Math 120

Taught by Ravi Vakil
Notes by Chris Fifty

Fall 2023

Contents

1 September 27

1.1 Administrative

Course Textbook Abstract Algebra (Dummit + Foote). Homework questions from this book. A new textbook by Nuffi (Notes from the Underground).
Grading: Writing-In-Major Course

- Weekly short online assignments (5%)
- Problem Sets (20%)
- WIM (15%)
- Midterm (20%)
- Final (40%)

1.2 Intro

Several names in mathematics: ask yourself — why is this concept given a name. Why do they deserve a name?

Field (Vector Space)

Abelian Group

Ring Integral Domain and Modules

$\vdots$

Group

What is a Group? An object has symmetries: the ways you can act on an object to get something else (think of changing the sides of a Rubik's cube). Notion that you have an object, and you're doing something to it: symmetries on the objects or the actions on it.

Forget the object—abstract it away—and instead focus on the actions on that object.

Field Acts on Vector Spaces.

Suppose we have a system of 79 linear equations, with 26 unknowns, and there is only one solution that contains π.

$$3a + 4b - 3c + .. + 8z = 42 \qquad \vdots .... = 3$$

Throughout solving these equations, you're dividing, subtracting, and adding integer values, therefore you cannot get π (an irrational number).

Field is what makes linear algebra work.

Examples: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$.

Field. A field k is a set with different operations: $(k, + : k \times k \to k, \times : k \times k \to k, 0 \in k, \exists -a \text{ s.t. } a + -a = 0, 1 \in k \text{ s.t. } 1 \times a = a, \text{associativity, multiplicative inverse}, 1 \neq 0)$. This is a field: a set with many operations defined on it.

Does not need order or completeness (can have an ordered field, but rational numbers are not complete).

2 September 29

2.1 Administrative.

- Read Prelim, 1.1., 1.7, 2.1
- Sunday at noon is the first online assignment (due by midnight)
- Get on canvas.

2.2 Lecture

Field A field is the data of a set $(F, +, \times, 0, 1)$: a set, a binary operation: $F \times F \to F$, binary operation, zero element, and ones element.

Example $\mathbb{R}, \mathbb{Q}, \mathbb{C}$

Group A group $(G, \dot{}, e)$ composed of a (set, binary operation $G \times G \to G$, and an element e) such that:

associativity for every $x, y, z \in G$, $(x\dot{y})\dot{z} = x\dot{(}y\dot{z})$.

0-element/identity : $(e \cdot x) = (x \cdot e) = x$

inverse There exists $a \in G$ such that $a \cdot x = x \cdot a = e$. This necessarily implies the inverse is unique.

Proof. Suppose it is not unique. If a,b satisfy this for a value of x, then $(a \cdot x \cdot b) = a \cdot (x \cdot b) = e \cdot b = a \cdot e$, so $a = b$.

Examples : $(\mathbb{R}, +, 0)$

Abelian Group : A group that is commutative: $x \cdot y + y \cdot x$.

$\to$ $0 \neq 1$

$\to$ For all $a, b, c \in F$, $a(b + c) = ab + ac$

Example $(F, +, 0)$ is an abelian group,

Example $(F \backslash \{0\}, \times, 1)$ is an abelian group.

$\rightarrow$ $(\mathbb{R}, +, 0) = (\mathbb{R}, +)$ also gives us the notion of "-".

$\rightarrow$ $(\mathbb{R}\backslash\{0\}, \times, 1)$ also gives us a notion of division.

Example Invertible $n \times n$ matrices are a group but not an abelian group as invertible matrices are not necessarily commutative!

1. GL(n): general linear group over the field $\mathbb{R}$ or $\mathbb{C}$. Need to define a group over a field.

Example Rotating a sphere in 3D is a group but not an abelian group – the rotations are not commutative: pick a point on the pole and then rotate about this point. Combine with a different operation to show it is not commutative.

- Notice: you pick a point on the sphere and look where it goes.
- A group is an action on the points of the sphere.

Claim: $G_1 \times G_2$ of two abelian groups is an abelian group: where $\times$ is the cartesian product. $(g_1, g_2$ where $g_1 \in G_1$ and $g_2 \in G_2$. Do coordinate-wise operations to maintain abelian group structure. All the axioms are inherited from outer group structure. **Claim:** $(\mathbb{Z}\backslash 3, +)$ is the same group as rotations of a circle by 0, 120, 240. Different ideas, but the group action is the same: isomorphism between these two groups.

- Sets match up.
- Operations are the same.
- Exists mapping between each object in the set, so that group actions on each set maintains this mapping.

3 October 9

3.1 Administrative

- Ravi 4-6 PM MWF

3.2 Lecture: Quotient Groups, The Orbit-stabilitizer Theorem

Definition 1 (Quotient Group)**.** *H is a quotient group of G: $\phi : G \rightarrow H$ is a group homomorphism that is surjective onto H.*

A subgroup is a group homomorphism that is injective, and and isomorphism is a group homomorphism that is bijective.

Example 1 (Example of Quotients)**.**

- $\mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6$

- $\mathbb{R}^6 \to \mathbb{R}^3$ *with a full-rank linear transformation.*
- $GL(n)$ *($n \times n$) invertible matrix $\to$ (via determinant) $\mathbb{R}^x$ gives us a real number [not injective].*
- $GL_{\mathbb{R}}(n) \to \mathbb{R}^x \to \{\pm 1, \times\}$ *[tells us if orientation is is reversed].*

Definition 2 (Addition between Group and element)**.** *Let G be a group and $g \in G$. Then $g + G$ is defined as the set $\{g + g_1, g + g_2, ...\}$ for all elements in G.*

Definition 3 (Cosets of a Subgroup)**.** *$H < G$ and G is an abelian group. Cosets of H are $g + H$ where $g \in G$ (so cosets are subsets of G).*

Example 2. *Say $6\mathbb{Z} < \mathbb{Z}$. Then $0 + 6\mathbb{Z}$ is a coset, $1 + 6\mathbb{Z}$ is a coset, etc.*
$\mathbb{R}^1 \to \mathbb{R}^3$: $t \to (t, 2t, 5t)$ the cosets are the parallel lines with a scalar shift.
$(\mathbb{R}^+, \times) < (\mathbb{R}^\times, \times)$ $1 \times (\mathbb{R}^+, \times)$ is a coset, $(-1) \times (\mathbb{R}^+, \times)$ is a different coset.

Theorem 1. *Given $H < G$ abelian group and $g_1 + H$, $g_2 + H$, then either $g_1 + H = g_2 + H$ or $(g_1 + H) \cap (g_2 + H) = \emptyset$ because $g_1 - g_2 \in H$ or $g_1 - g_2 \notin H$.*

Proof. Suppose $g_3 \in g_1 + H$ and $g_2 + H$. THen $g_3 = g_1 + h_1$ for some $h \in H$ $= g_2 + h_2$. So $g_1 - g_2 = h_2 - h_1 \in H$, so they differ by an element of the subgroup (call it h). That means $g_1 + H = (g_2 + h) + H = g_2 + H$ (because h is already in our subgroup). □

Definition 4. *$H < G$, then cosets of H are G/H (quotient group of H). This is the set $\{g + H | g \in G\}$ = the cosets of H.*

Definition 5 (Orbit)**.** *Let H be a group acting on the set A. Define equivalence relation $\sim$ on A by $a \sim b \iff a = hb$ for some $h \in H$. For each $x \in A$, the equivalence class of x under $\sim$ is called the orbit of x under the action of H. The orbits under the action of H partition the set A into different equivalence classes.*

For example, rotating a sphere 180 degrees is a group action on a set of points so that $a = hb$.

Theorem 2 (Orbit-Stabilizer Theorem)**.** *(Abelian group version) Given an abelian group G acting on a set A and given $a \in A$, $orbit(a) \subset A$. $Stab(a) < G$. Claim: cosets of $Stab(a) < G$: $G/Stab(a)$ are in bijection with $orbit(a)$. This coset $g + Stab(a) \leftrightarrow g \circ a$*

Proof. $g_1 \circ a = g_2 \circ a \iff (g_1 = g_2) \circ a = a$: this is a group action can do these in any order $\iff g_1 - g_2 \in Stab(a) \iff g_1 + Stab(a) = g_2 + Stab(a)$. □

4 October 11

4.1 Administrative

- Problem Set 2 due 10/20.
- Office hours today 4-6 PM

4.2 Lecture

Last time: abelian cosets of a subgroup $H < G$ tile (partition) a group and orbit-stabilizer theorem.

Define a notion of G acting on a set A, and we've defined the Stabilizer of a and the orbit of a for elements $a \in A$. Cosets are of the form $g + H \subset G$. Then the set of cosets effectively tile G: two cosets are either the same or have 0 overlap.

Orbit stabilizer theorem: $g \circ a$ (element of the orbit of a) is in bijection with $g + Stab(a)$. Is a bijection between these two sets: each element is a "set".
$G_1 \to G_2$ homomorphism: map of sets preserving group operations
$G_1 \to G_2$ subgroup: injective map of sets
$G_1 \to G_2$ quotient group: surjective map of sets
$G_1 \to G_2$ isomorphism: bijective mapping of sets.
$G \to G|H$ or $g \to g + H$ is a quotient group.

$\mathbb{Z}/32\mathbb{Z}$ taken the quotient of $8\mathbb{Z}|32\mathbb{Z}$ is $\mathbb{Z}|8\mathbb{Z}$ because $8\mathbb{Z}|32\mathbb{Z}$ is $\mathbb{Z}|4\mathbb{Z}$. $G_1 < G_2 < G_3$ so $G_3|G_1|G_2|G_1 = G_3|G_2$
What are the finite abelian groups of the finite groups?

- $\mathbb{Z}/6$ isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/3$
- $\mathbb{Z}/100 = \mathbb{Z}/4 \times \mathbb{Z}/25$ (some isomorphism between these groups)
- $\mathbb{Z}/60 = \mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/5$

This is called the Chinese remainder theorem:
In the problem set, we saw $1 = 4a + 25b$ via the euclidean algorithm. Given a number mod 4 and mod 25, can we find a number that satisfies these properties?
$\mathbb{Z}/mn = \mathbb{Z}/m \times \mathbb{Z}/n$ if m, n are relatively prime.

$\mathbb{Z}/k$ can be factored into its $\mathbb{Z}/x$ where x is the prime factor raised to the appropriate power.
Suppose $H < G$ and this is a finite abelian group. Then $|H|$ is a factor of $|G|$. This is Lagrange Theorem. Because you can partition G by cosets of H. The size of G is the size of H times the number of cosets of H: $|G| = |H| \times |G|H|$. The quotient group are the individual tiles of the cosets that tile H.
Suppose $g \in G$ with binary operation additon. Then $0, g, 2g, 3g, ...0$ then we have a subgroup isomorphic to $\mathbb{Z}/n$ when it cycles back to 0. If $ord(g) = n$, then ...

Theorem 3. *Suppose G is a finite abelian group and $g \in G$. Then $ord(g)||G|$. The order of any element of G must divide the cardinality of $|G|$.*

Have to get something that matches up, that means a 0 appeared earlier.
Idea behind factoring finite abelian groups:
$G_{100} = G_4 \times G_{25}$. Every element of G_{100} is a factor of 100 (i.e. 2, 5, 10, etc.). $G_2 < G$ is a subgroup of G with elements of power 2^n. Let $G_5 < G$ be elements order 5^n (only intersection is 1). Will use $1 = 4(-6) + 25(1)$

5 October 13

5.1 Lecture: Chinese Remainder Theorem, The Isomorphism Theorem, and Rings

All theorems discussed today are for Abelian groups. **Chinese Remainder Theorem:** $\mathbb{Z}/p^aq^br^c \to \mathbb{Z}/p^a \times \mathbb{Z}/q^b \times \mathbb{Z}/r^c$ if $n = p^aq^br^c$ prime factorization. Main idea: if $|G|$ is a group of size $p^aq^br^c$ then it is isomorphic to $G_p \times G_q \times G_r$. More generally (from the integers), you can break a finite abelian group into pieces.
Once you define abelian groups, what are the finite abelian groups? Can define the finite groups, and then realize you can take products between abelian groups to develop more finite abelian groups.
$\mathbb{Z}/mn$ is a group but not a field: if $m = 2, n = 3$, then $2 \cdot 3 = 0$ which violates the definition of a field as two non-zero elements multiplied together are 0.

The Isomorphism Theorem: Given a group homomorphism $\phi : G \to H$ of an abelian group. $ker(\phi) < G$. Then $G|ker(\phi) \leftrightarrow$ image of ϕ (isomorphism to the image of ϕ). [Also G "mod" the kernel equivalent to the quotient group].
Proof. Orbit-stabilizer theorem. G is acting on H: know e the identity is in H. Orbit of e under the action of G is the image of ϕ that is $G|stab(G)$ that is the kernel.

Action of G on H: $g \circ h = \phi(g)h$, so $g \circ e = \phi(g)e = \phi(g)$ as e is the identity, and this is the definition of the image. Kernel of ϕ is the stabilizer of G.
$g \circ h$ is function composition between $g \in G$ and $h \in H$ which is the group action $\phi(g)$ applied to elements of h: $\phi(g)h$ where this is multiplication.
Example. $\mathbb{Z} \to \mathbb{Z}/6$ via ϕ. Then $ker(\phi) = 6$, so $\mathbb{Z}|6\mathbb{Z}$ is the image of this map: $\mathbb{Z}/6$.
The 3rd isomorphism theorem: [for abelian groups] $J < H < G$, abelian. $(G|J)|(H|J) = G|H$.
The 4th isomorphism theorem: [Lattice] Isomorphism Theorem: G is an abelian group. Let $H < G$. Then you can form a lattice of subgroups. Then all the subgroups of $G|H$ correspond to all of the subgroups containing H: i.e. the groups in the lattice between G and H.
$2\mathbb{Z}|8\mathbb{Z}$ are the even numbers mod 8.

6 October 16

6.1 Announcements

1. Online assignment # 3 due Sunday at noon.
2. Writing in major topic: why you can't double the
3. Read Chapter 7

6.2 Lecture

Important Recent Ideas "Cosets tile the group." $g_1 + H = g_2 + H \iff g_1 - g_2 \in H$ $g_1 + H \cap g_2 + H = \emptyset \iff g_1 - g_2 \notin H$ "Orbit Stabilizer Theorem": Orbit: group acting on a set, and an element of the set. An "orbit" is the set all the points that the point go to under a group action. $G|Stab(a) \leftrightarrow orbit(a)$ $g + Stab(a) \iff g \circ a$

"First Isomorphic Theorem $\phi : G \to H$" $G|ker(\phi) \iff im(\phi)$
$g + ker(\phi) \iff \phi(g)$

"Third Isomorphic Theorem: $K < H < G$"
$(G|K)|(H|K) \to G|H$

"Fourth Isomorphic Theorem: $H < G$
Subgroups of G containing $H \iff$ subgroups of $G|H$.

Understand and be able to replicate the proofs for each of these!

Theorem 4 (Second Isomorphism Theorem)**.** *G is abelian, $A < G$ and $B < G$. Then $A \cap B < G$ and $A+B < G$ where $A+B := \{a+b | a \in A, b \in B\}$. $(A+B)|B$ is isomorphic to $A|(A \cap B)$*

Example: $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 6\mathbb{Z}$ where $A = 2\mathbb{Z}$ (even integers), $B = 3\mathbb{Z}$ (odd integers), $A \cap B = 6\mathbb{Z}$ and $A + B = \mathbb{Z}$. *Proof.* Consider $\phi : A \to (A + B)|B$ and $a \to a + B$. Is this map ϕ surjective? Yes: $a' + b' + B \in (A + B)|B$ and $a' + B$. $a + B = 0 + B$ is the kernel of $A \cap B$. Just use the First isomorphic theorem on $\phi : A \to (A + B)|B$ and then show the kernel of this map is $(A \cap B)$.
Why is it that ϕ is surjective? $a + B = a_1 + b_1 + B \Rightarrow a_1 + b_1 - a \in B$ and $a_1 = a$ makes this true!

Reality Check:
G is an abelian group and $g \in G$. $< g >$ subgroup generated by g with $< g >= .. - 2g, -g, 0, g, 2g, ...$ cyclic subgroup. If g is finite, then $0, g, 2g, ..., 0$ where this span is the order of g which is the order of the subgroup generated by g: $| < g > |$. $< g >= \mathbb{Z}|(| < g > |\mathbb{Z})$.

Lagrange Theorem: Order of g — $|G|$. And moreover if $ord(g) = 6$, $ord(2g) = 3$, $ord(3g) = 2$.

Motivating example: $\mathbb{Z}|6\mathbb{Z} \to \mathbb{Z}|2\mathbb{Z} \times \mathbb{Z}|6\mathbb{Z}$

Theorem 5 (Chinese Remainder Theorem for Finite Abelian Groups)**.** *Suppose G is a finite abelian group with order ab so that a, b are relatively prime. Then we can find integers $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Let $G_a \subset G$ those elements G with $ag = 0$ with $a \in \mathbb{Z}$ and $g \in G$. The elements of G where we add to itself a times and the results is 0. Observe that this is a subgroup: $G_a < G$. and*

$G_b < G$. The order of any element of G_a is a factor of a. Consider $g \in G_a \cap G_b$, then $g = e$ because a, b relatively prime.

$\phi : G_a \times G_b \to G$. $(g_1, g_2) \to g_1 + g_2$. What is the kernel of ϕ? $g_1 + g_2 = 0$ so $g_1 = -g_2$ Therefore, must be the identity: $g_1 = g_2 = 0$.

Claim: ϕ is surjective. For any element $g \in G$, $g = g_1 + g_2$ where $g_1 \in G_a$ and $g_2 \in G_2$.

$g = 1 \cdot g = (ax + by)g = a(xg) + b(yg) = b(yg) + a(xg)$.

Then by the first isomorphic theorem, $G_a \times G_b \to G$ because the kernel is the identity.

6.3 October 23

6.4 Administrative

1. Midterm on Monday.
2. Midterm in class (shorter).
3. Nov. 10: writing in the major assignment [will be on canvas].
4. Final version due after Thanksgiving on week 9-10.
5. Feedback after Nov. 10 draft [highly recommend].

Writing in the major assignment: Straight edge + compass $\Rightarrow$ reduced it to if you start with two points on the plane, and then make a coordinate system, and then start constructing points, what points can you construct? Know exactly which points on the plane you can construct: (a, b) such that $a, b \in K$, the field of constructable numbers. K is the smallest subfield of the real numbers that is closed under square roots.

K :=smallest subfield of $\mathbb{R}$ closed under square roots.

Want to show the following things: $\cos 20$, $2\sqrt[3]{2}$, $\sqrt{\pi} \notin K$. Trisecting an angle, doubling a circle, not in K.

Warmups: $\sqrt{7}$ is not rational. Assume it is rational: $\sqrt{7} = \frac{u}{v}$ such that u, v relatively prime. $7v^2 = u^2$ therefore $7|u \to 7|v$.

Another way $x^2 - 7 = 0$ $\frac{u}{v}^2 - 7 = 0 \Rightarrow u^2 = 7v^2$ so $u = \pm 1, \pm 7$ and $v = \pm 1$, plug these in and none work.

If $u, v \in \mathbb{Q}$ and $u + v\sqrt{7} = 0$, then $\sqrt{7} = -\frac{u}{v}$ is rational, so this can't happen (unless $v, u = 0$ because you can't divide by 0).

3) $\overline{u + v\sqrt{7}} = u - v\sqrt{7}$. Question: $u + v\sqrt{7}$ where $u, v \in \mathbb{Q}$, and $\mathbb{Q}(\sqrt{7}) = \{u + v\sqrt{7} | u, v \in \mathbb{Q}\} \subset \mathbb{R}$. Claim: is a field.
Missing: multiplicative inverse. $\frac{2+\sqrt{7}}{3+19\sqrt{7}} = ? + ?\sqrt{7}$ if it is a field. Solve by multiplying by 1 (complex conjugate). Don't need to show that it has a zero divisor since $ab = 0 = a^{-1}ab = 0 \Rightarrow b = 0$

Conjugation : $\mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}(\sqrt{7})$ conjugation gives an isomorphism of a field with itself. Only works when you have the square root of something not in your field, but the number in the square root in in your field: $\sqrt{4}$ or π don't work.

New field: $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{1 + \sqrt{5}})$. Already it's in the field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$, or it's a bigger field containing all of $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{1 + \sqrt{5}})$.

$\mathbb{Q}(\sqrt{5}, \sqrt{7})$ contains $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt{35})$.

Fact: $\cos 20$ is a root of $x^3 - \frac{3}{4}x - \frac{1}{8} = 0$.
$\cos 20$ is not rational because if it were $8x^3 - 6x - 1 = 0$, and if $x = \frac{u}{v}$ u, v relatively prime, then plugging in this value into the equation would give us $8u^3 - 6uv^2 = v^3$, and therefore, $u = \pm 1$ must be a factor of both left and right side. Similarly, $8u^3 + v^3 + 6uv^2$, so v is a factor of both the left and right side, so $v = \pm 1$ or ± 2. Therefore, no solution in $\mathbb{Q}$.

Maybe, there is a solution that looks like $a + b\sqrt{7}$ a root? Maybe there is a solution like this with $ak, b \in \mathbb{Q}$. Then when you plug in $a + b\sqrt{7}$ into x, you get 0. And you can flip the signs of the $a + b\sqrt{7} \Rightarrow a - b\sqrt{7}$ to get another root! And it's different because $b \neq 0$. So now you've found two roots, but the final root is $-2a$, a rational number, therefore no solution.

Also no solution $a + b\sqrt{5}$ where $a, b \in \mathbb{Q}(\sqrt{7})$. No root when you add root 7, root 5, so on and so forth. No root where you have finitely many square roots in it. Therefore, you cannot write $\cos 20$ so you can't trisect an angle. Same proof shows you can't double a ....

π is transcedental, and anything you can construct is a polynomial. Hard separate fact.

7 October 25

7.1 Administrative

1. Midterm on Monday.

2. WIM: two deadlines. First deadline; Nov. 10 [bonus office hours are after the midterm].

7.2 Lecture: Return to Rings

Definition 6 (Ring). *$(R, +, 0, \times, -)$: a set with a binary operation $+$ that gives it the structure of the abelian group with 0 as an identity. Moreover, $\times$ is a second binary operation that is commutative with multiplicative identity 1. Moreover, the distributive law holds. This definition differs from the course textbook.*

Ring homomorphism: $\phi : R \to S$ as well as an isomorphism (bijection).
Quotient ring: $\phi : R \to S$ surjection.
Subring $\phi : R \to S$ injection. [Our subrings need a 1 because our ring has a 1 vs. textbook does not require a 1].

Integral domain: If $xy = 0$, then $x = 0$ or $y = 0$ [no zero divisors].

Example 3 (Examples of Rings). *1. $\mathbb{Q}(i) \subset \mathbb{C} := \{a + bi | a, b \in \mathbb{Q}\}$. In fact, this forms an integral domain $\Rightarrow$ field.*

2. $\mathbb{Z}[i] \subset \mathbb{C} = \{a + bi | a, b \in \mathbb{Z}\}$ is also a ring.

3. $\mathbb{Z}[\pi] = \{a_0 + a_1\pi + ... + a_n\pi^n | a_0, ..., a_n \in \mathbb{Z}\} \subset \mathbb{R}$. π is transcedental, so 0 polynonial is all zeros. $\cong \mathbb{Z}[t]$ [all polynomials with integer coefficients].

Given $\phi : R \to S$ ring homomorphism. Define $Im(\phi) \subset R$ is a ring. $\mathbb{Z}[t] \to \mathbb{R}$ has an image that is a ring.

$kernel(\phi) \subset R$ where $ker(\phi) := \phi^{-1}(0) \subset R$. This is (in general) not a subring: $1 \notin ker(\phi)$ in general. But the kernel is a subgroup: $(ker\phi, +, 0)$.

Example 4 (Examples of Ring Homomorphisms). *1. $\mathbb{Z}[t] \to \mathbb{R}$ and $t \to \pi$. $ker\phi = 0$*

2. $\mathbb{Z}[t] \to \mathbb{R}$ and $t \to \sqrt{2}$

3. $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ $\mathbb{R}[x] \to \mathbb{R}$ $n \to n \mod 6$. $ker\phi = 6\mathbb{Z}$ [multiples of 6].

4. $\mathbb{R}[x] \to \mathbb{R}$ with $f(x) \to f(y)$. $0 \in ker(\phi)$, $\{(x-1)f(x)\} = ker\phi$ — anything of the form $(x-1)f(x)$ is in the kernel.

5. $\mathbb{R}[x, y] \to \mathbb{R}$ with $f(x, y) \to f(0, 0)$ $ker\phi = 0 + ?x + ?y$.

Definition 7 (Ideal). *Every kernel $I = ker\phi$ has the following 2 properties: $I \subset R$ is an ideal of R if (1) $(I, +, 0)$ is an abelian subgroup of $(R, +, 0)$ (2) For every element $x \in I$, $a \in R$, $a \times x \in I$: $aI \subset I$ – multiply any element in ideal*

by an element in your ring, and that element is in the ideal.

For example, any multiple of 6 multiplied by any other integer remains an integer of 6.

Claim: Given a ring homomorphism, and given $x \in R$ with $\phi(x) = 0$, and $a \in R$, then $\phi(ax) = 0$.
Proof: $\phi(ax) = \phi(a)\phi(x) = \phi(a)0 = 0$.
Moreover, any ideal is a kernel.

If $I \subset R$ is an ideal, then you can "quotient" by I. Define the quotient ring: R/I. Given $(R, 0, +, \times, 1)$, we are going to produce something new R/I.

I is a subgroup of R, so $(R/I, 0, +)$ is a subgroup. Then the questions are what to multiply and what the unit is.

Multiplication is defined by $(x + I)(y + I) = (xy + I)$. Is it well-defined? $x + I = x' + I$ and $y + I = y' + I$, is it true that $xy + I = x'y' + I$? If $x - x' \in I$ and $y - y' \in I$, is it true that $xy - x'y' \in I$?

$x - x' = i \in I$ and $y - y' = j \in I$, is it true that $xy - x'y' \in I$? $xy - x'y' \in I$? $xy - x'y + x'y - x'y' = (x - x')y + x(y - y') = iy + xj \in I$ because anything times the ideal is in the ideal.

8 October 27

Midterm: Goes until 7.3: quotienting by ideals. Know the isomorphism theorems and how to use them. First isomorphism theorem is special case of orbit-stabilizer theorem. Also know the chinese remainder theorem for abelian groups, and know why it's true.

Chinese remainder theorem: for abelian groups, $\mathbb{Z}/6 \to \mathbb{Z}/6 \times \mathbb{Z}/3$.
There will be a trivial euclidean algorithm question. Will not be asked to know the constructable things. Section 4.1: permutations is not really necessary.Do not need non-abelian groups: like normal subgroups. No reference sheet on the midterm: know orbit-stabilizer, subgroup test, etc. Will need to know about polynomial rings.

Last time: $I \subset R$ and S quotient rings that correspond to each other. Ring mod an ideal is a quotient ring. A map from a ring to a quotient ring has a kenrel that is an ideal.

First isomorphism theorem: $\phi : R \to S$. Then $R/ker\phi \cong im\phi$ with isomorphism $r + ker\phi \iff \phi(r)$.

Fourth Iso Theorem for Rings: can make a diagram of ideals for the ideals in a ring. If you write the corresponding ideals of R/I, then all the ideals between R and I will match perfectly with the lattice structure between R/I and 0. In particualr, if there is an ideal J between R and I, there is a quotient group J/I between R/I and 0. In particular, $R/J \cong (R/I)/(J/I)$. You can quotient groups by subgroups, but you can't necessarily quotient rings by subrings.

Field of Fractions: Suppose R is an integral domain (i.e. $\mathbb{Z}, \mathbb{R}[x], etc.$). Consider $\frac{a}{b}$ with $b \neq 0$ for any two elements in our integral domain. Then define equivalence $\frac{a}{b} = \frac{c}{d}$ if $ad - bc = 0$. Define Fraction Field of a ring $FF(R) = \frac{a}{b}$ with $b \neq 0$ and $\frac{a}{b} = \frac{c}{d}$ if $ad - bc = 0$.

Several things to worry about: if $\frac{a}{b} = \frac{c}{d} = \frac{e}{f}$ then is $\frac{a}{b} = \frac{e}{f}$, is $af = be$? Can use integral domain to show this rigorously.

We also need to show its a field.
Define $\frac{a}{b} \times \frac{c}{d} = ..$, $\frac{a}{b} + \frac{c}{d} = ...$ and verify these are well-defined for a field. Verify 1 sits inside the Fraction Field, and $1 \neq 0$ because in our integral domain $1 \neq 0$. We can also invert: $\frac{a}{b} = \frac{0}{1} \iff a = 0$. To make all this work, there's things that we need to check (but we don't need lowest terms!!).

9 November 1

Ideals: $I, J \subset R$, then $I \cap J$ is an ideal where I, J is an ideal and R is a ring.

However; $I \cup J$ is not necessarily an ideal. Example: multiple of 2 and multiple of 3 $2\mathbb{Z}$ and $3\mathbb{Z}$, but the union of these two sets is not an ideal. This is not closed under addition as we can take 2 from $2\mathbb{Z}$ and 3 from $3\mathbb{Z}$, but $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Generated ideal: $x \in R$, (x) is an ideal $= \{rx\} \subset R$. Similarly, an ideal can be generated by finitely many things: $(a_1, ..., a_n) = \{r_1a_1 + ... + r_na_n \in R\}$.

$I + J$ is an ideal, but it's unclear if you can take an arbitrary sum.

Definition 8. $(a_i)_{i \in S} = \{r_1a_1 + r_2a + 2 + ...$ *where* $r_i \in R\}$ *where almost all coefficients are zero (all but finitely many coefficients are zero). Only finitely many sums are allowed because of our definition. Want an ideal that contains every* a_i*: take all ideals that contain* a_i *and then intersect them all: this is an ideal.*
Two equivalent: have a bunch of generators $\{a_i\} \subset R$*. Consider all ideals containing* $\{a_i\}$*. Then take the intersection of all the ideals containing* $\{a_i\}$ *is an ideal:* $\cap I$*.*

Definition 9 (Prime Ideal)**.** *An ideal* $P \subset R$ *is prime if* R/P *is an integral domain.*

If $x, y \in R/P$ and $xy = 0$ in R/P, then either x or y is 0 in R/P. In the book, this is equivalently written as if $xy \in P$, then $x \in P$ or $y \in P$.

Definition 10 (Maximal Ideal)**.** *An ideal $M \subset R$ is maximal if R/M is a field if and only if $M \neq R$ and there does not exist an ideal Z $M \subset Z \subset R$ [no ideal in between M and R).*

$\Rightarrow k = R/M$ is a field. Ideals of k are k and (0). Then by the fourth isomorphism theorem, then there are no ideals between M and R.

$\Leftarrow$ if $S = R/M$ has no ideals, other than S and 0, why is it a field? Note that $S \neq 0$. Need to check that everything besides 0 is invertible to verify S is a field.

Question: if $a \in S$, $a \neq 0$, how do you know that a is invertible? How do you know that there is some multiple of a, $s \in S$ such that $sa = 1$. How do you know that 1 is a multiple of a: $1 \in (a)$?

Aside: Every ring $R \neq 0$ has a maximum ideal. This is equivalent to the axiom of choice.

Axiom of Choice: [also known as Zorn's Lemma].

Integral domain / Field: A new field! Elements are ordered pairs of integers $(a, b) \in \mathbb{Z}$ such that $b \neq 0$ and $(a, b) = (c, d)$ if $ad = bc$ [two points are the same if there's a line through the origin connecting them].

Declare $0 \in F$ to be the vertical line: $(0, a)$ for $a \in \mathbb{Z}$.

Declare $1 \in F$ to be $(1, 1) = (2, 2) = (a, a)$ for any $a \neq 0$: the perfectly diagonal line in $\mathbb{Z} \times \mathbb{Z}$.

Define addition: $(a, b) + (c, d) = (ad + bc, bd)$
Define multiplication $(a, b) \times (c, d) = (ac, bd)$

As a check, we need to ensure two elements from the same equivalence class yield identical results as $(1, 1) = (7, 7)$. Need to check if $(a, b) = (a', b')$ then $(ad + bc, bd) = (a'd + b'c, b'd)$.

Clearly, this is $(a, b) = \frac{a}{b}$ and $F = \mathbb{Q}$. Therefore, the rational numbers do indeed form a field. We really didn't use much about the integers to make this work.

More generally, $a, b \in \mathbb{Z}$, $b \neq 0$, $a, b \in$ an integral domain, $b \neq 0$. Then this will still work if in an integral domain rather than $\mathbb{Z}$.

Even more generally $a, b \in R$ integral domain, then $b \in S$ $S \subset R$ that is closed under multiplication.

Example: $R = \mathbb{Z}$, $S = \{1, 2, 2^2, ...\}$. Fractions with denominators a power of 2. Also all non-zero integers that are odd: $S = \{1, 3, 5, 7...\}$.
Covered everything up to 7.5, and we've already done the Chinese Remainder Theorem.

10 November 3

Chinese Remainder Theorem: $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (rings).

What's in common? $gcd(2, 3) = 1$ so $\exists a, b \in \mathbb{Z}$ such that $2a + 3b = 1$. Can also say this in terms of ideals: the ideal generated by 2,3 is the unit ideal $\mathbb{Z}$ and $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$. These three statements are equivalent.

More generally, want to do this with an arbitrary ring R.

Definition 11. *R ring, $I, J \subset R$ ideals. We say I and J are* ***comaximal*** *if $I + J = R \iff \exists i \in I, j \in J$ such that $i + j = 1$.*

Proposition 1. *If $I, J \subset R$ are comaximal, then $IJ = I \cap J$*

Proof:
($\Rightarrow$) $IJ = (ij)$ the ideal generated by elements in the first ideal times elements in the second ideal. i.e. $R = R[x, y]$, $I = (x, y)$ and $J = (x^2, y)$, then $IJ = (x^3, x^2y, xy, y^2)$.

Take any $a \in I$ and $b \in J$, then $ab \in I \cap J$.

($\Leftarrow$) take $c \in I \cap J$. $c = (i+j)c$ because $(i+j) = 1$ for some i, j, and $ic+cj \in IJ$ as $ic \in I$ and $cj \in J$.

Theorem 6 (Chinese Remainder Theorem for 2 ideals)**.** *R is a ring. I, J are co-maximal ideals.*
$R/(IJ) \cong R/(I \cap J) \cong R/I \times R/J$

Proof: Consider the ring homomorphism: $\phi : R \to R/I \times R/J$ by the first isomorphism theorem. $R/ker\phi \cong im\phi$. The kernel of $\phi = I \cap J$. Image is all of $R/I \times R/J$ as ϕ is surjective.

Claim $R \to R/I \times R/J$ is surjective: given any $s + I$ and $t + J$, $s, t \in R$. Then $\phi() = (s + I, t + J)$ for some input of ϕ. and that input is $(js + ti)$ as $(js + ti)$ mod $I = (js + ti + is) = s(i + j)$. Therefore, this is surjective.

Theorem 7 (CRT (3 ideals))**.** *R is a ring. I, J, K are ideals that are pair-wise co-maximal.*

$R/(IJK) \cong R/(I \cap J \cap K) \cong R/I \times R/J \times R/K$.

Proof: Use 2-ideal case: $R/IJ \cong R/(I \cap J) = R/I \times R/J$. All you need to show is that $IJ + K = R$ or $I \cap J + K = R$. Which means that $R/IJK \cong R/IJ \times R/K \cong R/I \times R/J \times R/K$.

Claim: Suppose $I + J = R$, $I + K = R$, $J + K = R$. Then WTS either $IJ + K = R$ or $I \cap J + K = R$ (actually the same). $I + J = R$, ... $\Rightarrow i_1 + j_1 = 1$, ... $i_2 + k_2 = 1$ and $j_3 + k_3 = 1$. Therefore, $i_1 + j_1 - (i_2 + k_2) + j_3 + k_3 = 1$ Therefore, $(i_1 - i_2) + (j_1 + j_3) + (k_3 - k_2) = 1$. So something in I + something in J + something in $K = 1$.

Corollary 1. $(\mathbb{Z}/100)^\times \cong (\mathbb{Z}/4)^\times \times (\mathbb{Z}/25)^\times$
$(R/IJ)^\times \cong (R/I)^\times \times (R/J)^\times$

11 November 6

Last Time Rings. Now we're finishing Chaper 7 completely. There are several main concepts including the Chinese Remainder theorem for Rings.

Know about the unique factorization of positive integers: a positive integer that is not 1 can be factored uniquely into primes. Why is that true? Once we say this correctly, we will have a better view. This concept generalizes to arbitrary algebraic structures.

Euclidean Algorithm [Generalized to non-integers] Suppose we have a ring R (i.e. $\mathbb{Z}$) that is an integral domain: $xy = 0 \iff x = 0$ or $y = 0$. You also have $k[t]$ polynomials over a field as an integral domain.

We also have a **notion of size**: $\mathbb{R}\backslash\{0\} \to \mathbb{Z}$.
$\mathbb{Z} \to \mathbb{Z}$ via $x \to |x|$
$k[t] \to \mathbb{Z}$ via $p(t) \to \deg(p(t))$.

Given any $a, b \in R$ and $b \neq 0$, then $a = qb + r$ wiht $q, r \in R$ and $|r| < |b|$. Where $|b|$ is ...

For $\mathbb{Z}$: $ax + by = d$ where d is the "smallest".

$Ideal(a, b) \subset R$, $(a, b) = d$ where $d = gcd(a, b)$.

Polynomials: $k[t]$: how to divide one polynomial by another and get a quotient (long division of polynomials.

Need: Euclidean norm: $|R| \to \mathbb{Z}^{\geq 0}$ via the $\{\}$ map where $|r| < |b|$ in Euclidean Algorithm.

Euclidean Domain: The thing you need for this to work.

Def of Norm: $|xy| = |x||y|$.
Another Example: [Gaussian Integers] $a+bi$ where $a, b \in \mathbb{Z}$. $|a+bi| = a^2+b^2$.

What is q? If you have $\alpha, \beta \in \mathbb{Z}[i]$, how to find q, r? $Q(i) : c+di$ where $c, d \in \mathbb{Q}$ with $\mathbb{Q}$ as a field. Consider $\frac{\alpha}{\beta} = c+di$. Take $q \in \mathbb{Z}[i]$ with $|q - \frac{\alpha}{\beta}| \leq \frac{1}{\sqrt{2}}$, so $r = \alpha - q\beta \in \mathbb{Z}[i]$. Hope is that $|r| < |\beta|$. $|r| = |\alpha - q\beta| < |\beta|$.

Consider $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, then $\alpha = q\beta + r$ where $q, r \in \mathbb{Z}[i]$ and $|r| < |\beta|$.

$gcd(10+3i, 14-i)$ allows you to fin the gcd of these values: $(3+i)+(-1)(3) = i$ but can massage this to get to 1 because they differ by a unit: (multiply by i^3).

Two elements of a ring are associates if $x = unit \times y$ or equivalently $y = unit \times x$ or equivalently $(x) = (y)$ [ideal generated by x is equal to the ideal generated by y] $\Rightarrow x = uy$ where u is a unit. Similarly $y = vx$ where v is a unit. Therefore $x = uvx$ so $uvx - x = 0$ and $x(uv - 1) = 0$ and $x \neq 0$ as we're in an integral domain so $uv = 1$.

Midterm Stats:
Out of 50 [maximum possible socre].
≤ 20: How to spend your time to improve.
≥ 20: doing fine-well.
≥ 25: really good.
≥ 30: fantastic.
Question 5: Tough
Look at what you understand, look at what you didn't understand. Learn the lessons + understand the cases as well.

12 November 10

Euclidean Algorithms
Integral domains R. $N : R \to \mathbb{Z}^{\geq 0}$.
Positive norm: Euclidean algorithm $a = qb + r$ where r is smaller than b.
Claim: Euclidean Domains $\Rightarrow$ Principal Ideal Domains. Every ideal is principal. *Proof:* $I \subset R$. If there is a non-zero element. Take an element of smallest non-zero norm.

Claim: $I = (b)$ (ideal is generated by b). $I = (b) \to (b) \subset (b)$.

If $a \in I$, $a = qb + r$.

Unique Factorization: Let R be an integral domain. $r \in R$ could be 0 or a unit u: $(u) = R$ exists, then $uv = 1$.

If r is not 0 or a unit, say r is irreducible. If whenever $r = st$, then s or t is a unit. i.e. $5 \in \mathbb{Z}$ or $-5 \in \mathbb{Z}$.

Every element of the ring is *irreducible* or *reducible*.

Definition 12 (prime)**.** *r is prime if (r) is a prime ideal.*

This is not the same thing as irreducible. For example, $-5 \in \mathbb{Z}$ is prime.
If $xy \in (r)$, then $x \in (r)$ or $y \in (r)$. Can't prove that one implies the other in a general integral domain.

Definition 13. *r,s are **associates** if $r = unit \times s$ or equivalently $(r) = (s)$.*

Claim: If p is prime, then p is irreducible. $p \in R$ integral domain. *Proof:* (p) is a prime ideal. $p = ab$. Goal a or b is a unit.
$a, b \in (p)$, so $a \in (p)$ or $b \in (p)$. Say $a \in (p)$. $a = kp$. $p = kpb \iff kpb - p = 0$ so $p(kb - 1) = 0$. Because we're in an integral domain $kb = 1$.

Note: In a pid (principal ideal domain), irreducibles are prime. *Proof:* Suppose r is irreducible. If $r = ab$, then a or b is a unit.

Suppose $ab \in (r)$. Why is $a \in (r)$ or $b \in (r)$? i.e. $ab = kr$.

Why can you write that a is a multiple of r or b is a multiple of r?

Define: Unique factorization domain.
Suppose R is an integral domain. We say R is a unique factorization domain if for every element $r \in R$, $r \neq 0$ or a unit, can write $r = p_1 \times p_2 \times .. \times p_n$ the product of primes in R where n is finite.

For any other prime factorization, $r = q_1 \times q_2 \times ... \times q_n$, then $m = n$, but $p_i \neq q_i$ necessarily (i.e. $6 = 2 \times 3 = (-2) \times (-3)$). The products are the same up to units.

Examples without unique factorization $\mathbb{Z}[2\sqrt{3}] = \mathbb{Z}[\sqrt{12}] = a + b\sqrt{12}$
$(a + b\sqrt{12})(a - b\sqrt{12}) = a^2 - 12b^2$.
$\sqrt{12} \times \sqrt{12} = 12 = 2 \times 2 \times 3$.

$\mathbb{R}[w, x, y, z]/(wz - xy)$ is an integral domain. $wz = xy$ in this integral domain.

$x^n + y^n = z^n$ has no solution in the integers?
Would love to factor this: $x^n = z^n - y^n$. If $n = 2$, then difference of squares.

$\mathbb{Z}[\zeta]$ n^{th} root of 1.
$x^n = (z - y)(z - \zeta y) \cdot \cdot (z - \zeta^{n-1} y)$. Is this a unique factorization domain?

Every prime number is irreducible because you can only factor it into itself (in a unique factorization domain).

In a principal ideal domain, every prime is irreducible (and this is also the case in a unique facotrization domain).

WTS: every euclidean domain is a principal ideal domain and every principal ideal domain is a unique facotrization domain.

Fields are examples of Euclidean domains which are examples of PIDs $\subseteq UFD \subseteq Integraldomain \subset Rings$.

Theorem 8. *Suppose R is a principal ideal domain. Then R is a unique factorization domain.*

Proof: Suppose $r \in R$ and r is not 0 or a unit. First goal: find a factorization. $r = r_1 r_2 = r_1 ....$ to factorize. So what can go wrong? How do you know it terminates if you have no notion of size? $(r) \subset (r2) \subset (r4) \subseteq (r6) \subseteq ..$ In other words, r is a multiple of r2, r2 is a multiple of r4, ...

Consider the union $\cup(r_{2n})$. An element of this union is a multiple of r_{kn} for some k even. The trick is that Emmy Noether: this is an ideal, and every ideal is principal, so it's generated by a single element (s). So (s) is in r_{2n} for some n. THe ideals can't get any bigger once you reach a certain step.

13 November 13

Groups in General: [Chapter 2]
$(G, \cdot, e)$ where G is a set, $\cdot$ is a binary operation, and e is an identity element. $\cdot$ is associative. $\forall x \in G$, $x \cdot e = x$. $\exists y \in G$ such that $\forall x \in y$, $y \cdot x = x \cdot y = e$. **this left inverse is equal to the right inverse.**

$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. Need to check: $(x \cdot y)^{-1} \cdot (y^{-1} x^{-1})$ and then rearrange parentheses.

Examples of non-abelian groups: $GL_n(F)$.

Symmetric Group: S_n on n numbers. [Permutation group]. What is an element of the permutation group? How do you describe the elements and how do you multiply them?

Consider S_5: π is a permutation on 5 elements. How to compose them? The following definition is a communal choice: $\pi_1(\pi_2(x))$ apply π_2 first. Can write this in *cycle notation* for the elements of the group: $(1)(2,4)(3)(5)$ [2 goes to 4] or simply write the elements that change for simplicity $(2,4)$. Or for S_{100}

$g = (3, 9, 1, 0)(2, 4, 8, 7)(x)$.

$(12) \cdot (13) = (132)$ and $(13) \cdot (12) = (123)$.

$S_{3000}(12)(13) = (132) = (321)$ 1 goes to 3, 3 goes to 2. First function sends 1 to 3 and second function keeps 3 put. Second function sends 1 to 2. So if we start with 1 we have: $1- > 3$ followed by $3- > 3$ and then $3- > 1$ and finally $1- > 2$ if we continue to apply this to elements to get a cycle. Therefore the full thing is (132).

Composition of Symmetric groups: $(2, 3, 7, 9)(10, 1, 8)$ is equivalent to $(1, 8, 10)(2, 3, 7, 9)$. What is the inverse? $g^{-1} = (10, 8, 1)(9, 7, 3, 2)$.

$(12)(345) = g^{-1}$ and $(12)(543) = g$.
$g^{-1}(2598)(67)(1, 11)g$: this is called conjugating by g.
starting at 1 we get $(1398)(2, 11)(4)(5)(67)(2, 11)$.

The patter is to simply apply elements on the left cycle to things in the middle.
i.e. $(132)(98)(1547, 10)g =¿$ (35479)?
Now know how to do $g^{-1}\sigma g$ or in matrix notation: $M^{-1}NM$. Alternatively: $g\sigma g^{-1}$ and MNM^{-1} [change of basis]. Change of basis is conjugation.

14 November 15

Today: Group actions, normal subgroups, quotients, orbit-stabilizer, First-Isomorphism theorem.

Dihedral Group: The symmetries of a regular n-gon. D_{2n}, or D_{10} as the symmetries of a pentagon. You can rotate it or you can flip it. If you label the vertices $1-5$ for a pentagon, then $D_{10} < S_5$, and we can selectively permute the vertices with rotations or flips of the vertices. This group has size $2n$ because there are n rotations and 2 reflections for each rotation.

r, s generate D_{2n} where $r = (12345)$ and $s = (25)(34)$. So composing r and s allow us to compose this gorup (i.e. any rotation and/or reflection).

For instance: s, sr, ..., sr^{n-1}, e, r, r^2, ..., r^{n-1} are the 10 elements of the group, and any composition of them maps back to one of these elements.

Example: $rs = sr^{-1}$ [see this geometrically]. and $srs^{-1} = r^k$, $s^2 = e$ and $r^n = e$. The generators r, s satisfy these relationships. Claim: using any set of s, r, we can turn it into one of the 10 unique combinations of r and s. Groups often have these nice relations from which you can get everything.

Subgroups and Cosets. $H < G$, we can have left cosests or right cosets. gH is not necessarily Hg.

Example: $G = S_3$ and $H = \{e, 112)\}$. $(23)H = \{(23), (23)(121)\}$ and H$(23) = \{(23), (12)(23)\}$.

Set of left coset is denoted as G/H and set of right coset is denoted as $H\ G$.

Theorem 9. *Suppose $H < G$ and $g_1, g_2 \in G$. Then it could be that $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$. Must tile the group – no overlap.*
Further, $g_1H = g_2H \iff g_1^{-1}, g_2 \in H$ xor $g_1^{-1}g_2 \notin H$.

$g_1H = g_2H$ if these are completely the same subset, then $g_1^{-1}g_1H = H = g_1^{-1}g_2H$, so these two are the same subsets of G. $e \in H$, so $g_1^{-1}g_2e \in H$ and $g_1^{-1}g_2 \in H$.

Suppose $g_1H \cap g_2H = \emptyset$. Then $H \cap g_1^{-1}g_2H = \emptyset$ but $e \in H$, so so $g_1^{-1}g_2 \in g_1^{-1}g_2H$, so $g_1^{-1}g_2 \notin H$.

Now suppose $x \in g_1H \cap g_2H$. Then $x = g_1h_1$ for some $h_1 \in H$ and $x = g_2h_2$ for some $h_2 \in H$. Then $g_1^{-1}g_2 = h_1h_2^{-1} \in H$.

Corollary 2. *The **left** cosets tile the group. The **right** cosets tile the group in a different way.*

If $|G|$ is finite. Then $|G| = |H|/|G/H|$

Corollary 3 (Lagrange's theorem.)**.** $|G| = |H|/|G/H|$. *$|G/H|$ is called the index of the subgroup. Moreover, any group of size p prime is isomorphic to $\mathbb{Z}/p$.*

Group Actions G acting on a set A.
New axioms! Same thing as a group homormorphism from $\phi : G \to S_A$. Whenever you have a group action, this is equivalent to a group homomorphism mapping g to elements of the permutation group S_a. One group action permutes the elements in the set in some way/shape/or form.

Could not say this before because S_A is the symmetric group: the group of permutations on the set (and the set may not be finite).

15 November 17

Tiling Theorem. $H < G$. $g_1, g_2 \in G$. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$. This is equivalent to either $g_1^{-1}g_2 \in H$ or $g_1^{-1}g_2 \notin H$.

Group Action. Group G acting on a set A. The kernel of the action is equivalent to the kernel of the group homomorphism: $\phi : G \to S_A$ $ker\phi$.
Orbit-Stabilizer Theorem. Group G acting on a set A. So we immediately have a homomorphism $\phi : G \to S_A$.

There is a bijection $G/Stab(a)$ with orbit(a) given by $g(Stab(a)) \iff g \circ a$.
Proof. Perhaps [two cosets of Stab a] $g_1Staba = g_2Staba$ ... $= g_1 \circ a = g_2 \circ a \iff g_1^{-1}g_2 \in Staba \iff (g_1^{-1}g_2) \circ a = a \iff (g_1^{-1}) \circ (g_2 \circ a) = a \iff (g_1)(g^{-1}) \circ g_2a \iff g_2 \circ a = g_1 \circ a$.

Group Surjection Subgroups: $ker\phi : G \to H$ via ϕ. $N \to G$. Can I make $G \to H$?

Given: $ker\phi$: $G \to H$ via b. $G/ker\phi$.

More generally, given $G \to H$ between groups with ϕ, $ker\phi$ is a subgroup. G is a action on H. $G \times H \to H$. $(g, h) \to \phi(g)h$.

G acting on H. $orbit(e_H)$ [orbit of the identity of H] is the image of ϕ. What's the stabilizer of e? What are the elements of g that send e to e. The kernel of ϕ is the stabilizer of e: $ker(\phi) = Stab(e_H) = \{g \in G | g \circ e_H = e_H\}$.
Given any group homomorphism, you get an action of G on H (where the action of G on the set of H).
Orbit stabilizer. Bijection of sets with $G/ker\phi \iff im\phi$. In particular, $g(ker\phi) \iff \phi(g)$.

What is the group structure on $G/ker\phi$? Want $g_1(ker\phi) \cdot g_2(ker\phi) = g_1g_2(ker\phi)$. Want to define a group structure on the quotient set. Once we answer this, we have the first iso theorem.
Given $H < G$, want a group structure on G/H.

Important Definition [new thing]: We say a subgroup $N < G$ is normal [i.e. quotientable] if for all pairs of elements $g \in G$; $gN = Ng$ [left coset is equal to the right coset]. Equivalent to $gNg^{-1} = N$. Equivalently, for all $n \in N$, $gng^{-1} \in N$.
Write this as $N \triangleleft G$.

Example: $G = S_3$ [smallest non-abelian group]. $H = \{e, (12)\}$ is a two-element non-normal subgroup. Consider (123): $(123)H = \{(123), (13)\}$. Also consider $H(123) = \{(123), (12)(123) = (1)(23)\}$.

Moreover, find g such that $g(12) \neq (1, 2)g$. or equivalently $g(12)g^{-1} \neq (12)$.

Subgroups that are normal: $\{e\}$ and $H = G$ and $H = \{e, (123), (132)\}$. Last one has 2 cosets in G. Index 2 thing is automatically normal.

For any g, $gHg^{-1} = H$. If you take any element of the group, $g(123)g^{-1} \in H$ will be a 3-cycle in H. Changes the numbers but keep the cycle number the same.
Example: Suppose $\phi : G \to H$ is any group homomorphis. Claim: $ker\phi$ is normal.
For any elements of the group and any element of the kernel, $g \in G$, $g \in ker\phi$, $gng^{-1} \in ker\phi$. i.e. $\phi(gng^{-1}) = e_H$. You do i.e. $\phi(g)\phi(n)\phi(g^{-1}) = e_H$ where $\phi(n) = e_H$. So $\phi(g)\phi(g^{n-1}) = e_H$. So kernels are normals.

Theorem 10. *Suppose $N \triangleleft G$. Then the following is a group structure on G/N:* $(g_1N)(g_2N) = (g_1g_2)N$

Proof: g_1N is a subset of G, and g_2N is another subset of G. And if you multiply them in all possible ways you get $(g_1g_2)N$. If $g_1N = g_1'N$ and $g_2N = g_2'N$ is $g_1g_2N = g_1'g_2'N$, if so we win (well-defined).

$g_1N = g_1'N \to g_1^{-1}g_1' \in N$ and $g_2^{-1}g_2' \in N$, is it true that $(g_1g_2)^{-1}(g_1'g_2') \in N$? i.e. $g_2^{-1}g_1^{-1}g_1'g_2' \in N$? We know $g_1^{-1}g_1' \in N$. And because N is normal, all the conjugates are in N (and left and right cosets are equal). Can conjugate it by ...

16 Nov. 27

16.1 Administrative

- Problem Set 4 is out. [due on Friday].
- Trajectory for the next 2 weeks is posted.
- WIM paper is due on Wednesday.

Today:

- Centralizers and normalizers
- Towards the second iso theorem.
- "Unique factorization" for finite groups (the Jordan-Holder Theorem)
- Before thanksgiving we reached chapter 9, but now we're in chapter 2.
- Want to chat about centralizers and normalizers and then unique factorization for groups.

Second Isomorphism Theorem for Groups. (Section 3.2)

Proposition 2 (Prop. 13, Prop. 14, Cor. 15)**.** *G group (not necessarily abelian). If we have $H, K < G$ subgroups, define*
$HK \subset G$ (not necessarily a subgroup) $HK = \{hk | h \in H, k \in K\}$. i.e. $G = S_3$ and $H = \{e, (12)\}$ and $K = \{e, (23)\}$, then HK is not a subgroup. $|HK| = 4$ and $|G| = 6$, so by lagrange's theorem, $|HK|$ must divide 6

Prop 13 *If H, K are finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.*
Proof: $H \times K \to HK$ by $(h, k) \to hk$. Clearly this is surjective since that's how we define the elements of HK. Not necessarily a group, so can't use first Iso theorem. LHS has size $|H||K|$ and RHS has size $|HK|$ [clearly]. Want to show that given something on the right, there are exactly $|H \cap K|$ elements of $(h, k) \in H \times K$ with $hk = h_1k_1, ...$ Well if $hk = h_1k_1$ this is true $\iff$ $h^{-1}h = k_1k^{-1} \in H \cap K$ since LHS is in H and RHS in K. For every $\alpha \in H \cap K$, I'll tell you a different $(h_1, k_1) \in H \times K$ with $h_1k_1 = hk$. If $h_1^{-1}h = k_1k^{-1} = \alpha$, then $h_1 = h\alpha^{-1}$ and $k_1 = \alpha k^{-1}$.

Prop 14 *HK is a subgroup $\iff$ $HK = KH$.*
Proof: If $HK = KH$ then why is HK a subgroup? Identity is clearly in there. Is $(h_1k_1)(h_2k_2) \in HK$? $h_1(k_1h_2)k_2$ can be written as $h_1(h_3k_3)k_2$ where each h is in H and k is in K as $HK = KH$. Clearly, this is an element of H times an element of K $= (h_1h_3)(k_3k_2) \in HK$. Final thing: closed under inverses. Is $(hk)^{-1} \in HK$ $(hk)^{-1} = k^{-1}h^{-1} = h_4k_4$ as $h^{-1} \in H$ and $k^{-1} \in K$.

Now suppose HK is a subgroup. Is $HK = KH$? Can I rewrite hk as k_5h_5 for $k_5 \in K$ and $h_5 \in H$. $(hk)^{-1} \in HK = k^{-1}h^{-1}$ and HK is a subgroup, therefore closed under inverses, so this is h_6k_6 and moreover $hk = k_6^{-1}h_6^{-1}$.

Go back to Section 2.2: Centralizers and Normalizers. A group G can act on itself by conjugation: $g \circ h = ghg^{-1}$. This is a group action. G can also act on Subsets of G. If $A \subset G$, then we say g **centralizes** A if $gag^{-1} = a$ for all $a \in A$. Every element of a is preserved by g.

Will be a question on the final about this: difference between centralizer and normalizer.
However, g **normalizes** A if $gag^{-1} \in A$ for all $a \in A$.
If G is abelian, then every g centralizes and normalizes every A.

The centralizser of $A <$ the normalizer of A, and they are both subgroup of G.

The normalizer of A acts on A: it's a group action that sends elements of A to other elements of A.

If g centralizes G, we say g is in the *center* of G. $Z(G) < G$ [and moreover, it's a normal subgroup] where $Z(G)$ is the center.

Denote $C_G(A)$ as the centralizer and $N_G(A)$ as the normalizer. $C_G(A) \cap_{a \in A}$

$Stab(a)$. If A is a normal subgroup, then the normalizer of A is the entire group: $N_G(A) = G$.

Cor. 15:[Section 3.3.] If $H < N_G(K)$, $H, K < G$. Then HK is a subgroup of G.
Proof: From Prop. 14, we need to show that $HK = KH$. We know that $hKh^{-1} = K$ for all $h \in H$ [definition of the normalizer]. In other words, $hK = Kh$ for all $h \in H$. This means $HK = KH$ (by taking the union over all $h \in H$).

2nd Iso. Theorem. G, $A, B < G$. $A < N_G(B)$, then AB is a subgroup. Statement: $A/A \cap B \cong AB/B$. Specifically, B is a normal subgroup of AB because when we conjugate B we get B back: $abBb^{-1}a^{-1}$ where the middle term is $\in B$, so this is simply $aBa^{-1} = B$.

$A \to AB/B$ by $a \to aB$. The kernel of this map are the things in A that go to the identity in aB, so $ker(\phi) A \cap B$.
So $A \cap B$ is normal in A because it's the kernel of this map.

17 November 29

If F is a field, **Claim:** $F[x]$ is a unique factorization domain. How do we know this? It is an Euclidean Domain [because it has a division algorithm].

F_p^x form an abelian group [units of this field] have $p-1$ elements. How many solutions are there in $x^{p-1} \equiv 1 \mod p$ in F_p, so there are $p-1$ solutions in F_p [F_p is $\mathbb{Z}/p\mathbb{Z}$]. And it has roots $1, 2, ..., p-1$.

Factor $(x^{p-1}-1) \equiv (x-1)(x-2)\cdot ... \cdot (x-(p-1))$. **Note F_p^* are the non-zero elements of the group/field.**

$x^2 \equiv 1(\mod p)$ – what are the solutions?

$$x^2 - 1 \equiv 0$$
$$(x-1)(x+1) \equiv 0$$

So these are the only two roots mod p. What about fourth roots mod p?

$$x^4 \equiv 1 \mod p$$
$$(x-1)(x+1)(x^2+1) \equiv 0$$

Question: Is there an element of (F_p^*) of order 4? If $p \equiv 3 \mod 4$, then $|F_p^| = 4k+2$ (size of the group is 1 less than p-1) where $p \equiv 3 \mod 4$ so

$p = 4k + 3$.

$a^2 + b^2 = n$: which n can be written as a sum of two squares? Consider $\mathbb{Z}[i] = a + bi$ where $a, b \in \mathbb{Z}$ has a unique factorization because it has a division algorithm. The size $\mathbb{Z}$ is $|a + bi| = a^2 + b^2$.

New ring, so the primes in the integers are not primes here. The meaning of the word "prime" depends on what ring you're in: 5 is not prime: $5 = (2+i)(2-i)$.

$|(a + bi)(c + di)| = |a + bi||c + di|$: norm is multiplicative/factors. So $((ac - bd)^2 + (bc + ad)^2) = (a^2 + b^2)(c^2 + d^2)$.

In $\mathbb{Z}[i]$ if $|z| = 0$, then $z = 0$. If $|z| = 1$, then $|z| = \pm 1, \pm i$ units. If $|z| > 1$, then z is not a unit: $zy = 1$ so $|z||y| = 1$, so z is a unit.

Old-fashioned prime in $p \in \mathbb{Z}$, maybe it factors in $\mathbb{Z}[i]$. Take the prime factorization: it can only factor into at most 2 pieces of size p: $p = \alpha\beta$, then $|\alpha| = |p| = p$.

Conclusion: either p is prime or $p = \alpha\overline{\alpha}$.

Every prime in $\mathbb{Z}[i]$ is one of these. Reason: Suppose $a + bi$ is prime. Then $|a + bi| = a^2 + b^2$.
Take an old-fashion prime $p \in \mathbb{Z}$ that is a factor of $a^2 + b^2$. If p is a prime in $\mathbb{Z}[i]$, then $p|(a + bi)\overline{(a + bi)}$.

18 December 4

Jordan Holder Theorem: [Did the first half on Dec. 1st class that you missed].
Proposition: Suppose D is a group and we have two **normal** subgroups, B, C inside D. And D/C, D/B is simple and $B \neq C$. Then $B \cap C$ is normal in C and $D/B \cong C/(C \cap B)$.

Proof: Consider the group homomorphism $C \to D/B$ (simple group by hypothesis). What is the image of C in D/B. C is normal in D, so the image of ϕ is normal in D/B [isomorphism theorem]. But $C \not\subset B$, so $im\phi \neq B/B$ normal in D/B. Can't be the one element subgroup, so it must be everything because this group is simple. So $im\phi = D/B$ so ϕ is surjective.

By the first iso theorem, $C/ker\phi \to D/B$ is an isomorphism [$ker\phi$ is normal].

Normal: The image of a normal subgroup is always normal.
Prop Suppose $B \triangleleft D$ and $C \triangleleft D$ then the image of C in D/B is normal in D/B.
Proof. The image of C in D/B is CB/B: C times everything in B mod B.
Ponder/Exercise: the above. When you take the quotient of something,

what is the image of that subgroup in the quotient?

"Factoring S_n" [with the Jordan-Holder Thm.]: What are the finite groups in S_n? One group of size p where p is prime $\mathbb{Z}/p$. Jordan Holder: how to factor groups into smaller supbgroups.

S_n has size $n!$.

Def. Alternating subgroup $A_n \triangleleft S_n$. It's a group that's normal and the quotient group is $\mathbb{Z}/2$. Will give us a group homomorphism from $S_n \to \mathbb{Z}/2 = \{\pm 1\}$. We'll call these odd permutations or even ones.

A_n is simple except if $n = 1$ and $A_1 = S_1 = \{1\}$. If $n = 2$ $A_2 \triangleleft S_2$ where A_2 has order 1 but S_2 has order 2.

$A_3 \triangleleft S_3$ where A_3 has size 3 and S_3 has size 6. $|A_4| = 24/2 = 12$. All the rest are simple: e.g. $|A_5| = 60$. Only simple group of size < 168 not $\mathbb{Z}/p$. These are the only exceptions.

Define A_n = kernel of the sign function: $S_n \to \{\pm 1\}$.
Def. sgn: $S_n \to \{\pm 1\}$.
Given: $\sigma : \{1, ..., n\} \to \{1, ..., n\} \in S_n$.

How often are the two cups are out-of-order: $sign(\prod_{1 \le i \subset j \le n}(\sigma(j) - \sigma(i))) \in \{\pm 1\}$. Same as sign function for determinant.

A_n are the permutations with sign $+1$ (that have an even number of permutations or the permutation matrix represented by A_n has determinant 1: it permutes the basis elements so if the first element becomes the third element, the first row will be one-hot with a 1 in the 3rd column).

Let's factor S_2: S_2 has size 2, so it's simple. $A_3 \triangleleft S_3$ is a kernel of a map, so it's normal. It has size 3, so it's simple: $\{e\} \triangleleft A_3 \triangleleft S_3$ with quotients $\mathbb{Z}/3$ and $\mathbb{Z}/2$.

$\{e\} \triangleleft ... \triangleleft K_4 \triangleleft A_4 \triangleleft S_4$ Where the quotients are $\mathbb{Z}/2$, $\mathbb{Z}/2$, $\mathbb{Z}$ 3, $\mathbb{Z}/2$.

This relates to how you solve cubic, and quartic polynomial equations. It also shows that you cannot solve a random quintic polynomial.
Section called alternating groups [today]. Last friday was Jordan-Holder thm.

19 December 6

Talking about simple groups and alternating groups.

Theorem Suppose G is a finite group, and p is a prime factor of $|G|$. *claim:* Then there is an element of order p in G. If $|G| = 8$, there must be an element of order 2, but there does not necessarily need to be an element of order 4 or 8: $|G| = 8 = \mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z}/2$.
Proof: Consider the following group action. The group is $\mathbb{Z}/p\mathbb{Z}$ acting on the set of $\{x_1, ..., x_p\} \in G$ such that their product is the identity: $x_1 \cdot ... \cdot x_p = e$.

Set A size: $|G|^{p-1}$ as $X_p = (x_1 \cdot \cdot ... \cdot x_{p-1})^{-1}$. A is a set of lists $(x_1, x_2, ..., x_p)$. And we assume $p||G|$, so $p|A$.

Use orbit stabilizer thm: each orbit $|\mathbb{Z}/p\mathbb{Z}| = |stab(A)||orb(a)|$ using the action $\mathbb{Z}/p\mathbb{Z}$ shifting everyting to the right by k steps.

If the stabilizer of $x_1..., x_p = \mathbb{Z}/p\mathbb{Z}$, then they're all the same, so $x^p = e$, i.e., element of order p other than e.

There must be some $x \neq e$ with $x^p = e$ (and in fact, there must be $(p-1)$ of them) because $|A| = |G|^{p-1}$.

A_n is the alternating subgroup – only contains elements that are an even number of swaps..
Theorem: A_5 is simple and $|A_5| = 60$.
Claim: If $n \geq 4$, then (123) and (124) are conjugate in A_n.
Fake proof: (34)(123)(34) = (124): stick in 1 on the right of (34)(123)(34)1 and see where it goes: goes to and therefore we have (124). Fake: because there are not an even number of swaps.

Claim: If $N \triangleleft A_n$ and $n \geq 4$ and $(123) \in N$, then every 3-cycle is in N.
Pf: (12)(34)(123)((12)(34))$^{-1}$ where the conjugate of ((12)(34)) = ((12)(34)).
Tldr: break up odd number of swaps into even number of them.

Claim: If $n \geq 3$, the 3 cycles generate A_n.
Claim: The swaps (i.e. 2-cycles) generate S_n.
For any sequence of cups, I can unscramble them just by swapping two cups at a time (i.e. 2-cycles).

For the 3-cycle case, that's mixed up with an even permutation, choose one of the cups and put it in place first. Can continue doing this until the last 3 cups: $2, 1$ are still scrambled, then you're not in A_n. All the cups are in order except the first two which are swapped: then you're not in A_n because this requires a single swap (not an even number of permutations).

Say we know that A_5 is simple: (Thm 12).
Suppose $\{e\} = N \triangleleft A_n$ where $n > 6$. Goal: 3-cycle in N, then $N = A_n$.

20 December 8

Cayley's Dums Theorem If G is a finite group, then $G \leq S_n$ for some symmetric group.

You can understand a group by its actions, and G acts on itself (by left multiplication), so it's really just a permutation of G, hence a subset of S_{10}. What's the kernel of this action? Only the identity: when you left multiply by e, the group doesn't change. Used first iso theorem: $G/ker\phi \cong im\phi < S_G$ where $G \to S_G$ via ϕ.

Class Equation Consider the action of G on itself where G is a finite group: $g \circ h = ghg^{-1}$ is the conjugation action of G on itself. Previous example was "left multiplication" action of G on itself.

$G = \cup$orbits and therefore $|G| = \sum |orbits|$. If $h \in G$, then $|orbit(h)| * stab(h) = |G|$. $stab(h) = \{g \in g | ghg^{-1} = h \& gh = hg\} = C_G(h)$ the centralizer of h.

$|G| = \sum_{orbits} \frac{|G|}{C_G(h)}$ where h is any element in the orbit.
class equation $= |Z(n)|$ (i.e. the center of G that has size 1) $+ \sum_{\text{orbits of size bigger than 1}} |G|/|C_G(h)|$.

Every $p-group$ i.e. $|G|^k$ where $k = p^a$ can be factored into subgroups isomorphic to $\mathbb{Z}/p\mathbb{Z}$.
Sylow Theorems: Suppose G is a finite group and $|G| = p^a m$ where p is prime and m is co-prime to p. Define a $p - subgroup$ of G is a subgroup who's size is a power of p. Know this must be at least size p^a.

We define a p$-sylow$ subgroup to be a subgroup of maximum size: p^a.

If n_p is the number of $p - Sylowes$, then $n_p | m$ and $n_p \equiv 1 \mod p$.

If P is a $p - Slow$ subgroup and Q is any $p-$subgroup, then $\exists$ a conjugate $gQg^{-1} \leq P$. As a consequence, all p-sylows are conjugate.

Suppose $|G| = 21$; claim: it's not simple – it has a normal subgroup. A normal subgroup is going to be a sylow subgroup: 3 or 7.

n_3, n_7: know there's a subgroup of size 3 and another subgroup of size 7; but we don't know which one is "1" yet. n_7 ...

[Final]: Four central things
1. Euclidean Algorithm: $ax + by = 1$ if a and b are relatively prime. Chinese remainder theorem: $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
2. Groups! Quotient groups, cosets, subgroups, normal, group actions, orbits, stabilizers, isomorphism theorems. Labrange's theorem.

21 Textbook

21.1 Preliminaries

Cardinality: The **cardinality** or **order** of a set A will be denoted by $|A|$ is the number of elements in A.
Cartesian Product: The **cartesian product** of two sets A, B is a new set $A \times B = \{(a, b)|a \in A, b \in B\}$.
Domain and Co-domain: Let $f : A \to B$, then A is the domain of f and B is the co-domain of f.
Well-defined functions: It is important to ensure f is well-defined: i.e., f is unambiguously determined. Every point in the domain maps exactly to one element in the co-domain. Non-well-defined functions may have a single point in the domain map to two different points in the co-domain.
Range: The **range** or **image** of a function f is $f(A) = \{b \in B|b = f(a) \text{ for some } a \in A\}$. Observe $f(A) \subseteq B$.
The pre-image of f is the set $f^{-1}(C) = \{a \in A|f(a) \in C\}$ for a given subset C of B. This is the pre-image of set C under function f.
left and right inverses: f has a **right inverse** if $\exists h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B and a **left inverse** if $\exists g : A \to B$ such that $g \circ f$ is the identity map on A (i.e. $(g \circ f)(a) = a \ \forall a \in A$).

21.2 Section 1.1 Basic Axioms and Examples

Binary Operation on a set G is a function $\cdot : G \times G \to G$ for any $a, b \in G$.

- A binary operation is *associative* if for all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- A binary operation is *commutative* if for all $a, b \in G$, $a \cdot b = b \cdot a$

Closed under $\cdot$ If H is a subset of G, and the restriction of $\cdot$ to H is a binary operation on H (i.e., $\forall a, b \in H$, $a \cdot b \in H$), then H is said to be **closed** under $\cdot$. **Group:** a **group** is an ordered pair $(G, \cdot)$ where G is a set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $\cdot$ is associative.
2. $\exists$ identity element: $\forall a \in G$, $\exists e \in G$ such that $a \cdot e = a$.
3. $\exists$ inverse element: $\forall a \in G$, $\exists a^{-1} \in G$ such that $a \cdot a^{-1} = e$.

An **Abelian** Group is a Group that is commutative.

Definition 14 (Element Order)**.** *For G a group and $x \in G$, define the order of x to be the smallest positive integer n such that $x^n = 1$. Denote this integer as $|x|$.*

Definition 15 ($n\mathbb{Z}$)**.** *$n\mathbb{Z}$ is the set of integers divisible by n*

Definition 16 ($\mathbb{Z}/n\mathbb{Z}$)**.** *$\mathbb{Z}/n\mathbb{Z}$ is the set of integers mod n. This is also the quotient group of $\mathbb{Z}$ with $n\mathbb{Z}$.*

Elements of $\mathbb{Z}/n\mathbb{Z}$ are called the residuals $\overline{a} = \{a + nk|k \in \mathbb{Z}\}$

21.3 Section 1.6 Homomorphisms and Isomorphisms

What does it mean when two groups "look" the same? In other words, when do they have the same group theoretic structure? This is the notion of an *isomorphism* between groups.

Definition 17 (homomorphism)**.** *Let $(G, \circ)$ and $(H, \star)$ be groups. A map $\phi : G \to H$ such that $\phi(x \circ y) = \phi(x) \star \phi(y)$ for all $x, y \in G$ is called a homomorphism. Without group actions, this is $\phi(xy) = \phi(x)\phi(y)$.*

Informally, a function ϕ is a homomorphism if it respects the group structures of its domain and co-domain. Performing one operation in the domain before the function is equivalent to performing the operation after the function.

Definition 18 (isomorphism)**.** *The map $\phi : G \to H$ is called an isomorphism and G and H are said to be isomorphic $G \cong H$ if*

1. *ϕ is a homomorphism*
2. *ϕ is a bijection.*

Informally, two groups are isomorphic if there is a bijection between them that preserves the group operations. Intuitively, G and H are the same group, except that the elements and the operations may be written differently in G and H.

21.4 Section 1.7 Group Actions

Definition 19 (Permutation)**.** *A permutation of a set A is simply a bijection from A onto itself.*

Definition 20 (Group Action)**.** *A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$ for all $g \in G$ and $a \in A$) satisfying the following properties:*

1. *$g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$, $a \in A$*
2. *$1 \cdot a = a$ for all $a \in A$*

Note: $\cdot$ is not the binary operation of G! $g \cdot a \in A$, not necessarily $\in G$ Informally, we say G is a group acting on a set A, and applying two group actions on an element of A is equivalent to the product $(g_1 g_2)$ within the group being applied to that same element.

Fact 1. *Let the group G act on the set A. Then for each fixed $g \in G$, we get a map σ_g defined by*

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

Two important facts are:

1. *for each fixed $g \in G$, σ_g is a permutation of A.*

2. *the map from G to S_A defined by $g \to \sigma_g$ is a homomorphism.*

Proof of 1. To show σ_g is a permutation of A, it suffices to show that σ_g has a 2-sided inverse. For any $a \in A$

$$\begin{aligned}(\sigma_g^{-1} \circ \sigma_g)a &= \sigma_g^{-1}(\sigma_g(a)) \\ &= g^{-1}(g(a)) \\ &= (g^{-1} \circ g)(a) \\ &= 1 \cdot a = a\end{aligned}$$

The same can be repeated with $\sigma_g \circ \sigma_g^{-1}$ to show the right-inverse. □

Proof of 2. Define $\phi : G \to S_A$ be defined by $\phi(g) = \sigma_g$. To show ϕ is a homomorphism, we must show $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$. For any $a \in A$:

$$\begin{aligned}\phi(g_1 g_2)(a) &= \sigma_{g_1, g_2}(a) \\ &= (g_1 g_2)(a) \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \sigma_1(\sigma_2(a)) \\ &= (\sigma_1 \cdot \sigma_2)(a) \\ &= (\phi(g_1) \circ \phi(g_2)(a)\end{aligned}$$

□

Informally, every element $g \in G$ acts on A in a manner consistent with the group operations in G.

Definition 21 (Permutation Representation)**.** *The homomorphism from G to S_A given by ϕ is called the permutation representation associated to the given action.*

The actions of a group G on a set A (i.e. $g \cdot a$) and the homomorphisms from G into the symmetric group S_A are in bijective correspondance.

21.5 Section 2.1: Subgroups

Definition 22 (Supgroup)**.** *Let G be a group. The subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses: $\forall x, y \in H$, $x^{-1} \in H$ and $xy \in H$. If H is a subgroup of G we write $H \leq G$.*

Subgroups of G are just subsets of G that are themselves groups with respect to the operation defined in G, i.e., the binary operation on G restricts to give a binary operation on H which is associative, has the identity in H, and has inverses in H for all the elements of H.

Proposition 3 (The Subgroup Criterion)**.** *A subset H of a group G is a subgroup if and only if*

1. $H \neq \emptyset$
2. $\forall x, y \in H$, $xy^{-1} \in H$

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proof of nonempty and closed under multiplication in finite group. This is a bit tricky, but relies on the element order of every element in G. Recall the order of $x \in G$ is the smallest positive integer n such that $x^n = 1$, and the element order is linked to the cardinality of the set G.
For any element $x \in H$, it must be the case that $x^a = x^b$ for some $b > a$ because the set is finite, but $\{x, x^1, ...\}$ is infinite. Then $x^b = x^{b-a+a} = x^{b-a}x^a$ and $x^{b-a} = 1$ as $x^b = x^a$. So the order of all elements in H is finite. Further, for any $x \in H$, $x^1 x^{n-1} = 1$, so we have inverses too. □

21.6 Section 2.2 Centralizers, Normalizers, Stabilizers, and Kernels

We will review several important families of subgroups for an arbitrary group G.

Definition 23 (Centralizer of a set)**.** *Define $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the centralizer of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, so $C_G(A)$ is the set of elements of G that commute with every element of A.*

We can prove this is a subgroup of G.

Definition 24 (Center)**.** *$Z(G) = \{g \in G | gx = xg \text{ for all } x \in g\}$ is the center of G: the set of elements commuting with all the elements of G.*

This is also a subgroup as $G(G) = C_G(G)$ by the definition of a centralizer; however, $G_G(A)$ is more general as it can act on an arbitrary set A rather than the group G itself.

Definition 25 (Normalizer)**.** *Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Define the normalizer of A in G to be the set $N_G(A) = \{g \in G | gAg^{-1} = A\}$.*

Notice that if $g \in C_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$, so $G_G(A) \leq N_G(A)$. $N_G(A)$ is also a subgroup of G.

Definition 26 (Stabilizer)**.** *If G is a group acting on a set S and s is some fixed element of S, then the stabilizer of s in G is the set $G_s = \{g \in G | g \cdot s = s\}$*

We can prove $G_s \leq G$.

Definition 27 (Kernel)**.** *The kernel of an action is a subgroup, where the kernel of the action of G on S is defined as $\{g \in G | g \cdot s = s \text{ for all } s \in S\}$*

While the stabilizer of an element of a set S is the set of group actions that do not change s, the *kernel* of a group is the set of actions that do not change any element of s when they act on this set.

21.7 Section 2.3 Cyclic Groups and Cyclic Subgroups

Let G be any group and $x \in G$. One way of forming a subgroup H of G is by letting H be the set of all integer (positive, negative, and zero) powers of x (this guarantees closure under inverses and products at least as far as x is concerned). This section is devoted to studying these subgroups that are generated by a single element.

Definition 28 (Cyclic Group)**.** *H is cyclic if it can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$ (where the usua operator is multiplication). In additive notation, H is cyclic if $H = \{nx | n \in \mathbb{Z}\}$. In both cases, we shall write $H = \langle x \rangle$ and say H is generated by x (and x is a generator of H).*

A group may have more than one generator: $H = \langle x \rangle = \langle x^{-1} \rangle$.

Proposition 4. *if $H = \langle x \rangle$, then $|H| = |x|$, so*

1. *if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, ..., x^{n-1}$ are all distinct elements of H.*
2. *if $|H| = \infty$, then $x^n \neq 1$ fora ll $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

Proposition 5. *Let G be a group and let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.*

1. *If $|x| = \infty$, then $|x^a| = \infty$*
2. *If $|x| = n < \infty$, then $|x^a| = \frac{n}{gcd(n,a)}$*

Proposition 6. *Let $H = \langle x \rangle$.*

1. *If $|x| = \infty$, then $H = \langle x^a \rangle \iff a = \pm 1$*
2. *Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle \iff gcd(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$ where ϕ is Euler's function.*

21.8 Section 2.4 Subgroups Generated by Subsets of a Group

Given an arbitrary subset of a group G, that we'll call A, what is the smallest subgroup of G containing all elements of A? We show that closing A under multiplication and taking inverses yields this smallest subgroup.

Proposition 7. *If $\mathcal{A}$ is a nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.*

Definition 29 (Subgroup Generated by A)**.** *If A is any subset of the group G, define $\langle A\rangle = \cap_{A\subset H, H\leq G} H$ to be the intersection of all subgroups H of G that contain A. This is called the subgroup of G generated by A.*

Observe that $\langle A\rangle$ is the unique minimum element of $\mathcal{A}$ as $\mathcal{A}$ can be larger than $\langle A\rangle$.

Definition 30 (Closure of a set A)**.** *Define the closure of A as $\overline{A} = \{a_1^{\epsilon_1}, \cdot a_2^{\epsilon_2} \cdot \cdot \cdot a_n^{\epsilon_n} | n \in \mathbb{Z}, n \geq 0$ and $a_i \in A$, $\epsilon_i = \pm 1$ for each $i\}$*

So $\overline{A}$ is the set of all finite products of elements of A and inverses of elements of A.

Proposition 8. $\overline{A} = \langle A\rangle$

This is a meaningful proposition: it gives us a way to construct an arbitrary subgroup from a set.

21.9 Section 3.1: Quotient Groups

Definition 31 (Fibers of Homomorphism)**.** *Let ϕ be a homomorphism from $G \to H$. Then the fibers of ϕ are the sets of elements of G projecting to single elements of H: $\phi^{-1}(h) = \{g \in G | \phi(g) = h\}$ (i.e. the preimage of h).*

This definition suggests the fibers themselves form a group. Let X_a be the pre-image of a and X_b be the pre-image of b. Then as a, b are part of group H, and ϕ is a homomorphism, $X_a \cdot X_b = X_{ab}$.

This multiplication is associative as multiplication in H is associative. Similarly, the "identity" fiber is the pre-image of the identity of H, and inverse fibers must also exist as H is a group.

Roughly speaking, the group G is partitioned into sub-sets (fibers), and these pieces themselves have the structure of a group, called the *quotient* group of G. As we define multiplication of fibers by multiplication in H, by construction the quotient group with this multiplication is naturally isomorphic to the image of G under the homomorphism ϕ: there's a bijection between the set of fibers and the image of ϕ.

Definition 32 (Kernel)**.** *If ϕ is a homomorphism $\phi : G \to H$, the kernel of ϕ is the set $\{g \in G | \phi(g) = 1\}$*

and will be denoted by $ker(\phi)$ (here 1 is the identity of H).

Definition 33 (Quotient Group)**.** *Let $\phi : G \to H$ be a homomorphism with kernel K. The quotient group, $G|K$, is the group whose elements are the pre-image of ϕ with group operators defined above: namely if X is the fiber of a and Y is the fiber of b, then the product of X with Y is defined to be the fiber of the product ab.*

Definition 34 (Coset)**.** *For any $N \leq G$ and any $g \in G$, let*

$$gN = \{gn | n \in N\} \text{ and } Ng = \{ng | n \in N\}$$

be called respectively a left coset and right coset of N in G. Any element of a coset is called a representative for the coset.

Theorem 11. *Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with the operation defined by*

$$uK \circ vK = (uv)K$$

forms the quotient group $G|K$.

Informally, the set of cosets of the kernel K, with binary operation described as above, are equal to the quotient group $G|K$.

The cosets of an arbitrary subbgroup of G partition G (i.e. their union is all of G and distinct cosets have trivial intersection).

Proposition 9. *Let N be any subgroup of the group G. Then the set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G$, $uN = vN \iff v^{-1}u \in N$ and in particular, $uN = vN \iff u, v$ are representatives of the same coset.*

Essentially, cosets have trivial intersection and partition G.

Definition 35 (Normal Subgroup)**.** *A subgroup N of G is called normal ($N \triangleleft G$) if every element of G normalizes N (i.e. $gNg^{-1} = N$ for all $g \in G$).*

Normal subgroups are the "abelian components" of a group.

Theorem 12. *Let N be a normal subgroup of G. Then*

1. *$N_G(N) = G$: The normalizer of N in G is equal to the entire group G: this is because every element of G normalizes N.*
2. *$gN = Ng$: Abelian property.*
3. *The operation of left cosets of N in G makes the set of left cosets into a group. Suppose u, v are elements belonging to left cosets. THen $uN = vN$ if and only if u, v belong to the same left coset.*

21.10 Section 3.2: Lagrange's Theorem

One of the most important invariants of finite groups is its order. In particular, the order of a quotient group of a finite group $|G/N|$ (quotient of N with G) is $\frac{|G|}{|N|}$. This is somewhat remarkable; we know the order of a quotient group without knowing its elements.

Theorem 13 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G, and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.*

Corollary 4. *If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1$ for all $x \in G$.*

Proof. $|x| = |\langle x \rangle|$, so applying Lagrange's Theorem to $H = \langle x \rangle$ tells us the order of this subgroup divides the order of G, and therefore the order of $|x| = |\langle x \rangle|$ divides the order of G. □

Corollary 5. *If G is a group of prime order p, then G is cyclic, and hence $G \cong Z_p$ [the cyclic group of order p].*

We can now look at converses of Lagrange's theorem: if n divides $|G|$, must G have a subgroup of order $\frac{|G|}{n}$?

Theorem 14 (Cauchy's Theorem)**.** *If G is a finite group, and p is a prime dividing $|G|$, then G has an element of order p.*

Theorem 15 (Sylow's Theorem)**.** *If G is a finite group of order $p^\alpha m$ where p is a prime and p does not divide m, then G has a subgroup of order p^α*

Definition 36. *Let H and K be subgroups of a group an define $HK = \{hk | h \in H, k \in K\}$.*

Proposition 10. *If H and K are finite subgroups of a group, then $|HK| = \frac{|H||K|}{|H \cap K|}$*

Proposition 11. *If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.*

21.11 3.4 Composition Series and the Holder Program

Proposition 12. *If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.*

Definition 37 (Simple Group)**.** *A (finite or infinte) group G is called simple if $|G| > 1$ and the only normal subgroups of G are 1 and G.*

Note: Z_n is the cyclic group of order n: i.e. the group generated by a single element $< x >$ that has order n. This group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Definition 38 (Composition series)**.** *In a group G, a sequence of subgroups*

$$1 = N_0 \leq N_1 \leq ... \leq N_k = G$$

is called a composition series if $N_i \triangleleft N_{i+1}$ and N_{i+1}/N_i is a simple group. This The quotient groups N_{i+1}/N_i are called the composition factors of G.

Theorem 16 (Jordan-Holder)**.** *Let G be a finite group with $G \neq 1$. Then*

1. *G has a composition series.*
2. *The composition factors in a composition series are unique. Namely, if $1 = N_0 \leq N_1 \leq ... \leq N_r = G$ and $1 = M_0 \leq M_1 \leq ... \leq M_s = G$ are two composition series for G, then $r = s$ and there is some permutation π of $\{1, 2, ..., r\}$ such that $M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$*

This allows us to classify all finite groups up to isomorphism by

1. Find all finite simple groups.
2. Find all ways of putting simple groups together to form other groups.

22 3.5: Transpositions and the Alternating Group

As we saw in 1.3, every element of S_n [the permutation group] can be written as a product of disjoint cycles in an essentially unique fashion. However, any single element can be written as a product of cycles. For example:
$\sigma = (123) = (13)(12) = (12)(23)$.
Recall (123)1 sends 1 to 2, 2 to 3, and 3 to 1. This is equivalent to sending 1 to 2, 2 to 1 and then 1 to 3 (so 2 to 3), and finally 3 to 1. In this example, we represent a cycle as a (nondisjoint) product of 2-cycles.

Definition 39 (Transposition)**.** *A 2-cycle is called a transposition.*

And it can be shown any permutation in S_n can be written as a product of disjoint cycles [how we represent it: i.e. (1 2 3)], and in particular, can be rewritten as a product of transpositions.

Definition 40 (The Alternating Group)**.** *The alternating group of degree n, denoted A_n, is the kernel of the homomorphism ϵ (i.e. the set of even permutations) where ϵ is the sign function: $\epsilon(\sigma) \in \{\pm 1\}$. Simply, it's the set of σ in S_n that are even.*

22.1 Section 7.1: Basic Definitions and Examples of Rings

Definition 41 (Ring)**.** *A **ring** R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) that satisfy:*

1. *$(R, +)$ is an abelian group.*
2. *$\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$*
3. *The distributive laws hold in R: for all $a, b, c \in R$, $a+b)\times c = (a\times c)+(b\times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$*

Moreover, the ring R is said to be commutative if multiplication is commutative. Similarly, the ring R is said to have an identity (or contain a 1) if there is an element $1 \in R$ with $1 \times a = a$ for any $a \in R$.

Example 5 (Functions as Rings)**.** *We can view a set of functions: $f : X \to A$ as a ring under the usual definition of pointwise addition and multiplication of functions:*
Pointwise addition: $(f + g)(x) = f(x) + g(x)$
Multiplication: $(fg)(x) = f(x)g(x)$.

Definition 42 (Division Ring or Skew Field)**.** *A ring R with identity 1, where $1 \neq 0$ is called a division ring or skew field if every nonzero element $a \in R$ has a multiplicative inverse: $\exists b \in R$ such that $ab = 1 = ba$*

Definition 43 (Field or Commutative Division Ring)**.** *A field (or effectively a commutative division ring) is a division ring that is commutative.*

Definition 44 (Zero Division)**.** *A nonzero element a of R is called a zero divisor if there is a nonzero element $b \in R$ such that ab or ba is equal to 0.*

Definition 45 (Unit)**.** *Let R be a ring with identity 1 such that $1 \neq 0$. An element u of R is called a unit in R if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted by $R^\times$*

Observe that a *field* is a ring R with identity 1, $1 \neq 0$, and where every nonzero element is a unit: $F^\times = F - \{0\}$.

Definition 46 (Integral Domain)**.** *A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.*

Proposition 13 (Cancellation Law)**.** *Assume $a, b, c \in R$ and a is not a zero-divisor. Then if $ac = ab$, either $a = 0$ or $b = c$.*

Corollary 6. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain and let a be a nonzero element of R. By the cancellation law, the map $x \to ax$ is an injective function. Since R is finite, and the domain is equal to the co-domain, this map is also surjective. In particular, $\exists b$ such that $ab = 1$, so a must be a unit in R. Since a was any nonzero element, all nonzero $a \in R$ are units, and R is a field. □

Definition 47 (Subring)**.** *A subring of the ring R is a subgroup of R that is closed under multiplication.*

As $(R, +)$ is an abelian group, this effectively means that the operations of $+, \times$ when restricted to $S \subset R$ give S the structure of a ring. To check if a subset is a subring, it sufficies to show the subset is closed under subtraction and multiplication (or addition and multiplication if 1 is in your ring).

22.2 Section 7.2: Polynomial Rings, Matrix Rings ,and Group Rings

Example 6 (Polynomial Rings). *$a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ is a polynomial of degree n with $n \geq 0$ and $a_i \in R$ with R being a commutative ring with identity. $a_n x^n$ is called the leading term, and a_n is called the leading coefficient. The polynomial is monic if $a_n = 1$.*

The set of all polynomials is called the ring of polynomials in the variable x with coefficients in R will be denoted as $R[x]$.

Addition: $a_n x^n + b_n x^n = (a_n + b_n)x_n$
Multiplication: $(ax^i)(bx_j) = abx^{i+j}$ and then apply distributive law to the sum.

Example 7 (Matrix Rings). *Fix an arbitrary ring R and let n be a positive integer. Let $M_n(R)$ be teh set of all $n \times n$ matrices with entries from R.*

The element $(a_{ij}) \in M_n(R)$ is an $n \times n$ square matrix of elements of R whose entry in row i and column j is $a_{ij} \in R$.

Addition and multiplication follow from typical matrix addition and multiplication.

Example 8 (Group Rings). *Fix a commutative ring R with identity $1 \neq 0$ and let $G = \{g_1, g_2, ..., g_n\}$ be any finite group with group operation written multiplicatively. Define the group ring, RG, of G with coefficients in R to be teh set of all formal sums:*

$$a_1 g_1 + a_2 g_2 + ... + a_n g_n$$

with $a_i \in R$, $1 \leq i \leq n$. If g_1 is the identity of G, we write $a_1 g_1$ as a_1. Similarly, the element $1g$ is simply g.

Addition is "componentwise": $(a_1 g_1 + a_2 g_2 + ... + a_n g_n) + (b_1 g_1 + b_2 g_2 + ... + b_n g_n) = (a_1 + b_1)g_1 + ... + (a_n + b_n)g_n$

For multiplication, define $(ag_i)(bg_j) = (ab)g_k$ with ab in R and $g_i g_j = g_k$ as the product in group G. This product is then extended to all formal sums (i.e. must include a sum of all elements in the finite group) by the distributive laws: $(a_1 g_1 + ... + a_n g_n) \times (b_1 g_1 + ... + b_n g_n) = \sum_{g_i g_j = g_k} a_i b_j$.

22.3 Section 7.3: Ring Homomorphisms and Quotient Rings

Definition 48 (Ring Homomorphism). *A ring homomorphism is a map $\phi : R \to S$ satisfying*

1. *$\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$ (so ϕ is a group homomorphism on the additive operator).*

2. $\phi(ab) = \phi(a)\phi(b)$ *for all* $a, b \in R$

A *bijective* ring homomorphism is called an *isomorphism.*

Definition 49 (Kernel)**.** *The kernel of the ring homomorphism* ϕ*, denoted* $ker\phi$ *is the set of elements of* R *that map to 0 in* S*:* $\{x \in R | \phi(x) = 0 \in S\}$*.*

Proposition 14. *Let* R *and* S *be rings and let* $\phi : R \to S$ *be a homomorphism. Then*

1. *The image of* ϕ *is a subring of* S
2. *The kernel of* ϕ *is a subring of* R*. Furthermore, if* $\alpha \in ker(\phi)$*, then* $r\alpha$ *and* $\alpha r \in \ker \phi$ *for every* $r \in R$*. Specifically,* $ker(\phi)$ *is closed under multiplication by elements from* R*.*

Recall that for groups, when ϕ is a homomorphism, the fibers of the homomorphism have the structure of a group that is isomorphic to the image of ϕ. In other words, the cosets of the domain group are isomorphic to the image of the homormorpism. A similar property is true for rings.

Let $\phi : R \to S$ be a ring homomorphism with kernel I. Since R and S are abelian groups under addition, ϕ is a homomorphism of abelian groups and the fibers of ϕ (i.e. pre-image of a point in the image: $\phi^{-1}(s) = \{x \in R\}$ = fiber in R are the additive cosets $r + I$ of the kernel I. The set of these fibers have the structure of a ring (where each fiber is an individual element in the ring) that is naturally isomorphic to the image of ϕ: if X is the fiber of $a \in S$—i.e. $\phi^{-1}(a) = X$—and Y is the fiber over $b \in S$, then $X + Y$ is the fiber over $a + b$ and XY is the fiber over ab. In your favorite terminology, $X + Y = \phi^{-1}(a + b)$ and $XY = \phi^{-1}(ab)$. Formally,

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I) \times (s + I) = (rs) + I$$

This ring of cosets is called the *quotient ring* of R by $I = ker(\phi)$ and is denoted R/I. Note that because $(R, +)$ is abelian, the subgroup I is necessarily normal, and therefore the quotient R/I of cosets of I is automatically an additive abelian group. For an arbitrary subgroup I, it remains to see if the *multiplicative* structure induced from multiplication in R. In general the answer is no, but this leads to the notion of an *ideal* in R for which this subgroup does induce a quotient ring. Later, we will see the *ideals* of R are exactly the kernels of the ring homomorphisms of R. Taking $\alpha, \beta \in I$ we have:

$$(r + \alpha)(s + \beta) + I = rs + I$$
$$rs + \alpha s + r\beta + \alpha\beta + I = rs + I$$

Therefore, αs, $r\beta \in I$ and moreover $\alpha\beta \in I$. It then must be the case that $\alpha\beta \in I$, and that for any element in I, $\alpha s \in I$ and $r\beta \in I$. So I is also closed by multiplication on the left and right with elements from R. Such I that are closed under multiplication on the left and right by elements of R are called the *ideals* of R.

Definition 50 (Ideal)**.** *Let R be a ring, let I be a subset of R and let $r \in R$.*

1. *$rI = \{ra | a \in I\}$ and $Ir = \{ar | a \in I\}$*
2. *A subset I of R is called an ideal of R if*
   (a) *I is a subring of R*
   (b) *I is closed under multiplication by elements from R: $rI = Ir \subseteq I$ for all $r \in R$*

The course textbook emphasizes *left* and *right* ideals as commutativity of rings is not assumed, and for commutative rings, these two notions coincide. **to prove a subset I of a ring R is an ideal, it is necessary to prove that I is nonempty, closed under subtraction, and closed under multiplication by all elements in R.** If R has a 1, then $(-1)a = -a$, so it suffices to show closed under addition rather than subtraction (as multiplication by -1 emulates subtraction). Finally, the kernel of any ring homomorphism is an ideal.

To summarize, if I is an ideal of R, then the operations of the quotient group R/I is a ring under:

1. $(r + I) + (s + I) = (r + s) + I$
2. $(r + I) \times (s + I) = (rs) + I$

Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition 51 (Quotient Ring)**.** *When I is an ideal of R, the ring R/I with the operations above is called the quotient ring of R by I.*

Theorem 17 (First Isomorphism Theorem for Rings)**.** *If $\phi : R \to S$ is a homomorphism of rings, then teh kernel of ϕ is an ideal of R, the image of ϕ is a subring of S and $R/ker\phi$ is isomorphic as a ring to $\phi(R)$.*

Conversely, if I is any ideal of R, then the map $R \to R/I$ defined by $r = r + I$ is a surjective ring homomorphism with kernel I [this homomorphism is called the natural projection of R onto R/I].

Thus, every ideal is the kernel of a ring homomorphism and vice-versa.

Theorem 18 (Second Isomorphism Theorem for Rings)**.** *Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R $A \cap B$ is an ideal of A, and $(A + B)/B \cong A/(A \cap B)$*

Theorem 19 (Third Isomorphism Theorem for Rings)**.** *Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.*

Theorem 20 (Fourth (or Lattice) Isomorphism Theorem for Rings)**.** *Let I be an ideal of R. The correspondance $A \iff A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal if and only if A/I is an ideal of R/I.*

If I and J are ideals in the ring R, then the set of sums $a + b$ with $a \in I$ and $b \in J$ is not only a subring of R [2nd isomorphism theorem], but is also an *ideal* in R.

Definition 52 (Properties of Ideals)**.**

1. *Define the sum of I and J by $I + J = \{a + b | a \in I, b \in J\}$*
2. *Define the product of I and J, dentoed by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.*
3. *For any $n \geq 1$, define the n^{th} power of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i.*

22.4 Section 7.4: Properties of Ideals

Definition 53 (Ideal Generated by A)**.** *Let A be any subset of the ring R.*

1. *Let (A) denote the smallest ideal of R containing A, called the ideal generated by A.*
2. *Let RA denote the set of all finite sums of elements fo the form ra with $r \in R$ and $a \in A$, i.e., $RA = \{r_1 a_1 + r_2 a_2 + ... + r_n a_n | r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$.*
3. *An ideal generated by a single element is called a principal ideal.*
4. *An ideal generated by a finite set is called a finitely generated ideal.*

We can also say $(A) = \cap_{A \subseteq I} I$, or the ideal generated by the set A is equal to the intersection of all ideals that contain A.

Consider the principal ideal (a) composed of elements ra for some $r \in R$. Then an element $b \in R$ belongs to (a) if and only if $b = ra$, or equivalently b is a multiple of a, or equivalently a divides b in R. Similarly, $b \in (a) \iff (b) \subseteq (a)$.

Example 9 (Integer Polynomials)**.** *Consider the ideal $(2, x)$ generated by 2 and x in $\mathbb{Z}[x]$: $\{2p(x) + xq(x) | p(x), q(x) \in \mathbb{Z}[x]\}$. This is not a principal ideal: i.e.*

it cannot be $(a(x))$ *for some* $a(x) \in \mathbb{Z}$.

Suppose $(2, x) = (a(x))$ *for some* $a \in \mathbb{Z}[x]$. *Then* $2 \in (a(x))$ *so* $2 = a(x)p(x)$ *for some* $p(x) \in \mathbb{Z}[x]$ *and* $a = \{\pm 1, \pm 2\}$. *If* $a = \pm 1$, *then* $(a(x))$ *is not a proper ideal as it is equal to* $\mathbb{Z}[x]$. *So* $a = \pm 2$. *Then* $(2) = (-2) = x$ *because* $x \in (2, x)$, *so* $2q(x) = x$ *for some* $q(x) \in \mathbb{Z}[x]$. *This is impossible for integer coefficient polynomials.*

Proposition 15. *Let* I *be an ideal of* R. *Then*

1. $I = R$ *if and only if* I *contains a unit (i.e. a such that* $aa^{-1} = 1$
2. *If* R *is commutative, then* R *is a field* $\iff$ *its only ideals are* 0 *and* $R.d$

Corollary 7. *If* R *is a field, then any non-zero ring homomorphism from* R *into another ring is injective.*

Proof. The kernel of a ring homomorphism is an ideal, and the only ideals of R are R and 0. As the kernel of a non-zero ring homomorphism is a proper ideal (i.e. not the entire set), then the kernel is 0, and ϕ is injective. □

Definition 54 (Maximal Ideal)**.** *An ideal* M *in an arbitrary ring* S *is called a maximal ideal if* $M \neq S$ *and the only ideals containing* M *are* M *and* S.

A ring does not need to have any *maximal ideals* – take for example the group $\mathbb{Q}$ and define multiplication to be trivial: $ab = 0$. In this instance, the ideals are simply the subgroups, and as $\mathbb{Q}$ has no maximal subgroups, there are no maximal ideals.

Proposition 16. *In a ring with identity, every property ideal is contained in a maximal ideal.*

This proof uses *Zorn's Lemma* which in-turn assumes the axiom of choice. *Zorn's Lemma* states that a partially ordered set (i.e. for certain pairs of elements, one precedes the other) containing upper bounds for every chain (i.e. a subset of elements in the set that are ordered), then the set contains at least one maximal element.

Proposition 17. *Assume that* R *is commutative. The ideal* M *is a maximal ideal if and only if the quotient ring* R/M *is a field.*

This shows us how to construct fields: take a commutative ring, and quotient it by an maximal ideal.

Definition 55 (Prime Ideal)**.** *Let* R *be a commutative ring. An ideal* P *is called a prime ideal if* $P \neq R$ *and whenever the product* ab *of two elements* $a, b \in R$ *is an element of* P, *then at least one of* a *and* b *is an element of* P.

A prime "ideal" is a fairly natural generalization of the notion of a "prime" in the integers $\mathbb{Z}$. For example, let n be non-negative integer. Then the ideal $n\mathbb{Z}$ is a *prime* ideal provided $n \neq 1$ (to ensure the ideal is proper) and perovided every

time the product ab of two integers is an element of $n\mathbb{Z}$ at least one of a, b is an element of $n\mathbb{Z}$. Put another way, whenever n divides ab, n must either divide a or b. This is equivalent to the usual definition that n is a prime number, and the prime ideals of $\mathbb{Z}$ are simply the ideals $p\mathbb{Z}$ where p is prime.

Proposition 18. *Let R be a commutative ring. Then the ideal P is a prime ideal in R $\iff$ the quotient ring R/P is an integral domain (i.e. has no nonzero divisors).*

Corollary 8. *Let R be a commutative ring. Every maximal ideal of R is a prime ideal.*

22.5 Section 7.6: The Chinese Remainder Theorem

Throughout this section, assume that all rings are commutative with an identity $1 \neq 0$.

Definition 56 (Cartesian Product of Rings)**.** *For rings R_1, R_2, define the Cartesian product $R_1 \times R_2$ as the set of ordered pairs (r_1, r_2) such that $r_1 \in R_1$ and $r_2 \in R_2$.*

1. $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$
2. $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$

A function $\phi : R \to (X, Y)$ is homomorphism $\iff$ the induced map into each component is a homomorphism.

For prime numbers in $\mathbb{Z}$, we say a, b are relatively prime if $(a, b) = 1$—or equivalently—a solution to $na + mb = 1$. We seek to generalize this notion of relative primeness to arbitrary groups.

Definition 57 (Comaximal)**.** *The ideals A and B of the ring R are said to be* ***comaximal*** *if $A + B = R$.*

Theorem 21 (Chinese Remainder Theorem)**.** *Let $A_1, A_2, ..., A_k$ be ideals in R. Then the map:*

$$R \to R/A_1 \times R/A_2 \times ... \times R/A_k$$

defined by $r \to (r + A_1, r + A_2, ..., r + A_k)$ is a ring homomorphism with kernel $A_1 \cap A_2 \cap ... \cap A_k$.

If for each $i, j \in \{1, 2, ..., k\}$ with $i \neq j$, the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap ... \cap A_k = A_1 A_2 \cdots A_k$, so
$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap ... \cap A_k) \cong R/A_1 \times R/A_2 \times ... \times R/A_k$

22.6 Section 8.1: Euclidean Domains

Assume that all rings are commutative.

Definition 58 (Norm in an Integral Domain)**.** *Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a **norm** on the integral domain R. The norm is essential a measure of "size" in R.*

Definition 59 (Euclidean Domain)**.** *The integral domain R is said to be an **Euclidean Domain** if there is a norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$, there exists elements q and r in R with*

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the quotient and the element r is called the remainder of the division.

This property enables the Euclidean Algorithm by successive "divisions" to find a r_n, the last nonzero remainder.

Proposition 19. *Every ideal in a Euclidean Domain is principal. MOre precisely, if I is any nonzero ideal in the Euclidean Domain R, then $I = (d)$ where d is any nonzero element of I of minimum norm.*

Definition 60 (GCD of Ideals)**.** *If I is the ideal of R generated by a and b, then d is the greatest common divisor of a and b if*

1. *I is contained in the principal ideal (d) and*
2. *if (d') is any principal ideal ocntaining I, then (d) $\subseteq$ (d')*

The greatest common divisor of the ideal generated by (a, b)—if it exists—is a generator for the unique smallest principal ideal containing a and b.

Proposition 20. *If a and b are nonzero elements i the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then then d is a greatest common divisor of a and b.*

This explains why the symbol (a, b) is used to denote both the ideal generated by a and b as well as the greatest common divisor of a and b.

Proposition 21 (Uniqueness of GCDs)**.** *Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e. (d) = (d'), then $d' = ud$ for some unit u in R.*

Theorem 22. *Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then*

1. *d is a greatest common divisor of a and b and*
2. *the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an R-linear combination of a and b, i.e. there exists elements x and y in R such that*

$$d = ax + by$$

22.7 Section 8.2: Principal Ideal Domains (P.I.D.s)

Definition 61 (Principal Ideal Domain)**.** *A **Principal Ideal Domain** is an integral domain in which every ideal is principal (i.e. generated from a single element: (a)).*

We showed in 8.1 that every Euclidean Domain is a Principal Ideal Domain, so results about Principal Ideal Domains will also hold for Euclidean Domains. **However, every Principal Ideal Domain is not necessarily an Euclidean Domain**. We think of Principal Domains as one step more general than Euclidean Domains: every ideal can be generated by a single value, but there's no sense of "size".

Conceptually, Principal Ideal Domains are a natural class of rings beyond fields (where the ideals are the trivial (0) and (1)). However, differing from Euclidean Domains, Principal Ideal Domains do not have a notion of "norm" or "size". This result has tangible applications: greatest common divisors exist in P.I.D.s; however unlike in Eucliean Domains, we cannot apply the Euclidean algorithm to compute them as there's no notion of "size".

Proposition 22. *Let R be a P.I.D. adn a, b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then*

1. *d is a greatest common divisor of a and b.*
2. *d can be written as an $R-$lienar combination of a adn b: i.e. there are elements x and y in R with $d = ax + by$.*
3. *d is unique up to multiplication by a unit of R.*

22.8 Section 8.3: Unique Factorization Domains (U.F.D.s

Taking another step more general, *every Principal Ideal Domain is a Unique Factorization Domain*; however, not every Unique Factorization Domain is a Principal Ideal Domain.

Definition 62. *Let R be an integral domain.*

1. *Suppose $r \in R$ is nonzero and is not a unit. Then r is called irreducible in R if whenever $r = ab$, then at least one of a or b must be a unit in R*
2. *The nonzero element $p \in R$ is called prime if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p|ab$ for any $a, b \in R$, then either $p|a$ or $p|b$.*
3. *Two elements a, b of R differing by a unit are said to be associates in R: $a = ub$ for some unit u in R.*

It is not true in general that an irreducible element is necessarily prime. However, if R is a PID, notions of prime and irreducible elements are the same.

Proposition 23. *In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.*

Proposition 24. *In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.*