Retrospective Course Overview

Math 145, Abstract Algebra, Duchin

What are the big themes from the first semester of Abstract Algebra?

We spent most of the semester on material from Chapters 3, 4, and 5 of the book, supplemented by outside material.

Chapter 3: Groups

What is a group? Group axioms. Why can only one thing act like the identity?

Group examples. You should know these intimately: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(F_n, \cdot)$, $(S_n, \circ)$, $(\mathbb{Z}_n^*, \cdot)$, $(\mathbb{Z}^n, +)$, rigid motions of a shape (under composition)

You have many different ways of denoting permutations $\sigma \in S_n$ and should be able to work with each of them. Every permutation can be written as a product of disjoint cycles (in more than one way) or as a product of not-necessarily-disjoint transpositions. $A_n \leq S_n$ is the subgroup of even permutations.

Groups you should be able to work with from presentations: dihedral groups D_n, Heisenberg group $H(\mathbb{Z})$

Major concepts: generators, cyclic groups, product $G \times H$ of groups, order of an element, order of the group and Lagrange's theorem (order of subgroup divides order of group, order of element divides order of group) plus why it works, commuting, abelian groups, the center of a group (stuff that commutes with everything), conjugation, subgroups, homomorphism, isomorphism (injective and surjective), and kernel

Cosets and quotients. G/H is always a set of cosets, and it has a group structure via $(aH)(bH) = (ab)H$ if and only if H is normal. Normal subgroups are exactly those groups that are kernels of group homomorphisms.

Cosets of H define an equivalence relation (two things are equivalent if they are in the same coset). The quotient is the set of cosets $\{aH\}$—or to put it another way, it is the set of equivalence classes $[a]$.

Example: $n\mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$ and it is the kernel of the natural map $\mathbb{Z} \to \mathbb{Z}_n$.

Ring, field examples. The following are rings, so they are groups under addition and their units form a group under multiplication: $\mathbb{Z}$ (but it hardly has any units), $\mathbb{Z}_n$, $n \times n$ matrices.

The following are fields, so they are groups under addition and their nonzero elements form a group under multiplication: $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Working with groups. Tables for group operations, Cayley graphs, generators and relations, normal forms

Chapter 4: Polynomials

Axioms for rings and fields, the polynomial ring $F[x]$ (defined formally, not functionally), ring and field constructions like $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[\sqrt[3]{2}]$, and multivariable variants like $F[x, y]$. You can certainly also form $R[x]$ over a ring rather than a field but it won't have all the same properties.

Basic terminology includes: factor, reducible/irreducible, monic, degree, coefficient, root

Division-related algorithms. $F[x]$ supports division with remainder, so we have a remainder theorem, a division algorithm, and a Euclidean algorithm. To have these results it is important that F is a field, so that we can get the *matching coefficients* step in long division.

From Euclidean algorithm we get a *gcd* and the fact that it can be written as a linear combination of the parts. Degrees are additive (when you multiply polynomials) because F has no zero divisors.

Roots: c is a root of $f(x)$ iff $f(c) = 0$ iff $x - c \mid f(x)$ iff $f \in \langle x - c \rangle$.

A polynomial is irreducible iff it generates a prime ideal—otherwise its factors multiply into the ideal without being in it themselves. We have unique factorization for polynomials in $F[x]$ by the same proof as unique factorization of integers into primes: any irreducible that divides f divides at least one of its factors $f = gh$, so it can't appear in one factorization but not another.

Quotients and equivalence. We can write $f \equiv g \pmod{p}$ to mean that $p|(f - g)$ or in other words that f and g are equivalent in $F[x]/\langle p(x) \rangle$. This is done in analogy with $a \equiv b \pmod{n}$ which means that a and b differ by a multiple of n, so they are equivalent in $\mathbb{Z}_n$

This fits into division with remainder: if f has remainder r on division by g, then $f \equiv r \pmod{g}$.

The quotient ring $F[x]/\langle f \rangle$ has all the polynomials of degree less than $\deg f$ as representatives, because $a_n x^n \equiv -a_{n-1}x^{n-1} - \cdots - a_0$ lets you reduce arbitrary polynomials to that form.

Kronecker extensions. If p is irreducible, then $F[x]/\langle p(x)\rangle$ is a field called a Kronecker extension of F, and in it, $[x]$ is a root of p.

Whether or not it's a field, $F[x]/\langle f\rangle$ is always a ring, with addition and multiplication defined for cosets.

Fundamental example: $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$.

Chapter 5: Commutative Rings

This chapter essentially reviews all the major properties of the polynomial ring $F[x]$ and gives them names, in order to see what facts about rings can be generalized from $F[x]$.

Integral domains. These are rings with cancellation—i.e., no zero divisors.

Homomorphisms of rings and fields. Remember that $\phi(1) = 1$ is part of the definition of a ring homomorphism—you don't need to specify that in groups or fields because it follows from the existence of inverses. The kernel of a ring homomorphism is defined as $\phi^{-1}(0)$ (the source elements that are "killed" by the map). Some examples: inclusion, projection, and evaluation homomorphisms.

Ideals. Ideals: subsets of rings closed under "addition from within and multiplication from without."

Prime, principal, and maximal ideals, quotient rings. The quotient ring R/I is an integral domain iff I is prime, and what's more it's a field iff I is maximal. (Maximal implies prime but not vice versa.)

Examples: $\langle x\rangle$ in $\mathbb{Z}[x]$ is prime but not maximal (because $\langle 2, x\rangle$ is bigger). $\langle 2, x\rangle$ in $\mathbb{Z}[x]$ is not principal.

A *principal ideal domain* (or PID) is a ring in which every ideal is principal. If there's a gcd algorithm, then you can prove that $\langle f, g\rangle = \langle d\rangle$, which lets you reduce an ideal generated by any finite number of elements to an ideal with just one generator. Thus $\mathbb{Z}$ and $F[x]$ are PIDs.

Other important concepts. Direct sum: $R_1 \oplus \cdots \oplus R_n$ is a ring (with componentwise $+, \cdot$).

Field of fractions: if D is an integral domain, then $Q(D)$ can be defined as "formal fractions" $\frac{a}{b}$ (with $b \neq 0$) under the equivalence relation $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$. Then addition and multiplication are defined as usual for fractions. This construction allows us to define $F(x)$, the smallest field containing F and x, as the fraction field $Q(F[x])$.

Free groups revisited

First, we can write $\langle\langle R\rangle\rangle$ for the normal closure (the smallest normal subgroup containing R). If we do, then we can see that every group is a quotient of a free group: if $G = \langle S|R\rangle$ and $|S| = n$, then $G \cong F_n/\langle\langle R\rangle\rangle$. This just works because F_n supplies the n generators and $r \equiv e$ "kills" the relators and identify the group elements that differ by a relator.

Word length in any group G with generators S is the shortest spelling of a group element using letters from S, and it defines a distance between group elements. Left-multiplication is a rigid motion, and this can be used to make the free group F_2 equidecomposable with *two* copies of F_2. (This is the heart of the Banach-Tarski paradox that allows you to "double the ball" in space with rotations.)

Stuff I skipped

Things that are important and/or interesting but were not emphasized in my treatment of the material.

Theorem 1 ("First isomorphism theorem" or "Fundamental homomorphism theorem")**.** *For any group homomorphism $\phi : G \to H$, there is an isomorphism from the quotient $G/\ker(\phi)$ to the image $\phi(G)$. The same is true for rings: $R/\ker(\phi) \cong \phi(R)$ is a ring isomorphism.*

To prove this, you use the very natural construction $g + \ker(\phi) \mapsto \phi(g)$ and you just check that the homomorphism and bijection properties!

Theorem 2 (Cayley's theorem)**.** *Every finite group G is isomorphic to a subgroup of some S_n.*

How do you prove this? Well, let $n = |G|$ and just label the elements of G with the labels $\{1, 2, \ldots, n\}$ (it doesn't matter how). Then a map from $G \hookrightarrow S_n$ is just given by mapping each g to the permutation of the labels that you get by left-multiplication by g.

A group G is called *simple* if it has no normal subgroups except for $\{e\}$ and G itself. It turns out that the alternating groups A_n are simple for $n \geq 5$, but that's not obvious.