Class schedule: Math 8510, Fall 2023

WEEK 1: 8/23–8/25. Course overview most of Wednesday. Lecture covering the Chapter 1 slides (pp. 1–29), and the Chapter 2 slides (pp. 1–5).

Summary & key ideas. We introduced *Cayley graphs.* Then, we saw a number of examples of groups: cyclic, dihedral, freize groups, and the quaternions. We saw how these defined algebraic *relations* which allowed us to describe them with a *group presentation* – basically, an algebraic encoding of a Cayley graph. We finished Chapter 1 by formally defining a group. Moving onto Chapter 2, we saw how the n^{th} roots of unity in the complex plane are a cyclic group, generated by any primitive n^{th} root of unity, and how the polynomial $f(x) = x^n - 1$ factors into irreducible cyclotomic polynomials. Next, we introduced cycle graphs, which highlight the individual orbits in a group. We saw two canonical generating sets for the dihedral group D_n: a rotation and reflection $D_n = \langle r, f \rangle$, and two reflections, $D_n = \langle s, t \rangle$.

New definitions and examples to learn:

- Be able to recognize the Cayley graphs of $D_n = \langle r, f \rangle$, $D_n = \langle s, t \rangle$, and Q_8, as well as the group presentations.
- Know the formal definition of a group.
- Be able to construct and interpret a cycle graph of a group.

Left as exercises (make sure you can do these!):

- Every element $g \in G$ has a unique inverse.
- The identity element $e \in G$ is unique.
- $\mathbb{Z}_n = \langle k \rangle$ if and only if $\gcd(n, k) = 1$.

To do:

- Read over the slides that we have covered and please ask questions that you have! This is the "information overload" part of the course – think of it like you just joined a basketball team and are "learning the playbook."
- Try out the proofs that were left as Exercises.

WEEK 2: 8/28–9/1. Three lectures covering the Chapter 2 slides (pp. 18–60), and Chapter 3 slides (pp. 1–24).

Summary & key ideas. Much of the week was spent in Chapter 2, exploring examples of groups, and multiple ways to represent them: Cayley graphs, cycle graphs, and matrices. We started with how to represent groups like V_4, C_n and D_n with 2×2 complex-valued matrices. Then, we introduced directs product and stated the classification theorem of finitely generated abelian groups. Then, we moved onto permutations, and S_n and A_n. After that, built some lesser-known groups like dicyclic, diquaternion, semidihedral, and semiabelian (Dic_n, DQ_n, SD_n, and SA_n). We defined linear and affine groups, and discussed the classification (or lack there of) of finite groups.

We finished the week with the beginning of Chapter 3, and seeing subgroup lattices of all groups of order 4, 6, and 8. Then, we showed that subgroup of cyclic groups are cyclic, and then moved onto cosets. The left and right cosets of a subgroup H partition G, but these partitions are generally different. The normalize of H are the left coset that are also right cosets – in our pictures the "*union of blue cosets*." The number of conjugate subgroups of $H \leq G$ is in some sense a "measure of how close/far from being normal H is." This is equal to the index $[G : N_G(H)]$ of the normalizer.

New definitions and examples to learn.

- Know how to represent D_n with complex-valued 2×2 matrices.
- How to construct a cycle graph given a group.
- How to write a complete list of all abelian groups of some fixed order.
- How to compose permutations and find their order, and inverses.
- The definition of S_n and A_n and basic properties (e.g., nonabelian, trivial center, their sizes).
- S_n is minimally generated by $n-1$ adjacent transpositions, or by a transposition and an n-cycle.
- How to construct/recognize Cayley graphs of D_n, Dic_n, DQ_n, SD_n, and SA_n
- How to represent D_n, Dic_n, DQ_n, SD_n, and SA_n with 2×2 matrices over $\mathbb{C}$.
- *Memorize the subgroup lattices of all groups of order* 4, 6*, and* 8.
- Learn the one-step subgroup test.
- Left and right cosets of H, and the normalizer $N_G(H)$ of H (the left cosets that are right cosets).
- What it means for a subgroup to be normal, moderately unnormal, vs. fully unnormal.
- The center of a group.

Left as exercises (make sure you can do these!):

- The intersection of any collection of subgroups is a subgroup.
- One-step subgroup test: $H \subseteq G$ is a subgroup iff $x, y \in H \ \Rightarrow\ xy^{-1} \in H$.
- The subgroup of $\mathbb{Z}$ generated by $a_1, \ldots, a_k$ is $\langle \gcd(a_1, \ldots, a_k) \rangle \cong \mathbb{Z}$.
- "*Boring but useful coset lemma:*" $xH = H$ iff $x \in H$.
- $aH = bH$ iff $a \in bH$.
- All cosets have the same size (the map $H \to xH$, $h \mapsto xh$ is bijective).
- Lagrange's theorem: If G is finite and $H \leq G$, then $|G| = [G : H] \cdot |H|$.
- If $[G : H] = 2$, then $H \trianglelefteq G$.
- $Z(G) \leq G$ and is normal.
- $H \trianglelefteq N_G(H) \leq G$.
- gHg^{-1} is a subgroup of G, for any $H \leq G$ and $g \in G$.

To do:

- Read over the slides that we have covered and please ask questions that you have!
- Memorize the structure of the Cayley graphs for D_n, Dic_n, SD_n, and SA_n.
- Memorize (be able to construct from scratch) the subgroup lattices of C_4, V_4, C_6, D_3, D_4, Q_8, C_8, $C_4 \times C_2$, and C_2^3.
- Learn what the center $Z(G)$ is for our familiar groups: D_n, S_n, A_n, Dic_n, etc.
- Familiarize yourself with our convention of coloring cosets red vs. blue.
- Try out the proofs that were left as Exercises.

WEEK 3: 9/4–9/8. Labor Day Monday. Two lectures covering the Chapter 3 slides (pp. 10–59) and Chapter 4 slides (pp. 1–12).

Summary & key ideas. Subgroups that are "lattice automorphism invariant" are called *unicorns*, and they must be normal. By conjugating every subgroup in a lattice by some $x \in G$, we can often characterize the conjugacy classes by inspection, and use this to identify the normalizers of each subgroup. We saw that "conjugacy preserves structure," and interpreted this in the symmetric group, dihedral group, and frieze groups. Finally, we finished Chapter 3 with quotients, and showing how G/N is a group iff $N \trianglelefteq G$.

We finished the week with homomorphisms – basic definitions, basic properties, and big ideas. We stated and proved the fundamental homomorphism theorem (FHT), that $G/\operatorname{Ker}(\Phi) \cong \operatorname{Im}(\phi)$, which says that *every homomorphic image is a quotient.* We saw several ways to interpret it, using Cayley graphs and Cayley tables.

New definitions and examples to learn.

- Conjugacy classes of elements
- The centralizer of an element
- Memorize the conjugacy classes of elements in D_n and S_n.
- Given a subgroup $H \leq G$, find its normalizer, and to find all conjugate subgroups, simply conjugate it by one element in each left coset of $N_G(H)$.
- Given an element $h \in G$, find its centralizer, and to find all conjugate elements, simply conjugate it by one element in each left coset of $C_G(h)$.
- Homomorphism, embedding, quotient, preimage, kernel.
- Know that $\phi(1) = 1$ and $\phi(g^{-1}) = \phi(g)^{-1}$.
- Know the statement of the FHT: $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$.

Left as exercises (make sure you can do these!):

- If $|H| = 2$, then $H \trianglelefteq G$ iff $H \leq Z(G)$.
- If $aH = bH$, then $Ha^{-1} = Hb^{-1}$, and hence $aHa^{-1} = bHb^{-1}$.
- Conjugacy is an equivalence relation on subgroups and on elements.
- Every normal subgroup is the union of conjugacy classes.
- The centralizer $C_G(h)$ of h is a subgroup of G.
- $xHx^{-1} = yHy^{-1}$ iff x and y are in the same coset of the normalizer, $N_G(H)$.
- x and y are conjugate in G iff the are in the same coset of the centralizer, $C_G(h)$.
- If $N \trianglelefteq G$, then the cosets G/H forms a group, where $aH \cdot bH = abH$.
- The kernel of a homomorphism is normal.
- The preimage $\phi^{-1}(g)$ is the coset gN of the kernel, $N = \operatorname{Ker}(\phi)$.

To do:

- Get good at being able to determine the conjugacy classes in a subgroup lattice just by inspection. Use this to find the normalizer of each subgroup.
- Learn how to identify normal subgroups that are the "base of a conjugate fan."
- Get good at being able to determine the conjugacy classes of elements in a group, mostly by inspection. Use this to find the centralizer of an element, or vice-versa.
- Make sure that you can prove the fundamental homomorphism theorem.
- Try out the proofs that were left as Exercises.

WEEK 4: 9/11–9/15. Three lectures covering the Chapter 4 slides (pp. 13–79).

Summary & key ideas. We proved the rest of the four *isomorphism theorems*. The first, from last Friday, is the *fundamental homomorphism theorem* (FHT), that $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. Knowing that all homomorphic images are quotients, the other isomorphism theorems tell us about the structure of quotients. The *correspondence theorem* characterizes the subgroups, and the *fraction theorem* characterizes the quotients by these subgroups. The big idea is that taking a quotient corresponds to "chopping off the subgroup lattice" at the kernel. The diamond isomorphism theorem describes a certain "duality" inherent to subgroup lattices. We saw how the commutator subgroup is the smallest subgroups whose quotient is abelian.

We saw how to construct semidirect products both visually and algebraically, using automorphisms. The inner automorphisms are those that can be realized by conjugations; others are "outer." The inner automorphism group $\operatorname{Inn}(G)$ is normal in $\operatorname{Aut}(G)$, and is isomorphic to $G/Z(G)$. We characterized when a group G is isomorphic to a direct or semidirect product of two of its subgroups. Then, we learned how to spot this in the subgroup lattice: N and H must generate G, and intersect trivially. If both are normal, then G is a direct product, and if only one is, its a semidirect product. This lead to the difference between "internal" and "external (semi)direct products.

New definitions and examples to learn.

- Two ways to show two groups are isomorphic: construct a bijective homomrphism, or use the FHT.
- What it means for a function to be well-defined, and when this needs to be verfied.
- Know the statements of the isomorphism theorems, and how to interpret them in terms of subgroup lattices.
- The inner and outer automorphism groups.
- The definition of a semidirect product $A \rtimes_\theta B$, given $\theta\colon B \to \operatorname{Aut}(A)$.
- The commutator subgroup and abelianization.

Left as exercises (make sure you can do these!):

- Show that every homomorphism can be factored as a quotient, followed by an embedding.
- The commutator subgroup G' is normal, and G/G' is abelian.
- $\operatorname{Aut}(\mathbb{Z}_n) \cong U_n$, the groups of units of $\mathbb{Z}_n$.

To do:

- Get good at being able to identify quotients of a group by inspection, using only the subgroup lattice.
- Given a group G, be able to identify the conjugacy classes of its subgroups by inspection, from the subgroup lattice, from knowledge of conjugacy classes of its quotients.
- Be able to identify the commutator subgroup G' in the lattice by inspection.
- Given a subgroup lattice of G, be able to quickly identify all ways that G breaks up as a direct or semidirect product of its subgroups.
- Try out the proofs that were left as Exercises.

WEEK 5: 9/18–9/22. Three lectures covering the Chapter 5 slides (pp. 5–74).

Summary & key ideas. A group action is a homomorphism $\phi\colon G \to \mathrm{Perm}(S)$. Think of having a "group switchboard", where every element has a button. Pressing the a-button followed by the b-button is the same as pressing the ab-button. Common actions include G acting on itself, its subgroups, or cosets. Every action has "five fundamental features": orbits, stabilizers, fixators, kernel, and fixed points. These often arise a familiar algebraic objects. The orbit-stabilizer and orbit-counting theorems quantify the relationships of these quantities. We also saw how to use actions to prove other structural theorems about groups.

A action is *free* if there are no nontrivial "loops" in the action graph. It is *transitive* if there's only one orbit. Actions that are both of these are *simply transitive*, and the resulting action diagrams have the structure of a Cayley graph.

We discussed how "every left action has an equivalent right action", and formalized what it means for two general actions to be equivalent. Every transitive action is equivalent to G acting on cosets of a subgroup H (a stabilizer) by multiplication, and every simply transitive action is equivalent to G acting on itself by multiplication. We then saw a number of examples of simply transitive actions that arise from tilings – finite, affine, and hyperbolic.

Finally, we saw the definition of an *equivariant map*, which is a "structure-preserving map" between actions (or G-sets), like how a homomorphism is a structure-preserving map between groups. Formally, a surjection $\sigma\colon S \to S$ is equivariant if it commutes with the action of the group. The group $\mathrm{Eq}_G(S)$ of equivariant bijections of a set can be thought of as the group of symmetries of the action graph.

New definitions and examples to learn

- Both definitions of a group action (homomorphism $\phi\colon G \to \mathrm{Perm}(S)$ and a map $G \times S \to S$).
- The 5 fundamental features of a group actions (orbit, stabilizers, fixators, kernel, fixed points).
- Our two theorems on orbits: orbit-stabilizer and orbit-counting.
- Common groups actions: G acting on itself by multiplication or conjugation, on its subgroups by conjugation, or cosets by multiplication. Also, $\mathrm{Aut}(G)$ acting on G, or on conjugacy classes of G.
- Free, transitive, and faithful actions.
- Equivariant maps between actions, and equivariant bijections.

Left as exercises (make sure you can do these!):

- Verify that our two definitions of a group action are equivalent.

To do:

- Know how to construct an action graph given a group action.
- Be confortable with the "group switchboard analogy" of group actions, and how to interpret the five fundamental features in terms of it.
- Know how to find the "five fundamental features" of an action from an action graph.
- Know how to construct a fixed point table, and how to spot (four of) our five fundamental features.
- Be able to prove the orbit-stabilizer theorem.

- For our common actions (G acting on itself by multiplication or conjugation, on its subgroups by conjugation, or cosets by multiplication), comfortable with (i) what familiar algebraic objects arise as our "five fundamental features", and (ii) what our two theorems on orbits tell us.
- Understand why elements in the same orbit have conjugate stabilizers.

WEEK 6: 9/25–9/29. Three lectures covering the Chapter 5 slides (pp. 75–111) and Chapter 6 slides (pp. 1–2 and 10–32).

Summary & key ideas. We started with the "p-group lemma": if a p-group G acts on a set, then $|\operatorname{Fix}(\phi)| \equiv |S|$ modulo p. We then proved a few properties of normalizers of p-groups and p-subgroups, which was basically this lemma applied to a particular group action. Next up were the *Sylow theorems*, which tell us a lot about a group G of order $|G| = p^n m$, where $p \nmid m$ is prime. Before we stated these, we proved a few basic results about *p-groups*, which are subgroups of order p^n. If a p-group G acts on a set S, then $|\operatorname{Fix}(\phi)| \equiv |S|$ modulo p. The main utility of this lemma is that by setting up a particular group action, we get that in any group G, a (non-maximal) p-subgroup H must have a normalizer that is *strictly bigger* than H. That is, H cannot be fully unnormal, unless $|H| = p^n$.

A "maximal" p-subgroup (i.e., one of order p^n) is called a *Sylow p-subgroup.* The first Sylow theorem tells us that *p-groups of all possible sizes exist, and they're nested into "towers" in the subgroup lattice.* The second Sylow theorem says that the *top of these towers (the Sylow p-subgroups) form a single conjugacy class.* We proved both of these. Along the way, we took a "mystery group" of order 12, and deduced as much as we could about its structure just from its size, and the Sylow theorems. We used the 3rd Sylow theorems to prove that there are no simple groups of order n, for certain values of n. We finished Wednesday's class with the classic musical number, *Finite simple group of order* 2.

We skipped the proof (which is through a series of four lemmas), that finite abelian groups are products of cyclic groups, because a more general statement will be done in Math 8520 in the setting of modules. We proved that A_n is simple for all $n \geq 5$. To do this, we first analyzed the conjugacy classes. Upon restricted S_n to A_n, each class is either preserved, or splits in two, depending on whether the centralizer $C_{S_n}(\sigma)$ is contained in A_n or not. The proof that A_n is simple rests on two basic properties: A_n is generated by 3-cycles, and all 3-cycles are conjugate. We showed how *every* nontrivial normal subgroup contains a 3-cycle, and thus every 3-cycle.

Finally, we introduced what it means for a group G to be an *extension of H by N*, how to interpret this as an exact sequence $1 \to N \hookrightarrow G \twoheadrightarrow H \to 1$. and what it means for two extensions to be equivalent. We always have $N \trianglelefteq G$ and $H \cong G/N$, but in some cases, we also have $G \cong N \rtimes H$ (right split) or even $G \cong N \times H$ (left split).

New definitions and examples to learn

- p-subgroups and Sylow p-subgroups.
- Simple groups.
- Know that A_n is simple for all $n \geq 5$.
- Conjugacy classes in A_n either are the same as S_n, or are split in two.

- What it means for G to be an extension of N by H, and types of short exact sequences (right split when $G \cong N \rtimes H$ and left split when $G \cong N \times H$).

Left as exercises (make sure you can do these!):

- Show that the center of a p-group is nontrivial.

To do:

- Learn the statements of the Sylow theorems.
- Practice using the 3rd Sylow theorem to prove that groups of a certain order are not simple. Usually this means showing that $n_p = 1$ for some prime.
- Be able to determine whether an extension is right or left split by inspection the subgroup lattice.

WEEK 7: 10/2–10/6. Three lectures covering the Chapter 6 slides (pp. 33–75). HW 6 due Friday.

Summary & key ideas.

We proved that a short exact sequence $1 \to N \to G \to H \to 1$ splits (is "right split") if and only if $G \cong N \rtimes H$. Additionally, it is left split if and only if $G \cong N \times H$, but that is left for homework.

Next, we started at the top of a subgroup lattice and took "simple steps" down to the bottom, which defined a composition series. This shows that every group can be built from simple extensions. The Jordan-Hölder theorem says that every composition series has the same (simple) factors, which can be thought of as a "unique factorization theorem" for groups. Groups are *solvable* iff all of these factors are cyclic (the other possibility are non-abelian simple groups). Another way to "climb down" a subgroup lattice is to take "maximum abelian steps" down, which reaches the bottom iff G is simple. This defines the *derived series*, of iteratively taking the commutator subgroup. Groups that are simple can alternatively be described as those that can be built using only *abelian extensions*.

We then looked at a way to "climb up" a subgroup lattice – by jumping up to the center, chopping it off there (via a quotient $G/Z(G)$), and repeating this process. If these "maximal central ascents" eventually reach the top, then G is *nilpotent*. Alternatively, we can climb down a subgroup lattice via "maximal central descents", by iteratively taking $L_{k+1} = [G, L_k]$. This reaches the bottom iff the ascending central series reaches the top, and if so, then both take the same number of steps. We built a so-called *chutes and ladders diagram* by annotating a subgroup lattice with maximal central ascents (blue) and descents (red) from each normal subgroup.

The ascending and descending central series of a nilpotent group are examples of a *central series*, which goes from the bottom to the top of a subgroup lattice, with each step being a central extension. In this framework, G is nilpotent iff it can be built using only *central extensions*.

New definitions and examples to learn

- The descending central series.
- Chutes and ladders diagrams.

- A (general) central series.
- Learn the 6 equivalent conditions of nilpotent groups.
- A composition series of a group.
- The derived series of a group.
- Two equivalent conditions of what it means to be solvable (composition factors are cyclic, or the derived series reaches the bottom).
- Maximal central ascents and descents.

Left as exercises (make sure you can do these!):

- If $N \leq G$, then G/N is abelian iff $G' \leq N$.
- If $K \leq H \leq G$, then $[K, K] \leq [H, H]$.
- $\phi([h, k]) = [\phi(h), \phi(k)]$, and $\phi([H, K]) = [\phi(H), \phi(K)]$.
- If $N \trianglelefteq G$, then G is solvable iff N and G/N both are (see picture from class).
- If H/N and K/N are central in G/N, then so is HK/N.
- G is the product of its Sylow p-subgroups iff they're all normal.

To do:

- Be able to find all composition series of a group G by inspection, using the subgroup lattice.
- Be able to find the derived series of a group by inspection, using the subgroup lattice.
- Be able to find the ascending central series of a group by inspection, using the subgroup lattice.
- Be able to construct the chutes and ladders diagram, from inspection of the subgroup lattice.
- Go over the details of the proof that $L_k \leq Z_{n-k}$, which we rushed at the end of class.

WEEK 8: 10/9–10/13. Three lectures covering the Chapter 6 slides (pp. 76–83), and the Chapter 7 slides (pp. 1–30). HW 7 due Friday.

Summary & key ideas.

We finished Chapter 6 by proving a number of equivalent conditions of what it means for G to be nilpotent (normalizers always group, all Sylow p-subgroups are normal, every maximal subgroup is normal, etc.)

We started Chapter 7 by looking at commutative diagrams, and what it means for a map f to factor through another map. There are two "types" for $f = h \circ g$: (i) given f and g, when does h exist, and (ii) given f and h, when does g exist.For one of these, existence implies uniqueness if the maps are surjective, and for the other one, if the maps are injective. In other words, surjective functions have right inverses, and injective functions have left inverses.

We formalized the co-universal property of quotient groups, and then abstract this to general universal and co-universal properties. In general, when a particular object is the "largest" or "smallest" with respect to a particular property, we usually have a (co-)universal property lurking. For example, "*G/N is the largest quotient that collapses N*", or "*G/G' is the largest abelian quotient of G*." In a universal property, the map goes between the domains, and in a co-univeral property, it goes between the co-domains. Most books don't distinguish these, and call them both "universal properties." We phrased central descents and ascents in terms of a co-universal and universal property.

We motivated the ideas of product vs. co-product by asking what is the limit of $\mathbb{R}^n$ as $n \to \infty$, which can be thought of as a vector space or abelian group. Loosely speaking, the "product" is the smallest space P that projects onto each factor $P \twoheadrightarrow X_i$, and the "co-product is the smallest space S for which each factor embeds into, $X_i \hookrightarrow S$. In vector spaces (or abelian groups), ths former is the Cartesian product (all sequences), and the latter is the direct sum (all sequences where all terms have finite support).

New definitions and examples to learn

- Know the two "types" of factoring maps, and which one works (existence implies uniqueness) for quotients and which one works for embeddings.
- Know the cancelation laws: surjective maps right-cancel (they have right inverses), and injective maps left-cancel (they have left inverses).
- What it means for a map ϕ from G to descend to a map from G/N.
- A universal and co-universal pair.

WEEK 9: 10/17–10/21. Three lectures covering the Chapter 7 slides (pp. 7–41). HW 8 due Friday.

Summary & key ideas.

We introduced the notion of a *category* $\mathcal{C}$, which consists of a class $\mathrm{Ob}(\mathcal{C})$ of *objects* (e.g., sets, groups, vector spaces, topological spaces) and a class $\mathrm{Hom}(\mathcal{C})$ of structure-preserving maps called *morphisms* (e.g., functions, homomorphisms, linear maps, continuous functions). One can think of a category as a massive direct multigraph where we require identity morphisims for every object, and composition and associativity of morphisms. The concepts of being 1-to-1 and onto are abstract by *monomorphisms* (those that left cancel) and *epimorphisms* (those that right cancel), and we can abstract concepts like product and coproduct as well via universal constructions.

A *functor* is a structure-preserving map between categories. Examples include the fundamental group, that sends a topological space to a group, and the abelianization, that sends G in **Grp** to G/G' in **Ab**. Functors can be covariant or contravariant, if they "reverse the arrows". The map that sends a vector space to its dual is contravariant. One can think about this as the "transpose map" that sends column vectors to row vectors, and A to A^T.

New definitions and examples to learn

- The product and co-product of a family of groups.
- A category.
- Types of morphisms in a category: monomorphism, epimorphism, isomorphism.
- Functors – both covariant and contravariant.

To do:

- Be able to statement the co-universal properties of quotient groups and commutators, and draw the corresponding diagram.
- Practice the "diagram stacking" technique of showing uniqueness of a (co-)universal property.

WEEK 10: 10/23–10/27. Three lectures covering the Chapter 6 slides (pp. 42–72). HW 9 due next Tuesday.

Summary & key ideas.

An *initial* (resp., *terminal*) object in a category has a unique morphism to (resp. from) every object. In **Grp**, the trivial group is both initial and terminal, which is called a *zero object*. In **Set**, the initial object is $\emptyset$, and every singleton set is terminal. Initial (resp. terminal) objects are equivalent up to equivalence. If a family $\{A_i\}$ of objects has a coproduct (resp., product), then we can carefully construct a category for which that is the unique initial (resp., terminal) object. This gives uniqueness of coproducts (resp., products) for free. If a category has a zero object, then the composition of the unique maps $A \to \mathbf{0} \to B$ is the *zero morphism* 0_{AB}. This can be used to show that the "projection morphisms" π_j from a product are epimorphisms, and the "inclusion morphisms" ι_j into a coproduct are monomorphisms.

A *free group* on a set S is the group $G = \langle S \mid \ \rangle$. This is the "largest" group on S, in that every other group generated by S is a quotient of it. We can formalize this with a univeral property, that we will actually use as the formal definition. Such a definition does not guarantee existence, so we had to construct it. We did this by using *semigroups*, which are like groups but without inverses or an identity element. It is straightforward to show that the *free semigroup* on a set exists – it is simply the set of all words over that set. Given the set S, we took a disjoint copy S' that we can think of as "formal inverses", and consider the free semigroup on $T := S \cup S'$. Then, we defined an equivalence relation where $tt'x = x$, $xtt' = x$, and the resulting quotient was a group. We showed that this group is free on S using the universal property.

A category is *concrete* if there is a faithful functor to **Set**, i.e., if every underlying object has a natural set structure. In concrete categories, we can define the notion of a free object. In **Ab**, free objects are direct sums. To formalize this, we defined a *basis* of an abelian group, which shares some properties of a vector space basis.

New definitions and examples to learn

- Initial, terminal, and zero objects in a category.
- Free groups and free objects.
- A basis of an abelian group.

Left as exercises (make sure you can do these!):

- Verify the claim that the set of nonempty words over S is a free semigroup on S.
- Fill in the details of the proof sketch that free abelian groups are direct sums.

To do:

- Go over the details of the proof that the quotient X/R of our free semigroup is indeed a free group. (Everything is on the slides.)

WEEK 11: 10/30–11/3. Three lectures covering the Chapter 6 slides (pp. 72–97) and the Chaper 7 slides (pp. 1-27). HW 9 due Tuesday.

Summary & key ideas. We formalized the notion of a group presentation, $G = \langle S \mid R\rangle$, as the quotient of the free group F_S by the smallest normal subgroup containing the set R of relators. If we want to show that a mystery group $M = \langle S_1 \mid R_2\rangle$ is isomorphic to a familiar group $F = \langle S_2 \mid R_2\rangle$, then we (i) use generators and relations to show that $|M| \leq |F|$, and then (ii) find a map $\theta\colon S_1 \twoheadrightarrow S_2$ that preserves relations.

Next, we looked at what coproducts are in the categories **Ab** and **Grp**. In **Ab**, they are direct sums, and in **Grp**, they are a new construction called *free products*. The free product of $A = \langle S_1 \mid R_1\rangle$ and $B = \langle S_2 \mid R_2\rangle$ is the group $A * B = \langle S_1 \sqcup S_2 \mid R_1 \sqcup R_2\rangle$. We have already seen examples of this without realizing it: $C_2 * C_2 \cong D_\infty$, and $C_3 * C_2 \cong \mathrm{PSL}_2(\mathbb{Z})$.

Then, we looked at "amalgamated free products", which can be thought of taking the free product of two groups and identifying them along a common normal subgroup. This can be defined in general categories as a *fiber coproduct*, or a *pushout*. The celebrated Siefert van-Kampen theorem from topology says that the fundamental group, as a functor $\pi_1\colon \mathbf{Top} \to \mathbf{Grp}$, preserves pushouts. The dual notion of this is a *fiber product*, or *pullback*, and that concluded the section of groups.

A *ring* is an additive abelian group with an additional binary operation (multiplication), that satisfies the distributive law. Loosely speaking, rings are sets where we can add, subtract, and multiply, but not necessarily divide. There are three types of "substructures" of interest: subgroups (closed under $+$ and $-$), subrings (also closed under $*$), and ideals (closed under $*$ from *any* $r \in R$). In a noncommutative ring, there can be a distinction between left, right, and two-sided ideals (or just "ideals"). The *subring lattice* of R is just the subgroup lattice, with subgroups colored depending on whether they are ideals, subrings that aren't ideals, or subgroups that aren't subrings. There are 11 rings of order 4, and we saw all of them. The eight that have additive subgroup $\mathbb{Z}_2^2$ all have distinct subring lattices. We also saw some examples of infinite rings, including the *Hamitonians*, which are numbers of the form $a + bi + cj + dk$, that contain $\mathbb{C}$ as a subring.

A *unit* of a ring R is an element with a multiplictive inverse. Proper ideals cannot contain units. A *zero divisor* is an element $x \in R$ for which $xy = 0$ for some $y \neq 0$. Rings in which every nonzero element is a unit are called *division rings*: *fields* if commutative, and *skew fields* otherwise. For example, $\mathbb{Q}(\sqrt{m})$ is a fiefld, and $\mathbf{H}$ a skew field. An *integral domain* is a commutative ring with 1 that has no (nonzero) zero divisors – basically a "field without inverses." Every finite integral domain is a field. The cancelation property $ax = ay$ implies $x = y$ holds as long as a is not a zero divisor. Two-sided ideals are precisely the subrings of R that we can quotient out by. In the *quotient ring* R/I, we define multipliction as $(x + I)(y + I) := xy + I$.

New definitions and examples to learn

- A group presentation $G = \langle S \mid R\rangle$.
- Free product with amalgamation.
- A ring, and what it means to be commutative, have identity, etc.
- Left, right, and two-sided ideals, and how to define the ideal generated by a set, $I = (X)$.
- The Hamiltonians.
- Units and zero divisors.

- Division rings, fields, skew fields.

Left as exercises (make sure you can do these!):

- The coproduct of groups is their free product.
- If R has 1, then $(X) = \big\{r_1x_1s_1 + \cdots + r_nx_ns_n \mid n \in \mathbb{N},\ r_i, s_i \in R,\ x_i \in X\big\}$.

To do:

- Be able to read and construct subring lattices, and the difference between ideals, subrings, and subgroups.
- Familiarize yourself with examples of rings that we'll see a lot: matrices, polynomials, Hamitonians.

WEEK 12: 11/6–11/10. Three lectures covering the Chapter 7 slides (pp. 28–75). HW 10 due Tuesday.

Summary & key ideas.

A *ring homomorphism* is a group homomorphism $f\colon R \to S$ that also satisfies $f(xy) = f(x)f(y)$ for all $x, y \in R$. Kernels are (two-sided) ideals, and there are four isomorphism theorems for rings that are analogous to the ones for groups.

By the correspondence theorem, an ideal $M \subseteq R$ is maximal iff R/M is simple, and if R is commutative, this is equivalent to R/M being a field. Zorn's lemma says that every nonempty poset in which every chain has an upper bound has a maximal element. This is equivalent to the axiom of choice, and it can be used to show that every ideal $I \subsetneq R$ is contained in a maximal ideal. This rests on the fact that ideals cannot contain units, and so any union $I_1 \subseteq I_2 \subseteq \cdots$ will also be a proper ideal. This is in stark contrast to subgroups, in which the union of a chain $H_1 \subseteq H_2 \subseteq \cdots$ of proper subgroups need not be proper. An example of this is the *Prüfer group*, consisting of the p^n-th roots of unity, for all $n \in \mathbb{N}$.

The *characteristic* of a field, $\text{char}(\mathbb{F})$ is the minimal n such that $n1 = 1 + \cdots + 1 = 0$, or zero if there is no such n. If $\text{char}(\mathbb{F})$ is finite, then it must be prime. Every finite field has the form $\mathbb{F}_p[x]/(f)$, for some irreducible polynomial $f(x)$. By thinking of a finite field K as an $\mathbb{F}_p$-vector space, taking a basis, and counting elements, we immediately conclude that $|K| = p^n$. Similarly, we can deduce that if $K \subseteq L$ are finite fields of order p^n and p^m, then n divides m. Soon, we'll prove the a degree-n polynomial can have at most n roots. For now, that implies that any finite subgroup of the multiplictive group of a field must be cyclic. (Otherwise, it would contain a copy of $C_q \times C_q$ for some prime, which would give q^2 roots to the polynomial $f(x) = x^q - 1$).

Henceforth, assume R to be commutative. An ideal P is *prime* if $ab \in P$ implies either $a \in P$ or $b \in P$. Over the integers, prime ideals are of the form (p) for some prime number p. An equivalent characterization to P being prime is that R/P is an integral domain. Since M is maximal iff R/M is field, and fields are integral domains, every maximal ideal is prime. A weaker condition than prime is a *primary ideal*, which means that $ab \in P$ implies $a \in P$ or b^n for some $n \in \mathbb{N}$. For the integers, there are ideals (p^n) generated by prime powers.

A *radical* of a ring R is an ideal of "bad elements," for which R/I is "nice." The two most common example are the *nilradical* and the *Jacobson radical.* The nilradical is the intersection of all prime ideals, or equivalently, the set of all nilpotent elements (all $x \in R$ such that $x^n = 0$ for some n). The Jacobson radical is the intersection of all maximal ideals, or equivalently, the set of all $x \in R$ for which $1 - rx$ is a unit for every $r \in R$. The quotient $R/\operatorname{Nil}(R)$

is a subproduct of integral domains, and the quotient $R/\operatorname{Jac}(R)$ is a subproduct of fields. We can also define these concepts for ideals, not just rings. For example, the *radical* of I, denoted $\sqrt{I}$, is the intersection of the nonzero prime ideals containing I. The *Jacobson radical* $\operatorname{jac}(I)$ of I is the intersection of all maximal ideals containing it. Note that $\operatorname{Nil}(I) = \sqrt{0}$ and $\operatorname{Jac}(R) = \operatorname{jac}(0)$.

New definitions and examples to learn

- Ring homomorphisms and the definition of a quotient ring R/I.
- The characteristic of a field.
- Maximal ideals and simple rings.
- Zorn's lemma and how to apply it.
- Know how to construct the finite field $\mathbb{F}^{p^n}$.
- Prime and primary ideals.
- A subdirect product of rings.
- The radical $\sqrt{I}$ and Jacobson radical $\operatorname{jac}(I)$ of an ideal.
- The nilradical $\operatorname{Nil}(R) = \sqrt{0}$ and Jacobson radical $\operatorname{Jac}(R) = \operatorname{jac}(0)$ of a commutative ring.

Left as exercises (make sure you can do these!):

- Proofs of the ring isomorphism theorems, assuming the results of the group isomorphism theorems. (Much of this is just showing that the maps are not just group, but ring isomorphisms.)
- Given a chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals, $\cup I_k$ is an ideal.
- Show that every non-unit is contained in a maximal ideal.

To do:

- Learn the statements and meaning of the ring isomorphism theorems.
- Learn how to construct a finite field $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f)$.
- Verify the examples and non-examples of prime ideals.
- Formalize the proof sketch to verify that if $\mathbb{F}_{p^n}$ contains $\mathbb{F}_{p^m}$, then $n \mid m$.
- R is an integral domain iff $\{0\}$ is a prime ideal.

WEEK 13: 11/14–11/18. Three lectures covering the Chapter 8 slides (pp. 76–85) and Chapter 9 slides (pp. 1–23). HW 11 due Tuesday.

Summary & key ideas. We showed how a ring R with a multiplicative semigroup D without zero divisors sits inside a ring where every $d \in D$ is a unit. We constructed such a ring, denoted $D^{-1}R$, as the set of ordered pairs ("fractions") under a natural equivalence relation. This is the "smallest" such ring, and satisfies a co-univeral property. A special case of this is when $D = R^*$ in an integral domain, and the result is the *field of fractions*. We can actually allow D to have zero divisors, but the canonical map $R \to D^{-1}R$, $r \mapsto r/1$ is no longer injective.

Next, we begun looking at divisibility and factorization in integral domains. Since $a \mid b$ iff $(b) \subseteq (a)$, the key idea is that *concepts on divisibility are much cleaner in the language of ideals*. In rings in which every ideal is principal (generated by a single element), the lattice of ideals is basically the lattice of divisors, and so divisbility and factorization are very well-behaved. These rings are called *principal ideal domains* (PIDs). In contrast, when unique factorization fails, like $3 \cdot 3 = (2-\sqrt{-5})(2+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$, there are non-principal ideals, like $(3, 2-\sqrt{-5})$.

We say that elements $a, b \in R$ are *associates* if $a \mid b$ and $b \mid a$. An element p is *irreducible* if its only divisors are associates and units. It is *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$. In a PID, these concepts coincide. In general, we always have prime $\Rightarrow$ irreducible. For example, $3 \mid (2-\sqrt{-5})(2+\sqrt{-5}) = 9$ is irreducible but not prime because $3 \nmid (2 \pm \sqrt{-5})$.

A weaker condition than a ring being a PID is being *Noetherian*: every ideal is finitely generated. Equivalentally, every ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes.

In a principal ideal domain (PID), properties of divisibility can be read right off the "lattice of ideals." Since $a \mid b$ iff $(b) \subseteq (a)$, the smallest ideal containing (a) and (b) is $(\gcd(a,b))$, and their intersection is $(\operatorname{lcm}(a,b))$. Irreducibles are primes, and prime ideals are maximal. A *unique factorization domain* (UFD) is a weaker type of ring than a PID, where (i) every nonzero element is a product of irreducibles, and (ii) every irreducible is prime. Failure of (ii) would lead to an infinite chain $I_1 \subsetneq I_2 \subsetneq \cdots$, which would imply that R isn't Noetherian (and certinaly not a PID). Examples of UFDs that aren't PIDs are $\mathbb{Z}[x]$ and $F[x,y]$. Non-examples of UFDs include $\mathbb{Z}[\sqrt{-5}]$ (unique factorization fails) and $\mathbb{Q}[x, x^{1/2}, x^{1/4}, \dots]$ (non-atomic).

We discussed a few other types of domains, like Bézout comains, where every ideal (a,b) is generated by the GCD (i.e., $d = ax + by$ for some $x, y \in R$), and GCD domains, where every ideal (a,b) *contains* an ideal generated by the GCD. In a Bézout domain, all finitiely generated ideal are principal; the ring $\mathbb{Z} + x\mathbb{Q}[x]$ is an example.

New definitions to learn

- The field of fractions F_R of an integral domain.
- The ring of fractions of D in R, where D is a multiplicative semigroup without zero divisors.
- Basics of divisibility (a divides b, or b is a multiple of a, associates, irreducibles, units).
- Principal ideals and principal ideal domains (PIDs).
- Common divisors and multiples; GCD and LCM in a PID.

New examples to learn

- Rings where unique factorization fail.
- Irreducibles that are not prime.
- Prime, primary, and radical ideals ideals in $\mathbb{Z}$.

Left as exercises (make sure you can do these!):

- Fill in the details of the construction of the ring of fractions (HW).
- Check that the map $\iota\colon r \mapsto \frac{r}{1}$ is a monomorphism (HW).

WEEK 14: 11/21–11/25. One lecture covering Chapter 9 slides (pp. 24–37). HW 12 due Tuesday.

Summary & key ideas.

In the integers, the Euclidean algorithm is used to compute the GCD of two numbers. Though GCDs exist in PIDs, there does not necessarily always exist a Euclidean algorithm to compute them. However, we can define the class of rings for which there is such an algorithm, and we call these *Euclidean domains*. Formally, this involves a *degree function* $d\colon R^* \to \mathbb{Z}$ satisfying some basic properties (non-negativity, monotonicity, and division-with-remainder). In $\mathbb{Z}$, this "degree" is just $|n|$, and in $F[x]$, it is $\deg(f(x))$. We proved some basic properties about PIDs, like how the elements with minimal degree are precisely the units, and how every Euclidean domain is a PID.

Finally, we revisited the *quadratic field* $\mathbb{Q}(\sqrt{m})$ for a fixed square-free $m \in \mathbb{Z}$, and this is isomorphic to $\mathbb{Q}[x]/(x^2 - m)$. The *field norm* in this ring is defined as $N(a + b\sqrt{m}) = a^2 - mb^2$. If $m < 0$, then this is simply the square of the complex absolute value, $N(z) = z\bar{z} = |z|^2$. If $m > 0$, then this need not even be a norm in the analysis sense, since $a^2 - mb^2$ can be negative. The rational numbers $\mathbb{Q}$ have $\mathbb{Z}$ as a subring, which are the roots of degree-1 monic polynomials in $\mathbb{Z}[x]$. Analogously, the field $\mathbb{Q}(\sqrt{m})$ has a subring of roots of degree-2 monic polynomials in $\mathbb{Z}[x]$, called "quadratic integers". This ring, denoted R_m, is $\mathbb{Z}[\sqrt{m}]$ if $m \equiv 2$ or 3 mod 4, and $\mathbb{Z}\big[\frac{1+\sqrt{m}}{2}\big]$ otherwise. If $m > 0$, then they all lie on the real line, are harder to analyze, and aren't as well understood. For $m < 0$, if $m \equiv 2, 3 \pmod 4$, then $R_m = \mathbb{Z}[\sqrt{m}]$ are lattice points in $\mathbb{C}$ of a retangular lattice.

New definitions and examples to learn

- UFDs, Euclidean domains, Noetherian rings.
- The quadratic field $\mathbb{Q}(\sqrt{m})$, quadratic integers R_m, and field norm.

Left as exercises (make sure you can do these!):

- A ring is Noethering if and only if every ideal is finitely generated.
- Verify that $f(x) + I \mapsto f(\sqrt{m})$ is an isomorphism $\mathbb{Q}[x]/(x^2 - m) \to \mathbb{Q}(\sqrt{m})$.
- The field norm is multiplicative: $N(xy) = N(x)N(y)$.
- $x \in \mathbb{Q}(\sqrt{m})$ is a unit iff $N(x) = \pm 1$.

To do:

- Study the types of rings that we've seen (commutative, integral domains, UFDs, PIDs, Euclidean domains, and fields), know examples of each, which classes are contained in other classes, etc.

Week 15: 11/27–12/1. Two lectures covering Chapter 9 slides (pp. 38–63). Midterm Wednesday. HW 13 due Friday.

Summary & key ideas.

We showed that this a Euclidean domain iff $m = -2$ or -1, i.e., these rectangulars aren't "too tall". If $m \equiv 1 \pmod 4$, then $R_m = \mathbb{Z}\big[\frac{1+\sqrt{m}}{2}\big]$ are the lattice points of a triangular lattice. These are a Euclidean domain (for $m < 0$) iff $m = -3, -7, -11$, i.e., these triangles aren't "too tall." We discussed some known results about these rings from number theory, like that R_m for $m < 0$ is a PID but not Euclidean domain iff $m = -163, -67, -43$, or -19.

In rings that fail to be a UFD, like $\mathbb{Z}[\sqrt{-5}]$ (because $3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$), there are irreducibles that are no longer prime. The *class group* from algebraic number theory describes, in some sense, the degree to which unique factorization fails. Each integer prime $p \in \mathbb{Z}$ does one of three things upon passing to the larger ring R_m: it *splits* (factors) as $p = z\,\overline{z}$, is *inert* (remains prime), or is *ramified* (is a perfect square, $p = \overline{z}^2$). It is easiest to characterize this behavior in terms of ideals: splitting means $(p) = P_1P_2$ for distinct prime ideals, inert means (p) is a prime ideal, and ramified if $(p) = P^2$. This is all the tip of the iceberg of the topic of *class field theory*, from algebraic number theory.

Finally, we finished with *Sunzi's remainder theorem.* The most basic version says that any system of k equations $x \equiv a_j \pmod{n_j}$ has a solution, as long as $n_1, \dots, n_k$ are pairwise co-prime, and any two solutions are equivalent modulo $n_1 n_2 \cdots n_k$. We generalized this to PIDs, then to commutative rings, and then to arbitrary rings, by replacing

- $x \equiv a_i \pmod{n_i}$ with $x \equiv a_j \pmod{I_j}$,
- $\gcd(n_i, n_j) = 1$ with $I_i + I_j = R$.
- solutions being equivalent modulo $n_1 n_2 \cdots n_k$ with solutions in the same coset of $I_1 I_2 \cdots I_n$ (for commutative rings), and then $I_1 \cap \cdots \cap I_k$ (for general rings).

The proof will be left for next week.

New definitions and examples to learn

- The difference between split, inert, and ramified primes in R_m.

To do:

- Learn the statement of Sunzi's remainder theorem, both in $\mathbb{Z}$ and for general rings and ideals.

Week 16: 12/4–12/8. Three lectures covering Chapter 9 slides (pp. 64–84) and supplemental material. HW 14 due Friday.

Summary & key ideas. We prooved Sunzi's remainder theorem in arbitrary rings.

Henceforth, let R be a UFD. A polynomial in $R[x]$ is *primitive* if the GCD of its coefficients is 1. We proved Gauss' lemma: if $f(x)$ and $g(x)$ are primitive, then so is $f(x)g(x)$. Finally, we proved the theorem that if we can't factor a polynomial (i.e., if its irreduicible) in $R[x]$, then we can't factor it in $F[x]$, where F is the field of fractions of R. Finally, we formulated Eisenstein's criterion: if a prime p divides all coefficients of $f(x) = a_n x^n + \cdots + a_1 x + a_0$ except a_n, and $p^2 \nmid a_0$, then $f(x)$ is irreducible.

We finished with Hilbert's basis theorem: If a ring R with 1 is Noetherian (equivalently, every ideal is finitely generated), then $R[x_1, \ldots, x_n]$ is Noetherian as well.

New definitions and examples to learn

- Eisenstein's criterion.

To do:

- Study for the final exam!