MATH 561
MODERN ALGEBRA I
FALL 2018

Week 1

Algebra is the study of computational operations. The first purpose people had for studying algebra at some modest level of abstraction was extracting solutions to polynomial equations. Algebra was then heavily influenced by demands from number theory and invariant theory which led to a formalization and abstraction of sets with abstract algebraic operations. Groups, the simplest of these objects, will be the focus of the first half of our course. Groups form the backbone of the mathematical understanding of symmetry, and the topics we'll see concerning their structure and classification are a reasonable blueprint for understanding more complicated algebraic objects. Rings provide the setting for writing down and solving polynomial equations as well as understanding the concepts of primeness and divisibility, these will constitute the material for the second half of the course.

0.1. **Examples.** We'll begin by cooking up some examples of algebraic operations on sets.

First we have the integers $\mathbb{Z}$, they come equipped with addition $n, m \to n+m$ and multiplication $n, m \to nm$. Addition has an identity: $0 \in \mathbb{Z}$, this means that $0 + n = n$ for any $n \in \mathbb{Z}$. Multiplication has an identity as well: $1 \in \mathbb{Z}$, so we have $1n = n$. Addition and multiplication and commutative operations: $n + m = m + n$, $nm = mn$, and multiplication distributes over addition $k(n + m) = kn + km$. Furthermore, both addition and multiplication are associative, this means that if we do these operations on three or more elements it doesn't matter what order we choose: $(n+m)+k = n+(m+k)$, $n(mk) = (nm)k$. Addition also has a concept of inverse: for any n there is $-n$ so that $n + (-n)$ is 0, the additive identity. That's a lot of structure, and it means that the integers $\mathbb{Z}$ form a *commutative ring*. In particular, when we only consider addition, $\mathbb{Z}$ is a *group*.

The rational numbers $\mathbb{Q}$ are similar to the integers, except that when we forget 0 they also form a group. For any non-zero rational number $r = \frac{p}{q}$, there is another rational number $\frac{1}{r} = \frac{q}{p}$ with $r\frac{1}{r} = 1$. This makes

$\mathbb{Q}$ into a *field*, which is a special kind of ring. Other examples of fields are the real numbers of $\mathbb{R}$ and the complex numbers $\mathbb{C}$.

Now we'll build two new algebraic objects using our favorite field $\mathbb{K}$. What follows is largely here to get you used to notation.

Definition 0.1. *Let $M_{n,n}(\mathbb{K})$ be the set of $n \times n$ matrices with entries in the field $\mathbb{K}$. Let $GL_n(\mathbb{K})$ be the set of nonsingular $n \times n$ matrices.*

Exercise 0.1. *Which properties of listed above for the integers are satisfied by the matrix multiplication and addition operations on $M_{2,2}(\mathbb{K})$?*

Exercise 0.2. *Which of the group properties listed above does the multiplication operation on $GL_2(\mathbb{K})$ satisfy?*

Definition 0.2. *let $\mathbb{K}[x_1, \ldots, x_n]$ be the set of polynomials in the variables $x_1, \ldots, x_n$. A polynomial which involves no variables corresponds to an element of $\mathbb{K}$, we say that this it ss a "scalar."*

Exercise 0.3. *Show that polynomial addition and multiplication make $\mathbb{K}[x_1, \ldots, x_n]$ into a commutative ring, like $\mathbb{Z}$ above.*

Exercise 0.4. *Find some polynomial in two variables $p(x, y)$ which cannot be written as the product of two non-scalars.*

Exercise 0.5. *Do any non-scalar polynomials have multiplicative inverses?*

0.2. **The Integers.** The integers $\mathbb{Z}$ have a number of other very nice, but slightly less algebraic properties. Let $\mathbb{Z}_{\geq 0}$ be the set of non-negative integers.

(1) *Well ordering*: Any non-empty subset $A \subset \mathbb{Z}_{\geq 0}$ has a minimal element.

(2) *GCD*: For any $n, m \in \mathbb{Z} \setminus \{0\}$ there is a unique common divisor $GCD(n, m)$ such that any other common divisor of n and m divides $GCD(n, m)$.

(3) *LCM*: For any $n, m \in \mathbb{Z} \setminus \{0\}$ there is a unique common multiple $LCM(n, m)$ such that any other common multiple of n and m is divisible by $LCM(n, m)$.

(4) *The Division Algorithm*: if $n, m \in \mathbb{Z}$ with $m \neq 0$ then there are unique $q, r \in \mathbb{Z}$ such that $n = mq + r$ and $0 \leq r < |m|$.

The Division Algorithm is a key component of the *Euclidean Algorithm*, which allows us to compute $GCD(n, m)$. For $n, m \in \mathbb{Z} \setminus \{0\}$ we form a of divisions:

$$\begin{aligned} n &= q_0 m + r_0 \\ m &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \end{aligned}$$

We have $|m| > |r_0| > \ldots > |r_n| \geq 0$, so the sequence of remainders eventually terminates with:

$$r_{n-1} = q_{n+1} r_n.$$

At this point we have $r_n = GCD(n, m)$. Notice that we can write $r_n = r_{n-2} - q_n r_{n-1}$, and that likewise $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$. Going back up the chain, we can write $GCD(n, m) = r_n$ as $an + bm$ for some $a, b \in \mathbb{Z}$.

Definition 0.3. *Remember that we say* n divides m*, written* $n \mid m$ *if we can write* $m = nd$ *for some* $d \in \mathbb{Z}$*. A number* $p \in \mathbb{Z}$ *is said to be* prime *if* $p > 1$ *and* $p \mid ab$ *implies* $p|a$ *or* $p|b$*.*

The fundamental theorem of arithmetic asserts that the primes constitute the fundamental multiplicative building blocks of the integers.

Theorem 1 (FTA)**.** *If* $n \in \mathbb{Z}$*,* $n > 1$ *then* n *can be written uniquely as* $p_1^{a_1} \cdots p_k^{a_k}$ *for primes* $p_1, \ldots, p_k$*.*

Here uniqueness means that if we have another such factorization $n = q_1^{b_1} \cdots q_\ell^{b_\ell}$ then $\ell = k$ and the $q_1, \ldots, q_\ell$ can be reordered so that $q_i = p_i$ and $a_i = b_i$ for all $1 \leq i \leq k$. The fundamental theorem lets us write $GCD(n, m)$ and $LCM(n, m)$ in a very natural way.

Exercise 0.6. *Let* $n = p_1^{a_1} \cdots p_k^{a_k}$ *and* $m = p_1^{b_1} \cdots p_k^{b_k}$ *with* $a_i, b_i \geq 0$. *Show that* $GCD(n,m) = p_1^{min(a_1,b_1)} \cdots p_k^{min(a_k,b_k)}$ *and* $LCM(n,m) = p_1^{max(a_1,b_1)} \cdots p_k^{max(a_k,b_k)}$.

If $GCD(n,m) = 1$ we say that n and m are *relatively prime*. Notice that this means that there are integers $a, b \in \mathbb{Z}$ such that $an + bm = 1$.

Exercise 0.7. *Show that* $GCD(n,m) = 1$ *if and only if there is some* $\mathbb{Z}$*-combination* $an + bm$ *equal to* 1.

For $n \in \mathbb{Z}_{\geq 0}$, the value of the *Euler* ϕ*-function* $\phi(n)$ equals the number of integers $1 \leq a \leq n$ with $GCD(a,n) = 1$.

Exercise 0.8. *Show that if* $GCD(n,m) = 1$ *then* $\phi(nm) = \phi(n)\phi(m)$. *Show that if* p *is a prime then* $\phi(p^a) = p^a - p^{a-1}$.

0.3. **Modular arithmetic.** For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$ we write $a = b \pmod{n}$ if $n \mid (b - a)$, if this holds we say that a is *congruent* to b modulo n. Congruence modulo n defines an equivalence relation on $\mathbb{Z}$; we let $\mathbb{Z}/n\mathbb{Z}$ be the set of integers modulo this equivalence. For any $a \in \mathbb{Z}$ we let $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ denote its associated congruence class; this is the set of integers which differ from a by a multiple of n:

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$$

Exercise 0.9. *Show that there are precisely* n *congruence classes in* $\mathbb{Z}/n\mathbb{Z}$, *namely* $\overline{0}, \ldots, \overline{n-1}$. *Show that the division algorithm can be used to determine congruence class.*

We can define operations on $\mathbb{Z}/n\mathbb{Z}$ by porting them over from $\mathbb{Z}$:

$$\overline{a}\overline{b} = \overline{ab}$$
$$\overline{a} + \overline{b} = \overline{a+b}$$

Exercise 0.10. *Show that these operations are well-defined, and that* $\overline{1}$ *and* $\overline{0}$ *are multiplicative and additive identities in* $\mathbb{Z}/n\mathbb{Z}$. *Show that* $\overline{-a}$ *is an additive inverse to* $\overline{a}$. *Furthermore, show that these operations satisfy the same commutivity, associativity, and distributivity properties satisfied in* $\mathbb{Z}$.

The exercise above implies that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring, just like $\mathbb{Z}$, and furthermore that $\mathbb{Z}/n\mathbb{Z}$ is a group with respect to addition. The

map $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\pi_n(a) = \overline{a}$ is said to be a *homomorphism* of commutative rings (resp. groups).

To finish, let's look at using what we've learned to prove something about $\mathbb{Z}/n\mathbb{Z}$. Let $(\mathbb{Z}/n\mathbb{Z})^*$ be the subset of congruence classes in $\mathbb{Z}/n\mathbb{Z}$ which have a multiplicative inverse. Since addition and multiplication are well-defined, this means that for $\overline{a}$ to be in $(\mathbb{Z}/n\mathbb{Z})^*$ we must have $sa = 1 + tn$ for some $s \in \mathbb{Z}$. But then 1 is a linear combination of a and n, which we recall means that $GCD(a, n) = 1$. Conversely, if $GCD(a, n) = 1$ we can write $sa + tn = 1$ for some $s, t \in \mathbb{Z}$, so $sa = 1 - tn$ and $\bar{s}\overline{a} = 1[\text{ mod } n]$. So we have proved that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid a \leq n, GCD(a, n) = 1\}$. It follows that $\mid (\mathbb{Z}/n\mathbb{Z})^* \mid = \phi(n)$.

Week 2

Symmetry in mathematics is expressed in the language of groups. Groups are also a great example of an algebraic structure because they have few axioms which yield a rich universe of examples. A group is a set G equipped with a binary operation $\circ : G \times G \to G$; we write the product of two elements g, h under this operation as $g \circ h$ or sometimes gh if the operation is clear from context. This operation needs to satisfy three properties:

(1) $\circ$ is associative: $g \circ (h \circ k) = (g \circ h) \circ k$,

(2) there is an identity element $e \in G$ so that $e \circ g = g \circ e = g$,

(3) for any $g \in G$ there is a corresponding inverse element g^{-1} so that $g \circ g^{-1} = g^{-1} \circ g = e$.

It's common to write 1 for the element e when we think of $\circ$ as a "multiplication", and 0 for e when we think of $\circ$ as "addition." The latter situation comes up when $\circ$ is a commutative operation: $\forall g, h \in G$, $g \circ h = h \circ g$. In this case we say G is an *Abelian* group. Let's look at some examples of groups.

Example 0.4. *We've already seen that $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ satisfy the axioms of a group under $+$. In particular, for any $a, b, c \in \mathbb{Z}$ we can verify that $a + (b + c) = (a + b) + c$ [Mod n], and that $\overline{-a} = \overline{n - \overline{a}}$[Mod n]. The class of any multiple of n serves as the identity in $\mathbb{Z}/n\mathbb{Z}$.*

Example 0.5. *A unit of a ring is an element with a multiplicative inverse. The units $\mathbb{Z}^* = \{1, -1\}$ are easily seen to form a commutative group under multiplication. The same holds for the units $(\mathbb{Z}/n\mathbb{Z})^* \subset \mathbb{Z}/n\mathbb{Z}$. We've seen that multiplication is associative in this set, and by definition it contains 1, and every element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ has a multiplicative inverse. Furthermore, if $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$, then the product $b^{-1}a^{-1}$ of their multiplicative inverses is a multiplicative inverse of their product: $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aa^{-1} = 1$. This means that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group under multiplication.*

Example 0.6. *Consider the ring $M_{n,n}(\mathbb{K})$ of $n \times n$ matrices with entries in $\mathbb{K}$ under addition and multiplication. The units $M_{n,n}(\mathbb{K})$ are those matrices with multiplicative inverse, namely $GL_n(\mathbb{K})$. We have already seen that this set is a group under matrix multiplication.*

Example 0.7. *As you might have guessed by now, the units R^* in any ring R form a group under multiplication. If R is a field (ie every element except 0 has a multiplicative inverse, like $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$), then $R^* = R \setminus \{0\}$.*

Example 0.8. *The previous examples highlight how groups can emerge naturally from other algebraic objects, but almost any type of mathematical object -algebraic or not- has a natural group associated to it. If we have a notion of transformations, we can always look at those transformations which take the object isomorphically onto itself, usually this is called an automorphism.*

Let $[n]$ denote the set of natural numbers $\{1, \ldots, n\}$. We call an invertible map of sets $\sigma : [n] \to [n]$ a permutation *on the set $[n]$, and we denote the set of all permutations by S_n. We always have the identity permutation $Id : [n] \to [n]$ which sends any $i \in [n]$ to itself; this is the identity element in S_n. The composition $\sigma_1 \circ \sigma_2$ of any two permutations is also a permutation; in particular, it is bijective since it can be inverted by $\sigma_2^{-1} \circ \sigma_1^{-1}$.*

There are a number of useful ways to represent members of S_n. First, we have wiring diagrams*. For $\sigma \in S_n$ we make two columns of dots labelled $1, \ldots, n$, then we draw an arrow from i in the left column to $\sigma(i)$ in the right column.*

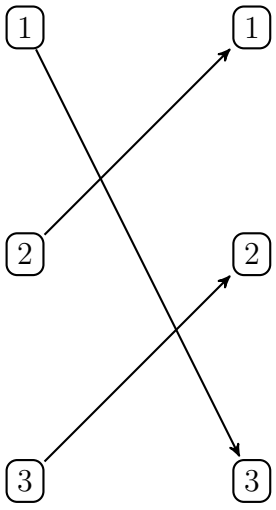

FIGURE 1. $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$

Two wiring diagrams can be composed simply by making three columns, drawing the required arrows from the two diagrams, and following where the paths lead.

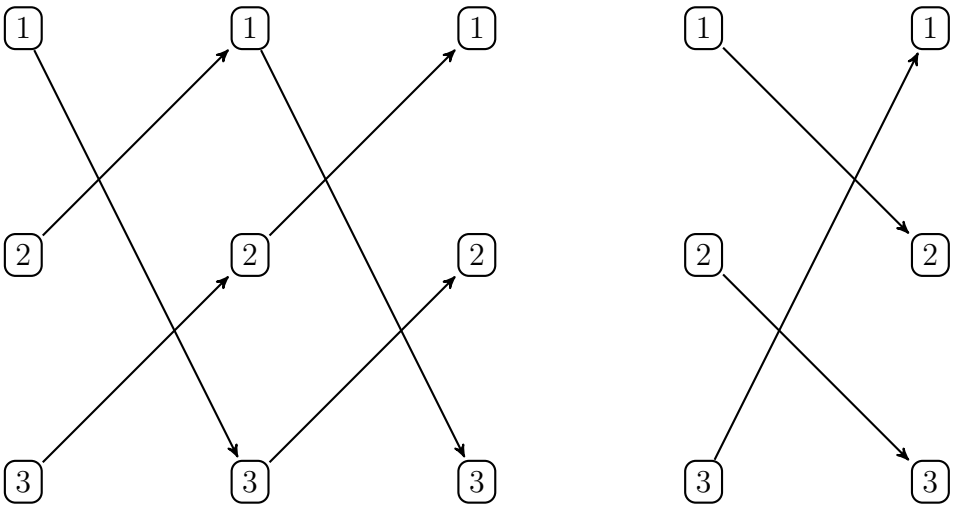

FIGURE 2. $\sigma^2(1) = 2$, $\sigma^2(2) = 3$, $\sigma^2(3) = 1$

The "inverse" of a wiring diagram is obtained by flipping the right and left columns, and the identity wiring diagram has all horizontal arrows. We call the column on the left the "input layer" of the wiring diagram, and the column on the right is the

It's easy to turn a wiring diagram into a matrix. For σ we can build a matrix $P(\sigma)$ by putting a 1 in each entry (i, j) where there is an arrow from j to i, and a 0 elsewhere. This is the "permutation matrix" of the permutation σ.

$$P_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The fact that σ is bijective implies that each input is connected to exactly one output in the wiring diagram. In turn, this means that each row and column of P_σ contains precisely one 1. This latter property also characterizes permutation matrices. It is easy to see that the identity permutation is sent to the identity matrix, where the only non-zero entries are at locations (i, i).

Exercise 0.11. *A "swap" is a wiring diagram with only two edges which aren't horizontal.*

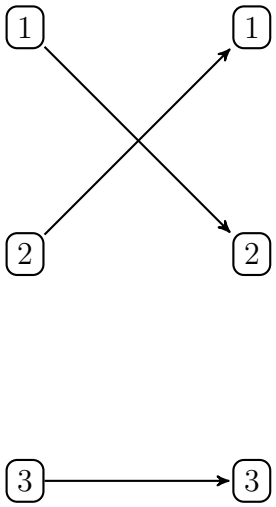

FIGURE 3. A swap: $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$

Show that any wiring diagram can be expressed as a "product" of swaps. Is this expression unique? Conclude that any permutation matrix is the product of permutation matrices with only two off-diagonal non-zero entries.

Exercise 0.12. *For a permutation σ the "sign" $sgn(\sigma)$ is defined to be the determinant $det(P_\sigma)$. Show this number is always ± 1 as follows:*

(1) *show that the sign of a "swap" is always -1,*

(2) *use the property that any P_σ is a product of swaps.*

Show that the parity of the number of swaps in a decomposition of P_σ is an invariant of σ.

The permutation group S_n is the symmetry group of a set of size n with no structure. Other common groups express the symmetries of more complicated objects. The symmetry group D_{2n} of a regular planar n-gon is called the dihedral group. We can label the vertices of a regular n-gon with elements of the set $[n]$, and any symmetry of the n-gon takes the set of vertices bijectively onto itself. In this way, D_{2n}

can be viewed as a subset of the permutation group S_n. There are two basic moves we will consider, flipping across a bisector, and rotating.

Any element of D_{2n} takes the vertex 1 to some $1 \leq j \leq n$, and by rotating the n-gon we see that any vertex j can be achieved by some symmetry. Furthermore, 2 must be taken to either $j+1$ or $j-1$ by a symmetry of the n-gon, and by flipping across the unique bisector going through j we see either can be achieved. Furthermore, these properties (where 1 goes, where 2 goes) determine the symmetry entirely. We conclude that $|D_{2n}| = 2n$. This is the reason for the $2n$ in the notation (honestly I'd prefer D_n, but I'm not in charge of math).

Algebraic objects can emerge naturally by considering a problem like "describe the symmetries of a regular n-gon," but they can also be constructed directly. A group can be specified by giving a set of "generators" and a set of equations or "relations" which must hold among them. We can then just insist on studying the unique group specified by that information. Now we'll look at how to build D_{2n} out of "generators and relations." The generators should be the most basic building blocks of the group, so for D_{2n}, we'll take $R \in D_{2n}$ to be the clockwise rotation $1 \to 2, 2 \to 3, \ldots, n \to 1$. The proof in the paragraph above suggests that we actually only need one more generator $S \in D_{2n}$, this is the move which flips the n-gon along the unique bisector through 1: $1 \to 1, 2 \to n, 3 \to n-1, \ldots, i \to n+2-i, \ldots$.

Exercise 0.13. *We saw above that D_{2n} can be viewed as a subset of S_n. Draw the wiring diagrams for $R, S \in D_8 \subset S_4$.*

Let's let $1 \in D_{2n}$ be the "do nothing" identity element. By checking where each power R^i takes 1 we see immediately that $1 \neq R \neq R^2 \neq \ldots \neq R^{n-1}$, $R^n = 1$. In this way, the powers of R look remarkably like $\mathbb{Z}/n\mathbb{Z}$. It's also easy to show that $S \neq S^2 = 1$. The element S flips the cyclic orientation of the n-gon from clockwise to counter clockwise, and vice-versa. This means that $S \neq R^i$ for any i, because the rotation R preserves this orientation. We can also see that $S \neq SR^i$ for any $1 \leq i < n$ because 1 is fixed by S, but not by SR^i. Since D_{2n} is a group we also get that $SR^i \neq SR^j$ for any $1 \leq i \neq j < n$ (just divide both sides by the smaller power). We conclude that:

$$D_{2n} = \{1, R, \ldots, R^{n-1}, S, SR, \ldots, SR^{n-1}\}. \tag{1}$$

Exercise 0.14. *Check that $RS = SR^{-1}$ for any i. Conclude that D_{2n} is not commutative, and also that $R^i S = SR^{-i}$ for any i.*

We have found a "presentation" of D_{2n} by generators and relations:

$$D_{2n} = \langle R, S \mid R^n = S^2 = 1, RS = SR^{-1} \rangle. \tag{2}$$

Exercise 0.15. *Assuming only the relations in the equation above, show that any product of R, S can be reduced to R^i or SR^i for some i.*

Week 3

Let's return to the symmetric group S_n. The proof that D_{2n} has order $2n$ followed a useful strategy: we used the realization of a group as a set of symmetries of some object to capture the behavior of the group itself. This idea also helps us evaluate the order of S_n.

How can we construct a permutation $\sigma \in S_n$? We must first choose the index i_1 where σ sends 1; there are n such choices. The element σ is a bijection on $[n]$, so after we've chosen $i_1 = \sigma(1)$, we must choose $i_2 = \sigma(2)$ from the set $[n] \setminus \{i_1\}$ to ensure that 1 and 2 are not sent to the same element; there are $n-1$ such choices. Continuing this way, we choose i_j from the set $[n] \setminus \{i_1, \ldots, i_{j-1}\}$, which has order $n-j+1$. We conclude that $|S_n| = n \times (n-1) \times (n-2) \cdots 2 \times 1 = n!$.

We've seen how to represent elements of S_n with wiring diagrams and the permutation matrices P_σ, both of these make important properties of permutations more accessible. In particular, we've seen been introduced to the sign $sgn(\sigma)$ of a permutation as $det(P_\sigma)$, and we've seen that it's (-1) taken to the power of the number of "swap" matrices needed to make P_σ. Now we'll learn a third way to represent permutations.

A "cycle" is a permutation which cyclically permutes some subset of $[n]$ and leaves the rest of the set fixed. For example, the permutation $\sigma \in S_3$ such that $\sigma(1) = 2$, $\sigma(2) = 3$ and $\sigma(3) = 1$ is a cycle; you can see the wiring diagram of this element on the right hand side of Figure 0.8. We represent σ by writing (123). In general, if $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{m-1}) = a_m$ and $\sigma(b) = b$ for any $b \in [n] \setminus \{a_1, \ldots, a_m\}$, then we represent σ by writing $(a_1 a_2 \cdots a_m)$. We'll say that two cycles $(a_1 \cdots a_m)$, $(b_1 \cdots b_k)$ are disjoint if they don't share any indices. Any element of S_n can be written as a product of disjoint cycles.

- Start with the smallest element a you haven't considered yet (ie 1). If $\sigma^k(a) = a$ we write $(a\sigma(a)\sigma^2(a) \cdots \sigma^{k-1}(a))$.
- Find the smallest element not appearing yet, and repeat the previous step. Write the cycle you obtain to the left of the previous cycle.
- Eliminate all cycles of length 1.

Exercise 0.16. *Find the cycle decomposition of the identity element.*

Finding the inverse of a permutation from its cycle decomposition is easy: simply reverse the order of the numbers in each cycle!

$$[(132)(5698)]^{-1} = (231)(8965). \tag{3}$$

Finding the cycle decomposition of a composition of two permutations also isn't so bad. Remember that when we compose two permutations $\sigma \circ \tau$ we think of the resulting bijection's action on $[n]$ as going from right to left. So in order to compute $\sigma \circ \tau(i)$ we first compute $\tau(i)$, then we plug the result into σ. In terms of cycle decompositions, this means that we find i in the decomposition of τ, we find the element "to the right" of i, namely $\tau(i)$ (remember that "to the right" is read cyclically, if i appears at the end of a cycle, we wrap back around to the beginning), then we find the element "to the right" of $\tau(i)$ in the cycle decomposition of σ. This is $\sigma(\tau(i))$. Proceeding this way through the algorithm above results in the cycle decomposition of $\sigma \circ \tau$.

Let's compute $\sigma \circ \tau$ when $\sigma = (132)(45)$ and $\tau = (5312)$.

$$\sigma \circ \tau = (132)(45)(5312) \tag{4}$$

Starting with 1, we see that $\tau(1) = 2$ and $\sigma(2) = 1$, so we begin by writing (1). For 2, we see that $\tau(2) = 5$, $\sigma(5) = 4$, so we can write (24.... Next, $\tau(4) = 4$ and $\sigma(4) = 5$, so our cycle grows to (245.... Now, $\tau(5) = 3$ and $\sigma(3) = 2$, this is where we started so we can close the cycle off to get (1)(245). It remains to see what happened to 3. We have $\tau(3) = 1$ and $\sigma(1) = 3$, so we're finished: $\sigma \circ \tau = (1)(245)(3) = (245)$.

The fact that "any wiring diagram can be expressed as a product of swaps" has useful ramifications for permutations. In the language of cycle decomposition it means that "any cycle can be expressed as a (non-disjoint) product of 2−cycles." We can see how this works immediately by verifying the following equation in cycles:

$$(a_1 \dots a_m) = (a_1 a_2)(a_2 a_3) \cdots (a_{m-1} a_m). \tag{5}$$

Likewise we can decompose any 2-cycle into a product of special 2−cycles. Let $s_i = (i, i+1)$, then we can write:

$$(i, i+j) = s_i(i+1, i+j)s_i. \tag{6}$$

An induction argument then allows us to express $(i, i+j)$ as a product of the s_i. This shows that S_n can be generated by the $n-1$ elements $s_1, \dots, s_{n-1}$; it turns out there is a very efficient set of relations among these generators which give a presentation of S_n. The following are the

relations of the Coxeter presentation:

- $s_i^2 = 1$
- $s_i s_j = s_j s_i$, $i \neq i \pm 1$
- $(s_i s_{i+1})^3 = 1$.

Exercise 0.17. *Verify that the Coxeter relations hold among $s_i \in S_n$.*

We'll finish off this week by formally defining the notion of group homomorphism. We've seen plenty of these already, there is a homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which sends a number a to its equivalence class modulo n. There is also a group homomorphisms $S_n \to GL_n(\mathbb{K})$ sending σ to P_σ.

Definition 0.9. *Let H and G be groups, and let $\phi : H \to G$ be a map of sets, then ϕ is said to be a group homomorphism if $\phi(h_1 h_2) = \phi(h_1)\phi(h_2)$.*

Notice in this definition that the product on the left is computed in H and the product on the right is computed in G. Roughly speaking, ϕ preserves the structure of the groups H and G.

Exercise 0.18. *Verify that $\phi(1_H) = 1_G$ and that $\phi(h^{-1}) = \phi(h)^{-1}$.*

A homomorphism $\phi : H \to G$ is called an "isomorphism" if ϕ is a bijection of sets. In this case H and G are said to be *isomorphic* as groups.

Exercise 0.19. *Show that if $\phi : H \to G$ is an isomorphism then $\phi^{-1} : G \to H$ is also an isomorphism.*

We've seen with D_{2n} and S_n that the structure of a group can be revealed by realizing it as the group of symmetries of some object. Let X be a set and G be a group. A *group action* is a map $a : G \times X \to X$; we usually write $a(g, x)$ as $g \circ x \in X$. Two properties are required:

(1) $1_G \circ x = x$,

(2) $g_1 \circ (g_2 \circ x) = (g_1 g_2) \circ x$.

In particular, each $g \in G$ defines a set map $\sigma_g : X \to X$, where $\sigma_g(x) = g \circ x$. Property (2) above immediately implies that $\sigma_{g_1 g_2} =$

$\sigma_{g_1}\sigma_{g_2}$. Furthermore, $\sigma_{1_G} = \sigma_g\sigma_{g^{-1}}$ so we can conclude that each σ_g is a *permutation* of X. It follows that we have a group homomorphism $\phi_a : G \to S_X$, $\phi_a(g) = \sigma_g$, where S_X is the group of permutations of the set X.

Exercise 0.20. *Let $|X| = n$, and suppose that X has a group action by G, conclude that there is a group homomorphism from G to $GL_n(\mathbb{C})$.*

Week 4

For any homomorphism $\phi : H \to G$ we can consider the kernel $Ker(\phi) \subset H$; this is the set of elements in H which are mapped to 1_G by ϕ. Think of this as a direct generalization of the kernel of a linear map in linear algebra. Let's verify some properties of the kernel:

- $1_H \in Ker(\phi)$,
- if $h_1, h_2 \in Ker(\phi)$ then $\phi(h_1h_2) = \phi(h_1)\phi(h_2) = 1_G1_G = 1_G$, so $h_1h_2 \in Ker(\phi)$,
- if $h \in Ker(\phi)$ then $\phi(h^{-1}) = \phi(h)^{-1} = (1_G)^{-1} = 1_G$.

We can conclude that $Ker(\phi)$ is itself a group with respect to the group operation in H. Just like in linear algebra, kernels are a useful instrument to measure properties of the homomorphism ϕ.

Proposition 0.10. *A homomorphism $\phi : H \to G$ is an injection if and only if $Ker(\phi) = \{1_H\}$.*

Proof. Suppose that $Ker(\phi) = \{1_H\}$, then if $\phi(h_1) = \phi(h_2)$, we must have $\phi(h_1h_2^{-1}) = \phi(h_1)\phi(h_2)^{-1} = \phi(h_1)\phi(h_1)^{-1} = 1_G$, so $h_1h_2^{-1} \in Ker(\phi)$. But then $h_1h_2^{-1} = 1_H$, so $h_1 = h_2$. If on the other hand, ϕ is a bijection, then if $\phi(h) = 1_G = \phi(1_H)$, we must have $h = 1_H$. □

0.4. **Groups acting on themselves.** If we consider a group action $a : G \times X \to X$, then we call the kernel $Ker(\phi_a)$ of the corresponding homomorphism $\phi_a : G \to S_X$ the kernel of the group action. These are all of the elements which "do nothing," ie they are the $g \in G$ for which $\sigma_g : X \to X$ is the identity map on X. Group actions are useful because they give us a way to view an abstract group G as something more familiar: a set of permutations or a set of matrices. This suggests a natural question: Give a finite group G, is it always possible to find an action $a : G \times X \to X$ for which ϕ_a is a bijection? In other words, can we view any finite group as a set of matrices or a set of permutations? The answer is yes, and the actions which do the trick are defined next.

Definition 0.11. *We'll define some group actions of G on itself, or rather the underlying set $\mathbf{G}$ of G:*

- *The LEFT action $a_L : G \times \mathbf{G} \to \mathbf{G}$ is $a_L(g, \mathbf{h}) = g\mathbf{h}$,*

- *The RIGHT action* $a_R : G \times \mathbf{G} \to \mathbf{G}$ *is* $a_R(g, \mathbf{h}) = \mathbf{h}g^{-1}$,
- *The CONJUGATION action* $a_C : G \times \mathbf{G} \to \mathbf{G}$ *is* $a_C(g, \mathbf{h}) = g\mathbf{h}g^{-1}$.

Proposition 0.10 makes it easy to verify that ϕ_{a_L} is an injection. If $g \in Ker(\phi_{a_L})$ then $\sigma_{a_L,g} : \mathbf{G} \to \mathbf{G}$ is the identity map. But by definition $\sigma_{a_L,g}(1_G) = g$, so we must have $g = 1_G$.

Exercise 0.21. *Verify the the right action* a_R *also has* $Ker(\phi_{a_R}) = \{1_G\}$*, so* ϕ_{a_R} *is an injection.*

The homomorphism $P_- \circ \phi_{a_L} : G \to GL_{|G|}(\mathbb{C})$ obtained by composing the map ϕ_{a_L} with the representation of the symmetric group by permutation matrices is also an injection; this map is referred to as the *Cayley representation* of G.

Homomorphisms are very useful for studying groups, so it makes sense to go ahead and utilize a similar class of maps for group actions.

Definition 0.12. *Let* X *and* Y *be equipped with group actions by a group* G*. We say that a map of sets* $\psi : X \to Y$ *intertwines the actions of* G *on* X *and* Y *if* $\psi(g \circ x) = g \circ \psi(x)$ *for any* $x \in X$*.*

Going with the linear algebra analogy, we can think of an intertwiner $\psi : X \to Y$ as something like a map of vector spaces, where G plays the role of the scalars.

Exercise 0.22. *Let* G *be a group with underlying set* $\mathbf{G}$*, and let* $i : \mathbf{G} \to \mathbf{G}$ *be the map* $i(\mathbf{g}) = \mathbf{g}^{-1}$*. Verify that* i *intertwines the left* a_L *and right* a_R *actions of* G *on* $\mathbf{G}$*.*

0.5. **Subgroups.** A group homomorphism $\phi : H \to G$ is something like a snapshot of H. We see a blurry image of H inside G which perhaps forgets some information. If we're lucky and the kernel is trivial, this snapshot is very accurate and we can view H as a part of the group G. We say then that H is isomorphic to a *subgroup* of G. If homomorphisms are like images of a group, then subgroups are like helpful spies that work from the inside to tell us how the group is put together.

Proposition 0.13. *A subset* $H \subseteq G$ *is a subgroup if and only if for any* $h_1, h_2 \in H$ *we have* $h_1 h_2^{-1} \in H$ *as well.*

Exercise 0.23. *Verify that if the conditions of Proposition 0.13 hold for* $H \subseteq G$ *then* H *is a group when considered with the group operation coming from* G*.*

Let's have a look at the subgroups of the cyclic groups $\mathbb{Z}/n\mathbb{Z}$. For any $d \mid n$ we can define a surjective homomorphism $\phi_{d,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ by sending $1 \in \mathbb{Z}/n\mathbb{Z}$ to $1 \in \mathbb{Z}/d\mathbb{Z}$. The kernel $Ker(\phi_{d,n})$ is generated by the equivalence class of d in $\mathbb{Z}/n\mathbb{Z}$. Since d has order $\frac{n}{d}$, we see that we've found an isomorphic copy of $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$ inside of $\mathbb{Z}/n\mathbb{Z}$. In fact, as we'll see now, the kernels $Ker(\phi_{d,n})$ are all the subgroups of $\mathbb{Z}/n\mathbb{Z}$.

Proposition 0.14. *Suppose $A \subset \mathbb{Z}/n\mathbb{Z}$ is a subgroup, then A is the cyclic group $\langle a \rangle$ generated by some equivalence class $a \in \mathbb{Z}/n\mathbb{Z}$. Furthermore, $\langle a \rangle = \langle GCD(a, n) \rangle$.*

Proof. We can assume that the subgroup A contains some non-zero element; so let $1 \geq a < n$ be the smallest integer representing an element of A. Clearly $\langle a \rangle \subseteq A$, so we need to show the reverse inclusion. Let $1 \geq b < n$ represent some other non-zero element of A, then $b > a$, so we can divide: $b = qa + r$, with $r < a$. Since the equivalence classes of both qa and b are in A, r must represent an element of A as well. But a was assumed to be the smallest such number, so $r = 0$ and $qa = b$. It follows that every element of A is generated by the equivalence class of a.

Suppose the equivalence class of b (with $1 \geq b < n$) is in $\langle a \rangle$, then $n \mid (b - qa)$, so $n \mid (b - q'GCD(a, n))$ for some q, q', since $GCD(a, n) \mid a$. It follows that $\langle a \rangle \subseteq \langle GCD(a, n) \rangle$. On the other hand, we can write $GCD(a, n) = sa + tn$ for integers s, t. It follows that $GCD(a, n)$ is a multiple of a modulo n, so $\langle GCD(a, n) \rangle \subseteq \langle a \rangle$. □

As a consequence of Proposition 0.14, we can see the order of the equivalence class a in $\mathbb{Z}/n\mathbb{Z}$ is the same as the order of $GCD(a, n)$. Since $GCD(a, n) \mid n$, this is $\frac{n}{GCD(a,n)}$.

Now we will define a few natural subgroups associated to subsets of a group G and group actions. Let G be a group, let $A \subset G$ be some non-empty subset, and let $a : G \times X \to X$ be a group action.

- for $x \in X$, the stabilizer $G_x \subset G$ is $\{g \mid g \circ x = x\}$,
- the centrilizer $C_G(A)$ is the set $\{g \mid gag^{-1} = a \forall a \in A\}$, notice that this is the intersection of the stabilizers $G_a \subset G$ of the elements in A under the conjugation action of G on itself,
- the center $Z(G) \subset G$ is $C_G(G)$,

- define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$, the normalizer $N_G(A)$ is the set $\{g \mid gAg^{-1} = A\}$.

Exercise 0.24. *Show that each set defined above is actually a subgroup of G.*

We've defined subgroups of a group G by taking the kernels of homomorphisms, and by properties extracted from group actions. These are "implicit" ways of defining a subgroup: we have defined the subgroup according to how it behaves or what it does. We can also "parametrically" define subgroups. We've done this already by considering the cyclic groups $\{g^i \mid 0 \leq i\} =< g >\subseteq G$ generated by elements of a group. We need one fact about subgroups to make things precise.

Proposition 0.15. *Let I be some index set, and $H_i \subset G$ be a subgroup for $i \in I$, then $\bigcap_{i\in I} H_i \subset G$ is also a subgroup.*

Proof. For any $g, h \in \bigcap_{i\in I} H_i$ we know that $gh^{-1} \in H_i \ \forall i \in I$. It follows that $gh^{-1} \in \bigcap_{i\in I} H_i$. □

Now for any subset $A \subset G$ we can talk about the subgroup generated by A.

Definition 0.16. *For a non-empty subset $A \subset G$ we let $\langle A\rangle \subset G$ be the smallest subgroup of G containing A. In particular $\langle A\rangle$ is the intersection of all subgroups of G which contain A.*

The following proposition describes $\langle A\rangle$ in a different way.

Proposition 0.17. *As a set, $\langle A\rangle \subset G$ is the set $W(A)$ of all products $a_1^{n_1} \cdots a_k^{n_k}$ where $a_i \in A$ and $n_i \in \mathbb{Z}$.*

Proof. It is clear that $a_1^{n_1} \cdots a_k^{n_k} \in H$ for any subgroup H which contains A, so $W(A) \subseteq \langle A\rangle$. On the other hand if $g = a_1^{n_1} \cdots a_k^{n_k}$ and $h = b_1^{m_1} \cdots b_\ell^{m_\ell}$ then $gh^{-1} = a_1^{n_1} \cdots a_k^{n_k} b_\ell^{-m_\ell} \cdots b_1^{-m_1}$ (socks and shoes!), which is clearly also in $W(A)$. This shows that $W(A)$ is itself a subgroup which contains A, so we must have $\langle A\rangle \subseteq W(A)$. □

Now given any two subgroups $H_1, H_2 \subseteq G$ we can form the smallest subgroup which contains them $\langle H_1 \cup H_2\rangle \subset G$ and the largest subgroup contained in them $H_1 \cap H_2$. This makes the collection of subgroups of G into a *lattice*.

Week 5

0.6. **Lattice of subgroups.** We say a poset P is a *lattice* if for any pair of elements a, b we can find a least upper bounded $a \vee b \in P$ and a greatest lower bound $a \wedge b \in P$. For a group G we can consider the poset of subgroups $P(G)$, where the partial order relation is given by inclusion. If $H, K \subset G$ are two subgroups, we've seen that $H \cap K$ and $\langle H, K \rangle$ are the greatest lower bound, and least upper bound by inclusions. We can therefore refer to the lattice of subgroups $P(G)$ of a group. We'll take some time to describe this lattice for cyclic groups.

Proposition 0.18. *Let C be a cyclic group ($\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some n), then any subgroup $A \subset C$ is also cyclic.*

Proof. The subgroup A is a subset of C, which we can think of as being indexed by a set of numbers (all integers, or $1, \ldots, n$). We consider the set of elements $A_+ \subset A$ with positive index ($A \cap Z_{>0}$ or A itself, respectively). Notice that this set is always non-empty since A is closed under applying a minus sign. Let $a \in A_+$ be the *least* element of this set. Now, if $b \in A_+$, we can divide b by a:

$$b = qa + r, \tag{7}$$

where $0 \leq r < a$. Now we must have $r = b - qa \in A$, so r must be 0, else a was not the least member of A_+. It follows that b is in the cyclic group generated by a. Now any member of A is either in A_+ or is $-b = -qa$ for some $b \in A_+$, so $A = \langle a \rangle \subset C$. □

By definition, for any $a, b \in C$ we have $\langle a \rangle \subseteq \langle b \rangle$ if and only if $b \mid a$. From Proposition 0.14, we know that every subgroup of $\mathbb{Z}/n\mathbb{Z}$ is of the form $\langle d \rangle$ for some d which divides n. This means that the lattice $P(\mathbb{Z}/n\mathbb{Z})$ is just the lattice of divisors of n upside down.

0.7. **Quotients.** When we formed $\mathbb{Z}/n\mathbb{Z}$ we did so by defining an equivalence relation on $\mathbb{Z}$ using the subgroup $\langle n \rangle = n\mathbb{Z}$. It makes sense to wonder if something like this works for any subgroup H of a group G.

Definition 0.19. *Let $H \subset G$ be a subgroup. We define an equivalence relation $\sim_H$ on G as follows:*

$$u \sim_H v \quad \leftrightarrow \quad v^{-1}u \in H. \tag{8}$$

Let's check that this is actually an equivalence relation. If $u \in G$ then clearly $u^{-1}u = 1_G \in H$, so $u \sim_H u$. If $u \sim_H v$ then $v^{-1}u \in H$,

so since H is a subgroup $(v^{-1}u)^{-1} = u^{-1}v \in H$, and $v \sim_H u$. Finally, if $u \sim_H v$ and $v \sim_H w$ then $w^{-1}u = (w^{-1}v)(v^{-1}u) \in H$, since H is a subgroup, so $u \sim_H w$.

The equivalence classes of $\sim_H$ are called cosets.

Definition 0.20. *For $g \in G$ and $H \subset G$, the left coset gH is $\{gh \mid h \in H\}$.*

Proposition 0.21. *For $u, v \in G$, $u \sim_H v$ if and only if $uH = vH$.*

Exercise 0.25. *Prove the proposition above.*

We let G/H denote the set of left cosets of H in G, or equivalently the set obtained from G from the equivalence relation $\sim_H$. We can see from the definition that $h \in H$ if and only if $hH = H$. Also, the set G/H carries a natural action by the group G: $g \circ kH = (gk)H$.

Theorem 2 (Lagrange's theorem)**.** *If G is a finite group and $H \subset G$ is a subgroup then $|H|$ divides $|G|$, and the number of left H cosets in G is $\frac{|G|}{|H|}$.*

Proof. We'll show that all the cosets gH have the same size, which in turn implies that they are all size $|H|$. Fix gH, and define a map $\sigma_g : H \to gH$ by $\sigma_g(h) = gh$. This map is onto by definition of gH, and if $gh_1 = gh_2$ we can divide by g on the left to conclude that $h_1 = h_2$, so it is also $1 - 1$. Since cosets are equivalence classes, they are disjoint, it follows that $|G| =$ The Number Of Cosets $\times |H| = |G/H| \times |H|$. □

The number of left cosets is called the index $|G : H|$, if G is infinite this might still be finite, for example $\mathbb{Z}/n\mathbb{Z}$.

Corollary 0.22. *If G is a finite group, and $g \in G$ then $|g|$ divides $|G|$.*

0.8. **Normal subgroups.** The quotient $\mathbb{Z}/n\mathbb{Z}$ is much more than a set, it's a group! Does the same thing work for G/H? Put another way, is there a product we can place on G/H that turns it into a group? If we're going to use $\mathbb{Z}/n\mathbb{Z}$ as a model, here is a natural candidate:

$$g_1H \circ g_2H = g_1g_2H. \tag{9}$$

It seems pretty apparent that this operation inherits the nice properties of the product in G, like associativity and inverses, so what could go wrong? We have yet to verify that this map is even well-defined. That is, if we pick two different representatives $g_1' \sim_H g_1, g_2' \sim_H g_2$, is it still the case that $g_1'g_2' \sim_H g_1g_2$?

Let's look at a restricted class of subgroups. Let $\phi : G \to H$ be a homomorphism, and $K = Ker(\phi)$ be its kernel. Suppose that $u \sim_H a, v \sim_H b$, does it follow that $uv \sim_H ab$? To check this, we need $(ab)^{-1}(uv)$ to be a member of K. We can simplify a little bit: $(ab)^{-1}(uv) = b^{-1}a^{-1}uv$. We know that $a^{-1}u \in K$ and $b^{-1}v \in K$, but $a^{-1}u$ is stuck there in between b^{-1} and v (notice we'd be done if G were Abelian!). We haven't used the fact that K is a kernel yet, so let's apply the homomorphism:

$$\phi(b^{-1}a^{-1}uv) = \phi(b^{-1})\phi(a^{-1}u)\phi(v) = \tag{10}$$

$$\phi(b^{-1})1_G\phi(v) = \phi(b^{-1}v) = 1_G.$$

So we get that $(ab)^{-1}(uv) = b^{-1}a^{-1}uv \in Ker(\phi) = K$. As a consequence it makes sense to define $aK \circ bK = abK$, since we'll get the same answer regardless of which elements of aK and bK we use. This allows us to define a group structure on G/K. This property of K is closely related to the fact that it is a special kind of subgroup.

Definition 0.23. *We say a subgroup $N \subset G$ is a normal subgroup (denoted $N \trianglelefteq G$) if for any $g \in G$ and $n \in N$ we have $gng^{-1} \in N$.*

If K is the kernel of $\phi : G \to H$, and $k \in K$, then for any $g \in G$ we have $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1_H$. This is a good time to mention:

Theorem 3 (First isomorphism theorem)**.** *If $\phi : G \to H$ is a homomorphism, then ϕ is injective if and only if $Ker(\phi) = \{1_G\}$, $Ker(\phi) \trianglelefteq G$,and $G/Ker(\phi) \cong \phi(G)$.*

Proof. Let $K = Ker(\phi)$ as above. We need to verify that the map $\hat{\phi} : G/K \to \phi(G)$ sending gK to $\phi(g)$ is awell-defined, onto, and $1-1$ group homomorphism. If $u \sim_K v$ then $v^{-1}u \in K$ so $\phi(v^{-1}u) = 1_H$. In turn we get (check!) that $\phi(v) = \phi(u)$, so $\hat{\phi}$ is well-defined. The map $\hat{\phi}$ is onto by definition - just observe that any element of G is in some K coset (so we could use that element to represent the coset under $\hat{\phi}$ by the fact that $\hat{\phi}$ is well-defined), and any element of $\phi(G)$ is the image of an element from G by definition. For $a, b \in G$, $\hat{\phi}(aK \circ bK) = \hat{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \hat{\phi}(aK)\hat{\phi}(bK)$, so $\hat{\phi}$ is also a group homomorphism. To show it is $1-1$ (and therefore an isomorphism), note that if $\hat{\phi}(aK) = \hat{\phi}(bK)$ then $\phi(a) = \phi(b)$, so $b^{-1}a \in K$ and $a \sim_K b$.

We've shown $G/K \cong \phi(G)$, and it follows that G is $1-1$ if and only if $K = \{1_G\}$. We already saw above that $K \trianglelefteq G$. $\square$

Kernels are normal subgroups, so it follows that any subgroup which is not normal cannot be the kernel of a homomorphism.

Exercise 0.26. *Find all of the normal subgroups of S_3. What's the deal with S_4?*

Now we can ask about the converse statement to (part of) the First Isomorphism Theorem: is every normal subgroup the kernel of some homomorphism? The answer will turn out to be *yes*. We'll show this by first showing that the natural product on G/N is well-defined if and only if $N \trianglelefteq G$, extending the case of kernels that we discussed above. Then we can consider the surjection $G \to G/N$, which has kernel N since $gN = N$ if and only if $g \in N$.

Proposition 0.24. *The natural product on G/N is well-defined if and only if $N \trianglelefteq G$.*

Proof. We first assume that $N \trianglelefteq G$. We must show that if $u \sim_N a$ and $v \sim_N b$ then $uv \sim_N ab$. We have $uv \sim_N ab$ if and only if $(ab)^{-1}uv \in N$, so let's compute $(ab)^{-1}uv = b^{-1}a^{-1}uv = b^{-1}(a^{-1}u)b(b^{-1}v)$. We know that $a^{-1}u, b^{-1}v \in N$, and since N is normal $b^{-1}(a^{-1}u)b \in N$. This shows that the product is well-defined.

Now suppose that the product is well-defined, then since $1_G \sim_N n^{-1}$ for any $n \in N$, and $g^{-1} \sim_N g^{-1}$ for any $g \in G$, we conclude that $1_G g^{-1}N = n^{-1}g^{-1}N$. But this means that $gng^{-1} = (n^{-1}g^{-1})^{-1}g^{-1} \in N$. Since n and g were arbitrary, N must be normal. $\square$

Corollary 0.25. *If N is normal, then N is the kernel of a homomorphism: $G \to G/N$.*

Week 6

0.9. **Other isomorphism theorems.** For subgroups $A, B \subseteq G$ we can form $\langle A, B\rangle \subset G$, the smallest subgroup containing A, B. Now we'll see that when a few additional assumptions hold, the underlying set of this group has particularly nice description. Taking a step back, we'll first consider the following *subset* of G associated to A and B:

Definition 0.26. *For subgroups $A, B \subseteq G$ we let $AB = \{ab \mid a \in A, b \in B\}$.*

Example 0.27. *Consider $n\mathbb{Z}, m\mathbb{Z} \subset \mathbb{Z}$, what is $n\mathbb{Z} + m\mathbb{Z}$? Put into words, this is the set of all integers which can be represented as $nA+mB$ for some $A, B \in \mathbb{Z}$. Let's first check that this is a subgroup of $\mathbb{Z}$. Clearly if $r = nA+mB$ and $s = nC+mD$ then $r-s = nA+mB-mD-nC = n(A-C)+m(B-D)$, so $n\mathbb{Z}+m\mathbb{Z}$ satisfies our one-step subgroup check. It follows that $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$, since all subgroups of cyclic groups are cyclic. Any element of this subgroup is divisible by $GCD(n, m)$, and we know that $GCD(n, m) = nK + mL$ for some $K, L \in \mathbb{Z}$. It follows that $m\mathbb{Z} + n\mathbb{Z} = GCD(n, m)\mathbb{Z}$.*

Example 0.28. *Consider $\langle(12)\rangle, \langle(23)\rangle \subset S_3$:*

$$\langle(12)\rangle\langle(23)\rangle = \{1, (12), (23), (123)\}. \tag{11}$$

This set does not contain (132)*, ie the inverse of* (123)*, so it cannot be a subgroup of S_3.*

The two examples above show that we have to be careful AB because it is not always a subgroup of G. In particular, in the first example we used the commutativity of $+$ in $\mathbb{Z}$ to conclude that $nA + mB - mD - nC = n(A - C) + m(B - D)$ which showed that $n\mathbb{Z} + m\mathbb{Z}$ satisfied the subgroup criterion. Even without this commutativity we still get the following counting formula which serves as a generalization of Lagrange's Theorem, and a preview of the Second Isomorphism Theorem.

Proposition 0.29. *Let $A, B \subseteq G$, where G is finite, then we have the following counting formula:*

$$|AB| = \frac{|A||B|}{|A \cap B|} \tag{12}$$

Proof. The set AB is a union of left cosets aB, where $a \in A$; if we can count the number of distinct cosets of this form, we can prove the result. Let's check: $a_1B = a_2B$ if and only if $a_2^{-1}a_1 \in B$. Since $a_1, a_2 \in A$, this happens if and only if $a_2^{-1}a_1 \in A \cap B$, which in turn holds if and only if $a_1A \cap B = a_2A \cap B$ as $A \cap B$ cosets in A. It follows from Lagrange's theorem that there are $\frac{|A|}{|A \cap B|}$ of these, and each has size $|B|$. □

Now we can give a condition that implies AB is a group.

Proposition 0.30. *The set AB is a group if and only if $AB = BA$ as sets (note: this does NOT mean that their elements commute!).*

Proof. Suppose that $AB = BA$, then for $g = a_1b_1, h = a_2b_2$ we can compute $gh^{-1} = a_1b_1b_2^{-1}a_2^{-1}$. Since $AB = BA$ we can write $b_1b_2^{-1}a_2^{-1} = a_3b_3$ for some $a_3 \in A$, $b_3 \in B$, so $gh^{-1} = a_1a_2b_3 \in AB$. It follows that AB is a group by our subgroup criterion.

Now suppose that AB is a subgroup of G. Since $A, B \subset AB$ we must have $BA \subset AB$. Now if $ab \in AB$ then it is the inverse of some other $a_0b_0 \in AB$, so $ab = (a_0b_0)^{-1} = b_0^{-1}a_0^{-1} \in BA$. □

As corollary we see that if $A \subseteq N_G(B)$ then AB is a subgroup of G. In particular, if $B \trianglelefteq G$ then AB is a subgroup for all subroups $A \subseteq G$. If $AB = BA$ then AB is a subgroup of G which contains both A and B, so it follows that $\langle A, B\rangle \subset AB$ by definition. However, in Proposition 0.17 we also saw that $\langle A, B\rangle$ is the set $W(A \cup B)$ of all "words" that we can make using the product operation and elements from A, B. Clearly $AB = \{ab \mid a \in A, b \in B\} \subset W(A \cup B) = \langle A, B\rangle$, so we have $\langle A, B\rangle = AB$ if $AB = BA$ or equivalently, if AB is a group.

Exercise 0.27. *Show that if $N_1, N_2 \trianglelefteq G$ then $N_1N_2 = \langle N_1, N_2\rangle \trianglelefteq G$ and $N_1 \cap N_2 \trianglelefteq G$.*

Now we'll finish with the Second and Third Isomorphism theorems. The proofs of these theorems are straightforward applications of material we've already seen.

Theorem 4 (Second isomorphism theorem)**.** *Let $A, B \subset G$ be subgroups, and suppose that $A \subseteq N_G(B)$, then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A/A \cap B$.*

Proof. We've seen that AB is a subgroup. Now we have $B \subseteq N_G(B)$ for free and $A \subseteq N_G(B)$ by assumption, so $AB \subseteq N_G(B)$, so $B \trianglelefteq AB$. This implies that AB/B is a group, and there is a surjective homomorphism $\phi : AB \to AB/B$ with kernel B. The kernel of the restriction of this map to $A \subset AB$ is the set of cosets of the form $aB = 1_GB$,

in other words elements $a \in A$ which are also in B: $A \cap B$. Since $A \cap B = Ker(\phi\mid_A)$, $A \cap B \trianglelefteq A$. But any element in the image of ϕ can be written as $\phi(a)$ for some $a \in A$; it follows that $A/A\cap B \cong AB/B$. $\square$

Theorem 5 (Third isomorphism theorem)**.** *Let $H, K \trianglelefteq G$ with $H \subseteq K$, then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.*

Proof. It is straightforward to check $K/H \trianglelefteq G/H$. Let $\phi : G/H \to G/K$ be the map that takes gH to gK for $g \in G$. Note that if $g_1K = g_2K$ then we must have $g_2^{-1}g_1 \in K \subseteq H$, so this map is well-defined. We also see immediately that ϕ is surjective. The kernel of ϕ are gH such that $gK = 1_GK$, so $g \in K$, and $gH \in K/H$. $\square$

We've been implicitly discussing a basic sort of problem in algebra. When we have a homomorphism $\phi : G \to H$, and a quotient map $\pi : G \to G/N$, when can we lift ϕ to a homomorphism $\hat{\phi} : G/N \to H$ (see Figure 0.9)?

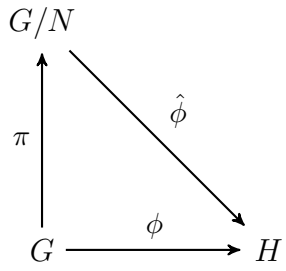

FIGURE 4. Lift of the map $\phi : G \to H$.

The answer is that this can be done if and only if $N \subset Ker(\phi)$.

0.10. **Group Actions Again.** Let $a : G \times X \to X$ be a group action. This structure induces an equivalence relation on X, where $x \sim_a y$ if and only if $x = g \circ_a y$ for some $g \in G$.

Exercise 0.28. *Check that $\sim_a$ is actually an equivalence relation.*

Equivalence classes under $\sim_a$ are called *orbits* of the group action. We let $\mathcal{O}_x$ denote the orbit containing $x \in X$; put more plainly, the elements in $\mathcal{O}_x$ are the elements of X that x can get to using the elements of G. Notice that each orbit $\mathcal{O}_x$ is itself a set equipped with a G-action. We say that the action a is *transitive* if X is itself an orbit. In this way, any "complicated" G-set X can be decomposed into a disjoint union of sets with transitive G-actions, in particular $|X|$ is a sum of orders of orbits $|\mathcal{O}_x|$.

Example 0.31. *For any subgroup $H \subset G$, there is a group action on the set of left cosets G/H by left multiplication. This action is transitive, since $gH = g(1_G H)$ for any $g \in G$.*

For any $x \in X$ as above, we can look at the collection of elements $G_x \subset G$ which don't do anything to x; this is called the stabilizer. We can check that if $g(x) = x$ and $h(x) = x$ then $gh^1(x) = x$, so G_x is always a subgroup of G.

Example 0.32. *The stabilizer of $1_G H \in G/H$ is the set of elements in G which left translate $1_G H$ to itself, in other words: $gH = H$. This happens if and only if $g \in H$, so $G_{1_G H} = H$.*

Our example of the quotient set G/H turns out to be much of the story of what's going on with general group actions. This is the content of the orbit-stabilizer theorem.

Theorem 6. *[Orbit-Stabilizer theorem] Let $a : G \times X \to X$ be a group action, with $x \in X$, then there is an isomorphism of sets equipped with G actions:*

$$\mathcal{O}_x \cong G/G_x. \tag{13}$$

In particular, if G is finite then $|G| = |\mathcal{O}_x||G_x|$.

Proof. We define a map $\psi : G/G_x \to \mathcal{O}_x$ by $\psi(gG_x) = g \circ_a x$. First we check that this map is well-defined. If $h^{-1}g \in G_x$ then $x = h^{-1}g \circ_a x = h^{-1}(g \circ_a x)$, so $h \circ_a x = g \circ_a x$. We also immediately get that this map is onto, since any element in $\mathcal{O}_x$ is of the form $g \circ_a x = \psi(gG_x)$. As defined, this map also respects the G-actions on both sides since $\psi(g \circ (hG_x)) = \psi((gh) \circ G_x) = gh \circ_a x = g \circ_a (h \circ_a x) = g \circ_a (\psi(hG_x))$. It remains to see that ψ is $1-1$. If $\psi(gG_x) = \psi(hG_x)$ then $g \circ_a x = h \circ_a x$, so $h^{-1}g \circ_a x = x$, and $h^{-1}g \in G_x$. □

The distinction between normal and other subgroups suggests that only the normal subgroups are useful. This is wrong. Theorem 6 is nice because it suggests a use for non-normal subgroups of G: they are the stabilizers of elements under group actions. Furthermore, for each subgroup $H \subseteq G$ we get a realization of $\pi_H : G \to S_{G/H}$ as a set of permutations on the set G/H. Now we'll use the orbit-stabilizer theorem to prove a nice result in elementary number theorem.

Theorem 7 (Fermat's Little Theorem)**.** *Let a be an integer and p be a prime, then $p \mid a^p - a$.*

Proof. This proof should bear some resemblance to a problem you did in HW5. Without loss of generality we can assume that $a > 0$. We'll consider colorings of the vertices of a regular p-gon, drawing our colors from the set $[a]$. The set $C(a,p)$ of these colorings has size a^p. Furthermore, any cyclic permutation of the vertices of the p-gon yields another coloring; this is a group action of $\mathbb{Z}/p\mathbb{Z}$ on $C(a,p)$. The orbits of this action must have order 1 or p, since $p = |\mathbb{Z}/p\mathbb{Z}|$ is prime. Now, observe that an orbit has order 1 if and only if all the vertices are assigned the same color; it follows that there are a such orbits. All other orbits have size p, so we can write $a^p = |C(a,p)| = a + mp$, where m is the number of orbits of size p. □

Exercise 0.29. *Let G be a finite group. Show that if p is the smallest prime dividing the order of G, then any subgroup of G of index p is normal.*

- *Let $[G : H] = p$, and consider the kernel K of the homomorphism $\pi_H : G \to S_{G/H}$,*
- *Use an isomorphism theorem to conclude that $[G : K] = [G : H][H : K] = pk$ for $k = [H : K]$,*
- *Show that G/K is isomorphic to a subgroup of S_p,*
- *Conclude that k divides $(p-1)!$, and that $k = 1$, so $H = K \trianglelefteq G$.*

0.11. **Conjugation action and the class equation.** We've discussed how a group G can act on itself by conjugation, $a_C : G \times \mathbf{G} \to \mathbf{G}$, $a_C(h, \mathbf{g}) = h\mathbf{g}h^{-1}$. We'll apply some of the technology of orbits and stabilizers to this action to deduce a few counting formulas for finite groups. First we observe that the action a_C can be extended to an action on the whole powerset $\mathcal{P}(G)$ of the group G. For any $S \subset G$ we can define $gSg^{-1} = \{ghg^{-1} \mid h \in S\}$. We say two sets are conjugate if they are elements of the same conjugation orbit in $\mathcal{P}(G)$. The number of conjugates to a given $S \subset G$ is equal to the order of its conjugacy class, which in turn equals $[G : G_S] = \frac{|G|}{|G_S|}$, where G_S is the stabilizer of S under conjugation. We can recognize G_S as nothing more than the normalizer $N_G(S)$. Furthermore, if $S = \{s\}$ is a singleton we have $N_G(\{s\}) = C_G(s)$, the centralizer of s. This is all we need to prove the Class Equation for a finite group G.

Theorem 8 (Class Equation)**.** *Let $g_1, \ldots, g_r$ be representatives of the distinct conjugacy classes in G which are not in the center $Z(G)$, then:*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]. \tag{14}$$

Proof. For any group action $a : G \times X \to X$, with distinct orbits $\mathcal{O}_1, \ldots, \mathcal{O}_r$ we have $|X| = \sum_{i=1}^{r} |\mathcal{O}_i| = \sum_{i=1}^{r} [G : G_i]$. The elements in $\mathbb{Z}(G)$ each are in a conjugacy class of size 1. □

Example 0.33. *If A is an Abelian group, then $A = Z(A)$ and $C_A(a) = A$ for every $a \in A$. In this case we might say that the class equation isn't that interesting.*

Example 0.34. *If P is a group of prime power order, $|P| = p^a$, then $[P : C_P(g_i)]$ is also always a prime power. The class equation then implies that p divides $|Z(P)|$. Since $1_P \in Z(P)$, we must have that the center of P is non-trivial.*

Exercise 0.30. *Show that any group of order p^2 for a prime p is Abelian.*

Example 0.35. *Conjugation of elements in S_n is very easy to describe. In linear algebra, conjugation is change of basis, that is if P is invertible, then the matrix representation of the linear transformation underlying A with respect to the basis given by the columns of P is PAP^{-1}. Using the permutation matrix representation of S_n, we see that if σ has cycle decomposition $(a_1, \cdots)(b_1 \cdots) \cdots$, then $\tau\sigma\tau^{-1}$ has cycle decomposition $(\tau(a_1), \cdots)(\tau(b_1), \cdots) \cdots$.*

It follows that any two members of the same conjugacy class have the same disjoint cycle type. In fact, we can show more. If we suppose σ and τ have the same disjoint cycle type, we can order the cycle lengths smallest to largest, including 1 cycles for the sake of completeness. Now each integer appears exactly once in each list. Let ω be the unique permutation which takes the σ list to the τ list, then $\sigma = \omega\tau\omega^{-1}$.

From the above discussion it follows that the number of conjugacy classes in S_n is equal to the number of ways to partition n.

0.12. **The simplicity of A_n.** We can understand which groups can be realized as homomorphic images of a group G, these are precisely the quotient groups G/N, where $N \trianglelefteq G$. If G has no non-trivial ($= \{1_G\}, G$) normal subgroups, we can conclude that the image of any homomorphism out of G is either isomorphic to G itself, or is the identity. Groups with this property are said to be *simple*.

Example 0.36. *The cycic group $\mathbb{Z}/p\mathbb{Z}$ for a prime p is a simple group. Indeed, any subgroup of $\mathbb{Z}/p\mathbb{Z}$ is itself a cyclic group $\langle d\rangle$ for $d \mid p$. Since p is prime, $d = 1$ or p.*

We'll give a proof that the alternating group $A_n = Ker(sgn) \subset S_n$ is a simple group for $n \geq 5$. First we will need some supporting results.

Lemma 0.37. *The group A_5 is simple.*

To prove this lemma we'll use a basic observation about conjugacy classes: any normal subgroup $N \trianglelefteq G$ is a disjoint union of conjugacy classes. Put another way, if $g \in N$ then the whole conjugacy class containing g is also in N, and these classes do not overlap. Also, N always contains the conjugacy class of the identity.

Proof. Cutting out a lot of computation, we have 5 conjugacy classes in A_5, these are the conjugation orbits (in A_5!) $\mathcal{O}_{(1)}$, $\mathcal{O}_{(12345)}$, $\mathcal{O}_{(21345)}$, $\mathcal{O}_{(12)(34)}$, and $\mathcal{O}_{(123)}$. These have orders $1, 12, 12, 15, 20$, respectively. If $N \trianglelefteq A_5$ then $|N|$ divides $60 = |A_5|$, but there is no way to add some selection of these orders up to get a number that divides 60, except 1 (trivial group) and 60 (whole group). □

Next we have two well-known results about 3-cycles in A_n.

Lemma 0.38. *For $n \geq 5$, any two 3-cycles are conjugate in A_n.*

Proof. Let (abc) be a 3-cycle. We can find $\sigma \in S_n$ such that $\sigma(abc)\sigma^{-1} = (123)$, so that $(123) = \sigma^{-1}(abc)\sigma$. If $\sigma \in A_n$ we're clearly done, so suppose this is not the case and let $\omega = \sigma(45)$, so $\omega^{-1}(abc)\omega = (45)\sigma^{-1}(abc)\sigma(45) = (45)(123)(45) = (123)$. □

Notice that this proof required the existence of at least 5 distinct indices.

Lemma 0.39. *For any n, A_n is generated by 3-cycles.*

Proof. The idea is very easy: every pair of transpositions $(ab)(cd)$ can be realized as a product of 3-cycles. Since every element of A_n is an even product of transpositions, this proves the result. If $\{a, b\} \cap \{c, d\} = \emptyset$ then $(ab)(cd) = (dac)(abd)$. If $a = d$, then $(ab)(ac) = (acb)$. □

These two lemmas give us a strategy for proving that a normal subgroup of A_n is either 1 or A_n: Show that if $N \neq \{1\}$, then it must contain a 3-cycle. If it does, then all 3 cycles are contained in N by Lemma 0.38, and by Lemma 0.39 this implies that $N = A_n$. We will use one more technical lemma.

Lemma 0.40. *If $n \geq 5$ then any $1 \neq \sigma \in A_n$ has a conjugate $\tau\sigma\tau^{-1} \neq \sigma$ such that $\sigma(i) = \tau\sigma\tau^{-1}(i)$ for some $1 \leq i \leq n$.*

Proof. Relabelling as necessary, we may write $\sigma = (1 \cdots r)\omega$, where r is the longest cycle length coming from σ, and the the indices appearing in the cycle decomposition of ω are disjoint from $\{1, \ldots, r\} \subset [n]$.

Now we have some cases.

$\mathbf{r \geq 3}$: Take $\tau = (345)$. Then $\sigma(1) = 2$ and $\tau\sigma\tau^{-1}(1) = 2$, but $3 = \sigma(2) \neq \tau\sigma\tau^{-1}(2) = 4$.

$\mathbf{r = 2}, \sigma$ is a product of >2 transpositions: This implies that $n \geq 6$, so without loss of generality we can write $\sigma = (12)(34)(56)\cdots$. Now let $\tau = (12)(35)$, then $\sigma(1) = 2$, $\tau\sigma\tau^{-1}(1) = 2$, $\sigma(3) = 4$ and $\tau\sigma\tau^{-1}(3) = 6$.

$\mathbf{r = 2}, \sigma$ is a product of 2 disjoint transpositions: Without loss of generality can write $\sigma = (12)(34)$. Let $\tau = (132)$, so $\tau\sigma\tau^{-1} = (13)(24)$. These aren't the same element, and they both fix 5. □

Theorem 9. *For $n \geq 5$, the group A_n is simple.*

Proof. Like many proofs of this fact, we will work by induction. Our base case is done by Lemma 0.37, so fix n and suppose that A_m is simple for all $5 \leq m < n$. Let $N \trianglelefteq A_n$ and pick $1 \neq \sigma \in N$. By Lemma 0.40 we find a conjugate ω of σ which takes the same value as σ for some i. We know N is normal, so $\omega \in N$, and we know that $\sigma^{-1}\omega \in N$ is not the identity and fixes i.

Let $G_i \subset A_n$ be the subgroup of elements which fix i. These are the elements of A_n whose cycle decompositions do not involve the index i. It is straightforward to show that this is a copy of A_{n-1}.

Exercise 0.31. *Show G_i is isomorphic to A_{n-1}.*

We have shown above that $G_i \cap N$ is strictly larger than $\{1\}$, so it follows that $G_i \cap N \trianglelefteq G_i$ is a non-trivial normal subgroup of G_i. By our induction hypothesis, this means that $G_i \cap N = G_i$. We conclude that N contains a 3-cycle, so $N = A_n$. □

Week 7

0.13. **Automorphisms.** For any type of mathematical object where the word "isomorphism" makes sense, we can consider the isomorphisms between the object and itself, these are called *automorphisms*. For a group G the set of automorphisms is denoted $Aut(G)$.

Exercise 0.32. *Show that when $Aut(G)$ is a group when it is equipped with the composition operation.*

This doesn't really rely on the fact that G is a group, it works any time we talk about automorphisms, and it's one of the reasons groups are so ubiquitous and important in mathematics. We have already seen automorphisms hiding in the background of our discussion of normal subgroups. If $N \trianglelefteq G$ then we can define a map $\phi : G \to Aut(N)$ using the conjugation action.

Proposition 0.41. *Let $\phi : G \to Aut(N)$ be the map defined by $g \to \phi_g$, where $\phi_g(n) = gng^{-1}$. Then ϕ is a homomorphism with kernel $C_G(N)$.*

Proof. For any $h, g \in G$ we can compute $\phi_h \circ \phi_g : N \to N$ is the map which sends n to $hgng^{-1}h^{-1}$; this is precisely ϕ_{hg}. Furthermore, it follows that $\phi_g^{-1} = \phi_{g^{-1}}$, so each ϕ_g is $1-1$ and *onto*. Since $\phi_g(nm) = gnmg^{-1} = gng^{-1}gmg^{-1} = \phi_g(n)\phi_g(n)$, we see that each ϕ_g is an automorphism. It follows that $\phi : G \to Aut(N)$ is a group homomorphism. Now, if $\phi_g(n) = n \ \forall n \in N$ we must have $gng^{-1} = n$. This implies that $Ker(\phi) = C_G(N)$. □

We have a few observations. If $H \subseteq G$ is a subgroup, any automorphism $\phi \in Aut(G)$ restricts to give an isomorphism between H and $\phi(H) \subset G$. For any subgroup H we have that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. Also, we see that there is always a map from G to its own group of automorphisms $Aut(G)$ with kernel $Z(G)$. This subgroup of $Aut(G)$ is denoted $Inn(G)$, and is called the group of inner automorphisms.

Proposition 0.42.

$$Inn(G) \trianglelefteq Aut(G) \tag{15}$$

Proof. Let $\phi_g \in Inn(G)$ be an inner automorphism, and let $\psi \in Aut(G)$. Fixing $h \in G$ we compute: $\psi \circ \phi_g \circ \psi^{-1}(h) = \psi(g\psi^{-1}(h)g^{-1}) = \psi(g)\psi(\psi^{-1}(h))\psi(g^{-1}) = \psi(g)h\psi(g)^{-1} = \phi_{\psi(g)}(h)$. In particular, $\psi \circ \phi_g \circ \psi^{-1} = \phi_{\psi(g)} \in Inn(G)$. □

The quotient group $Aut(G)/Inn(G)$ is called the *outer automorphism group* of G and is denoted $Out(G)$.

Example 0.43. *Let's describe the automorphism group of $\mathbb{Z}/n\mathbb{Z}$. Any isomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ must take 1 to an element of order n in $\mathbb{Z}/n\mathbb{Z}$. We know that $\langle\phi(1)\rangle = \langle GCD(\phi(1), n)\rangle$ and that $|GCD(\phi(1), n)| = \frac{n}{GCD(\phi(1),n)}$. It follows that $GCD(\phi(1), n) = 1$. We also verify that $\phi, \psi \in Aut(\mathbb{Z}/n\mathbb{Z})$ and $\phi(1) = \psi(1)$ then $\phi(m) = \psi(m)$ for any $1 \leq m \leq n$, because 1 is a generator of $\mathbb{Z}/n\mathbb{Z}$. Moreover, for any $1 \leq a \leq n$ with $GCD(a, n) = 1$ we know that $|a| = n$, so the map $\phi_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi_a(1) = a$ is an isomorphism. We conclude that $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times = \{a \mid GCD(a, n) = 1\}$.*

0.14. **The Cauchy and Sylow Theorems.** We mentioned earlier that Lagrange's Theorem has no converse; that is, if $d \mid |G|$ it does not follow that there is a subgroup of G of order d. The Cauchy and Sylow theorems are pretty much the best we can do to get a result along these lines. A subgroup $P \subset G$ is called a p-group for a prime p if its order is p^a for some $a \geq 0$ (of course this means that $p^a \mid |G|$). First we'll consider Cauchy's Theorem.

Theorem 10 (Cauchy's theorem)**.** *Let G be a finite group, and suppose that $p \mid |G|$, then G contains a subgroup P of order p.*

Proof. (This was outlined in HW5, and is also quite similar to our proof of Fermat's Little Theorem). Here are the major steps of McKay's proof of this result. Let $S = \{(x_1, \ldots, x_p) \mid x_i \in G, x_1 \cdots x_p = 1\}$.

Show that $|S| = |G|^{p-1}$,

Show that a cyclic permutation of an element of S **is in** S,

Conclude that $|G|^{p-1} = m + pn$**, where** m **is the number of cyclic orbits of size** 1 **and** n **is the number of orbits of size** p,

Prove that orbits of size 1 **under this action correspond to** x **such that** $x^p = 1$,

Now, since $p \mid m$ and the orbit of $(1, \ldots, 1)$ has size 1, we conclude that $m > 0$ and that there must be an element $g \in G$ of order p. □

Example 0.44. *Let $a > 1$ and consider $\mathbb{Z}/p^a\mathbb{Z}$. If we take $\langle p^{a-1}\rangle \subset \mathbb{Z}/p^a\mathbb{Z}$ we obtain a subgroup of order p.*

Exercise 0.33. *Find an explicit subgroup of D_{2n} of order p for any $p \mid 2n$.*

Exercise 0.34. *Find an explicit subgroup of S_n of order p for any $p \mid n!$.*

Cauchy's theorem says that there is always a p-group of smallest possible (non-triviall) order for any $p \mid |G|$. Sylow's theorem establish a similar result, but for the largest possible order.

Definition 0.45. *A subgroup $P \subset G$ is said to be a Sylow p-subgroup of G if $|P| = p^a$ for some $a \geq 0$ and p^a is the maximum power of p which divides $|G|$.*

We denote the set of Sylow p-subgroups of G by $Syl_p(G)$, and we let $|Syl_p(G)| = n_p(G)$.

Theorem 11. *[Sylow's theorem] Let G be a group and let p be a prime dividing $|G|$, then:*

(1) *$Syl_p(G) \neq \emptyset$,*

(2) *Any two members of $Syl_p(G)$ are conjugate,*

(3) *$n_p(G) = 1 + kp$ for some k, and $n_p(G) = [G : N_G(P)]$ for any $P \in Syl_p(G)$.*

Week 8

Rings! (and sometimes "Rng"s) The integers $\mathbb{Z}$ provided a useful model for developing the theory of groups, even though we found that they are much richer objects outside the Abelian case. In this respect, groups are a generalization of $\mathbb{Z}$ equipped with the addition operation. Rings are a generalization of $\mathbb{Z}$ equipped with both addition and multiplication.

Definition 0.46. *A ring R is a set equipped with two binary operations $+$ and $\times$ which satisfy:*

(1) *$(R, +)$ is an Abelian group,*

(2) *$\times$ is an associative operation,*

(3) *$\times$ distributes over $+$: $a \times (b + a) = a \times b + a \times c)$.*

Usually we will also insist that R contains a multiplicative identity element $1 \in R$. When $\times$ is a commutative operation, R is said to be a commutative ring.

Notice that, just like in $\mathbb{Z}$, we don't insist that non-zero elements of R have multiplicative inverses. A ring with $1 \in R$ such that all non-zero elements are invertible is called a division ring. When a commutative ring has this property, it's called a field.

Example 0.47. *The integers $\mathbb{Z}$ form a ring, as do $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The latter three are fields.*

Example 0.48. *We've seen that for any $n \in \mathbb{Z}$ the quotient set $\mathbb{Z}/n\mathbb{Z}$ can be equipped with an Abelian group structure just by checking that addition is well-defined on cosets. Multiplication of non-zero cosets works as well. Let $a-a', b-b' \in n\mathbb{Z}$, then $a(b-b') \in n\mathbb{Z}$ and $b'(a-a') \in n\mathbb{Z}$, so:*

$$ab - a'b' = a(b - b') + b'(a - a') \in n\mathbb{Z}. \tag{16}$$

It's straightforward to check that 1 is a multiplicative identity in $\mathbb{Z}/n\mathbb{Z}$, and that multiplication is commutative. It follows that $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring. Is it a field?

Example 0.49. *Let i, j, k satisfy the relations*

$$i^2 = j^2 = k^2 = -1, \ \ ij = -ji = k, \ jk = -kj = i, \ ki = -ik = j. \tag{17}$$

We'll make a 4-dimensional real vector space $\mathbb{H}$ by considering sums of the form $a + bi + cj + dk$, and equip it with a multiplication operation using the expected distributive law and the relations above. The resulting non-commutative ring is called the ring of real quaternions. The quaternions have a multiplicative identity, $1 + 0i = 0j + 0k$, and all non-zero quaternions have multiplicative inverses:

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \tag{18}$$

It follows that the real quaternions are a division ring.

Example 0.50. *Let $\mathbb{Z}[x]$ be the set of polynomials in one variable with coefficients in $\mathbb{Z}$. By now you are familiar with polynomial addition and multiplication, so you can check that $\mathbb{Z}[x]$ is a commutative ring with identity.*

Example 0.51. *The matrices $M_{n\times n}(\mathbb{Z})$ make a non-commutative ring with identity under matrix multiplication and matrix addition. In fact, you can check that $M_{n\times n}(R)$, where R is any ring with unity is also a ring.*

Elements in a ring R with multiplicative inverses are called units, this set is denoted $R^\times$. You can check that $R^\times$ is always a group. Sometimes when we take the product of two elements in a ring we get 0 (think up an example for matrices), ie $uv = 0$. In this case we say that u and v are 0-divisors.

Exercise 0.35. *Show that a 0-divisor is not a unit, so that fields cannot contain 0-divisors.*

Definition 0.52. *An "integral domain," or sometimes just "domain" is a commutative ring with unity which contains no 0-divisors.*

Suppose a is not a 0-divisor, and $ab = ac$, then we can show that $a = 0$ or $b = c$. Indeed, we have $a(b-c) = 0$, so $a = 0$ or $b-c = 0$. This is a type of "cancelation" property, which holds for any three elements in a domain.

Example 0.53. *Let $\mathbb{Z}[i]$ be the set of elements $a + bi$ where $i^2 = -1$, this is the ring of Gaussian integers. This is a domain, and moreover it can be shown that the Euclidean algorithm can be carried out in $\mathbb{Z}[i]$ using the "measurement of size" $N(a + bi) = a^2 + b^2$ in place of the usual ordering on $\mathbb{Z}_{\geq 0}$. This latter function is called a "norm."*

Week 9

Let's look at a few more examples of rings.

Example 0.54. *More about polynomial rings. Let R be an integral domain, then we can consider the ring $R[x]$ of polynomials over R in one variable. For any $p(x) \in R[x]$, the degree $deg(p)$ is the highest power that appears in $p(x)$.*

We can check the following properties:

(1) $deg(pq) = deg(p) + deg(q)$,

(2) $p \in R[x]$ *is a unit if and only if* $p \in R^\times$,

(3) $R[x]$ *is also an integral domain.*

Both (1) *and* (3) *are consequences of the fact that R has no* 0 *divisors. Then* (1) *implies that a unit must have degree* 0.

Example 0.55. *For any group G we can form the group ring $\mathbb{Z}[G]$. The underlying Abelian group of this ring is $\mathbb{Z} \oplus \cdots$, where there is* 1 *copy of $\mathbb{Z}$ for each element of G. Multiplication is then defined in a similar fashion to the product operation in polynomial rings:*

$$(n_1 g_1 + \cdots + n_k g_k)(m_1 h_1 + \cdots + m_\ell h_\ell) = \cdots + n_i m_j g_i h_j + \cdots . \tag{19}$$

If $1 < |G| < \infty$ then $\mathbb{Z}[G]$ always has 0*-divisors, let $|g| = m$:*

$$(1 - g)(1 + g + \cdots + g^{m-1}) = 1 - g^m = 0. \tag{20}$$

Example 0.56. *Taking $G = \mathbb{Z}$ gives us a special case of the group ring. The poorly denoted $\mathbb{Z}[\mathbb{Z}]$ is a ring over $\mathbb{Z}$ with a single invertible generator $t = [1]$. This ring is also known as the Laurent polynomial ring $\mathbb{Z}[t, t^{-1}]$. Laurent polynomials are much like normal polynomials, except we allow negative exponents.*

Just as with groups, the theory of rings becomes much more meaningful when we understand how to relate rings to each other. Ring homomorphisms are maps between rings which preserve all of the relevant algebraic operations.

Definition 0.57. *A ring homomorphism $\phi : R \to S$ is a map satisfying $\phi(a + b) = \phi(a) + \phi(b)$ (in other words it is a map of groups on the underlying Abelian groups of R and S), and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$. A bijective ring homomorphism is called an isomorphism.*

The image $\phi(R) \subset S$ is also closed under multiplication, and if ϕ is a map of rings with unity, it also must contain 1, making it a subring of S.

Any ring homomorphism $\phi : R \to S$ has a kernel $Ker(\phi)$, namely the subgroup of R consisting of those elements which are sent to 0. We can say even more about $Ker(\phi)$; note that if $r \in Ker(\phi)$ then for any $f \in R$, $\phi(fr) = \phi(f)\phi(r) = \phi(f)0 = 0$. Similarly $\phi(rh) = \phi(r)\phi(h) = 0$, so $Ker(\phi)$ is closed under left and right multiplication by elements in R. Note that if $1 \in Ker(\phi)$ then $1f \in Ker(\phi)$ for any $f \in R$, so $R = Ker(\phi)$; so $Ker(\phi)$ is generally not a ring with unity. These observations establish that $Ker(\phi) \subset R$ is a subring, but with the additional property that it is closed under multiplication with *any* element of R.

Definition 0.58. *A subgroup $I \subset R$ is called a two-sided ideal if is closed under left and right multiplication by elements of R.*

From what we have already seen, the kernel of any ring homomorphism is an ideal, so we can think of ideals as the analogue of "normal subgroup" for a ring. Just as with normal subgroups, we can ask if an ideal $I \subset R$ is the kernel of some ring homomorphism. Let's develop the ideal of "quotient ring" first before we address this question. Just as with groups, we can consider the quotient R/I for any subgroup $I \subset R$.

The quotient R/I is naturally an Abelian group since $I \trianglelefteq R$, so it makes sense to ask when the induced multiplication operation on cosets $(r+I)(s+I) = (rs+I)$ makes sense. The following proposition should remind you of our classification of kernels of group homomorphisms.

Proposition 0.59. *Let $I \subset R$ be a subgroup, then the natural multiplication operation is well-defined on R/I if and only if I is a two-sided ideal of R.*

The quotient R/I is called the quotient ring of I.

Theorem 12 (First Isomorphism Theorem Of Rings)**.** *Let $\phi : R \to S$ be a ring homomorphism.*

(1) *$Ker(\phi)$ is a (two-sided) ideal of R, and $\phi(R) \cong R/Ker(\phi)$.*

(2) *If $I \subset R$ is any (two-sided) ideal then the map $R \to R/I$, $r \to r + I$ is a surjective ring homomorphism with kernel I.*

Example 0.60. *Let A be commutative with unity, and consider a polynomial $p(x) \in A[x]$. The principal ideal $\langle p(x)\rangle \subset A[x]$ is the set of elements of the form $p(x)q(x)$ where $q(x)$ ranges over all polynomials in $A[x]$. The quotient $A/\langle p(x)\rangle$ can be thought of as the ring generated by A and an element $\bar{x}$ (the image of $x \in A[x]$) which satisfies the equation $p(x) = 0$. In particular $q(\bar{x}) = r(\bar{x})$ in the quotient if and only if $q(x) - r(x)$ is divisible by $p(x)$.*

If $A = \mathbb{Q}$ (or some other field), we compute the image of $q(x) \in A[x]$ in $A[x]/\langle p(x)\rangle$ using the division algorithm. In particular, we can write $q(x) = p(x)d(x)+r(x)$, where $deg(r(x)) < deg(p(x))$. Then we see that $q(\bar{x}) = r(\bar{x})$, and that $r(x)$ must be the unique minimal degree element in the coset $q(x) + \langle p(x)\rangle$.

Proof of the first isomorphism theorem and the preceding proposition work by first proving the corresponding fact for Abelian groups and then showing that the relevant maps and operations work with multiplication. The same strategy works for the following theorem.

Theorem 13 (Second, Third, and Fourth Isomorphism Theorem of Rings)**.** *Everything in sight only needs to be a ring (no assumptions of commutativity or unity).*

(1) *Let $R \subset S$ be a subring and $I \subset S$ be an ideal, then the set $R + I \subseteq S$ is a subring, $R \cap I$ is an ideal of R, and $R + I/I \cong R/R \cap I$.*

(2) *Let $I \subset J \subset R$ be ideals, then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.*

(3) *Let I be an ideal of R, then the correspondence $A \to A/I$ is an inclusion preserving bijection between the set of subrings of R which contain I and the set of subrings of R/I, and A is an ideal of R if and only if A/I is an ideal of R/I.*

We close by mentioning some operations on ideals.

Definition 0.61. *Let $I, J \subset R$ be ideals,*

(1) *the sum ideal $I + J = \{a + b \mid a \in I, b \in J\}$,*

(2) *the product ideal IJ is the set of finite sums of elements of the form $ab, a \in I, b \in J$,*

(3) *the intersection ideal $I \cap J$ is just the set-theoretic intersection.*

Notice that $IJ \subset I \cap J$, but $IJ \neq I \cap J$.

Week 10

Now we assume that R is a ring with a multiplicative identity $1 \in R$. Let $X \subset R$ be an subset, then we can define several ideals associated to X:

(1) $\langle X \rangle \subset R$ is the smallest ideal (under inclusion) containing X.

(2) RX is the set of finite sums of left multiples of elements of X. XR and RXR are defined similarly.

It is straightforward to verify that an intersection of ideals is an ideal, so we have $\langle X \rangle = \bigcap_{X \subset I} I$, where the intersection runs over all ideals containing X. We can modify the definition of $\langle X \rangle$ and consider $\langle X \rangle_L$, the smallest left ideal containing X, the smallest right right ideal $\langle X \rangle_R$, or the smallest two-sided ideal $\langle X \rangle_{LR}$.

Exercise 0.36. *Show that $\langle X \rangle_L = RX$, $\langle X \rangle_R = XR$, and $\langle X \rangle_{LR} = RXR$. Conclude that if R is a commutative ring then $RX = XR = RXR = \langle X \rangle$.*

We've remarked before that any ideal $I \subset R$ containing a unit must be R itself. The following is a consequence of this observation.

Proposition 0.62. *A commutative ring K with unity is a field if and only if its only ideals are 0 and K.*

A noncommutative version of this fact states that a ring D with unity in which the only left ideals and right ideals are 0 and D must be a division ring. Notice in particular that a ring might have no non-trivial two-sided ideals, but may have non-trivial left and right ideals. This happens with the matrix ring $M_{n \times n}(K)$, when K is a field. The following proposition is probably the most general thing we can say about the existence of ideals.

Definition 0.63. *An ideal $M \subset R$ is said to be maximal if it proper, and is not contained in any other proper ideals.*

Proposition 0.64. *Let R be a ring with unity, then every proper two-sided ideal is contained in a two-sided maximal ideal.*

Proof. This proof uses a classic technique involving Zorn's lemma. Let I be a proper two-sided ideal and let $\mathcal{S}(I)$ be the set of all two-sided

ideals containing I. Notice that $\mathcal{C}(I)$ is non-empty, and has partial order given by inclusion. Let C be a chain in $\mathcal{S}(I)$, and let $M_C = \bigcup_{J \in C} J$. Every element of C is closed under left and right multiplication, so M_C is as well. Furthermore, if $f, g \in M_C$ then $f \in J_1$ and $g \in J_2$ for some J_1, J_2 containing I, it follows that $J_1 \subset J_2$ or $J_2 \subset J_1$ since C is a chain. As a consequence, $f - g$ is contained in the bigger one. This proves that M_C is an ideal. If it weren't proper, then $1 \in J \subset M_C$ for some J containing I, which contradicts how we formed C. This proves that each chain has an upper bound, so by Zorn's Lemma, there is a maximal element in $\mathcal{S}(I)$. □

The isomorphism theorems give us a way to relate the structure of ideals in a ring R with that of a quotient ring R/I. This means that if we take a maximal ideal $M \subset R$ in a commutative ring, we should expect that R/M has no ideals. In particular, a quotient of a commutative ring is a field if and only if the quotient ideal is maximal.

Maximal ideals M of commutative rings have another nice property, if we take $f, g \in R$ such that $fg \in M$, then we can consider the image of these elements under the quotient map $\phi : R \to R/M$. Since R/M is a field and $\phi(fg) = 0$, we must have $\phi(f) = 0$ or $\phi(g) = 0$, so $f \in M$ or $g \in M$. We can compare this property to prime numbers: if $p \mid ab$ then $p|a$ or $p|b$.

Definition 0.65. *A proper ideal $P \subset R$ a commutative ring is said to be prime if for any $f, g \in R$ if $fg \in P$ then $f \in P$ or $g \in P$.*

Prime ideals are meant to directly generalize prime numbers, and from what we've just mentioned above, any maximal ideal in a commutative ring with unity is prime.

Proposition 0.66. *Let $P \subset R$ be an ideal in a commutative ring with unity, then P is a prime if and only if R/P is an integral domain.*

Proof. This proof mimics what we've already said for maximal ideals. Let $\phi : R \to R/P$ be the quotient map, then $\phi(fg) = 0$ can only happen in R/P if and only if $\phi(f)$ or $\phi(g)$ is 0. □