Weekly schedule: Math 4120, Fall 2022

Note: the pages correspond to an older version of the slides; not the ones posted here. Several chapters have since been split into two.

- **WEEK 1: 8/24–8/26**. Course overview Wednesday. One lecture Friday covering the Chapter 1 slides (pp. 1–18). HW 1 due next Friday.

  Summary & key ideas. We introduced *Cayley graphs*, and saw several examples of groups: the symmetries of a rectangle, and of a triangle. These define algebraic *relations*. The same group can have very different looking Cayley graphs depending on generating sets. We discussed the Rubik's cube group, mostly just for fun, but there is some deep group theory involved in that.

  To do:
  - Read over the slides we covered, formulate any questions you may have.
  - Look at the HW 1 problems, and attempt #1(abcf), #2(abcef), #3(ac).
  - Look ahead at slides for next week: Chapter 1 (pp. 19–40).

  Learn / memorize:
  - The three basic properties of a group (closure, identity, inverses)
  - Cayley graphs for $V_4 = \langle r, h \rangle$ and the "triangle symmetry graph" $D_3 = \langle r, s \rangle$ and $\langle s, t \rangle$.
  - Be able to use Cayley graphs to multiply elements, compute inverses, and find relations (two paths that correspond to the same element).

- **WEEK 2: 8/29–9/2**. Three lectures covering the Chapter 1 slides (pp. 19–49), and the Chapter 2 slides (pp. 1–10). HW 1 due Friday.

  Summary & key ideas. We learned how to label Cayley graphs with actions. This motivated the idea of a *group presentation.* Finally, we learned about infinite summetry group. One-dimensional symmetry groups are called *frieze group*, and we classifed all 7 of them.

  The 2D analogue of these are were "17 different types of wallpaper", and the 3D analogue are the 230 "crystal groups." 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.

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.

Learn / memorize:

– Be able to label nodes of a Cayley graph with group elements.
– How to multiply elements in Q_8.
– Presentations for groups we've seen (V_4, D_3, Q_8).
– Be able to differentiate various groups we've seen from their Cayley tables. One good way is to count the number of times the identity appears on the main diagonal (the # of $g \in G$ for which $g^2 = 1$).
– The formal definition of a group.
– The formal definition of a the order of a group, and the order of an element.
– The definition of the n^{th} roots of unity, and which ones are primitive.

- **WEEK 3: 9/5–9/9**. Three lectures covering the Chapter Chapter 2 slides (pp. 11–53). HW 2 due Friday.

  Summary & key ideas. We defined cyclic groups, both additively as $\mathbb{Z}_n = \langle 1 \rangle$ and multipliatively as $C_n = \langle r \rangle$. Finite cyclic groups describe rotations of an n-gon. The fully symmetry groups of n-gons are the *dihedral groups* D_n. We saw how to represent the group C_n and D_n with 2×2 matrices using roots of unity. There are infinite version of both of these: $C_\infty \cong \mathbb{Z}$ and D_∞ both occured as frieze groups.

  We introduced the notion of a *cycle graph*, which contains all of the *maximal* cyclic subgroups in G. This gives a very different picture of the group vs. a Cayley graph, but both are useful. 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 graphs 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 graph, and another from a Cayley table.

  Finally, We learned about permutation matrices, and how our previous observation of how there were two canonical ways to label a permutahedron (Cayley graph for S_n) with permutations (swap coordinates, vs. swap numbers) can be realized by right-multiplying row vectors vs. left-multiplying column vectors.

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 2.

Learn / memorize:

– When does $\langle k \rangle$ generate $\mathbb{Z}_k$ (or equivalently, $\langle r^k \rangle$ generate C_n).
– The cycle graphs for D_n and Q_8.
– How to construct a cycle graph given a group.
– How to construct Cayley graphs and presentations for D_n.
– How to represent C_n and D_n with 2×2 matrices over $\mathbb{C}$.
– That $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ iff $\gcd(n, m) = 1$.
– *How to write a complete list of all abelian groups of some fixed order.* (I recommend the "prime power" classification.)
– 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: $S_n = \langle (12), \dots, (n\, n{-}1) \rangle$ and $S_n = \langle (12), (12 \cdots n) \rangle$.
– How to determine the parity of a permutation (even vs. odd).

- **WEEK 4: 9/12–9/16**. Three lectures covering the Chapter 2 slides (pp. 54–108). HW 3 due Friday.

Summary & key ideas. We generalized the quaternion group $Q_8\{\pm 1, \pm i, \pm j, \pm k\}$ 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* $\mathrm{Dic}_n = \langle \zeta_n, j \rangle = \langle r, s \rangle$. In these groups, all non-powers of $r = \zeta_n$ (i.e., elements of the form $r^k s$) have order 4. Then, we saw another to extend the quaternion group: starting with the canonical matrix representations $Q_8 = \langle R_4, S \rangle$ and $D_n = \langle R_n, F \rangle$ add in the reflection matrix F to get the *diquaternion group*, $\mathrm{DQ}_8 = \langle i, j, f \rangle = \langle R_4, S, F \rangle$. If $n = 2^m$, then we can do both of these to get the *generalized diquaternion group* $\mathrm{DQ}_n = \langle \zeta_n, j, f \rangle = \langle R_n, S, F \rangle$.

Next, we explored how to "rewire" the inner cycle of the Cayley graph 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. They are all generated by the "reflection matrix" F, and a 2×2 diagonal matrix with ζ_n in the $(1, 1)$-entry. The difference is in the $(2, 2)$-entry, which could be $\pm\zeta_n$ or $\pm\bar{\zeta}_n$.

Moving on, we reviewed direct products, and explored a visual "inflation method" to construct a Cayley graph of $A \times B$ from graphs of A and B, respectively: inflate B-nodes like "balloons" and stick in A-Cayley graphs, and re-connect nodes across balloons. A *semidirect product* results if we "rewire" A-graphs (an *automorphism*) before inserting them. We explored this for cyclic groups. We saw that 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. We finished with a fun contest: how many groups are there of order 2048.

To do: Read over the slides, formulate any questions you may have. Familiarize yourself with the Cayley graphs 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 graph 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).

Learn / memorize:

- Be able to construct the Cayley graph of $\mathrm{Dic}_n = \langle r, s \rangle$. Know that $|r| = n$ and $|r^i s| = 4$ for all $i = 0, \dots, n$.
- Given a Cayley graph of D_n, SD_8, SA_8, or $C_n \times C_2$, be able to write down a group presentation.
- Know how to construct the groups Dic_n, DQ_n, SD_n, and SA_n with 2×2 matrices.
- Know that $D_n \cong C_n \rtimes C_2$, and if n is even, then $D_n \cong D_{n/2} \times C_2$.
- Be able to recognize Cayley graphs of groups that are semidirect products (when it is obvious from inspection; it may not alway be).

- **WEEK 5: 9/19–9/23**. Three lectures covering the Chapter 3 slides (pp. 1–36). HW 4 due Friday.

  Summary & key ideas. We started by looking at the subgroup lattices of some of our familiar small groups. We prove a few basic properties, like how the intersection of subgroups is a subgroup, and how all subgroups of a cyclic group are cyclic.

  Next, we learned about cosets – every subgroup $H \leq G$ partitions G into left cosets, and right cosets, though these may be different. The *normalizer* of H is the union of left cosets that are right cosets – in class, these were the "blue cosets." Moreover, H is a *normal subgroup* if every left coset is a right coset. Note that we always have $H \trianglelefteq N_G(H) \trianglelefteq G$. The *index* of H is $[G : H] := |G|/|H|$, the number of left (or right) cosets of H. Another caveat: $xH = Hx$ does *not* necessarily imply $xh = hx$ for all $h \in H$. However, every group G has a *center*, which is the subgroup $Z(G)$ of elements that commute with everything. We often like to label the edges in a subgroup lattice with the index, and this is multiplictive, in that $[G : K] = [G : H][H : K]$.

  To do: Read over the slides, formulate any questions you may have. Practice writing down the algebraic definitions that we learned in class (the left coset xH, the right coset Hx, the index $[G : H]$, and the normalizer $N_G(H)$, the center $Z(G)$). Be able to prove some of the basic statements that we did in class. For example, that sets like $\cap H_\alpha$, $Z(G)$, or $N_G(H)$, are subgroups, that index-2 subgroups are normal, that all cosets have the same size, that $xH = H \Leftrightarrow x \in H$, or that $[G : K] = [G : H][H : K]$. Understand visually, *why* if a and b are in the same coset of H, then $aH = bH$.

  Learn / memorize:

  - Our "boring but useful coset lemma": $xH = H$ iff $x \in H$.
  - Be able to construct the subgroup lattices of C_4, V_4, C_6, D_3, C_8, D_4, Q_8).
  - Be able to construct the subgroup lattice of a cyclic group $\mathbb{Z}_n$.
  - Given a subgroup lattice and subgroups H and K, be able to identify their intersection $H \cap K$ and what the generate, $\langle H, K \rangle$.
  - Given a subgroup $H \leq G$, be able to partition G by the left cosets of H, and by the right cosets, and to find the normalizer – all by just using the Cayley graph.
  - Given a subgroup lattice of G, be able to label each edge with the corresponding index, $[H : K]$.
  - Know which particular subgroup is the center $Z(G)$ for all of our familiar examples of groups.

- **WEEK 6: 9/26–9/30**. Three lectures covering the Chapter 3 slides (pp. 37–75). HW 5 due Friday.

  Summary & key ideas. Given $H \leq G$, the proportion of left cosets of H that are right cosets meausures 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 graph.

  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 $AB \leq G$.*

  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*. 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 $g \in G$.

  To do:

  – *Keep learning your subgroup lattices!!!*
  – Practice determining the conjugacy classes of subgroups using the lattices, by inspection. In particular, be able to identify normal subgroups – G, $\langle e \rangle$, those of index 2, "unicorns," an the "bases of a conjugate fan".
  – Practice finding the normalizer of a subgroup using the lattice, purely by inspection.
  – Practice finding conjugate subgroups using a Cayley graph.
  – Practice identifying the subgroup NH in a lattice, given subgroups $N, H \leq G$ (say $N \trianglelefteq G$).
  – Practice taking the quotient of G by a normal subgroup, using a Cayley graph (collapse the left cosets).
  – Learn how to prove that multiplication of cosets is well-defined.

Learn / memorize:

- Three ways to check if a subgroup H is normal: showing $ghg^{-1} \in H$ for all $g \in G$ is often the easiest.
- Be able to prove that if $[G : H] = 2$, then $H \trianglelefteq G$.
- How to read the "reduced" subgroup lattices that I call "*conjugacy posets*," which are used by GroupNames and LMFDB.
- Be able to recognize the subgroup lattices of some of our larger familiar groups: $C_4 \times C_2$, C_2^3, A_4, Dic_6, DQ_8, SA_8).
- *The size of a conjugacy class of H is the index of its normalizer:* $\mathrm{cl}_G(H) = [G : N_G(H)]$.
- How to multiply cosets in a quotient group: $aN \cdot bN = abN$. Also, meorize the definition (concept) of what it means for the binary operation $aN \cdot bH := abN$ to be well-defined.
- G/N is a group iff $N \trianglelefteq G$.
- $|\,\mathrm{cl}_G(h)| = 1$ iff $h \in Z(G)$. (Be able to prove this.)

- **WEEK 7: 10/3–10/7**. Three lectures covering the Chapter 3 slides (pp. 76–90) and Chapter 4 slides (pp. 1–21). HW 6 due Friday.

  Summary and big ideas: We began with 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. We also saw the following relationship: *the size of the conjugacy class* $\mathrm{cl}_G(x)$ *is equal to the index of its centralizer,* $C_G(x)$, which is analogous to a result for subgruops: *the size of the conjugacy class* $\mathrm{cl}_G(H)$ *is equal to the index of its normalizer,* $N_G(H)$. Soon, we will see why these are actually special cases of a broader theorem.

  To do:
  - Practice finding the conjugacy classes of an element, when you *a priori* know its centralizers, and vice-versa.
  - Be able to partition a group by the conjugacy classes of the elements.
  - Practice writing down definitions of the new concepts without looking at your notes.

  Learn / memorize:
  - Learn the proof that $z \in G$ is central iff its conjugacy class has size 1.
  - Memorize how the elements of D_n are partitioned into conjugacy classes – the cases of n being even and odd are different.
  - Know that two permutations in S_n are conjugate iff they have the same *cycle type.*
  - Memorize the definition of a homomorphism, and its key property, $\phi(ab) = \phi(a)\phi(b)$.

- **WEEK 8: 10/10–10/14**. Two lectures covering the Chapter 4 slides (pp. 22–38). Midterm 1 Wednesday. HW 7 due Friday.

  Summary and big ideas: 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*: $G/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. We saw how to apply the FHT for showing that $G/N \cong H$.

  The FHT is the first of four "isomorphism theorems," and on Friday, we saw the second one, the *correspondence theorem*. Loosely speaking, the FHT says that "*every homomorphism image is a quotient*," and the correspondence theorem characterizes the subgroups of a quotient. Specifically, the subgroups of G/N are of the form H/N, where $N \leq H \leq G$. There are several nice visualization of this: the subgroup lattice of G/N can be formed by "chopping everything off below N", and then all of its properties (normal subgroups, conjugacy classes, intersections, subgroup index, etc.) are inherited from the lattice of G. Another way to visualized this, which will be explored in HW 8, is with our "shoebox diagrams" where shoeboxes represent cosets.

  To do:
  - Be able to explain in simple terms what the FHT and correspondence theorem tell us about the structure of a quotient group.
  - Practice deducing properties about a subgroup lattice from what we know about smaller groups that arise as quotient.

  Learn / memorize:
  - Learn the statement of the FHT theorem.
  - Learn the proofs of the FHT and the correspondence theorem, since you will have to prove one of the isomorphism theorems on Midterm 2 and the final exam.
  - Be able to prove that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ using the FHT.
  - Memorize what it means for a binary operation and/or homomorphism to be *well-defined*, and under what conditions you need to verify this in a proof.
  - Make sure you have memorized the subgrop lattices of our smallish groups.

- **WEEK 9: 10/17–10/21**. Three lectures covering the Chapter 4 slides (pp. 39–72). HW 8 due Friday.

  Summary and big ideas: We started with the last two isomorphism theorems: the fraction theorem characterizes quotients of quotients ("chop off the lattice twice"), and the diamond theorem characterizes quotients of AB/B, and highlights a structural duality inherent in subgroup lattices. Next, we looked at several consequences of the isomorphism theorems: if $H \leq S_n$ has an odd permutation, then exactly half of its permutations are odd. Every homomorphism can be factored as a quotient followed by an embedding. The subgroup of a quotient is the quotient of a subgroup.

  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 $\mathrm{Inn}(G) \cong G/Z(G)$. In other words: "*two elements, x and y determine the same inner automorphism iff they differ by a central element: $x = yz$ for some $z \in Z(G)$.*" Automorphisms that are not inner are called *outer* and the *outer automorphism group* is the quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Examples of outer automorphisms include any automorphism of an abelian group, the map $f \mapsto rf$ that "rotates" the axes in D_n (even n), and any nontrivial permutation of $\{i, j, k\}$ in Q_8.

  To do:
  - Be able to identify the commutator subgroup G' and abelianization G/G' simply by inspecting the subgroup lattice.
  - Finish the details of the proof that $G/Z(G) \cong \mathrm{Inn}(G)$; it's just a straightforward application of the FHT.

  Learn / memorize:
  - Learn the statement of the fraction and diamond isomorphism theorems.
  - Learn the proofs of the fraction and diamond isomorphism theorems – both amount to defining a map and then applying the FHT.

- **WEEK 10: 10/24–10/28**. Three lectures covering the Chapter 4 slides (pp. 73–86) and Chapter 5 slides (1–24, 26). HW 9 due Friday.

  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 graphs*, which can be thought of as generalization of a Cayley graphs.

  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 graph, 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 *fixator* $\mathrm{fix}(g)$ 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 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 fixed point table".

  To do:
  - Get good at determining whether G is a semidirect or direct product of two of its subgroups simply by inspecting the subgroup lattice.
  - Given a group action, be able to determine the orbits, stabilizers, fixators, as well as the kernel and set of fixed points.
  - Get good at the "group switchboard analogy", and how to interpret our "five fundamental features" in that setting.

Learn / memorize:

- The formal mathematical definitions of our five fundamental features: orb(s), stab(s), fix(g), Ker(ϕ), and Fix(ϕ) – from the concept, not from memory. Know which is a subset of S and which is a subgroup of G.
- The formal statements of the orbit-stabilizer and orbit-counting theorem.
- How to quickly recognize our "five fundamental features" by inspection, in terms of the action graph, and fixed point tables.

- **WEEK 11: 10/31–11/4**. Three lectures covering the Chapter 5 slides (26–71). HW 10 due Friday.

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

  We then considered 4 standard ways that a group can act on its features: G acts on (i) its elements by multipliction, (ii) its elements by conjugation, (iii) its subgroups by conjugation, and (iv) cosets of a fixed $H \leq G$ by multipliction. In each case, we interpreted our "five fundamental features" in this setting, as well as the orbit-stabilizer and orbit counting theorems. In many cases, we got new theorems with very little work. For example, as special cases of the orbit-stabilizer theorem, we got $|\operatorname{cl}_G(g)| = [G : C_G(g)]$ and $|\operatorname{cl}_G(H)| = [G : N_G(H)]$.

  For the last of these four actions – G acting on the cosets of some $H \leq G$, the action graph can be constructed from collapasing the Cayley graph 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 $\operatorname{Aut}(G)$, and its normal subgroup $\operatorname{Inn}(G)$, naturally act on G.

  We finished by covering several topics briefly, to summarize the main ideas. First, we defined what it meant for two actions to be *equivalent*. Earlier in the class, we saw how S_n acts on permutations of $\boldsymbol{123\cdots n}$ two ways: where (ij) swaps the i and j coordinates, or the digits i and j. One of these is the result of a right action of S_n, and the other, (an equivalent) left action.

  To do:
  - Review our four common actions: G acting on itself by multiplication, or conjugation, on its subgroup by conjugation, or cosets of a fixed $H \leq G$ by multipliction. For each one, learn what our "five features" are, and if they are known by more familiar algebraic terms.
  - Be able to collapse a Cayley graph by the right cosets of a subgroup, and understand what group action this is an action graph of.
  - Go back and look at all of the pretty picture on action equivalence, simply transitive actions, and tilings.

  Learn / memorize:
  - Learn the proof of the orbit-stabilizer theorem.
  - Be able to construct a fixed point table, and learn how to read off the stabilizers, fixators, kernel, and fixed points from it.

- Use the orbit-counting theorem to determine the number of orbits of an action by the average size of a fixator.
- Inner vs. outer automorphisms, examples of each (e.g., Q_8, D_3, D_4), and be able to prove that $G/Z(G) \cong \mathrm{Inn}(G)$.
- Learn the results of the statements of several theorems we proved about normal subgroups: (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.

- **WEEK 12: 11/7–11/11**. Fall Break Monday. Two lectures covering the Chapter 5 slides (72–92). HW 11 due next Monday.

  Summary and big ideas: The *Sylow theorems* 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 (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:
  - Be able to interpret the statements of the first Sylow theorems in a subgroup lattice, and describe them in simple terms (e.g., "tower of p-subgroups").

  Learn / memorize:
  - The definitions of p-subgroup and Sylow p-subgroup.
  - Learn the statements of the first two Sylow theorems.

- **Week 13: 11/14–11/18**. Two lectures covering the Chapter 5 slides (pp. 93–101, 115–117). Midterm 2 Wednesday. HW 11 due this Monday, HW 12 due next Monday.

  Summary and big ideas: We stated and proved the 3rd and final 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.

  To do:
  - Practice using the 3rd Sylow theorem to show that there are no simple groups of order n, for certain fixed n.
  - Watch the 3blue1brown video on actions and the monster group.

  Learn / memorize:
  - The statement of the 3rd Sylow theorem, and how to use it.

Week 14: 11/21–11/25. One lecture covering Chapter 7 slides (pp. 1–14). HW 12 due this Monday.

Summary and big ideas: 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. 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. 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.

Learn / memorize:

- 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, $I = (X)$.

To do:

- Be able to read and construct subring lattices, and the difference between ideals, subrings, and subgroups.

Week 15: 11/28–12/2. Three lectures covering Chapter 7 slides (pp. 15–49). HW 13 due Friday.

Summary and big ideas: We started with a number of examples of rings. For any group G and ring R, we can define a *group ring*, RG. 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 (fields and skew fields), 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 $\mathbb{Q}[x]$. A *ring homomorphism* is a group homomorphism $\phi\colon R \to S$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in R$. The kernel $I = \mathrm{Ker}(\phi)$ is always normal, and the quotient R/I is a ring. We already know it is an additive group – the sum of cosets is $(r + I) + (s + I) = r + s + I$. We also showed that multiplication is well-defined: $(r + I)(s + I) = rs + I$. There are four isomorphism theorems, which are analogous to the isomorphism theorems for groups. The proofs basically involve showing that a group homomorphism is also a ring homomorphism.

A (proper) ideal I is *maximal* if there are no other ideals J satisfying $I \subsetneq J \subsetneq R$. By the correspondence theorem, I is maximal iff R/I is simple (no nonzero proper ideals), and we showed that a commutative ring is simple iff it is a field. We saw a number of example of maximal ideals, and determine their quotient fields: $\mathbb{Z}/(p) \cong \mathbb{Z}_p$, $\mathbb{Z}[x]/(x, p) \cong \mathbb{Z}_p$, $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$, and $\mathbb{F}[x, y]/(x, y) \cong \mathbb{F}$.

Learn / memorize:

- Units and zero divisors in a ring. Know examples of both.
- Types of rings: integral domains, division ring (fields and skew fields).
- Make sure you can prove the isomorphism theorems for rings, assuming the isomorphism theorems for groups.

To do:

- There were a lot of new definitions introduced – make sure you can write them down formally.
- Practice writing quotient rings and using both binary operations.
- Know examples of maximal ideals in various fields, and what their quotient fields are.
- There were a number of very short proofs of basic results. Make sure you can do these on your own, as they've come up on exams.

Week 16: 12/5–12/9. Three lectures covering Chapter 7 slides (pp. 50–69). HW 14 due Friday.

Summary and big ideas: 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 $f(x)$.

Henceforth, assume R to be commutative. 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 $f(x) = x^q - 1$).

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 related concept is the *radical* of an ideal I, denoted $\sqrt{I}$, which is the set of element $r \in R$ for which $r^n \in I$ for some n. The *nilradical* of R is the radical of the zero ideal $\mathfrak{N}_R := \sqrt{0}$, or equivalently, the set of nilpotent elements ($a \in R$ for which $a^n = 0$). We showed that it is also the intersection of all nonzero prime ideals, which by the correspondence theorem, means that $\sqrt{I}$ is the intersection of nonzero prime ideals contaning I. The *Jacobson radical* $\text{jac}(I)$ of an ideal is the intersection of all maximal ideals containing I, and the Jacobson radical of R is the intersection of all maximal ideals. Though it's beyond the scope of the class, the Jacobson radical can also be defined elementwise, as those $r \in R$ that annihilate all simple R-modules.

Learn / memorize:

- Know how to construct the finite field $\mathbb{F}^{p^n}$.
- Learn the definition of prime and primary ideals.
- Be able to prove that P is prime iff R/P is an integral domain.

- Know the definition of the radical $\sqrt{I}$ and Jacobson radical $\mathrm{jac}(I)$ of an ideal, and also of the nilradical $\mathfrak{N}_R = \sqrt{0}$ and Jacobson radical $\mathrm{Jac}(R) = \mathrm{jac}(0)$ of a commutative ring.

To do:

- Practice adding and multiplying elements in finite fields: $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$, where f is a degree-n irreducible polynomial. Familiarize yourself with the abelian groups $\mathbb{F}_q$ and $\mathbb{F}_q^\times$.
- Study for the final exam and ask any questions that you have.