself. Furthermore, it is easy to see that the number of automorphisms is the same as the degree of the extension.

Lec 44 - Mar 28 (Week 24)

Recall that a primitive nth root of unity is a generator for the group of nth roots; we denote the whole group by μ_n. Clearly, if $m \mid n$, then any mth root of unity is also an nth root. Symbolically, $\mu_m \subseteq \mu_n$.

Definition 18.2

We denote by $\Phi_n(x)$ the monic polynomial of degree $\varphi(n)$ whose roots are precisely the primitive nth roots of unity.

Since the primitive mth roots are in μ_n if $m \mid n$, then we have that:

$$\Phi_n(x) \mid (x^n - 1)$$

Corollary

Every nth root of unity is a primitive mth root for some $m \mid n$. Furthermore:

$$x^n - 1 \;=\; \prod_{m \mid n} \Phi_m(x)$$

Example

For the first few n, we have:

1. $\Phi_1(x) = x - 1$
2. $\Phi_2(x) = x + 1$
3. $\Phi_3(x) = (x - \omega)(x - \overline{\omega}) = x^2 + x + 1$
4. $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{x^2-1} = x^2 + 1$
5. $\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = x^4 + \cdots + x + 1$
6. $\Phi_6(x) = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \cdots = x^2 - x + 1$

For any prime p:

$$\Phi_p(x) \;=\; \frac{x^p - 1}{x - 1} \;=\; x^{p-1} + \cdots + x + 1$$

Source: Primary Source Material

The cyclotomic fields and hence the cyclotomic polynomials are important for various reasons; many interesting fields are contained within cyclotomic fields.

Definition 18.3

Given a polynomial $f(x) = (x - \alpha_1)^{m_1} \cdots (x - \alpha_n)^{m_n}$ where each α is distinct, the m_i's are called the **multiplicity** of the corresponding root a_i's.

If $m_i = 1$ for all i, we say that f is **multiplicity free**, or **separable**. Otherwise, f is **inseparable**.

Lemma

Over a field $\mathbb{F}$ with $\operatorname{char}(\mathbb{F}) = 0$, any irreducible polynomial is separable.

Funny things happen in $\operatorname{char}(\mathbb{F}) = p > 0$.

Example

Consider $\mathbb{F}_2[x]$, and let $f(x) = x^2 - t$ for some variable t. Then, in some extension field:

$$(x - \sqrt{t})(x + \sqrt{t}) = (x + \sqrt{t})^2$$

So, we see it is inseparable. But, in $\mathbb{F}_2(x)$, we see that f is indeed irreducible.

Source: Primary Source Material

In a field of prime characteristic, notice that:

$$(a+b)^p \;=\; a^p + \underbrace{\qquad\qquad\qquad}_{\text{coeff's here divisible by } p} +b^p$$

In other words, $(a+b)^p = a^p + b^p$. Since $(ab)^p = a^p b^p$, then $x \mapsto x^p$ is a field homomorphism. If $\mathbb{F}$ is finite, it is injective, and therefore an automorphism. This is called the **Frobenius automorphism**. Since every $x \in \mathbb{F}$ is a pth power, we can write $f(x) = g(x^p)$ for some g.

Over $\mathbb{R}$, a polynomial f has a as a repeated root with multiplicity k if:

$$f(a) \;=\; 0 \;=\; f'(a) \;=\; \ldots \;=\; f^{(k-1)}(a)$$

Note that this also works with char p.

Consider $f(x) = x^p - x$; the roots are things that equal their pth power. Then:

$$f'(x) = px^{p-1} - 1 = 0 - 1 = -1 \neq 0$$

So we see that f has no repeated roots, and thus is separable. Over $\mathbb{F}_p$, consider $f(x) = x^{p^k} - x$. Again, $f'(x) = -1 \neq 0$. So $f(x)$ is separable, and thus has p^k roots in some extension field. The set of roots of f is a field $\mathbb{F}_{p^k}$ of order p^k.

Theorem 18.1

Every finite field is $\mathbb{F}_{p^k}$ for some prime p and integer $k \geq 1$.

Of course $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, but $\mathbb{F}_{p^2} \neq \mathbb{Z}/p^2\mathbb{Z}$, etc. For each p, we get a tower of fields:

[fieldtree]

Given a field $\mathbb{F}$, we can consider $\operatorname{Aut}(\mathbb{F})$. For any $\varphi \in \operatorname{Aut}(\mathbb{F})$, note that:

$$\varphi(1) \;=\; 1 \qquad \varphi(2) \;=\; \qquad \varphi(n) = n \quad n \in \mathbb{Z}$$

So φ fixes $\mathbb{Z}$ and hence fixes $\mathbb{Q}$, if $\operatorname{char}(\mathbb{F}) = 0$. Otherwise, it fixes $\mathbb{Z}/p\mathbb{Z}$ if $\operatorname{char}(\mathbb{F}) = p$.

If $\mathbb{E}/\mathbb{F}$ is an extension, we write $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ for the automorphisms of $\mathbb{E}$ which fix $\mathbb{F}$ pointwise. For instance:

$$\operatorname{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, z \mapsto \overline{z}\}$$
$$\text{But } \operatorname{Aut}(\mathbb{C}) \text{ is enormous.}$$

19 Galois Theory, Briefly

Lec 45 - Apr 02 (Week 25)

Due to time, we won't be proving most things for this unit. Thankfully, the proofs themselves aren't typically that hard; the hard part is setting up / building up to them, which we will do.

Consider the group $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$. Suppose $H \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$. Let $L \subseteq \mathbb{K}$ be the set of elements of $\mathbb{K}$ fixed by each element of H:

$$L = \{x \in \mathbb{K} : \varphi(x) = x, \varphi \in H\}$$

We see that L is a field, called the **fixed field** of H.

The association between H and the fixed field of H reverses order: if $H_1 \leq H_2 \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, writing L_i as the fixed field of H_i, then $L_2 \subseteq L_1$. Similarly, if $L_1 \subseteq L_2$, then $H_2 \leq H_1$.

Example

Recall the splitting field of $x^3 - 2$:
[diagram]
One automorphism of $\mathbb{K}$ is complex conjugation. It takes $\omega \mapsto \overline{\omega} = \omega^2$ and fixes $\sqrt[3]{2}$, the real root. So the fixed field of $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathbb{Q}[\sqrt[3]{2}]$.

Source: Primary Source Material

Suppose $\mathbb{K}/\mathbb{F}$ is a splitting field of $f(x)$. Any automorphism of $\mathbb{K}$ must take a root α of $f(x)$ to another root β. If f is irreducible, then the automorphism is uniquely determined by the root. Thus:

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}]$$

Moreover, we have equality if $\mathbb{K}/\mathbb{F}$ is separable.

Definition 19.1

An extension $\mathbb{K}/\mathbb{F}$ is a **Galois extension**, or simply **Galois**, if $|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$.

Theorem 19.1

An extension $\mathbb{K}/\mathbb{F}$ is Galois iff $\mathbb{K}$ is the splitting field of a separable polynomial.

Example

Let $\mathbb{K} = \mathbb{F}[\sqrt{D}]$ for some nonsquare D. Note $[\mathbb{K} : \mathbb{F}] = 2$. The only non-trivial automorphism is $\sqrt{D} \mapsto -\sqrt{D}$:

$$a + b\sqrt{D} \mapsto a - b\sqrt{D}$$

Then $|\mathrm{Aut}(\mathbb{K} : \mathbb{F})| = 2$.

Source: Primary Source Material

Consider $\mathbb{F} = \mathbb{Q}, \mathbb{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. This is known as a "biquadratic extension".

[diagram]

A basis is given by $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Then:

	1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
id	1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
$\sqrt{2} \mapsto -\sqrt{2}$	1	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{6}$
$\sqrt{3} \mapsto -\sqrt{3}$	1	$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{6}$
$\sqrt{6} \mapsto -\sqrt{6}$	1	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{6}$

We have 4 automorphisms, and $[\mathbb{K} : \mathbb{F}] = 4$, so these are all of them.

Furthermore, $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is abelian of order 4, with elements of order 1 and 2. So $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \simeq C_2 \times C_2$, the Klein 4-group. Notice:

[diagram]

So both the group and field lattice have the same shape. But we have to be careful; more generally, the (sub)field lattice should be inverted; it so happens in this case that the inversion is the same shape.

One more example: take the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

[diagram]

Notice that this is precisely the group S_3 (equivalently D_3). Indeed, the group lattice of S_3 is given by:

[diagram]

...

Theorem 19.2: Fundamental Theorem of Galois Theory

Suppose $\mathbb{K}/\mathbb{F}$ is Galois.

Then, there is an order-reversing isomorphism between the lattice of subfields of $\mathbb{K}$ containing $\mathbb{F}$, and the subgroups of $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$, according to which a subgroup corresponds to its fixed field.
[diagram]
Moreover, if $H \trianglelefteq G$, then $\mathbb{L}/\mathbb{F}$ is Galois, and $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \simeq G/H$.

If H, H' are subgroups of $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ with fixed fields L, L', then $H \cap H'$ has fixed field LL'. Analogously, HH' has fixed field $L \cap L'$.

Some extensions $\mathbb{K}/\mathbb{F}$ are Galois, and its Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is abelian (like quadratic extensions). In such cases, we say $\mathbb{K}/\mathbb{F}$ is an **abelian extension**. These are quite special.

Example

An important example: cyclotomic fields $\mathbb{Q}[\mu_n]/\mathbb{Q}$. We have:

$$\mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

where the action takes a primitive root to one of its powers. For example:

- $\mathbb{Q}[\mu_2] = \mathbb{Q}$
- $\mathbb{Q}[\mu_3] = \mathbb{Q}[\sqrt{-3}]$
- $\mathbb{Q}[\mu_4] = \mathbb{Q}[i] = \mathbb{Q}[\sqrt{-1}]$
- $\mathbb{Q}[\mu_8] = \mathbb{Q}[i, \sqrt{2}]$

Source: Primary Source Material

Theorem 19.3: Kronecker-Weber Theorem

Any abelian extension is contained in a cyclotomic field. “thats a really hard theorem”

Amongst the regular n-gons, which of them are constructible?

A number of the form $n^2 + 1$ which happens to be prime is known as a “Fermat prime”. For instance, the first few are given as $2, 5, 17, 37, 101$, and so on. (this seems wrong?)

As it turns out, the regular n-gon is constructible if and only if:

$$n = 2^r p_1 \cdots p_k$$

where each p_i is a Fermat prime.

friday: insolvability of the quintic! (which really refers to irreducible polynomials of degree ≥ 5) note that this doesn’t mean they can *never* be solved, but that “generally” they cannot be.

Lec 46 - Apr 04 (Week 25)

Incorrect definition of Fermat prime last time - a Fermat prime is a number of the form $2^{2^\alpha} + 1$ which happens to be prime. The first few are $3, 5, 17, 257, 65537$. In fact, these are the only known ones.

Onto the other poster child of Galois theory. COnsider $x^3 - 2$:

[diagram]

The field $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$ has basis $\{1, \sqrt[3]{2}, \omega\}$, and lies completely within the reals. Note that it is, in particular, not Galois(?).

Definition 19.2

A Galois extension is **cyclic** if its Galois group (the group of automorphisms) is cyclic.

Consider $\mathbb{F}[\sqrt[n]{a}]$. This has an nth root of a; it must necessarily contain *all* the roots of $x^n - a$ iff $\mathbb{F}$ contains μ_n, the (primitive) nth roots of unity. In this situation, any element of $\mathrm{Gal}(\mathbb{F}[\sqrt[n]{a}]/\mathbb{F})$ must permute those roots. In particular:

$$\sigma : \sqrt[n]{a} \mapsto \omega \sqrt[n]{a} \qquad \omega \in \mu_n$$

It is easy to see that $\sigma(\omega' \sqrt[n]{a}) = \omega\omega' \sqrt[n]{a}$, and σ fixes ω'. This is because we assumed $\mathbb{F}$ contains μ_n(?). This gives us a homomorphism $\mathrm{Gal}(\mathbb{F}[\sqrt[n]{a}]/\mathbb{F}) \longrightarrow \mu_n$. This map is injective, and so $\mathrm{Gal}(\mathbb{F}[\sqrt[n]{a}]/\mathbb{F})$ is a subgroup of μ_n, a cyclic group. Thus, $\mathrm{Gal}(\mathbb{F}[\sqrt[n]{a}]/\mathbb{F})$ is necessarily cyclic.

We want to take a polynomial $f(x) \in \mathbb{F}[x]$ and find a formula for its roots. For example:

$$(\sqrt{2} + 3)\left(\frac{1}{\sqrt[3]{12 - \sqrt{5} + \frac{1}{3 + \sqrt[5]{7}}}}\right) + 3$$

Such an element is in an extension $\mathbb{L}/\mathbb{F}$ for which:

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_t = \mathbb{L}$$

where each $\mathbb{K}_i/\mathbb{K}_{i-1}$ is of the form $\mathbb{K}_i = \mathbb{K}_{i-1}\sqrt[n_i]{a_i}]$. If we assume that $\mathbb{F}$ contains all the μ_{n_i}’s, then each $\mathbb{K}_i/\mathbb{K}_{i-1}$ is cyclic. Note we can always assume $\mathbb{F}$ contains the necessary roots of unity by putting them in at the beginning of the chain:

$$\mathbb{F} \subseteq \mathbb{F}[\mu_{n_1}] \subseteq \mathbb{F}[\mu_1, \mu_2] \subseteq \cdots \subseteq \mathbb{K}_1 \subseteq \cdots$$

Each step is still cyclic.

On the Galois group side, each quotient G_{i-1}/G_i will be cyclic, which means that $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable. (Sidenote: this is why these groups are called solvable; it's primarily about solving polynomials.) The converse is also true: if $\mathbb{L}$ is the splitting field of some $f(x) \in \mathbb{F}[x]$ and $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable, then each root of f is an element of $\mathbb{L}$, which is obtained by adding nth roots to $\mathbb{F}$.

A technical subtlety: this works if $\mathrm{char}\,(\mathbb{F}) = 0$ or p, and p does not divide any n_i.

We would be done if we could find a polynomial of degree 5 whose Galois group is A_5. According to the book, we can consider $x^5 - 6x + 3$ (possibly incorrect signs), which indeed has Galois group A_5.

Let's go back to the cubic. We write $y^3 + ay^2 + by + c$. If we substitute $y = x - \frac{a}{3}$, then we get $x^3 + px + q$, which has no quadratic term. Thus, we can focus on solving this simpler equation.

We write the *discriminant* as $D = -4p^3 - 27q^2$; in particular, $D = 0$ iff the polynomial has a repeated root (this is worked out in the book).

If f is irreducible, consider its splitting field $\mathbb{L}$, so $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is in S_3. In particular, it must be either S_3 or A_3. Happily (or maybe not, because it's a perfect exam question -joe), if D is a square in $\mathbb{F}$, then $\mathrm{Gal} = A_3$. If it is not, then $\mathrm{Gal} = S_3$.

...and that's all folks!