Weekly schedule: Math 4130, Spring 2023

- **WEEK 1: 1/11–1/13**. Course overview Wednesday. One lecture Friday on reviewing ring theory, covering the Chapter 7 slides (pp. 1–15). HW 1 due next Friday.

  Summary & key ideas. A ring R is first and foremost an additive abelian group. We review the three different types of substructures of a ring, which are all "subgroups with extra structure". A subgroup $H \leq R$ can be either
  - an *ideals* (closed under multiplication by R)
  - an *subrings that are not ideals*; (closed under multiplication by H)
  - *subgroups that are not subrings* (not closed under multiplication).

  The *subring lattice* is simply the subgroup lattice with colors denoting the type of substructure. The ring $\mathbb{Z}_3^3$ exhibited all three substructures. We also saw all 11 rings of order 4, though this was mostly to get more familiar with the substructures.

  To do:
  - Familiarize yourself with subring lattices, what the colors mean, and the difference between $\langle S \rangle$ and (S).

  - Be able to write down and identify different examples of substructures of $\mathbb{Z}[x]$, like $\langle x \rangle$, (x), $\langle 2 \rangle$, (2), $\langle x, 2 \rangle$, and $(x, 2)$. Know which polynomials each contains, which is a ideal, subring, etc.
  - Know examples of left ideals that are not right ideals.

  Learn / memorize:
  - Be able to write down formal mathematical definitions of a ring, subring, and ideal.
  - Be able to construct the subring lattice of $\mathbb{Z}_2^2$ and $\mathbb{Z}_3^2$ from scratch.

- **WEEK 2: 1/16–1/20**. MLK Day Monday. Two lectures on reviwing ring theory, covering the Chapter 7 slides (much of pp. 16–62, but some slides skipped). HW 0 due next Monday.

  Summary & key ideas. We discussed the ideal generated by a set $S \subseteq R$, which is the smallest ideal that contains S. If R contains 1, then this is equal to the set of all "linear combinations", much like a number of other similar definitions we've seen. However, if R does not contain 1, then we only get one containment! We saw examples like $R = 2\mathbb{Z}[x]$, with $S = \{2\}$, and also $S = \{2, x\}$.

  We reviewed the notions of units and zero divisors. A big idea is the *proper ideals cannot contain units.* Integral domains are rings with 1 that have no zero divisors.

  We reviewed how the quotient ring R/I is defined, and how to add and multiply cosets. Then we reviewed the four ring isomorphism theorems, and saw that they were almost completely analogous to those for groups. The FHT says that *every homomorphic image is a quotient.* Then the correspondence theorem chacterizes the substructures of a quotient R/I – the subrings have the form S/I and the ideals have the form J/I, for S and J that contain I. In terms of the subring lattice, this just means that *taking the quotient amounts to chopping off the lattice at I, while preserving the colors.* The fraction theorem says that $(R/I)/(J/I) \cong R/J$, which means that chopping the lattice off at I, and then at J, has the same effect as originally chopping it off at J. Finally, the diamond theorem describes an inherient structural duality within subring lattices.

  There are two "imporant" types of ideals: *maximal* and *prime* ideals. This week we reviewed maximal ideals: these are those for which R/I is simple (by the correspondence theorem). If R is commutative, then I is maximal iff R/I is a field (because fields avoid units!). We saw some subring lattices of finite fields along the way. Unlike groups, which need not have maximal subgroups (like the Prüfer group that we saw), every ideal is contained in a maximal ideal. We need some tools from set theory for this. Specifically, Zorn's lemma, which is equivalent to the axiom of choice, is needed to carry out unions *transfinititely.* In understanding this, we saw some fun facts about ordinal arithmetic along the way, like how $1 + \omega = \omega \neq \omega + 1$.

  To do:
  - Make sure you understand how to interpret all of the isomorphism theorems in terms of subring lattices.

  Learn / memorize:
  - Learn the definitions of units, zero divisors, kernels, and ring homomorphisms.
  - Be able to prove (in 1 line) that if an ideal I contains a unit, then $I = R$.
  - Be able to prove (in 1 line) that $\text{Ker}(\phi)$ is an ideal.
  - Be able to prove (in 1 line) the FHT for rings, assuming the FHT for groups.
  - Know that I is maximal iff R/I is a field.

- Learn the common examples of maximal ideals, and what their quotient fields are. E.g., $(p) \subseteq \mathbb{Z}$, and $(p, x) \subseteq \mathbb{Z}[x]$, and $(x) \subseteq F[x]$, and $(x, y) \subseteq F[x, y]$, and $\mathbb{F}_p[x]/(f(x))$ for an irreducible degree-n polynomial.

- **WEEK 3: 1/23–1/27**. Three lectures on the Chapter 7 slides (pp. 70–89). HW 1 due Friday.

  Summary & key ideas. Given an integral domain, its *field of fractions* is the smallest field that contains it. We can construct this by defining an equvalence relation on a set $R \times R^*$ of ordered pairs, where $(a, b) \sim (c, d)$ iff $ad = bc$. Addition and multiplication is defined in the predictable manner. This can be formalized via a *(co-)universal property*, and visualized with a commutative diagram.

  The construction of the field of fractions can be generalized to $R \times D$, where $D \subseteq R$ is any multiplicatively closed subset (D for "denominator") containing no zero divisors. The resulting ring is called the *localization at D*, denoted $D^{-1}R$, and it is the smallest ring that contains R in which everything in D has a multiplicative inverse. A common example of this is $D = R - P$, the complement of a prime ideal. Finally, via the universal property, this construction can be generalized to the case when D contains zero divisors, but the map $\iota \colon R \to D^{-1}R$ 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.

  To do:
  - Know the field of fractions for some basic rings (e.g., $\mathbb{Z}$, $\mathbb{F}[x]$, and $\mathbb{Z}[\sqrt{-m}]$).
  - Be able to state basic properties about divisibility into the language of ideals.
  - Be able to explain in simple terms why PID are "nice rings."
  - Be able to use explicit examples of unique factorization failing (e.g., $3 \mid (2 - \sqrt{-5})(2 + \sqrt{-5}) = 9$) to find a non-principal ideal and a non-prime irreducible.

  Learn / memorize:
  - The definition of a prime ideal, principal ideal, and PID.
  - The definitions of associates, irreducible and prime elements, and that "prime $\Rightarrow$ irreducible."

- **WEEK 4: 1/30–2/4**. Three lectures on the Chapter 7 slides (pp. 90–119). HW 2 due Friday.

  Summary & key ideas. 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 $(\operatorname{lcm}(a,b))$. 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 $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Q}[x, x^{1/2}, x^{1/4}, \dots]$.

  We defined a *Eulidean domain* to be a ring where the division algorithm works: given $a, b \in R$ with $b \neq 0$, we can write $a = bq + r$, with $d(r) < d(b)$, where $d \colon R^* \to \mathbb{Z}_{\leq 0}$ is a *degree function* satisfying $a \mid b \Rightarrow d(a) \leq d(b)$. Examples include $\mathbb{Z}$, $\mathbb{Z}[i]$, $F[x]$. We showed that units are the elements of R of minimal norm, and the every Euclidean domain is a PID, by showing that every ideal I is generated by any element $d \in I$ of minimal norm.

  For every squarefree $m \in \mathbb{Z}$, there is a *quadratic field* $\mathbb{Q}(\sqrt{m})$. This has a subring R_m consisting of roots of monic polynomials. If $m \equiv 2, 3 \pmod 4$, then $R_m = \mathbb{Z}[\sqrt{m}]$, but $R_m = \mathbb{Z}\big[\frac{1+\sqrt{m}}{2}\big]$ for $m \equiv 1 \pmod 4$. If $m < 0$, then the former consists of complex numbers on a "rectangular" grid, and the latter lies on a "triangular" grid. The *field norm* is $N(a + b\sqrt{m}) = a^2 - m^2 b$, which is the square of the complex norm if $m < 0$, otherwise it could take negative values. It's multiplictive property, $N(xy) = N(x)N(y)$, is quite useful. Two important examples are the *Gaussian integers*, $R_{-1} = \mathbb{Z}[i]$ and the *Eisenstein integers*, $R_{-3} = \mathbb{Z}\big[\frac{1+\sqrt{-3}}{2}\big]$. We saw examples of primes in these rings, and in R_{-5}, which has non-prime irreducibles. Each prime $p \in \mathbb{Z}$ when passing to R_m can do one of three things:
  - *inert*: if (p) is a prime ideal in R_m
  - *split*: if $(p) = P_1 P_2$ for distinct prime ideals P_i
  - *ramified* if $(p) = P^2$ for a prime ideal P.

  These can be characterized with quadratic residues mod p, but that's not a priority in this class.

  The *(ideal) class group* measures how unique factorization fails in a UFD. The elements are equivalence classes of ideals, where $I \sim J$ if $\alpha I = \beta J$ (i.e., I and J have "a common multiple"). The identity element are the principal ideals. We saw that $\mathrm{Cl}(R_{-5}) \cong \mathbb{Z}_2$, $\mathrm{Cl}(R_{-14}) \cong \mathbb{Z}_4$, and $\mathrm{Cl}(R_{-30}) \cong \mathbb{Z}_2^2$.

  To do:
  - Be able to explain why rings like $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Q}[x, x^{1/2}, x^{1/4}, \dots]$ aren't UFDs.
  - Given a PID, know how to identify $(\gcd(a,b))$ and $(\operatorname{lcm}(a,b))$ in the lattice of ideals.

- Be able to interpret the behavior of primes p in R_m (inert, splits, ramified) in terms of subring lattices.
- Be able to identify non-prime irreducibles in a picture of a ring like R_{-5} or R_{-6}.

Learn / memorize:

- The definition of a UFD and Euclidean domain.
- Learn examples of UFDs that aren't PIDs.
- Learn examples of Euclidean domains and their degree functions.
- The definition of the ring R_m of quadratic integers (both "rectangular" and "triangular" types).
- The definition of a prime that splits, is inert, or ramifies, in R_m.

- **WEEK 5: 2/6–2/10**. Three lectures on the Chapter 7 slides (pp. 120–139). HW 3 due Friday.

Summary & key ideas. The ring R_m of quadratic integers is *norm Euclidean* if it is a Euclidean domain with degree function $d(x) = |N(x)|$, i.e., the *field norm* $N(a + b\sqrt{m}) = a^2 - mb^2$ of $\mathbb{Q}(\sqrt{m})$. We showed that R_m is norm-Euclidean in the "rectangular" cases for $m = -2, -1, 2, 3$, and left the "triangular cases" of $m = -11, -7, -3, 5, 13$ for the HW. It turns out that rings like R_{69} and R_{14} are Euclidean but not norm Euclidean, which is just bizarre (D.A. Clark, 1994).

The *Sunzi remainder theorem* from number theory dates back to 3rd century China, and it guarantees that a system of linear congruences (mod $n_1, \dots, n_k$) have a solution if the $n_1, \dots, n_k$ are pairwise co-prime. We formulated four versions of this, each more general than the other: for PIDs, commutative rings, and finally for general rings. This required us to define what it means for ideals to be co-prime: $I + J = R$. We proved the most general version of this. We discussed several group-theoretic analogues, including an old HW exercises, that $G/(A \cap B) \cong G/A \times G/B$, and a new HW problem on idempotents.

We finished with looking at polynomial rings. If R is an integral domain, then $R[x]$ is as well. A useful technique is to "reduce coefficients mod I", and we showed that $(R/I)[x] \cong R[x]/(I)$, where $(I) := I[x]$. Finally, we showed that $I \trianglelefteq R$ is prime iff $(I) \trianglelefteq R[x]$ is prime.

To do:

- Review the slides and ask any questions that you have.

Learn / memorize:

- Learn the definition of the product IJ of two ideals.
- Learn the definition of co-prime ideals.
- Memorize the formulation of the Sunzi remainder theorem.

- **WEEK 6: 2/13–2/17**. Three lectures on the Chapter 7 slides (pp. 140–151), and the Chapter 5 slides (pp. 109–114). HW 4 due Friday.

  Summary & key ideas. We continued to study polynomial rings. A polynomial 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.

  Next, we moved onto Hilbert's basis theorem: if a ring R with 1 is Noetherian (i.e., every ideal if finitely generated), then so is $R[x]$. Inductively this means that $R[x_1, \dots, x_n]$ is as well. We saw an explicit example using $R = 2\mathbb{Z}$ for how it fails if $1 \notin R$.

  Finally, we spent a day with the alternating groups A_n, and proved that they are simple. The conjugacy class of an element $\sigma \in S_n$ is precisely the set of element with the same cycle type. In A_n, these conjugacy classes are either the same, or they split into two classes of equal size. This is basically just due to the diamond theorem, and whether the centralizer $C_{S_n}(\sigma)$ lies in A_n or not (in which case, exactly half of it lies in A_n). Next, we proved that all 3-cycles are conjuagte in A_n (for $n \geq 5$), and they all generate A_n. Finally, we showed that *every* normal subgroup $N \neq \langle 1 \rangle$ of A_n contains a 3-cycle, and hence every 3-cycle, and so $N = A_n$. In other words, A_n does not contain any normal subgroups, other than A_n and $\langle 1 \rangle$. Thus, A_n is simple for $n \geq 5$.

  To do:
  – Practice using Eisensten's criterion to show that a polynomial is irreducible.

  Learn / memorize:
  – Hilbert's basis theorem: if R is Noetherian, then $R[x_1, \dots, x_n]$ is as well.
  – A_n is simple for all $n \neq 4$.

- **WEEK 7: 2/20–2/24**. Three lectures on the Chapter 6 slides (pp. 1–32). Quiz 2 Wednesday. HW 5 due Friday.

  Summary & key ideas. If $N \trianglelefteq G$ and $Q = G/N$, then G is an *extension of Q by N*. This can be described by saying that the sequence $N \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$ is *exact*, which means that if $\mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$. Sometimes, this is expressed as a *short exact sequence*, $1 \to N \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q \to 1$. This has a pleasing visual interpretation in the subgroup lattice: Q is "sitting on top of" N. Though we always have $N \trianglelefteq G$ and $H \cong G/N$, in some cases, we also have $G \cong N \rtimes H$ (right split) or even $G \cong N \times H$ (left split).

  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*.

  To do:

  – Be able to describe in plain and simple terms (intuitive, in terms of subgroup lattices) what the following concepts mean:

    (1) Extension of Q by N
    (2) Composition series
    (3) Derived series.
    (4) Solvable group.

  – Be able to determine whether an extension is right or left split by inspection the subgroup lattice.
  – Be able to find all composition series of a group G by inspection, using the subgroup lattice.
  – Be able to find the derived series by inspection, using the subgroup lattice.

  Learn / memorize:

  – Be able to construct subgroup lattices (by isomorphism type, not necessarily generators) of C_4, V_4, D_3, C_6, Q_8, D_4 from memory.
  – Be able to recognize subgroup lattices of larger groups like A_4, Dic_6, and Q_{16}.
  – What it means that G is an extension of Q by N, and how to encode this in terms of a subgroup lattice.
  – Definitions: group extension, composition series, derived series, solvable group.
  – Two equivalent conditions of what it means to be solvable (composition factors are cyclic, or the derived series reaches the bottom).

- **WEEK 8: 2/27–3/3**. Two lectures on the Chapter 6 slides (pp. 33–43). Midterm 1 Wednesday. HW 6 due Friday (extended until Monday night).

  Summary & key ideas. Given $N \trianglelefteq G$, we showed showed that G is solvable iff N and G/N are both solvable. This has as nice "almost picture proof" involving concatenating composition series of N and G/N and using the correspondence theorem. We also briefly discussed a *chief series* of a group, which is a maximal normal series. In contrast, a composition series is a maximal subnormal series.

  The *ascending central series* (ACS) of G is a normal series $\langle 1 \rangle = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots$ defined inductively by "*jumping up to the center, taking the quotient, and repeating this process.*" If this reaches the top of the lattice in m steps, then G is *nilpotent*, of nilpotency class m. If G is nilpotent, it is solvable. This is intuitive because G being nilpotent means it can be built with central extension, whereas solvable groups can be built with abelian extensions (central implies abelian, but not conversely).

  The process described above are called *maximal central ascents*, and we can define (not necessarily maximal) central ascents similarly: H is a central ascent from $N \trianglelefteq G$ iff G/H is central in G/N. We proved the central series lemma: *H/N is central in G/N iff* $[G, H] \leq N$. This encourages us to try to (almost) "invert" this process: given $N \trianglelefteq G$, the subgroup $[G, N]$ is contained in N; we call it a *maximal central descent*, ad define intermedate groups as *central descents*. We can visualize these together with the *chutes and ladders diagram* of a group, which is its subgroup lattice annotated with red a blue arrows out of every subgroup: red for the maximal central descents, and blue for the maximal central ascents. The ascending and descending central series can be read right off of this diagram.

  To do:
  - Keep studying subgroup lattices! Be able to recognize C_4, V_4, C_6, D_3, D_4, Q_8, $C_4 \times C_2$, A_4, Dic_6, D_6, Q_{16}, D_8, SD_8, SA_8, $\mathrm{SL}_2(\mathbb{Z}_3)$.
  - Practice taking maximal central ascents and descents on subgroup lattices. Try constructing the chutes and ladders diagram of the groups above.
  - Practice finding the derived series, composition series, chief series, and the upper and lower central series on subgroup lattices, by inspection.

  Learn / memorize:
  - The definition of a normal series, and a subnormal series.
  - Learn what the *center* is in the groups above.

- **WEEK 9: 3/6–3/10**. Three lectures on the Chapter 6 slides (pp. 43–62), and Chapter 10 slides (pp. 1–7). Quiz 3 Monday. HW 7 due Friday.

  Summary & key ideas. The *descending central series* (DCS) is a normal series $G = L_0 \trianglerighteq L_1 \trianglerighteq \cdots$, which each L_{k+1} is defined inductively as "*the lowest we can go down so the previous subgroup L_k is central in the quotient*" (technically, G/L_k is central in G/L_{k+1}). We showed that this reaches the bottom of the lattice iff the ascending central series reaches the top, and they do so in the same number of steps. In the language to think of about this: the ASC is the result of taking maximal central ascents up the lattice, and the DSC is the result of taking maximal central descents down. The key step in the proof was showing that $L_{n-k} \leq Z_k$ for all k. In other words, the ASC and DSC form a "crooked ladder," with the L_i's lower than the correponding Z_j's.

  We finished with a summary of a number of equivalent conditions for what it means for G to be nilpotent, proving a few and skipping others (they were Math 8510 HW): (i) the ASC reaches the top, (ii) the DCS reaches the bottom, (iii) G has no fully unnormal subgroup, (iv) all Sylow p-subgroups are normal, (v) G is the direct product of its Sylow p-subgroups, and (vi) every maximal subgroup of G is normal.

  A number of classic problem that stumped the ancient Greeks (e.g., squaring the circle, doubling the cube, trisecting an angle, the unsolvability of the quintic) have elegant solutions involving field theory. Since fields are simple rings, every nonzero field homomorphism $\phi\colon K \to L$ is an embedding. We call ϕ, and L, an *extension.* The unfortunate notation L/K is used to denote this. A key observation is that if $K \subset L$, are fields, then L is a K-vector space. The *degree* of the extension is simply the dimension of this vector space, i.e., the size of a basis. For example, $\mathbb{Q}(\sqrt{2})$ has basis $\{1, \sqrt{2}\}$, and $\mathbb{Q}(\sqrt{2}, i)$ has basis $\{1, \sqrt{2}, i, \sqrt{2}i\}$.

  To do:
  - Be able to prove that every nonzero field homomorphism is injective.
  - Be able to prove that if $K \subseteq L$ are field extensions, then L is a K-vector space.

  Learn / memorize:
  - Learn the basic field theory definitions, and the definition of a vector space.
  - Memorize the six equivalent conditions of what it means for G to be nilpotent.

- **WEEK 10: 3/13–3/17**. Two lectures on the Chapter 10 slides (pp. 8–20). For Friday: watch the (old) *Lecture 6.3: Polynomials and irreducibility* (23:53–38:20) and *Lecture 6.4: Galois groups* (34 min); the links are on Canvas or a pre-2021 Math 4120 webpage. Quiz 4 Wednesday. HW 8 due Friday (okay to turn it in the Monday after spring break).

  Summary & key ideas. The degree of a simple field extension $K(\alpha)$ is the degree of a minimal polynomial of α over K. The *splitting field* of a polynomial is the smallest field that contains all of its roots. A field F is *algebraically closed* if every polynomial in $F[x]$ splits; like the complex numbers $\mathbb{C}$. We analyzed several examples, like $\mathbb{Q}(\sqrt{2}, i)$ and $\mathbb{Q}(\sqrt[3]{2}, \omega)$, and observed that their subfield lattices had the same structure as several familiar subgroup lattices, but upside-down. There is also a *tower law* for fields: if $F \subseteq E \subseteq K$ are extensions, then $[K : F] = [K : E][E : F]$. A field extension generated by a single element is called *primitive.* The primitive element theorem says that every finite-degree extension of $\mathbb{Q}$ has a primitive element, i.e., if $[K : \mathbb{Q}] < \infty$, then $K = \mathbb{Q}(\alpha)$. These results will be proven later.

  The automorphism group of a field extension K of $\mathbb{Q}$ is called its *Galois group*, denoted $\mathrm{Gal}(K)$. The Galois group of a polynomial $f(x)$ is the Galois group of its splitting field, denoted $\mathrm{Gal}(f(x))$. We saw several examples of Galois groups: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})) \cong C_2$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)) \cong V_4$, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \zeta_3)) \cong D_3$.

  To do:
  - Be able to draw the subfield lattices of the field extensions we've seen: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

  Learn / memorize:
  - Learn the examples of field extensions we've seen, and what a basis for each is: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.
  - Learn the new definitions we've seen: what it means for $K(\alpha)$ to be *algebraic*, the minimal polynomial of α, the *splitting field* of a polynomial, a *primitive element*, the *Galois group* of a field extension, and of a polynomial.
  - Learn the Galois groups of the fields listed above.

- **WEEK 11: 3/27–4/1**. Watch the (old) *Lecture 6.5: Galois group actions and normal field extensions* (26 min), *Lecture 6.6: The fundamental theorem of Galois theory* (31 min). The links are on Canvas or a pre-2021 Math 4120 webpage. HW 8 can be turned in Monday. HW 9 due Friday.

  Summary & key ideas. The Galois group permutes the roots of a polynomial. This means that there is a *group action* of $\mathrm{Gal}(f(x))$ on its roots. If $f(x)$ is irreducible, then this action is transitive (i.e., has only one orbit). An extension K of F is *normal* if every irreducible polynomial $f(x) \in F[x]$ splits in $K[x]$. In other words, "*if K contains one root of an irreducible polynonmial, it must contain all of them.*" The degree of a normal extension is equal to the order of its Galois group; otherwise it is strictly greater than the order. In other words, the order of $\mathrm{Gal}(f(x))$ is the degree of the extension of its splitting field.

  The *fundamental theorem of Galois theory* (roughly) says that the subfield lattice of K has the same structure as the subgroup lattice of $\mathrm{Gal}(K)$, but ‘’upside-down." Moreover, the normal field extensions correspond to normal subgroups. These results are stated this week, and will be proven next week. A polynomial $f(x)$ is solvable by radicals iff its Galois group $\mathrm{Gal}(f(x))$ is solvable. Thus, in order to find a polynomial that isn't solvable, it suffices to find one that has Galois group S_5. Any degree-5 polynomial with exactly two complex roots is such an example – because it contains an element of order 5 (Cayley's theorem), which is a 5-cycle, and complex conjugation is a 2-cycle. Together, these generate S_5, which isn't solvable.
  To do:
  - Practice determining which subfields are normal, and which polynomials they are splitting fields of.
  - Revisit the subfield lattices of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, and explore the lattice of $\mathbb{Q}(\sqrt[4]{2}, i)$.
  - Compare the subfield lattices of the examples above to the subgroup lattices of the corresponding Galois group.
  - Be able to explain the main ideas behind the FTGT, and solvability by radicals in terms of the Galois group.

  Learn / memorize:
  - Learn the definition of what it means for an extension field to be *normal.*

- **WEEK 12: 4/3–4/7**. Watch the (old) *Lecture 6.7: Ruler and compass constructions* (23 min), and *Lecture 6.8: Impossibility proofs* (17 min). The links are on Canvas or a pre-2021 Math 4120 webpage.

  Summary & key ideas. The problem from the ancient Greeks about ruler and compass constructions have elegant solutions from field theory. Every *constructable number* lives in some extension of $\mathbb{Q}$ of degree 2^n. Doubling the cube would require constructing $\sqrt[3]{2}$, squaring the circle would require $\mathbb{Q}(\sqrt{\pi})$, and trisecting an angle would require $\cos(20^\circ)$, and none of these live in an extension of $\mathbb{Q}$ of degree 2^n.

  We spent the last two days proving the results that were used in the YouTube videos in the previous week, including:
  - Minimal polynomials are irreducible, and unique (up to scalars).
  - Every element in $F(\alpha)$ can be written uniquely as $s = r(\alpha)$, for some polynomial $r(x) \in F[x]$.
  - If α, β have the same irreducible polynomial over F, then $F(\alpha) \cong F(\alpha)$.
  - The degree of the field extension, $[F(\alpha) : F]$, is equal to the degree of the minimal polynomial, $m_\alpha(x)$.
  - Tower law of field extensions: if $F \subseteq E \subseteq K$, then $[K : F] = [K : E][E : F]$.
  - Primitive element theorem: If $[K : F] < \infty$, then $K = F(\alpha)$ for some $\alpha \in K$.

  To do:
  - Be able to identity a primitive element for the small examples of splitting fields that we have seen. Your first "guess" is probably right.

  Learn / memorize:
  - Learn and understand what $[F(\alpha) : F] = m_\alpha(x)$ means, and how to apply it.
  - Given some algebraic number α, be able to write the generic form of an element of the field $F(\alpha)$.

- **WEEK 13: 4/10–4/14**. Midterm 2 Friday. HW 9 extended until Friday.

  Summary & key ideas. We summarized the main ideas of Galois theory, with examples, and proceeded with the proof of the *fundamental theorem of Galois theory* (FTGT). The key ingredient is a pair of maps

  $$\mathcal{F}\colon \big\{\text{subgroups of } \mathrm{Gal}(K)\big\} \longrightarrow \big\{\text{subfields of } K\big\}$$
  $$\mathcal{G}\colon \big\{\text{subfields of } K\big\} \longrightarrow \big\{\text{subgroups of } \mathrm{Gal}(K)\big\},$$

  defined as
  - $\mathcal{F}(H) =$ "*the (subfield of) elements of* K *fixed by every* $\phi \in H$"
  - $\mathcal{G}(E) =$ "*the (subgroup of) automorphisms of* $\mathrm{Gal}(K)$ *that fixes every* $e \in E$."

  These maps are *order-reversing*:

  $$J \leq H \quad\Rightarrow\quad \mathcal{F}J \supseteq \mathcal{F}H, \qquad\qquad E \subseteq L \quad\Rightarrow\quad \mathcal{G}E \geq \mathcal{G}L.$$

  Moreover, if $K : F$ is a Galois extension (every $\alpha \in K$ gets moved by some automorphism) , then they are *bijections*, and preserve the (subfield) degree and (subgroup) index. That is, if $J \leq H \leq \mathrm{Gal}(K)$ and $F \subseteq E \subseteq L \subseteq K$,

  $$[\mathcal{F}J : \mathcal{F}H] = [H : J], \qquad [\mathcal{G}E : \mathcal{G}L] = [L : E].$$

  To do:
  - Study for Midterm 2, on group extensions, composition series, solvable and nilpotent groups.
  - Demonstrate how $\mathcal{F}$ and $\mathcal{G}$ fail to be "nice" for a non-Galois extension, like $K = \mathbb{Q}(\sqrt[3]{2})$.

  Learn / memorize:
  - Be able to define the maps $\mathcal{F}$ and $\mathcal{G}$.

  - Be able to find the specific subfields and subgroups of the maps $\mathcal{F}$ and $\mathcal{G}$, for "small" examples, like the splitting field of $f(x) = (x^2 - 2)(x^2 + 1)$ and $x^3 - 2$.

- **WEEK 14: 4/17–4/21**. Three lectures on examples of Galois groups, cyclotomic extension, and the Galois correspondence via the maps $\mathcal{F}$ and $\mathcal{G}$. HW 10 due Friday.

  Summary & key ideas. A *cyclotomic extension* is a field extension of the form $K = F(\zeta)$, where $\zeta = e^{2\pi i/n}$ is a (primitive) root of unity. The Galois group is

  $$\mathrm{Gal}(K) = \big\{\sigma_k \mid \gcd(n,k)\big\} \cong \mathrm{Aut}(\mathbb{Z}_n) \cong U(n) = \mathbb{Z}_n^\times,$$

  where $\sigma_k \colon \zeta \mapsto \zeta^n$. It acts simply transitively on the primitive roots of unity. The Cayley table of $\mathrm{Gal}(x^n-1)$ is the same as the Cayley table of $\mathbb{Z}_n^\times$, but replacing k with σ_k. It's also the same as the Cayley table of $\mathrm{Aut}(\mathbb{Z}_n)$, where σ_k is the "k-ling" (e.g., doubling, tripling) map.

  The Galois group of $x^n - b$, where $b \geq 2$, is "usually" the semidirect product of the normal subgroup $\langle\rho\rangle \cong C_n$, where $\rho\colon \sqrt[n]{b} \mapsto \zeta\sqrt[n]{b}$, and $\mathrm{Gal}(x^n-1) \cong U(n)$. One exception is $\mathrm{Gal}(x^8-2)$, because $\zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, and $\sqrt{2} = (\sqrt[8]{2})^4$. This group has different relations than $\mathrm{Gal}(x^8-3)$, because ζ_8 does "not have a power of $\sqrt[8]{3}$ in it."

  To do:
  - Be able draw the action graph of $\mathrm{Gal}(x^n-1)$ on the n roots of unity.
  - Explore the Galois groups of x^3-2, x^4-2, x^5-2, and x^6-2.
  - Understand the difference of $\mathrm{Gal}(x^8-2)$ vs. $\mathrm{Gal}(x^8-3)$ – why one of these has order 16 and the other 32.
  - Your time is best spent understanding the examples of Galois groups that we have seen in class and on the homework (there are not too many of them), and the maps $\mathcal{F}$ and $\mathcal{G}$.

  Learn / memorize:
  - $\mathrm{Gal}(x^n-1) \cong \mathbb{Z}_n^\times$
  - Memorize which group $\mathbb{Z}_n^\times$ is for $n = 3, \dots, 12$. And know how to rederive it if you forget.

- **WEEK 15: 4/24–4/28**. HW 11 due Friday. Two lectures on free groups, free products, and group presentations, covering the slides from *Chapter 7: Universal constructions*, pp. 51-54, 74-79, 83-87. We also mentioned in passing, a few other topics for background and context from this chapter, including factoring maps, category theory, the fundamental group of a topological space, and free abelian groups. On the last day of class, we returned to Galois theory and sketched the proof of the fundamental theorem (FTGT), and one direction of the fact that $f(x)$ is solvable by radicals iff $\mathrm{Gal}(f(x)$ is a solvable group.

  Summary & key ideas. We started by revisiting the notion of a group presentation. We can always write a relation as a word that is the identity; these are "relators". For example, $a = b$ just means $ab^{-1} = 1$. Formally, we will consider presentations of the form $G = \langle S \mid R\rangle$, where S are the generators, and R is the set of relators.

  A *free group* on a set S is the group $G = \langle S \mid \;\rangle$, i.e., the group of all words in the generating set (and inverses), subject to no relations, other than the "trivial" ones of the form $ss^{-1} = 1$, and $s^{-1}s = 1$. The free group is the "largest" group on S, in that every other group generated by S is a quotient of it. Sometimes, (like in Math 8510), this property is taken as the actual definition, which can be formalized as a *universal property*, using a triangular commutative diagram. The Cayley diagram of the free group $F_2 = \langle a, b \mid \;\rangle$ looks "fractal-like," because it has no loops. Surprisingly, if $n, m \geq 2$, the free group F_n embeds into the free group F_m.

  A related concept is the *free product* of groups. Specifically, 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: $C_2 * C_2 \cong D_\infty$ (a frieze group!), and $C_3 * C_2 \cong \mathrm{PSL}_2(\mathbb{Z})$ (recall the tiling of hyperbolic triangles in the upper half-plane).

  Then, 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. Loosely speaking "*adding generators induces a quotient.*" Thus, if $G_1 = \langle S_1 \mid R_1\rangle$ has "more generators, and/or fewer relations" than $G_2 = \langle S_2 \mid R_2\rangle$, there is a quotient $G_1 \twoheadrightarrow G_2$. To apply this: if we want to show that a "mystery group" $M = \langle S_1 \mid R_1\rangle$ 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.

  Returning to Galois theory: an intermediate subfield E, where $F \subseteq E \subseteq K$ is *stable* if $\phi(E) = E$ for all automorphisms $\phi \in \mathrm{Gal}(K : F)$. This is equivalent to the corresponding group being *normal*, and this is the last piece we needed for the FTGT.

  A *simple extension* of a field F is one of the form $F(\alpha)$, where $\alpha^n \in F$ – basically just adjoining an n^{th} root. An *extension by radicals* of F is an extension K that can be constructed iteratively by simple extensions. Loosely speaking, at every step of the way, we are adjoining a root of a polynomial $x^{n_i} - b_i$. At the end of the day, this can be achieved by:

- adjoining an n^{th} root of unity (an abelian extension), where $n = n_1 n_2 \cdots n_k$
- adjoining p_i^{th} root, for $i = 1, \ldots, k$ (each is a cyclic extension).

This *sequence of field extensions* correspond to a *sequence of abelian extensions of groups*, via the Galois correspondence. Since all extensions are abelian, $\mathrm{Gal}(f(x))$ has a compositions series with cyclic factors, and thus is solvable.

To do:

- Understand what is meant by "*adding generators induces a quotient.*"
- Be able to show that $M = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$ is V_4, by (i) using relations to show that $|M| \leq 4$, and then (ii) mapping a and b to 2×2 matrices.
- In very rough terms, be able to explain the idea of the fundamental theorem of Galois theory.
- In very rough terms, be able to explain the steps in the proof that the polynomial $f(x) = x^5 - 10x^2 + 2$ is not solvable by radicals.

Learn / memorize:

- The difference between a free group on S, and a free product of groups G_1 and G_2.

Finals week: 5/1–5/5. Final exam Friday 3–5:30pm.

To do: Study! The exam will be cumulative.