Class schedule: Math 4120, Spring 2022

- **Week 1: 1/12–1/14**. Course overview Wednesday. One lecture Friday covering the Chapter 1 slides (pp. 1–11). Approximate YouTube content: Lectures 1.1–1.2. HW 1 due next Friday.

  Summary & key ideas. We introduced *Cayley diagrams*, and saw several examples of groups: the symmetries of a rectangle, and of a triangle. We saw how these defined algebraic *relations*.

  To do: Read over the slides, formulate any questions you may have. Look at the HW 1 problems, and attempt #1abc, #2abc, #3a.

- **Week 2: 1/17–1/21**. No class Monday (MLK Day). Two lectures covering the Chapter 1 slides (pp. 12–39). Approximate YouTube content: Lectures 1.3–1.4. HW 1 due next Monday.

  Summary & key ideas. We saw how the same group can have very different looking Cayley diagrams depending on generating sets. Thus far, we have seen 3 groups of size 8. We discussed the Rubik's cube group, cyclic groups, and learned how to label Cayley diagrams with actions. This motivated the idea of a *group presentation*. Finally, we learned about (infinite) frieze groups and classified them.

  To do: Read over the slides, formulate any questions you may have. *Familiarize yourself with the presentations of all of the groups we have seen.* Finish HW 1.

- **Week 3: 1/24–1/28**. Three lectures covering the Chatper 1 slides (pp. 40–56), and the Chapter 2 slides (pp. 1–26). Approximate YouTube content: Lectures 1.5, 1.6 2.1, 2.2, and supplemental material (roots of unity). HW 2 due next Monday.

  Summary & key ideas. We saw that there were "17 different types of wallpaper", and "230 types of crystals." The quaternion group Q_8 was the first abstract group we've seen that doesn't the describe symmetries or actions. By constructing Cayley tables, we were able to see the concept of a *quotient*. We finally gave the formal definition of a group, and several examples of "things that look like groups but aren't", illustrating why a formal definition is needed. Moving into Chapter 2, we learned about roots of unity and how to factor $x^n - 1$ using cyclotomic polynomials. Then, we saw defined cyclic groups, both additively as $\mathbb{Z}_n = \langle 1 \rangle$ and multipliative as $C_n = \langle r \rangle$. Finally, we introduced the dihedral groups D_n, and the notion of a *cycle diagram*. We saw how to represent the group C_n and D_n with 2×2 matrices.

To do: Read over the slides, formulate any questions you may have. Be able to distinguish between a *minimal* and *minimum* generating set. Know how to generate C_n and D_n several different ways. Memorize how to represent the groups V_4, C_n, and D_n with 2×2 matrices. Be able to construct the cycle graph of an abstract group using its Cayley diagram. Finish HW 2, #1–4.

Week 4: 1/31–2/4. Three lectures covering the Chapter 2 slides (pp. 27–60). Approximate YouTube content: Lectures 2.3, 2.4. HW 2 due this Monday, HW 3 due next Monday.

Summary & key ideas. We saw how to construct the direct product of two groups, and prove that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ iff $\gcd(n, m) = 1$. We stated the big theorem that every finite (and finitely generated) abelian group is a direct product of cyclic groups. We saw two ways to classify these: by "prime powers", and "elementary divisors." We introducted permutations, and several ways of encoding them, with *cycle notation* being our go-to method. We learned about even vs. odd permutations. The *symmetric group* S_n consists of all $n!$ permutations, and the *alternating group* A_n consists of all $n!/2$ even permutations. We saw a number of ways to arrange Cayley diagrams of S_4 on various Archimedean solids, and explored different ways to generated S_n. Finally, we stated *Cayley's theorem*: every finite group is isomorphic to a collection of permutations. We saw two algorithms for how to construct such permutations: one from a Cayley diagram, and another from a Cayley table.

To do: Read over the slides, formulate any questions you may have. Be able to write down all abelian groups of order n for a fixed n. Get good at composing permutations in cycle notations, and basic properties such as order, parity, etc. Remember than the cycle $(12 \cdots n)$ is an even permutation iff n is odd, and vice-versa. Know how to generate the symmetric group as both $S_n = \langle (12), \ldots, (n\ n{-}1) \rangle$ and $S_n = \langle (12), (12 \cdots n) \rangle$. Finish HW 3.

Week 5: 2/7–2/11. Three lectures covering the Chapter 2 slides (pp. 61–102). Approximate YouTube content: Lecture 3.4 (0:00–17:02), and supplemental material on permutation matrices, some "lesser known" groups (dicyclic, diquaternion, semidihedral, and semiabelian), rewirings, and automorphisms of cyclic groups. HW 3 due this Monday, HW 4 due next Monday.

Summary and big ideas: We learned about permutation matrices, and how our previous observation of how there were two canonical ways to label a permutahedron (Cayley diagram for S_n) with permutations (swap coordinates, vs. swap numbers) can be realized by right-multiplying row vectors vs. left-multiplying column vectors. Next, we generalized the quaternion groups by replacing $i = \sqrt{-1} = \zeta_4 = e^{2\pi i/4}$ with a larger (even) root of unity ζ_n, to define the *dicyclic group* $\mathrm{Dic}_n = \langle \zeta_n, j \rangle$.

Then we explored how to "rewire" the inner cycle of the Cayley diagram for D_n to define new groups. If n is a power of 2, then there are two new ways to do this, leading to the *semidihedral* and *semiabelian* groups, respectively. We saw how to represent all of these groups with 2×2 matrices involving roots of unity. Next, we reviewed direct products, and explored a visual "inflation method" to construct a Cayley diagram of $A \times B$ from diagrams of A and B, respectively: inflate B-nodes like "balloons" and stick in A-Cayley diagrams, and re-connect nodes across balloons. A *semidirect product* results if we "rewire" A-diagrams (an *automorphism*) before inserting them. We explored this for cyclic groups.

To do: Read over the slides, formulate any questions you may have. Familiarize yourself with the Cayley diagrams of Dic_n, DQ_8, SD_8, and SA_8, and the standard matrix representations of D_n, Dic_n, DQ_n, SD_n, and SA_n. Understand how to "rewire" a Cayley diagram of C_n, how to iterate this process, and why $\mathrm{Aut}(C_n) \cong U_n$. Be able to construct a semidirect product $C_n \rtimes C_m$, for certain n and m that you are given (not all will work).

Week 6: 2/14–2/18. Three lectures covering the Chapter 2 slides (pp. 103–115) and Chapter 3 slides (pp. 1–24). Approximate YouTube content: Lectures 3,1, 3.2, and supplemental material on finite groups. HW 4 due this Monday, HW 5 due next Monday.

Summary and big ideas: If $n = 2^m$, then there are four semidirect products of C_n with C_2: the abelian group $C_n \rtimes C_2$, dihedral group D_n, semidihedral group SD_n, and semiabelian group SA_n. We saw how if $n = 2m$ is even, then D_n is isomomorphic to a direct product of two proper subgroups. We discussed groups of matrices, where the coefficients come from a *field* – a set of numbers where we can add, subtract, multiply and divide. Examples of groups of matrices include the *general linear* ($\det \neq 0$) and *special linear* ($\det = 1$) groups, and affine groups. An example that will reappear is $\mathrm{SL}_2(\mathbb{Z}_3)$, a group of order 24, that is also isomorphic to the *binary tetrahedral group*, 2T, an order-24 subgroup of the *Hamiltonians* (like the quaternions but with coefficients from $\mathbb{R}$). We briefly discussed the goals of breaking up groups into "building block groups", and the surprising fact that there are so many p-groups.

Moving onto Chapter 3, we looked at the subgroups of both groups of order 4, both groups of order 6, and all 5 groups of order 8. These can be visualized in a *subgroup lattice*. To show that a subset $H \subseteq G$ is a subgroup, we learned about the short "one-step subgroup test." We proved that subgroups of cyclic groups are cyclic. Next, we introduced the notion of a *coset*, both visually and algebraically. We saw that left and right cosets are generally different, and proved some basic properties, like the $xH = H$ iff $x \in H$, and how the cosets partition the group.

To do: Read over the slides, formulate any questions you may have. Memorize the subgroup lattices of all groups of order 4, 6, and 8, i.e., be able to construct them without notes. Be able to write down all subgroup of the cyclic group $\mathbb{Z}_n$, and find their orders. Know how to verify that a subset $H \subseteq G$ is a subgroup. Given a subgroup $H \leq G$, be able to find its left and right cosets, both using the Cayley diagram, and algebraically.

Week 7: 2/21–2/25. Three lectures covering the Chapter 3 slides (pp. 25–68). Approximate YouTube content: Lectures 3.3, 3.4 (17:03–23:16) 3.5, 3.6. HW 5 due this Monday, HW 6 due next Monday.

Summary and big ideas: We learned about the tower law ("subgroup index is multipliative"), the center of a group (the elements that commute with everything), and the normalizer of a subgroup (union of left cosets that are also right cosets). The proportion of such cosets is the (reciprocal of the) *degree of normality* of H, and this meausure how close/far a subgroup is to being normal. We also studied conjugate subgroups, and learned the very important tidbit: *the number of conjugate subgroups is the index of the normalizer*. In many cases, we can identify the conjugacy classes and normalizers simply by inspecting the subgroup lattice. Certain subgroups are always normal, such as unicorns, those contained in the center, and those of index 2. We saw two subgroups of order 16 that had the same subgroup lattice. Conjugacy classes of subgroups look like "fans", and their "bases" are always normal. This means that simply group have a very restrictive structure, and we saw the lattice of A_5 as an example. We also looked at conjugate subgroups algebraically, starting with the important fact that $aH = bH$ need not imply $Ha = Ha$, but it does imply that $Ha^{-1} = Hb^{-1}$. This gave us a nice way to find conjugate subgroups on a Cayley diagram. Next, we learned that if A normalizes B (i.e., $aB = Ba$ for all $a \in A$), then AB is a subgroup of G. A weaker but more common condition is: *if at least one of A or B is normal, then $AB \leq G$*. Finally, we formalized the notion of a quotient: G/N is a group iff $N \trianglelefteq G$. Specifically, G/N is the set of left (or right) cosets, and we define $aN \cdot bN := abN$. This works iff N is normal, and is the very important concept of the operation being *well-defined*.

To do: Read over the slides, formulate any questions you may have. Be able to label edges of a subgroup lattice with the index, $[H : K]$. Know examples of where $xH = Hx$ even though $xh \neq hx$, elementwise. Learn the center $Z(G)$ of some of our favorite groups (e.g., D_n, S_n, A_n, Q_8, Dic_n). Be able to find the normalizer of a subgroup H, and know that it is at least H itself (worse case; fully unnormal) and at most G (best case; normal). Be able to find all conjugate subgroups of H from the Cayley diagram. Know all three ways to check that a subgroup is normal, and be aware that sometimes, one of them is much easier than the rest. Get good at being able to determine the conjugacy classes and normalizers of a

subgroup lattice just by inspection, though this is not always possible. Be able to recognize unicorn subgroups. However, given a conjugacy class, you should be able to find the normalizer of one of its subgroups. Given two subgroups A and B in a lattice, determine if AB is a subgroup, and if so, which one it is. Given a normal subgroup $N \trianglelefteq G$, be able to construct a Cayley table of the quotient G/N.

Week 8: 2/28–3/4. One-and-a-half lectures covering the Chapter 3 slides (pp. 73–82). Approximate YouTube content: Lecture 3.7. Midterm 1 Wednesday. HW 6 due this Monday, HW 7 due next Monday.

Summary and big ideas: We proved that G/N is a group if and only if N is normal. Then, we moved onto the idea of conjugating elements: x and y are conjugate if $x = gyg^{-1}$ for some $g \in G$. A theme in mathematics is *conjugate elements have the same structure*. We showed the conjugate elements have the same order, and saw visual interpretations in frieze and dihedral groups. This allowed us to classify conjugate classes of elements in D_5 and D_6.

To do: Read over the slides, formulate any questions you may have. Memorize the definition $aN \cdot bN = abN$, and be able to state and prove what it means for that binary operation on G/N to be *well-defined*. Know that $z \in G$ is central iff its conjugacy class has size 1, and be able to prove this. Be able to partition a group by the conjugacy classes of the elements.

Week 9: 3/7–3/11. Three lectures covering the Chapter 3 slides (pp. 83–90) and the Chpater 4 slides (pp. 1–24). Approximate YouTube content: 4.3 (7:01–13:27). HW 7 due this Monday, HW 8 due next Monday.

Summary and big ideas: Two permutations are conjugate in S_n if and only if they have the same cycle type. The *centralizer* of an element $h \in G$ is the subset $C_G(h)$ that commutes with h. We saw that $|\operatorname{cl}_G(h)| = [G : C_G(h)]$, i.e., the more things that commute with h, the fewer conjuates it has. This is analogous to normalizers and conjugacy classes of subgroups; recall that $|\operatorname{cl}_G(H)| = [G : N_G(H)]$, i.e., the more things that commute with H (set-wise), the fewer conjugates it has.

Moving onto Chapter 4, we defined the notion of a *homomorphism*, which is a structure-preserving map between groups. There are two types of homomorphisms: *embeddings* (occurs when one group is a subgroup of another), and *quotient maps*, when one group is a quotient of another. The *kernel* of a homomorphism is the set of elements that get mapped to the identity, and this is a normal subgroup. We stated and proved the *fundamental homomorphism theorem*: $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$, which says that "*every homomorphism image is a quotient.*

To do: Read over the slides, formulate any questions you may have. Know how to identify the conjugacy classes of permutations in S_n. Be able to find the centralizers of group elements from knowing the conjugacy classes, and vice-versa. Learn the definition of a homomorphism $\phi\colon G \to H$, its kernel, and the preimage of an element $h \in H$. Get used to working with the property $\phi(ab) = \phi(a)\phi(b)$, and the facts that $\phi(1) = 1$ and $\phi(g^k) = \phi(g)^k$, even if k is negative (be able to prove these facts). Be able to prove that the kernel is a subgroup and that it is normal. Be able to formally state what it means for a map $\phi\colon G/N \to H$ to be *well-defined*. Learn the proof of the fundamental homomorphism theorem.

Week 10: 3/14–3/18. Three lectures covering the Chapter 4 slides (pp. 25-70). Approximate YouTube content: Lecture 4.3 (13:28–32:52), 4.5, 4.6, and supplemental material on automorphisms and semidirect products. HW 8 due this Monday, HW 9 due the Monday after spring break.

Summary and big ideas: We saw how to apply the FHT for showing that $G/N \cong H$. Then we saw the last three isomorphism theorems. The FHT theorem says that "every homomorphic image is a quotient." The correspondence theorem characterizes subgroups of quotients of N (they are just quotients of subgroup that contain N), and the freshman theorem characterizes quotients of quotients. Both of these were difficult algebraically, but had very intuitive interpretations in terms of subgroup lattices, and "shoeboxes" (cosets). Finally, the diamond theorem chacterizes quotients of the form AB/B.

Next, we moved onto commutators, which can be thought of as the "nonabelian parts" of a group. These generate the *commutator subgroup* G', and the quotient G/G' is the largest abelian quotient of G. This also has a nice subgroup lattice interpretation.

Finally, we moved onto automorphisms, which are isomorphisms from a group to itself. This allowed us to extend the Chapter 2 concept of "structure-preserving rewiring" from cyclic groups to all groups, and we saw several examples: V_4 and D_3. This allowed us to construct semidirect products like $V_4 \rtimes B$. The set of automorphisms forms a group $\mathrm{Aut}(G)$. The *inner automorphisms* are those that are conjugations, e.g., $g \mapsto x^{-1}gx$, and these form a normal subgroup $\mathrm{Inn}(G) \cong G/Z(G)$. Automorphisms that are not inner are called *outer* and the *outer automorphism group* is the quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

To do: Read over the slides, formulate any questions you may have. Be able to apply the FHT to establish $G/N \cong H$; we've seen a number of examples like this. Learn the proofs all of the isomorphism theorems on your own (one of these will be on the midterm and final exam). Be able to construct the subgroup lattice of a quotient, by "chopping" the lattice at that subgroup. Be able to determine what

G/N is isomorphic to, just by inspection of the subgroup lattice of G. Be able to interpret all of the isomorphism theorems in terms of subgroup lattices. Given a subgroup lattice, be able to find the commutator subgroup by inspection. Given a group G, be able to construct the inner automorphism group, $\mathrm{Inn}(G) \cong G/Z(G)$ and outer automorphism group $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Week 11: 3/28–4/1. Three lectures covering the Chapter 4 slides (pp. 70-81), and the Chapter 5 slides (pp. 1–30). HW 9 due this Monday, HW 10 due next Monday.

Summary and big ideas: We saw how to define a semidirect product $A \rtimes_\theta B$ algebraically, where $\theta\colon B \to \mathrm{Aut}(A)$. We also learned that $G = NK$ is (i) isomorphic to $N \times K$ iff both N and K are normal, and $N \cap K = \langle e \rangle$, and (ii) isomorphic to $N \rtimes K$ iff N is normal and $N \cap K = \langle e \rangle$, and in this case, θ is an inner automorphism. This gave us a way to identify direct and semidirect products from the subgroup lattice by inspection alone: find two subgroups, N and H, that generate G, intersection trivially, and at least one is normal.

We introduced the concept of a group action: a homomorphism $\phi\colon G \to \mathrm{Perm}(S)$. This should be thought of as a "group switchboard": every element $g \in G$ has a "button", and pressing the g-button rearranges the set S. The only rule is that "*pressing the a-button and then the b-button has the same effect as pressing the ab-button.*" We saw several examples of this with D_4, like how it acts on a set of "binary squares", how it acts on itself by multiplication, or by conjugation, and how it acts on its subgroups by conjugation. These all result in *action diagrams*, which can be thought of as generalization of a Cayley diagram.

Every action has five fundamental features. Three are "local": given $s \in S$, its *orbit* $\mathrm{orb}(s)$ is the connected component in the action diagram, and its *stabilizer* $\mathrm{stab}(s)$ are the elements of G that fixes it. We can also take a group element $g \in G$, and define its *fixed point set* $\mathrm{fix}(g)$ to be the set of $s \in S$ that it fixes. The best way to visualize these is to construct a "*fixed point table*", and look at the rows and columns. There are two "global features": the kernel $\mathrm{Ker}(\phi)$ is the set of "broken buttons", also just the intersection of the stablizers. The set of fixed points, $\mathrm{Fix}(\phi)$, are the elements in S that don't get moved by anything; this is also the intersection of all $\mathrm{fix}(g)$.

We stated and proved two fundamental theorems about orbits: (i) the *orbit-stabilizer theorem*: that $|G| = |\mathrm{orb}(s)| \cdot |\mathrm{stab}(s)|$, for any $s \in S$, and (ii) the *orbit counting theorem*: that the number of orbits is the average size of $\mathrm{fix}(g)$, i.e., the "average number of checkmarks per row in the orbit table".

To do: Given a subgroup lattice, be able to identify all pairs N and H for which $G \cong N \times H$, or $G \cong N \rtimes H$, just by inspection. Given a group action, be able to determine the orbits, stabilizers, fixed point sets, as well as the kernel and set of fixed points. Get good at the "group switchboard analogy", and be able to write down formal definitions of the aforementioned terms (from the concept, not from memory). Learn the statements of the orbit-stabilizer and orbit-counting theorem, and be able to apply them to specific actions.

Week 12: 4/4–4/8. Three lectures covering the Chapter 5 slides (pp. 31–44, 53–70). HW 10 due this Monday, HW 11 due next Monday.

Summary and big ideas: We considered the action of a group G acting on its subgroups by conjugation. In this setting, the orbits are conjugacy classes, the stablizers are normalizers, and the kernel and set of fixed points are the normal subgroups. We got an an immediately corollary of the orbit-stabilizer theorem that $\mathrm{cl}_G(H) = [G : N_G(H)]$. We also saw the action of G on the cosets of some $H \leq G$. The action diagram can be constructed from collapasing the Cayley diagram of G by the right (not left!) cosets of H. This was useful for proving a few results about subgroups of small index: (i) if G has no subgroup of index 2, then any subgroup of index 3 is normal, and (ii) if $[G : H] = p$ for the smallest prime dividing $|G|$, then H is normal.

We also observed that the automorphism groups $\mathrm{Aut}(G)$, and its normal subgroup $\mathrm{Inn}(G)$, naturally act on G. We skipped over the section on "action equivalent", though briefly summarized the main ideas. 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.

To do: Given a group G action on itself, its subgroups, or cosets, be able to determine the orbits, stabilizers, fixed point sets, as well as the kernel and set of fixed points. Usually these will be familiar algebraic objects. Be able to interpret these

in a "fixed point table." Learn the definitions of p-subgroup and Sylow p-subgroup. Given a group of order $|G| = p^n m$, know how big its Sylow p-subgroups are. Learn the statements of the first two Sylow theorems and be able to interpret them in a subgroup lattice.

Week 13: 4/14–4/18. Three lectures covering the Chapter 5 slides (pp. 71–80, 87–89), and the Chapter 7 slides (pp. 1–19). HW 11 due this Monday, HW 12 due next Monday.

Summary and big ideas: We stated and proved the 3rd Sylow theorem, that the number n_p of Sylow p-subgroups divides m (where $|G| = p^n \cdot m$) and is equivalent to 1 modulo p. Then, we saw how to use this to establish that groups of particular orders are not simple – all that is needed is to show that $n_p = 1$ for some prime p. We finished Chapter 5 with the classification of finite simple groups, which was finally completed in 2004 after 50 years and over 10000 pages.

We then moved onto ring theory. A *ring* is an additive abelian group R with an additional binary operation that satisfies the distributive law. Basically, a set in which we *can add, subtract, multiply, but not necessarily divide*. Rings can be commutative ($rs = sr$ for all $r, s \in R$) or noncommutaitve, and they may or may not have a multiplicative identity element 1. Most finite rings are not all that interesting, and very few are noncommutative with 1. Thus, most of our examples from from familiar algebraic objects like sets of numbers ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), polynomials $R[x]$, functions, and $n \times n$ matrices. We also saw how to define a *group ring* for any group G. The Hamiltonians are defined as "quaternions but with real coefficients." Elements in a ring that have multiplicative inverses are called *units*. If the product of two nonzero elements is zero, then those are called *zero divisors*.

We saw example of various kinds of rings: fields, division rings, and integral domains. We showed that finite integral domains are fields, and that in integral domains enjoy the *cancelation* property: if $ax = ay$, then $x = y$. A subgroup $I \subseteq R$ is an *ideal* if it is invariant under multiplication. There are left, right, and two-sided ideals. These are to rings what normal subgroups are to groups. We saw several examples of ideals in polynomial rings, such as (x), (2), and $(x, 2)$ in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

To do: There were a lot of new definitions and examples introduced, and these need to be learned. Make sure you know the definition of ring, unit, zero divisor, subring, ideal, integral domain, division ring, and field. Familiarize yourself with the examples that we saw in class.

Week 14: 4/18–4/22. Two lectures covering Chapter 7 slides (pp. 19–39). Midterm 2 Wednesday. HW 12 due this Monday, HW 13 due next Monday.

Summary and big ideas: Two-sided ideals are to rings what normal subgroups are to groups. We define the quotient ring R/I as the set of cosets, and defined how to multiply cosets: $(x+I)(y+I) := xy+I$. We define ring homomorphisms, and showed that the kernel is a two-sided ideal. This lead to the ring isomorphism theorems, which were analogous to the ones for groups.

A *maximal ideal* M of R is a proper ideal that is contained in no strictly larger proper ideals. If R is commutative, then by the correspondence theorem, R/M is simple iff M is maximal, and this is also equivalent to R/M being a field (because fields have no non-trivial proper ideals). We saw examples of maximal ideals in common rings like $\mathbb{Z}$, $R[x]$, and $F[x,y]$, and then saw how to construct finite fields. The quotient $\mathbb{Z}_p[x]/(f)$, for a degree-n polynomial is a finite field of order p^n. It is unique up to isomorphism, and all finite fields of order p^n for some $n \geq 0$.

An ideal P of R is *prime* if $ab \in P$ implies either $a \in P$ or $b \in P$. Prime ideals in $\mathbb{Z}$ are just (p) for some prime p. A fundamental result (HW) is that P is prime iff R/P is an integral domain, and it follows that every maximal ideal is prime.

To do: Be able to prove the basic results on ring theory that we learned: kernels are ideals, the FHT for rings, that M is maximal iff R/M is a field, that P is prime iff R/P is an integral domain.

Week 15: 4/25–4/29. Two lectures covering Chapter 7 slides (pp. 40–61). HW 13 (originally due Monday) merged with a shorted version of HW 14, due this Friday.

Summary and big ideas: The (nonzero) integers have some basic properties that we usually take for granted: numbers can be factored uniquely into primes, every pair has a unique GCD and LCM, and there is a Euclidean algorithm that can find the GCD. Perhaps surprisingly, these need not always hold in integral domains. This motivates us to formalize "irreducible" and "prime". Though prime $\Rightarrow$ irreducible, the converse fails. For example, in $\mathbb{Z}[\sqrt{-5})$ the number 3 is irreduible but not prime because $3 \mid (2+\sqrt{-5})(2-\sqrt{-5}) = 9$, but $3 \nmid (2 \pm \sqrt{-5})$.

Fortunately, there is a type of ring where such "bad things" don't happen: a *principle ideal domain* (PID), which means that every ideal I is generated by a single element, $I = (a)$. Examples include $\mathbb{Z}$, $\mathbb{Z}[i]$, any field F, and $F[x]$. We formalized the defnition of a GCD and LCM, and showed that they exist and are unique in an aribitrary PID. We also showed that in a PID, every irreducible is

prime. Alternatively, we can define a *unique factorization domain* (UFD) to be any ring where every irredicble is prime , and every nonzero number is a product of irreducibles. We showed that every PID is a UFD.

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 learned about the ring *algebraic integers*, which are roots of monic polynomials in $\mathbb{Z}[x]$. For each square-free m, the ring R_m is the intersection of algebraic integers that lie in $\mathbb{Q}(\sqrt{m})$. We saw that some of these are Euclidean domains, some are "norm-Euclidean", and others are just PIDs. It is still an open problem to determine this for all m. Curiously, there are exactly four rings R_m, for $m < 0$, that are PIDs but not Euclidean: $m = -19, -43, -67, -163$. We finished the class with some pretty pictures of the algebraic integers in the complex plane.

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.

Finals week: 5/2–5/6. Final exam Friday 8–10:30am.

To do: Study! The exam will be cumulative. You will have to do the following: prove an isomorphism theorem, classify all abelian groups of a certain order, use the Sylow theorems to show that there are no simple groups of a certain order, prove a few basic results about groups and rings (e.g., prove something is a subgroup, normal, or an ideal), apply the isomorphism theorems, analyze a group action, and answer questions about a group from its subgroup lattice. This is not a comprehensive list – there will be other things not explicitly mentioned here, but everything listed above *will* be on the final.