MATH 250A: Groups, Rings, and Fields

Jad Damaj

Fall 2022

Contents

Chapter 1

Groups

1.1 August 25

1.1.1 Groups

Two ways to define groups

- concrete: group = symmetries of an object X. Here a symmetry is a bijection $X \to X$ with inverse that preserves "structure" (topology, order, binary operation, ...)

Example 1.1.1. The rectangle has 4 symmetries.
The icossahedron has 20×3 symmetries since after fixing the first face there are 3 possible rotations.
Vector space $\mathbb{R}^k$: $n \times n$ matrices with $\det \neq 0$, denoted $GL_n(K)$

- abstract definition:

Definition 1.1.2. A group is a set G with a binary operation $G \times G \to G$ by $(a, b) \mapsto ab, a\times, a+b, \ldots$ with "Inverse" : $G \to G$ by $a \mapsto a^{-1}$ and "Identity": $1, 0, e, I, \ldots$ satsifying the axioms:
$1x = x1 = x \quad x(x^{-1}) = (x^{-1})x = 1 \quad (xy)z = x(yz)$

We can go from the concrete definition to the abstract one: the binary operation is composition, the identity is the trivial symmetry, inverses given y "undoing' a symmetry.

Is an abstract group the symmetries of something?

Theorem 1.1.3 (Cayley's Theorem)**.** Any abstract group is the group of symmetries of some mathematical object.

Recall group actions :

Definition 1.1.4. Given a group G, a set S, a (left) gtroup action is a map $G \times S \to S$ by $(g, s) \mapsto g(s), gs$ satisfying $g(h(s)) = gh(s)$, $1s = s$.

To prove Cayley's theorem we need to find :

1. a set S acted on by G

2. structure on S so that $G =$ all symmetries.

What is S? Take $S = G$.

Need to define the action of $GonG$. There are 8 natural ways to do this.
First 4, we defin4 $G \times S \to S$ by

- $g(s) = s$ trivial action
- $g(s) = gs$ group product
- Try $g(s) = sg$ Fails since G not necesarily commutative: $g(h(s)) = (sh)g \neq s(gh) = gh(s)$
- $g(s) = sg^{-1}$ works since $g(h(s)) = g(sh^{-1}) = sh^{-1}g^{-1} = s(gh)^{-1} = gh(s)$
- $g(s) = gsg^{-1}$ adjoint action

The above group action is known as a left group action, We define a right group action in a similar way : $S \times G \to S$ by$(s, g) \mapsto (s)g, s^g$ satisfying (sg)h = s(gh), $s1 = s$.

We now define right group actions of G on G: $S \times G \to G$ by

- $(s, g) \mapsto s$
- $(s, g) \mapsto sg$
- $(s, g) \mapsto g^{-1}s$
- $(s, g) \mapsto g^{-1}sg$

Now we have $S = G$, S=set acted on by G using left action $g(s) = gs$ - left translation. So we have shown $G \subseteq$ symmetries of S.

Want : G =symmetries of S + "structure". Let structure on S= right action of G on S.
We now have 3 copies of G:

1. set $S = G$
2. G acts on left on S (G = symmetries of S)
3. G acts o the right on S (Structure of S)

Object $S = S$ + right G action

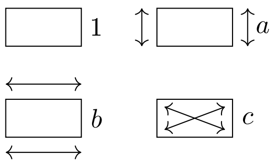
What are the symmetries of this?
Bijection $f : S \to S$ preserving the right G-action. eg. $f(sg) = f(s)g$
Need to check:

1. Left G-action of G preserves the right G-action
2. Anything that preserves the right G-action is given by left multiplication of an element of G

Check (1): For $g \in G$ need $(gs)h = g(sh)$, follows by commutativity
Note: left G-action does not preserve right G-action: $g(hs) \neq h(gs)$ in general

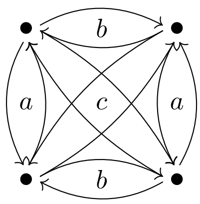
Check (2): Suppose $f : S \to S$ preserves the right G-action, $f(sh) = f(s)h$ for all $h \in G$. Need to find $g \in G$ such that $f(s) = gs$. Take $s = 1$, $f(1) = g1 = g$ so $g = f(1)$. If $g = f(1)$, then $f(s) = gs$ since $gs = (f(1))s = f(1s) = f(s)$.
So we have G = symmetries of (Set G + right G action)

Example 1.1.5. G=symmetries of rectange, set $S = G$



	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

We get the graph:



Cayley graph: Point for each $g \in G$ Draw a line from g to h with $gf = h$.

Goal of Group theory

1. Classify all groups
   - Hard but can do special cases: Groups of order 60, finite subgroups of rotations in $\mathbb{R}^3$, all finite simple groups, symmetries of crystals
2. Given a group G, classify all ways G can act on something (called a representation of G)
   - Permutation representation : G acts on a set S
   - Linear representation : G acts on a vector space

Example 1.1.6. Poncaire group = symmetries of space time
elementary particle: space of states = vector space acted on by G = linear group of G

1.1.2 Review of homomorphisms, isomorphims

Definition 1.1.7. A homomorphism is a map $f : G \to H$ that preserves structure
eg. $f(gh) = f(g)f(h)$, $f(1) = 1$, $f(g^{-1}) = f(g)^{-1}$

Note: last two properties can be derived from the first.

Example 1.1.8. $\exp(x) = e^x : (\mathbb{R}, +) \to (\mathbb{R}, \times)$
$\exp(x + y) = \exp(x)\exp(y)$, $\exp(0) = 1$, $\exp(-x) = \exp(x)^{-1}$

Definition 1.1.9. The kernel of a homomorphism f is the set of elements with image the identity.

Example 1.1.10. $\mathbb{R} \to$ rotation is the plane by $\theta \mapsto$ rotation by angle θ.
nontrivial kernel : multiples of 2π.
We get the short exact sequence: $0 \to 2\pi\mathbb{Z} \to \mathbb{R} \to \text{rotations} \to 0$

Definition 1.1.11. A sequence of homomorphisms $A \to B \to C$ is exact if Image $A \to B$ = Kernel $B \to C$

$0 \to A \to B$ means $A \to B$ is injective
$A \to B \to 0$ means $A \to B$ is surjective

Definition 1.1.12. $f : A \to B$ is an isomorphim if it is a homomorphism with an inverse. We say A, B are isomorphic. "basically the same"

Example 1.1.13. $2\pi\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

Example 1.1.14. $\mathbb{Z}/4\mathbb{Z}$, integers mod 4 with addition: $\{0, 1, 2, 3\}$ and $(\mathbb{Z}/5\mathbb{Z})^\times$, under multiplcation: $\{1, 2, 3, 4\}$ are isomorphic.
We map $0 \to 1 = 2^0$, $1 \to 2 = 2^1$, $2 \to 4 = 2^2$, $3 \to 3 = 2^3$ eg. $x \mapsto 2^x$

1.1.3 Classify all finite groups up to isomorphim

Definition 1.1.15. The order of a group G = number of elements in G

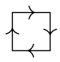
Order 1: $e \times e = e$ 1 group - trivial group
Order 2: 1 group - e, f with $f^2 = e \cong \mathbb{Z}/2\mathbb{Z}$
Order p for p prime: only one group $\mathbb{Z}/p\mathbb{Z}$ (integers modulo p)

Definition 1.1.16. For $g \in G$ the order of g is the smallest $n \geqslant 1$ with $g^n = 1$

Theorem 1.1.17 (Lagrange's Theorem)**.** If $g \in G$, the roder of g divides the order of G.

Example 1.1.18. Suppose $|G| = p$, (p prime). Pick $g \in G$ with $g \neq e$. Order of g divides $|G| = p$ so is either 1 or p. Can't be one since $g \neq e$. So elemenets of G $1, g, \ldots, g^{p-1}$ are all distinct since $g^p = 1$, $g^x \neq 1$ for $0 \leqslant x < p$ and if $g^i = g^j, g^{i-j} = 1$. Thus, these must be all elements of G.

Order 4:

- Ex : $\mathbb{Z}/4\mathbb{Z}$, symmetries of rectangle, $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$, symmetries of 
- only 2 groups of order 4

1.2 August 30

1.2.1 Langrange's Theorem

Order 4: $\mathbb{Z}/4\mathbb{Z}$, symmetries of rectangle
How to show not isomorphic?
Find some property (preserved by isomorphism) that one group has but the other does not.

Property: Order of elements

- in $\mathbb{Z}/4\mathbb{Z}$, 0, 1, 2, 3 have orders 1, 4, 2, 4 respectively
- all nontrivial elements of the group of symmetries of the rectangle have order 2

Note: counting elements of each order works for small gorups but 2 groups of order 16 with same number of elements of each order

Classification: By Lagrange's theorem, each element has order 1, 2, or 4

1. Have an element of order 4: g, group $= \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$
   In general, if a group of n elements has an element of order n, it is $\cong \mathbb{Z}/4\mathbb{Z}$
2. All elements have order 1 or 2.
   Suppose G is finite and has this property. Then G commutes since $(gh)^2 = ghgh = 1 = g^2g^2$ so $gh = hg$.
   Note: only true for prime 2, there is a group of order 27 such that all elements have order 1 or 3 but is not commutative
   Write group operation as $+$. G is a vector space over $\mathbb{F}_2$ (field of 2 elements). So $G \cong \mathbb{F}_2^k$ for osme set $|G| = 2^k$. We get 1 group of order 4 with all elements of order 1 or 2.

Group of order 4 is product of 2 groups, $\mathbb{F}_2^2 = \mathbb{F}_2 \oplus \mathbb{F}_2$.
Suppose G, H are gorups, $G \times H$ is a gorup under operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2)$

Example 1.2.1. $\mathbb{C}^\times \cong \mathbb{R}_{\geqslant 0} \times S^1$, $z = |z| \cdot e^{i\theta}$

Chinese Remainder Theorem: (m, n) coprime, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
We have maps $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $g : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. This gives $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. If $(m, n) = 1$, then the map is injecitve since if $h(k) = 0$, $k \equiv 0 \mod m, \mod n$

Infinite Products: $G_1 \times G_2 \times G_3 \times \cdots$, set of all elements $(g_1, g_2, g_3, \ldots,)$
Infinite Sums: Like infinite products but all but finitely many of g_1 are 1.

Example 1.2.2. Roots of $1 = e^{2\pi q}$, $q \in \mathbb{Q}$.
Infinite sum $G_2 + G_3 + G_5 + G_7 + G_11 + \cdots$ $(G_p =$ roots of order p^n for some $n \geqslant 1)$

Symmetry of Platonic Solids

Faces	Name	Rotations	Rotations + Reflections		
4	tetrahedron	$12 = 4 \times 3$	24	$\to$ not a product	
6	hexahedron (cube)	$24 = 6 \times 4$	48	product $\mathbb{Z}/2\mathbb{Z} \times$ rotations	All except tetrahedron have
8	octahedron	$24 = 8 \times 3$	48		
12	dodecahedron	$60 = 12 \times 5$	120		
20	icosahedron	$60 = 20 \times 3$	120		

symmetry $\begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$ fo reflections in $\mathbb{R}^3$, so it commutes with everything

For the tetrahedron, we have $\begin{pmatrix} -1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$

Order 5: $\mathbb{Z}/5\mathbb{Z}$

Exercise 1.2.3. Find a graph as small as possible with symmetries $\mathbb{Z}/5\mathbb{Z}$

Order 6: 3 obvious examples: $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, symmetries of the triangle

- $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
- group of symmetries of the triange is not abelian
  Permutation Notation: $(5\,2\,1\,3)$ = function sending $5 \to 2$, $2 \to 1$, $1 \to 3$, $3 \to 5$
  (Insert Figure)
  $(1\,2)(2\,3) = (1\,2\,3)$ but $(2\,3)(1\,2) = (1\,3\,2)$

Definition 1.2.4. A subgroup of a group G, is a subset closed under group operations.

Theorem 1.2.5 (Lagrange's Theorem)**.** If H is a subgroup of G, $|H|$ divides $|G|$.

Special Case: If H = powers of g, $1, g, g^2, \ldots, g^{n-1}$, $|H| = |g|$

Construction of subgorups: Pick a set S acted on by G, pick $s \in S$.
H: elements g with $gs = s$ (elements fixing s). Then H is a subgroup.
Lagrange (Converse to Cayley's Thm): If H is a subgroup of G we can find a set acted on by G, such that H=elements fixing $s \in S$.

Given a gorup G, subgroup H. We want to construct: a set S acted on by G.
Consider G=symmetries of triangle, $H = \{(1)(2)(3), (2\,3)\}$ fixing 1.
How do we write 1, 2, 3 in terms of G, H?
Left cosets of H: $1 \leftrightarrow$ elements g with $g(1) = 1$ (H), $2 \leftrightarrow$ elements g with $g(1) = 2$ ($(1\,2)H$), $3 \leftrightarrow$ elements g with $g(1) = 3$ ($(1\,3)H$)

Left cosets of H are sets of the from aH (some fixed $a \in G$).
Define $g_1 \approx g_2$ if $g_1 = g_2 h$ for some $h \in H$. This is an equivalence relation:
Reflexivity: $g_1 \approx g_1$ group identity, 1
Symmetry: $g_1 \approx g_2 \to g_2 \approx g_1$ group inverses, h^{-1}
Transitivity: $g_1 \approx g_2, g_2 \approx g_3 \to g_1 \approx g_3$ group operation, $h_1 h_2$
G = disjoint union of cosets (equivalence classes of $\approx$) and any two cosets have the same same $|H|$ since we have a bijection $H \to aH$ byb $h \mapsto ah$ with inverse $h \mapsto a^{-1}h$.
So $G = \#$ cosets $\times$ size of cosets $= \#$ elements of S $\times$ |subgroup of elements fixing s|
Note: We assume S is transisitve - if $s_1, s_2 \in S$. $g(s_1) = s_2$ for some g

Rotations of a dodecahedron: 12 (faces) $\times$ 5 = 20 (vertices) $\times$ 3 = 30 (edges) $\times$ 2 = 60

Conways Group: has order 8315553613086720000
Acting on Frames: # 8252375 Group fixing each frame: 1002795171840

Special Cases of Lagrange:

- Fermat: $a^p \equiv a \mod p$ (p prime), $a^{p-1} \equiv 1 \mod p$ $(a, p) = 1$
  Group $(\mathbb{Z}/p\mathbb{Z})^\times$ integers modulo p under $\times$ has order $p - 1$.
  Lagrange: order of a divides $p - 1$ so $a^{p-1} \equiv 1$
- Euler: $a^{\varphi(m)} \equiv 1 \mod n$ $(a, m) = 1$
  $(\mathbb{Z}/m\mathbb{Z})^\times$= group of elements coprime to m, mod m, order $= \varphi(m)$

$m = 8$: $\varphi(m) = 4$, $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. Euler $a^4 \equiv 1 \mod 8$ (a odd) but we see $a^2 \equiv 1 \mod 8$

Right Cosets: $Ha \leftrightarrow$ elements of a set acted on, on the right by G. $S \times G \to S$
Are left cosets the same as right cosets? sometimes

Example 1.2.6. Take G = symmetries of triangle. $H = \{1, (2\,3)\}$. Find the left, right costs of H in G.
Left: $H = \{1(2\,3)\}, (3\,1)H = \{(3\,1), (3\,2\,1)\}, (1\,2)H = \{(1\,2), (1\,2\,3)\}$
Right: $H = \{1(2\,3)\}, (3\,1)H = \{(3\,1), (1\,2\,3)\}, (1\,2)H = \{(1\,2), (3\,2\,1)\}$
so left cosets $\neq$ right cosets

Definition 1.2.7. Index of H in G, $[G : H]$= # cosets of H in G.

Left or right cosets? $[G : H][H] = |G|$ when G finite so # left cosets = # right cosets.
In gernal, right cosets → left cosets by $Ha \mapsto a^{-1}H$ so # left cosets = # right cosets

1.2.2 Normal Subgroups

G/H = set of left coset of G. Is G/H a group?
How to definte $(g_1H) \times (g_2H)$? g_1g_2H
Problem: not well defined - suppose we have g_1, g_2, g_1h_1, g_2h_2. Want $g_1g_2H = g_1h_1g_2h_2H$
Is $h_1g_2 = g_2(h \in H)$? not in general
Want: $ghg^{-1} \in H$ for all $g \in G$. If this holds, then we can turn G/H into a group.

Definition 1.2.8. If H satisfies the above property, H is called a normal subgroup of G.

Example 1.2.9. G = symmetries of triangle. $H = \{(2\,3), 1\}$. Is H normal?
$(1\,2)(2\,3)(1\,2)^{-1} = (1\,3) \notin H$ so H is not normal

What about $H = \{1, (1\,2\,3), (1\,3\,2)\}$. Is H normal?
H has index 2 in G. $[G : H] = \frac{|G|}{|H|} = 2$. We claim any subset of order 2 is normal.
There are only 2 left cosets: H, things not in H. Similarly for right cosets. So right cosets = left cosets. So H is normal.
Classifying Groups of Order 6

- orders of elements 1, 2, 3, 6
- If element of order 6, group must be cyclic
- Want element of order 3

Lagrange: order of element divides order of group
Converse: If n divides $|G|$, does G have a subgroup of order n?
No: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no element of order 4
Yes: if n is prime (Cauchy)
So G has elements a, b of order 2,3 and subset $(1, b, b^2)$ has order 2 so it is normal.

1.3 September 1

1.3.1 Semidirect Products

Groups of Order 6:
2 subgroups A, B of order 2,3 $\quad |A| \cdot |B| = |G|$, $A \cap B = \{e\}$

In general, suppose that for a group G, subgroups A, B

1. $|G| = |A| \cdot |B|$
2. $A \cap B = \{e\}$

Want to reconstruct G from A, B
$G = AB = \{ab \,|\, a \in A, b \in B\}$, # pairs $(a, b) = |G|$

If $a_1b_1 = a_2b_2$, $a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{e\}$ so $a_1 = a_2, b_1 = b_2$
Every element of G can be written uniquely as a product of $a \in A$, $b \in B$

Problem: What is $a_1b_1 \cdot a_2b_2$? $\quad = a_3b_3$
Easy case: $ab = ba$ for all $a \in A$, $b \in B$ $\quad (a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2)$
We can view G as the product of $A, B \to G = A \times B$
Slightly less easy case: A is a normal subgroup of G. We get an action of the group B on the group A.
Define the action of B on A by $b(a) = bab^{-1} \in A$ (A normal)
This determines the product on G. $(a_1b_1)(a_2b_2) = a_1(b_1a_2b^{-1})b_1b_2 = \underbrace{a_1b_1(a_2)}_{\in A} \times \underbrace{b_1b_2}_{\in B}$.

Suppose given groups A, B action of V on A. We construct the semidirect product of A and B, $A \rtimes B$ on the set $A \times B$ with the product given by : $(a_1, b_1)(a_2, b_2) = (a_1b_1(a_2), b_1b_2)$. We can check this is a group.

Order 6
So $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ defined by the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z}$.
$\mathrm{Sym}(\mathbb{Z}/3\mathbb{Z})$: either $f(1) = 1$ or $f(1) = 2$ so only two possible homomorphisms $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Sym}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$: identity and trivial homomorphisms
So groups of order 6:

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ trivial action $\cong \mathbb{Z}/6\mathbb{Z}$
- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ nontrivial action $\cong S_3$

1.3.2 Cauchy's Theorem

Theorem 1.3.1 (Cauchy's Theorem)**.** If $p \mid |G|$ (p prime), G has an element of order p.

Proof. We use induction on the size of the group: can assume true for any peroper subgroups and quotient groups
G abelian: pick $g \in G$. If $p| \, |g|$, g has order pn so g^n has order p.
If $p \nmid |g|$, look at $G/\langle g\rangle$. $\langle g\rangle$ normal since G is ableian, p divides $|G/\langle g\rangle|$. Pick $h \in G/\langle g\rangle$, order divisible by p. Lift h_1 in G. Then $p| \, |h_1$.

Standard Error: Can't always lift h to element of the same order
$G \cong \mathbb{Z}/4\mathbb{Z}$, $g = 2$. $G/\langle g\rangle$ has order 2 so take nontrivial element. Its lift does not have order 2 in G

Definition 1.3.2. The center of G is the elements that commute with all elements of G.

Lemma 1.3.3. Suppose G is nonotrivial, all proper subgroups have index divisible by p. Then the center of G is divisible by p.

Proof. Look at left action of G on itself by conjugation. G = union of orbuts where a, b in the same orbit if there is some g such that $g(a) = b$. $|G| = \sum$(size of orbits)
Size of orbit = $|G|$/subgroup of elements fixing a point. Either 1 or divisble by p so

> $G = \underbrace{1+1+1}_{\text{size 1}}+\cdots+\underbrace{pn_1+pn_2}_{\text{size }>1}+\cdots$. Since G divisible by p # orbits with one element is. Theorem follows since Center of G = elements with orbit of size 1.

> **Proof** (Cauchy's Theorem (Cont))**.** Case 1: Some proper subgorup has order dvisible by p.
> Such a subgroup has an element of order divisble by p by induction.
> Casse 2: All proper subgroups have index divisible by p. By lemma, center of G has order divisble by p
> Center of G is abelian so it has an element of order p.

Order 7: $\mathbb{Z}/7\mathbb{Z}$

Order 8: Obvious examples: Producst $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z}$, symmetries of a square (D_8) - dihedral group.
Orders of elements: $1, 2, 4, 8$

- If element has order 8, group is cylic
- If all elements have order 1 or 2, group is vector field over $\mathbb{F}^2$ so is $(\mathbb{Z}/2\mathbb{Z})^2$

So can assume G has an element a, of order 4. $a^4 = 1$. Subgroup $A = \{1, a, a^2, a^3\}$ has index 2 so is normal.
Quotient group has order 2 so $\cong \mathbb{Z}/2\mathbb{Z}$
We have an exact sequence $1 \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$

Problem: Given $1 \to A \to G \to B \to 1$ How to construct G form A, B?
Possibilities: $G = A \times B$, or $A \rtimes B$, not always the case:

- $1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$ not a semidirect product
- $1 \to \mathbb{Z}/3\mathbb{Z} \to S_3 \to \mathbb{Z}/2\mathbb{Z} \to 1$ $S_3 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

We get an action of B on A by conjugation so considering $1 \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$ we can take the nontrivial element b of $\mathbb{Z}/2\mathbb{Z}$. Cant say $b^2 = 1$, but $b^2 \in A$. Also B acts on A by conjugation.
So we have $\mathbb{Z}/4\mathbb{Z} = \{1.a, a^2, a^3\}$ $a \mapsto bab^{-1}$: $a \mapsto a$ or $a \mapsto a^{-1}$
Possibilities:

	$bab^{-1} = a$	$bab^{-1} = a^{-1}$
$b^2 = 1$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	D_8
$b^2 = a$ $b^2 = a^3$	$\mathbb{Z}/8\mathbb{Z}$ $(a = 1, b = 2)$	Impossible
$b^2 = a^2$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	Quaternions

Semidirect Products
$a = b^2$, $ab = ba \to a^2 = 1$

Quaternion group: generated by a, b with $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^{-1}$
Does it exst? Yes: have be viewed in $M_2(\mathbb{C})$- $a = \begin{pmatrix} i & \\ & -1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
Usually denote elements: $I = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}$, $J = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, $K = IJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$
Quaternions $Q_8 = \{i, I, J, J, -1, -I, -J, -K\}$ satisfying $I^2 = j^2 = K^2 = 1$, $IJ = K$, $JK = 1$, $KI = J$
Hamilton's Quaternions(H) = all numbers $a + bi + cj + dk$ a, b, c, d real
Nonzero elements of H form a gorup. Problem: Show inverses exist.
$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^+d^2 > 0$ so
$(a + bI + cj + dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$
Can also look at $S^3 \subset H = \{a + bi + cj + dk \,|\, a^2 + b^2 + c^2 = d^2 = 1\}$
For $z = a + bi + cj + dK$, $\overline{z} = a - bi - cj - dk$ let $z\overline{z} = N(z)$

We see $N(z_1z_2) = N(z_1)N(z_2)$ so if $N(z) = 1$ closed under $\times$ so is a group.

Only spheres that are a group are S^0, S^1, S^3. Elements of $\mathbb{R}, \mathbb{C}, H$ with absolute value 1.

Note: $Q_8 \subseteq S^3$

1.3.3 Burnside's Lemma

Problem: How many ways to arrange 8 rooks on a chess board so that no 2 attack each other?
8 ways for first row, 7 for second, ..., so $8! = 40320$ total
Suppose we want to count them up to symmetry:

- For 3×3: (Insert Figure)
  can only have 2

Approximate number $= \frac{\text{total \# of elements}}{\text{order of group}} = \frac{8!}{8} = 7! = 5050$

General problem: Suppose we have a group G acting on a set S. How many orbits? $\geqslant \frac{|S|}{|G|}$
Answer:

Lemma 1.3.4 (Burnside's Lemma)**.** # of orbits = average number of fixed points of $g \in G$, eg. $s \in S$ with $g(s) = s$

Proof. Count number of pairs $(g, s) \in G \times S$ with $g(s) = s$ in 2 ways:

1. Sum over G: $\sum_{g \in G}$ (# fixed by g)
2. Sum over S: Each orbit contributes (size of orbit) $\times$ (# of elements fixing a point) $= |G|$
   so sum $= |G| \times$ # of orbits

So # of orbits $= \frac{1}{|G|} \sum_g$ # fixed points = avg # fixed points

1.4 September 6

1.4.1 Burnside's Lemma

Example 1.4.1. Find the number of ways to arrange 8 nonattacking rooks on a chessboard up to symmetry.
Recall - # of orbits of a set = average number of fixed points $= \frac{1}{|G|} \sum_{g \in G}$ # fixed points of g.
G = dihedral group D_8, acting on $8! = 40320$ ways to arrange 8 rooks
Elements of D_8:

- Trivial (Insert Figure): $8! = 40320$
- 180° rotation (Insert Figure) : 8 options for 1rst, 6 options for 2cnd, ... so $8 \times 6 \times 4 \times 2$
- 90° rotation (Insert Figure): 6 options for 1rst, 2 options for 2cnd so 6×2

2 elements g_1, g_2 are called conjugate if $g_1 = gg_2g^{-1}$ for some g (Formalizes notion of "looks the same")
$g_1 =$(Insert Figure) $g_2 =$(Insert Figure) $g =$ (Insert Figure) exchanging g_1, g_2.
If two elements are conjugate then they have the same number of fixed points.
$g_1(s) = s \to g_2(gs) = gg_1g^{-1}gs = gs$

- (Insert Figure): conjugate with 90° rotation so 6×2
- (Insert Figure): conjugate and have 0 since rotates rook to the same column/row
- (Insert Figure): conjugate. $C_n = \#$ ways to place rooks on $n \times n$ chessboard invariant under transformation. $c_0 = 1, c_1 = 1$.
  Case 1 : (Insert Figure) Case 2: (Insert Figure)
  so $c_n = c_{n-1} + (n-1)c_{n-2}$ and $c_n = 1, 1, 2, 4, 10, 26, 76, 232, 764$

So # of ways to place rooks $= \frac{1}{8}(1 \times 8! + 1 \times 384 + 2 \times 12 + 2 \times 0 + 2 \times 764) = 5282$
Slighly more than original guess $\frac{40320}{8} = 5040$

Example 1.4.2. Find the number of ways to color a cube with n different colors up to symmetry.

1.4.2 Groups of order p^2

Order 9: Obvious examples $= \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Classify all groups of order p^2 (p prime): only ex are $\mathbb{Z}/p^2\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^2$
(1): Every group of order p^n (p prime, $n > 0$) has nontrivial order

Proof. Recall, if all proper subgroups have index divisible by p, $p \mid |G|$ then G has nontrivial center. So if $|G| = p^n$, $n > 0$, we see G has nontrivial center. □

Implies that if $|G| = p^n$, G is nilpotent. ie. repeatedly modding out by the center gives you the trivial group.
$G_0 = G$, $G_1 = G_0/Z(G_0)$, $G_2 = G_1/Z(G_1)$, ... If G_n is trivial for some n, G is caleld nilpotent.
This gives an exact sequence: $1 \to Z(G_i) \to G_i \to G_{i+1} \to 1$
Note: A group may still have nontrivial center even after modding out by the original center: $G = D_8$, $G/Z(G) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
S_3 (order 6) is not nilpotent

(2): If $G/Z(G)$ is cyclic then G is abelian.

Proof. Consider $1 \to Z(G) \to G/Z(G) \to 1$. $Z/(G)$ is powers of g_1, lift g_1 to g in G.
Every element in G is of the form zg^n ($z \in$ center) so all commute $z_1 g^{n_1}, z_2 g^{n_2}$:
z_1 commutes with $z_2 g^2 n$, g^{n_1} commutes with z_2, and g^{n_1} commutes with g^{n_2} □

(3): Every group of order p^2 is abelian.
Note: not true for p^3, consider D_8, Q_8 of order 2^3

Proof. Center is nontrivial so has order $\geqslant p$. $G/Z(G)$ has order 1 or p so it is cyclic so G is abelian. □

(4): Every group of order p^2 is $(\mathbb{Z}/p^2\mathbb{Z})$ or $(\mathbb{Z}/p\mathbb{Z})^2$

Proof. Case 1 : elements of order $p^2 \to G$ is cyclic $\cong \mathbb{Z}/p^2\mathbb{Z}$
Case 2: all elements have order p or $1 + G$ abelian. G is really a vector field over $\mathbb{F}_p$ the field with p elements so $G = \mathbb{F}_p \oplus \mathbb{F}_p$. □

1.4.3 Dihedral Groups

Order 10: $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $D_{10} = (\mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$

Groups of Order $2p$: G has a subgroup of order p, index 2 so is normal. G has a subgroup of order 2 so $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, determined by action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/p\mathbb{Z}$.
Symmetries of $\mathbb{Z}/p\mathbb{Z}$: map generator $1 \to$ elment of order p. $n \mapsto na\ p\ \ |a$
Symmetries $= (\mathbb{Z}/p\mathbb{Z})^{\times}$ nonzero integers mod p under $\times$. Only elements of order 2 are $\pm a \mod p$
$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}2\mathbb{Z}$ (trivial action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/p\mathbb{Z}$)
$G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}2\mathbb{Z}$ ($\mathbb{Z}/2\mathbb{Z}$ acting by -1 on $\mathbb{Z}/p\mathbb{Z}$) = dihedral group.

Dihedral Groups: symmetries of a regular n-gon ($n \geqslant 3$). Order $2n$
(Insert Figure)

What is the center of D_{2n}? ($n \geqslant 2$)? Order 2 if even, order 1 if odd.

Why does D_{12} split as a product?
(Insert Figure) $D_12 = D_6 \times \mathbb{Z}/2\mathbb{Z}$ = symmetries of triangels $\times$ 180° rotation commutes with elements and flips the two triangles
D_{10} (Insert Figure) Problem: 180° does not flip two squares.
D_{2n} can be split $D_{2n} \times \mathbb{Z}/2\mathbb{Z}$ for $D_4, D_{12}, D_{20}, D_{28}$ ($\equiv 2 \mod 4$)

Involutions in dihedral groups (elements of order 2)
D_{2n} (Insert Figure)

Reflection Groups (generated by relations)
(Insert Figure) Suppose g and h are relations. If $g^2 = 1$, $h^2 = 1$, $(gh)^n = 1$

- Fid property of all finite groups that doesn't hold for all infinite groups, in the language of groups.

Property: If g, h are involutions, either g, h are conjugates or some involution commutes with g, h
$g^2 = 1$, $h^2 = 1$, $(gh)^n = 1$ for some n (since group finite)
n even: D_{2n} has nontrivoal element in center
n odd: All involutions commute
Fails for ∞ dihedral group $g^2 = 1$, $h^2 = 1$ (Insert Figure)
Order 12: $\mathbb{Z}/12\mathbb{Z}$, products - $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $S_3 \times \mathbb{Z}/2\mathbb{Z}$, rotations of tetrahedrons, semidirect products- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$.

Binary Dihedral: S^3(= unit quaternions) is a group acting on $\mathbb{R}^3 = bi + cj + dk$ - rotations in $\mathbb{R}^3$
$1 \to \pm 1 \to S^3 \to$ rotaitons on $\mathbb{R}^3 \to 1$ where ± 1 act trivially on $\mathbb{R}^3$
$1 \to \pm 1 \to \hat{G} \to G =$ finite reflecction group. Ex: group over D_{2n}
Binary dihedral groups of order $4n$ so binary dihedral group of order 12. (Q_8 binary dihedral group of order 8)
5 groups of order 12.

1.5 September 8

1.5.1 Sylow Theorems

Order 12: $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $S_3 \times \mathbb{Z}/2\mathbb{Z}$, A_4, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

Sylow Theorems:

- Lagrange: if $H \subseteq G$, $|H| \mid |G|$
- If $m \mid |G|$ can we find a subgroup of order G?
  No: A_4=reflections of tetrahedron has no subgroup of order 6

Theorem 1.5.1 (Sylow's Theorems). 1. If $p^n \mid |G|$ (p prime) then G has a subgroup of order p^n if n is maximal, called p-Sylow subgroup.

2. Number is $1 \mod p$, divides $|G|$
3. All p-sylow subgroup are conjugate (so all isomorphic)
4. Any p-subgroup is contained in some sylow p-subgroup.

Example 1.5.2. $G = D_8$, contains two non-conjugate elements of order 2 - (Insert Figure)

Example 1.5.3. $G = D_8$, has nonisomorphic subgroups of order 4
(Insert Figure)

Proof. 1. Existence. We proceed by induction on the order of the group.
Case 1: G has some proper subgroup H,index not divisible by p.

- Pick sylow p-subgroup of H. This is a sylow p-subgroup of G.

Case 2: All Sylow p-subgroups have index divisble by $p \to$ center if G has order divisible by p.

- pick $g \in$ center, $g^p = 1$. Look at $G/\langle g\rangle$. Pick p-sylow subgroup. Inverse image in G is a sylow p-subgroup.

2. Number of Sylow subroups is $1 \mod p$
   Key idea: look at action of Sylow p-subgroup S on set of sylow p-subgroups by conjugation
   All orbits have size power of p. Orbit $\{S\}$ has size 1. No other orbits of size 1. if $\{T\}$ orbit of size 1, then S normalizes T so ST of order p^m, $m > n$. impossible.
   1 orbit of size 1, all other orbits have size p^k, $k > 0$. Divisible by p so total is $1 \mod p$
3. All Sylow p-subgroups are conjugate
   Suppose not, then if S is a p-sylow subgroup, number of conjugates is divisble by $p - 1$. Suppose T is a non-conjugate p-subgroup and let T act on the set of p-sylow subgroups conjugate to S. T can have no fixed points so the total number of p-sylow subgroups conjugate to S is divisble by p, contradiction.
4. Numberof Sylow p-subgroups divides the order of G
   Look at action of G on sylow p-subgroups. Transitive so # subgroups $= \frac{|G|}{|\text{subgroup fixing1}|}$ which divides G.
5. Any subgroup with order power of $p \subseteq$ some sylow p-subgroup

Apply to groups of order $12 = 2^2 \times 3$
We know that G has subgroups of order 3 and 4.
Case 1: subgroup of order 3 is normal.

- Give G semiproduct $(\mathbb{Z}/3\mathbb{Z}) \rtimes$ (order 4 group)
  4 cases:

	Action trivial	Nontrivial
$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	binary dihedral
$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$	$S_3 \times \mathbb{Z}/2\mathbb{Z}$

  Case 2: Sylow 3 subgroups not normal
  # subgroups - divides 12, 1 mod 3, not 1 $\to = 4$, call them S_1, S_2, S_3, S_4. $S_i \cap S_j = \{e\}$ so we have 8 elements of order 3, 1 element of order 1, 3 "mystery" elements.
  G has 2-sylow subgroups of order 4, at most one so must be normal. So $G =$ (group of order 4) $\rtimes \mathbb{Z}/2\mathbb{Z}$, only nontrivial action on: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong$ relfection of tetrahedron.

Example 1.5.4. Apply to groups of order 56.

Application: Nilpotent Groups
Following are equivalent:

1. Group is nilpotnent (center >1 , $G/$center is nilpotent or $|G| = 1$)
2. Any proper subgroup H has $N(H)$ strictly bigger than H.
3. ALl Sylow subgroups are normal
4. G is product of groups of prime power order.

(1) $\to$ (2): Suppose H is a subgroup.
Case 1: H does not contain $Z(G)$. $Z(G) \subseteq N(H)$.
Case 2: H contains $Z(G)$, look at $H/Z(G) \subseteq G/Z(G)$

(2) $\to$ (3): If S is a sylow p-subgroup of G. Then $N(S)$ is its own normalizer. $e \subseteq S \subseteq N(S) \subseteq G$. Suppose $g \in G$ normalizes $N(S)$ g takes S to a sylow p-subgroup of $N(S)$. This subgroup is conjugate to S in $N(S)$ so $gSg^{-1} = hSh^{-1}$ for $h \in N(S)$ so gh^{-1} normalizes S so $gh^{-1} \in N(S)$, since $h \in N(S)$, $g \in N(S)$.
Now, if $N(S)$ proper subgroup then $N(N(S)) > N(S)$ so must have $N(S) = G$ so there is only one sylow subgroup.

(3) $\to$ (4): Main step - members of different sylow subgroups comute.
S is a sylow p-subgroup, T is a sylow q-subgroup with $p \neq q$, want $st = ts$ for $s \in S$, $t \in T$
Follows from: If A, B normal subsets of G, and $A \cap B = \{e\}$ the elements of A commute with the elements of B. Look at $aba^{-1}b^{-1}$, commutator of a, b ($=1 \leftrightarrow a, b$ commute). $aba^{-1} \in B$ so $aba^{-1}b^{-1} \in B$ and $ba^{-1}b^{-1} \in A$ so $aba^{-1}b^{-1} \in A$ so $aba^{-1}b^{-1} = e$

(4) $\to$ (1): Follows since 1. p-groups are nilpotent, 2. product of nilpotent groups is nilpotent

Order 15: One group is $\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Consider $p \neq q$, $p > q$. G has sylow p-subgroup, number is $1 \mod p$, divides pq, $q < p$ so only possibility is 1. So since p is normal $G = \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.
How doe s$\mathbb{Z}/q\mathbb{Z}$ act on $\mathbb{Z}/p\mathbb{Z}$? $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times$ order $p-1$ so if q does not divides $p-1$ only action is trivial so only subgroup is cylic subgroup of order pq
If $q|p-1$, $\mathbb{Z}/q\mathbb{Z}$ can act nontrivially on $\mathbb{Z}/p\mathbb{Z}$. Essentially one action $(\mathbb{Z}/p\mathbb{Z})^\times$ elements of order q forms a cyclic subgroup of order q.
Exactly two groups of order pq.
Order 16: Complete List

- 5 abelian: $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, $(\mathbb{Z}/2\mathbb{Z})^4$
- 4 more, have subgroups of order $\mathbb{Z}/8\mathbb{Z}$: Generalized quaternion = binary dihedral, dihedral, groups generated by $a^8 = 1$ $b^2 = 1$, $bab^{-1} = a^3$ or a^5, if a^3 called semi-dihedral.
- Products: $D_8 \times \mathbb{Z}/2\mathbb{Z}$, $Q_8 \times \mathbb{Z}/2\mathbb{Z}$
- Semidirect Product: two of form $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$
  one of form: $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ (Pauli group)

1.5.2 Classification of Abelian Groups (finite)

All products of cylic-subgroups (not unique) eg. $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
Product is unique up to order either, $n_1, n_2, \ldots$ satisfying $n_1 | n_2 | n_3 \cdots$ or n_i prime powers.
eg. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} (2|6)$ or $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ $(2^2, 3$ prime powers)

1.6 September 13

1.6.1 Classificaiton of Finitely Generated Abelian Groups

Classify all finite abelian grousp G.

- Write group law as $+$
- pick finite number of generators $g_1, \ldots, g_n$ (every element in G is of the form $m_1 g_1 + \cdot + m_n g_n$ with $m_i \in \mathbb{Z}$)

Classificaiton still works for finitely generated abelian groups.
Relation: $a_1 g_1 + \cdots + a_n g_n 0$
Take some $a_{1,1} g_1 + \cdot + a_{1,n}, a_{2,1} + \cdots + a_{2,n}, \ldots$ generating all relations.
We get a matrix $\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ & & \vdots & \end{pmatrix}$
Change matrix:

1. Permute rows
2. Permute columns
3. Add a multiple of one row to another row. $\{R_1, R_2\} \equiv \{R_1, R_2 + nR_1\}$
4. Add a multiple of one column to another. $g_1, \ldots, g_n$ generators then $g_1 + ng_2, g_2, \ldots,$ also generators.

Do row, column operations to simplify matrix

- Arrage $a_{1,1}$ to be as small as possible (> 0). Possible unless all $a_{ij} = 0$
  $a_{1,1}$ divides $a_{1,2}$ since if $a_{1,2} = ka_{1,1} + r$ with $0 \leqslant r < a_{1,1}$, as $a_{1,1}$ is minimal , $r = 0$. Can meake $a_{1,2} = 0$.
  Similarly, we can make $a_{1,3}, a_{1,4}, \ldots, a_{2,1}, a_{2,2}, \ldots$ all 0 to get a matrix $\begin{pmatrix} a_{1,1} & 0 & \cdots & \cdot \\ 0 & a_{2,2} & a_{2,3} & \cdots \\ \vdots & a_{3,2} & \ddots & \\ \vdots & \vdots & & \end{pmatrix}$

We can repeat this with $a_{2,2}$ to get $\begin{pmatrix} a_{1,1} & & & 0 \\ & a_{2,2} & & \\ & & \ddots & \\ 0 & & & a_{n,n} \end{pmatrix}$ giving relations $a_{1,1}g_1 = 0$, $a_{2,2}g_2 = 0, \ldots$
so group is $\mathbb{Z}/a_{1,1}\mathbb{Z} \oplus \mathbb{Z}/a_{2,2}\mathbb{Z} \oplus \cdot \oplus \mathbb{Z}/a_{n,n}/\mathbb{Z}$ with $a_{1,1}|a_{2,2}|a_{3,3}| \ldots$
If $\mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z} \cong bZ/b_1\mathbb{Z} \oplus \mathbb{Z}/b_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/b_m\mathbb{Z}$ with $a_1|a_2|a_3|\cdots$ and $b_1|b_2|b_3|\cdot$ then $n = m$, $a_1 = b_1$, $a_2 = b_2, \ldots$
Key idea - look at the number of homomorphisms from G to $\mathbb{Z}/m\mathbb{Z}$

How many abelian groups of order p^n (p prime)?
$\mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \cdots$ $a_i = p^{k_i}$, $k_1 \leqslant k_2 \leqslant k_3 \leqslant \cdots$, $k_1 + k_2 + k_3 + \cdots = n$.

n	# partitions
0	1
1	1 1
2	2 $2, 1+1$
3	3 $3, 2+1, 1+1+1$
4	5 $4, 3+1, 2+2, 2+1+1, 1+1+11$
5	7 $5, 4+1, \ldots$

Order 18: Normal subgroup of order 3^2 so group is order 9 $\rtimes \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/9\mathbb{Z}$- 2 actions of $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^3$- 3 actions of $\mathbb{Z}/2\mathbb{Z}$ (thinking of this as a vector space over $\mathbb{Z}/3\mathbb{Z}$ consider linear transformations of order 2, $V = V^+ \oplus V^-$, egienspaces of ± 1, dimension of $V = 0, 1, 2$)
One of the groups $(\mathbb{Z}/3\mathbb{Z})^3$ is wreath product.
Suppose G, H aer groups. Take product of $|G|$ copies of H. $H^{|G|} = H \times H \times \cdots$, G acts on $H^{|G|}$ so we have the semidirect product of $H^{|G|} \rtimes G$
More generally, if G acts on Ω, can form $H^{|\Omega|} \rtimes G$

Example 1.6.1. $H = \mathbb{Z}/3\mathbb{Z}$, $G = \mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z} \to$ wreath product of order 18.
$H = \mathbb{Z}/2\mathbb{Z}$, $G = \mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z} = D_8$.

Example 1.6.2. 1. Symmetry of graphs (Insert Figure)

2. Sylow subgroups of symmetric groups
   Want to consider Sylow 2-subgroups of S_10. Highest power of 2 dividing $10! = \lfloor \frac{10}{8} \rfloor + \lfloor \frac{10}{4} \rfloor + \lfloor \frac{10}{2} \rfloor = 5 + 2 + 1 = 8$. (Insert Figure)

- Any group of order p^n is a subgroup of some $(\mathbb{Z}/p\mathbb{Z}) \wr (\mathbb{Z}/p\mathbb{Z}) \wr (\mathbb{Z}/p\mathbb{Z})$

Physics - Gauge Theories
G=gauge group. Symmeties = (continuous maps of spacetime $\to G$) $\rtimes$ (Automorphims of spacetime)
Order 20: $(\mathbb{Z}/5\mathbb{Z}) \rtimes$ (order 4)
5 possibilities: $\mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$, $D_{10} \times \mathbb{Z}/2\mathbb{Z} = D_{20}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (elements of order 2, binary tetrahedral), $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (Frobenius Group)

Frobenius Group is a group G acting on a set S transitively and faithfully such taht

1. If g fixed two points of S then g is the identity
2. S is not the regular action of G of a group on teh set.

Example 1.6.3. $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ "$ax + b$" group. Take F a field and consider all linear transformations $x \mapsto ax + b$, $x \in F$, $a \neq 0, b \in F$ = matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ $a \neq 0$
S_3 also Frobenius gorup, "$ax + b$" for $\mathbb{Z}/3\mathbb{Z}$
A_4 acts on 4 points also a Frobenius group.

Frobenius: If G is a Frobenius group then put $N=$ identity $\cup$ elements with no fixed point, then N is a normal subgroup of $G=$ Frobenius kernel
For A_4, the frobenious kernel is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
Thompson: N is nilpotent
Order 21: $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ is first non-abelain group of odd order.
Order 24: Look at Sylow 3-subgroups , $\mathbb{Z}/3\mathbb{Z}$, either 1 or 4
if 1: $\mathbb{Z}/4\mathbb{Z} \rtimes$ (order 8)
if 4: We get an action of G on 4 points (Sylow 3-subgroups) so we have a homomorphism $G \to S_4$. Kernel has order $1, 2, 3$ or 6. 6, 3 not possible since no normal subgroup of order 3 so 2 possibilities:

1. Kernel is 1, $G \cong S_4$ (no normal Sylow Subgroup)
2. $1 \to \mathbb{Z}/2\mathbb{Z} \to G \to$ Aut binary dihedral group

1.6.2 Symmetric Groups - S_n

Order is n! What are its conjugacy classes?
General element: $(1\,3\,5)(2\,4)(6\,8\,9)$ cycle shape = lengths of cycles in order.
2 elements of group aer conjugate $\leftrightarrow$ they have the same cycle shape
Problem: Given a, b, having the same cycle shape. Find g with $gag^{-1} = b$
eg. $a = (1\,3)(2\,5\,9)(4\,6\,8)(7), b = (5\,7)(1\,3\,6)(2\,4\,9)(8)$ can define g to map elements to corresponding element in other cycle eg. $1 \to 5, 3 \to 7, 2 \to 1, \ldots$
How many conjugacy classes of S_n? eg. How many cycle shapes?
$(n_1)(n_2)(n_3)\cdots\ \ 0 \leqslant n_1 \leqslant n_2 \leqslant n_3\ n_1 + n_2 + n_3 + \cdots = n$, number of partitions of n
What is the set of conjugates of the cycle shape $1^{k_1}2^{k_2}3^{k_3}\cdots\ \underbrace{1\cdots1}_{k_1}\cdot\underbrace{2\cdots2}_{k_2}\cdots$

is $|S_n/$ size of subgroup fixing one of the permutations
Find an element of S_n commuting with these, $S_{k_1}, 2^{k_2}S_{k_2}, 3^{k_3}S_{k_3}, \ldots$ so $\# = \frac{n_1}{k_1!2^{k_2}k_2!3^{k_3}k_3!\cdots}$
S_4:

4	$\frac{24}{4} = 6$
$3\ 1$	$\frac{24}{3\cdot 1} = 8$
2^2	$\frac{24}{2^2 2!} = 8$
$2\ 1^2$	$\frac{24}{2\cdot 1^3\cdot 2!} = 6$
1^4	$\frac{24}{1^4\cdot 4!} = 1$

1.7 September 15

1.7.1 Normal Subgroups of S_n

1. Trivial subgroup
2. S_n
3. Alternating group A_n of index 2.
   Look at $\Delta(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$. S_n acts on polynomials by permuting $x_1, \ldots, x_n$. Takes $\Delta \to \Delta$ or $-\Delta$. A_n=subgroup mapping Δ to Δ. Index 2 in S_n $(n > 1)$.
4. S_4 has a normal subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (weird exception).

No other normal subgroups.
Symmetries of Platonic Solids

		Rotations	All Symmetries
4	Tetrahedron	12-A_4	24-S_4
8, 6	Octrahedron , Cube (Dual)	24 - S_4	48-$S_4 \times \mathbb{Z}/2\mathbb{Z}$
20, 12	Icosahedron, Dodecahedron (Dual)	60 - A_5	120-60 $\times \mathbb{Z}/2\mathbb{Z}$

Here dual means faces of one can be identifies with the vertices of the other

$1 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to S_4 \to S_3 \to 1$
S_4- symmetries of octahedron, has 3 diagonals
S_3 - permutations of 4 diagonals

Definition 1.7.1. G is solvable if G is abelian or G has normal subgroup with $N, G/N$ solvable.

$1 \to N \to G \to G/N \to 1$
$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$ such that G_i normal in G_{i+1}, G_{i+1}/G_i abelian.
For S_4, $1 \underbrace{\subseteq}_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \underbrace{\subseteq}_{\mathbb{Z}/3\mathbb{Z}} A_4 \underbrace{\subseteq}_{\mathbb{Z}/2\mathbb{Z}} S_4 \to$ polynomial of degree 4 can be solvable with radicals.

Order 27$=3^3$, groups of order p^3

Example 1.7.2. Abelian - $\mathbb{Z}/p^3\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^3$
Non abelian - $p = 2$: $D_8 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}, Q_8$

p odd: $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, $\begin{pmatrix} 1 & & * & * \\ & 1 & & * \\ 0 & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$ in $\mathbb{Z}/p\mathbb{Z}$, all elements order p, nonabelian

$M_n(\mathbb{R}) : \exp(A) = I = A + \frac{A^2}{2!} + \cdots$

- Converges: Norm(A), $||A|| = \sup_v \frac{|A(v)|}{||v||}, v \in \mathbb{R}^n$. $||Av|| \leqslant ||A||\,||v||$
- Properties: $\exp(A + B) = \exp(A) + \exp(B)$ if $AB = BA$
- Can define $\log(1 + A) = A - A^2/2 + A^3/3 - \cdots$ defined for $||A|| < 1$

Define exp, og for matrices in $\mathbb{Z}/p\mathbb{Z}$

1. Some do not converge
2. terms of this sum are not even defined $\frac{A^p}{p!}, p! = 0$ in $\mathbb{Z}/p\mathbb{Z}$

1. Ok if A is nilpotent, $A^n = 0$, $1 + A + \frac{A^2}{2!} + \cdots + \frac{A^{n-1}}{(n-1)!}$
2. Of if, $A^n = 0$ $n < p$, $0!, 1!, \ldots, (p-1)!$ all nonzero mod p

So we can we can define $\exp(A)$ over $bZ/p\mathbb{Z}$ is $A^{p-1} = 0$

$A = \begin{pmatrix} 1 & & * & * \\ & 1 & & * \\ 0 & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$ strictly upper triangular $n \times n$ matrices over $\mathbb{Z}/p\mathbb{Z}$, $A^{n+1} = 0$ so if $n < p$ can define $\exp(A), \log(A)$

$G = \begin{pmatrix} 1 & & * & * \\ & 1 & & * \\ 0 & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$ matrices over $\mathbb{Z}/p\mathbb{Z}$. If $n < p$ all elements have order p.
Note: If all elements have order $2 \to G$ abelian but all elements order $3 \not\to G$ abelian
Groups of order p^3 are analogs of Heisenberg group Heisenberg group: Fuctions on $\mathbb{R}$. (1) translations $f(x) \to f(x+\lambda)$, (2) multiply by $e^{2\pi i x \mu}$ $f(x) \to f(x)e^{2\pi i x\mu}$
Order they are applied in matters: $f(x) \to f(x+\lambda) \to f(x+\lambda)e^{2\pi i x\mu}$ vs. $f(x) \to f(x)e^{2\pi i \mu x} \to f(x+\lambda)e^{2\pi i\mu(x+\lambda)}$. Differ by $e^{2\pi i \mu\lambda}$, forms circle group.
$1 \to S^1 \to$ Heisenberg $\to \mathbb{R} \times \mathbb{R} \to 1$
$p^3 : 1 \to \mathbb{Z}/p\mathbb{Z} \to$(order p^3) $\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to 1$
Order 2^5: 51 groups, 2^{10} : 49487365421 groups, $p^n :\sim p^{\frac{2}{27}n^2}$
Typical: $1 \to (\mathbb{Z}/p\mathbb{Z})^a \to G \to (\mathbb{Z}/p\mathbb{Z})^b \to 1$
Choose bases $u_1, \ldots, u_a$ and $v_1, \ldots, v_b$. $i < j$ $v_i v_j v_i^{-1} v_j^{-1}$ = something in $(\mathbb{Z}/p\mathbb{Z})^a$

Order 48: Binary Dihedral

Example 1.7.3. Prove all groups of order < 60 are simmple (tricky cases: 30, 48, 56)

A_5- first non solvable simple group.
Any finite group can be built out of simple groups: $1 \subseteq G_0 \subseteq G_1 \subseteq \cdots$ G_i normal in G_{i+1}, G_{i+1}/G_i simple.
Order 60: Rotations of Tetrahedron $\cong A_5$

Show A_5 is simple

Conjugacy Classes	Order	Number	
(1) Trivial element	1	1	
(2)	3	20	(Faces)
(3)	2	15	(Edges/2)
(4) 1/5 rev	5	12	(# vertices)
(5) 2/5 rev	5	12	(# vertices)

Warning: Conjugacy classes of A_5 not quite same as conjugacy classes of S_n
$(1\,2\,3\,4\,5)(2\,1\,3\,4\,5)$ conjugate in S_5 but not A_5
Let H be a normal subgroup of A_5

1. H union of conjugacy classes
2. So $H = 1+$ "subset" of $\{12, 12, 15, 20\}$
3. $|H|$ divides 60

So only optiosn are $|H| = 1$ or $|H| = 1 + 12 + 12 + 15 + 20 = 60$
So A_5, only normal subgroups of S_5 are $1, A_5, S_5$ since if H normal in S_5, $H \cap A_5 = A_5$ or 1. If A_5, $H = A_5$. If $1, |H| \leqslant 2, H = 1$.
A_n simple for $n \geqslant 5$ by induction on n. Idea: Consider $A_n \subseteq A_{n+1}$ $(n \geqslant 5)$. If H is normal in A_{n+1}, $H \cap N$ normal in A_n so $H \cap A_n = A_n$ or 1.

Order 120: How do we build a group out of $\mathbb{Z}/2\mathbb{Z}, A5$?
3 ways:

1. $A_5 \times \mathbb{Z}/2\mathbb{Z}$ symmetries of Icosahedron
2. S_5 normal A_5, quotient $\mathbb{Z}/2\mathbb{Z}$ $1 \to A_5 \to S_5 \to \mathbb{Z}/2\mathbb{Z} \to 1$
3. Binary icosahedral $1 \to \mathbb{Z}/2\mathbb{Z} \to \hat{A}_5 \to A_5 \to 1$

(1), (2) have center of order 2. (3) has one element of order 2.

Poncaire: Compact 3-manifold with trivial fundamental group is S^3
Poncaire Homotopy Sphere: S^3/(Binary Icosahedral). Fundamental group = binary icosahedral, H_1 aelianization of fundamental group = $\{1\}$

1.8 September 20

1.8.1 Categories

Example 1.8.1.

Objects	Morphisms
Groups: G, homomorphimss $G \xrightarrow{f} H$	
Sets: S, functions $S \xrightarrow{f} T$	
Topological spaces: X, continuous maps $X \xrightarrow{f} Y$	

Axioms

- For any two objects we have a set of morphisms $A \to B$ $\text{Mor}(A, B)$.
- Can compose morphisms: $A \to B, B \to C$, we get a morphism $A \to C$
- Identity morphism: $I_A : A \to A$ satisfying $f : A \to B$, $I_b f = f <\ f I_A = f$
- Function composition is associative

Example 1.8.2. Rings, varities, and differentiable manifolds

Example 1.8.3. A group. Object: only 1 object. Morphisms: elements of group. Composition is group product.

Example 1.8.4. A poset (partially order set). Set S with $\leqslant$. Category: objects = elements of S. Morphisms: morhpisms from A to B, 1- morphism if $A \leqslant B$, none if $A \nleqslant B$.

Basic Theme: Ignore structure of objects, define everything using morphisms.
epimorphisms: analogs of surjective maps. Normal definition of surjective uses internal structure of T.
$f : S \to T$ is an epimorphism if whenever 2 morphisms $T \underset{h}{\overset{g}{\rightrightarrows}} U$ if $gf = hf \to g = h$

Example 1.8.5. $f : S \to T$ (S, T sets) f surjective $\leftrightarrow$ f is an epimorphism

Warning: Sometimes epimorphism $\neq$ surjection

Example 1.8.6. Look at category of rings (morphisms = homomorphims)
$f : \mathbb{Z} \to \mathbb{Q}$ not surjective but is an epimorphism of rings.

Fawcett: In category of planar graphs 4 color theorem $\leftrightarrow$ epimorphisms are surjective.
Dual Concept: Dual of surjectivity is injectivity
monomorphism: $f : S \to T$, if $R \underset{h}{\overset{g}{\rightrightarrows}} T$ $fg = gh \to g = h$

Example 1.8.7. If S, T subsets, $f : S \to T$ is injectivity $\leftrightarrow$ f is monomorphism (also true for rings, groups, ...)

1.8.2 Functors

Original Idea: Category of topological spaces → category of abelian groups

(Insert Figure)

If C, D categroies, a functor from C to D consist of

1. Object $F(X)$ for each object $X \in C$
2. Morphism $f : X \to Y \to$ morphism $F(f) : F(X) \to F(Y)$

Axioms: Behaves in "obvious" way. $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$, $F(fg) = F(f)F(g)$

Example 1.8.8. Forgetful Functor, (Category of Groups) → (Category of Sets) by $G \mapsto$ underlying set, $G \to H \mapsto G \to H$

Chapter 2

Rings

2.1 September 27

2.1.1 Category Theory

We answer one final question: If a morphism is an epimorphism and a monomorphism, is it an isomorphism
Sets, Abelian groups: Yes
Rings: No $\quad \mathbb{Z} \hookrightarrow \mathbb{Q}$, mono + epi, not isomorphism
Top Spaces: ($\mathbb{R}$, discrete $\to$ ($\mathbb{R}$, ususal)

2.1.2 Rings

We can define a ring concretely as the set of endomorphisms of an abelian group

Definition 2.1.1. *A ring is a set R with $+, \times$ such that R forms an abelian group under addition, $\times$ is associative, $+, \times$ satisfy left/right distributive laws.*

Two ambiguities in definition:

- Ambiguity 1: Does it has multiplicative identity, 1?
  Algebra: Yes, Analysis: No
- Basic

Example 2.1.2 (Basic Examples)**.** Field $\mathbb{R}, \mathbb{C}$. Integers $\mathbb{Z}$, Gaussian Integers $\mathbb{Z}[i]$ $m + ni$ with $i^2 = 1$.
Polynomials ring $R[x]$, matrices $M_n(\mathbb{R})$ $n \times n$ matrices (endomorphisms of vector space $\mathbb{R}^n$).
Can form more generla M_n(ring). Algebraic Geometry: $\mathbb{C}[x, y]/y^2 = x^2 - ax + b$

Many things in group theory have an analog in rings

Groups	
Acts on Sets	Acts linea
Symmetric Groups (all permutations of a set)	$M_n(R)$ all
Permutation Representation	Linear Rep
G acts on A, B, G acts on $A \cup B$	Ring acts on
$\lvert A \cup B \rvert = \lvert A \rvert + \lvert B \rvert + \lvert A \cap B \rvert$	R=field, $\dim(M + N)$

This fails for 3 vector spaces: $|A \cup B \cup C| = |A| + |B| + |V| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$ but $\dim(L + M + N) \neq \dim L + \dim M + \dim N - \dim(L \cap M) - \dim(M \cap N) - \dim(N \cap L) + \dim(M \cap N \cap L)$
(Consider 1 dimensional subsets of $\mathbb{R}^3$)

Analog of Cayley's Theorem: Every ring = endomorphisms of some abelain group preserving some "structure" R as an abelian group is acted on by R on the right. Linear maps of R preserving action on right = R acting on left

Definition 2.1.3. A (left) module M over R is an abelian group acted on by R.
$R \times M \to M$ such that $r(m_1 + m_2) = rm_1 + rm_2$, $r(sm) = (rs)m$, $1m = m$, $(r_1 + r_2)m = r_1m + r_2m$

Analog of group acting on a set. Can have left modules, right modules, and two-sided modules

Example 2.1.4 (Burnside Ring of a Group)**.** Take S_3 looks at all ways G acts on a finite set (up to iso). Make into ring.
$A + B = A \sqcup B$, $A \times B = A \times B$ (as sets)
Note: What about -?
If G acts on A, $A = A_1 \cup A_2 \cup \cdots$ A_i is an orbit of A, G acts transitively on each A_i
How can S_3 act on transitively on a set A. Subgroups of $S_3 \leftrightarrow$ transitive action on A + point of A

S_3 subgroups	Action	
(1)	Acts on 6 points	1
(1 2), (1 3), (2 3)	Acts on 3 points	3
(1 2 3) (1 3 2)	Acts on 2 points	2
G	Acts on 1 point	1

Elements of R are $a\,1 + b\,2 + c\,3 + d\,6$. What about $\times$? Compute products of 1, 2, 3, 6

(Insert Figure)

Problem: R does not have $-$
A: Construction of Grothendeick Ring
Idea: Start with $\mathbb{N}$ (integers $\geqslant 0$), construct $\mathbb{Z}$. pairs (m, n) representing $m - n$, $(m_1, n_1) \equiv (m_2, n_2)$ if $m_1 + n_2 = m_2 + n_1$
Copy this idea to construct an abelian group from an abelian monoid. This does not work in general.
Subtle Problem: If we have $m_1 - n_2 \equiv m_2 - n_2$ iff $m_1 + n_2 = m_2 + n_2$ this is not an $\equiv$ relation
Suppose $m_1 - n_1 \equiv m_2 - n_2$, $m_2 - n2 \equiv m_3 - n_3$. Want to show $m_1 - n_1 \equiv m_3 - n_3$. $m_1 + n_2 = m_2 + n_1$, $m_2 + n_3 = m_3 + n_2$ so $m_1 + n_2 + n_3 = m_2 + n_1 + n_3 = n_1 + m_3 + n_2$. Need to cancel n_2. Can't do this in gneral, $x + y = x + z$ does not imply $y = z$
Fix: Define $\equiv$ by $m_1 - n_2 \equiv m_2 - n_2$ iff $m_1 + n_2 + x = m_2 + n_1 + x$ for some x
Check: This is an equivalence relation. We get an abelian group from the $\equiv$ classes.

This gives us functors: Groups $\underset{G}{\overset{F}{\rightleftarrows}}$ Monoid where G is the forgetful function, F maps a monoid to its Grothendeick group. G, F adjoint, eg. maps from M $G(A)$ "same as" maps from $F(M)$ A
Back to ring of S_3: elements of form $a\,1 + b\,2 + c\,3 + d\,6$ $a, b, c \in \mathbb{Z}$ possibly < 0

Example 2.1.5. Group ring of G (over R). Ring "generated" by G
Set of all formal elements $\sum_{g \in G} r_i g$ $r_i \in R$ almost alll 0. $+, \times$ on group ring "obvious"

$G = \mathbb{Z}/4\mathbb{Z}$. group ring over $\mathbb{C}$. Elements if $\mathbb{C}[G]$ are of the form $a_0 + a_1 g + a_2 g^2 + a_3 g^3$ $a_i \in \mathbb{C}$ = vector space over $\mathbb{C}$ of dimension 4.
$\mathbb{C}[G]$ splits as a product of rings.
Product of R, S is $R \times S$ with "obvious" $\times, +$

Products in Categories: If R, S objects, $R \times S$ object such that:

- We have morphisms (Insert Figure)
- $R \times S$ is the best possible object like this. (Insert Figure)

Suppose $R \times S$ product of R, S. How do we recover R, S from $R \times S$?
Look at $u_1 = (1, 0)$, $u_2 = (0, 1)$, $u_1^2 = u_1$, $u_2^2 = u_1 <$ $u_1u_2 = u_2u_1$, $u_1 + u_2 = 1$ (u such that $u^2 = u$ is called idempodent)
$1 =$ sum of commuting irreducibles. Then we can recover R from $R \times S$ by $(R \times S)(u_1)$
To break up $\mathbb{C}[G]$ we want to write 1 as sum of idempotents
Example 2.1.6. $G = \mathbb{Z}/2\mathbb{Z} = \{a + bg\}, g^2 = 1$. $(a + bg)^2 = a + bg \to a^2 = 2abg + b^2g = a + bg$ so $a^2 + b^2 = a$, $2ab = b$. $a = \frac{1}{2}, b = 0 \to \frac{1+g}{2}, \frac{1-g}{2}$ so $\mathbb{C}[G] = \frac{1+g}{2}\mathbb{C}[G] + \frac{1-g}{2}\mathbb{C}[G] \cong \mathbb{C} + \mathbb{C}$
For $G = \mathbb{Z}/4\mathbb{Z}$, $\frac{1+g+g^2+g^3}{4}, \frac{1-g+g^2-g^3}{4}, \frac{1+ig+-g^2-ig^3}{4}, \frac{1-g-g^2+ig^3}{4}$ all idempodent, $\mathbb{C}[G] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}$
Example 2.1.7. Monoid ring. Monoid = integers $\geqslant 0$ under x. Allow infinite sums.
"infinite"
$\left(\sum \frac{a_m}{m^2}\right)\left(\sum \frac{b_m}{m^2}\right) = \sum \frac{c_m}{m^s}$ $c_1 = a_1b_1, c_2 = a_2b_1$

2.2 September 29

2.2.1 More Examples of Rings

Chapter 3

Representation Theory

3.1 October 4

3.1.1 Representation Theory

A representation of a group G is something acted on by G
Problem: Given G, find all Representations

- Sets: permutation representations
- Vector space: linear representation - over $\mathbb{C}$: complex representation, over finite fields: modular representation, Abelian group: integral

Example 3.1.1. $G =$ icosahedral group $=$ order 60
permutation representations: 20 faces, 12 vertices, 1 point (trivially), G (regular representation)
linear representations:

1. Trivial action on $\mathbb{C}$ (G acts trivially)
2. 3-dim rep   icosahedron $\subseteq \mathbb{R}^3 \subseteq \mathbb{C}^3$
3. Permuation representaiton $\to$ linear representation by taking element as a basis for vector space
4. Regular represenation: V has basis G

How can we classify permutations representations?
Any permutation representation $=$ disjoint union of transisitive sets so it is enough to classify transitive permutations. They correspond to conjugacy classes of subgroups of H, G acts on G/H. Subgroups are hard to classify.

Primitive Representations
Suppose G acts on points, points grouped into boxes. G acts on boxes.

Example 3.1.2. $K \subseteq H \subseteq G$, G acts on $\underset{\text{“points”}}{H/K} \to \underset{\text{“boxes”}}{G/K}$. This happends when H is not maixmal. Maximal subgroups $\leftrightarrow$ prime representation.
Analog for linear representations
Suppose v, W reps of G, so is $V \oplus W$
A representaiton is called decomposable if it can be written as $\oplus$ of nonzero representations. Representations

that are not decomposable are called indecomposable.
Suppose W is a representaiton of G containing a representation V, $0 \neq V, W$, $0 \subseteq V \subseteq W$. W is reducible. If no such V exists, W is called irreducible (analogous to primitive permutation representations)
Decomposable $\to$ reducable

Fundamental counterexample to everything: $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$
Representation of $\mathbb{Z}$ on $\mathbb{C}$ by $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.
$V = \begin{pmatrix} * \\ 0 \end{pmatrix}$, also a representation of $\mathbb{Z}$. $\mathbb{Z}$ acts trivially on V and W/V but not on W.
$0 \to V \to W \to W/V \to 0$ does not split.
If $W = V \oplus U$, $\mathbb{Z}$ acts trivially on V, U so trivially on W.
W indecomposable ubt not irreducible.

Classify complex representations of $\mathbb{Z}/2\mathbb{Z}$. Element $g, g^2 = 1$
G acts on vector space W over $\mathbb{C}$. Take eigenvalues of g. $g^2 = 1$ so eigenvalues ± 1.
$W = W^+ \oplus W^-$, $v = \frac{v+g(v)}{2} + \frac{v-g(v)}{2}$. W^+ sum of 1 dimensional subspaces with $g = 1$. W^- sum of 1 dimensional subspaces with $g = -1$. 2 indecomposable reps $\mathbb{C}^+ : g = 1$, $\mathbb{C}^- : -1$ 1 dimensional.
What about representations of $\mathbb{Z}/2\mathbb{Z}$ on a vector space over $\mathbb{F}_2$ (Can't divide by 2)
Get other indecomposable rep: g acts as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on $(\mathbb{F}_2)^2$

Representations of group $\mathbb{Z} \leftrightarrow$ invertible linear transformations.
Want to classify representations up to isomorphism
Complex linear represenations of $G \leftrightarrow$ modules over group rings $\mathbb{C}[G]$
Classify finitely generated modules over Euclidean ring:
THey are all $\sum$ of modules of the form R/p^n, p prime.
Proof: Copy proof for $\mathbb{Z}$
$\mathbb{C}[x]$ is Euclidean, almost group ring of $\mathbb{Z}$, $\mathbb{C}[x, x^{-1}]$
Finitely generated modules over $\mathbb{C}[x]$ all have form $\bigoplus \mathbb{C}[x]/p^n$, $p = 0$, prime (irreducible poly $x - \alpha$
Any finitely generated module over $\mathbb{C}$ is $\oplus$ of

1. $\mathbb{C}[x] = \mathbb{C}[x]/(0)$ (∞ dimensional so we don't consider it)

2. $\mathbb{C}[x]/(x-\alpha)^n, \alpha \in \mathbb{C}$, $n \geqslant 1, n \in \mathbb{Z}, \alpha \neq 0$

   This consists of transformations $\begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$. Basis $1, (x-\alpha), \dots, (x-\alpha)^{n-1}$ so every linear transformation of vectors on $\mathbb{C}$ is conjugate to

$$\begin{pmatrix} \begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix} & & 0 \\ & \begin{pmatrix} \beta & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \beta \end{pmatrix} & \\ 0 & & \ddots \end{pmatrix}$$

$$\text{indecomposable: } \alpha, n \left.\begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}\right\} n, \text{ irreducible} \leftrightarrow n = 1$$

When are all indecomposable maps irreducible?
Holds for finite groups over $\mathbb{C}$, compact groups over $\mathbb{C}$, finite dimensional semi-simple Lie groups.
Fails for: finite groups over finite fields, represenions of $\mathbb{Z}$ over $\mathbb{C}$
(Finite Dimensional) Complex representations of finite groups are completeley reducible $\to \bigoplus$ irreducible representations.
Key point: Suppose $V \subseteq W$ (V, W finite dimensional represenations of G) Can we write $W = V \oplus U$? U invariant under G.
Why not take $U = V^\perp$ (orthogonal complement)? Problem: $V^\perp$ might not ber invariant under G $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$
When does G perserve orthogonal complement? Does if f preseves the innter product. $(u, v) = (gu, gv)$ eg. g is unitary, $g^{-1} = \overbrace{g^t}$
Recall V has a hermetian $(\, , \,)$. Linear in first slot, antilinear in second, $(u, v) = \bar{(}v, u)$, $(u, u) > 0$ if $u \neq 0$
How to make inner prodyct over G? Take average over G.
Define new $(\, , \,)$ by $(\, , \,)^G = \sum_{g \in G} (gu, gv)$, hermetian, invariant under g.
Vital key point: $(\, , \,)^G$ not degenerate: $(u, v) = 0$ for all $v \to u = 0$. $(u, u)^G > 0$ if $(u \neq 0)$
Fails if we try to copy this for finite fields $\mathbb{F}_p$

Example 3.1.3. $G = S_3$, order 6
Indecomposable representations?

1. Tivial representaion on $\mathbb{C}$
2. $S_3 \to \mathbb{Z}/2\mathbb{Z}$ so every representation of $\mathbb{Z}/2\mathbb{Z}$ representation of S_3
3. 2 dimensional reprsentation, S_3 acts on triangle $\subseteq \mathbb{R}^2$

Other representations: S_3 acts on 3 points: 1, 2, 3. Permutation representation $\to$ linear representation of S_3 on $\mathbb{C}^3$, reducible. Consider $v_1 + v_2 + v_3$ preserved by S_3 so $\mathbb{C}^3 = \mathbb{C}^+ \oplus$(2 dimensional representation)

How to describe representations?
We could give a matrix for every element of G: (1) Tiresome, (2) Hard to see if 2 representations equivalent
Frobenius: enough to give the trace of elements of G. $\mathrm{tr}(ghg^{-1} = \mathrm{tr}(h))$ so enough to give trace on each conjugacy class of G.

Example 3.1.4. $G = \mathbb{Z}/2\mathbb{Z}$:

	1	g
χ_0	1	1
χ_1	1	-1

$G = S_3$:

	1	(1 2) (2 3) (3 1)	(1 2 3) (1 3 2)
χ_0	1	1	1
χ_1	1	-1, 1	
χ_2	2	0	-1

Representation theory can help prove difficult theorems about groups.
Burnsides $p^a q^b$: Groups of order $p^a q^b$ are solvable.

3.2 October 6

3.2.1 Representations of Finite Abelian Groups

We make the following observations about the character table of S_3

1. Columns are orthogonal (under $\sum_\chi \chi(g)\overline{\chi(h)} = 0$ g, h not conjugate, $|G|$, g, h conjugate)
2. # columns = # rows (# conjugacy classes = # irreducible reps)
3. Rows are orthogonal (under $\sum_g \chi_i(g)\overline{\chi_j(g)} = 0$, $i \neq j$, $=|G|$, $i = j$ $= \sum_{\text{conj classes } \{g\}} \chi_i(g)\overline{\chi_j(g)})\times$(size of conjugacy class)

Problem: Given a finite abelian group find the character table
Observation: All irreducible representations are one dimension
Reason: Pick some $g \in G$. g acts on V has an eigenvector with eigenvalue λ. Look at V_λ=all vectors with eigenvalue λ. V_λ acted on by G. If $h \in G$, $v_\lambda \in V_\lambda$, $hv_\lambda \in V_\lambda$ since $g(hv_\lambda) = h(gv_\lambda) = \lambda hv_\lambda$ so $V = V_\lambda$ as V is irreducible.

So linear representations of G are "same as" homomorphisms $G \to \mathbb{C}^*$. $1 \in G \to$ some z with $z^n = 1$, nth root of unity.
Dual group of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ $a \mapsto e^{2\pi iab/n}$ $b = 0, 1, \ldots, n-1$
If G is cylic, $G \cong \hat{G}$ but no natural isomorphism since depends on choice of generator and root of 1.
Any finite abelian groups is is a product of cylic groups $G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots$
$\mathrm{Hom}(G, \mathbb{C}^*) \leftrightarrow \mathrm{Hom}(\mathbb{Z}/n_1\mathbb{Z}, \mathbb{C}^*) \times \mathrm{Hom}(\mathbb{Z}/n_2\mathbb{Z}, \mathbb{C}^*) \times \cdots$ so $\hat{G} \cong \widehat{\mathbb{Z}/n_1\mathbb{Z}} \times \widehat{\mathbb{Z}/n_2\mathbb{Z}} \times \cdots \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \cong G$. Any finite abelian group is isomorphic to its dual (not canonically).
Typical character tables:

$\mathbb{Z}/5\mathbb{Z}$:

1	5	5	5	5
1	1	1	1	1
1	z	z^2	z^3	z^4
1	z^2	z^4	z	z^3
1	z^3	z	z^4	z^2
1	z^4	z^3	z^2	z

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

1	2	2	2
1	a	b	c
1	1	1	1
1	1	-1	-1
1	-1	1	-1
1	-1	-1	1

Vector spaces: $V \cong V^*$ not canonical, $V \cong V^{**}$ canonical, $v \in V, v^* \in V^*$ $v(v^*) = v^*(v)$
G finite abelian, $G \cong \hat{G}$ not canonical, $G \cong \hat{\hat{G}}$ canonical: $g \in G, \hat{g} \in \hat{G}$ homomorphism by $\hat{G} \to G$ by $g(\hat{g}) \to \hat{g}(g)$
Check Properties of character tables:

1. Table is square: # conjugacy classes = # irreducible representations since $|G| = |\hat{G}|$
2. Rows orthogonal: want to show $\sum_g \chi_i(g)\overline{\chi_j(g)} = \begin{cases} |G| & i = j \\ 0 & i \neg j \end{cases}$. $\overline{\chi_j(g)} = \chi_j(g)^{-1}$ since $|\chi_j(g)| = 1$ so suffices to show $\sum_g \chi(g) = \begin{cases} G & \chi \text{ trivial} \\ 0 & \chi \text{ nontrivial} \end{cases}$. Pick some h with $\chi(g) \neq 1$. $\sum_g \chi(hg) = \sum_g \chi(h)\chi(g) = \chi(h)\sum_g \chi(g)$ and $\sum_g \chi(hg) = \sum_g \chi(g)$ so $(1-\chi(h))\sum \chi(g) = 0$ so since $\chi(h) \neq 1$, $\sum_g \chi(g) = 0$
3. Columns orthongonal

So characters of G from an orthogonal basis for the vector space of all complex functions on G. So for function f from G to $\mathbb{C}$ we have $\sum a_\chi \chi(g)$, $a_\chi = (f, \chi) = \sum f(g)\overline{\chi g}$. a_χ called fourier coefficients.

Fourier analysis: f periodic, $f(x + 2\pi) = f(x)$. $f = \sum_{n>0} a_n \sin(nx) + \sum_{n \geqslant 0} b_n \cos(nx)$. $G=$ group, $R/2\pi\mathbb{Z}$. Dual group of $G=$ homomorphisms from G to $\mathbb{C}^n$. $\hat{C} = \mathbb{Z}$ by $x \mapsto e^{inx}$ $(n \in \mathbb{Z})$
$e^{inx} = \cos nx + i \sin nx = \sum c_n e^{inx}$, $\hat{\hat{G}} = G$. $\text{Hom}(\mathbb{Z}$, complex numbers with $|z| = 1)$
$G = \mathbb{R}, \hat{G} = \text{Hom}(\mathbb{R}, S^1)$ $x \mapsto e^{i\pi xy}$ $y \in \mathbb{R}$ so $\hat{G} \cong G$
Fourier Transform: $\int y\hat{f}(y)e^{i\pi xy}dx$
Specific cases of pantiyagin duality: $G =$ locally compact abelian group, $\hat{G} =$ maps to S^1, $G \cong \hat{G}$
What happens if field is not $\mathbb{C}$?

1. Field has characterstic 0 but is not algebraically closed. Can get irreducible representations of dim >1
   Ex: Field $F = \mathbb{R}$, $G = \mathbb{Z}/3\mathbb{Z}$

   Over $\mathbb{C}$:

1	1	1
1	ω	ω^2
1	ω^2	ω

   Over $\mathbb{R}$:

1	1	1
2	-1	-1

2. Char >0. Syppose characteristic is $p > 0$. Look at maps of $\mathbb{Z}/p\mathbb{Z}$. Only irreducible representation is trivial one. Only possible eigenvalues is $\lambda = 1$ since $\lambda^p = 1, (\lambda^p - 1) = (\lambda - 1)^p$
   Look at representations that are indecomposable but not irreducible. Decomposable $\leftrightarrow$ linear transformation $T^p = 1$ ie. $(T-1)^p = 0 \leftrightarrow$ nilpotent matrices with $N^p = 0$. (0), $\begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 & & \\ 0 & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$
   so we have p distinct representations.

Application: Dirichlet's Theorem: Given arithmetic progression $an + b$, $(a, b) = 1$ contains ∞ primes.
Ex: ∞ primes of the form $4n + 1$. We consider the character table of $(\mathbb{Z}/a\mathbb{Z})^*$

$a = 4$:

	1	3
χ_0	1	1
χ_1	1	-1

Dirichlet L-series: $\sum_n \frac{\chi(n)}{n} : \frac{1}{1^s}+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\cdots, \frac{1}{1^s}-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\cdots$
$\sum_n \frac{\chi(n)}{n} = \prod_p \frac{1}{1-\chi(p)p^s}$ so $\log\left(\sum \frac{\chi(n)}{n}\right) = \sum_{n.p} \frac{\chi(p^n)}{p^{ns}n}$ so we get $\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{2\cdot 9^s}+\cdots$, infinite at $s=1$, $-\frac{1}{3^s}+\frac{1}{5^s}-\frac{1}{7^s}+\frac{1}{2\cdot 9^s}+\cdots$ finite at $s=1$, nonzero since series converges to $\frac{\pi}{4}\neq 0$
Define $f=1$ if $n\equiv 1 \mod 4$, 0 otherwise. Function on $(\mathbb{Z}/4\mathbb{Z})^*$ = linear combinations of $\chi_0, \chi_1 = \frac{1}{2}(\chi_0+\chi_1)$.
$\frac{1}{2}$ sum if $\frac{1}{5^s}+\frac{1}{2\cdot 9^s}+\frac{1}{13^2}+\cdots = \sum_{n,p\equiv 1 \mod 4} \frac{1}{p^{ns}n}$ is infinite on $s=1$. Sum of terms $\frac{1}{np^{ns}}$ $n\geqslant 2$ is finite so $\sum_{p\equiv 1 \mod 4} \frac{1}{p} = \infty$
Key point: $\sum \frac{\chi(n)}{n^s} \neq 0$ at $s=1$ (if $\chi\neq$ trivial) hard step

3.3 October 11

3.3.1 Orthogonality relations

Character Tables:

- rows orthogonal: weight by size of conjugacy classes
- Norm of row = $|G|$
- columns orthogonal
- norm of columns = $|G|$/(size of conjugacy class)

Special Cases

1. # conjugacy classes = # characters
2. $\sum d_i^2 |G|$ (d_i = dimension of irreducible characters)

Quaternion Group

- Find 1-dimensional elements ≡ same as characters of abelianized group = G/(normal subgroup generated by $ghg^{-1}h^{-1}$)
  Note that this is adjoint to the forgetful functor.
- Abelianization of $Q = Q/\{\pm 1\} = (\mathbb{Z}/2\mathbb{Z})^2$ - 4 characters
- Use orthogonality relations, $\sum d_i^2 = G$. $1^2+1^2+1^2+1^2+d^2 = 8$, $d=2$. Last rep given by row orthogonality.

1	-1	$\pm i$	$\pm j$	$\pm k$
1	1	2	2	2
1	1	1	1	1
1	1	-1	-1	1
1	1	-1	1	-1
2	-2	0	0	0

Dihedral group of order 8 has same character table as Q. Possible for different groups to share the same character table.
Alternating Group - A_4

- Use permutation represntation of A_4 of 4 points so 4 dimension representation with this basis.

- What is its characeter? What is the character of permutation representation (on n points) of an n dimension vector space?
  trace = # fixed points so permutation rep has character $(4, 0, 1, 1)$, not irreducible.

- How many copies of 1-dimensional element. $(,) = 12 = |G|$ with trivial character so can subtract out to get $(3, -1, 0, 0)$, norm = 12 - so is irreducible.

S_4

- Abelianization $= \mathbb{Z}/2\mathbb{Z}$
- Permutation representation: $(4, 0, 2, 0, 1, 0)$ reduce to irreducible representation $(3, 1, -1, 0, 1)$
- Have product of 3 dimensional representation with 1 dimensional representation

1	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)
1	6	3	8	6
1	1	1	1	1
1	-1	1	1	-1
3	1	-1	0	1
3	-1	-1	0	1
2	0	2	-1	0

Abelian groups: If χ_1, χ_2 are irreducible characters so is $\chi_1\chi_2$
Non abelian group: χ_1, χ_2 usually not irreducible. It is irreducible if χ_1 has dimension 1.
If G acts on V, χ_1 a character, we get a representatio no V by $g \mapsto \chi_1(g) \cdot g$

Finding Normal subgroups from character tables
Suppose V is an irreducible representaion of dimension d, character χ. What is $\chi(g)$? Diagonalize g, diagonal entries = roots of 1. $\chi(g) = z_1 + z_2 + \cdots + z_d$ where z_i is a root of 1. Now, $|z_1 + \cdots + z_n| \leqslant d$, equality holds if all z_i are equal. if $z_1 + \cdots + z_n = d$, all $z_i = 1$ so if $\chi(g) = \chi(1)$, g acts trivially on rep.
For S_4, element $(1), (1\,2)(3\,4)+$ conjugates act trivially in 2 dimensonal representation, form a normal subgroup.

Example 3.3.1. Binary Dihedral group of order 24 $\overset{\text{onto}}{\to}$ A_4 so get representations of dimension $1, 1, 1, 3$

Example 3.3.2. A_5 = alternating group = rotations of icosahedron
A_5 acts on $\mathbb{R}^3$ so get 3-dimensional representations with characters as trace of rotations of icosahedron
Use outer automorphism $A_5 \subseteq S_5$ to get a rep
Now, $1^2 + 3^2 + 3^2 + x^2 + y^2 = 60$ so $x = 4, y = 5$. Perm rep $(5, 1, 2, 0, 0)$ with irreducible $(4, 0, 1, -1, -1)$.

1	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)
1	1	1	1	1
3	-1	0	$1 - 2\cos\frac{2\pi}{5}$	$1 - 2\cos\frac{4\pi}{5}$
3	-1	0	$1 - 2\cos\frac{4\pi}{5}$	$1 - 2\cos\frac{2\pi}{5}$
4	0	1	-1	-1
5	1	-1	0	-0

Example 3.3.3. S_5, binary dihedral group of order 120, symmetry group S_6

3.3.2 Proofs Of Orthogonality Relations

1. All representations of G can be made unitary (,) invariant under G.
   Define (,) by taking any (,) make invariant under G be taking average
2. Want to show if χ is an irreducible character, $(\chi, 1) = 0$, $\sum_g \chi(g) = 0$

Suppose V is an irreducible representation (finite dimensional) with no fixed vectors ($\neg 0$), then $\sum_g \chi(g) = 0$. This holds for all irreducible representations except fo the trivial one. Pick $v \in V$, $\sum_{g \in G} g(v) = 0$ since no fixed vectors $\neq 0$

3. Suppose V, W are irreducible representaions. Look at vector space $\mathrm{Hom}(V, W)$. Have rep by G, dim $=$ $\dim V \times \dim W$ character $\chi_W \overline{\chi_V}$, χ_V, χ_W characters of V, W. Enough to check for one factor $\chi_{\mathrm{Hom}(V,W)}(g) = \chi_W(g)\chi_V(g)$. Choose basesof V, W such that g is diagonal. Split V, W into sum of 1-dimensional spaces acted on by g. Suffices to show case where $V, W, \dim = 1$

Schur's Lemma: Suppose V, W irreducible representations, then $\mathrm{Hom}_G(V, W)$, homomorphisms invariant under g ie. fixed points of G on $\mathrm{Hom}(V, W)$ has dimension $\begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{if } V \ncong W \end{cases}$.
$V \to W$ invariant under G, image is invariant subspace so is 0 or W as W is irreducible. Kernerl is invariant subspace of V so is 0 or V as V is irreducible. so map is either 0 or isomorphism.
If V, W not isomorphic, no maps $V \to W$ invariant under G.
If $V = W$, then $\mathrm{Hom}(V, V)$ is a division algebra (eg. ring where elements have inverse), finite dimensional algebra over $\mathbb{C}$, algebraically closed, any division algebra is $\mathbb{C}$. So $\mathrm{Hom}_G(V, W) = \mathbb{C}$

Example 3.3.4. Look at real reps of $\mathbb{Z}/3\mathbb{Z}$

$$\begin{vmatrix} 1 & g & g^2 \\ 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} \quad \begin{vmatrix} 1 & g & g^2 \\ 1 & 1 & 1 \\ 2 & -1 & -1 \end{vmatrix}$$

$\mathrm{Hom}(V, V) = \mathbb{C}$, $\mathbb{C}$ division algebra over $\mathbb{C}$

Example 3.3.5. $G = Q_8$ acts on quaternions H by left multiplication. 4-dim real representation, 2-dim complex representation. $\mathrm{Hom}_G(V, V) = H$ action given by right multiplication. H division algebra over $\mathbb{R}$.

Row orthogonality: If V, W irreducible, then $\sum_g \chi_V(g)\overline{\chi_W(g)} = 0$ $V \ncong W$ $|G|$ if $V \cong W$. Look at character $\mathrm{Hom}(V, W) = \chi_V \overline{\chi_W}$. If $W \ncong V$, $\mathrm{Hom}(V, W)$ doesnt contain any invariant characters so is 0. So $\sum_g \chi_v(g)\overline{\chi_w(g)} = 0$. If $V = W$, $\mathrm{Hom}(V, V)$ is a 1-dimensional subspace so $\sum_g \chi_V(g)\overline{\chi_W(g)} = |G|$

> **Corollary 3.3.6.** Any representation is determined by its characters.

$V = \bigoplus V_i$ (V_i irreducible) by complete irreduciblility. By orthogonality, number of irreducible representatiosn W appears is $\frac{(\chi_W, \chi_V)}{|G|}$.
Fails over field with char > 0
$G = \mathbb{Z}/p\mathbb{Z}$ Field $= \mathbb{Z}/p\mathbb{Z}$. Rep: $g \to \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$ trivial 2-dim representation, $g^n \to \begin{pmatrix} 1 & n & 0 & 1 \end{pmatrix}$ indecomposable.

Chapter 4

Polynomials

4.1 October 18

4.1.1 Polynomials

Recall:

1. Polynomials over a field have a Euclidean division algorithm
   For f, g, $f = gq + r$, $\deg(r) \leqslant \deg(g)$ $(g \neq 0)$, $\deg(0) = -\infty$

2. $k[x]$ has a unique factorization

Primes of $\mathbb{Z} \leftrightarrow$ irreducible polynomials

Example 4.1.1. Sieve of Eratosthenes:
on $\mathbb{Z}$: $\cancel{1}, \boxed{2}, \boxed{3}, \cancel{4}, \boxed{5}, \cancel{6}, \boxed{7}, \cancel{8}, \cancel{9}, \cancel{10}\cdots$
on $\mathbb{F}_2[x]$: $\cancel{1}, \boxed{x}, \boxed{x+1}, \cancel{x}^2, \cancel{x}^2+1, \cancel{x}^2+x, \boxed{x^2+x+1}, x^3\cdots$
only need to write polynomials such that constant term nonzero, sum of coefficient is odd.
$\boxed{x^2+x+1}, \boxed{x^3+x+1}, \boxed{x^3+x^2+1}, \boxed{x^4+x+1}, \cancel{x}^4+x^2+1, \boxed{x^4+x^3+1}, \cancel{x}^4+x^3+x^2+x+1$
Recall: If $f(x)$ has a root $x - a$. $f(x) = (x-a)g(x)$ since $f(x) = (x-a)g(x) + r$, $\deg f \leqslant 0$.
If R is an integral domain, polynomial in $R[x]$ has $\leqslant \deg f$ roots.
This is false in general: $R = \mathbb{Z}/8\mathbb{Z}$ $f(x^2-1)$ has 4 roots $x = 1, 3, 5, 7 \mod 8$

Corollary 4.1.2. $(\mathbb{Z}/p\mathbb{Z})^*$ cyclic, prime p has primitive roots.

Proof. We show that a finite subgroup of F^* (for a field of F) is cyclic. G has $\leqslant n$ elements, with $g^n = 1$ (any $n \geqslant 1$) since polynomial $x^n - 1$ has $\leqslant n$ roots so by the structure theorem for abelian groups $G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots$ $n_2|n_1, n_3|n_2, \ldots$. If $n_2 > 1$, G has $\geqslant n_2^2$ elements of order n_2 so $n_2 = n_3 = \cdots = 1$

Example 4.1.3. $F = \mathbb{Z}/7\mathbb{Z}$ $F^* = 1, 2, 3, 4, 5, 6$ cyclic group generated by 3.
$F =$ Quaternions, $\mathbb{H} = a + bi + cj + dk$ not a field, is a division ring
$\mathbb{H}$ contains a finite subset $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ not cyclic
$x^2 + 1 = 0$ has infinite roots $a_i + b_j + c_k$ with $a^2 + b^2 + c^2 = 1$
$F = \mathbb{C}$, polynomial $x^2 - 1 = 0$ has ∞ solutions

Useful Fact: If polynomail of deg $\leqslant n$ has $> n$ roots it is 0
Warning: A polynomial f can vanish at all points of a field, still not be 0.
$F =$ finite field, $\mathbb{Z}/p\mathbb{Z}$. $\quad f(x) = x^p - x$, roots all points of F

Polynomials over rationals form a UFD.
What about integers. $\mathbb{Z}[x]$ has no diivsion with remainder, not euclidian. Not all ideals principle. Consider $I =$ polynomials with even constant terms $(2\, x)$

$6x^2 - 18x + 12 = 6(x^2 - 3x + 2) = 2 \cdot 3(x-2)(x-1)$. Note we have a factorization into irreducible polynomials such that coefficents have no common factors, primes of $\mathbb{Z}$
We will show:

1. Irreducible polynomials $\mathbb{Z}[x]$ are prime

2. primes of $\mathbb{Z}$ are prime in $\mathbb{Z}[x]$

We define the content $c(f)$ of a polynomia lin $\mathbb{Z}[x]$ is the largest integer such that $\frac{f(x)}{c(x)}$ in $\mathbb{Z}[x]$ $=$ common divisor of all coefficents, eg. $c(6x^2 - 18x + 12) = 6$
Key property: $c(f)c(g) = c(fg)$
Obvious: $c(f)c(g) \leqslant c(fg)$ $\quad$ Problem: $c(f)c(g) \geqslant c(fg)$
Divide f, g by $c(f), c(g)$ to get polynomial with $c(h) = 1$. Need to show that if $c(f) = 1, c(g) = 1$ then $cf(g) = 1$
Suppose $p|c(fg)$, (p prime) $p\ \ |c(f)$, $p\ \ |c(g)$. $f = a^n x^n + \cdots + a_i x^i + a_{i-1}x^{i-1} + \cdots a_0$, $g = b_m x^m + \cdots + b_j x^j = b_{j-1}x^{j-1} + cdots + b_0$ with $a_{i-1}, \ldots, a_0, b_{j-1}, \ldots, b_0$ divisible by p, a_i, b_j not divsible by p. Now look at fg, the coefficent of x^{i+j}, $a_{i+j}b_0 + a_{i+j-1}b_1 + \cdots + a_i b_j + a_{i-1}b_{j+1} + \cdots + a_0 b_{i+j}$. All terms except $a_i b_j$ divisble by p so the coefficient of x^{i+j} is not divisble by p. So prime does not divide $c(fg)$ so $c(fg) = 1$, since p was any prime.

We can show that $\mathbb{Z}[x]$ has unique factorization. Follows from:

1. $\mathbb{Q}[x]$ has unique factorization

2. $c(fg) = c(f)c(g)$

Key Steps: Show that if f is a prime of $\mathbb{Z}$ or polynomial of $\mathbb{Z}[x]$ irreducible in $\mathbb{Q}[x]$ with $c(f) = 1$, then f is prime, ie. if f divides gh, f divides g or f divides h.
2 cases:

1. f prime of $\mathbb{Z} \to$ if $p|gh$, $p|c(g)c(h)$ so $p|c(g)$ or $p|c(h)$ so $p|g$ or $p|h$

2. f=poly, $c(f) = 1$ similar

Bonus: If ring R has unique factorization so does the ring of polynomials $R[x]$

> **Proof.** Same proof but with $R = \mathbb{Z}$. Key point: define content c, $c(fg) = c(f)c(g)$

Can extend this: $k[x, y]$ polynomial in 2 variables. $k[x, y] = k[x][y]$ with $k[x]$ UFD so $k[x][y]$ is a UFD.
Repeating this: $k[x_1, \ldots, x_n]$ is a UFD. Still holds for polynomials in infinite variables as each polynomial only contains finitely many variables.
Problem: Given polynomial in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$

1. Is it irreducible?

2. Factor into irreducibles

Is there an algorithn for this? yes - kronecker's algorithm
Recall: If a polynomial has $>\deg f$ roots, it is 0. If f, g, deg $\leqslant n$ and same at $>n$ points, they are equal. If $f = gh$,

Bad news: This is really slow (not polynomial time)
Problem 1: Need to factor integers Problem 2: High number of possibilities for g
Laadf adfadf found polynomial time algorithm for $\mathbb{Q}[x]$
can extend algorithm to $\mathbb{Z}[x_1, \ldots, x_n]$
Similar problem: Does polynomial $f(x_1, \ldots, x_n)$ in $\mathbb{Z}[x_1, \ldots, x_n]$ have roots? No algorithm
Easy Checks for small polynomials in $\mathbb{Z}[x]$ $f(x)$ is irreducible if leading coefficient is 1, irreducible modulo p, $f = gh \to f = gh \mod p$

Example 4.1.4. $x^4 - 3x^3 + 2x - 5$ is irreducible since irreducible modulo 2, $(x^4 + x^2 + 1)$

Warning: Some polynomials look irreducible but are reducible (Auslafllll polynomials)
$x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$, however $x^4 + y^4$ irreducible
Landry: factored

4.2 October 20

4.2.1 Polynomials

Eisenstein: Id $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, a_i divisble by p, a_0 not divisible by p^2, then $f(x)$ is irreducible.

Proof. Suppose $f = gh$ with $g = x^m + b_{m-1}x^{m-1} + \cdots + b_0$, $h = x^[n-m] + \cdots + c_0$, $b_0c_0 = a_0$ so exactly one is divisble by p. Suppose $p|b_0$, $b_i, \ldots, b_0$ divisible by p, b_{i+1} not, coefficient of x^{i+1} in gh is $b_{i+1}c_0 + b_ic_i + \cdots$ not divisible by p a contradiction, so f irreducible.

Applications:

1. Easiest way to write down high degree irreducible polynomials (eg. $x^11 - 4x + 2$)
2. pth roots of 1: roots of $x^p - 1$, $1, z, z^2, \ldots,$ $z = e^{2\pi i/p}$.
   What is irreducible polynomial with z as a root? $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$.
   To show irreducible, let $y = x - 1$, $\frac{(y+1)^p - 1}{(y+1)-1} = y^{p-1} + \binom{p}{1}y^{p-2} + \cdots + \binom{p}{2}y + \binom{p}{1}$ irreducible by Eisenstein.
   Ex: $z^{p^n} = 1$, $\frac{x^{p^n} = 1}{x^{p^n - 1} - 1}$ is irreducible.

Eisenstein polynomials come from totally ramified extensions.
$\mathbb{Z} \subseteq \mathbb{Z}[i]$, $z = (1+i)^2\times$ unit $=$ (prime)$^2\times$ unit, 2 degree extension: totally ramified.
$\mathbb{Z} \subseteq \mathbb{Z}[z]$, $z = e^{2\pi i/p}$, how does z factorize in $\mathbb{Z}[x]$?
$p = (1-z)(1-z^2)\cdots(1-z^{p-1})$, $(1-z^i) =$ unit $\times(1-z)$, $(1-z^i) = (1-z)(1+z+z^2+\cdots)$, $(1-z) = (1-z^i)(1+z^i+z^{2i}+\cdots)$ so $p = (1-z)^{p-1}\times$unit - totally ramified.
$\mathbb{Z} \subset \mathbb{Z}[\alpha]$ algebraic number, $p = (\beta)^n\times$ unit, β satisfies Eisenstein polynomial
Fast Factorization of polynomials over finite fields
Special case: For finite $\mathbb{Z}/p\mathbb{Z}$, p odd prime. Factor $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. We will find linear factors $(x-\alpha)$ (roots of f).
Key idea: consider $x^p - x = (x-1)(x-2)\cdots(x-p-1)$ all possible linear factors.
Take $\gcd(f, x^p - x)$ in $\mathbb{Z}/p\mathbb{Z}[x] = \prod(x-a)$, $(x-a)|f$
How do we find $\gcd(f, x^p - x)$ fast? Russian Peasant Algorithm.

- Fast multiplication: to find $m \times n$, write m in binary $m = 2^{a_0} + 2^{a+1} + \cdots$, compute $n, 2n, 4n, 8n, \ldots$

- For $a^b \mod p$, for some a, b, p, $a \times a \times \cdots$ $|b|$ steps too slow. $b = 2^{b_0} + 2^{b_1} + \cdots$, $a, a^2, a^4, \ldots \mod p$ $a^b = (a^{2^{b_0}}) \times a^{2^{b_1}} \cdots)$
- For $(f, x^p - x)$, p large. $x^p - x = qf + r$ find $x^p - x \mod f(x)$, calculate using Russian Peasant algorithm.

Now, assume f only distinct linear factors, $(x-a)$. Problem: find a_i
$f|(x^p - x)$, $x(x^{p-1} - 1) = x(x^{\frac{p-1}{2}} - 1)(x^{\frac{p+1}{2}} + 1)$ so $(f, x^p - x) = (f, x^{\frac{p-1}{2}} - 1)(f, x^{\frac{p+1}{2}} + 1) \times x$ unless all roots are roots of $x^{\frac{p-1}{2}} - 1$ or $x^{\frac{p+1}{2}} + 1$
What if this doesn't break f into the product of smaller polynomails. Change f to $f(x-a)$, try again

4.2.2 Polynomials over Noetherian Rings

4.3 October 25

4.3.1 Symmetric polynomials

Symmetric group on $\{1, \ldots, n\}$ so acts on $x_1, \ldots, x_n$ so acts on $k[x_1, \ldots, x_n]$ (k field). A symmetric polynomial is a polynomial fixed by S_n

Example 4.3.1.
1. $x_1 + x_2 + \cdots + x_n$
2. $x_1 x_2 \cdots x_n$
3. $x_1 x_2 + x_1 x_3 + \cdots = \sum_{i<j} x_i x_j$
4. $e_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$ - elementary symmetric functions
   Can think of these as coefficents of a polynomial: $f(z) = (z - x_1)(z - x_2) \cdots (z - x_n) = z^n - e_1 z^{n-1} + \cdots \pm e_n$
5. $h_k = \sum_{i_1 \leqslant i_2 \leqslant \cdots} x_{i_1} x_{i_2}$, $h_2 = x_1^2 + x_1 x_2 + \cdots + x_2^2 + \cdots$
6. $p_k = x_1^k + x_2^k + \cdots x_n^k$
7. Schur polynomials: Ex - $(x_1^5 x_2^2 x_3 - x_1^5 x_3^2 x_2 + x_2^5 x_3^2 x_1 + \cdots) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \sigma(x_1)^5 \sigma(x_2)^3 \sigma(x_3)$. Not symmetric since changes sign with odd permutations, so dividde by $\prod_{i<j}(x_i - x_j)$

Special Case of invariant theory: G acts on a set X - look at polynomials in elements of X invariant under G
Problem: Describe ring of invariants
Main Theorem: Symmetric polynomials = polynomial ring in $e_1, \ldots, e_n$, $k[e_1, \ldots, e_n]$
Need to show:

1. Any symmetric polynomial is a polynomial in $e_1, \ldots, e_n$
2. No relations between $e_1, \ldots, e_n$

Key idea: Choose order on monomials: Many ways to do this.
Order by:

1. Total degree: ($X_1^{n_1} X_2^{n_2} \cdots$ has total degree $n_1 + n_2 + \cdots$)
2. Lexographic ordering: $x_1^{n_1} x_2^{n_2} \cdots < x_1^{m_1} x_2^{m_2} \cdots$ if $n_1 < m_1$ or $n_1 = m_1$ and $n_2 < m_2, \ldots$

Suppose $f(x_1, \ldots, x_n)$ is a polynomial, look at largest monomial in it $c x_1^{n_1} x_2^{n_2} x_3^{n_3} \cdots$ get rid of it by subtracting monomial in $e_1, e_2, \ldots, e_n$. Subtract $c(x_1 + x_2 + x_3 + \cdots)^{n_1 - n_2} (x_1 x_2 + \cdots)^{n_2 - n_3} (x_1 x_2 x_3 \cdots)^{n_3 - n_4} \cdots = c e_1^{n_1 - n_2} e_2^{n_2 - n_3} e_3^{n_3 - n_4} \cdots$. This eliminates the largest monomials in f so get a "smaller" polynomial. Ordering on monomials has same order type as the integers so by induction can reduce f to 0 by monomials in $e_1, \ldots, e_n$.
Problem: We did not use the fact that f is symmetric and seem to have proved every polynomial can be expressed in $e_1, \ldots, e_n$

- Want to ensure that in the above sum $n_i - n_{i+1} \geqslant 0$, follows that $n_1 \geqslant n_2 \geqslant n_3$ since f symmetric

So we get a basis for the symmetric polynomials: $e_1^{n_1} e_2^{n_2} \cdots \ 0 \leqslant n_1 n_2 \ldots$
Many different bases: $h_1^{n_1} h_2^{n_2}$, schur polynomials, $p_1^{n_1} p_2^{n_2} \cdots$
How do we convert between other bases?

Example 4.3.2. Express polynomials p_k in terms of $e_1, \ldots, e_n$.

4.4 October 27

4.4.1 Power Series

Recall: holomorphic functions $\mathbb{C} \to \mathbb{C}$ can be written as power series: $a_0 + a_1 z + a_2 z^2 + \cdots$
can add and multiply in obvious way $(a_0 + a_1 z + a_2 z^2 + \cdots)(b_0 + b_1 z + b_2 z^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0) z + \cdots$
Formal power series $\mathbb{C}[[z]]$ = all series $a_0 + a_1 + a_2 z^2 + \cdots$ dont worry about convergence
Works over any ring R: we get $R[[z]]$, check this is a ring
Can repeat: $R[[x]][[y]] = R[[x, y]] = a_{0\,0} + a_{0\,1} x + a_{1\,0} y + a_{1\,1} x^2 \cdots$. Contains polynomials in $R[x, y]$

Basic Properties:
k field. Look at $k[[x]]$. Find ideals of ring (For polynomials $k[x]$ all principle: (f) f is some poly)
Find units of $k[[x]]$ (for $k[x]$, units just k^*). $1 + x$ unit in $k[[x]]$ (not in $k[x]$) $(1 + x)(1 - x + x^2 - x^3 + \cdots) = 1$.
If $a_0 + a_1 x + a_2 x^2 + \cdots \in k[[x]]$, $a_0 \neq 0$ then it is a unit. Take $a_0 = 1$, then f is $1 + A$ where $A = a_1 x_1 + a_2 x_2 + \cdots$
$(1 + A)^{-1} = 1 - A + A^2 - A^3 + \cdots$, well defined power series since A has no constant.

Ideals of $k[[x]]$ are $(0), (x), (x^2), (x^3), \ldots$ PID
Suppose I is an ideal $\neq 0$, $f \in I$, $a_n x^n + a_{n-1} x^{n-1} + \cdots$ n minimal such that $a_n \neq 0$. $f = x^n (\underbrace{a_n + a_{n+1} x + \cdots}_{\text{unit}})$
so $(f) = I$, all elements divisible by x^n

$k[[x]]$ is a UFD. Only prime up to unit is x. Any element $= x^n \times$ unit
Polynmial ring $k[x_1, \ldots, x_n]$ is Noetherian, UFD. Is same true for $k[[x_1, \ldots, x_n]]$?
Try to copy proof of polynomial ring ie, prove if R is Noetherian, so is $R[[x]]$
Problem: The proof for $R[x]$ uses leading coefficients, fails for power series.
Idea: Instead of looking at leading coefficent, deifne $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ where I_0 is the set of constant terms of elements of I, I_1 set of a_1 in terms of form $a_1 x + a_2 x^2 + \cdots$. Then ideal of R, $I_n \subseteq I_{n+1}$ (if $a_n x^n + \cdots \in I_n$, $a_n x^{n+1} + \cdots = x(a_n x^n + \cdots) \in I_{n+1}$). This terminates $I_n = I_{n+1} = I_{n+2} = \cdots$ for some n.
Generators for I: finite set of power series whose constant terms generate I_0, finite set of power sereis $a_1 x + \cdots$ such that a_1 generate $I_1, \cdots$ continue through I_n. This gives a finite set of generators for I
Ex: What does the proof that $R[[x]]$ is noetherian not work for polynomial rings.

If f power series in $k[[x_1, \ldots, x_n]]$ then f is a unit $\leftrightarrow$ constant term $\neq 0$. Ideals very complicated for $n \geqslant 2$
Is $k[[x_1, \ldots, x_n]]$ a UFD? yes. Easy for $n = 1$. Try to copy proof that $k[x_1, \ldots, x_n]$ is a UFD.
R UFD $\to R[x]$ UFD. R UFD does not imply that $R[[x]]$ is a UFD.
Proof fails since we used content. If R ring, Q field of quotients of R, a polynomial $\mathbb{Q}[x]$ $a_0 + a_1 + a_2 x^2 + \cdots + a_n x^n$ can be written as $c(b_0 + b_1 x + \cdots + b_n x^n)$ with $b_i \in R$, c called content of f.
Content for formal power series is not well defined. $R = \mathbb{Z}$, $Q = \mathbb{Q}$ $1 + \frac{x}{2} + \frac{x}{2^2} + \cdots \neq$ (rationals)$\times$ element of $\mathbb{Z}[x]$

Weierstrass Preparation Theorem: Formal power series in several variables over a field
Idea: we can write formal power series as polynomial of one of variables

More precisely, given power series $f \in k[[x, y, z, \ldots]]$, containing x, $f = y^* r(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$, a_i power series in $y_1, y_2, \ldots$ with 0 constant term.

Proof. Do case of $k[[x, y]]$. Draw picture of f

$$\begin{array}{|ccc}
\boxed{a_{n\,0}x^n} & & \\
\vdots & \underline{\qquad\qquad\qquad} & \\
a_{2\,0}x^2 & & \\
a_{1\,0}x & a_{1\,1}xy & \\
a_{0\,0} & a_{0\,1}y & a_{0\,n}y^2
\end{array}$$

Want to keep x^n but make all coefficients outside the box 0.
Problem: multiply f by some unit to acheive this
Step 1: pick smallest coefficent of $x^n \neq 0$ (if not smallest, f is divisble by y so look at f/y). Can assume $f(x) = x^n + \cdots$ no terms in x^i, $i < n$. We have $x^n + a_{n+1\,0}x^{n+1} + \cdots$ multiply by $(1 - a_{n+1\,0})$, unit, to get $(x^n + 0x^{n+1} + \cdots)$. Can repeat this, multiplying by $(1 - *x)(1 - *x^2)(1 - *x^3)\cdots$ well defined power series.
Now, look at $x^n + *x^n y + \cdots$ multiply by $(1 - *y)$ to get rid of y term. Repeating this, move up columns, multiply by infinite products of units to make all above line 0. So we can write $f = y^* \times$ unit $\times (x^n + a_{n-1}x^{n-1} + \cdots)$, decomposition is unique.

Application: Use Weierstrass to show that $k[[x, y]]$ is a UFD.
Key step: If f, is irreducible, f is prime.
Suppose f is irreducible, $f|gh$. By using Weierstrass preparation, can assume f, g, h polynomials in x. We know $fr = gh$ for some r, r must be polynomial in x. So f, g, h polynomials in $k[[y]][x]$ this is a UFD, so $f|g$ or $f|h$ since f is irreducible in $k[[y]][x]$

Warning: If f, g are polynomials in $R[[x]]$ abd $f|g$ in $R[[x]]$ this does not imply that $f|g$ in $R[x]$, consider $f = 1 + x, g = 1$ in $R[[x]]$

Warning: Irreducible polynomials in $k[x, y]$ need not be irreducible in $k[[x, y]]$

Example 4.4.1. $y^2 - x^2 - x^3$, easy to check that irreducible in $k[x, y]$. Factors as $(y + x\sqrt{1+x})(y - x\sqrt{1-x})$, $\sqrt{1-x} \in \mathbb{C}[[x]]$, since $y^2 - x^2 - x^3 = y^2 - (x^2 - x^3) = y^2 - (x\sqrt{1+x})^2$

Warning: Ring of convergent power series of $\mathbb{C}$ is not a UFD, despite being contained between 2 UFDs: $\mathbb{C}[x] \subseteq$ convergent power series $\subseteq \mathbb{C}[[z]]$.
$\sin(x)$, zeros: $0, \pm\pi, \pm 2\pi = x(x - \pi)(x + \pi)(x - 2\pi)(x + 2\pi)\cdots$ cant be expressed as finite product.
Both $\mathbb{C}[z], \mathbb{C}[[z]]$ Noetherian but ring of convergent power series not noetherian.
$I =$ all holomorphic functions vanishing at all but finite # of integers ideal but not finitely generated.
Can also find $I_0 \subseteq I_1 \subseteq I_2 \subseteq$, vanishing on $\mathbb{Z} \subseteq$ vanishing on $\mathbb{Z}\backslash\{0\} \subseteq$ vanishing on $\mathbb{Z}\backslash\{0, 1\} \subseteq \cdots$