Math 331-1: Abstract Algebra
Northwestern University, Lecture Notes

Written by Santiago Cañez

These are notes which provide a basic summary of each lecture for Math 331-1, the first quarter of "MENU: Abstract Algebra", taught by the author at Northwestern University. The book used as a reference is the 3rd edition of *Abstract Algebra* by Dummit and Foote. Watch out for typos! Comments and suggestions are welcome.

Contents

Lecture 1: Introduction to Groups

Abstract algebra is the study of algebraic structures, which are sets equipped with operations akin to addition, multiplication, composition, and so on. Manipulating and solving equations—the basic concepts you would have seen in a previous "algebra" course—play a role as well, but now our focus is much more squarely on the underlying structures which allow such manipulations to work. Ultimately, the goal is to use the various tools available—in particular the notions of "sub" and "quotient" structures—to classify a given algebraic structure to the extent possible.

That is a very vague brief introduction, so let us say a bit more about what we mean by an "algebraic structure". In subsequent quarters we will be studying what are called *rings* and *fields*, which in some sense provide vast generalizations of the notion of "numbers". Both of these are sets equipped with two operations which are assumed to satisfy some appropriate properties, but as a first step towards understanding "algebra" we begin this quarter with the notion of a *group*, which only involves a set equipped with a single operation. Historically groups arose in the following way.

Groups and polynomials. We are all familiar with the quadratic formula, which gives an explicit description of the roots of a polynomial of degree 2, say with real coefficients:

$$ax^2+bx+c=0 \implies x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

The key observation for us is that this expression for the roots involves only the coefficients of the given polynomial and some basic algebraic operations: addition, subtraction, multiplication, division, and taking a square root. If we go back a degree, it is also true that the roots of a linear polynomial can be expressed in terms of its coefficients and basic algebraic operations (only division is needed in this case!):

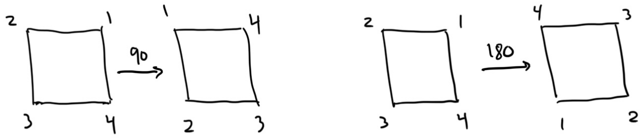
$$ax+b=0 \implies x=-\frac{b}{a}.$$

The search for analogous formulas for polynomials of higher degree is a problem which dates back centuries, even millennia! The *cubic formula* for polynomials of degree 3 is much more complicated than the quadratic formula above (it requires higher-order root extractions), and the *quartic formula* for polynomials of degree 4 even more so (you can see what they look like on Wikipedia!), but the point is that such formulas exist. However, in the 19th century it was proven that no analogous *quintic formula* for polynomials of degree 5 existed. This seems quite surprising at first, since it is not all all clear what breaks down when we make the jump from degree 4 to degree 5. It turns out, as we'll see fully in the spring, that the reason for this has to do with the structure of the "group of permutations" of the roots of such polynomials.

We will avoid giving any formal definitions for now, but here is the basic (and at this point quite vague) idea. Consider the polynomial x^2-2 with roots $\sqrt{2},-\sqrt{2}$. There are two possible permutations of the roots in this case—do nothing, or exchange them—which thus form a "permutation group" with two elements. The polynomial x^3-2 has three roots: $\sqrt[3]{2}$ and two complex conjugate roots. There are $3!=6$ ways of permuting these 3 roots, and so we get a group of permutations with 6 elements in this case. Now consider $(x^2-2)(x^2-3)$. This has roots $\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}$, and there are $4!=24$ ways of permuting these. However, in this case it turns out that not all of these 24 possible permutations should actually be allowed; the issue is that permuting, say, $\sqrt{2}$ and $\sqrt{3}$ exchanges roots of the two factors x^2-2 and x^2-3, and, for reasons we will leave for the spring, this should not actually be a valid permutation. We only get four allowable permutations—the two coming from permuting $\pm\sqrt{2}$ and the two which permute $\pm\sqrt{3}$—and thus a group with 4 elements.

The upshot is that the question as to whether or not we can express the roots of a polynomial in a certain way is intimately related to properties of these groups of root permutations, and that properties of these groups reflect properties (or "symmetries") of the roots. To give an answer as to why a quintic formula does not exist—although not an answer which will make any sense as this point—the fact is that there exist polynomials of degree 5 which have the so-called *alternating group* A_5 as its group of root permutations, and A_5 has the property of being a *simple, non-abelian* group; it is this property which prevents there from being a nice way of expressing the roots of such a polynomial. (All groups which arise from polynomials of degree 4 or less—one example being the alternating group A_4—are either non-simple or simple *and* abelian, so there is nothing which stands in the way of there being a nice way of expressing the roots.) We will soon understand what all of these terms above mean, but we mention this now in order to give some motivation for the study of groups.

Symmetries of a square. Before giving the definition of a the term "group", we give one example. Let D_8 be the set of *rigid symmetries* of a square, which are the rigid/physical movements we can do to a square which result in the same square. (No "stretching" allowed!) For instance, we can rotate the square counterclockwise by 90°, or by 180°, or by 270°. Rotating by something like 45° is not a symmetry since this technically results in a "diamond" and not the literal square you began with. In order to distinguish between these rotations, we label the four vertices of the square and use this labeling to keep track of which symmetry is which:

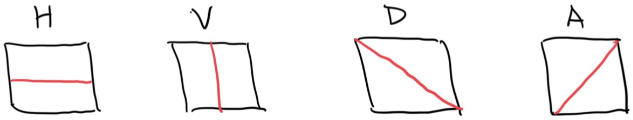


Rotating by 360° is the same as rotating by 0°, and any further rotations are the same as one of the four we have so far, so we get four distinct rigid motions so far: $0, 90, 180, 270 \in D_8$. (We'll drop the degree ° symbol from the notation.) We can *compose* such rotations with one another, leading to equalities such as

$$90 \cdot 180 = 270 \quad \text{and} \quad 90^4 = 0,$$

where we interpret 90^4 as $90 \cdot 90 \cdot 90 \cdot 90$. We are thinking of composition here as a type of "multiplication", so we are not literally saying that 90 times itself four times in the usual sense results in 0.

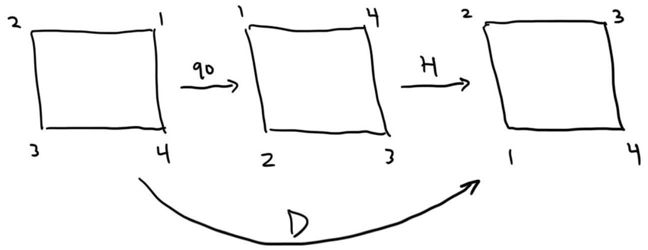
In addition to rotations, there are four *reflections* which give rise to symmetries: a horizontal reflection H, a vertical reflection V, reflection D across the main diagonal, and reflection A across the "anti-diagonal":



It turns out that these eight symmetries give all possible rigid motions of a square, so that

$$D_8 = \{0, 90, 180, 270, H, V, D, A\}.$$

Now, we can consider compositions which involve reflections as well. For instance, we can compute $H \cdot 90$, which is the result of first rotating by 90 and then reflecting horizontally (as is usual with compositions, we read from right to left when performing the required operation):



The same overall result can be obtained by performing the reflection D alone on the original square, so the composition $H \cdot 90$ is the same as D:

$$H \cdot 90 = D.$$

In a similar way, you can work out that "multiplying" any two elements of D_8 still results in an element of D_8, so that D_8 is *closed* under the operation of composition.

Here are some other key algebraic properties to notice. First, composition is associative, so that it does not matter how we group elements:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ for all } x, y, z \in D_8.$$

Second, 0 serves as an *identity* element for composition, meaning that "multiplying" 0 with any element, in any order, results in that other element:

$$0 \cdot x = x = x \cdot 0 \text{ for all } x \in D_8.$$

And finally, each element of D_8 has an *inverse*, which is an element we can compose it with in order to result in the identity element:

$$\text{for all } x \in D_8, \text{ there exists } y \in D_8 \text{ such that } x \cdot y = 0 = y \cdot x.$$

Indeed, 90 and 270 are inverses of one another, and $0, 180, H, V, D$, and A are their own inverses.

In this way, D_8 shares some similarities with, say, the set of integers $\mathbb{Z}$ under addition: addition is associative, the integer 0 serves as an identity element for addition, and any integer has an "additive inverse", namely its negative. The notion of a group—the fundamental object of study in this course—was developed precisely to study such "similar" algebraic structures in a unified way.

Definition of a group. A *group* is a set G equipped with a binary operation $\cdot$ which

- is *associative*: $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$;
- admits a *two-sided identity*: there exists $e \in G$ such that $e \cdot g = g = g \cdot e$ for all $g \in G$; and
- admits *two-sided inverses*: for all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = e = g^{-1} \cdot g$.

(To say that $\cdot$ is a *binary operation* on G simply means that it acts on two elements of G and produces a single element of G.) Thus, D_8 under composition of rigid motions is a group, as is $\mathbb{Z}$ under addition.

We will develop the basic properties of some standard examples over the next few days, but for now we finish with a word about notation and terminology. It is common to think about the operation $\cdot$ as a type of "multiplication" and to refer to it as such, so that we will usually speak of the "product" of g and h for instance. Because of this, it is also common to drop the operation $\cdot$ from the notation altogether, and use gh alone to denote the product of g and h. But keep in mind that this "multiplication" is meant to be computed using whatever binary operation our group is equipped with, which in some cases might actually be "addition". In the "additive" group $\mathbb{Z}$ for instance, "mn" actually means $m+n$. Similarly, we use g^{-1} to denote the inverse of g due to our "multiplicative" frame of mind, but in $\mathbb{Z}$ for example "m^{-1}" actually means $-m$. In general, we will default to using multiplicative notation when working with an abstract group, but will use more standard symbols like $+$ in the concrete examples which use them. In the abstract setting, we will use e to denote the identity element of a group, or e_G if we need to make the dependence on the group G clear. (Technically, the symbol G alone cannot quite refer to a group alone, since a group should be a set *together with* a binary operation, and a given set G might have multiple binary operations which turn it into a group; each of these groups are considered to be different, but nevertheless it is common to use the set G as the single notation for the entire group, with the binary operation implicitly assumed to be present.)

Lecture 2: Integers mod n

Warm-Up 1. The definition of a group requires that inverses and an identity element exist, but it does not outright state that these should be unique. However, this is a simple consequence of the definition, as we now show. The basic point of this and the next Warm-Up is to provide some first examples of working with abstract groups, relying solely on the definition of "group" itself. Recall that when working with abstract groups in this way we default to using multiplicative notation.

Let G be a group and suppose $e, e' \in G$ are both identity elements. Then

$$e = ee' = e'$$

where the first equality holds since e' is an identity, and the second this e is an identity. Thus $e = e'$ so that there is only one identity element.

Similarly, let $g \in G$ and suppose $h, k \in G$ are both inverses of g. Then

$$gh = e = gk$$

by definition of an inverse. Multiplying both sides on the left by h gives

$$h(gh) = h(gk).$$

By associativity this is the same as

$$(hg)h = (hg)k.$$

Since $hg = e$ because h is an inverse of g, this becomes

$$eh = ek,$$

and by definition of the identity we thus get $h = k$. Hence there is only one inverse of g.

Note that in this latter proof we exploited all properties in the definition of "group": associativity, the definition of identity, and the definition of inverse. This argument would not have worked had we had a different definition of "group" in mind, so, as with all things in abstract mathematics, the definition we gave is the way it is precisely so that we carry our arguments like the one above. Moving forward we will not be so pedantic as we were here and explicit list each step in such an argument—instead, we will say things like "multiplying both sides of $gh = gk$ on the left by g^{-1} gives $h = k$" without directly mentioning where associativity and the other properties come in.

Now that we have proven in general that identities and inverses are unique, we do not have to check that this is the case in any particular example we care about. Indeed, this is of course why mathematicians care about proving things in the most general "abstract" way possible, so that we know our argument will always apply.

Exercise. The associativity property given in the definition of a group is only stated for products of three elements at a time, but in fact it extends to any number of elements so that there is never any ambiguity in an expression like $g_1 g_2 \cdots g_n$. We will take this for granted going forward, but if you have never thought about why this is true, it is a nice exercise in induction you can work out for yourself if interested.

Here's the statement. We will use the notation $g_1 g_2, \ldots, g_n$ to denote the specific product obtained by multiplying g_1 and g_2, and then the result by g_3, and then the result of that by g_4, and so on. So, for instance:

$$g_1 g_2 g_3 g_4 := ((g_1 g_2) g_3) g_4.$$

The claim is that this specific grouping of the product is the same as any other grouping: fix $\ell \geq 1$ and show that for any $m \geq 1$ and $\ell + m$ elements $g_1, \cdots, g_{\ell+m}$, we have

$$(g_1 g_2 \ldots g_\ell)(g_{\ell+1} g_{\ell+2} \cdots g_{\ell+m}) = g_1 g_2 \ldots g_{\ell+m}.$$

(Proceed by induction on m. The induction step will use the base case of three elements—which holds by definition—in addition to the induction hypothesis.)

Warm-Up 2. Suppose G is a group such that $g^2 = e$ for all $g \in G$. We show that the group multiplication on G is *commutative*, which means $ab = ba$ for all $a, b \in G$. Let us also take this opportunity to introduce some terminology. The *order* of an element $g \in G$ is the smallest positive integer $n \in \mathbb{N}$ such that $g^n = e$, and we say that g has *infinite order* if no such n exists. Thus the assumption on G in this Warm-Up says that all elements of G have order at most 2, or equivalently that every non-identity element has order 2. (The identity is the only element of order 1.) We will also use the term "order" in the following (seemingly) different way: the *order* of G itself is the number of elements it has. So, for instance, D_8 has order 8 and $\mathbb{Z}$ has infinite order. (Later on we might distinguish between different types of "infinite order" coming from the notion of the *cardinality* of a set.) We will see later that these two uses of the term "order" are not really different, and that the order of an element is a special case of the order of a group.

One more piece of terminology: a group is *abelian* it its multiplication operation is commutative. Thus, this Warm-Up is asking to show that any group for which every non-identity element has order 2 must be abelian. (The term "abelian" comes from the name Abel, who in the early 1800's was the first person to prove that no general quintic formula existed.)

Let $a, b \in G$. Then ab is in G so $(ab)^2 = e$ by the assumption on G; in other words

$$abab = e.$$

(We omit parentheses in order to not clutter up our work, which we can do by associativity.) Since $a^2 = e$ and $b^2 = e$ as well (so a and b are their own inverses), multiplying $abab = e$ on the left by a and on the right by b gives $ba = ab$, so G is abelian as claimed.

Some more examples. So far we have seen D_8 under composition and $\mathbb{Z}$ under addition as examples of groups. In D_8, 90 and 270 have order 4, while $180, H, V, D, A$ all have order 2. The only element of $\mathbb{Z}$ with finite order is 0, so every nonzero integer has infinite order. Another standard example is $\mathbb{R}^\times$, the set of nonzero real numbers, under ordinary multiplication; the identity element is 1, and the inverse of any element is its reciprocal. Here, only 1 and -1 have finite order.

To give another example which you would have seen in another context, although likely not using the language and notation of "groups", we can take the group $GL_n(\mathbb{R})$ of *invertible* $n \times n$ *matrices* with real entries:

$$GL_n(\mathbb{R}) := \{A \mid A \text{ is an invertible } n \times n \text{ matrix over } \mathbb{R}\}.$$

(The "GL" here stands for "general linear" group, which is a standard term used to refer to the set of invertible linear transformations on some space.) The identity element is, of course, the identity matrix. This group is non-abelian when $n > 1$ (i.e. matrix multiplication does not commute in general), and you might recall formulas like $(AB)^{-1} = B^{-1}A^{-1}$ for invertible matrices. In fact, this type of formula is true in any group: $(gh)^{-1} = h^{-1}g^{-1}$, and the proof is the same as what it is for matrices.

Consider now $GL_n(\mathbb{Z})$, which is the group of invertible $n \times n$ matrices with *integer* entries. The key point here is that in order for an integer matrix A to be in $GL_n(\mathbb{Z})$ requires that its inverse *also* be in $GL_n(\mathbb{Z})$, which means that it should have integer entries as well. For instance,

$$\begin{bmatrix} 2 & -1 \\ 4 & 6 \end{bmatrix}$$

is in $GL_n(\mathbb{R})$ but not in $GL_n(\mathbb{Z})$ since its inverse has non-integer entries. (In fact, you can show that an invertible integer matrix has an inverse which is itself an integer matrix if and only if its determinant is ± 1. This comes from taking determinants of both sides of $AA^{-1} = I$, using the fact that $\det(AA^{-1}) = (\det A)(\det A^{-1})$, and using the fact that the determinant of an integer matrix is an integer.) The point is that there is a difference in asking whether an integer matrix has inverse over $\mathbb{R}$ versus over $\mathbb{Z}$, and such subtleties will be important going forward. Later we will consider replacing $\mathbb{Z}$ or $\mathbb{R}$ with other types of "numbers" and looking at other types of matrices.

Integers mod n. We now introduce a fundamental example of a group, which will play a key role in understanding the structure of arbitrary groups, and in particular abelian groups. This example is based on the notion of *modular arithmetic*, which we now define. Fix a positive integer $n \in \mathbb{N}$. We say that two integers $a, b \in \mathbb{Z}$ are *equivalent* (or *congruent*) mod n if their difference $a - b$ is divisible by n. For instance, 3 is equivalent to 9 mod 6, and to 27 mod 6. (The notation $a \equiv b \bmod n$ is commonly used to denote this.) The intuition is that upon dividing by 6, 9 and 27 both leave a remainder of 3, which is why they are equivalent to 3 mod 6. In general, this notion of congruence says that we will only care about remainders when dividing by n, and "identify" things which give the same remainder.

Any integer is equivalent to precisely one of $0, 1, 2, \ldots, n-1$ mod n, so we define the set of *integers mod n* to be

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.$$

(The reason for the notation $\mathbb{Z}/n\mathbb{Z}$ we are using will become clear later when we discuss *quotient groups*, of which this is a basic example. The notation $\mathbb{Z}_n$ is also commonly used, but we will prefer $\mathbb{Z}/n\mathbb{Z}$ since $\mathbb{Z}_n$ also has other meanings, at least when n is prime.) We define *addition mod n* to be addition as usual, only that we interpret the result as an element of $\mathbb{Z}/n\mathbb{Z}$ depending on what is it equivalent to. For instance, $3 + 5 = 8 \equiv 2 \bmod 6$, so we would say that

$$3 + 5 = 2 \text{ in } \mathbb{Z}/6\mathbb{Z}.$$

Here are a few more sums in $\mathbb{Z}/6\mathbb{Z}$: $1 + 5 = 0$, $4 + 5 = 3$, and $2 + 2 = 4$. With this operation, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group of order n. Indeed, 0 is the identity and the inverse of $k \in \{1, \ldots, n-1\}$

is $n-k$. In $\mathbb{Z}/6\mathbb{Z}$ for instance, 1 and 5 are inverses, 2 and 4 are inverses, and 3 is its own inverse (so it has order 2).

Direct products. Given two groups G and H, the *direct product* $G \times H$ is the group which as a set is the usual Cartesian product:

$$G \times H := \{(g,h) \mid g \in G \text{ and } h \in H\}$$

and whose group operation is given by component-wise multiplication:

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2).$$

To be clear, here g_1g_2 is computed using the multiplication of G and h_1h_2 using the multiplication of H. The identity is (e_G, e_H) and inverses are given by $(g,h)^{-1} = (g^{-1}, h^{-1})$. We can easily extend this idea in order to define the direct product of more than two groups.

We mention this construction now in order to state—without proof at this point—that every finite abelian group is in fact the "same" as a direct product of groups of the form $\mathbb{Z}/n\mathbb{Z}$. (We will, of course, also have to clarify what we mean by "same" here.) This and related facts will go a long way towards understanding the structure of abstract groups in general, especially finite ones. For instance, as we will see, it turns out that there are only two "distinct" groups of order 4: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Multiplication mod n. We define *multiplication mod n* on $\mathbb{Z}/n\mathbb{Z}$ in the same way as addition: multiply as normal but then interpret the result as an element of $\mathbb{Z}/n\mathbb{Z}$. For instance:

$$2 \cdot 3 = 0,\ 4 \cdot 5 = 2,\ \text{and } 5 \cdot 5 = 1 \text{ in } \mathbb{Z}/6\mathbb{Z}.$$

This first equality in fact implies that neither 2 nor 3 can have a *multiplicative inverse* in $\mathbb{Z}/6\mathbb{Z}$: if 2 had an inverse, we could multiply both sides of $2 \cdot 3 = 0$ on left by it in order to obtain $3 = 0$, which is not true, and similarly if 3 had an inverse. The final equality above shows that 5 is its own multiplicative inverse in $\mathbb{Z}/6\mathbb{Z}$.

We define $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the group of elements of $\mathbb{Z}/n\mathbb{Z}$ which have a multiplicative inverse, equipped with the operation of multiplication mod n. This is a group since, by definition, we are only including things which do have an inverse. (The notion $^\times$ is commonly used to extract elements from a set which have a multiplicative inverse. For instance, we previously used $\mathbb{R}^\times$ to denote the set of nonzero real numbers, which are precisely the real numbers which have a multiplicative inverse, and we could also write $\mathbb{Z}^\times = \{\pm 1\}$.) In the $n = 6$ case, it turns out that

$$(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$$

since only 1 and 5 have multiplicative inverses mod 6. (The fact that $4 \cdot 3 \equiv 1 \bmod 6$ prevents 4 from having an inverse.)

It is no coincidence that in the $n = 6$ case the two elements $1, 5$ which have multiplicative inverses are precisely those which are relatively prime to 6—this is true in general:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$$

where *gcd* denotes the *greatest common divisor*. The reason as to why comes from a result in number theory known as *Bezout's Lemma*:

> The greatest common divisor of $a, n \in \mathbb{Z}$ is the smallest positive integer which can be expressed as $ax + ny$ for $x, y \in \mathbb{Z}$.

(We will not prove this here since this is not a course in number theory, but it is a nice little exercise to do on your own if you have never seen it before.) With this at hand, we see that there exists $x \in \mathbb{Z}$ satisfying $ax \equiv 1 \bmod n$ if and only if there exists $k \in \mathbb{Z}$ such that $ax - 1 = nk$ (by definition of equivalence mod n), which after rearranging as $ax + n(-k) = 1$ we see is true if and only if the greatest common divisor of a and n is 1 by Bezout's Lemma. Thus, we have a complete description of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$; in particular, if p is prime, then $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \dots, n-1\}$ consists of all nonzero elements of $\mathbb{Z}/p\mathbb{Z}$, which will be an important observation later.

Lecture 3: Dihedral Groups

Warm-Up 1. We say that an element g of a group G *generates* G if everything in G can be written as a product of copies of g or its inverse. In other words, $G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$, where we interpret g^0 as the identity and g^{-k} as $(g^{-1})^k$. If such $g \in G$ exists, we say that G is *cyclic*. For instance, all additive groups $\mathbb{Z}/n\mathbb{Z}$ are cyclic, generated by 1 in each case.

We find all elements which generate the multiplicative groups $(\mathbb{Z}/7\mathbb{Z})^\times$ and $(\mathbb{Z}/9\mathbb{Z})^\times$, which are in fact cyclic. First, we have

$$(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}.$$

The powers (computed mod 7) of each of these are:

g	g^2	g^3	g^4	g^5	g^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Thus we see that 3 and 5 are the only elements which generate all of $(\mathbb{Z}/7\mathbb{Z})^\times$. (They have order 6, which matches up with the order of $(\mathbb{Z}/7\mathbb{Z})^\times$.) Note that once we knew 3 was a generator, we could have immediately concluded that 5 would also be generator, since $5 = 3^{-1}$: saying that all elements of G can be written in terms of g and g^{-1} alone, is the same as saying that all elements can be written in terms of g^{-1} and $(g^{-1})^{-1} = g$ alone.

For $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$, we have:

g	g^2	g^3	g^4	g^5	g^6
1	1	1	1	1	1
2	4	8	7	5	1
4	7	1	4	7	1
5	7	8	4	2	1
7	4	1	7	4	1
8	1	8	1	8	1

Thus, 2 and $2^{-1} = 5$ generate $(\mathbb{Z}/9\mathbb{Z})^\times$, and no other elements do.

In general, it is true that for p prime, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. (We will see this later—next quarter—as a special case of the general fact that "the group of units of a finite field is cyclic".) However, this is not an if and only if, as the case of $(\mathbb{Z}/9\mathbb{Z})^\times$ shows.

Warm-Up 2. We show that $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic, by showing that no element generates the entire group. We have

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}.$$

In this case, we have: $3^2 = 1, 5^2 = 1$, and $7^2 = 1 \bmod 7$, so no element generates everything, since such an element would necessarily have order 4 in this case. In particular, all odd powers of $3, 5, 7$ result in the $3, 5, 7$ respectively, and all even powers result in the identity.

Orders in products. We briefly stated last time that *products* of the cyclic groups $\mathbb{Z}/n\mathbb{Z}$ in fact give rise to "all" possible finite abelian groups, so let us just say a bit more about the structure of such products. First, note that the $(\mathbb{Z}/8\mathbb{Z})^\times$ example above is an abelian group with 4 elements, so if our claim about classifications of such groups is accurate, $(\mathbb{Z}/8\mathbb{Z})^\times$ should be the "same" as either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $(Zn8)^\times$ is not cyclic, it cannot be the same as $\mathbb{Z}/4\mathbb{Z}$—which is cyclic—which leaves $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as the only possibility. The idea is that if we think of $3 \in (\mathbb{Z}/8\mathbb{Z})^\times$ as corresponding to the element $(1, 0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $5 \in (\mathbb{Z}/8\mathbb{Z})^\times$ as corresponding to $(0, 1) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 1 as corresponding to $(0, 0)$, and 7 to $(1, 1)$, then the *structure* of these two groups are essentially the same:

$$3 \cdot 5 = 7 \text{ mimics } (1, 0) + (0, 1) = (1, 1),\ (5 \cdot 7) = 3 \text{ mimics } (0, 1) + (1, 1) = (1, 0),\ \text{etc.}$$

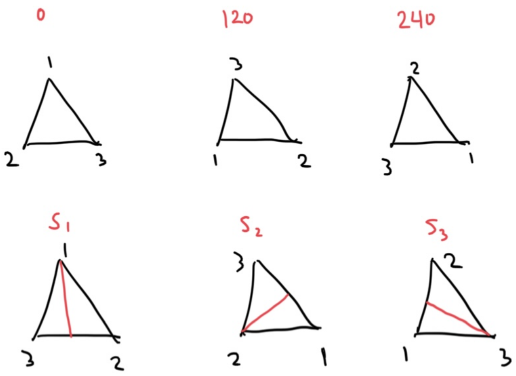
(The correct language is that $(\mathbb{Z}/8\mathbb{Z})^\times$ is *isomorphic* to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, which is a term we will soon define.)

Second, note that orders in product groups in general are simple to compute. If g has order n in G, and h has order m in H, then (g, h) will have order in $G \times H$ equal to the least common multiple of n and m. The point is that if g has order n, then only powers of g which are multiples of n will result in the identity, and similarly for h and multiples of m, so that both powers "match up" in the correct way needed to give (e_G, e_H) precisely when we take the least common multiple and multiples of it. For instance, $(2, 1) \in \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ has order $3 \cdot 8 = 24$ since 2 has order 3 in the first factor and 1 has order 8 in the second, and $(1, 2)$ has order $lcm(6, 4) = 12$.

Dihedral groups. For $n \geq 3$, we define the *dihedral group* D_{2n} to be the set of symmetries/rigid motions of a regular n-gon, which is a group under composition:

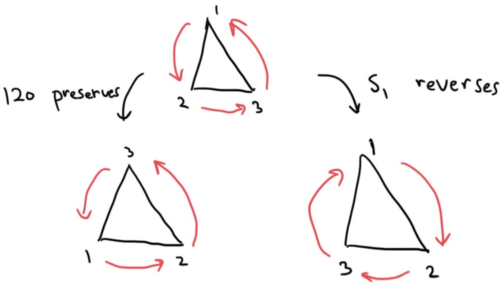
$$D_{2n} := \{\text{symmetries of a regular } n\text{-gon}\}.$$

(The $2n$ refers to the number of elements overall. Be aware: another common notation for this group is D_n where n is instead the number of vertices. Apparently, algebraists prefer to use D_{2n} whereas geometers prefer D_n. Being a geometer myself, I do prefer D_n, but will use D_{2n} to align with the book.) We looked at the $n = 4$ case back on the first day, and similar to that example it is the case that D_{2n} in general consists of n rotations and n reflections. For instance, D_6, the rigid motions of a triangle, consists of counterclockwise rotations by $0, 120, 240$, and reflections s_1, s_2, s_3, each across a line passing through a vertex and the midpoint of the opposite side:



Using the labeled vertices, we can compute products such as $s_1 \cdot 120 = s_2$, recalling that on the left we first rotate by 120 and then reflect using s_1.

Rotations and reflections. Let us take a brief aside to recall/introduce some facts about rotations and reflections from linear algebra. In the computation $s_1 \cdot 120 = s_2$ above, it was in fact possible to know beforehand that $s_1 \cdot 120$ would result in a reflection, using the observation that rotations *preserve orientation* whereas reflections *reverse* orientation. That is, given a counterclockwise orientation of the vertices 1 to 2 to 3 to 1, rotations maintain this counterclockwise nature while reflections turn it into a clockwise ordering:



From this one can see that products of two orientation-preserving transformations are still orientation-preserving, as are products of two orientation-reversing transformations, while the product of a transformation which preserves orientation with one which reverses it will itself be orientation-reversing. Thus, $s_1 \cdot 120$ must be a reflection. (Of course, to see that this reflection is s_2 requires actual computation.)

For another perspective, the rotations and reflections of D_{2n} can each be described via 2×2 matrices; for instance

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

describes counterclockwise rotation by an angle of θ. The orientation-preserving or reversing nature of each is reflected in the determinant: rotations by determinant 1 and reflections have determinant -1. Then again we see from $\det(AB) = (\det A)(\det B)$ what to expect when composing two elements of D_{2n}, in terms of whether the result is a rotation or a reflection.

Generators and relations. Returning to D_{2n} in general, using the discussion above we can come up with a simpler way of describing its elements and group structure. We let r denote *clockwise* rotation by $\frac{2\pi}{n}$. (We could have very well let r denote the counterclockwise rotation instead, but again I'll use the convention the book uses. So, in the case of a square, r denotes what we previously called 270.) Then $1, r, r^2, \ldots, r^{n-1} \in D_{2n}$ give all the rotations, where we denote the identity rotation by 1. If we let s denote reflection across the line segment through vertex 1 (which passes through another vertex when n is even and the midpoint of a side when n is odd), we claim that $s, sr, sr^2, \ldots, sr^{n-1} \in D_{2n}$ give all the reflections, so that explicitly

$$D_{2n} = \left\{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{-1}\right\}.$$

Indeed, from above we know that sr^i in general will be a reflection (orientation-reversing times orientation-preserving), and these are all distinct since $sr^i = sr^j$ implies $r^i = r^j$.

The point is that r and s alone *generate* all of D_{2n}, meaning that every element can be written solely in terms of products of r's and s's and their inverses. Moreover, it turns out that all possible products of elements in D_{2n} can be derived solely from the following *relations*:

$$r^n = 1, \; s^2 = 1, \; rs = sr^{-1}.$$

The first and second come from the orders of r and s, while the third comes from a direct computation. (In the case of a square, with upper-right vertex being the one labeled 1, this third relation becomes $270 \cdot A = A \cdot 90$, which holds since both sides are H.) For instance, for something like r^2sr, we can compute:

$$r^2sr = r(rs)r = r(sr^{-1}r) = (rs)r^{-1}r = rs = sr^{-1} = sr^{n-1}.$$

Thus, the entire group structure can be determined from knowledge of r, s, and these relations. We denote this via the notation:

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle,$$

which is called a *presentation* of the group D_{2n}. The first part of the notation "r, s" gives the generators, and the second "$r^n = s^2 = 1, rs = sr^{-1}$" the relations. Presentations will be a useful way of encoding the data of various groups, where the key is that we have abstracted away any geometric/numerical/whatever meaning, so that we can focus solely on the actual *group* structure within.

Lecture 4: Symmetric Groups

Free groups. Before looking at some Warm-Up problems, we first introduce the following concept in order to give some more context behind the notion of a "presentation". Given a set S, the *free group* on S (or *generated* by S) is the group $\langle S \rangle$ whose elements are the "words" made up of the "letters" in S and their "inverses":

$$\langle S \rangle = \{g_1 g_2 \dots g_k \mid \text{ each } g_i \text{ is in } S \text{ or is the "inverse" of something in } S\}.$$

By the "inverse" of something in S, we mean that for each $s \in S$ we introduce a new symbol (or "letter") s^{-1} to use in our "words". Thus, for instance, if S consists of the letters of the English alphabet, then "algebra" is an element of $\langle S \rangle$, as is "a^{-1}lgeb^{-1}ra".

The point is that we give no other meaning to $g_1 g_2 \dots g_k$ and interpret it solely as a "word" regardless of whether it makes sense to "multiply" g_i and g_j in some way. The group operation is simply *concatenation* of words, were we literally just stick two words together:

$$(g_1 \dots g_k)(h_1 \dots h_\ell) = g_1 \dots g_k h_1 \dots h_\ell.$$

The identity is the *empty word* consisting of no letters at all, and the only additional condition we impose is that whenever we see a letter s and its inverse s^{-1} next to each other, we can get rid of both them in order to force s^{-1} to behave like an inverse of s should. So, for instance, the free group $\langle x, y \rangle$ on two letters x and y consists of expressions of the form $g_1 \dots g_k$ where each g_i is x, y, x^{-1}, or y^{-1}. Thus, we have the following examples of elements:

$$x^2y^3xy^{-3}x, \; yxyxyx^3y^{-2}, \; \text{ and so on.}$$

An example of a product computation is given by:

$$(xy)(y^{-1})x^2 = x(yy^{-1})x^2 = x(\underbrace{\qquad}_{\text{empty word}})x^2 = x^3.$$

All free groups on non-empty sets of generators have infinite order. The free group on a single generator is essentially just $\mathbb{Z}$, if we think of the generator as "1". (More precisely, any free group on a single generator is "isomorphic" to $\mathbb{Z}$.)

With this in mind, we can think about a presentation of a group as the result of taking the free group on the generators and *imposing* some additional relations on top of that. Thus, for the dihedral group

$$D_{2n} = \big\langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \big\rangle,$$

we take the (infinite) free group on two letters r and s, and impose the additional restrictions that r^n and s^2 should be the identity, and rs should equal sr^{-1}. Note how these restrictions turn an infinite group into one with only eight elements. After we discuss the notion of a *quotient group* we will be able to give a more precise meaning to "taking the free group on the generators and *imposing* some additional relations."

Warm-Up 1. We identify, to the extent possible, the groups with the following presentations:

$$\big\langle x \mid x^3 = x^5 = 1 \big\rangle, \quad \big\langle x, y \mid x^2 = y^2 = 1, xy = yx \big\rangle, \quad \big\langle x, y \mid x^2 = y^2 = 1 \big\rangle.$$

In the first case, we note that the given relations imply the following:

$$x^3 = 1 = x^5 \implies 1 = x^2, \text{ so that then } x^2 = 1 = x^3 \implies 1 = x.$$

Thus the presentation $\langle x \mid x^3 = x^5 = 1\rangle$ describes the *trivial* group whose only element is the identity. Note that had we been given only a single relation involving a power of x, like $\langle x \mid x^3 = 1\rangle$, we would get a finite cyclic group, so $\mathbb{Z}/3\mathbb{Z}$ in this case, which is the "only" group generated by a single element of order 3.

For the second presentation, we have two elements x and y of order 2. (Here, the given relations will not force $x = 1$ nor $y = 1$ upon us, so we use the convention that in such a situation we assume that the generators are not identities. The only time a generator will be allowed to be an identity is when that requirement is *required* by the given relations, as was the case in the first presentation above.) This at first elements which look like:

$$xyxyxyxyx, \text{ or more generally "words" alternating in } x\text{'s and } y\text{'s.}$$

There is no need to have more than one x or y in a row since $x^2 = 1 = y^2$, which also shows there is no need to an additional symbol for inverses since $x^{-1} = x$ and $y^{-1} = y$. But now, the additional relation $xy = yx$ (so that x and y commute) allows us to group all the x's together and all the y's together in order to simply this expression down to

$$x^{\text{some power}}y^{\text{some power}},$$

which, depending on types of powers show up here, is either $1, x, y$ or xy since $x^2 = y^2 = 1$. Thus this group only has these four elements:

$$\langle x, y \mid x^2 = y^2 = 1, xy = yx\rangle = \{1, x, y, xy\},$$

and is in fact a presentation of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if we interpret x as $(1, 0)$ and y as $(0, 1)$. (Then xy is $(1, 1)$.) The observation here is that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the "only" group generated by two commuting elements of order 2.

Finally, the third presentation is similar to the one above, only that we drop the restriction that the generators commute. Thus we get elements which are alternating expressions in x and y like

$$xyxyxyxyx$$

only with no way of simplifying this down further. Hence, explicitly this group is:

$$\{g_1 \dots g_k \mid \text{each } g_i \text{ is either } x \text{ or } y, \text{ with no two } x\text{'s or } y'\text{s occurring consecutively}\},$$

with $x^2 = y^2 = 1$ as the only restriction. If we think of x as given a "copy" of $\mathbb{Z}/2\mathbb{Z}$ and y another copy of $\mathbb{Z}/2\mathbb{Z}$ in this group, the resulting group is called the "free product" of $\mathbb{Z}/2\mathbb{Z}$ with itself, and is denoted by $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$. In general, the *free product* $G * H$ of G and H is similar to the notion of a free group in that we take "words" formed by the "letters" in G and H, only that here we do allow ourselves to multiply things in G together and things in H together, but not something thing in G with something in H; so, we can rewrite something like g_1g_2hg as $(g_1g_2)hg$ where g_1g_2 is the product as computed in G, but we cannot rewrite something like ghg in anyway. In $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$, even though both groups are the same, we still do not give any meaning to the "product" xy where $x \in \mathbb{Z}/2\mathbb{Z}$ and $y \in \mathbb{Z}/2\mathbb{Z}$ since they come from different "copies" of $\mathbb{Z}/2\mathbb{Z}$. The notion of a free product will not play a big role going forward, so no worries if the details are still unclear.

Warm-Up 2. We show that $\langle x, y \mid x^2 = y^2 = 1, (xy)^4 = 1\rangle$ is also a presentation of D_8. Comparing to the standard presentation $D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1}\rangle$, we see that neither x nor y behave like the rotation r. Instead, both behave like reflections due to $x^2 = y^2 = 1$. The claim is that D_8 can in fact be generated by (appropriately chosen) reflections. For instance, if we take $x = A$ and $y = H$, then $xy = 90$, and since 90 and A generate everything, so to do A and H. Moreover, $(xy)^4 = 90^4 =$ identity holds here, so we see that the given presentation does indeed describe D_8. The generators are not unique, and picking any two reflections such that xy is either 90 or 270 will work. (In a similar way, even though the book uses $r = 270$ and $s = A$ in the presentation $\langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1}\rangle$, taking $r = 90$ and $s = H$ for instance is just as valid and still gives the correct third relation $rs = sr^{-1}$.)

But, note that if we take $x = H$ and $y = V$, we do not in fact get D_8. In this case x and y commute since $xy = 180 = yx$, and xy has order 2 instead of 4. The point is that when we give the relations as

$$x^2 = y^2 = 1, (xy)^4 = 1,$$

we are again working under the convention that the only additional relations we impose are the ones we can derive from these, and in this case $(xy)^2 = 1$ does not follow from the relations above alone. Thus, $x = H$ and $y = V$ does not give a valid way to interpret x and y in the presentation $\langle x, y \mid x^2 = y^2 = 1, (xy)^4 = 1\rangle$, and neither does $x = A$ and $y = D$ for instance, since these give an additional relation $(xy)^2 = 1$ not derivable from the given ones. For $x = H, y = V$ the correct presentation is

$$\langle x, y \mid x^2 = y^2 = 1, (xy)^2 = 1\rangle,$$

which is precisely the same as the second presentation in Warm-Up 1. (The second Warm-Up from Lecture 2 shows that $x^2 = y^2 = (xy)^2 = 1$ is equivalent to $x^2 = y^2 = 1, xy = yx$.) This reflects the fact that $\{0, 180, H, V\}$ is a subgroup of D_8 which is "isomorphic" to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and similarly if we use $x = A, y = D$ instead. We only get a valid description of D_8 as $\langle x, y \mid x^2 = y^2 = 1, (xy)^4 = 1\rangle$ by taking $x = A, y = H$ or V (or vice-versa), or $x = D, y = H$ or V (or vice-versa). Again, this distinction will become clearer once we give a proper definition of a "presentation" in terms of quotient groups.

Symmetric groups. Given a set Ω, the *symmetric group* S_Ω on Ω (also called the *permutation group* of Ω) is the group of all bijections from Ω to itself:

$$S_\Omega := \{f : \Omega \to \Omega \mid f \text{ is bijective}\}$$

under the operation of composition of functions. The identity is the identity function, and inverses exist because a function is invertible if and only if it is bijective. A bijection will "permute" (i.e. rearrange) the elements of Ω amongst themselves (hence the name "permutation group"), and we think of this as being the most general type of "symmetry" possible: there are no geometric (as in D_{2n}) nor other constraints on this type of symmetry. One of the basic things we will prove later is that *any* (abstract) group can be viewed as a subgroup of a permutation group—in fact in multiple different ways—which fits with the idea that groups in general are things which are used to describe "symmetry" in various contexts.

When Ω is finite, say $\Omega = \{1, 2, \dots, n\}$, we use S_n to denote the corresponding symmetric group and call it the symmetric group on n letters. (The elements of Ω could have been n other things and not necessarily the numbers $1, 2, \dots, n$, but we can always relabel its elements using these numbers without changing the actual group structure.) If we take a permutation (i.e. rearrangement) of 1234 like 3124 for instance (say $n = 4$ in this case), the corresponding function $\{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ is the one which sends each number in 1234 to the number which is now in its location in 3124 after rearranging:

$$1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 4.$$

There are $n!$ many such permutations, so S_n has order $n!$.

Cycles. Thinking of elements S_n as functions is definitely the way to go, but computing products from this perspective seems challenging without having some better notation available to describe these functions. (Thinking about elements as rearrangements of $123 \dots n$ instead makes products even harder to wrap your head around.) So, we now introduce a convenient notation for describing arbitrary permutations, which will make much of their structure clearer.

A *k-cycle* is a permutation (i.e. bijective function) given by the notation

$$(a_1 a_2 \dots a_k), \text{ where } a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\} \text{ are distinct}$$

which we read as saying that a_1 is sent to a_2, a_2 is sent to a_3, a_3 to a_4, and so on, until at the end a_k is sent back (or, "cycles" back) to a_1. By convention, any number not appearing within the cycle is assumed to be sent to itself under the corresponding function. For instance, $(1234) \in S_5$ describes the function which sends:

$$1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1, 5 \mapsto 5.$$

Viewed as an element of S_6 instead, (1234) does the same as above except that it also sends 6 to 6. The identity permutation is usually denoted simply by (1). Note that a different ordering of the numbers within a cycle can in fact describe the same cycle; for instance, (123) is the same as (231) and as (312) since, as *functions*, they do the same thing. The inverse of a cycle is simply obtained by reversing the ordering: $(a_1 a_2 \dots a_k)^{-1} = (a_k \dots a_2 a_1)$.

It is a fact that any permutation in S_n can be written as a product of disjoint cycles, where *disjoint* means that the cycles share no numbers in common. This product decomposition is unique up to the ordering in which the cycles appear, as we will see in some examples. Looking at a few examples makes clear that any permutation can indeed be expressed in this way, but we will give a proper proof later after we have a few more concepts developed.

For instance, let us compute the product (123)(25)(324) by writing the resulting permutation as a product a disjoint cycles. We begin by determining the cycle to which 1 belongs. Recalling that in (123)(25)(324) we read from right to left, we first apply the permutation (324) to 1, resulting in 1 still. (Recall that a number not appearing within a cycle is assumed to be sent to itself.) Next we apply (25) to the resulting 1, which still gives 1. Finally, we apply (123) to 1 to get 2, so overall the permutation given by the product (i.e. composition) (123)(25)(324) sends 1 to 2:

$$(123)(25)(324) = (12\ldots)\ldots$$

with the dots representing things still to-be-determined. We continue on with this same cycle, by next determining what happens to 2: 2 is sent to 4 under (324), and then neither (25) nor (123) affect 4, so overall 2 is sent to 4:

$$(123)(25)(324) = (124\ldots)\ldots$$

Next, 4 is sent to 3 under (324), which is left alone by (25) and is then sent to 1 under (123), so overall 4 is sent to 1, which closes off this first cycle:

$$(123)(25)(324) = (124)\ldots$$

We begin to determine a next cycle by first looking at the smallest number which has not been used up yet, in this case 3: 3 is sent to 2 under (324), which is sent to 5 under (25), which is left alone by (123), so overall 3 is sent to 5:

$$(123)(25)(324) = (124)(35\ldots)\ldots.$$

We can then work out that 5 is sent to 3, so the second cycle is complete and we have our desired disjoint cycle expression:

$$(123)(25)(324) = (124)(35).$$

The manner in which we construct this disjoint cycle expression, by starting each new cycle with a number not used up so far, does suggest that we will necessarily end up with disjoint cycles in the end, but perhaps it is not clear at this point why it is that once a number *is* used up in a cycle, it will not appear again as a non-initial point in any further cycle; again, we will prove this later. Note that disjoint cycles commute, so that we could also write the above as

$$(123)(25)(324) = (124)(35) = (35)(124).$$

Finally, we note that orders are easy to compute in cycle form. The order of a k-cycle is precisely k, since this is the fewest number of "advancements" needed to have each a_i cycle back to itself in $(a_1 \ldots a_k)$. The order of a product of disjoint cycles is then the least common multiple of the individual cycle lengths. For instance, the order of

$$(123)(25)(324) = (124)(35)$$

is $3 \cdot 2 = 6$. Indeed, we have

$$[(124)(35)]^k = \underbrace{(124)(35)(124)(35)\cdots(124)(35)}_{\text{each }(124)(35)\ k\text{ times}} = (124)^k(35)^k,$$

where we use the fact that disjoint cycles commute in order to group all the (124)'s together and (35)'s together, and in order to get the identity k should be a multiple of 3 and 2, the individual cycle lengths. But a warning: it is only with this disjoint cycle form that this least common multiple fact works; for instance, (12)(234) has order 4 since it equals (1234), not order $2 \cdot 3 = 6$.

Lecture 5: Homomorphisms

Warm-Up 1. We show that S_n is generated by its *transpositions*, which is another name for 2-cycles. Indeed, note that

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k).$$

This comes from the fact that for $i \neq k$, a_i first appears in $(a_i a_{i+1})$ in the product on the right (reading right to left), and then a_{i+1} does not appear again as we keep reading to the left, so overall a_i goes to a_{i+1} for $i \neq k$. Then, the product on the right sends a_k to a_{k-1}, which is then sent to a_{k-2}, which is then sent to a_{k-3}, and so on until we end up with a_1 as the result. Taking an arbitrary permutation, writing it as a product of disjoint cycles, and then decomposing each cycle into transpositions as above then proves our claim.

In fact, even more is true: S_n is generated by transpositions of the form $(i\ i{+}1)$, which transpose two consecutive numbers; that is, $(12), (23), (34), \dots, (n-1\ n)$ alone generate S_n. This will be left to the homework, and comes down to showing that an arbitrary transposition can be written as a product of these.

Warm-Up 2. Cutting down the list of generators further, we claim that (12) and $(123 \dots n)$ generate S_n. Indeed, first note that

$$(12 \dots n)(12)(12 \dots n)^{-1} = (23),$$

which comes via a direct computation. (Recall that $(12 \dots n)^{-1} = (n \dots 21)$.) Next:

$$(12 \dots n)(23)(12 \dots n)^{-1} = (34),$$

which is the same as $(12 \dots n)^2 (12)(12 \dots n)^{-2} = (34)$. In general, one can verify that products of the form

$$(12 \dots n)^k (12)(12 \dots n)^{-k}$$

give all the specific transpositions $(12), (23), \dots, (n-1\ n)$. Since these generate S_n, this shows that (12) and $(12 \dots n)$ generate S_n as well.

Set $x = (12)$ and $y = (12 \dots n)$, so that $x^2 = 1$ and $y^n = 1$. We can then work out a relation expressing an alternate form for xy, say with y on the left instead. Doing so would yield a presentation of S_n which looks like:

$$S_n = \langle x, y \mid x^2 = y^n = 1, \text{some } xy \text{ relation} \rangle.$$

However, in this case the presentation is unlikely to be so useful, for now at least. When thinking about S_n we will for now always think of it in terms of explicit permutations, as opposed to a more abstract generators and relations approach. For dihedral groups, on the other hand, the generators and relations approach is often simpler to work with. (For $n = 3, 4$, the geometric definition is probably just as simple, although for larger polygons the geometry is tougher to see.)

D_{2n} as a subgroup of S_n. Here is another perspective on D_{2n}. Each element in fact induces a distinct permutation of the vertices of the n-gon, so that to each permutation we can associate an element of S_n. For instance, in D_8 where we take the standard numbering of the vertices of a square we have used before (upper right vertex is 1, upper left is 2, lower left 3, and lower right 4), the rotation 90 has the following effect on the vertices: $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1$. Thus, 90 corresponds to the 4-cycle (1234). The reflection H gives (23)(14), and other permutations are simple to compute.

The upshot is that in this way we can view D_{2n} as (isomorphic to) a subgroup of S_n. In fact, when $n = 3$ we have that D_6 gives every element of S_3 since all permutations of the vertices are realizable by rotations and reflections, but this is not the case for larger dihedral groups. We thus have three perspectives on what D_{2n} is: a group consisting of rotations and reflections of an n-gon, an abstract group given by generators and relations, and a permutation (sub)group. Each perspective will shed light on different aspects of the structure of D_{2n}.

Some other groups. We mention a few more examples of groups which the book introduces at this point. First, we have already seen the matrix groups $GL_n(\mathbb{R})$ and $GL_n(\mathbb{Z})$. We can replace $\mathbb{R}$ and $\mathbb{Z}$ by other objects, and obtain for instance $GL_n(\mathbb{C})$, the group of invertible *complex* matrices, and $GL_n(\mathbb{Z}/m\mathbb{Z})$. (A matrix with entries in $\mathbb{Z}/m\mathbb{Z}$ is invertible if and only if its determinant is in $(\mathbb{Z}/m\mathbb{Z})^\times$, a fact whose proof is similar to analogous fact for $GL_n(\mathbb{Z})$.) Of particular interest is $GL_n(\mathbb{Z}/p\mathbb{Z})$ for p prime, which we will look more carefully later.

The *quaternion group* is the group of order 8 given by the elements:

$$Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$$

under multiplication. Here we interpret i, j, k all as "square roots" of -1, so that $i^2 = j^2 = k^2 = -1$. In addition, the products of these can be determined from

$$ij = k \qquad jk = i \qquad ki = h.$$

This group is non-abelian (for instance one can work out that $ji = -k$), and is distinct from D_8. (We will look at more general *quaternions* $a + bi + cj + dk$ next quarter, as a 4-dimensional generalization of complex numbers.)

Homomorphisms. So far we have considered standalone groups on their own, but now we move towards considering how groups relate to one another. The key notion which allows us to do so in that of a homomorphism:

> A *homomorphism* from a group G to a group H is a function $\phi : G \to H$ such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. (We say that ϕ *preserves multiplication.*)

To be clear, the product $g_1 g_2$ on the left uses the operation of G and the product $\phi(g_1)\phi(g_2)$ on the right uses the operation of H. The point is that ϕ relates these two operations to each other.

One basic consequence of this definition is that ϕ must send the identity e_G of G to the identity e_H of H. Indeed, since $e_G e_G = e_G$, we have:

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G),$$

and multiplying by $\phi(e_G)^{-1}$ gives $\phi(e_G) = e_H$ as claimed. In a similar way, one can show that $\phi(g)^{-1} = \phi(g^{-1})$ for any $g \in G$: $\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e_G) = e_H$ and multiply by $\phi(g)^{-1}$.

Examples. Here are a couple of first examples. First, for any $n \in \mathbb{Z}$, "multiplication by n " gives a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$: $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = nx$ for all $x \in \mathbb{Z}$. The fact that this preserves "multiplication" (which is actually addition in this case) is the distributive property:

$$n(x + y) = nx + ny.$$

For another example, take $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ to be the map which sends an invertible matrix to its determinant. It is a basic property of determinants that $\det(AB) = (\det A)(\det B)$, which is the multiplication-preservation requirement.

Another example. Let us determine *all* homomorphisms $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. There are 4^5 possible functions between these sets, coming from the fact that each of the 5 elements can be sent to one of 4 possible values, but the homomorphism condition places a strong restriction on which of these functions are actually homomorphisms. The key observation is that since the domain $\mathbb{Z}/5\mathbb{Z}$ is cyclic, any homomorphism is completely determined by the value of $\phi(1)$, or more generally the value of ϕ on any generator. Indeed, if we know $\phi(1)$, then we know

$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1), \text{ and } \phi(k) = \underbrace{\phi(1) + \cdots + \phi(1)}_{k \text{ times}}.$$

So, we are down to figuring out the possible values of $\phi(1)$, of which at first glance there are at most 4. But now, since 1 has order 5 in the domain, it must be true that

$$\phi(1) + \phi(1) + \phi(1) + \phi(1) + \phi(1) = \phi(5) = \phi(0) = 0,$$

where at the end we use the fact that homomorphisms send identities to identities. Thus, the value of $\phi(1)$ in $\mathbb{Z}/4\mathbb{Z}$ must have order dividing 5, which leaves order 1 as the only possibility. Hence we must have $\phi(1) = 0$, which then forces everything in the domain to be sent to zero, so that there is only one homomorphism $\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.

Isomorphisms. We can now make the idea that two groups are the "same" precise:

> An *isomorphism* $G \to H$ is a homomorphism which is bijective, or equivalently invertible. We say that two groups G and H are *isomorphic* if there exists an isomorphism between them, and denote this by $G \cong H$.

An isomorphism $G \to H$ thus gives a way to move back and forth between elements of G and H, all while preserving the group operations at every step along the way. It is in this sense that should think of G and H as being the "same" group, since any property which G has H will have, and vice-versa; the point is that group the *structure* of isomorphic groups is the same, even if the elements and group operations "look different". Various notions we have seen are preserved by isomorphisms, such as the properties of being abelian or cyclic, orders of elements, the *number* of elements of a given order, etc.

If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is automatically a homomorphism as well, which comes from applying ϕ^{-1} to both sides of

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$

and doing some rewriting.

Examples. Back in the first Warm-Up of Lecture 3 we showed that the multiplicative groups $(\mathbb{Z}/7\mathbb{Z})^\times$ and $(\mathbb{Z}/9\mathbb{Z})^\times$ were both cyclic of order 6, which proves that each is isomorphic to the additive $\mathbb{Z}/6\mathbb{Z}$:

$$(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z} \quad \text{and} \quad (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}.$$

Explicit isomorphisms $\phi : (\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{Z}/6\mathbb{Z}$ and $\psi : (\mathbb{Z}/9\mathbb{Z})^\times \to \mathbb{Z}/6\mathbb{Z}$ can be described by sending generators to generators: set $\phi(3) = 1$ and $\psi(2) = 1$, which determine everything else. For instance, since $3^2 = 2$ in $(\mathbb{Z}/7\mathbb{Z})^\times$, we have

$$\phi(2) = \phi(3 \cdot 3) = \phi(3) + \phi(3) = 1 + 1 = 2 \text{ in } \mathbb{Z}/6\mathbb{Z}.$$

(To be clear, the inputs into ϕ uses multiplication mod 7, while the outputs use addition mod 6.)

As another example, which we have seen, the subgroup $\{0, 180, H, V\}$ of D_8 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. An explicit isomorphism $\phi : \{0, 180, H, V\} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is given by

$$\phi(0) = (0,0) \quad \phi(H) = (1,0) \quad \phi(V) = (1,0) \quad \phi(180) = (1,1).$$

The homomorphism requirement is reflected in the fact that $H \cdot V = 180$ corresponds to $(1,0) + (0,1) = (1,1)$. Also note that all non-identity elements in both groups have order 2.

Classifying groups. And now with what we have developed so far, we claim that we can give a complete list of all groups of order at most 11, meaning that any group of order at most 11 will be isomorphic to exactly one in this list. To be clear, we do not yet have all the tools needed to *prove* that this list is complete, but we have enough to describe the groups in the list.

First, there are the cyclic groups $\mathbb{Z}/n\mathbb{Z}$ for $n \leq 11$. There are also products of these, at least products whose orders are at most 11. For instance, in the order 9 case, every group of order 9 turns out to be isomorphic to either $\mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Next, there are the dihedral groups D_{2n} for $n \leq 5$. The symmetric group S_3 has order 6, but this is actually isomorphic to D_6 (recall how the rotations and reflections of a triangle induce every possible permutation of the vertices) and so is already on the list.

The only remaining group occurs in the order 8 case, where the full list of groups of order 8 is:

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad D_8 \quad Q_8,$$

where Q_8 is the quaternion group we introduced earlier in this lecture. (This is why we introduced this group now, so that we could fully characterize all groups of order 8.) We will soon develop the tools needed to justify all this, and will in fact work our way up towards larger orders, say order at most 60 if we want a complete list.

Lecture 6: Group Actions

Warm-Up 1. We determine the number of homomorphisms from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ to D_8. There are 8^8 total such *functions*, but the homomorphism conditions cuts down the possibilities much further. The key observation is that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is generated by two elements, one $(1,0)$ of order 2 and one $(0,1)$ of order 4, which commute. A homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to D_8$ is completely determined by its values on generators, since in this case for instance we have:

$$\phi(m,n) = \phi(m(1,0) + n(0,1)) = \phi(1,0)^m \phi(0,1)^n$$

to due to preservation of multiplication.

Now, since $(1,0)$ has order 2 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\phi(1,0)$ must have order dividing 2, meaning order 1 or 2. Thus the only possibilities are:

$$\phi(1,0) = 0, 180, H, V, D, A.$$

Since $(0,1)$ has order 4 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\phi(0,1)$ must have order dividing 4, but everything in D_8 has order dividing 4 so this places no restrictions on what $\phi(0,1)$ can be. However, since $(1,0)$ and $(0,1)$ commute, it must be the case that $\phi(1,0)$ and $\phi(0,1)$ commute as well:

$$\phi(1,0)\phi(0,1) = \phi((0,1) + (1,0)) = \phi((1,0) + (0,1)) = \phi(0,1)\phi(1,0).$$

This restricts the possible values of $\phi(0,1)$, since for instance $\phi(1,0) = H$ and $\phi(0,1) = D$ is not valid since these do not commute.

Thus we can now count the possibilities. When $\phi(1,0) = 0$ or 180, $\phi(0,1)$ can be anything since every element of D_8 commutes with both 0 and 180. This gives $8 + 8 = 16$ homomorphisms so far. When $\phi(1,0) = H$ or V, then $\phi(0,1)$ can only be $0, 180, H$ or V since these are the only things which commute with H or V. This gives another $4 + 4 = 8$ possibilities. Finally, when $\phi(1,0) = D$ or A, we get that $\phi(0,1)$ can only be $0, 180, D$, or A, giving $4 + 4 = 8$ more homomorphisms. We conclude that there are $16 + 8 + 8 = 32$ homomorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to D_8$ in total.

Warm-Up 2. Assuming the result that any finite abelian group is isomorphic to a direct product of cyclic groups $\mathbb{Z}/n\mathbb{Z}$ (to be proved later), we determine the product to which the abelian multiplicative group $(\mathbb{Z}/15\mathbb{Z})^\times$ is isomorphic. Since this group has order 8:

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\},$$

the possible products of cyclic groups are:

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

(Note that $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ via the homomorphism $(a, b) \mapsto (b, a)$ which swaps components, so it is in fact included in the list above.)

To determine which of these is our group, we compute the orders of elements in $(\mathbb{Z}/15\mathbb{Z})^\times$.

element	1	2	4	7	8	11	13	14
order	1	4	2	4	4	2	4	2

Right away we can rule out $\mathbb{Z}/8\mathbb{Z}$, since there is no element of order 8 and hence $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic, as would be required in order to be isomorphic to $\mathbb{Z}/8\mathbb{Z}$. Since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no element of order 4, this cannot be isomorphic to $(\mathbb{Z}/15\mathbb{Z})^\times$ either since isomorphisms preserve orders of elements.

Thus $(\mathbb{Z}/15\mathbb{Z})^\times$ must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Indeed, the orders of elements match up: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has four elements of order 4:

$$(0, 1), (0, 3), (1, 1), (1, 3)$$

and three elements of order 2:

$$(0, 2), (1, 2), (1, 0).$$

If we assume, as we said we would, that any finite abelian group is isomorphic to a product of cyclic groups, then we are done. But, we will construct an explicit isomorphism

$$\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/15\mathbb{Z})^\times$$

anyway. In general, constructing explicit isomorphisms is not always straightforward, but we will develop enough theory later so that this is usually not necessary. In this case, let us first set

$$\phi(0, 1) = 2$$

since we need $\phi(0, 1)$ to be an element of order 4 in $(\mathbb{Z}/15\mathbb{Z})^\times$. (This is not the only possibility.) Then, since ϕ should be a homomorphism, we get:

$$\phi(0, 2) = \phi(0, 1)^2 = 4 \text{ and } \phi(0, 3) = \phi(0, 1)^3 = 8.$$

Now let us set

$$\phi(1,0) = 11.$$

Then everything else is determined:

$$\phi(1,1) = \phi(1,0)\phi(0,1) = 7 \quad \phi(1,3) = \phi(1,0)\phi(0,1)^3 = 13 \quad \phi(1,2) = 14$$

and of course $\phi(0,0) = 1$. This then defines an explicit bijection $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/15\mathbb{Z})^\times$, which is a homomorphism because we computed everything from knowledge of $\phi(1,0)$ and $\phi(0,1)$ alone precisely in order to force it to be a homomorphism.

Products of cyclic groups. Let us briefly note that it is simple to determine when a product of cyclic groups is itself cyclic. For instance, it is true that $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Indeed, $(1,1)$ in the former group has order equal to the least common multiple of 2 (the order of 1 in the first factor) and 3 (the order of 1 in the second factor), and so is 6. Since $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ has order 6 and has an element $(1,1)$ of order 6, it is generated by this element and hence is cyclic. Thus $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ (sending a generator to a generator always gives rise to an isomorphism), so that $\mathbb{Z}/6\mathbb{Z}$ is in fact the only abelian group of order 6, up to isomorphism.

In general $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ is cyclic, and hence isomorphic to $\mathbb{Z}/mn\mathbb{Z}$ if and only if m and n are relatively prime. Indeed, being relatively prime is equivalent to having their least common multiple be mn, which is the condition needed to have $(1,1)$—or anything of the form (generator,generator)—be of order mn. This extends to products of more than two cyclic groups, so that for instance:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

are all isomorphic, so that there is only one abelian group $\mathbb{Z}/30\mathbb{Z}$ of order 30.

Group actions. The notion of a group action gives a general way in which we can view a given group as a group of "symmetries", in multiple ways. First, we give some notation. Given a function

$$G \times X \to X$$

where G is a group and X a set, we will denote the element of X to which (g,x) is sent as $g \cdot x$, which we think of as "g acting on x":

$$(g,x) \mapsto g \cdot x.$$

An *action* of G on X is then a map $G \times X \to X$ such that:

- $e \cdot x = x$ for all $x \in X$, and
- $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

The first requirement says that the identity should "act as the identity", and the second says that "composing" actions should correspond to multiplication. We will often use the notation $G \curvearrowright X$ to mean that G acts on X, or in other words that there is a group action of G on X.

Examples. $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by the usual product of a matrix and a vector: $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ defined by $A \cdot \mathbf{x} = A\mathbf{x}$ for $A \in GL_n(\mathbb{R})$ and $\mathbf{x} \in \mathbb{R}^n$. Certainly the identity matrix I satisfies $I\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$, and the second requirement in the definition of an action comes from the way in which the product of two matrices is defined: $A(B\mathbf{x}) = (AB)\mathbf{x}$.

The definition we gave for the symmetric group S_n comes precisely from viewing S_n as acting on $\{1, 2, \ldots, n\}$: $S_n \curvearrowright \{1, 2, \ldots, n\}$ is defined by $\sigma \cdot x = \sigma(x)$ for all $x \in \{1, 2, \ldots, n\}$, where $\sigma(x)$

is the result of applying the bijection σ to x. And as a final example, the fact that any rotation or reflection of a regular n-gon permutes the vertices can be viewed as defining an action of D_{2n} on $\{1,2,\dots,n\}$: label the vertices of the n-gon using $1,2,\dots,n$, and define $D_{2n} \curvearrowright \{1,2,\dots,n\}$ by having $g \in D_{2n}$ permute the vertices. For instance, if we take the standard counter-clockwise labeling of the vertices of a square with 1 in the upper-right corner, the rotation $90 \in D_8$ acts as: $90 \cdot 1 = 2, 90 \cdot 2 = 3, 90 \cdot 3 = 4, 90 \cdot 4 = 1$; in other words, 90 acts as the cycle (1234).

Homomorphisms to permutation groups. The data of an action of G on X can be rephrased more compactly as follows. For each $g \in G$, acting on each element of X by g induces a function $x \mapsto g \cdot x$ from X to X. This function is in fact bijective, with inverse given by the function induced by g^{-1}; that is, the composition of the function induced by g with the function induced by g^{-1}, in either order, is the identity function:

$$g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

and

$$g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x$$

for all $x \in X$. Thus we can view the action as giving a map $G \to S_X$, where S_X is the group of permutation (i.e. bijective functions) on X:

$$\text{send } g \in G \text{ to the permutation defined by } x \mapsto g \cdot x.$$

The second requirement in the definition of an action then says precisely that this map $G \to S_X$ is a homomorphism, since multiplication in G corresponds to composition in S_X. Conversely, given a homomorphism $G \to S_X$, we can get an action of G on X by having $g \in G$ act on X by the corresponding element of S_X. The upshot is that an action of G on X is the same as a homomorphism $G \to S_X$, and it is in this way that we can view an action as giving a way to interpret G as a group of permutations on X. The power of this idea will come from applying it to different possible sets X in order to extract information about G.

Lecture 7: Some Subgroups

Warm-Up 1. Given an action of G on X and an element $x \in X$, we define two important sets associated with the action: the *orbit* Gx through and the *stabilizer* G_x of x by:

$$Gx := \{g \cdot x \mid g \in G\} \quad \text{and} \quad G_x := \{g \in G \mid g \cdot x = x\}.$$

The orbit through x is thus the subset of X consisting of all things obtained by acting on x by various group elements, and the stabilizer of x is the subset of G consisting of all group elements which *fix*, or *stabilize*, x. In fact, stabilizers are subgroups of G, as can be seen from:

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \quad \text{and} \quad g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

when $g \cdot x = x$ and $h \cdot x = x$.

Let $SO_3(\mathbb{R})$ denote the group of 3×3 orthogonal matrices of determinant 1, which geometrically represent 3-dimensional rotations. (The "*SO*" stands for "special orthogonal"; the term "special" in this context refers to the determinant 1 condition.) Then $SO_3(\mathbb{R}) \curvearrowright \mathbb{R}^3$ by matrix multiplication. We describe the orbits and stabilizers of this action.

For $\mathbf{x} \in \mathbb{R}^3$, applying any rotation to $\mathbf{x}$ results in a vector of the same length as $\mathbf{x}$, and as we vary the rotation used we obtain all possible such vectors. This says that the orbit through $\mathbf{x}$ is the sphere centered at the origin of radius $\mathbf{x}$:

$$SO_3(\mathbb{R})\mathbf{x} = \text{sphere of radius } \mathbf{x} \text{ centered at } \mathbf{0}.$$

(We allow here for a sphere of radius 0, which arises when $\mathbf{x} = \mathbf{0}$.) The *orbit space* of this action, which is the set of orbits, is the collection of all spheres centered at the origin.

For $\mathbf{x} \in \mathbb{R}^3$, the stabilizer of $\mathbf{x}$ consists of all those rotations which leave the vector $\mathbf{x}$ unchanged:

$$SO_3(\mathbb{R})_{\mathbf{x}} = \{A \in SO_3(\mathbb{R}) \mid A\mathbf{x} = \mathbf{x}\}.$$

(In more linear-algebraic terms, this is the set of matrices which have $\mathbf{x}$ as an eigenvector of eigenvalue 1, at least in the $\mathbf{x} \neq \mathbf{0}$ case.) For $\mathbf{x} \neq \mathbf{0}$, any such rotation can be viewed as occurring around the "axis" spanned by $\mathbf{x}$, or equivalently as a rotation of the plane passing through the origin which is orthogonal to $\mathbf{x}$. This subgroup of $SO_3(\mathbb{R})$ is in fact isomorphic to $SO_2(\mathbb{R})$, the group of 2-dimensional rotations. For instance, if $\mathbf{x}$ is on the z-axis, then the plane orthogonal to x is the xy-plane, which we can identity with $\mathbb{R}^2$, so that rotations of the xy-plane around the z-axis are indeed the same thing as elements of $SO_2(\mathbb{R})$. An explicit isomorphism $SO_2(\mathbb{R}) \to SO_3(\mathbb{R})_{\mathbf{x}}$ in this case is given by:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mapsto \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

where θ is the angle of rotation. By viewing any plane through the origin as isomorphic (in the linear-algebraic) sense to $\mathbb{R}^2$, we can similarly view any stabilizer of this action as being isomorphic to $SO_2(\mathbb{R})$. (The isomorphism between the stabilizer and $SO_2(\mathbb{R})$ in general is tougher to write down, but can be obtained via a "change of basis", which we will recall after the second Warm-Up.)

Warm-Up 2. We show that $g \cdot h := ghg^{-1}$ defines an action of a group G on itself, which we call the *conjugation* action. We also show that this is actually an action by *automorphisms*, which means that the bijection on G induced by each $g \in G$ is actually a group isomorphism. (An isomorphism $G \to G$ is called an *automorphism* of G, and the set $\operatorname{Aut}(G)$ of all such automorphisms is a group under composition. The claim here is that the map $G \to S_G$ obtained from the conjugation action actually has image contained in $\operatorname{Aut}(G) \subseteq S_G$, and so can be viewed as a homomorphism $G \to \operatorname{Aut}(G)$. In general, actions coming from homomorphisms $G \to \operatorname{Aut}(H)$, where H is some group, will play a special role in understanding the structure of abstract groups.)

First we have:

$$e \cdot h = ehe^{-1} = ehe = h \text{ for all } h \in G,$$

so e acts as the identity. Second, for any $g, k \in G$, we have:

$$g \cdot (k \cdot h) = g \cdot (khk^{-1}) = gkhh^{-1}g^{-1} = (gk)h(gk)^{-1} = (gk) \cdot h$$

for all $h \in H$. Thus conjugation is indeed an action of G on itself. (Note here we use the fact that $(ab)^{-1} = b^{-1}a^{-1}$ is true in any group.)

Finally, to say that this is an action by automorphisms means that:

$$g \cdot (h_1 h_2) = (g \cdot h_1)(g \cdot h_2)$$

for all $g, h_1, h_2 \in G$, since this is what it means for the induced map $G \to G$ defined by $h \mapsto g \cdot h$ to preserve multiplication. We check:

$$g \cdot (h_1 h_2) = g h_1 h_2 g^{-1} = g h_1 (g^{-1} g) h_2 g^{-1} = (g h_1 g^{-1})(g h_2 g^{-1}) = (g \cdot h_1)(g \cdot h_2)$$

as required. Thus G acts on itself by automorphisms under conjugation.

Example. Let us give an example of the conjugation action, which has a well-known interpretation in linear algebra. Take $GL_n(\mathbb{R})$ acting on itself by conjugation. Two matrices $A, B \in GL_n(\mathbb{R})$ are conjugate—meaning one can be obtained from the other after conjugating by some matrix—if there exists $S \in GL_n(\mathbb{R})$ such that $B = SAS^{-1}$. (In other words, A and B lie in the same orbit of the conjugation action.) The standard term for this scenario in linear algebra is that A and B are *similar* matrices, so similarity is just an instance of group conjugacy. In general, the orbits of the conjugation action are called the *conjugacy classes* of the group, so here to say that two matrices are similar just means that they lie in the same conjugacy class.

Now, you might recall the important fact from linear algebra that similarity corresponds exactly to performing a *change of basis*; that is, similar matrices describe the same linear transformation only with respect to possibly different bases. To make a connection with the first Warm-Up, recall we noted above that the stabilizer of $\mathbf{x}$ under the multiplication action of $SO_3(\mathbb{R})$ consisted of the subgroup of rotations which rotated the plane orthogonal to x, and that this could be viewed as being isomorphic to the group $SO_2(\mathbb{R})$ of 2-dimensional rotations. Now we can be more precise: any element of the stabilizer $SO_3(\mathbb{R})_{\mathbf{x}}$ is similar to an element of the "copy" of $SO_2(\mathbb{R})$ in $SO_3(\mathbb{R})$ consisting of those matrices of the form

$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which described rotations of the xy-plane. If we pick a basis for $\mathbb{R}^3$ consisting of $\mathbf{x}$ (in the $\mathbf{x} \neq \mathbf{0}$ case) and two vectors orthogonal to $\mathbf{x}$ and to each other (so spanning the plane orthogonal to $\mathbf{x}$), the matrix of a linear transformation in the stabilizer with respect to this basis will indeed be equal to one of the form above. Thus, by *conjugating* matrices of the form above, we can obtain rotational matrices around any axis spanned by a nonzero vector, and these rotational matrices make up the stabilizer of that vector. In this case then, the conjugacy class of a matrix of the form above consists of all possible rotations of the same angle θ occurring around any axis.

A few more adjectives. The book describes certain properties an action may or may not posses, such as being *faithful*, or *free*, or *transitive*, but we will put-off introducing these terms until they are actually needed.

Subgroups. We have already been informally using the notion of a *subgroup* of a group G, and now we will make this precise. A *subgroup* H of G is a nonempty subset of G which is:

- *closed under multiplication*: $hk \in H$ for all $h, k \in H$ where hk is the product in G, and
- *closed under inversion*: $h^{-1} \in H$ for all $h \in H$, where h^{-1} is the inverse in G.

The point is that H is then itself a group in its own right, under the same operation as on G, only sitting inside of the "larger" group G. (Note that $e_G \in H$ follows from the two properties above and the property of H being nonempty: for $h \in H$, $h^{-1} \in H$, and thus $hh^{-1} = e_G$ is as well.) We use $H \leq G$ notation for H being a subgroup of G.

As the book shows, there are equivalent ways of rephrasing the subgroups conditions: both can be combined into the single requirement that $hk^{-1} \in H$ for $h, k \in H$, and in the finite case the "closed under inversion" property can be dropped since the inverse of any element is a positive power of that element due to the fact that it has finite order. But, we will note really use these shorter descriptions, apart from in a few specific examples later.

Kernels and images. To any homomorphism $\phi : G \to H$ we can associate two important subgroups, one of G and one of H: the *kernel* $\ker \phi \leq G$ and the *image* $\phi(G) \leq H$ defined by

$$\ker \phi := \{g \in G \mid \phi(g) = e_H\} \quad \text{and} \quad \phi(G) := \{\phi(g) \in H \mid h \in G\}.$$

So, in words, the kernel is the set of all things which map to the identity, and the image is the set of all elements obtained as outputs. That these are indeed subgroups of G and H respectively follows from basic properties of homomorphisms, namely: $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ and $\phi(g)^{-1} = \phi(g^{-1})$. We will omit the precise check here, but it should be straightforward. We will discuss the importance of kernels and images later.

Centralizers and normalizers. We finish by introducing two more examples of subgroups, which will play an important role in topics to come. For any subset $A \subset G$, we define its *centralizer* $C_G(A)$ and *normalizer* $N_G(A)$ as follows:

$$C_G(A) := \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\} \quad \text{and} \quad N_G(A) := \{g \in G \mid gAg^{-1} = A\}.$$

(To clarify the notation in the second expression, gAg^{-1} denotes the set of all elements of A of the form gag^{-1} for $a \in A$, and is called the *conjugate* of A by g.)

Since $gag^{-1} = a$ is equivalent to $ga = ag$, we thus see that the centralizer of A in G is precisely the set of all elements of g which commute with *everything* in A:

$$C_G(A) = \{\text{elements of } G \text{ which commute with all elements of } A\}.$$

To say that $gag^{-1} = a$ is to say that g *centralizes* a, or in other words stabilizes a under the conjugation action of G on itself. Now, the condition $gAg^{-1} = A$ in the definition of the normalizer does *not* mean that g commutes with all things in A, only that the *set* of things obtained by conjugating elements of A by g is the same as the set A itself; the point is that gag^{-1} will be an element of A, but will not necessarily equal a itself. (So, note that $C_G(A)$ is contained in $N_G(A)$.) The check that these are both subgroups of G is straightforward, and we omit it here.

In the special case where $A = G$, the centralizer $C_G(G)$ of G in itself is most commonly called the *center* of G and is denoted by $Z(G)$. Thus, the center $Z(G)$ is the subgroup of G consisting of all elements which commute with every element of G. Note G is abelian if and only if $Z(G) = G$.

Example. A problem on Homework 1 computed the center of D_{2n}. The result was that

$$Z(D_{2n}) = \begin{cases} \{1\} & \text{when } n \text{ is odd} \\ \{1, r^{n/2}\} & \text{when } n \text{ is even.} \end{cases}$$

For instance, 180 commutes with everything in D_8, and so belongs to the center of D_8.

Another example. Take the subgroup $\langle r \rangle$ of rotations in D_{2n}. Certainly any rotation commutes with any other rotation, so all rotations belong to the centralizer of $\langle r \rangle$. However, no reflection will commute with *all* rotations, since in particular no reflection commutes with r itself:

$$r(sr^i) = sr^{-1}r^i = sr^{i-1} \neq (sr^i)r = sr^{i+1} \text{ since } r^{i-1} \neq r^{i+1}.$$

Thus $C_{D_{2n}}(\langle r\rangle) = \langle r\rangle$ only consists of the rotations.

However, the normalizer of $\langle r\rangle$ is in fact all of D_{2n}, which means that conjugating a rotation by *any* element of D_{2n} will always result in a rotation. One geometric reason is the fact that composing two reflections and a rotation or three rotations always results in a rotation, by keeping track of the orientation-reversing or orientation-preserving properties. Alternatively, we can compute directly (using $s^{-1} = s$) that:

$$(sr^i)r^j(sr^i)^{-1} = sr^ir^jr^{-i}s = sr^{i+j}sr^i = s^2r^{-i-j}r^i = r^{-j} \in \langle r\rangle.$$

Thus $N_{D_{2n}}(\langle r\rangle) = D_{2n}$ as claimed. (This fact, that the normalizer is the entire group, is what it means to say that $\langle r\rangle$ is a *normal* subgroup of D_{2n}. We will come back to normal subgroups, and their crucial role, soon enough.)

Lecture 8: Cyclic Groups

Warm-Up 1. We give interpretations of centralizers and normalizers in terms of appropriately chosen group actions. Let G be a group with $A \subseteq G$. Just as we introduced the action of G on itself by conjugation, we can also define a conjugation action of G on its *power set* 2^G, which is the set of all subsets of G:

$$G \curvearrowright 2^G := \{S \mid S \subseteq G\} \text{ via } g \cdot S := gSg^{-1}.$$

Recall here that gSg^{-1} is the set of all elements of G expressible as gsg^{-1} for some $s \in S$. (The notation 2^G for the power set of G is standard and comes from recognizing that to specify a subset of G is the same as to specify a function from G to a 2-element set, but we will not elaborate on this here.) That this is an action of G on 2^G can be checked directly.

The point then is that the normalizer $N_G(A)$ of A in G is precisely the stabilizer of A under this conjugation action of G on 2^G:

$$g \in \text{the stabilizer } G_A \iff gAg^{-1} = A \iff g \in N_G(A).$$

This gives one perspective on why $N_G(A)$ is a subgroup of G, since stabilizers are always subgroups. Next, consider now the action of this normalizer $N_G(A)$ on A, also by conjugation:

$$g \in N_G(A) \text{ acts as } g \cdot a := gag^{-1}.$$

(Note here that we act by the normalizer $N_G(A)$ instead of the entire group G solely to guarantee that the induced maps actually map A into A: each $g \in N_G(A)$ defines a bijection $g : A \to A$ by conjugating elements. For $g \notin N_G(A))$, the induced map would map A into some other set, and so would not be considered a permutation of A.) Each stabilizer of this action consists of those $g \in N_G(A)$ which stabilizer some $a \in A$, and so the centralizer $C_G(A)$ of A in G can be viewed as the *intersection* of all such stabilizers:

$$g \in C_G(A) \iff gag^{-1} = a \text{ for all } a \in A \iff g \in \text{the stabilizer } N_G(A)_a \text{ for all } a \in A$$

if and only if $g \in \bigcap_{a\in A} N_G(A)_a$. Since intersections of subgroups are always subgroups, this again gives a reason as to why centralizers are always subgroups. It is common to use the notation $C_G(a)$ to denote the centralizer of the singleton set $\{a\}$, which is the centralizer of a under the conjugation action above. With this notation we can write the stabilizer of A as $\bigcap_{a\in A} C_G(a)$.

But here is one more perspective. The conjugation action of $N_G(A)$ on A can be viewed as defining a homomorphism $\phi : N_G(A) \to S_A$, where S_A is the permutation group of A. The centralizer $C_G(A)$ is then the kernel of this homomorphism: $g \in \ker \phi$ if and only if the map induced by g on A is the identity function, which is true if and only if $gag^{-1} = a$ for all $a \in A$. Kernels are subgroups, and so centralizers are subgroups too.

Warm-Up 2. We determine the center of the group $GL_2(\mathbb{R})$. (The answer generalizes to $GL_n(\mathbb{R})$ for all n, but we use $n = 2$ just to simply the computation.) Suppose $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. This is in center when $AX = XA$ for all $X \in GL_2(\mathbb{R})$. In particular, this requires that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

which gives the conditions

$$a = a + c \qquad a + b = b + d \qquad c + d = d.$$

Hence we need $c = 0$ and $a = d$, so that A looks like $A = \left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right]$. Next, we also need

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & a \end{bmatrix},$$

which boils down to $a + b = a$, so that $b = 0$. Thus $A = \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right]$, so we conclude that the center consists of nonzero scalar multiples of the identity:

$$Z(GL_2(\mathbb{R})) = \{aI \mid a \in \mathbb{R}^\times\}.$$

The analogous statement holds for lager matrices, as can be seen by using other matrices in place of $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$, namely those which are the identity with a 1 in some other location.

Subgroups of cyclic groups. We now seek to give a complete description of all subgroups of a given cyclic group. To get a sense for the claims we will make, let us list concretely all the subgroups of $\mathbb{Z}/6\mathbb{Z}$:

$$\{0\},\ \{0,2,4\},\ \{0,3\},\ \{0,1,2,3,4,5\}.$$

The first observation is that each of these are cyclic, generated by 0, 2 or 4, 3, and 1 or 5 respectively. This holds true in general: any subgroup of a cyclic group is cyclic.

Indeed, suppose $G = \langle x \rangle$ is cyclic, generated by x, and let $H \leq G$ be a nontrivial subgroup. Then all elements of H (and G) can be expressed as powers of x, so let x^k for some $k > 0$ be the smallest positive power of x which is in H. (Such a positive power exists, since if a negative power is in H, its inverse will be positive power which is necessarily in H.) We claim that H is in fact generated by x^k. Pick any $h \in H$. Since $h \in G$ we can express h as a power of x, say $h = x^\ell$ for some $\ell \in \mathbb{Z}$. By the division algorithm there exists $q \in Z$ and $r \in \{0, 1, \ldots, k-1\}$ such that

$$\ell = kq + r.$$

But then we have:

$$x^r = x^{\ell - kq} = x^\ell (x^k)^{-q},$$

which is a product of elements of H is thus in H. But x^k was meant to be the smallest positive power of x which was in H, so since $0 \leq r < k$ we must have $r = 0$. Thus $\ell = kq$, so $x^\ell = (x^k)^q \in \langle x^k \rangle$, which shows that $H = \langle x^k \rangle$.

Orders in cyclic groups. Next we describe the order of any element in a cyclic group. We will restrict ourselves to finite cyclic groups, but the answer for an infinite cyclic group $G = \langle x \rangle$ is that all non-identity elements have infinite order. Going back to the case of $\mathbb{Z}/6\mathbb{Z}$, we see that

$$2, 4 \text{ have order } 3 \qquad 3 \text{ has order } 2 \qquad 1, 5 \text{ have order } 6.$$

The observation is that 3 is precisely 6 divided by the greatest common divisor of 6 and 2 (or 4), 2 is 6 divided by $gcd(3, 6)$, and 6 is $6/gcd(6, 1)$ or $6/gcd(6, 5)$. The claim is that if $G = \langle x \rangle$ is finite of order n, then x^k (for $k \neq 0$) has order $\frac{n}{gcd(n,k)}$.

We will give the proof for completeness, but note that it really is more of a proof about divisibility than it is about group theory. Set $d = gcd(n, k)$ and write n and k as $n = ds, k = d\ell$ for $s, \ell \in \mathbb{Z}$ which are relatively prime. (If they were not relatively prime, there would exist a common divisor of n and k larger than d.) With this notation, $\frac{n}{gcd(n,k)} = \frac{n}{d} = s$, so we first check:

$$(x^k)^s = x^{ks} = x^{d\ell s} = (x^n)^l = 1$$

since x has order n. For now denote the order of x^k by t, so that the above implies t divides s. Next, since x^k has order t we have

$$(x^k)^t = x^{kt} = 1,$$

so that n (the order of x) divides kt. Using the expressions for $n = ds$ and $k = d\ell$ from above, this gives that ds divides $d\ell t$, which implies s divides ℓt. Since s and ℓ are relatively prime, we have that s divides t. Hence s and t are positive and divide each other, so we get $\frac{n}{gcd(n,k)} = s = t = |x^k|$ as required.

Counting subgroups of cyclic groups. We know that all subgroups of a cyclic group are cyclic, and the final fact we need in order to describe all such subgroups (in the finite case) more explicitly is the following: if G is cyclic of order n, then for each divisor k of n there is a unique subgroup of G of order k, and moreover these are the only subgroups of G. Thus, the subgroups of a finite cyclic group correspond precisely to the divisors of n in a 1-to-1 manner. We will postpone the proof of this to next time.

Lecture 9: Generating Sets

Warm-Up 1. We identity the automorphism group $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ in terms of a better known group. Since the domain is cyclic, an automorphism $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is fully determined by its value on a generator, so in particular by the value of $\psi(1)$. This element generates a subgroup of $\mathbb{Z}/n\mathbb{Z}$, and so in order for ψ to be surjective (which is equivalent to injective since $\mathbb{Z}/n\mathbb{Z}$ is finite) this subgroup must be all of $\mathbb{Z}/n\mathbb{Z}$, meaning that $\psi(1)$ must be a generator of $\mathbb{Z}/n\mathbb{Z}$. By what we know about the structure of cyclic groups, $k \in \mathbb{Z}/n\mathbb{Z}$ has order

$$\frac{n}{gcd(k, n)},$$

and thus this equals n if and only if $gcd(k, n) = 1$. We conclude that $\psi(1)$ must be relatively prime to n in order for ψ to be an automorphism.

The number of positive integers smaller than n which are relatively prime is commonly denoted by $\phi(n)$, where ϕ is called *Euler's ϕ-function*, so the order of $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is $\phi(n)$. But $(\mathbb{Z}/n\mathbb{Z})^\times$ is also a group of order $\phi(n)$, and indeed we claim that $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. This can be seen by determining the group structure of $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ explicitly: the automorphism determined by $\psi(1) = m$ is explicitly defined by

$$\psi(k) = mk,$$

and composition amounts to multiplying these "m"'s:

$$\psi_1(\psi_2(k)) = \psi_1(m_2 k) = m_1 m_2 k$$

in a way which corresponds precisely to multiplication mod n. The identity automorphism corresponds to $m = 1$, and the inverse of ψ is the automorphism determined by $\psi^{-1}(1) = m^{-1}$, the multiplicative inverse mod n. Thus $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ is indeed isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

Warm-Up 2. We prove the final claim leftover from last time if $G = \langle x \rangle$ is cyclic of order n, then for each divisor k of n there is a unique subgroup of G of order k, and these are the only subgroups of G. Indeed, if k divides n, then $x^{\frac{n}{k}}$ has order

$$\frac{n}{gcd(n, \frac{n}{k})} = \frac{n}{\ell} = k,$$

where $\ell \in \mathbb{N}$ satisfies $n = k\ell$. (Note $gcd(n, \ell) = \ell$ since ℓ itself divides n.) Thus $\langle x^{\frac{n}{k}} \rangle$ has order k.

To show that $\langle x^{\frac{n}{k}} \rangle$ is the only subgroup of G of order k, suppose $H \leq G$ also has order k. Then H, being a subgroup of a cyclic group, is cyclic, so it is generated by some $x^s \in H$. Then

$$\frac{n}{\ell} = k = |H| = |x^s| = \frac{n}{gcd(n, s)},$$

so $\ell = gcd(n, s)$, and hence in particular ℓ is a divisor of s, say $s = \ell b$. But then any power of x^s is also a power of x^{ℓ}:

$$(x^s)^a = x^{as} = x^{a\ell b} = (x^{\ell})^{ab},$$

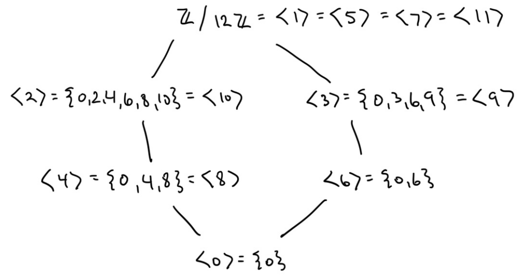
so $H = \langle x^s \rangle$ is contained in $\langle x^{\ell} \rangle$. Since H and $\langle x^{\ell} \rangle = \langle x^{\frac{n}{k}} \rangle$ both have order k, we thus conclude that $H = \langle x^{\frac{n}{k}} \rangle$, so that $\langle x^{\frac{n}{k}} \rangle$ is indeed the only subgroup of G of order k.

To see that there are no other subgroups of G (it is true in general that the order of any subgroup has to divide the order of the entire group, but we do not know this yet), take an arbitrary subgroup of G, which is thus cyclic. It is generated by some x^k, so the order of this subgroup is then $\frac{n}{gcd(n,k)}$, which is in fact a divisor of n. Thus this subgroup is already among the ones determined above.

Subgroup lattices. The *subgroup lattice* of a (finite) group is a picture which contains all of its possible subgroups, arranged according to which contains which. At this point we can thus determine the full subgroup lattice of any cyclic group. For instance, the subgroups of $\mathbb{Z}/12\mathbb{Z}$ are:

$$\langle 0 \rangle = \{0\},\ \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \mathbb{Z}/12\mathbb{Z},\ \langle 2 \rangle = \langle 10 \rangle,\ \langle 3 \rangle = \langle 9 \rangle,\ \langle 4 \rangle = \langle 8 \rangle,\ \langle 6 \rangle.$$

We draw them as follows, where a line segment indicates containment going upwards:

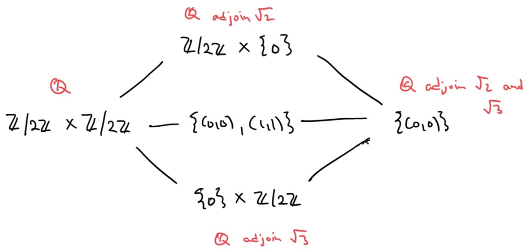


This is then the subgroup lattice of $\mathbb{Z}/12\mathbb{Z}$.

So far we can determine the full subgroup lattice of some other small groups of finite order, such as D_8 for instance, but this becomes more of a challenge as the order increases. But, at least for finite cyclic groups, we can determine the full lattice with relative ease.

Why do we care? Let us now go back to a motivation from the first day of class, to see why the subgroup lattice is a useful thing to have. Recall that the polynomial $(x^2-2)(x^2-3)$ has roots $\pm\sqrt{2}, \pm\sqrt{3}$, which can be permuted (in a still vague way which "preserves algebraic equations" and rules out other permutations) in four ways: fix or transpose $\pm\sqrt{2}$, and fix or transpose $\pm\sqrt{3}$. This group of permutations is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where each factor of $\mathbb{Z}/2\mathbb{Z}$ controls whether the same $\pm$ roots are transposed.

The fact is that each "branch" of the subgroup lattice of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ corresponds to one way of "introducing" the roots of $(x^2-2)(x^2-3)$:


$\mathbb{Q}$ adjoin $\sqrt{2}$
$\mathbb{Z}/2\mathbb{Z} \times \{0\}$
$\mathbb{Q}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\{(0,0),(1,1)\}$
$\{(0,0)\}$
$\mathbb{Q}$ adjoin $\sqrt{2}$ and $\sqrt{3}$
$\{0\} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}$ adjoin $\sqrt{3}$

(Here the contains go from right to left.) To start, note the coefficients of this polynomial all lie in $\mathbb{Q}$. In order to construct the roots $\pm\sqrt{2}$, which do not exist in $\mathbb{Q}$, we need to "adjoin" $\sqrt{2}$ to $\mathbb{Q}$ to construct a larger set of numbers:

$$\mathbb{Q} \to \mathbb{Q} \cup \{\sqrt{2}\} \cup \{\text{anything else needed to get a "consistent" set of numbers}\}.$$

We will give a precise meaning to "anything else needed to get a consistent set of numbers", and to what "consistent" means in this context, in the spring, but the idea is that once we introduce $\sqrt{2}$, we should also introduce things like $1+\sqrt{2}$, $-4+2\sqrt{2}$, and anything else obtained by adding/multiplying the things we have so far. (The precise language we will come to later is that we want the smallest *field* which contains $\mathbb{Q}$ and $\sqrt{2}$.) At this point we are able to describe the roots $\pm\sqrt{2}$ of our polynomial, so in order to be able to describe all roots we need only go one step further and "adjoin" $\sqrt{3}$:

$$\mathbb{Q} \to \mathbb{Q} \cup \{\sqrt{2}\} \cup \{\text{stuff}\} \to \mathbb{Q} \cup \{\sqrt{2}\} \cup \{\sqrt{3}\} \cup \{\text{more stuff}\}.$$

We claim that that the $\mathbb{Q}$ at the start corresponds to the full permutation group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (in a way which is to be determined later), and this specific way of "adjoining" elements corresponds to passing through one branch of the subgroup lattice, as labeled in the picture above. The bottom branch corresponds to the process where we *first* introduce $\sqrt{3}$ as a root, and *then* $\sqrt{2}$.

$$\mathbb{Q} \to \mathbb{Q} \cup \{\sqrt{3}\} \cup \{\text{stuff}\} \to \mathbb{Q} \cup \{\sqrt{3}\} \cup \{\sqrt{2}\} \cup \{\text{more stuff}\}.$$

(The middle branch in the picture above corresponds to adjoining $\sqrt{2}\sqrt{3} = \sqrt{6}$ first, but what is actually going on here requires clarification later.)

The upshot is that the structure of the subgroup lattice will eventually correspond to ways in which we can introduce the roots of a given polynomial. The ability or non-ability of finding a formula for all the roots will then be essentially controlled by the lattice itself.

Subgroups generated by sets. Cyclic subgroups are generated by single elements, but more generally we can consider subgroups generated by arbitrary subsets of a group. If $S \subseteq G$, we define the *subgroup generated by* S, denoted $\langle S \rangle$, to be the *smallest* subgroup of G which contains S. Here, "smallest" means with respect to set inclusion: if H is any subgroup of G which contains S, then $\langle S \rangle \subseteq H$. The point is that we include in $\langle S \rangle$ the set S and the bare minimum number of things needed in order to guarantee we actually get a subgroup, but no more.

You will see that this a different definition than what the book gives, but is in fact equivalent to it, as we will now prove. One remark is that the definition above does not actually say anything about such a "smallest" subgroup in fact exists, and indeed this is not at all obvious. We will often define objects in the coming quarters as being the "smallest" ones which have some property, but will still need to argue that something satisfying that definition does exist. This is likely why the book gives a more concrete definition for $\langle S \rangle$, but I prefer to use definitions which highlight the *point* of the object being defined (the point is that $\langle S \rangle$ is the smallest subgroup containing S), and show their existence afterwards.

So, the claim is that the definition we have given is equivalent to the equality

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H,$$

which is the book's definition. (This intersection is taken over all subgroups H of G which contain S.) It is always true that the intersection of any number of subgroups is a subgroup, so the key point is why this intersection is the *smalleset* subgroup containing S in the sense we defined above. In this case, the answer is simple: if K is any subgroup of G containing S, then K occurs as one of the subgroups H we are intersecting, and so

$$\bigcap_{S \subseteq H \leq G} H \subseteq K$$

simply because intersections are always subsets of each of the sets being intersected. This shows that $\bigcap_{S \subseteq H \leq G} H$ satisfies the defining property of being the smallest subgroup of G containing S, so we are done. Next time we will describe the elements of $\langle S \rangle$ more explicitly.

Lecture 10: Zorn's Lemma

Warm-Up 1. We show that, explicitly, the subgroup generated by $S \subseteq G$ is given by:

$$\langle S \rangle = \{s_1^{n_1} \cdots s_k^{n_k} \mid \text{each } s_i \in S, n_i \in \mathbb{Z}\}.$$

That is, $\langle S \rangle$ consists of all products of elements of S and their inverses. This just mimics the definition we gave of "free groups" earlier, only that here the group is not "free" since there is a predetermined multiplication on the elements of S we are using—namely that of G—along with whatever relations that entails.

First, the given set above is indeed a subgroup of G, simply because multiplying or inverting products of elements of S and their inverses still results in a product of elements of S and their inverses. Second, if H is a subgroup of G which contains S, then for each $s_1, \ldots, s_k \in S$ and $n_1, \ldots, n_k \in \mathbb{Z}$, we have $s_i^{n_i} \in H$ because H is a subgroup, and hence $s_1^{n_1} \cdots s_k^{n_k} \in H$ for the same reason. Thus H contains the subgroup defined above, so the subgroup defined above is the smallest subgroup of G containing S as claimed.

Warm-Up 2. We show that the multiplicative group $\mathbb{Q}^\times_{>0}$ of positive rational numbers is generated by the reciprocals of the prime numbers:

$$\mathbb{Q}^\times_{>0} = \{\tfrac{1}{p} \mid p \text{ is prime}\}.$$

(If we allowed negative reciprocals, we would get all of $\mathbb{Q}^\times$.) This is simply a reflection of the fact that any integer has a prime factorization. Indeed, let $\frac{a}{b} \in \mathbb{Q}^\times_{>0}$ with $a, b \in \mathbb{N}$, and write each of a, b as a product of primes:

$$a = p_1^{s_1} \cdots p_k^{s_k},\ b = q_1^{t_1} \cdots q_\ell^{t_\ell}$$

where each p_i, q_j is prime. Then:

$$\frac{a}{b} = p_1^{s_1} \cdots p_k^{s_k} \frac{1}{q_1^{t_1} \cdots q_\ell^{t_\ell}} = \left(\frac{1}{p_1}\right)^{-s_1} \cdots \left(\frac{1}{p_k}\right)^{-s_k} \left(\frac{1}{q_1}\right)^{t_1} \cdots \left(\frac{1}{q_\ell}\right)^{t_\ell},$$

which is a product of reciprocals of primes as required.

Finite generation. We say that a group G is *finitely generated* if there is a finite subset $S \subseteq G$ which generates it. In general, finitely generated groups are simpler to work with, since having a finite number of generators can help give explicit ways of performing various computations. Certainly any finite group is finitely generated (it generates itself), but infinite groups can be finitely generated as well: $\mathbb{Z}$ is generated by $\{1\}$, the free group on two letters $\langle x, y\rangle$ is generated by $\{x, y\}$, and $GL_n(\mathbb{R})$ is generated by the finite set of so-called *elementary matrices* for instance. (An elementary matrix is one which is obtained from the identity by performing one elementary row operation. The fact that any invertible matrix can be written as a product of these alone follows from the method commonly used in a linear algebra course to compute inverses by row-reducing.)

The product of an infinite number of copies of $\mathbb{Z}$ is not finitely-generated for instance, and neither is the group $\mathbb{Q}^\times_{>0}$ from the second Warm-Up. Note that this is not obvious: it is not so difficult to see that the generating set of the reciprocals of primes cannot be cut down to a finite generating set—essentially because are not divisible by other primes—but the claim is that *no* finite subset can generate the entire thing, which takes more work to prove.

In some sense, the notion of a finitely-generated group is an analog of that of a *finite-dimensional* space in linear algebra. For instance, consider the subgroup of $\mathbb{R}^n$ generated by $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$. Since the group operation here is addition, we will use additive instead of multiplicative notation. Then we have concretely:

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_k\rangle = \{m_1\mathbf{v}_1 + \cdots + m_k\mathbf{v}_k \mid \text{each } m_i \in \mathbb{Z}\}.$$

The observation is that this consists of *linear combinations* of $\mathbf{v}_1, \ldots, \mathbf{v}_k$, namely those with integer coefficients. This subgroup is thus analogous to the *span* of $\mathbf{v}_1, \ldots, \mathbf{v}_k$, only not actually the entire span since we are not using arbitrary real coefficients. But nevertheless, saying that a group is finitely-generated is essentially the group-theoretic equivalent of saying that a space is spanned by finitely many vectors in linear algebra. (We will consider these analogies more closely next quarter in the context of *modules* over *rings*.)

Maximality. To motivate the discussion of what's called *Zorn's Lemma* we will now undertake, we give the following definition: a proper subgroup H of G is said to be a *maximal* subgroup if it is not contained in a strictly larger proper subgroup, i.e. if $H \leq K \leq G$, then $H = K$ or $K = G$. (A *proper* subgroup is one which is not equal to the entire group.) For instance, the maximal subgroups of $\mathbb{Z}/n\mathbb{Z}$ are those generated by the primes dividing n.

A question we can ask is whether it is true that any group G contains subgroups which are maximal, or, even better, whether any given prescribed subgroup H is contained in a maximal subgroup. (That is, can H be "enlarged" to a maximal subgroup?) This specific question will not be so important for us this quarter in the context of groups, but the idea of "maximality" in this sense will be much more important in subsequent quarters in the context of rings and fields. We introduce it now in order to do something interesting, *and* to set the tone for the rest of the quarter as we now start to get into more intricate types of arguments.

The answer is that it is NOT true that any group must contain maximal subgroups, but it is true for finitely-generated ones at least, which you will show on the homework. This will give an example of why finite-generation can be a useful concept to have, and it will also illustrate an important result in modern mathematics: Zorn's Lemma. Zorn's Lemma is a result which is at core of many arguments in mathematics where we can show that a given object exists even when we are not able to construct it explicitly. Many of the objects we will consider in later quarters will arise in this way, and, as we will see, knowing existence alone is often all we actually need, so that the actual construction of said object is not necessary. This quarter Zorn's Lemma will not play a big role beyond our discussion here and the one homework problem, but we are covering it now in order to, as said above, set the tone for the rest of the course and because it is an amazing result which every serious student of mathematics should see at least one time in their development.

Zorn's Lemma. Here, then, is the statement of Zorn's Lemma:

> Suppose P is a nonempty, partially-ordered set in which every chain has an upper bound. Then P has a maximal element.

Of course, there are many undefined terms in the statement, and even once we define them the underlying meaning of Zorn's Lemma will take some getting used to, but the various examples we give of its use throughout the year should convince you that it truly is a remarkable tool. Ultimately, as said above, the point is that it gives a way to show that some object we care about exists (constructed as a "maximal" object within the appropriate context), even if we have no hope of constructing it explicitly.

Partial orders. A *partial order* on a set P is a relation $\leq$ satisfying:

- (reflexivity) $a \leq a$ for all $a \in P$,
- (transitivity) if $a \leq b$ and $b \leq c$, then $a \leq c$, and
- (anti-symmetry) if $a \leq b$ and $b \leq a$, then $a = b$.

Here, $\leq$ is purely a symbol we use to denote the given relation, but the point is that these properties suggest $\leq$ behaves as it if was an actual "ordering" on elements of P: anything should be "less than or equal to" itself, the "less than or equal to" relation should be transitive, and the only way in which two things can be "less than or equal to" each other is if they are the actually the same. We also use the strict notation $a < b$ to mean that $a \leq b$ and $a \neq b$.

Two key examples are the usual "less than or equal to" relation on $\mathbb{R}$, where $x \leq y$ literally means that x is less than or equal to y, and the partial order on a collection of subsets of a set given by $\subseteq$, where we interpret $A \subseteq B$ as saying that A is "less than or equal to" B. However, these examples have one important difference: in the case of $\mathbb{R}$, all elements are comparable to one another in the sense that given any $x, y \in \mathbb{R}$, it is true that $x \leq y$ or $y \leq x$, but this is not necessarily true when considering collections of subsets. A *chain* in P is a subset whose elements are all comparable to one another in this way. (A partial order in which all elements are comparable is called a *total order*, so a chain in P is then a totally-ordered subset of P.) The term “chain” comes from the idea that you can order all elements from “smaller” to “larger”, which in the countable case looks like:

$$\ldots \leq a \leq b \leq c \leq \ldots.$$

An *upper bound* of a subset S of P is an element $u \in P$ such that $s \leq u$ for all $s \in S$, which is the same way the term “upper bound” is used, say, in analysis. Finally, a *maximal* element of P is one for which there is nothing strictly larger: $a \in P$ is maximal if whenever $a \leq b$ for some $b \in P$, we have $a = b$. The usual (total) ordering on all of $\mathbb{R}$ has no maximal elements, but subsets of $\mathbb{R}$ might have maximal elements. If we take all subsets of a set S, then under $\subseteq$ the only maximal element is S itself, but a subcollection of only certain subsets might have zero, one, or more maximal elements.

Use in algebra. Zorn’s Lemma thus says that as long we know that any totally-ordered subset can be bounded above by something, then we can conclude that at least one maximal element exists. In the type of situation we care about, Zorn’s Lemma will be applied in the following way. Take P to be a collection of subsets of some set. Suppose further P has the property that for any subcollection $C \subseteq P$ of sets such that any two are comparable via $\subseteq$— meaning that given A and B in C it is always true that either $A \subseteq B$ or $B \subseteq A$—we have that the union $\bigcup C$ of all things in C also belongs to P. Then we can conclude that there is a set S in P which is not strictly contained within any larger element of P. Here, the partial ordering on P is given by $\subseteq$, C describes a chain in P with $\bigcup C$ being its upper bound in P, and the resulting S is a maximal element of P. Such maximal elements, as we’ll see, often have important properties we care about.

$\mathbb{R}^\omega$ has a basis. Here is one application of Zorn’s Lemma in linear algebra. Denote by $\mathbb{R}^\omega$ the set of infinite sequences of real numbers:

$$\mathbb{R}^\omega := \{(x_1, x_2, x_3, \ldots) \mid \text{each } x_i \in \mathbb{R}\}.$$

(This is analogous to elements of $\mathbb{R}^n$, only now with infinitely-many components.) Consider $\mathbb{R}^\omega$ equipped with vector addition and scalar multiplication defined as one would expect:

$$(x_1, x_2, \ldots) + (y_1, y_2, \ldots) = (x_1 + y_1, x_2 + y_2, \ldots) \text{ and } r(x_1, x_2, \ldots) = (rx_1, rx_2, \ldots).$$

We aim to show that $\mathbb{R}^\omega$ has a *basis* in the sense of linear algebra: a linearly independent subset of $\mathbb{R}^\omega$ which spans all of $\mathbb{R}^\omega$. Now, the trouble is that it is not actually possible to write down an explicit basis (!), so our proof is non-constructive. This is in stark contrast to the case of $\mathbb{R}^n$, where bases are easy to write down. Note that the obvious candidate of taking the vectors $\mathbf{e}_i$ which have a 1 in the i-th location and 0 everywhere else (which work in the $\mathbb{R}^n$ case) do not work in $\mathbb{R}^\omega$, since it is not true that anything in $\mathbb{R}^\omega$ can be written as a linear combination of *finitely many* of these $\mathbf{e}_i$, which is a technical requirement in the definition of “span” in the setting of infinite dimensions; the issue is that any linear combination of finitely many of the $\mathbf{e}_i$’s must eventually end in all zeroes! So, in fact, the $\mathbf{e}_i$ vectors only span the subspace of $\mathbb{R}^\omega$ consisting of sequences which are eventually zero, and so do not form a basis for entirety of $\mathbb{R}^\omega$.

Let I denote the collection of all linearly independent subsets of vectors in $\mathbb{R}^\omega$. Take any chain $C \subseteq I$. Then $\bigcup C$ is still a collection of linearly independent vectors in $\mathbb{R}^\omega$, and so is an upper bound for this chain in I. To see that $\bigcup C$ is still linearly independent, take any finite number of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \bigcup C$. (To say that a set of vectors is “linearly independent” technically means that any *finite* number of vectors taken from that set are linearly independent.) Each $\mathbf{v}_i$ comes from some $C_i \in C$. The fact that C is a chain implies that there exists $C_0 \in C$ which contains each of $C_1, \dots, C_n$, so $\mathbf{v}_1, \dots, \mathbf{v}_n \in C_0 \subseteq I$ must be linearly independent. Hence $\bigcup C$ is a linearly independent collection of vectors as claimed.

By Zorn's Lemma there thus exists a maximal linearly independent set B of vectors in $\mathbb{R}^\omega$. If these vectors did not span $\mathbb{R}^\omega$, picking $\mathbf{x} \in \mathbb{R}^\omega$ not in their span gives a linearly independent collection $B \cup \{\mathbf{x}\}$ which is strictly larger than B, contradicting maximality of B. Thus B must span $\mathbb{R}^\omega$, so that B is a basis of $\mathbb{R}^\omega$ as desired. In general, the same reasoning shows that any *vector space* (if you do not what this is yet, you will next quarter), even an infinite-dimensional one, has a basis. Note again here that we have no idea what this basis is, but it exists!

Lecture 11: Normal Subgroups

Warm-Up. Take P to be the set of all subgroups of a given group G, partially-ordered by set inclusion. Let C be a chain in P. We claim that the union of all subgroups in C is itself a subgroup of G. Now, the union of subgroups of group is not necessarily a subgroup in general (for instance, the union of $\langle 2 \rangle$ and $\langle 3 \rangle$ in $\mathbb{Z}$ is not closed under addition), so that the fact that this is true here depends heavily on the chain condition.

Clearly the union $\bigcup_{H \in C} H$ is nonempty since each H is nonempty. If $g \in \bigcup_{H \in C} H$, then $g \in K$ for some $K \in C$, in which case $g^{-1} \in K$ since K is a subgroup of G, and thus g^{-1} is in the union as well. Finally, if g_1, g_2 are in the union, then $g_1 \in H_1$ and $g_2 \in H_2$ for some subgroups $H_1, H_2 \in C$. Since C is a chain, we have either $H_1 \subseteq H_2$ or $H_1 \supseteq H_2$, so that both g_1, g_2 are contained in the same one; say $g_1, g_2 \in H_1$. Then $g_1 g_2 \in H_1$ since H_1 is a subgroup, so $g_1 g_2$ is in the union, and hence $\bigcup_{H \in C} H$ is a subgroup of G as claimed.

Now, Zorn's Lemma is applicable here since this union serves as an upper bound for the chain in P. But, the conclusion of Zorn's Lemma in this case is not so satisfying: a maximal subgroup of G exists, but of course G is in fact maximal in itself, so that we didn't actually need Zorn's Lemma to notice this. If we only consider proper subgroups in the definition of "maximal" (which is common), the problem is that P should only be taken to consist of proper maximal subgroups as well, but then the union of the elements in the chain above might not itself be a proper subgroup, so that it does not serve as an upper bound within P. This is why we need some type of restriction on G if we want to conclude that any such group has a (proper) maximal subgroup, such as being finitely-generated.

Choice implies Zorn. We finish our current discussion of Zorn's Lemma by saying something about where it comes from, and why we should believe it to be true. In class we only pointed out that it is equivalent to the *Axiom of Choice*, so that if we accept this axiom then we must accept Zorn's Lemma as well, but here we will elaborate more on this for those who are interested. (The Axiom of Choice is the claim that given any collection of nonempty sets, we can pick an element from each one simultaneously. The point is that there is no restriction on the number of nonempty sets we consider, it could even be an *uncountable* collection of nonempty sets.)

Let us give a very rough (emphasis on the very) sketch of the proof that the Axiom of Choice implies Zorn's Lemma. As stated before, Zorn's Lemma is actually equivalent to the Axiom of Choice, but the direction we look at here (choice implies Zorn) is the one which justifies the use of Zorn's Lemma as a valid tool in mathematics. We will not discuss the converse direction (Zorn implies choice), but if you ever take a topology course we'll just point out that one approach to the converse direction uses what's called *Tychonoff's Theorem* in topology. Our proof sketch is quite rough since we will get to a point where we would need to know much more advanced set theory—in particular properties of *cardinal* and *ordinal numbers*—to make it precise, but the basic idea will come across.

Suppose P is a nonempty, partially-ordered set in which every chain has an upper bound, and aiming for a contradiction suppose P did not contain any maximal elements. Then for any $a \in P$, we can always find some $b \in B$ such that $a < b$ since a is not maximal. Using the Axiom of Choice we can thus pick such an element $f(a)$ for any $a \in P$ all at once. Fix $a_0 \in P$, so that $a_0 < f(a_0)$. But by this construction we also have $f(a) < f(f(a))$, and so on we get:

$$a_0 < f(a_0) < f(f(a_0)) < f(f(f(a_0))) < \cdots .$$

This list gives a chain in P, so by the assumption of Zorn's Lemma this chain has an upper bound, call it a_1:

$$a_0 < f(a_0) < f(f(a_0)) < f(f(f(a_0))) < \cdots \leq a_1.$$

But now we can consider the chain

$$a_1 < f(a_1) < f(f(a_1)) < f(f(f(a_1))) < \cdots ,$$

which itself has an upper bound a_2:

$$a_1 < f(a_1) < f(f(a_1)) < f(f(f(a_1))) < \cdots \leq a_2.$$

Continuing in this way over and over (and over and over!) again gives a bunch of elements of P:

$$a_0 < f(a_0) < \cdots \leq a_1 < \cdots \leq a_2 < \cdots \leq a_3 < \cdots \leq a_4 < \cdots .$$

In fact, there would be so many elements of P listed here that this would imply (and this is the part which requires some pretty deep stuff which we will in no way attempt to make precise here) that the cardinality of P would be larger than that of any other set, and in particular P would have cardinality (strictly) larger that of P itself (or also of its power set), which is nonsense. Thus we conclude that P must have had a maximal element after all!

The big three. As stated above, the Axiom of Choice not only implies but is actually implied by Zorn's Lemma, so that they are equivalent. Just for the sake of interest, we give the statement of one more equivalent form of either of these: the *Well-Ordering Theorem*. A *well-ordering* on a set P is a total order in which every nonempty subset of P has a least (i.e. smallest) element. For instance, the usual ordering on $\mathbb{N}$ is a well-ordering, whereas the usual ordering on $\mathbb{R}$ is not. The Well-Ordering Theorem says that *every* set can in fact be well-ordered. In the case of $\mathbb{R}$, the point is that the usual order is *not* the one which works, but that there is *some* way to "order" the elements of $\mathbb{R}$ so that every nonempty subset does have a least element.

This is pretty surprising indeed, and the well-ordering on $\mathbb{R}$ which works would actually have no relation to the usual ordering. An explicit such well-ordering on $\mathbb{R}$ is not possible to write down, but nonetheless we know it must exist (if we accept the Axiom of Choice) since the Axiom of Choice, the Well-Ordering Theorem, and Zorn's Lemma are all equivalent to one another. These types of surprising results are the main reason why the Axiom of Choice—as obvious as it may seem—is viewed as quite controversial by many mathematicians: it has some seemingly paradoxical consequences which often say that a certain objects exists without giving any sense as to how to actually *construct* said object. There's an old joke that says: the Axiom of Choice is clearly true, the Well-Ordering Theorem is clearly false, and who knows about Zorn's Lemma? The joke, of course, is that the first of these seems obvious, the second seems like it could not possibly be true (since we cannot even imagine what a well-ordering of $\mathbb{R}$ would actually look like), and the third (Zorn) is such a complicated looking statement that no one really has any idea what it even means, and yet all three are actually saying the same thing in the end.

Towards quotient groups. Now, after this brief diversion, we return to the actual content of this course. We will begin to work towards the definition of a *quotient group*, and will start now with the overarching point of the constructions we will see. I feel that all too often books, such as ours, jump straight into the technical definitions required in order to construct quotient groups, but do not say much about the point of it all is. Moreover, the technical definitions tend to obscure the underlying idea and intent, but we will put this front and center.

Take a group G. The basic idea behind quotient groups is that we wish to "introduce" into G some *new* relations, and hope to still get a group in the end. For instance, consider the construction we gave earlier of the dihedral group D_8 from the free groups $\langle r, s\rangle$ on two generators: we take this free group—consisting of all "words" in r, s and their inverses—and then *impose* the relations

$$r^4 = 1,\ s^2 = 1,\ \text{and } rs = sr^{-1}.$$

In this case, in the end, we get a group of order 8 as a result. This is the construction we wish to mimic. So, let S be a subset of G. We use the elements of S to describe the new relations we want to impose, by *declaring* that each element of S should "become" the identity; in other words, we treat each element of S as being "equal" to the identity element. For instance, in the case of D_8, S would be the subset

$$S = \{r^4, s^2, srsr\},$$

whose elements are precisely the things which become equal to 1 in D_8. (Note that $srsr = 1$ is equivalent to $rs = sr^{-1}$, and indeed it is always true in any group that a relation given by having two expressions be equal to one another can always, after multiplying by inverses, be written as one in which a single larger expression equals the identity.)

Now, setting the elements of S to be "equivalent" to the identity gives rise to new relations as well, namely those which follow from the given ones; for instance, the three relations on D_8 above also give things like

$$r^4srsr = 1,\ (r^4s^2r^4)^{-1} = 1,\ \text{and so on.}$$

These additional relations come from the subgroup $\langle S\rangle$ generated by S, so we might as well assume that S was already a subgroup H to begin with, and we will do so.

Equality in quotients. We use the notation G/H (pronounced "G mod H"), to denote the object which results from declaring all elements of H to be equal to the identity. When this actually turns out to be a valid group (there are some subtleties, as we'll see), we call it a *quotient group*, in this case the "quotient of G by the subgroup H". The term "quotient" comes from a similarity which exists with ordinary quotients of integers, where in that case we "divide" an integer into pieces, just as (as we'll see) quotient groups do as well in an appropriate sense.

Now, what does it mean to say that $g = k$ in G/H? The point is that g and k might not literally be the same element in G, but only become the "same" after introducing the relations coming from H. Indeed, $g = k$ is equivalent to $g^{-1}k = e$, but in the context of G/H the symbol "e" really denotes any element of H (since we have declared all elements of H to be equal to the identity), so that "$g^{-1}k = e$" really means $g^{-1}k \in H$. Thus, we have:

$$g = k \text{ in } G/H \iff g^{-1}k \in H.$$

Denoting this element of H by $h = g^{-1}k$, we have that $gh = k$ in G. The point is that, if indeed $gh = k$ in G, then after "setting" h to be equal to the identity, the equation $gh = k$ becomes $ge = k$, or simply $g = k$. The set $gH = \{gh \mid h \in H\}$ is called a *coset* of H in G (we'll discuss cosets in more detail next time), and consists of all the elements of G which become equal to g in the quotient G/H:

$$g = k \text{ in } G/H \iff g^{-1}k \in H \iff k = gh \text{ for some } h \in H \iff k \in gH.$$

Thus, two elements become equal upon quotienting out by H if they "differed" by an element of H in G, in the sense above.

Example. Let us consider the following example, which finally clarifies the notation we've been using $\mathbb{Z}/n\mathbb{Z}$ for the additive group of integers mod n. For any $n \in \mathbb{N}$, the set of integer multiples of n—commonly denoted $n\mathbb{Z}$—is a subgroup of $\mathbb{Z}$. In the resulting quotient group $\mathbb{Z}/n\mathbb{Z}$ (where we "set" the elements of $n\mathbb{Z}$ to be equal to 0), we have that:

$$a = b \text{ in } \mathbb{Z}/n\mathbb{Z} \iff b - a \in n\mathbb{Z} \iff a \equiv b \bmod n.$$

(Note that $b - a$ is "$a^{-1}b$" written in additive notation.) Thus, equality in the quotient $\mathbb{Z}/n\mathbb{Z}$ corresponds precisely to equality mod n, as we've been using all along. Again, the point is that if $a = b + kn$, then a and b become the same once we declare that $nk \in n\mathbb{Z}$ should be zero.

Well-definedness. Now, we want to endow G/H with a group structure. But it is clear how we should proceed: we began with a group G at the start and imposed some new relations, so we can still (try to) use the the same group operation we had on G on G/H as well. That is, we attempt to define gk in G/H as simply $gk \in G$, where the only difference is that now gk might equal some things in G/H that it did not equal in G, due to the new relations we've introduced. With this definition, we automatically get associativity in G/H since associativity already held in G; there is still an identity element, only now it is in fact represented by *any* element of H (which are all equal in the quotient, so that the quotient does have only a single identity element); and the inverse of g is still g^{-1}, again only that possibly g^{-1} is equal to some new things as well.

But, this attempt to define a group structure on G/H runs into a subtle problem. Suppose that $g = k$ in G/H. Then, if there is any justice in the world, it *should* be true that for all $a \in G$ we have $ga = ka$. After all, if g and k are supposed to be the "same", then multiplying each by literally the same a should indeed result in equal quantities:

$$g = k \text{ in } G/H \text{ should imply } ga = ka \text{ in } G/H \text{ for all } a \in G.$$

If we write out what these equalities mean in G/H, this becomes the statement that

$$g^{-1}k \in H \text{ should imply } (ga)^{-1}(ka) \in H \text{ for all } a \in G.$$

The product on the right is $a^{-1}g^{-1}ka$, and so the condition we need to hold is that:

$$g^{-1}k \in H \implies a^{-1}(g^{-1}k)a \in H \text{ for all } a \in G,$$

or said another way with $h = g^{-1}k \in H$, we need that

$$h \in H \implies a^{-1}ha \in H \text{ for all } a \in G.$$

Thus, in order for the proposed group operation on G/H to be well-defined and give a valid function $G/H \times G/H \to G/H$ (which is what multiplication should be), it should be true that conjugating an element of H by an element of G should always result in an element of H. (Technically above we are conjugating by a^{-1}, but of course if we replace $a \in G$ by $a^{-1} \in G$—note the condition should hold for *all* elements of G—we get $aha^{-1} \in H$ as well.) This condition, because of its relation to quotient groups, is so important that we give a special name: normality.

Normal subgroups. A subgroup H of G is *normal* in G if $ghg^{-1} \in H$ for all $g \in G$. Using notation we introduced previously in relation to normalizers, this says that H is normal in G if $gHg^{-1} \subseteq H$ for all $g \in G$. We use $H \trianglelefteq G$ to denote that H is a normal subgroup of G. The point is that it is only for normal subgroups that the "quotienting" process described above works and produces a well-defined group structure on G/H.

Now, if this is true, then in particular we also have $g^{-1}Hg \subseteq H$, so that upon multiplying by g on the let and g^{-1} on the right we get $H \subseteq gHg^{-1}$ as well. Thus, the condition of normality can actually be written as an equality: $gHg^{-1} = H$ for all $g \in G$. (But, nevertheless, to actually check normality it is quicker to use $gHg^{-1} \subseteq H$ since this only requires one containment.) This equality says precisely that $g \in N_G(H)$ (the normalizer of H in G), so $H \trianglelefteq G$ if $N_G(H) = G$; indeed, this where the name "normalizer" comes from. Looking back to prior normalizer examples, you will see that we have already come across examples of normal subgroups, such as $\langle r \rangle \trianglelefteq D_{2n}$. Note also that every subgroup of an abelian group, such as $n\mathbb{Z}$ in $\mathbb{Z}$, is normal.

Example. We finish with an example which explicitly shows what goes wrong when we do not have normality. Take $\langle A \rangle = \{0, A\} \leq D_8$, where we use the rotation/reflection notation with A as the anti-diagonal reflection. This subgroup is not normal in D_8, since for instance

$$90 \cdot A \cdot 90^{-1} = D \notin \langle A \rangle.$$

Thus, it should be true that the multiplication on the quotient $D_8/\langle A \rangle$ resulting from the one on D_8 is NOT well-defined, so that $D_8/\langle A \rangle$ is not actually a group under this operation.

Indeed, we have $180 = D$ in $D_8/\langle A \rangle$ since $(180)^{-1}D = 180 \cdot D = A \in \langle A \rangle$. But, now consider $180 \cdot 90 = 270$ and $D \cdot 90 = V$. Since $(270)^{-1}V = 90 \cdot V = D \notin \langle A \rangle$, we have that

$$180 \cdot 90 = 270 \neq D \cdot 90 = V \text{ in } D_8/\langle A \rangle.$$

And so, even though 180 and D are the same in the quotient, $180 \cdot 90$ and $D \cdot 90$ are not the same in the quotient, so this attempt at defining multiplication in the quotient does not produce a well-defined operation, so we do not get a valid group structure.

Lecture 12: Cosets and Quotients

Warm-Up. We show that $\langle (123) \rangle$ is not normal in S_4 and find an example of elements $\sigma, \tau, \gamma \in S_4$ such that $\sigma = \tau$ but $\sigma\gamma \neq \tau\gamma$ in the quotient $S_4/\langle (123) \rangle$. (Thus we do not get a well-defined group structure on this quotient, which is expected by the lack of normality.) First, we have:

$$(34)(123)(34)^{-1} = (124),$$

which is not in $\langle (123) \rangle$ so this subgroup is not normal in S_4. Now, we have $(12) = (12)(123) = (23)$ in $S_4/\langle (123) \rangle$, but

$$(12)(34) = (12)(34) \quad \text{and} \quad (23)(34) = (234),$$

which are not equal in the quotient since $(12)(34)(234)^{-1} = (124) \notin \langle (123) \rangle$.

Cosets. Recall from last time that $g = k$ in G/H if and only if there exists $h \in H$ such that $gh = k$. The set $gH = \{gh \mid h \in H\}$ is called a *(left) coset* of H in G and thus (as we said before) consists of all elements to which g becomes equal in G/H. We will then formally *define* G/H to be precisely the set of cosets of H in G:

$$G/H := \{gH \mid g \in H\}.$$

The point is that G/H should, as a set, consist of distinct elements, and using this coset language gives us a formal way of "identifying" the elements of G which become the "same" after imposing the relations which come from H; in this setting, g and k are the "same" in G/H precisely when the cosets they determine are literally the same:

$$g = k \text{ in } G/H \iff gH = kH.$$

Indeed, note that if $gh = k$, so that $k \in gH$, then we have equivalently $g = kh^{-1} \in kH$, which does in fact imply that $gH = kH$ since then $gH = (kh^{-1})H = k(h^{-1}H) = kH$. (We use here the fact that any $h' \in H$ can be written as $h' = h^{-1}(hh') \in h^{-1}H$.) It follows that two cosets are thus either equal as sets or completely disjoint, which is what makes "grouping" elements of G into cosets in this way work: each element only gets "grouped" into a single coset. (Next time we will provide another perspective on this idea in terms of an equivalence relation.)

The group operation we have been informally using on G/H up until now can now formally be defined in terms of *coset multiplication*:

$$(g_1H) \cdot (g_2H) := (g_1g_2)H.$$

The point of course is that this group operation should simply mimic the group operation on G, only that now we allow elements of G to be "equal" when they give equal cosets. The work we did last time then shows that this operation indeed gives a well-defined group structure if and only if H is a *normal* subgroup of G: we can pick an element $k \in g_2H$ different from g_2 to represent the same coset $g_2H = kH$, and normality is what we need to say that using k instead of g_2 to perform the proposed group operation still gives the same answer:

$$(g_1H)(g_2H) = (g_1g_2)H \text{ is the same as } (g_1H)(kH) = (g_1k)H$$

when H is normal. Note also that the notion of normality can be expressed in terms of cosets: $gHg^{-1} = H$ is equivalent to $gH = Hg$ where Hg denotes the *right* coset corresponding to g, so H is normal in G when the left coset corresponding to any $g \in G$ is the same as the right coset corresponding to g.

Quotient groups. Thus, for a normal subgroup $H \trianglelefteq G$, we define formally define the *quotient* group G/H to be the set of cosets of H in G under the group operation defined above. The identity element is the coset $eH = H$ (which equals hH for any $h \in H$) and the inverse of gH is $g^{-1}H$. Now, we will abuse notation and use G/H to still denote the set of cosets of H in G even when H is not normal in G, but in this case we will not refer to G/H as being a group and will not consider multiplication of cosets, so that G/H will simply be a set without any extra structure.

The coset approach to defining quotient groups is the one most introductory books take, and serves to give a formal construction. Our book approaches quotient groups via kernels and "fibers", which we will clarify in a bit. We will, for the most part, actually avoid coset notation altogether when describing elements of G/H unless it is necessary to avoid confusion in various proofs. Instead, we will think of G/H as we first described it before introducing cosets: as G itself with new relations imposed. Thus, we will use g to denote both elements of G and elements of G/H, keeping in mind that G/H we might have $g = k$ without $g = k$ being literally true in G.

We feel that this better matches the way in which quotient groups are used in practice, and emphasizes the intent behind quotient groups (introduce new relations) better than the coset approach. The downside of our approach and notation is that we will need to be more careful about noting where various computations take place and where various equalities hold, but the trade-off will be worth it. (This will be even more true in subsequent quarters when we consider other types of quotient constructions.) Apart from using coset notation, if we truly do need to distinguish between an element of G and the element it gives in a quotient, it is common to use $\overline{g}$ to denote the quotient element corresponding to $g \in G$, which we think of as "g reduced mod H". Indeed, the book has been using this notation from the start when referring to elements of $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

One more remark: if we are to think of quotient groups as introducing new relations into G, we might think that the requirement of having subgroups be normal restricts the types of relations we can consider. After all, using the motivation from last time, if $S \subseteq G$ contains the new relations we wish to introduce, the subgroup $\langle S \rangle$ they generate is not necessarily normal, so that $G/\langle S \rangle$ is not defined as a group. However, this is not a problem: given $\langle S \rangle \leq G$, we can instead consider its *normal closure* N in G, which is the subgroup of G generated by all the conjugates of $\langle S \rangle$. This N is then always normal in G, and is in a sense the "smallest" normal subgroup of G containing all the relations in S; in turn, G/N is the "least trivial" group obtained G by introducing the relations in S. We will not discuss normal closures further in this course, but they give a precise why of being able to introduce whatever relations we want into G.

Example. We determine (somewhat informally for now) the better known group to which the quotient group

$$(\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle$$

is isomorphic. (Note $\mathbb{Z} \times \mathbb{Z}$ is abelian, so every subgroup is normal.) In this quotient we have $(1,2) = (0,0)$, so the idea is to use this relation to simply the description of elements in the quotient. From this equality (write it as $(1,0) + (0,2) = (0,0)$) we get:

$$(1,0) = (0,-2) \text{ in } (\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle$$

Thus the point is that this cuts down the number of generators in the quotient, so that instead of $(1,0)$ and $(0,1)$ being treated as "independent" generators, we can generate the entire quotient by $(0,1)$ alone. Concretely, any element in the quotient is given by a pair whose first coordinate is 0:

$$(a,b) = (0, b-2a) \text{ in } (\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle.$$

No two such elements $(0,m)$ and $(0,n)$ are equal to each other, since $(0,m) - (0,n) = (0, m-n)$ is in $\langle (1,2) \rangle$ only when $m = n$. Thus, we can see that the quotient is a cyclic group generated by one element $(0,1)$ of infinite order, meaning that it is isomorphic to $\mathbb{Z}$:

$$(\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle \cong \mathbb{Z}.$$

Informally, a possible isomorphism between these two comes precisely from the realization that $(a,b) = (0, b-2a)$: the entire data of an element (a,b) of the quotient is captured by a single integer $b - 2a$, which as b and a vary can take on any integer value. That the map

$$(\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle \to \mathbb{Z} \text{ defined by } (a,b) \mapsto b - 2a$$

is indeed an isomorphism is something we will postpone proving, in order to derive it from the general fact known as the *First Isomorphism Theorem*. For now, we note that this map is indeed well-defined, meaning that we can choose a different element of $\mathbb{Z}\times\mathbb{Z}$ to represent the same thing as (a,b) in the quotient without changing the value which the function above assigns to this element: if $(a,b)=(a',b')$ in $(\mathbb{Z}\times\mathbb{Z})/\langle(1,2)\rangle$, then $(a-a',b-b')=(k,2k)\in\langle(1,2)\rangle$, so

$$a'=a-k, b'=b-2k \text{ and thus } b'-2a'=(b-2k)-2(a-k)=b-2a.$$

Again, this observation will become more general in the context of the First Isomorphism Theorem.

Kernels and quotients. Given a homomorphism $\phi: G\to H$, its kernel $\ker\phi := \{g\in G \mid \phi(g)=e_H\}$ is always normal in G. Indeed, for any $g\in G$ and $x\in\ker\phi$, we have:

$$\phi(gxg^{-1})\phi(g)\phi(x)\phi(g^{-1})=\phi(g)e_H\phi(g)^{-1}=e_H,$$

so $gxg^{-1}\in\ker\phi$. Thus, the quotient group $G/\ker\phi$ always exists (as a group), and the First Isomorphism Theorem will tell us what group this quotient actually is. (Spoiler alert: it is isomorphic to the image $\phi(G)$ of ϕ.) Moreover, in fact *any* normal subgroup $H\trianglelefteq G$ arises in this way: if H is normal, G/H is a group, and the map

$$G\to G/H \text{ defined by } g\mapsto g$$

(which really means $g\mapsto\overline{g}=gH$, but again we prefer to think of g in the quotient as literally the same element as g in G, only subject to more relations) is a homomorphism whose kernel is precisely H: $h\in G$ gives the identity $h=e$ in G/H if and only if $h\in H$. Thinking of normal subgroups as kernels is how our book first introduces normality. The homomorphism $G\to G/H$ sending g to itself (viewed as an element in G/H, or viewed as sending g to $\overline{g}=gH$) is called the *canonical* or *natural projection* of G onto G/H.

But now we ask: what does it mean to say that $g_1=g_2$ in $G/\ker\phi$, or equivalently what do the cosets of $\ker\phi$ in G actually measure? The equality $g_1=g_2$ holds in this quotient if and only if $g_1^{-1}g_2\in\ker\phi$, which means

$$\phi(g_1^{-1}g_2)=e_H, \text{ or equivalently } \phi(g_1)^{-1}\phi(g_2)=e_H, \text{ or equivalently } \phi(g_1)=\phi(g_2).$$

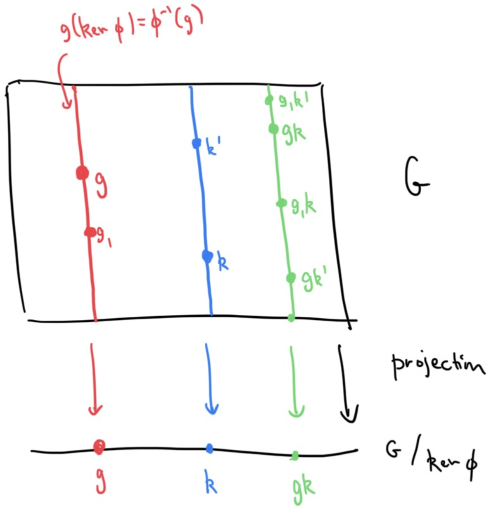
Thus, we have that $g_1=g_2$ in $G/\ker\phi$ precisely when g_1,g_2 gives the same image $\phi(g_1)=\phi(g_2)$ in H. In other words, g_1,g_2 here should belong to the *preimage* $\phi^{-1}(h)$ of the same element $h=\phi(g_1)=\phi(g_2)$ in H, which is the set of all things in G which map to h:

$$\phi^{-1}(h):=\{g\in G\mid\phi(g)=h\}.$$

A preimage of a single element is also called a *fiber* of ϕ, and the conclusion is that the cosets of $\ker\phi$ are precisely the fibers of ϕ:

$$\text{for } g\in G,\ g(\ker\phi) \text{ gives all elements in } G \text{ which map to the same thing in } H \text{ as } g.$$

The name “fiber” comes from the following picture. Visualize G as a plane, H as a line, and ϕ as a “projection” map:



The fibers/preimages are then the vertical lines lying above points on the line. The entire fiber gets "collapsed" into a single point upon taking the quotient, and the group operation on the quotient can be viewed as "multiplying" these fibers: take a point in one fiber, a point in another fiber, multiply them together in G, with the result being the fiber where the product lies. Normality guarantees that it does not matter which points from each fiber we actually use here, we always get the same *fiber* as a result.

Lecture 13: Lagrange's Theorem

Warm-Up 1. We (informally) identity the quotient group $(\mathbb{Z}\times\mathbb{Z})/\langle(5,5)\rangle$ as a simpler group. Note first that $(5,5) = (0,0)$ in the quotient, so that $(5,0) = (0,-5)$. This implies that any general (a,b) will be equivalent to one which has first coordinate among $0,1,2,3,4$, since we can subtract away enough 5's from a and "move" them over to the second coordinate, leaving the first coordinate as one of $0,1,2,3,4$. More precisely, if $a = 5q+r$ where $0 \leq r < 5$ according to the division algorithm, then

$$(a,b) = (5q+r,b) = (r,b-5q).$$

(Note we can also write r here as $a \bmod 5$.) Alternatively, we have

$$(a,b) = (a-5k,b-5k) \text{ for any } k \in \mathbb{Z},$$

and again for the appropriate $k = q$ the first coordinate $a-5k$ will be in the range $0,1,2,3,4$.

This all suggests that the first coordinate in an element of the quotient can actually be taken to be in $\mathbb{Z}/5\mathbb{Z}$, and moreover the way in which addition works in the quotient—where adding multiples of 5 to both coordinates does nothing—suggests the addition in this first coordinates should indeed be taking place mod 5. Now, even though the same thing is happening in the second coordinate, what happens there is dependent on the behavior in the first coordinate since it is the same $5k$ which is subtracted from both above. So, we will not get that the second coordinate can also be taken to be in $\mathbb{Z}/5\mathbb{Z}$, since this restriction would in return change the value of the first coordinate again. (Getting $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ as the group to which the quotient is isomorphic would require that we *independently* be able to reduce both coordinates mod 5.) Once we modify the first coordinate to be in $\mathbb{Z}/5\mathbb{Z}$, the second coordinate is fixed as in

$$(a,b) = (r,b-5q)$$

above. Since b is arbitrary, the value of $b-5q$ can be taken to be any integer, since any integer can be written as 5 less than some integer. Thus, we expect that the second coordinate comes from the entirety of $\mathbb{Z}$, so this quotient should be isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$:

$$(\mathbb{Z} \times \mathbb{Z})/\langle(5,5)\rangle \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}.$$

We could of course make the second coordinate take values in $\mathbb{Z}/5\mathbb{Z}$ and allow the first coordinate to be whatever instead, in which case we get $\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ as the answer. We will prove formally that this answer is correct later after we discuss the First Isomorphism Theorem.

Warm-Up 2. We show that if $G/Z(G)$ is cyclic, then G is abelian, which is our first example of using information about a quotient to derive information about a group. Recall that $Z(G)$ denotes the center of G—the subgroup of elements of G which commute with all elements of G—which is normal in G since every element of G in fact centralizes (and hence normalizes) $Z(G)$.

Let $x \in G/Z(G)$ be a generator (recall that we are denoting elements of $G/Z(G)$ simply by elements of G and let $g, h \in G$. Then in the quotient we have $g = x^k$ and $h = x^\ell$ for some $k, \ell \in \mathbb{N}$, which means that

$$g = x^k a \text{ and } h = x^\ell b \text{ for some } a, b \in Z(G).$$

Thus we compute:

$$gh = x^k a x^\ell b = x^k x^\ell ab = x^\ell x^k ba = x^\ell b x^k a = hg,$$

where we use the fact that $a, b \in Z(G)$ commute with all other elements. This shows that G is abelian as claimed. Note it was crucial here that $G/Z(G)$ be cyclic and not simply abelian. If $G/Z(G)$ were only abelian, we could say that $gh = hg$ in $G/Z(G)$, but this gives $gh = hga$ for some $a \in Z(G)$, which does not say that G is necessarily abelian. The point here is that $Z(G)$ and $G/Z(G)$ being abelian is not enough to guarantee that G is abelian, so there is a limit to the amount of information about G we can derive from knowledge of subgroups and quotients alone, in general.

Cosets and actions. Let us note that cosets arise as the equivalence classes of a certain equivalence relation. Indeed, given $H \leq G$ the relation

$$g \sim k \text{ defined by } g^{-1}k \in H$$

on G is an equivalence relation. (This is actually equivalent to H being a subgroup of G and not just a subset.) Two elements are in then the same equivalence class precisely under the same condition $g^{-1}k \in H$ which says that the cosets gH and kH are the same, so the equivalence classes for this equivalence relation are indeed the (left) cosets of H in G. As a consequence, we get immediately that two cosets are either disjoint or identical since this is true of equivalence classes in general.

We now make two observations regarding cosets and actions. First, consider the *right action* $G \curvearrowleft H$ of H on G given by *right* multiplication:

$$g \cdot h := gh.$$

(A right action is similar to a left action, only that the property $g \cdot (k \cdot x) = (gk) \cdot x$ holds in the "reverse" direction: $g \cdot (k \cdot x) = (kg) \cdot x$. It is for this reason that it is more common to write the action as occurring on the right, so that $(x \cdot k) \cdot g = x \cdot (kg)$ holds instead. Right actions will not play a major role for us, essentially because there is a standard way of turning a right action into a left action anyway. We'll omit the details here.) For a fixed $g \in G$, the orbit of this action is precisely the left coset of H corresponding to g:

$$gH = \{g \cdot h \mid h \in H\} = \{gh \mid h \in H\}.$$

(Using the left action of H on G given by left multiplication would produce the *right* cosets of H in G as the orbits.) Again, the fact that cosets arise as orbits implies immediately that they any two are either disjoint or identical.

The second observation is that there is a natural action $G \curvearrowright G/H$ of G on G/H—viewed here as simply the set of cosets without reference to any potential group structure (H is not necessarily normal in G)—again by left multiplication:

$$g \cdot (kH) := (gk)H.$$

Equivalently this action can be viewed as a homomorphism $G \to S_{G/H}$, where $S_{G/H}$ as usual denotes the group of permutations (i.e. self-bijections) of the set of cosets. The existence of such a homomorphism for any subgroup H will be useful later in studying properties of G itself.

Lagrange's Theorem. And now we come to the first truly nontrivial result in finite group theory: Lagrange's Theorem. By "nontrivial" we mean that this is the first result which really requires some new insight or construction (in this case the language of cosets), and not the "basic" language of groups alone. Even the facts we proved about cyclic groups previously—although certainly not necessarily easy—only really used basic properties of powers and orders, and not anything too deep. Of course, the use of the phrase "nontrivial" is subjective, and is meant to convey here the need to consider objects which seem to come out of nowhere; after all, how likely is it that someone would think of the idea of a "coset" in trying to prove what follows? It is this realization of the need to use cosets which we mean by calling this a "nontrivial" result.

Here is the statement, which we might have guessed from all the examples of subgroups we have seen so far: if G is a finite group and H a subgroup, then $|H|$ divides $|G|$. Thus, we have nontrivial constraint on what order of a subgroup could actually be. The basic idea of the proof is that given $g \in G$, there $|H|$ many elements in the coset gH, so that the number of elements of G gets *reduced* by a factor of $|H|$ when forming the set of cosets G/H. To be precise, write G as a disjoint union of its cosets:

$$G = \bigsqcup_{g \in G/H} gH.$$

More simply, if we denote the distinct cosets of H in G by $g_1H, \ldots, g_kH$, then

$$G = g_1H \sqcup \ldots \sqcup g_kH.$$

Since this is a disjoint union, we have:

$$|G| = |g_1H| + \cdots + |g_kH|.$$

But each coset g_iH has the same size as H since the map $g_iH \to H$ defined by $g_ih \mapsto h$ is a bijection. (Note here it is crucial that gh and gh' are distinct if h and h' are distinct.) Thus we get

$$|G| = \underbrace{|H| + \cdots + |H|}_{k \text{ times}} = k|H|,$$

so that $|H|$ divides $|G|$ as claimed.

This also shows that the *number* of distinct cosets—which is k in the notation above—also divides $|G|$. This number of cosets of H in G is called the *index* of H in G, and is denoted by $[G:H]$. (The book uses $|G:H|$ to denote the index, but $[G:H]$ is more common.) The proof of Lagrange's Theorem thus shows that

$$|G| = [G:H]|H|$$

when G is finite. (This also holds in the infinite case, in the sense that if the left side is infinite, at least one of the terms on the right is as well, and vice-versa.) Note that when H is normal in G, the index is precisely the order of the quotient group, and we get:

$$|G/H| = [G:H] = \frac{|G|}{|H|}$$

in the finite case. (This matches our intuition above, in that the number of elements of G gets reduced by a factor of $|H|$ when forming cosets.)

Consequences. And now we give a few basic consequences of Lagrange's Theorem. First is the fact that the order of any element $g \in G$ (G finite) has to divide $|G|$, which just comes from the fact that $|g| = |\langle g\rangle|$ and $|\langle g\rangle|$ divides $|G|$ by Lagrange's Theorem. As a second consequence, this then implies that for any $g \in G$, $g^{|G|} = e$ since $|G|$ is a multiple of $|g|$.

Third is the fact that any group of *prime* order must be cyclic! Indeed, if $|G| = p$ is prime, the order of any nonidentity $x \in G$ must divide $|G| = p$, and hence must be p itself since p is prime. This means $\langle x\rangle = G$, so G is cyclic as claimed. Thus we now have our first true group classification result: the only group (up to isomorphism) of prime order p is $\mathbb{Z}/p\mathbb{Z}$.

Lecture 14: First Isomorphism Theorem

Warm-Up 1. Suppose $|G| = pq$ where p, q are distinct primes. We claim that either G is abelian or G has trivial center $Z(G)$. Indeed, by Lagrange's Theorem, $|Z(G)|$ divides $|G| = pq$, and hence must be either $1, p, q$, or pq. If $|Z(G)| = pq$, then $Z(G) = G$ and G is abelian. If $|Z(G)| = p$ or q, then $G/Z(G)$ has prime order q or p respectively, which means that $G/Z(G)$ is cyclic, as we proved at the end of last time. But *this* then implies that G is abelian, as we proved in a Warm-Up last time. (Note that in this case $Z(G) = G$ after all since G is abelian, so that $Z(G)$ would have order pq and not p or q, meaning that the case $|Z(G)| = p$ or q case could not actually happen. But, we were not able to see this until after this case was completed.) The remaining case $|Z(G)| = 1$ is that $Z(G)$ is trivial, so we are done.

As an application, this gives a quick proof that D_{2p} has trivial center when p is prime, since then 2 and p are distinct and D_{2p} is certainly not abelian. Of course, D_{2n} has trivial center for any *odd* n, not just those that are prime, but the proof of this general fact (if you recall from the first homework) is a lot more computationally involved than this simpler proof in the n prime case.

Warm-Up 2. Suppose $K \leq H \leq G$ with G finite. We claim that the following equality among indices holds:

$$[G:K] = [G:H][H:K],$$

so that the product of the number of cosets of K in H with the number of cosets of H in G is the number of cosets of K in G. This type of equality will be useful in deriving information about the various groups occurring in such a chain $K \leq H \leq G$.

Let us denote the distinct elements of G/H and H/K by

$$G/H = \{g_1, \dots, g_m\} \quad \text{and} \quad H/K = \{h_1, \dots, h_n\}.$$

To be clear, we are saying here that not only are the g_i distinct in G and the h_j distinct in H, but that they are also distinct in the respective *quotients* above. We claim that the mn many elements g_ih_j give *all* the elements of and are *distinct* in G/K. If so, then $[G : K] = mn$, $[G : H] = m$, and $[H : K] = n$ in this notation, which gives the required equality. First, for any $g \in G$, there is some $g_i \in G/H$ to which is equivalent, meaning that

$$g = g_ih \text{ for some } h \in H.$$

But then this h is equivalent to some $h_j \in H/K$, so that

$$h = h_jk \text{ for some } k \in K.$$

Thus $g = g_ih = g_ih_jk$, so that $g = g_ih_j$ in G/K, and hence the g_ih_j do give all elements of G/K.

Now, to show that the g_ih_j give distinct elements of G/K, suppose some $g_ih_j = g_ph_q$ in G/K. Then

$$g_ih_j = g_ph_qk \text{ for some } k \in K.$$

Manipulating this gives $g_i = g_p(h_qkh_j)$, and since $h_qkh_j \in H$ (since $K \leq H$ and H is closed under multiplication), this means that $g_i = g_p$ in G/H. But $g_1, \dots, g_m \in G$ were assumed to give distinct elements of G/H, so it must be the case that $g_i = g_p$ in G as well. Hence the equality above becomes

$$g_ih_j = g_ih_qk, \text{ which implies } h_j = h_qk.$$

This now means that $h_j = h_q$ in H/K, so that in fact $h_j = h_q$ in H since $h_1, \dots, h_n \in H$ were assumed to give distinct elements of H/K. Thus $g_ih_j = g_ph_q$ in G/K implies that $g_i = g_p$ in G and $h_j = h_q$ in H, so that the elements $g_ih_j, 1 \leq i \leq m, 1 \leq j \leq n$ are all distinct in G/K as claimed.

Products of subgroups. As one more application of cosets, let us describe the size of the *product* HK of two subgroups $H, K \leq G$. This product is defined to be the set of all products hk with $h \in H$ and $k \in K$:

$$HK := \{hk \mid h \in h, k \in K\}.$$

Note (!!!) that this is *not* necessarily a subgroup of G, since it need not be closed under multiplication: $(h_1k_1)(h_2k_2)$ cannot always be rewritten as (something in H)(something in K). Indeed, it is true that HK is a subgroup if and only if $HK = KH$, since this is what is needed to "swap" the terms in the k_1h_2 in the middle of the product $(h_1k_1)(h_2k_2)$. (To be clear, by "swap" we mean to rewrite it as some hk instead, but it is not necessarily true that k_1h_2 will equal h_2k_1, which is why we have equality $HK = KH$ at the level of *sets*, not elements.) We will omit the details of this claim here, but will point out that there are various conditions—perhaps most importantly when at least one of H, K is normal in G—under which $HK = KH$ will hold; we'll come back to this when discussing the *Second Isomorphism Theorem.*

But regardless of whether HK is actually a subgroup of G, we can still speak about its size (assuming G is finite), and the claim is that

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

There idea is that there $|H|$-many choices for the first term in hk, and $|K|$-many for the second term, giving at most $|H||K|$-many such expressions. But, some of these might create duplicate products hk, and accounting for this reduces the size precisely by a factor of $|H \cap K|$. Here are the details. First, note that we can write HK as a union of those cosets of K which are determined by the elements of H:

$$HK = \bigcup_{h \in H} hK.$$

To keep track of only distinct cosets—and hence get a disjoint union—we note that for $h, h' \in H$:

$$h = h' \text{ in } G/K \iff h^{-1}h' \in K \iff h^{-1}h' \in H \cap K \iff h = h' \text{ in } H/(H \cap K),$$

where the second $\iff$ comes from the fact that h, h' were assumed to be in H to begin with. Thus, we can specify the distinct cosets hK using the elements of $H/(H \cap K)$, so:

$$HK = \bigsqcup_{h \in H/(H \cap K)} hK.$$

Each hK has the same size as K, so taking sizes above gives

$$|HK| = \sum_{h \in H/(H \cap K)} |K| = [H : H \cap K]|K|$$

since the size of $H/(H \cap K)$ is $[H : H \cap K]$. But this also equals $|H|/|H \cap K|$ by the proof of Lagrange's Theorem, and substituting this into the equality above gives our claim.

Analog in linear algebra. We mentioned a while back—when discussing the idea of subgroups generated by subsets—one analogy between group theory and linear algebra (generated subgroups vs spans), and here is another. We will phrase this in the context of *vector spaces* in general, but if you are unfamiliar with this concept you can simply think about $\mathbb{R}^n$ and its subspaces. (We we will discuss vector spaces in this course next quarter.) If U, W are subspaces of a vector space V, then the following dimension equality holds:

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W),$$

which mimics precisely "additive" version of the product subgroup equality derived above! Indeed, the product equality in additive notation is

$$|H + K| = |H| + |K| - |H \cap K|.$$

We will see a few more such analogies between group theory and linear algebra as we go, and will see the proper context which underlies them next quarter. (This is also analogous to the basic set-theoretic "inclusion/exclusion" equality: $|A \cup B| = |A| + |B| - |A \cap B|$ for finite sets A, B.)

Isomorphism Theorems. We now move to a collection of results, called the *isomorphism theorems*, which help to more simply identity various quotient groups. Of these, the first of them—appropriately called the *First Isomorphism Theorem*—is the most important and truly captures much of the intent behind introducing quotients.

Here is the statement:

> Suppose $\phi : G \to H$ is a homomorphism of groups. Then ϕ induces an isomorphism $G/\ker\phi \cong \phi(G)$, where $\phi(G)$ denotes the image of ϕ.

This, as we will see, gives a quick way of identifying quotients of the form $G/\ker\phi$, which really covers all quotients G/N as long as we can find ϕ whose kernel is a given N. The proof goes as follows. First, recall that cosets of $\ker\phi$ in G correspond to the unique elements of the image $\phi(G)$:

$$g = g' \text{ in } G/\ker\phi \text{ if and only if } \phi(g) = \phi(g').$$

In other words, $\ker\phi$ measures the failure of ϕ to be be injective, so that by "collapsing" all of $\ker\phi$ down to the identity in $G/\ker\phi$, we get an *injective* homomorphism:

$$\phi : G/\ker\phi \to H.$$

We are abusing notation by continuing to refer to this map as ϕ, but the point is that it literally does the same thing as the original ϕ: $g \mapsto \phi(g)$. This is still well-defined on the domain $G/\ker\phi$ since $g = g'$ in this quotient means precisely that $\phi(g) = \phi(g')$, so that the element of H we get does not depend on the representative we pick for a given coset $g(\ker\phi)$ in $G/\ker\phi$.

This new map is injective precisely because elements g, g' for which $\phi(g) = \phi(g')$ become the same in $G/\ker\phi$. Finally, by cutting down the codomain H to consist of only the image $\phi(G) \leq H$, we guarantee that ϕ becomes surjective as well:

$$\phi : G/\ker\phi \overset{\cong}{\to} \phi(G),$$

so that this map induced by ϕ is indeed an isomorphism. Thus, as long as we can identify a given normal subgroup $N \trianglelefteq G$ as being the kernel of some well-chosen ϕ, we can identity the quotient $G/N = G/\ker\phi$ by looking at the image of ϕ.

Another analog in linear algebra. Here is yet another analog between group theory and linear algebra. Given a linear transformation $T : V \to W$ between finite-dimensional vector spaces V, W (again, just think about a matrix transformation $A : \mathbb{R}^n \to \mathbb{R}^m$ if you are not familiar with the language of vector spaces), the *rank-nullity* theorem asserts that the following holds:

$$\dim V = \dim \operatorname{im} T + \dim\ker T.$$

(The dimension of $\operatorname{im} T$ is called the *rank* of T, and $\dim\ker T$ is the *nullity of* T, hence the name "rank-nullity" theorem. In the case where $T = A : \mathbb{R}^n \to \mathbb{R}^m$ is a matrix transformation, this equality says that $n = (\#\text{ of pivots in } \operatorname{rref} A) + (\#\text{ of free variables in} \operatorname{rref} A)$, where $\operatorname{rref} A$ denotes the reduced row-echelon form of A.) In additive notation, taking orders in the First Isomorphism Theorem above gives

$$|G| - |\ker\phi| = |\phi(G)|, \text{ or equivalently } |G| = |\phi(G)| + |\ker\phi|,$$

and the analogy is clear. If you know about *quotient vector spaces* already (which we will study next quarter from the more general point of view of quotient *modules*), you might recall that the rank-nullity theorem is just a reflection of the underlying isomorphism between $V/\ker T$ (as a vector space) and $\operatorname{im} T$, which looks even more like the First Isomorphism Theorem here.

Example. Previously we argued informally that $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 2)\rangle \cong \mathbb{Z}$, and now we give a concrete proof. The goal is to find a surjective homomorphism

$$\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

whose kernel is $\langle(1,2)\rangle$; if we can do so, the First Isomorphism Theorem immediately gives the isomorphism we want. (Surjectivity means that $\phi(Z\times\mathbb{Z})=\mathbb{Z}$.) To find ϕ we simply rely on the work we did last time, where we determined that

$$(a,b)=(0,b-2a) \text{ in } (\mathbb{Z}\times\mathbb{Z})/\langle(1,2)\rangle$$

and used the remaining coordinate $b-2a$ as a hint that the data of an element in $(\mathbb{Z}\times\mathbb{Z})/\langle(1,2)\rangle$ should be determined by this single integer $b-2a$. Thus, we use precisely this data to define our homomorphism, sending (a,b) to $b-2a$:

$$\phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} \text{ is defined by } \phi(a,b)=b-2a.$$

Now we check that this has the properties we want. First, ϕ is indeed a homomorphism:

$$\phi((a,b)+(c,d))=\phi(a+c,b+d)=(b+d)-2(a+c)=(b-2a)+(d-2c)=\phi(a,b)+\phi(c,d).$$

Next, we note ϕ is surjective since for any $b\in\mathbb{Z}$ we have $\phi(0,b)=b$. Finally (a,b) is in $\ker\phi$ if and only if $b-2a=0$ if and only if $b=2a$ if and only if $(a,b)=(a,2a)\in\langle(1,2)\rangle$. Thus, $\ker\phi=\langle(1,2)\rangle$, so the First Isomorphism Theorem gives

$$(\mathbb{Z}\times\mathbb{Z})/\langle(1,2)\rangle=(\mathbb{Z}\times\mathbb{Z})/\ker\phi\cong\phi(\mathbb{Z}\times\mathbb{Z})=\mathbb{Z}$$

as desired. The fact that the isomorphism $(a,b)\to b-2a$ is well-defined and is injective on the quotient is hidden within the machinery of the First Isomorphism Theorem.

Lecture 15: More Isomorphism Theorems

Warm-Up 1. We justify that $(\mathbb{Z}\times\mathbb{Z})/\langle(5,5)\rangle\cong\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}$, which we previously argued informally should be true. To do so we find a surjective homomorphism

$$\phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}$$

whose kernel is $\langle(5,5)\rangle$. Recall when we argued informally the idea that we can always reduce the first coordinate of (a,b) in the quotient mod 5 so that it takes on a value in $\mathbb{Z}/5\mathbb{Z}$: if $a=5q+r$ with $0\leq r<5$, then

$$(a,b)=(5q+r,b)=(r,b-5q) \text{ in } (\mathbb{Z}\times\mathbb{Z})/\langle(5,5)\rangle.$$

This suggests we should take the first coordinate of $\phi(a,b)$ to be $a \bmod 5$: $\phi(a,b)=(a \bmod 5,?)$. The second coordinate should take on the role of any integer value if we want ϕ to be surjective, but we also want it to be true that $\phi(a,b)=0$ if and only if $(a,b)=\langle(5k,5k)\rangle$. In our case, having the first coordinate of $\phi(a,b)$ be $a \mod 5$ already forces $a=5q$ to be a multiple of 5 when (a,b) is to be in the kernel, and then the $b-5q$ second coordinate in the equivalent form of (a,b) above becomes simply $b-a$, which suggests using $b-a$ as the second coordinate, Then for (a,b) to be in the kernel will require that $b=a$, so that b equals the same multiple of 5 as does a, which is precisely what we need in for (a,b) to be the subgroup $\langle(5,5)\rangle$ we are quotienting by.

So we define ϕ by

$$\phi(a,b)=(a \bmod 5, b-a).$$

That this is a homomorphism follows from the fact that the mod 5 operation is a homomorphism and that subtraction on $\mathbb{Z}\times\mathbb{Z}$ is a homomorphism (you can check the details). This ϕ is surjective since any integer can be written as $b-a$ for some integers a,b, and $(a,b)\in\ker\phi$ if and only if $(a \bmod 5, b-a)=(0,0)$, which is true if and only if $b=a=5q$ for some $q\in\mathbb{Z}$. Hence the kernel is $\langle(5,5)\rangle$, and so our claim follows from the First Isomorphism Theorem.

Warm-Up 2. Suppose $A\trianglelefteq G$ and $B\trianglelefteq H$. Then it is true that $A\times B$ is normal in $G\times H$. (We will omit this verification here, but it is straightforward.) We claim that

$$(G\times H)/(A\times B)\cong(G/A)\times(H/B).$$

Thus the "naive" answer of $\frac{G\times H}{A\times B}=\frac{G}{A}\times\frac{H}{B}$ we would expect if these symbols denoted literal fractions is in fact true. (This is why the G/H notion for quotients is nice: in many ways it lines up with how we expect "quotients" to behave!) To prove this, we consider the homomorphism

$$\phi: G\times H\to(G/A)\times(H/B) \text{ defined by } \phi(g,h)=(\overline{g},\overline{h}).$$

To be clear, $(\overline{g},\overline{h})$ on the right denotes its value as an element (i.e. in terms of cosets) in the product of quotients $(G/A)\times(H/B)$ while (g,h) on the left denotes an actual element of $G\times H$. But the point is that essentially (g,h) should be sent to (a version of) itself!

That ϕ is a homomorphisms follows from the way in which multiplication in quotients is defined, or in other words from properties of projection maps $K\to K/N$, and it is surjective since projection maps are surjective: any $\overline{k}\in K/N$ is (at least) the projection of $k\in K$. Also, $(g,h)\in\ker\phi$ precisely when $(\overline{g},\overline{h})=(\overline{e_G},\overline{e_H})$ in $(G/A)\times(H/B)$, which happens precisely when $g\in A$ and $h\in B$. Thus $\ker\phi=A\times B$, so the First Isomorphism Theorem gives our result.

As an application, this immediately gives that $(\mathbb{Z}\times\mathbb{Z})/(n\mathbb{Z}\times m\mathbb{Z})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$.

Example. Here is another basic example. The determinant map $\det: GL_n(\mathbb{R})\to\mathbb{R}^\times$ which sends an invertible matrix to its determinant is a homomorphism, with kernel equal to the special linear group $SL_n(\mathbb{R})$ of matrices of determinant 1. This map is surjective since any $x\in\mathbb{R}^\times$ arises as the determinant of *some* matrix (say the diagonal matrix with diagonal entries $x,1,\ldots,1$), so the First Isomorphism Theorem gives

$$GL_n(\mathbb{R})/SL_n(\mathbb{R})\cong\mathbb{R}^\times.$$

This says that, in some sense, the only data an invertible matrix maintains if we ignore those matrices which have determinant 1 is its determinant. Or, said another way, given the data of a nonzero determinant value and a matrix of determinant 1, we can produce the data of an arbitrary invertible matrix.

Second Isomorphism Theorem. The next isomorphism theorem we consider is a consequence of the first, but is worth highlighting as a useful result in its own right. As with the second Warm-Up, the statement makes sense if we think about quotients naively as "fractions", so the point is that this can actually be made precise. Here is the statement of the *Second Isomorphism Theorem*:

> Suppose $A,B\leq G$ with B normal in G. Then AB is a subgroup of G, B is normal in AB, $A\cap B$ is normal in A, and $AB/B\cong A/(A\cap B)$.

Let us digest this a bit. First, the final conclusion is the "naive" answer we expect when interpreting the quotient notation as a literal fraction: in some sense, in AB/B the B's "cancel out" leaving us with A, *except* that we have to now take into account the fact that when "canceling out" elements of B, those elements of $A\cap B$ also get "cancelled out". In this context, "cancelling out' means to "set equal to the identity". Thus, we do get A as the resulting quotient, only we cannot distinguish between those elements of A which are also B since these are being set equal the identity.

Second, apart from the final isomorphism alone, also important is the fact that AB will in fact be a *subgroup* of G. Recall that this is not true in general, and is a crucial part of the statement since otherwise AB/B would not make sense as a quotient group. That AB being a subgroup of G is implied by B being normal in G follows from a fact we mentioned previously when discussing products: HK is a group if and only if $HK = KH$. (We omitted the details previously, and will still do so, but you should work it out on your own.) In fact, AB being a subgroup holds under more general assumptions than B being normal in all of G as we have stated here—for instance, it is enough to have $A \leq N_G(B)$. (This is the assumption the book actually uses.) But, in the practical examples we will encounter later on, it will be the case that B is in fact normal in G, so we prefer to use this assumption in our phrasing of the Second Isomorphism Theorem without worrying about more general ones which work. To give a brief sense of the context in which this theorem will arise later, the setting of having a group AB equal to a product like this with B being normal in it is the typical one which leads to consideration of *semi-direct products* (in the case where $A \cap B = 1$), which is a tool we will use to help classify groups. The notion of a "semi-direct product" of groups was introduced in the Discussion 2 Problems handout, and we will review the necessary details when we actually need them.

Finally, we point out that the other conclusions in the statement—B is normal in AB and $A \cap B$ is normal in A—need to be there in order for the resulting quotients to in fact be *groups*. The point is that assuming B is normal in G is actually enough to guarantee that everything showing up in the quotient isomorphism $AB/B \cong A/(A \cap B)$ makes sense. Moreover, this gives an equality between indices $[AB : B] = [A : A \cap B]$, which also follows (in the case where G is finite) from the following equality we derived previously:

$$|AB| = \frac{|A||B|}{|A \cap B|}, \text{ or equivalently } \frac{|AB|}{|B|} = \frac{|A|}{|A \cap B|}.$$

Indeed, in some sense this previously inequality foreshadows the statement of the Second Isomorphism Theorem.

Proof of Second Theorem. The proof of "isomorphism" part of the Second Isomorphism Theorem is an application of the First Isomorphism Theorem. (We will omit the check here that B is normal in AB and that $A \cap B$ is normal in A under the assumption that B is normal in G, but these are straightforward verifications.) The goal is to find a surjective homomorphism

$$\phi : A \to AB/B$$

whose kernel is $A \cap B$. But essentially if we interpret A and AB/B in the right way, there is a clear candidate: note $A = A\{1\}$ is a subgroup of AB, and so elements of A can already be thought of as elements of AB/B, and thus we can take ϕ to *essentially* be the map that sends everything to itself: $\phi(a) = a$, only with a on the right thought of as an element of AB/B.

It is clear than that this map is a homomorphism. If we take any $ab \in AB/B$, then $a = ab$ in AB/B, so $\phi(a) = a = ab$ and ϕ is surjective. Finally, the kernel of ϕ consists of those elements of A which become trivial after modding out by B, but this is precisely those elements of A which are actually in B. Hence $\ker \phi = A \cap B$ and the First Isomorphism Theorem gives the result. The point is that the map which induces the isomorphism which is claimed to exist is an "obvious" one in the sense that we just send each element to a "version of" itself.

Third Isomorphism Theorem. The third theorem we consider says naively that when "dividing fractions with the same denominator, the denominators cancel out": $\frac{g/h}{k/h} = \frac{g}{k}$. To be precise:

> Suppose $H \leq K \leq G$ with H, K both normal in G. Then K/H is normal in G/H and we have an isomorphism $(G/H)/(K/H) \cong G/K$.

(Note the resulting isomorphism has on the left a "qoutient group of quotient groups"!) It should be clear that K/H is a subgroup of G/H, since the fact that K was closed under multiplication in G is not lost when introducing extra relations. That K/H is normal in G/H is also a straightforward verification, so we omit it.

The isomorphism which is claimed to exist, as in the case of the Second Isomorphism Theorem, is a consequence of the First Isomorphism Theorem. Define $\phi : G/H \to G/K$ by sending anything in G/H to itself: $\phi(g) = g$. This makes sense—and gives a well-defined map—precisely because H is assumed to be in K: $g \in G/H$ still determines a unique element of G/K since introducing *more* relations will not invalidate any equalities which existed beforehand. More concretely: if $g = g'$ in G/H, g will still equal g' in G/K because $g = g'h$ for some $h \in H \leq K$ immediately gives $g = g'h$ for some $h \in K$. This is crucial, since otherwise ϕ would not be well-defined.

This ϕ then preserves multiplication, is surjective, and has kernel equal to the elements of G/H that become the identity in G/K, which means those elements which were in $K/H \leq G/H$ to begin with. Thus $(G/H)/\ker\phi \cong \phi(G/H)$ is precisely the result we want. It is all just really a matter of making sure that the various elements we consider are we we say they are, by chasing through the definitions of the various quotients and groups we are considering.

Here is a simple application. For n dividing m, $n\mathbb{Z}$ contains $m\mathbb{Z}$ so $n\mathbb{Z}/m\mathbb{Z}$ is a subgroup of $\mathbb{Z}/m\mathbb{Z}$. Then the Third Isomorphism Theorem gives:

$$(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}.$$

Lecture 16: Simple and Solvable Groups

Warm-Up. Let $\mathbb{C}^\times I := \{zI \mid z \in \mathbb{C}^\times\}$ denote the group of nonzero complex scalar multiples of the $n \times n$ identity matrix. (This is actually the center of $GL_n(\mathbb{C})$, and so is normal in $GL_n(\mathbb{C})$.) We identity the quotient $GL_n(\mathbb{C})/\mathbb{C}^\times I$ as a quotient of $SL_n(\mathbb{C})$ instead. The key observation is that any matrix in $GL_n(\mathbb{C})$ can be written as a product of elements of $SL_n(\mathbb{C})$ and $\mathbb{C}^\times I$:

$$A = \left(\tfrac{1}{\sqrt[n]{\det A}}A\right)(\sqrt[n]{\det A} \cdot I).$$

Here, $\sqrt[n]{\det A}$ denotes an n-th root (any will work, pick one!) of the complex number $\det A \in \mathbb{C}^\times$, and the fact that the first term has determinant 1 follows from the general result that for any scalar c we have $\det(cA) = c^n \det A$. Thus $GL_n(\mathbb{C}) = SL_n(\mathbb{C}) \cdot \mathbb{C}^\times I$, so since $\mathbb{C}^\times I$ is normal in $GL_n(\mathbb{C})$ the Second Isomorphism Theorem gives

$$GL_n(\mathbb{C})/\mathbb{C}^\times I = (SL_n(\mathbb{C}) \cdot \mathbb{C}^\times I)/\mathbb{C}^\times I \cong SL_n(\mathbb{C})/(SL_n(\mathbb{C}) \cap \mathbb{C}^\times I).$$

A scalar multiple of I has determinant 1 if and only if the scalar used is an n-th root of unity (since $\det(cI) = c^n \det I$), so the intersection $SL_n(\mathbb{C}) \cap \mathbb{C}^\times I$ consists of these specific matrices. Hence

$$GL_n(\mathbb{C})/\mathbb{C}^\times I \cong SL_n(\mathbb{C})/\{n\text{-th roots of unity}\}.$$

Let us give some context behind this result, just for the sake of interest. The group $GL_n(\mathbb{C})/\mathbb{C}^\times$ is an example of what's called a *complex projective general linear group*, and arises in the study of *complex projective* $(n-1)$*-space*. (It is the group of so-called *projective transformations* on this space.) This result gives an alternate description of this group, and indeed shows that the complex projective general linear group is isomorphic to the *complex projective special linear group* of the same dimension. (In general, in projective geometry we study geometry "up to scalar multiplication", which is hence why we quotient $GL_n(\mathbb{C})$ and $SL_n(\mathbb{C})$ out by the appropriate "scalar" subgroups of each. In other words, in projective geometry we cannot distinguish between A and cA, so we should treat them as the "same".)

Fourth Isomorphism Theorem. Let us mention one more "isomorphism theorem", which gives information about subgroups of a quotient G/N in terms of the subgroups of G. We should note that this result is not commonly listed as one of the isomorphism theorems in other sources, but our book does and so we do too. (Some other sources also switch the position of the Second and Third Isomorphism Theorems; everyone agrees on what the First Isomorphism Theorem is though.)

The key observation is that any subgroup of G/N is of the form H/N where H is a subgroup of G which contains N. Indeed, the preimage of any subgroup H' of G/N under the projection map $\phi : G \to G/N$ will be a subgroup $H := \phi^{-1}(H')$ of G containing N (since any $n \in N$ maps to $\phi(n) = e \in H' \leq G/N$, and so is in H), and *its* image under the same projection map is $H' = \phi(H) = H/N$, showing that $H' = H/N$ is of the required form. Note that for any subgroup A of G, its image $\phi(A)$ under projection is a subgroup of G/N regardless of whether A contained N, but the point is that this same $\phi(A) \leq G/N$ is *also* the image of its preimage $\phi^{-1}(\phi(A))$, which contains the original A. Hence even $\phi(A) \leq G/N$ will still be of the required form, it's just that the required form is $\phi^{-1}(\phi(A))/N$ and not "A/N", which is not defined if A does not contain N.

The Fourth Isomorphism Theorem then describes, under this correspondence, properties of subgroups of G/N in terms of those of G which contain N. For instance:

- H/N is normal in G/N if and only if H is normal in G;
- the index $[G/N : H/N]$ of H/N in G/N equals the index $[G : H]$ of H in G;
- $\langle H/N, K/N\rangle = \langle H, K\rangle/N$ (angled brackets here referring to subgroups generated by);

and so on. We will not list all the properties here, but will point them out when needed. Ultimately, this is about relating the lattice of subgroups of G/N to that of G.

Simple groups. We now define two types of groups which will play a role going forward: those which are *simple* and those which are *solvable*. To set the stage, consider the problem of "reconstructing" a group G from the data of a normal subgroup N and the corresponding quotient G/N. We will visualize this scenario in the following way:

$$N \hookrightarrow G \twoheadrightarrow G/N,$$

where $\hookrightarrow$ denotes an injective homomorphism—in this case the inclusion of N into G—and $\twoheadrightarrow$ a surjective homomorphism, in this case the projection of G onto G/N. The problem is then, given N and Q, to find the groups ? which fit into the middle of:

$$N \hookrightarrow\ ?\ \twoheadrightarrow Q$$

and thus will contain $N \leq\ ?$ as a subgroup and have $Q \cong\ ?/N$ as a quotient. This is known as an *extension problem*: can we "extend" Q by N to fill in the middle? The goal is to use information about the "simpler" (say of smaller order in the finite case) groups N and $Q = G/N$ to derive information about G. In some sense, we ask if we can "break" G down into pieces, study those pieces, and then put them back together to form G.

Now given the setup $N \hookrightarrow G \twoheadrightarrow G/N$, if N itself had a normal subgroup $N' \trianglelefteq N$, we could then "break" N down in the same way:

$$N' \hookrightarrow N \twoheadrightarrow N/N'$$

and hope to use the even simpler pieces $N', N/N'$ to build up to N, and then use $N, G/N$ to build up to G. If N' itself has a normal subgroup we can do this again, and so on and so on.

A simple group is then one which cannot be "broken down" further in this way. To be precise, a group G is *simple* if it has no nontrivial, proper normal subgroup: if $N \trianglelefteq G$, then $N = 1$ or $N = G$. Simple groups, as we will see, play a role analogous to prime numbers, in that they form—in the finite case at least—the building blocks of all groups. So far, the only groups we have seen which are simple are the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ of prime order.

Composition series. The problem of "breaking a group down into simple pieces" is then made precise by the following notion. A *composition series* of G is a chain of subgroups:

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq N_n = G$$

from the trivial subgroup 1 up to G, were each N_{i-1} is normal in the next N_i (it is NOT the case that each N_i need be normal in G) *and* where each successive quotient N_i/N_{i-1} is simple. It is this "simple quotient" condition which says that the chain cannot be made any longer (i.e. broken down further): N_i/N_{i-1} is not simple if and only there exists $N_{i-1} \leq K \trianglelefteq N$ giving a nontrivial, proper normal subgroup K/N_{i-1} of N/N_{i_1} which would then make the chain above longer by inserting K between N_{i-1} and N_i. The successive quotients N_i/N_{i-1} are called the *composition factors* of the series. Note that N_1 is itself simple since it is the first composition factor N_1/N_0.

Not all groups have a composition series; for instance, $\mathbb{Z}$ does not since it has no nontrivial simple subgroups to play the role of N_1 in the chain, because every subgroup of $\mathbb{Z}$ is also infinite cyclic and hence not simple. But, it is true at least that all finite groups have a composition series, as you will prove on a homework problem. For example, one composition series of $\mathbb{Z}/12\mathbb{Z}$ is:

$$0 \trianglelefteq \underbrace{4\mathbb{Z}/12\mathbb{Z}}_{\langle 4 \rangle} \trianglelefteq \underbrace{2\mathbb{Z}/12\mathbb{Z}}_{\langle 2 \rangle} \trianglelefteq \mathbb{Z}/12\mathbb{Z}.$$

The composition factors (respectively going left to right) are: $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}$. (This is an application of the Third Isomorphism Theorem; for instance $(\mathbb{Z}/12\mathbb{Z})/(2\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.) Another composition series is given by:

$$0 \trianglelefteq 6\mathbb{Z}/12\mathbb{Z} \trianglelefteq 3\mathbb{Z}/12\mathbb{Z} \trianglelefteq \mathbb{Z}/12\mathbb{Z}$$

and a third by

$$0 \trianglelefteq 6\mathbb{Z}/12\mathbb{Z} \trianglelefteq 2\mathbb{Z}/12\mathbb{Z} \trianglelefteq \mathbb{Z}/12\mathbb{Z}.$$

These respectively (left to right) have composition factors $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$, so even though it is not true that a composition series itself is unique (there are three here), what is true is that the composition *factors* of each series are unique up to some rearrangement. (In fact, the terms in the composition factors mimic the possible prime factorizations of 12—$3 \cdot 2 \cdot 2, 2 \cdot 2 \cdot 3$, and $2 \cdot 3 \cdot 2$—which will be true of all composition series of $\mathbb{Z}/n\mathbb{Z}$ in general.)

This final observation is true in general for any finite group: any two composition series of a finite group have the same length, and the composition factors in any such series are the same up to permutation of the factors. This is the content of the *Jordan-Hölder Theorem*, which can be proved using the Second Isomorphism Theorem. We will not give a proof here since composition series will not play a big role in what we will be doing, but some of the exercises in the book outline one proof if you're interested in trying it out. (The idea is to first prove the special case where one series has length three, and then to induct on the minimal length of two given series in general. The length two case can only occur for simple groups and there is not much to say beyond that.)

Extensions. Given a composition series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq N_n = G$$

of G, we can then hope to "build" from N_1 all the way up to G in the manner described previously. To be precise, the simple groups N_1 and N_2/N_1 fit into the picture

$$N_1 \hookrightarrow N_2 \twoheadrightarrow N_2/N_1,$$

so if we have complete knowledge of these simple groups, we hope to obtain complete knowledge of N_2. Then N_2 and the simple group N_3/N_2 fit into

$$N_2 \hookrightarrow N_2 \twoheadrightarrow N_3/N_2,$$

so if we have built up N_2 and have complete knowledge of the simple group N_3/N_2, we hope to obtain complete knowledge of N_3. But then having built up to N_3, we hope to use complete knowledge of the simple group N_4/N_3 to next build up to N_4, then to N_5, and so on up to $N_n = G$.

We will say a bit next time about how part of this problem—having complete knowledge of all simple groups—has actually been fully solved in the finite case. However, the remaining part—knowing how to "build up" from simple groups to other groups—is intractable. The issue is that in general knowing N and G/N is not enough to actually identity G itself, since there can in fact be multiple groups which fit into the "extension problem" given by

$$N \hookrightarrow\ ?\ \twoheadrightarrow G/N.$$

In general, such a group is in the middle is called an *extension* of G/N by N, of which there can be many, so that even if all the simple groups needed can be well-understood, it might not be possible to solve all the resulting extension problems to see how to put them together correctly when building up to G. The best we can hope to do is to classify (maybe up to isomorphism) the possible extensions we get along the way, so that we get a range of possibilities for what G can be. We will not go into this much further, except for one scenario when we can say quite a bit more, that being when an extension of $Q = G/N$ by N can be described as a *semi-direct product* of Q and N. Indeed, semi-direct products arise precisely when trying to solve such extension problems, and were briefly previously when discussing the types of scenarios we'll see later on where the Second Isomorphism Theorem could prove useful. As we said back then, we'll save giving the formal definition until we actually need to do so later.

Solvable groups. Even though we will not do much with composition series, there is a related notion which *will* be crucially important for us, at least in the spring. A group G is *solvable* if there is a chain of normal subgroups from the trivial group 1 up to G:

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq N_n = G$$

with each successive quotient N_i/N_{i-1} being *abelian*. For instance, any abelian group G is solvable, simply because the two-term chain $1 \trianglelefteq G$ already satisfies the requirement in the definition. Dihedral groups are also solvable since

$$1 \trianglelefteq \langle r \rangle \trianglelefteq D_{2n}$$

has successive quotients $\langle r \rangle$ and $D_{2n}/\langle r \rangle \cong \mathbb{Z}/2\mathbb{Z}$, which are both abelian. In fact, any group of order less than 60 is solvable, which we will essentially prove (although we might not phrase it all completely in terms of the language of "solvability") in the remaining time this quarter. The smallest non-solvable group occurs in the order 60 case, and is a group we will define next time.

The notion of solvability above might seem to be quite random at first, but we will see in the spring that this is *precisely* (!!!) what is needed in order to say that the roots of polynomial can be described via an explicit algebraic formula. (Actually, this is a bit of a lie: what is actually needed are *cyclic* quotients, but for finite groups having abelian quotients is equivalent to having cyclic quotients, as we will see.) Indeed, the term "solvable" here comes exactly this relation to solving polynomial equations. The fact that there is a non-solvable group of order 60 but not of any smaller order is ultimately the reason why there exists a quartic (and quadratic and cubic) formula, but not a "quintic formula". We have much to look forward to!

Lecture 17: Alternating Groups

Warm-Up 1. We find all composition series of $\mathbb{Z}/30\mathbb{Z}$. First let us clarify an observation we made last time when considering $\mathbb{Z}/12\mathbb{Z}$, that a composition series should correspond to a way of expressing the prime factorization of 30. The second to last term $p\mathbb{Z}/30\mathbb{Z}$ in a composition series will be generated by some p, and in order this the corresponding quotient $(\mathbb{Z}/30\mathbb{Z})/(p\mathbb{Z}/30\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ to be simple requires that p be prime. But then the same will be true of the term before $p\mathbb{Z}/30\mathbb{Z}$ in the composition series: $pq\mathbb{Z}/30\mathbb{Z}$ (which is what a subgroup of $p\mathbb{Z}/30\mathbb{Z}$ would have to look like) will yield a simple quotient $\mathbb{Z}/q\mathbb{Z}$ only when q is prime, and so on the further to the left we move in the composition series. Thus we start by picking one prime dividing 30 to form the second-to-last term, then another (not necessarily different) prime to form the term before this, and so on.

Thus since $30 = 2 \cdot 3 \cdot 5$, there are 3 possible composition series, with composition factors $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ in some order. (So since $24 = 2 \cdot 2 \cdot 2 \cdot 3$, $\mathbb{Z}/24\mathbb{Z}$ has 4 composition series.) The composition series of $\mathbb{Z}/30\mathbb{Z}$ are:

$$0 \trianglelefteq 6\mathbb{Z}/30\mathbb{Z} \trianglelefteq 2\mathbb{Z}/30\mathbb{Z} \trianglelefteq \mathbb{Z}/30\mathbb{Z}$$
$$0 \trianglelefteq 6\mathbb{Z}/30\mathbb{Z} \trianglelefteq 3\mathbb{Z}/30\mathbb{Z} \trianglelefteq \mathbb{Z}/30\mathbb{Z}$$
$$0 \trianglelefteq 10\mathbb{Z}/30\mathbb{Z} \trianglelefteq 5\mathbb{Z}/30\mathbb{Z} \trianglelefteq \mathbb{Z}/30\mathbb{Z}$$

with composition factors $\{\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}, \{\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$, and $\{\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}\}$ respectively. (The fact that any finite group has a composition series and that composition factors are unique essentially gives a very elaborate proof of the Fundamental Theorem of Arithmetic!)

Warm-Up 2. Suppose $N \trianglelefteq G$. We show that if N and G/N are solvable, then G is solvable. Thus, "solvability" is a property preserved under the taking of extensions. This will be useful later when we come to a need to know whether a group is solvable or not, in that we can determine if it is by considering the hopefully simpler groups N and G/N.

This comes down to the correspondence between subgroups of G/N and those of N together with the Fourth Isomorphism Theorem. Since N is solvable there exists a chain

$$1 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq N$$

with each N_i/N_{i-1} abelian, and since G/N is solvable there exists a chain

$$N/N \trianglelefteq H_1/N \trianglelefteq \ldots \trianglelefteq H_{n-1}/N \trianglelefteq G/N$$

with each successive quotient abelian. Here, each H_i is a subgroup of G containing N, and we have used the fact that normal subgroups of H_i/N correspond to normal subgroups of H_i. This thus lifts to a chain of the form

$$N \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq G,$$

which together with the first chain above gives

$$1 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq N \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq G.$$

We already know from above that the successive quotients for the terms up to N are abelian, and for the remaining quotients the Third Isomorphism Theorem gives

$$(H_i/N)/(H_{i_1}/N) \cong H_i/H_{i-1},$$

so since the "quotients of quotients" on the left are abelian so are the quotients on the right. Hence G is solvable if N and G/N are.

Classification of simple groups. We will briefly mention one last fact, simply for the sake of interest and because it is truly a monumental achievement in modern mathematics of which any student should be aware. Looking back to the use of composition series to "build up" to arbitrary (finite) groups from simple groups, we mentioned that the process of "building up" in this way—i.e. the extension problem—was intractable in general, but that the problem of understanding the possible simple groups used in this process was in fact solved: the complete list of finite simple groups (up to isomorphism) is known. The problem of classifying finite simple groups in this way began in earnest in the 1950's, and was thought to be completed at first in the 1980's, only for some holes to be discovered soon after, which were finally fully overcome in the early 2000's.

Let us describe in a very rough way the list of finite simple groups. First, there are the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ of prime order, which make up the first *family* of finite simple groups. Next, there is a second family of groups denoted by A_n for $n \geq 5$, which we will define after this brief digression. Next we have the so-called groups of "Lie type" which in a very very rough sense are essentially groups which can be described as certain matrix groups, only with entries being a more elaborate type of "number", like something in $\mathbb{Z}/p\mathbb{Z}$ for instance. We will not give any more of a formal definition of a group of "Lie type" than this, but the point is that this comprises an infinite number of groups which can all be constructed or described in "similar" ways.

Finally, there are exactly 26 remaining finite simple groups which do not fall into any such nice "family" as opposed to those above, and whose existence might appear at first to be a random coincidence. These are the known as the *sporadic* simple groups. Of these, the one of largest order is called the *monster group* (yes, that is indeed the official name), due to the fact that its order is:

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

(Holy cow is that a huge number!) It is quite astonishing that a group of this crazy larger order could in fact be simple (this order is highly non-prime), let alone that anyone would have ever thought to look for it, *and* be able to actually construct it. Even crazier perhaps is the fact that monster group is now known to have connections to theoretical physics, but that is a story for another time and place. It is truly a testament to the power of mathematical thinking that this group, and indeed all finite simple groups, have indeed been found.

Parity of permutations. The groups A_n for $n \geq 5$ in the second family mentioned in the classification above are known as the *alternating groups*, which we will now work towards defining. First, we need the notion of what it means for a permutation $\sigma \in S_n$ to be *even* or *odd*:

> $\sigma \in S_n$ is an *even* permutation if it can be written as a product of an even number of transpositions, and it is an *odd* permutation if it can be written as a product of an odd number of transpositions.

(Recall that any permutation can be written as a product of *some* number of transpositions since the transpositions generate all of S_n.) The key point is that this definition makes sense, in that a permutation cannot be both even and odd simultaneously: a given permutation can be written as a product of transpositions in multiple different ways, but all such ways will always contain either an even number of 2-cycles overall or an odd number of 2-cycles overall. We will prove this fact shortly. The term "parity of a permutation " refers to this property of being either even or odd.

For instance, a single 2-cycle (ab) is odd, since it already consists of one transposition. A 3-cycle (abc) is even since

$$(abc) = (ab)(bc)$$

consists of two transpositions. Again, this type of expression is not unique, since we also have for instance

$$(abc) = (ab)(bc)(ac)(ac)(bc)(bc),$$

but what *is* unique is the parity of the number of transpositions used. A 4-cycle is odd:

$$(abcd) = (ab)(bc)(cd),$$

and so on in general a cycle of *even* length is odd and a cycle of *odd* length is even. (Note the mismatch between the parity of the length and the parity of the cycle as a permutation!) From this, it is easy to determine the parity of any permutation by looking at its disjoint cycle decomposition, since odd $\cdot$ odd = even, odd $\cdot$ even = odd = even $\cdot$ odd, and even $\cdot$ even = even.

Alternating groups. The *alternating group* A_n is then defined to be the subgroup of S_n consisting of the even permutations. That this is a subgroup follows from the fact that the identity permutation $(1) = (12)(12)$ is even, even times even is even, and inverting cycles preserve their lengths. The order of A_n is exactly half the order of S_n: $|A_n| = \frac{n!}{2}$. (Thus A_n has index 2 in S_n, and the non-identity coset consists of the odd permutations.) This can be seen from the fact that there are as many even permutations as there are odd ones, since the function

$$\{\text{even permutations}\} \to \{\text{odd permutations}\} \text{ defined by } \sigma \mapsto \sigma(12)$$

is a bijection between finite sets (it equals its own inverse).

So, for instance, A_4 is a group of order $\frac{4!}{2} = \frac{24}{2} = 12$. It contains the identity, all 3-cycles (of which there are 8), and 3 more elements which are products of two disjoint transpositions:

$$A_4 = \{(1), (123), (132), (134), (143), (124), (142), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

On a previous set of discussion problems it was shown (although we were not using the language of even and odd permutations at the time) that

$$N = \{(1), (12)(34), (13)(24), (14)(23)\}$$

is actually a normal subgroup of A_4, which shows that A_4 is not simple. We will show later, after we have a few more tools built up, that A_n is simple for $n \geq 5$. (A_5 has order $\frac{120}{2} = 60$, and is in fact the smallest non-abelian simple group, and the smallest non-solvable group.) This is not to say that A_n is simple *only* for $n \geq 5$, since $A_1 = A_2 = 1$ and $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ are simple as well; so, in fact, A_4 is the only non-simple alternating group.

Inversions. We now work towards proving that our notion of even vs odd when it comes to permutations is well-defined in that a given permutation can only be one of these. We give essentially the same argument as the book, but phrased in a different (I think simpler) way. (In fact, the book takes the concept we are about to introduce as the starting point in defining even vs odd, and then *later* shows that this can be recast in terms of the number transpositions required in a product expression. I prefer taking the latter approach as the definition, since we almost exclusively think of elements of S_n in terms of cycles anyway)

Given $\sigma \in S_n$, an *inversion* occurs whenever we have $i < j$ but $\sigma(i) > \sigma(j)$. (Here $\sigma(i)$ is the result of evaluating the *function* σ at $i \in \{1, 2, \dots, n\}$.) As the name suggests, an inversion occurs whenever σ "inverts" two elements in $\{1, 2, \dots, n\}$ in the sense that it swaps their ordering relative to one another. For instance, take the permutation $\sigma = (1423)$ which as a function sends each of 1234 respectively to

$$4312.$$

Here, σ inverts $1 < 2$ since $\sigma(1) = 4 > \sigma(2) = 3$, it inverts $1 < 3$ since $4 > 1$, and it also inverts $1 < 4$, $2 < 3$, and $2 < 4$. It does not invert $3 < 4$ since $\sigma(3) = 1 < \sigma(4) = 2$ still holds. (Visually, in the notation above, an inversion occurs whenever a number is larger than a number to its right.) Thus $\sigma = (1423)$ has 5 inversions. We define the *sign* of a permutation σ, denoted $sgn(\sigma)$, to be

$$(-1)^{\#\text{ of inversions}} = \begin{cases} 1 & \text{number of inversions is even} \\ -1 & \text{number of inversions is odd.} \end{cases}$$

The claim is that this notion of parity in terms of the number of inversions is the same as the one we defined previously, so that even permutations have sign 1 and odd permutations have sign -1.

Before proving this, let us clarify the book's approach to defining parity. Take the product of polynomials $x_i - x_j$ for $i < j$ among $1, 2, \dots, n$:

$$\prod_{1 \le i < j \le n} (x_i - x_j).$$

An element $\sigma \in S_n$ acts on this by permuting the indices:

$$\prod_{1 \le i < j \le n} (x_i - x_j) \mapsto \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Each resulting factor $x_{\sigma(i)} - x_{\sigma(j)}$ still occurs among our original factors $x_i - x_j$, only that the order of the indices might be switched: if σ inverts $i < j$, $x_{\sigma(i)} - x_{\sigma(j)}$ has the wrong index order, and so actually equals the *negative* of the factor $x_{\sigma(j)} - x_{\sigma(i)}$ in the original product. Thus the product above with permuted indices equals ± 1 the original product, with the sign coming from -1 raised to the number of indices which were inverted. Hence we recover the definition of $sgn(\sigma)$ we have given above. You can decide for yourself whether our approach or the book's is simpler to follow.

Parity makes sense. Let us finally then justify that the two notions of parity introduced above (number of transpositions vs sign) agree. The key point is that the inversion/sign approach depends only on the behavior of a permutation as a *function*, and hence whether we get $sgn = 1$ or -1 depends only on the permutation without any reference to what its cycle decompositions look like.

Take a transposition of adjacent terms $(a\ a+1)$, and consider the product $\tau = \sigma(a\ a+1)$ in relation to $\sigma \in S_n$ itself. We claim that τ and σ differ by exactly 1 in the number of inversions in each. First, τ and σ have the same effect on any $i \in \{1, 2, \dots, n\}$ which is not a or $a+1$, so the number of inversions in each can only differ when considering $a < a+1$. But:

$$\tau(a) = \sigma(a+1) \quad \text{and} \quad \tau(a+1) = \sigma(a),$$

so that if σ inverts $a < a+1$, τ will not, while if σ does not invert $a < a+1$, τ will. Hence σ and $\sigma(a\ a+1)$ do differ in their number of inversions by exactly 1; in other words, each time we multiply by an adjacent transposition $(a\ a+1)$, we change the number of inversions by 1.

We know from prior work that any $\sigma \in S_n$ can be written as a product of *adjacent* transpositions. (This was a previous homework problem: $(12), (23), \ldots, (n-1\ n)$ generate S_n.) An important observation is that using only adjacent transpositions as opposed to arbitrary transpositions does not alter whether we use an even or odd number overall: we have

$$(a\ a+k) = (a\ a+1)(a+1\ a+k)(a\ a+1),$$

and inductively continuing to break $(a+1\ a+k)$ down into an expression with $(a+2\ a+k)$, then $(a+3,\ a+k)$, and so on will result in an odd number (the 2 broken off at each step plus the $(a+k-1\ a+k)$ leftover in the end) of adjacent transpositions overall. Thus if we write σ as a product of transpositions, and then rewrite each of those in terms of only adjacent transpositions, the parity of the number used remains the same.

But each time we introduce a new adjacent transposition, the parity (in terms of number of inversions) changes as we showed above. Thus, suppose $\sigma \in S_n$ and write it has a product of any number of transpositions, which we can then take to be adjacent:

$$\sigma = \tau_1 \ldots \tau_k.$$

Since τ_1 has one inversion, $\tau_1\tau_2$ has an even number, then $\tau_1\tau_2\tau_3$ has an odd number, etc. Since the number of inversions—and hence its parity—depends only on σ as a function, the right side above must have this same parity, which means that k is even when $sgn(\sigma) = 1$ and odd when $sgn(\sigma) = -1$. Thus the two notions of parity agree and hence a permutation cannot be both even and odd (in the sense of our original definition) at the same time.

Lecture 18: Orbit-Stabilizer Theorem

Warm-Up 1. We find a composition series of A_4, and use it to show that A_4 is solvable. Last time we stated that

$$N = \{(1), (12)(34), (13)(24), (14)(23)\}$$

is a normal subgroup of A_4, as was shown on the Discussion 3 Problems handout. This N is abelian (it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), so any subgroup is normal. Thus for instance

$$1 \trianglelefteq \{(1), (12)(34)\} \trianglelefteq N \trianglelefteq A_4$$

is one possible chain of normal subgroups. The successive quotients going from left to right are: $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$, which are all simple, so this is a composition series. Other composition series are obtained by using either $(13)(24)$ or $(14)(23)$ instead of $(12)(34)$ to give the second term.

Since the quotients above are all abelian, this shows immediately that A_4 is solvable.

Warm-Up 2. We show that S_n can be realized as a subgroup of A_{n+2}. Define the map

$$\phi : S_n \to A_{n+2} \text{ by } \phi(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma(n+1\ n+2) & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then ϕ is a homomorphism, which can be checked by considering the different cases:

- if $\sigma, \tau \in S_n$ are both even, then $\sigma\tau$ is even and $\phi(\sigma\tau) = \sigma\tau = \phi(\sigma)\phi(\tau)$;

- if one of σ, τ is even and the other odd, then $\sigma\tau$ is odd and $\phi(\sigma\tau) = \sigma\tau(n{+}1\; n{+}2) = \phi(\sigma)\phi(\tau)$, where we use that $(n+1\; n+2)$ is disjoint from σ and τ to say it commutes with each; and
- if σ, τ are both odd, then $\sigma\tau$ is even and $\phi(\sigma\tau) = \sigma\tau = \sigma(n+1\; n+2)\tau(n+1\; n+2)$, which is $\phi(\sigma)\phi(\tau)$, where we use the fact that $(n+1\; n+2)$ has order 2.

Moreover, if $\phi(\sigma) = \phi(\tau)$, then either both of these elements of A_{n+2} fix $n+1$ and $n+2$, or they both transpose them: in the first case, we have have $\phi(\sigma) = \sigma$ and $\phi(\tau) = \tau$, so $\sigma = \tau$, while in the second case $\phi(\sigma) = \sigma(n{+}1\; n{+}2)$ and $\phi(\tau) = \tau(n{+}1\; n{+}2)$, so that $\sigma(n{+}1\; n{+}2) = \tau(n{+}1\; n{+}2)$ also implies $\sigma = \tau$. This shows that ϕ is injective, so S_n is isomorphic to the image of ϕ, which is the desired subgroup of A_{n+2}.

A_n **is normal.** We finish, for now, our discussion of A_n by pointing out that it is always a normal subgroup of S_n. This comes immediately from fact A_n has index 2: in general, if $[G : H] = 2$, then the left cosets of H are H, gH for some $g \notin H$, and the right cosets are H, Hg, so since the sets in each of these pairs are disjoint and together give everything in G, we must have $gH = Hg$, so that H is normal as claimed. (That index 2 implies normal also follows from the homework problem saying that a subgroup $H \leq G$ whose index is the smallest prime dividing $|G|$ must be normal, but the argument above is a lot simpler than this general fact.)

We can also see that A_n is normal by noting that it is the kernel of the *sign* homomorphism: $sgn : S_n \to \{\pm 1\}$. Here we view $\{\pm 1\}$ as a group under multiplication, and the fact that sgn preserves multiplication comes from the fact that even times even is even, even times odd is odd, and odd times odd is even, where here "even" and "odd" refer to permutations, not integers. The identity of $\{\pm 1\}$ is 1, and those permutations with $sgn = 1$ are precisely the ones which are even.

As a consequence, we can now say that S_4 is solvable:

$$1 \trianglelefteq \{(1), (12)(34)\} \trianglelefteq \{(1), (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4 \trianglelefteq S_4$$

has successive quotients which are all prime cyclic and hence abelian.

Orbit-stabilizer theorem. We will return to properties of permutation groups later, but for now take a brief detour to highlight a useful fact about group actions: the *orbit-stabilizer theorem.* The book states this as part of a proposition, but does not call it "orbit-stabilizer theorem" nor give it the prominence it deserves.

Here is the claim. Suppose we are given an action $G \curvearrowright X$. Recall that for $x \in X$, Gx denotes the orbit through x and G_x the stabilizer of x. The orbit-stabilizer theorem states that the index of G_x in G is equal to the cardinality of Gx:

$$[G : G_x] = |Gx|.$$

Thus, the size of any orbit for *any* group action of G can be obtained solely from information about the group and its subgroups alone. (In a sense then, this says that studying arbitrary group actions "essentially" comes down to studying the action of G on its subsets by left multiplication.) One of the more important consequences is then, that, when G is finite, we have

$$|G| = |G_x||Gx|$$

(this uses $[G : G_x] = \frac{|G|}{|G_x|}$), so that the order of G can be derived solely from knowledge of a single orbit and the corresponding stabilizer.

The orbit-stabilizer theorem follows from recognizing when two elements $g, h \in G$ give the same element in the orbit Gx: $g \cdot x = h \cdot x$ if and only if $x = (g^{-1}h) \cdot x$ if and only if $g^{-1}h \in G_x$ if and only if g and h determine the same coset of G_x in G. Thus, the number of distinct elements in Gx equals the number of distinct cosets of G_x (or, said another way so that this applies even in the infinite setting, we have a bijection between the orbit Gx and the set G/G_x of cosets), which gives our claim.

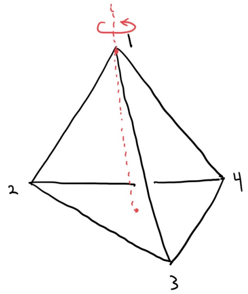
Example. Here is an example of the typical type of application of the orbit-stabilizer theorem. Previously we argued that D_{2n} has order $2n$ by stating that it consisted of n rotations and n reflections, or by using the generators and relations to explicitly describe all elements. We can also obtain this fact from the orbit-stabilizer theorem as follows, where the point is that we do not need to have any a priori knowledge about generators and relations, nor precisely how many rotations and reflections there will be ahead of time.

Consider the usual action of D_{2n} on $\{1, 2, \dots, n\}$, viewed as the vertices of a regular n-gon. Take vertex 1. For any other vertex, there is a rotation which will take 1 to it, so all vertices lie in the orbit of 1 under the action of D_{2n}. Also, the only non-identity element of D_{2n} which fixes 1 is the reflection across the line passing through 1, so the stabilizer of 1 has order 2. Thus the orbit-stabilizer theorem gives

$$|D_{2n}| = |\text{stabilizer}||\text{orbit}| = 2n,$$

just as we would expect.

Symmetries of a tetrahedron. Here is another example, now in a setting where do not know the answer ahead of time. Let G be the group of rigid (i.e. rotational) symmetries of a regular tetrahedron. (Recall that "rigid" symmetries are ones which can be realized by motions in $\mathbb{R}^3$, so reflections of a 3-dimensional solid do not count.) Label the vertices of the tetrahedron by $1, 2, 3, 4$:



For any vertex there is a rotation which will move vertex 1 to it, so the orbit through vertex 1 has size 4. Also, the only rotations which fix vertex 1 are those which occur around the line passing through 1 and the center of the opposite face, and there are 3 of these: the opposite face is an equilateral triangle, and there are three rotations of this triangle. Thus, the orbit-stabilizer theorem gives the order of G as:

$$|G| = |\text{stabilizer}||\text{orbit}| = 3 \cdot 4 = 12.$$

Now, to determine which group of order 12 we have, use the action above to realize G as a subgroup of S_4 upon permuting the vertices. (Note that different rotations induce different permutations, so the map sending an element of G to the element of S_4 it induces is indeed injective.) With the labeling above, the rotations which occur around the line passing through 1 and the center of the opposite face are:

$$(1), (234), (243).$$

The rotations which occur around the line passing through vertex 2 will only permute vertices $1, 2, 4$, and we get:

$$(1), (124), (142).$$

And so on, considering the rotations which fix each of the other two vertices will give the remaining 3-cycles, so thus far we have:

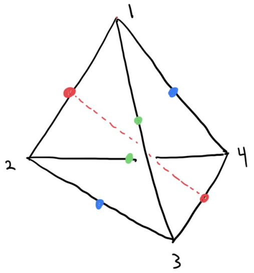
$$(1), (234), (243), (124), (142), (134), (143), (123), (132) \in G.$$

Products of any of two of these will also give elements of G, and by computing them (and knowing that G has 12 elements in order to avoid doing so much work), we get that G is exactly A_4:

$$G = \{(1), (234), (243), (124), (142), (134), (143), (123), (132), (12)(34), (13)(24), (14)(23).\}$$

(This essentially proves the fact that A_4 is generated by 3-cycles, which you will show on the homework is true for general n.)

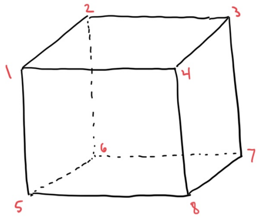
This finishes justifying our claim, but we can now try to visualize the exact rotations that produce $(12)(34), (13)(24), (14)(23)$. These are tougher to see than the ones which give 3-cycles, since the axes of rotations are not so straightforward to visualize. They arise by taking lines which pass through the midpoint of one edge and the midpoint of the *opposite* edge (same colors in the picture below):



If you think about the effect of rotating around *these* lines, you can convince yourself that such rotations will indeed transpose two pairs of vertices.

Lecture 19: More on Permutations

Warm-Up. We determine the rotational symmetry group G of a cube. For convenience, we label the vertices of the cube in the following way:



We first find the order of G. Each rotation in G induces a permutation of the vertices, so we get an action of G on the set of 8 vertices. Pick a vertex, say vertex 1. Then the orbit through 1 consists of all 8 vertices since any one vertex can be moved to any other via some rotation. (This is what it means to say that this action is *transitive*: there is only one orbit.) The stabilizer of vertex 1 consists of those rotations which occur about the axis connecting vertices 1 and 7, and there are three such rotations overall. (This is not to easy to see via the picture alone, but if you take an actual physical cube and spin it while holding two opposite vertices fixed, you will be able to easily see that there are three resulting rotations.) Thus the orbit-stabilizer theorem gives:

$$|G| = |G_1||G \cdot 1| = 3 \cdot 8 = 24.$$

Let us also derive this by considering a different action, where the size of the stabilizer is possibly simpler to identify. Any rotation also induces a permutation of the *faces* (i.e. sides) of the cube, so G acts on the set of 6 faces. This action is also transitive, since any one face can be rotated into any other, so there is only one orbit of size 6. The stabilizer of, say, the bottom face consists of those rotations which occur about the vertical axis, and there are 4 such rotations overall: $90, 180, 270, 0$. Thus we get $|G| = |G_{\text{bottom face}}||G \cdot (\text{bottom face})| = 4 \cdot 6 = 24$ as well.

Now the goal is to determine which group of order 24 we actually have. One approach is to use the action of G on the vertices to realize G as a subgroup of S_8: each rotation induces a *different* permutation of the 8 vertices, so we get an injective homomorphism $G \hookrightarrow S_8$ (this is what it means to say that this action is *faithful*: different elements induce different permutations.) whose image is a subgroup of S_8 which is isomorphic to G. So one answer as to what group G actually is to write down all of the resulting permutations. For instance, rotating around the vertical axis by 90 counterclockwise if viewed from above has the following effect on the vertices:

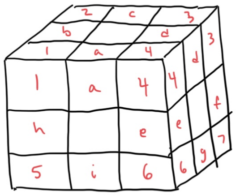
$$1 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1 \text{ and } 5 \mapsto 8 \mapsto 7 \mapsto 6 \mapsto 5,$$

so this rotation gives the permutation $(1432)(5876)$. Writing down all 24 permutations of S_8 we get is tedious and will not help to easily identity what G actually is. Alternatively, we could also consider the action (also faithful) on the faces to realize G as a subgroup of S_6, which gives "simpler" description of G than the first approach, but still not satisfying.

So we look for a better action to consider. Note that G is not abelian, since composition of 3-dimensional rotations is not commutative (composition of 2-dimensional rotations *is* commutative!), and G is not D_{24} since D_{24} has 12 elements of order 2 whereas G only has 9. (This is not so easy to see purely geometrically, but if nothing else you can write down G as a subgroup of S_8 or S_6 and determine the elements of order 2 from there.) Apart from D_{24}, the only other non-abelian group of order 24 we have worked with so far is S_4, so perhaps let us make a guess that $G \cong S_4$. If so, and to prove this, we should be looking for an action of G on a 4-element set.

In fact, we can take the action of G on the four *diagonals* of the cube, or equivalently on the set of *pairs* of vertices $\{1, 7\}, \{2, 8\}, \{3, 5\}, \{4, 6\}$ which form the endpoints of the diagonals. Any rotation induces a permutation of these 4 objects (diagonals or pairs), so we get a homomorphism $G \to S_4$. Different rotations will induce different permutations (it might take a little effort to see this geometrically!), so this action is faithful, meaning that the map $G \to S_4$ is injective. Thus G is isomorphic to the image, and since $|G| = 24$ this image has order 24 as well, meaning that the image is all of S_4. Hence $G \cong S_4$. This same action could also have been used to determine the order of G, although it might be a little tougher to do so here as opposed to using the action on the faces for instance. (For the action on the diagonals/pairs, there is a single orbit of size 4 and each stabilizer has order 6, which come from the three rotations which fix a specific vertex, *and* the three rotations which transpose that vertex with its opposite vertex, and thus leave the corresponding diagonal unchanged.) Thus this is a nice example where considering different actions is very useful: one action to find the order, and a different to identity the group afterwards.

Rubik's cube group. Let us take a brief digression to discuss a particularly interesting example of a group which can studied using these tools, the so-called *Rubik's cube group*, which everyone should see at least once in their lifetime. Consider a standard Rubik's cube:



with corners labeled with $1, \ldots, 8$ (corner 8 in the bottom, back, left corner is not visible in the picture above) and "edge" blocks labeled with $a, b, c, \ldots, \ell$ (12 total). Each "move" we can perform on the cube (rotate a face) induces a permutation of the corners and edges, so that we can describe such moves using cycle notation. (None the "center" pieces in the middle of each face ever move, so we need not keep track of them.) For instance, the rotation U (for "upper") of the top face by 90 *clockwise* if viewed from above is given by:

$$U = (1234)(abcd).$$

Then U^2 corresponds to rotating twice, U^3 is three times, and U^4 is the identity. Rotating each other face by 90 in a similar way (clockwise if viewed the right way) gives more permutations, commonly denoted by D, L, R, F, B for "down" (bottom face), "left", "right", "front", and "back".

The Rubik's cube group is then (almost!) defined to be the group generated by these 6 rotations:

$$G = \langle U, D, L, R, F, B \rangle.$$

The point is that an element of G corresponds to a certain configuration of the cube: perform the rotations dictated by the product expression for this element on the "trivial" identity configuration (where everything is in the correct place) to obtain the desired configuration. This is *mostly* the correct group but not quite, since we have made no mention of the *orientation* of each corner and edge, meaning which *color* each side actually uses. (Of course, when solving the cube the colors are important!) So, actually, G as defined above is only a *quotient* of the full Rubik's cube group, where we quotient out by the normal subgroup generated by all the configurations where each corner/edge is in the correct location, only with the orientation of each possibly incorrect in relation to the trivial configuration. (Try to convince yourself that this does give a normal subgroup! The effect of taking such a quotient is to focus first only on the position of each corner/edge, not yet on what color each side has.) The full Rubik's cube group should take these orientations into account as well.

Nevertheless, the group G above already gives a group-theoretic approach towards studying Rubik's cubes. To "solve" a cube from an initial configuration is then equivalent to figuring out how to express that configuration in terms of the generators U, D, L, R, F, B; if the configuration can be written as $g_1 g_2 \cdots g_k$ where each g_i is one of these generators, to solve the cube then means for perform the moves $g_k^{-1} \cdots g_2^{-1} g_1^{-1}$. The order of G can be found using the orbit-stabilizer theorem for instance (not so straightforward though!), and much other information about G and the full Rubik's cube group is also known. For instance, the fact that from any initial configuration it takes at most 20 moves to solve the cube is then a statement about how many generators it takes to express a given configuration. Many modern algorithms for solving cubes come from finding a *minimal* expression in terms of generators, and such considerations lead into the subject of *computational/combinatorial group theory*. Good stuff!

Existence of cycle decompositions. Let us now clarify one property of permutations we had deferred proving: the fact that any permutation $\sigma \in S_n$ can be written as a product of disjoint cycles, which is unique up to the order in which the cycles are written. This is in some sense obvious if you simply compute the disjoint cycle expression for a given, *explicit* permutation (as we have done numerous times before), but takes some thought to actually prove can always be done in a way which avoids having explicit information about the permutation available. Given $\sigma \in S_n$, one approach is to first consider the terms:

$$1, \sigma(1), \sigma^2(1), \ldots \in \{1, 2, \ldots, n\}.$$

Since there are only n choices for what these $\sigma^k(1)$ values can be, there must be some overlap so that $\sigma^k(1) = \sigma^\ell(1)$ for some $k < \ell$, and then $\sigma^{\ell-k}(1) = 1$, which guarantees that the cycle starting with 1 will in fact always "close up" on itself. Similarly for the cycle containing 2, or 3, etc. The non-obvious part is to prove that *disjoint* cycles arise: in particular, if $(1\ \sigma(1)\ \sigma^2(1)\ \ldots)$ is the cycle starting with 1 and $m \in \{1, 2, \ldots, n\}$ does not appear in this cycle, the claim is that the cycle starting with m will be disjoint from the one above. This can be done directly via a brute-force computation, which is not so bad at all, but then proving uniqueness of the disjoint cycle decomposition takes more effort still.

But here is a cleaner approach which uses machinery we have built up. For $\sigma \in S_n$, consider the action of $\langle \sigma \rangle$ on $\{1, 2, \ldots, n\}$. The orbits of this action are disjoint and have union equal to all of $\{1, 2, \ldots, n\}$. Since these orbits correspond to disjoint cycles (precisely because we are only acting on $\{1, 2, \ldots, n\}$ by powers of σ), we have our claim. The uniqueness of the disjoint cycle decomposition comes simply from the uniqueness of the orbits under the action above. (I think this is clear enough, but the book goes into this in a more in-depth way if you are not convinced.)

Cayley's Theorem. As we have seen in examples above, a group can be realized as a subgroup of a permutation (symmetric) group via a faithful action. Every group has at least one such faithful action—the action of the group on itself by left multiplication—so every group can be realized as such a subgroup, which is the statement of *Cayley's Theorem*:

> Every group is isomorphic to a subgroup of a permutation group.

To be sure, the action of G on itself by left multiplication is faithful since $g_1 h = g_2 h$ implies $g_1 = g_2$ by using the fact that h has an inverse. This action thus gives an injective homomorphism $G \to S_G$ (where S_G is the group of permutations/bijections on G), and its image is the subgroup of S_G to which G is isomorphic. This applies to infinite groups just as well as finite ones, although in the finite case $|G| = n$ we are able to realize G as a subgroup of a more familiar symmetric group S_n.

Historically, groups were first studied in the 19th century exclusively as subgroups of permutations groups. (Recall that groups arose via the problem of studying permutations of the roots of a polynomial, so permutations groups and their subgroups were the only groups known at that time.) The modern definition of a group as a set with a binary operation satisfying three properties was not in widespread use until much later, so the real point of Cayley's Theorem is to confirm that this modern definition does agree with the original notion of what a "group" was. Cayley's Theorem will not be so crucial for us as stated, but rather is important because it emphasizes the idea of thinking about abstract groups as groups of permutations, which *will* be crucial once we realize that this can happen in many different ways, not just via the action of of G on itself by left multiplication. For instance, the rotational symmetry group of a cube can in fact be realized as a subgroup of S_{24} (24 is the order of the rotation group) as Cayley's Theorem implies, but as we have seen it can also be realized as a subgroup of S_8, or S_6, or finally S_4, and all such realizations can shed light on some important aspect of that group.

Examples. Let us look at some basic examples. Under the action of $\mathbb{Z}/n\mathbb{Z}$ on itself by left multiplication (which is actually addition in this case), acting by 1 on each element does the following:

$$1+0=1, 1+1=2, 1+2=3, \ldots, 1+(n-2)=n-1, 1+(n-1)=n=0.$$

Thus, *as a permutation*, the action by 1 has the following effect:

$$0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto \ldots \mapsto n-1 \mapsto 0,$$

so that 1 corresponds to the n-cycle $(012\cdots n-1)$ under the map $\mathbb{Z}/n\mathbb{Z} \to S_n$ used in Cayley's Theorem. (Here we are viewing S_n as describing permutations on the set $\{0,1,\ldots,n-1\}$, but if we use the usual symbols $1,2,\ldots,n$ instead and "relabel" 0 as "n", then $1 \in \mathbb{Z}/n\mathbb{Z}$ corresponds to the n-cycle $(123\ldots n)$.) The action by 2 would be given by the permutation $(012\ldots n-1)^2$, and so on, so that $\mathbb{Z}/n\mathbb{Z}$ is thus isomorphic to the cyclic subgroup $\langle(012\ldots n-1)\rangle$ of S_n. (In the $n=6$ for instance, acting by 2 has the following effect:

$$0 \mapsto 2 \mapsto 4 \mapsto 0, 1 \mapsto 3 \mapsto 5 \mapsto 1,$$

so that 2 gives the permutation $(024)(135) \in S_6$, or $(246)(135)$ if we relabel 0 as 6 in order to use the standard elements $\{1,2,3,4,5,6\}$ on which S_6 acts.)

Other actions. Let us recall other standard actions which will be useful to consider. If H is a subgroup of G, then G acts on the set of cosets G/H of H also by left multiplication. (Note that this action is not faithful unless H is trivial, since otherwise $g_1H = g_2H$ does not mean $g_1 = g_2$.) In particular, if $[G:H]=k$, this gives a homomorphism $G \to S_k$, and considering different subgroups of different indices gives multiple such maps which can be used to study G. For instance, the claim from a recent homework problem that a subgroup whose index $[G:H]=p$ is the smallest prime dividing $|G|$ comes from studying the kernel of the resulting map $G \to S_p$.

G also acts on itself by conjugation, giving another homomorphism $G \to S_G$ different from the one in Cayley's Theorem; in fact, in this case the image actually lies in the group of automorphisms $\operatorname{Aut}(G)$, so that we have a map $G \to \operatorname{Aut}(G)$. If H is normal in G, we can also act by G on H via conjugation (normality is needed to guarantee that this is indeed an action *on* H), so get a map $G \to \operatorname{Aut}(H)$. It also makes sense to conjugate subgroups, so if X denotes the set of subgroups of G, we have an action of G on X by $g \cdot H := gHg^{-1}$ and hence a map $G \to S_X$. All such actions and maps into permutation groups will be useful in the coming weeks.

Lecture 20: Class Equation

Warm-Up 1. We find an explicit subgroup of S_8 which is isomorphic to the quaternion group Q_8, and we show that no such subgroup of S_7 exists. First, we obtain a subgroup of S_8 isomorphic to Q_8 via Cayley's Theorem and the action of Q_8 on itself by left multiplication. Let us label the elements of Q_8 using $1,2,\ldots,8$ as follows:

$$1 \rightsquigarrow 1, -1 \rightsquigarrow 2, i \rightsquigarrow 3, -i \rightsquigarrow 4, j \rightsquigarrow 5, -j \rightsquigarrow 6, k \rightsquigarrow 7, -k \rightsquigarrow 8.$$

Multiplication by -1 has the following effect:

$$1 \mapsto -1, -1 \mapsto 1, i \mapsto -i, -i \mapsto i, j \mapsto -j, -j \mapsto j, k \mapsto -k, -k \mapsto k,$$

so under the ordering above the permutation which corresponds to -1 is:

$$(12)(34)(56)(78).$$

Note this has order 2 in S_8, just as -1 does in Q_8. Left multiplication by i does the following:

$$1 \mapsto i \mapsto -1 \mapsto -i \mapsto 1, j \mapsto k \mapsto -j \mapsto -k \mapsto j,$$

so the corresponding permutation is

$$(1324)(5768).$$

(This has order 4 in S_8, just as i does in Q_8.) And so on, we can compute the permutations which left multiplication by any element of Q_8 induces to get:

$$\begin{array}{llll} 1 = (1) & -1 = (12)(34)(56)(78) & i = (1324)(5768) & -i = (1423)(5867) \\ j = (1526)(3847) & -j = (1625)(3748) & k = (1728)(3546) & -k = (1827)(3645). \end{array}$$

The subgroup of S_8 containing these 8 elements is then one which is isomorphic to Q_8.

Now, a realization of Q_8 as a subgroup of S_7 would correspond to a faithful action of Q_8 on a 7-element set $X = \{1, 2, \ldots, 7\}$. We are thus tasked with showing that no action of Q_8 on this X can be faithful, or equivalently that any no homomorphism $Q_8 \to S_7$ can be injective. The key realization is that any nontrivial subgroup of Q_8 contains -1, since -1 is the square of each of $\pm i, \pm j, \pm k$. Consider any action of Q_8 on X. Since

$$8 = |Q_8| = |\text{stabilizer}||\text{orbit}|$$

and any orbit has at most 7 elements, each stabilizer must have more than 1 element and will thus be nontrivial. (Said another way, for each $a \in X$ the 8 expressions $g_1 \cdot a, \ldots, g_8 \cdot a$, where $g_1, \ldots, g_8$ are the elements of Q_8, cannot all be distinct elements of X since X only has 7 elements, so some $g_i \cdot a = g_j \cdot a$ and then $g_j^{-1} g_i$ is a nontrivial element of the stabilizer of a.)

Thus each stabilizer contains $-1 \in Q_8$, and then do does their intersection. But this intersection is precisely the kernel of the induced map $Q_8 \to S_7$, so this kernel is nontrivial and hence this map is not injective, and thus no subgroup of S_7 is isomorphic to Q_8.

Warm-Up 2. We classify all groups of order 6, which we now have the tools needed to do so. Suppose G has order 6. First, by Cauchy's Theorem there exist elements $x, y \in G$ of order 2 and 3 respectively, which generated subgroups $\langle x \rangle, \langle y \rangle$ of orders 2 and 3. Since $\langle y \rangle$ has order 3, it has index $\frac{6}{3} = 2$, so it is automatically normal in G since $[G : \langle y \rangle] = 2$ is the smallest prime dividing $|G|$. We now consider two cases, depending on whether or not $\langle x \rangle$ is also normal in G.

If $\langle x \rangle$ is normal, then since $\langle x \rangle \cap \langle y \rangle = 1$ (this intersection is a subgroup of both $\langle x \rangle$ and $\langle y \rangle$, so it divides both of their orders), we have from a previous homework problem that the product $\langle x \rangle \langle y \rangle$ is a subgroup of G, and is in fact isomorphic to $\langle x \rangle \times \langle y \rangle$. Moreover, this product has the following order:

$$|\langle x \rangle \langle y \rangle| = \frac{|\langle x \rangle||\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = \frac{2 \cdot 3}{1} = 6,$$

so in fact this product is all of G, and hence $G = \langle x \rangle \langle y \rangle \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

If $\langle x \rangle$ is not normal, consider the action of G on the set $G/\langle x \rangle$ of cosets of $\langle x \rangle$. (This set of cosets is not a group since $\langle x \rangle$ is not normal, but it is certainly still a set on which G can act.) Since $|\langle x \rangle| = 2$, $|G/\langle x \rangle| = 3$, so this is an action of G on a 3 element set and hence gives a homomorphism

$$G \to S_3.$$

Any g in the kernel of this map acts trivially on each coset, so in particular it acts trivially on $\langle x\rangle$: $g\langle x\rangle = \langle x\rangle$. This requires that $g \in \langle x\rangle$, so $\ker\phi \leq \langle x\rangle$. But $\langle x\rangle$ has order 2, so either $\ker\phi = \langle x\rangle$ or $\ker\phi = 1$; the former is not possible since $\ker\phi = \langle x\rangle$ would force $\langle x\rangle$ to be normal in G, and we are assuming it is not in this case, so we must have $\ker\phi = 1$. Thus ϕ is injective, so G is (isomorphic to) a subgroup of S_3. Since $|G| = 6 = |S_3|$, we thus get $G \cong S_3$. Thus, there are precisely two groups of order 6: $\mathbb{Z}/6\mathbb{Z}$ and S_3.

Class equation. We now use the action of G on itself by conjugation to derive an equation which expresses the order of G (when G is finite) in a useful way. Recall that the orbits of the action of G on itself by conjugation are called the *conjugacy classes* of G; let us denote the conjugacy class containing $h \in G$ by $Cl(h)$:

$$Cl(h) := \{ghg^{-1} \in G \mid g \in G\}.$$

Since these are orbits for an action, distinct conjugacy classes are disjoint, so that we can express G as the disjoint union of these distinct classes:

$$G = \bigsqcup_{h_1,\ldots,h_r} Cl(h_i)$$

where $h_1, \ldots, h_r \in G$ are representatives of each conjugacy class. This then gives the equation

$$|G| = \sum_{h_1,\ldots,h_r} |Cl(h_i)|.$$

But those conjugacy classes which have size 1 are precisely those which correspond to elements of the center $Z(G)$ of G:

$$|Cl(h)| = 1 \iff ghg^{-1} = h \text{ for all } g \in G \iff h \in Z(G).$$

Thus we can rewrite the sum above by separating out those the sizes of those conjugacy classes which have only one element, to get:

$$|G| = |Z(G)| + \sum_{h_1,\ldots,h_k} |Cl(h_i)|$$

since there precisely $|Z(G)|$-many conjugacy classes of size 1, and where $h_1, \ldots, h_k$ denote (after possibly relabeling) those elements of G which give the distinct conjugacy classes of size larger than 1. The above equality is known as the *class equation*. By the orbit-stabilizer theorem, $|Cl(h_i)| = [G : C_G(h_i)]$ where $C_G(h_i)$ is the centralizer of h_i (which is the stabilizer for the conjugation action), so the class equation can also be written as

$$|G| = |Z(G)| + \sum_{h_1,\ldots,h_k} [G : C_G(h_i)].$$

Note that each $[G : C_G(h_i)] = |Cl(h_i)|$ in fact divides the order of G by the orbit-stabilizer theorem, which places restrictions on what this number can actually be.

Groups of prime-power order. As a first application of the class equation, we show that any group of prime-power order has a nontrivial center. (That we can derive this combinatorially from the class equation is quite amazing!) Suppose $|G| = p^n$ where p is prime. Since each

$$[G : C_G(h_i)] = |Cl(h_i)|$$

in the class equation is larger than 1 (since those classes of size 1 are grouped into the $|Z(G)|$ term instead) and divides $|G| = p^n$, we see that each such index/size must be divisible by p. But then p divides the left side of

$$|G| - \sum_{h_1,\ldots,h_k} |Cl(h_i)| = |Z(G)|,$$

so it must divide $|Z(G)|$ as well. But this order is certainly at least 1 because $e \in Z(G)$, so we conclude that $|Z(G)| \geq p$. Thus $Z(G)$ is nontrivial, and in fact has at least p elements.

Lecture 21: Conjugacy in S_n

Warm-Up 1. We classify all groups of order p^2, where p is prime. As a first step, we show that all such groups must be abelian. Indeed, suppose $|G| = p^2$. Then the center $Z(G)$ of G is non-trivial by the consequence of the class equation we saw last time. Thus either $|Z(G)| = p$ of $|Z(G)| = p^2$. If $|Z(G)| = p^2$, then $Z(G) = G$ and G is abelian. If $|Z(G)| = p$, then $G/Z(G)$ has order $p^2/p = p$ and so is cyclic, which implies that G is abelian by a previous Warm-Up we did. (As we pointed out back then, this then actually means that $|Z(G)| = p$ is not possible, since if G is abelian then $G = Z(G)$ so $Z(G)$ has order p^2. Cést la vie.)

Now, if there is an element in G of order p^2, then G is cyclic and isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$. Otherwise every non-identity element has order p. Pick two such elements x, y, each not in the cyclic generated by the other. Then both $\langle x\rangle, \langle y\rangle$ are normal in G since G is abelian, and $\langle x\rangle\langle y\rangle$ is a subgroup of G. Since x, y are not powers of one another, $\langle x\rangle \cap \langle y\rangle$ is trivial (this intersection has order dividing p, so if not trivial would have to equal both $\langle x\rangle = \langle y\rangle$), so $|\langle x\rangle\langle y\rangle| = |\langle x\rangle||\langle y\rangle| = p^2$. Thus

$$G = \langle x\rangle\langle y\rangle \cong \langle x\rangle \times \langle y\rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

in this case. Hence there are two groups of order p^2 for p prime: $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Warm-Up 2. Suppose G has prime-power order p^n. We show that G has a subgroup of each order p^i dividing p^n. First, $Z(G)$ is non-trivial, and of some prime-power order p^k where $1 < k \leq n$. Since $Z(G)$ is abelian, a problem on a recent homework then shows that $Z(G)$ has a subgroup of any order p^i dividing $|Z(G)| = p^k$, so this produces a subgroup of G of any order p^i for $1 \leq i \leq k$.

So, suppose we now want a subgroup of order p^i for $k < i \leq n$. The quotient $G/Z(G)$ has order $p^{n-k} < p^n$, so by induction we may assume that our claim (about existence of subgroups of a given order) is true for this group. In particular, $G/Z(G)$ has a subgroup of order p^{i-k}, which is of the form $H/Z(G)$ where H is a subgroup of G containing $Z(G)$. But then Lagrange's Theorem gives:

$$|H| = |H/Z(G)||Z(G)| = p^{i-k}p^k = p^i,$$

so H is our desired subgroup of G. We conclude that G has subgroups of all order p^i for $1 \leq i \leq n$. (Groups of prime-power order will play a big role soon in the context of the *Sylow Theorems.*)

Conjugacy in S_n. We now wish to understand conjugacy classes in S_n, and then in A_n. But for S_n we had a previous homework problem which gives us all the information we need: $\sigma, \tau \in S_n$ are conjugate if and only if they have the same *cycle type*, meaning that they have the same number of cycles of the same length appearing in their disjoint cycle decompositions. For instance, all permutations of the form

(2-cycle)(3-cycle)

in S_n for $n \geq 5$ will be conjugate to one another, and hence will all make-up one conjugacy class. Thus, conjugacy classes in S_n are completely determined by the possible cycle types. In S_5 for example, there are thus ... conjugacy classes:

- there one conjugacy class consisting of the identity alone (five 1-cycles);
- there is one conjugacy class consisting of transpositions (one 2-cycle and three 1-cycles);
- one class consists of products of two disjoint transpositions (two 2-cycles, one 1-cycle);
- one class consists of the 3-cycles (one 3-cycle, two 1-cycles);
- one class consists of products of disjoint 2- and 3-cycles; and
- one class consists of the 5-cycles

(Remark: the conjugacy classes of S_n thus correspond to the *partitions* of n, which are the ways of expressing n as a sum of positive integers. The number 5 for instance has 6 partitions, corresponding to the cycle types above: $1+1+1+1+1, 2+1+1+1, 2+2+1, 3+1+1, 3+2, 5$. Partitions are studied more carefully in a course on combinatorics, such as MATH 306.)

Counting permutations. We can easily determine the size of each conjugacy class above. For instance, the number of 3-cycles (abc) in S_5 can be found by making choices for each of a, b, c and then taking into account over-counting: there are 5 choices for a, 4 for b, and 3 for c, but then we have over-counted by a factor of 3 since (abc) gives the same permutation as (bca) and (cab). Thus the number of 3-cycles in S_5 is

$$\frac{5 \cdot 4 \cdot 3}{3} = 20,$$

so the conjugacy class $Cl((123))$ of (123) (containing all 3-cycles) has size 20 in S_5.

Along the same lines, there are $\frac{5\cdot4\cdot3\cdot2\cdot1}{5} = 24$ cycles of length 5 in S_5, which comes from picking each entry in $(abcde)$ and then dividing by an over-counting factor of 5 since the permutation $(abcde)$ can also be described by the cyclic permutations of $(abcde)$. Thus $Cl((12345)) = 24$. For the conjugacy class of $(12)(34)$, which consists of all products of disjoint transpositions, we count the possibilities $(ab)(cd)$ via

$$\frac{5 \cdot 4 \cdot 3 \cdot 2}{2 \cdot 2 \cdot 2} = 15.$$

where the over-counting factor of $2 \cdot 2 \cdot 2$ comes from the fact that each 2-cycle used can by cyclically permuted, but then also the fact that the order of the two transpositions themselves can be switched since $(ab)(cd) = (cd)(ab)$. Thus $Cl((12)(34))$ has 15 elements. The sizes of the remaining conjugacy classes can be determined similarly.

Conjugacy in A_n. But now if we consider conjugacy in A_n, the answer is not as clean as it was in S_n because conjugacy in S_n does not imply conjugacy in A_n. The issue is that the permutation γ such that $\gamma\sigma\gamma^{-1} = \tau$ in S_n might not be even, as would be required in order to say that σ and τ are still conjugate in A_n. For instance, in S_4 we have:

$$(1234)(123)(1234)^{-1} = (234),$$

but (1234) is odd, so this equality does not imply that (123) and (234) are conjugate in A_4. Of course, there might be some other permutation apart from (1234) which could *also* make (123) conjugate to (234), but it turns out in this case that no such permutation will in fact be even, so (123) and (234) are not conjugate in A_4. (This can be verified by a brute-force check.) Thus, (123) and (234) will actually determine different conjugacy classes in A_4.

To determine the size of a conjugacy class in A_n, it is better to use the orbit-stabilizer theorem and work with centralizers instead. For instance, the centralizer of a 5-cycle $\sigma = (abcde)$ in A_5 consists precisely of σ and its powers, so

$$C_{A_5}((abcde)) = \langle (abcde) \rangle$$

has order 5. Thus $|Cl(\sigma)| = [A_5 : C_{A_5}(\sigma)] = \frac{60}{5} = 12$, which means that the 24 5-cycles in A_5 (which make up one single conjugacy class in S_5) actually split up into *two* distinct conjugacy classes in A_5, each of size 12. (The same reasoning also works in S_5, with the same centralizer here as in A_5, only that the order of the entire group S_5 is 120 instead of $|A_5| = 60$, so we get $[S_5 : C_{S_5}(\sigma)] = \frac{120}{5} = 24$ as the size of the conjugacy class, as expected.)

For 3-cycles in A_5 however, the answer is indeed the same as in S_5 since all 3-cycles are in fact conjugate to one another *within* A_5. Actually, this is true for any $n \geq 5$: for any (abc), pick $\sigma \in S_n$ such that $\sigma(123)\sigma^{-1} = (abc)$; then if σ is even, this gives conjugacy in A_n too, while if σ is odd, then $\sigma(45)$ is even and realizes this conjugacy in A_n:

$$\sigma(45)(123)(\sigma(45))^{-1} = \sigma(45)(123)(45)\sigma^{-1} = \sigma(123)\sigma^{-1} = (abc).$$

(We use here that $n \geq 5$ so that (45) makes sense, and the fact that (123) and (45) commute. This fact about 3-cycles in A_n all being conjugate to one another is not true for $n = 4$, as shown by the examples of (123) and (234) mentioned previously.) If we argue using centralizers, say in the $n = 5$ case, the key point is that although the centralizer of $\sigma = (123)$ in A_5 is $\langle \sigma \rangle$ and thus has order 3, its centralizer in S_5 also includes (45) (which is odd) and the products $\sigma^k(45)$. Thus this centralizer has order 6 in S_5, so we get that the size of conjugacy class of (123) is:

$$[S_5 : C_{S_5}((123))] = \frac{120}{6} = 20 \text{ in } S_5, \text{ and } [A_5 : C_{S_5}((123))] = \frac{60}{3} = 20 \text{ in } A_5,$$

so that all 3-cycles do make up a single conjugacy class in A_5.

The remaining cycle type an element of A_5 can have is as the product of two disjoint transpositions, and here it also turns out that there is one single conjugacy class, just as there is in S_5. We will save this argument for next time, after which we will have determined the sizes of all conjugacy classes in A_5; we will then use this to show that A_5 is simple.

Lecture 22: Simplicity of A_n

Warm-Up. We determine the centralizer of (12)(34) in A_5, and then the size of conjugacy class to which it belongs. In order for $\sigma \in A_5$ to centralize (12)(34), we must have:

$$\sigma(12)(34)\sigma^{-1} = (\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4)) = (12)(34).$$

(The first equality comes from the main computation carried out in the homework problem where it was shown that conjugacy in S_n is determined by cycle type.) Thus σ must fix 5, and then there are two possibilities:

- $(\sigma(1)\ \sigma(2)) = (12)$ and $(\sigma(3)\ \sigma(4)) = (34)$, so that σ must fix or transpose $1, 2$, and fix or transpose $3, 4$. In S_5 the possibilities are thus $(1), (12), (34)$, and $(12)(34)$, but in A_5 only $\sigma = (1)$ and $\sigma = (12)(34)$ work.
- $\sigma(1)\ \sigma(2)) = (34)$ and $(\sigma(3)\ \sigma(4)) = (12)$, so that ether $\sigma(1) = 3, \sigma(2) = 4$ or $\sigma(1) = 4, \sigma(2) = 3$. Thus $\sigma = (13)(24)$ or $(14)(23)$. (In S_5, (1324) and (1423) also work.)

Hence $C_{A_5}((12)(34))$ has order 4, so the conjugacy class containing (12)(34) has size

$$|Cl((12)(34))| = [A_5 : C_{A_5}((12)(34))] = \frac{60}{4} = 15.$$

Since there are 15 permutations in S_5 with cycle type (2-cycle)(2-cycle) (as computed last time), this means that they all remain conjugate to each other in A_5 as well. (Note in S_5 the centralizer has order 8, so the conjugacy class has size $[S_5 : C_{S_5}((12)(34))] = \frac{120}{8} = 15$, as expected. The drop in a factor of 2 of the size of A_5 vs S_5 is cancelled out by the doubling in the size of the stabilizer.)

As a consequence of this and computations done last time, we now know there are 5 conjugacy classes in A_5 of sizes $1, 12, 12, 15, 20$, corresponding to the identity, the two classes containing 5-cycles, the class containing products of two disjoint transpositions, and the class containing 3-cycles.

A_5 is simple. We can now give a proof that A_5 is simple. The proof we give is not the only possible proof, but is a nice one which avoids so many brute-force computations. We will outline another brute-force proof afterwards. First, a general observation: if N is a normal subgroup of a group G, then N is a union of conjugacy classes of G. Indeed, if $h \in N$, then $ghg^{-1} \in N$ for all $g \in G$ by normality, so that the entirety of $Cl(h)$ is contained in N. Thus N is the union of the conjugacy classes $Cl(h) \subseteq G$ with h ranging throughout N. (In other words, if a normal subgroup intersects a conjugacy class of the larger group, then it must contain the entire class.)

Suppose $N \trianglelefteq A_5$. Then $|N|$ divides $|A_5| = 60$ by Lagrange's Theorem, and since N is a union of conjugacy classes of A_5, $|N|$ must be a sum of some or all of $1, 12, 12, 15, 20$ since these are all the possible sizes of these conjugacy classes. One possibility is $|N| = 1$, in which case N is trivial. Otherwise, N will contain the conjugacy class of the identity and at least one other class, so $|N| > 1$ is 1 plus at least one number among $12, 12, 15, 20$. The only way such a resulting number $|N|$ can also divide 60 is for it to be 60 itself:

$$|N| = 1 + 12 + 12 + 15 + 20 = 60,$$

so we conclude that $N = A_5$ in this case. Hence the only normal subgroups of A_5 are 1 and A_5, so A_5 is simple as claimed.

Just to contrast this proof with what happens for A_4, which is not simple, we will note without proof that the conjugacy classes of A_4 have sizes: $1, 3, 3, 4$. In this case, a nontrivial $N \trianglelefteq A_4$ can have order $|N| = 1 + 3 = 4$ dividing $|A_4| = 12$ (without using all of $1, 3, 3, 4$), highlighting the fact that A_4 does indeed have a normal subgroup of order 4

It's all about the 3-cycles. Here is an outline of a different, more computational approach to showing that A_5 is simple. In general, note that if $1 \neq N \trianglelefteq A_5$ is normal, the existence of a single 3-cycle in N is enough to guarantee that $N = A_5$. Indeed, if N contains a 3-cycle, then it must contain *all* 3-cycles since 3-cycles are all conjugate to one another in A_5 and conjugates of things in N are still in N by normality. But then since the 3-cycles generate A_5 (from a homework problem), we must have $A_5 = N$ as a result.

So, if we want to show that A_5 is simple, we must show that any nontrivial $N \trianglelefteq A_5$ contains *some* 3-cycle. Let $\sigma \in N$ be different from the identity. The goal is to then—based on what the cycle type of σ is—show that σ times some conjugate of σ is a 3-cycle, which is then in N by normality and the fact that N is closed under multiplication. This can be done through some brute-force computations: for instance, if $\sigma = (abcde)$ is a 5-cycle, you can work out that

$$\sigma[(ab)(cd)\sigma[(ab)(cd)]^{-1}]$$

is a 3-cycle; and if $\sigma = (ab)(cd)$ is a product of disjoint transpositions, then

$$\sigma(abe)\sigma(abe)^{-1}$$

will be a 3-cycle. In fact, a similar type of brute-force computation can be used to show that A_n is simple for all $n \geq 5$: take a non-identity σ in a nontrivial $N \trianglelefteq A_n$ and work out (depending on the cycle type of σ) through some conjugations and multiplications that you can produce a 3-cycle which will be in N. So, it is possible to prove that A_5 and A_n ($n \geq 5$) more generally is simple without anything fancy, but certainly there will be nothing very enlightening about this brute-force approach.

A_n is simple for $n \geq 6$. Instead, we prove that A_n is simple for $n \geq 6$ in a more clever way which avoids as many computations. We essentially follow the book's approach, although presented here in a (hopefully) clearer way. (The book argues by contradiction, which is a bit confusing and unnecessary if phrased slightly differently.) The one technical fact we will need is the following: for any $\sigma \in A_n$, there exists a conjugate τ of σ in A_n which is different from σ but nevertheless has the same effect as σ on some $i \in \{1, 2, \ldots, n\}$, meaning $\sigma(i) = \tau(i)$ for some $i \in \{1, 2, \ldots, n\}$. If the disjoint cycle decomposition of σ contains a cycle $(abc\ldots)$ of length at least 3, then

$$\tau = (cd)(ef)\sigma[(cd)(ef)]^{-1}$$

(where d, e, f are different from a, b, c and each other) has this property since $\tau(a) = b = \sigma(a)$ and $\sigma \neq \tau$ since $\tau(b) = d \neq \sigma(b)$; if the decomposition of σ contains only disjoint transpositions and there are at least three $(ab)(cd)(ef)$, then

$$\tau = (ab)(ce)\sigma[(ab)(ce)]^{-1}$$

works since $\tau(a) = b = \sigma(a)$ but $\tau(e) = d \neq \sigma(e)$; and if $\sigma = (ab)(cd)$, then

$$\tau = (acb)\sigma(acb)^{-1}$$

satisfies $\tau(a) = c \neq \sigma(a)$ and $\tau(e) = \sigma(e)$, where e is different from a, b, c, d.

So, for some $n \geq 6$ denote A_n by G (for cleaner notation) suppose N is a nontrivial normal subgroup of G. Pick a non-identity $\sigma \in N$. By the technical fact above there exists a conjugate τ of σ in A_n different from σ such that $\sigma(i) = \tau(i)$ for some $i \in \{1, 2, \ldots, n\}$. Then $\sigma^{-1}\tau(i) = i$, so $\sigma^{-1}\tau$ is a non-identity element of the stabilizer G_i. But τ is also N by normality, so $\sigma^{-1}\tau \in N \cap G_i$. This intersection is thus a nontrivial normal subgroup of G_i (normality is straightforward to check). But elements of $G_i \leq A_n$ can be viewed as permutations (still even!) of the $n - 1$ elements among $1, 2, \ldots, n$ which are not i, so that G_i is in fact isomorphic to A_{n-1}. By induction we may assume that G_i is thus simple (the base case $n = 5$ was worked out previously), so that the intersection $N \cap G_i$ above must actually equal G_i, which means that $G_i \leq N$. But G_i contains a 3-cycle since any 3-cycle (abc) where none of a, b, c are i will fix i, so we get that N contains a 3-cycle. Thus, as explained before, N contains all 3-cycles of A_n and hence equals A_n since A_n is generated by 3-cycles. We therefore conclude that A_n is simple for $n \geq 6$.

S_n is not solvable for $n \geq 5$. And now, using the simplicity of A_n for $n \geq 5$, we can show that S_n is not solvable for $n \geq 5$. (Just to hammer the point once again: this is the reason why no "quintic formula" exists.) This was actually a problem from discussion section, but we will reproduce the reason here. We use the fact, also covered in discussion, that for $n \geq 5$ the alternating group A_n is in fact the *only* nontrivial proper normal subgroup of S_n.

The chain of normal subgroups $1 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{n-1} \trianglelefteq S_n$ needed in the condition for solvability can only be

$$1 \trianglelefteq S_n \quad \text{or} \quad 1 \trianglelefteq A_n \trianglelefteq S_n$$

since A_n is simple and the only nontrivial proper normal subgroup of S_n. But in the first case the quotient $S_n/1 \cong S_n$ is not abelian, while in the second the first quotient $A_n/1 \cong A_n$ is also non-abelian. Hence no such chain with abelian quotients can exist, so S_n is not solvable.

Automorphisms of S_n. We will finish our current discussion of symmetric groups and their properties with one curious fact. Recall that, for any group, conjugation by $g \in G$ defines an automorphism of G. These are called the *inner automorphisms* of G. (The group of inner automorphisms of G in general is isomorphic to $G/Z(G)$, which we will leave for you to see why.) So we can ask whether any more automorphisms beyond these exist.

Here is the theorem: for $n \neq 6$, $\text{Aut}(S_n)$ consists of only the inner automorphisms, while for $n = 6$, $\text{Aut}(S_6)$ contains non-inner automorphisms. It is strange at first that the $n = 6$ case should be so different than *every other* n, but indeed it is. The proof of this fact is not something we will cover, but you can read about it in various sources if interested. We will likely see, in the context of the Sylow Theorems, how one might go about constructing the non-inner automorphism of S_6, although we will not give a complete construction.

Lecture 23: Sylow Theorems

Warm-Up. We show that for $n \geq 5$, A_n is the only nontrivial, proper normal subgroup of S_n. This was a problem from discussion section, but we reproduce it here since it is quite an important result. In particular, it was the key step in the argument we gave last time to show that S_n is not solvable for $n \geq 5$. Suppose $N \trianglelefteq S_n$ is proper. Then $N \cap A_n$ is a subgroup of A_n, and is moreover normal in A_n: for $\tau \in A_n$ and $\gamma \in N \cap A_n$, $\tau\gamma\tau^{-1} \in N$ since N is normal in S_n, and $\tau\gamma\tau^{-1} \in A_n$ since A_n is closed under multiplication. Thus since A_n is simple for $n \geq 5$, we must have $N \cap A_n = A_n$ or $N \cap A = 1$. If $N \cap A_n = A_n$, then $A_n \leq N$, but since A_n already has index 2 and N is proper in S_n, this implies $N = A_n$. (Otherwise there would be a subgroup of S_n of index between 1 and 2, which is nonsense.)

If $N \cap A_n = 1$ and $N \neq 1$, then N must be of the form $N = \{1, \tau\}$ for some odd permutation τ of order 2. (If N contained an odd permutation σ which was not of order 2, it would contain $\sigma^2 \neq 1$, which is even and hence N would intersect A_n non-trivially. If N contained two odd permutations of order 2, it would contain their even product and hence again N would intersect A_n non-trivially.) But then $\sigma\tau\sigma^{-1} \in \{1, \tau\}$ for any $\sigma \in S_n$ since N is normal, so that this product must in fact equal τ. This means that any $\sigma \in S_n$ commutes with τ, so that τ is in the center of S_n. But this center is trivial (see the Discussion 3 Problems), so this is not possible and thus N must be trivial.

The Sylow Theorems. Now we come to some of the most fundamental results in finite group theory: the *Sylow Theorems*. After Lagrange's Theorem, the Sylow Theorems (which give a general partial converse to Lagrange's Theorem) provide the key tools we need to understand the structure of finite groups in a general way, and are crucial to the problem of their classification. It is common to present these results as a collection of three theorems:

> ***Sylow 1***: Suppose $|G| = p^k m$ where p is prime and does not divide m, so that p^k is the largest power of p dividing $|G|$. Then G has a subgroup of order p^k. (Such a subgroup is called *Sylow p-subgroup* of G.)
>
> ***Sylow 2***: Any two Sylow p-subgroups of G are conjugate to one another: if P, Q are Sylow p-subgroups, then there exists $g \in G$ such that $gPg^{-1} = Q$. Also, any subgroup of G of prime-power order p^ℓ is contained in a Sylow p-subgroup.
>
> ***Sylow 3***: The number n_p of Sylow p-subgroups is congruent to 1 mod p and divides the factor m in $|G| = p^k m$. Moreover, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup.

Note that since a Sylow p-subgroup has prime-power order p^k, it itself has subgroups of each order p^i for $1 \leq i \leq k$ by a Warm-Up we did previously, so G does as well. (In general, a group of prime-power order p^t is called a p-group.)

The first Sylow Theorem is thus an existence result, and produces subgroups we can work with. The third Sylow Theorem places restrictions on how many such subgroups there can be, and the second Sylow Theorem then tells us something about how these different subgroups are related to one another. (Many, but not all, other sources transpose what we are calling Sylow 2 and Sylow 3. Everyone agrees, however, on which one is Sylow 1). We will use $Syl_p(G)$ to denote the set of Sylow p-subgroups of G.

Groups of order 12. Before proving the Sylow Theorems, we give an example which starts to illustrate their power and how to use effectively use them. Note how all the Sylow Theorems play a role here. We seek to say as much as we can say about groups of order 12. We will not be able to provide a complete classification yet, but we can already get pretty far.

Suppose G has order $12 = 2^2 \cdot 3$. Then G has Sylow 2-subgroups of order $2^2 = 4$, and Sylow 3-subgroup of order 3. The number n_2 of Sylow 2-subgroups then satisfies:

$$n_2 \equiv 1 \bmod 2 \quad \text{and} \quad n_2 \mid 3,$$

and the number n_3 of Sylow 3-subgroups satifies:

$$n_3 \equiv 1 \bmod 3 \quad \text{and} \quad n_3 \mid 4.$$

This gives the following possibilities: $n_2 = 1$ or 3, and $n_3 = 1$ or 4. As a general observation, note that $n_p = 1$ is equivalent to having a *normal* Sylow p-subgroup: if there is only one Sylow p-subgroup P, then for any $g \in G$, gPg^{-1} must equal P (so P is normal) since gPg^{-1} is also a Sylow p-subgroup; while if P is normal, then since any Sylow p-subgroup is conjugate to P, $gPg^{-1} = P$ gives all possible Sylow p-subgroups, so there is only one. Thus in the case where $n_2 = 1$ and $n_3 = 1$, the Sylow 2-subgroup P and Sylow 3-subgroup $Q \cong \mathbb{Z}/3\mathbb{Z}$ are each normal in G. Then PQ is a subgroup of G, and since $P \cap Q = 1$ because their orders are relatively prime, we have $|PQ| = |P||Q| = 2^2 \cdot 3 = 12$. Hence in this case we have

$$G = PQ \cong P \times Q \quad \text{(recall that this uses normality).}$$

We previously classified the groups of order p^2, so that $P \cong \mathbb{Z}/4\mathbb{Z}$ or $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and thus we get $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Now consider the case where $n_3 = 4$, so that there are four Sylow 3-subgroups of G. The action of G on $Syl_3(G)$—a set with 4 elements—by conjugation (the conjugate of a Sylow p-subgroup is still a Sylow p-subgroup) then produces a homomorphism $\phi : G \to S_4$. The kernel of this homomorphism consists of those elements of G which conjugate each Sylow 3-subgroup to itself, and thus is the intersection of the normalizers $N_G(P)$ of the Sylow 3-subgroups:

$$\ker \phi = \bigcap_{P \in Syl_3(G)} N_G(P).$$

The third Sylow Theorem also gives $n_3 = [G : N_G(P)] = |G|/|N_G(P)|$, so since $n_3 = 4$ we get $|N_G(P)| = 3$. This means $N_G(P) = P$ since $P \leq N_G(P)$. Thus the kernel above is the intersection of the four Sylow 3-subgroups, and so is trivial since each Sylow 3-subgroup has order 3. Hence $G \to S_4$ is injective, so that $G \leq S_4$ (or, more precisely, G is isomorphic to a subgroup of S_4). But the only subgroup of S_4 of order 12 is A_4 (S_4 only has one subgroup of index 2 by a problem from discussion), so $G \cong A_4$ in this case. (Here is an alternate argument: each Sylow 3-subgroup has 2 elements of order 3, and since any two Sylow 3-subgroups intersect trivially, this gives $4 \cdot 2 = 8$ distinct elements of order 3 in G. Thus G contains all eight 3-cycles of S_4, so it must be A_4 since the 3-cycles generate A_4.)

To summarize: if there is only one Sylow 2-subgroup and only one Sylow 3-subgroup, G is abelian and isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, while if there are four Sylow 3-subgroups, G is isomorphic to A_4. This leaves the case where there is only one Sylow 3-subgroup but three Sylow 2-subgroups. We will come back to this case later, to see that there are only two possibilities left for what G can be. For now, we at least know that the Sylow 3-subgroup must be normal in G (since there is only one). Both of the possibilities left will arise as *semidirect products* of the Sylow 3-subgroup and one of the Sylow 2-subgroups.

Proof of Sylow 1. We will now give a proof of the first Sylow Theorem, and save the other two for next time. We use the same proof as the book, but there are multiple other proofs available. All essentially proceed by induction, and build from a subgroup of prime-order at the start (Cauchy's Theorem) up to a subgroup of maximal prime-power order.

Write $|G| = p^k m$ where p does not divide m. We consider two cases: p divides the order of the center $Z(G)$, and p does not divide the order of $Z(G)$. If p divides $|Z(G)|$, pick using Cauchy's Theorem an element $x \in Z(G)$ of order p. Since x is in the center, it commutes with all $g \in G$ and hence $\langle x \rangle$ is normal in G. Then the quotient $G/\langle x \rangle$ is a group of order $p^{k-1}m$. By induction, $G/\langle x \rangle$ has a subgroup $H/\langle x \rangle$ of maximal prime-power order p^{k-1}, where H is a subgroup of G containing $\langle x \rangle$. This H then has order $|H/\langle x \rangle||\langle x \rangle| = p^{k-1}p = p^k$, so that H is a Sylow p-subgroup of G.

If p does not divide $|Z(G)|$, consider the class equation

$$|G| = |Z(G)| + \sum_{h_i} [G : C_G(h_i)]$$

where the h_i are representatives of the non-trivial conjugacy classes of G. Since p divides $|G|$ but not $|Z(G)|$, it cannot divide the sum of indices $[G : C_G(h_i)]$, so there exists some h_i such that p does not divide $[G : C_G(h_i)]$ specifically. But

$$[G : C_G(h_i)] = \frac{|G|}{|C_G(h_i)|} = \frac{p^k m}{|C_G(h_i)|},$$

so in order for p to not divide this it must be the case that all powers of p in the numerator of the fraction on the right also show up in the prime-factorization of the denominator. Thus $|C_G(h_i)| = p^k s$ for some s, so by induction $C_G(h_i)$ has a Sylow p-subgroup H of order p^k, which is then also a Sylow p-subgroup of G.

Lecture 24: More on Sylow

Warm-Up 1. Suppose G is a simple group of order $168 = 2^3 \cdot 3 \cdot 7$. We determine the number of elements of G which have order 7. The key observation is that any element of order 7 generates a subgroup of order 7, and so is contained in a Sylow 7-subgroup. The number n_7 of such subgroups satisfies

$$n_7 \equiv 1 \bmod 7 \quad \text{and} \quad n_7 \mid 2^3 \cdot 3 = 24,$$

and thus the possibilities are $n_7 = 1$ or $n_7 = 8$. But G is simple so a Sylow 7-subgroup cannot be normal, so we must have $n_7 = 8$. (Recall that in general $n_p = 1$ if and only if the Sylow p-subgroup is normal.) Now, any two Sylow 7-subgroups must intersect trivially since their intersection has order dividing 7 and is not 7. This means that each contains 6 elements of order 7 not contained in any other Sylow 7-subgroup, so we get $8 \cdot 6 = 48$ elements of order 7 overall.

Warm-Up 2. We show that no group of order 56 is simple. Since $56 = 2^3 \cdot 7$, a group G of order 56 has Sylow 2-subgroups of order 8 and Sylow 7-subgroups of order 7. The number of each satisfy:

$$n_2 \equiv 1 \text{ mod } 2 \text{ and divides } 7 \qquad\qquad n_7 \equiv 1 \text{ mod } 7 \text{ and divides } 8.$$

Thus the possibilities are $n_2 = 1, 7$ and $n_7 = 1, 8$. We claim that in fact at least one of these must actually be 1, so that there will be either a normal Sylow 2-subgroup or a normal Sylow 7-subgroup, and hence either way G is not simple.

Suppose $n_7 = 8$. The Sylow 7-subgroups intersect trivially and each contain 6 elements of order 7, so this gives $8 \cdot 6 = 48$ elements of order 7 in G. A single Sylow 2-subgroup gives another 8 elements of G (Sylow 2-subgroups and Sylow 7-subgroups intersect trivially because they have relatively prime orders), so so far we get $48 + 8 = 56$ elements in G. But this is the entire order of G already, so there cannot be any other Sylow 2-subgroups since a second such group would give at least one more elements in G. Thus in the case where $n_7 = 8$ we must have $n_2 = 1$, and hence either $n_7 = 1$ or $n_2 = 1$, so G is not simple.

Sylows never normalize each other. We now move towards proving the remaining Sylow Theorems. We will essentially follow the same proof as in the book, only we reorder some of the arguments to make them (we think) easier to digest, at the expense of proving only parts of the second and third Sylow Theorems at a time. Ultimately the proofs come down to looking at a certain conjugation action of one Sylow subgroup and determining the sizes of its orbits.

We begin first with a lemma, which amounts to saying that one Sylow p-subgroup cannot never normalize a different one. Proving this first is also the approach the book takes, although we will give a somewhat different phrasing of this result than the book does. Here is our claim:

> Suppose $g \in G$ has prime-power order p^i and P is a Sylow p-subgroup of G with $gPg^{-1} = P$. Then $g \in P$.

So, if an element of prime-power order normalizes a Sylow p-subgroup, it must actually be in that subgroup. As a consequence, if $Q, P \in Syl_p(G)$ are different Sylow p-subgroups, neither is contained in the normalizer of the other, for if Q did normalize P, the fact that any $g \in Q$ has prime-power order (since Q has prime-power order) implies $g \in P$ by the lemma, so that Q and P would actually be the same.

Consider the subgroup $\langle P, g\rangle$ of G generated by P and g. Since g normalizes P (and certainly elements of P do as well), we have that P is a normal subgroup of $\langle P, g\rangle$, so that the quotient $\langle P, g\rangle/P$ exists. Any element of $\langle P, g\rangle$ is a product of elements of P with powers of g:

$$p_1 g^{k_1} p_2 g^{k_2} p_3 g^{k_3} \cdots p_m g^{k_m}$$

(note the first p_1 or last g^{k_m} terms could be identities), so that any such product becomes a power of g alone in the quotient:

$$p_1 g^{k_1} p_2 g^{k_2} p_3 g^{k_3} \cdots p_m g^{k_m} = e g^{k_1} e g^{k_2} e g^{k_3} \cdots e g^{k_m} = g^{k_1 + \cdots + k_m} \text{ in } \langle P, g\rangle/P.$$

Thus $\langle P, g\rangle/P$ is cyclic of some prime-power order p^ℓ dividing the order p^i of g. By Lagrange's Theorem we then get $|\langle P, g\rangle| = p^i|P| = p^{i+k}$. But $P \leq \langle P, g\rangle$ has maximal prime-power order p^k in

G since it is a Sylow p-subgroup, so that we must actually have $P = \langle P, g\rangle$. (Otherwise $\langle P, g\rangle$ has largest prime-power order than P in G.) But this means that $g \in P$ as claimed.

Proof of first part of Sylow 3. We now prove that $n_p \equiv 1 \bmod p$. (Again, note we are structuring the proofs a bit differently than the book does.) Pick a Sylow p-subgroup P and consider the action of P on $Syl_p(G)$ by conjugation. (Elements of P conjugate Sylow p-subgroups to Sylow p-subgroups since the orders remain unchanged.) This action breaks up $Syl_p(G)$ into the disjoint union of orbits:

$$Syl_p(G) = (\text{orbit } 1) \sqcup \ldots \sqcup (\text{orbit } k).$$

The size of each orbit divides $|P| = p^k$, and so is either 1 or divisible by p. But there is precisely one orbit of size 1: the orbit containing P has size 1 since all elements of P normalize P, and no other orbit has size 1 since P does not normalize any other Sylow p-subgroup. (An orbit of size 1 occurs when $gQg^{-1} = Q$ for all $g \in P$.) Thus every other orbit, apart from the one containing P, has size divisible by p. Thus:

$$|Syl_p(G)| = 1 + (\text{sum of things divisible by } p),$$

so $n_p := |Syl_p(G)| \equiv 1 \bmod p$ as claimed. (The "sum of things divisible by p" goes away when taking the result mod p.)

Proof of first part of Sylow 2. Now we prove that all Sylow p-subgroups are conjugate to one another. Pick a Sylow p-subgroup P and let X denote the set of its conjugates in G:

$$X := \{gPg^{-1} \mid g \in G\}.$$

Each such conjugate is a Sylow p-subgroup of G, and we want to show $X = Syl_p(G)$ so that *all* Sylow p-subgroups arise this way. P acts on X by conjugation, and we can break up X into a disjoint union of orbits:

$$X = (\text{orbit } 1) \sqcup \ldots \sqcup (\text{orbit } k).$$

The exact same reasoning as before implies that there is one orbit of size 1 (the one containing $ePe^{-1} = P$), and that the others have size divisible by p. Thus again we get $|X| \equiv 1 \bmod p$.

Now, if X was not all of $Syl_p(G)$, there would exist $Q \in Syl_p(G)$ not in X. This Q also acts on X by conjugation, and we get:

$$X = (\text{orbit } 1) \sqcup \ldots \sqcup (\text{orbit } t).$$

But now, there is no orbit of size 1: if Q normalizes an entire conjugate gPg^{-1}, then $Q = gPg^{-1}$ by the technical lemma from before, so that Q would have been in X. Thus in this case all orbits have sizes divisible by p, so $|X| \equiv 0 \bmod p$. This contradicts $|X| \equiv 1 \bmod p$ from before, so no such Q can exist. Hence $X = Syl_p(G)$, so all Sylow p-subgroups are conjugate to P and thus each other.

Proof of rest of Sylow 3. Fix $P \in Syl_p(G)$. Since all Sylow p-subgroups of G are conjugate to P, the number n_p of Sylow p-subgroups is the number of such conjugates. But this is the size of the orbit of P under the action of G on its subgroups by conjugation, so

$$n_p = [G : N_G(P)]$$

by the orbit-stabilizer theorem. (The normalizer is the stabilizer for this action.) Moreover,

$$n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|} = \frac{p^k m}{p^k \ell} = \frac{m}{\ell}.$$

where $|N_G(P)| = p^k\ell$ and we use the fact that $P \leq N_G(P)$ in order to say that $|N_G(P)|$ has at least a factor of p^k in its prime-factorization, and no larger p-power since p^k is the largest power of p dividing $|G|$. Thus $n_p\ell = m$, so n_p divides m.

Proof of rest of Sylow 2. We finish our proof of the Sylow Theorems by proving that if $H \leq G$ has prime-power order p^i, then H is contained in some Sylow p-subgroup. The action of H on $Syl_p(G)$ by conjugation (again) gives

$$Syl_p(G) = (\text{orbit } 1) \sqcup \ldots \sqcup (\text{orbit } k).$$

As before, each orbit has size a power of p, and since $|Syl_p(G)| \equiv 1 \bmod p$, there must be at least one orbit of size 1. (If all orbits had size larger than 1 we would have $|Syl_p(G)| \equiv 0 \bmod p$.) But in order to have an orbit of size 1 means that $hPh^{-1} = P$ for all $h \in H$ and some Sylow p-subgroup P, which implies $H \leq P$ by the technical lemma from before.

Lecture 25: Applications of Sylow

Warm-Up 1. We classify groups of order $|G| = pq$ where $p < q$ are primes such that p does not divide $q - 1$. Let P be a Sylow p-subgroup and Q a Sylow q-subgroup of G. Since Q has index p, which is the smallest prime dividing $|G|$, Q is normal in G. (You can also see this by determining that $n_q = 1$.) The number of Sylow p-subgroups of G satisfies

$$n_p \equiv 1 \bmod p \text{ and divides } q,$$

so we get $n_p = 1$ or $n_p = q$ as possibilities. (Note q is prime.) But $n_p = q$ is ruled out by the fact that p does not divide $q-1$, so that q is not congruent to 1 mod p, and hence $n_p = 1$ and thus P is normal in G. Thus, since P and Q have trivial intersection (their orders are p and q respectively), we get $|PQ| = pq = |G|$, and since P, Q are both normal in G we have:

$$G = PQ \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

Thus $\mathbb{Z}/pq\mathbb{Z}$ is the only group with the given properties.

In particular, this applies to $15 = 3 \cdot 5$ since 3 does not divide $5 - 1$, so the only group of order 15 is $\mathbb{Z}/15\mathbb{Z}$. This is then an example of a non-prime order (prime-order groups are always cyclic) with the property that every group of that order must be cyclic. Similarly, every group of order $33 = 3 \cdot 11$ is cyclic, and there are many more examples of such orders.

Warm-Up 2. We show that every group G of order 30 contains $\mathbb{Z}/15\mathbb{Z}$ as a subgroup. We can actually give a quick answer to this based on a recent homework problem: since $30 = 2 \cdot 15$ where 15 is odd, a recent homework problem shows that G has a subgroup H of index 2, which then has order 15 and is thus isomorphic to $\mathbb{Z}/15\mathbb{Z}$ by the first Warm-Up.

Here is another method, which we look at only to clarify the book's approach. (The book makes this way more complicated than necessary.) Let P be a Sylow 3-subgroup and Q a Sylow 5-subgroup of G. Then we get

$$n_3 = 1, 10 \quad \text{and} \quad n_5 = 1, 6$$

as the possible numbers of such subgroups. But we cannot have both $n_3 = 10$ and $n_6 = 6$ simultaneously, since this would give $10 \cdot 2 = 20$ elements of order 3 (each Sylow 3-subgroup contains 2 elements of order 3, and they all intersect trivially) and $6 \cdot 4 = 24$ elements of order 5 (each Sylow 5-subgroup contains 4 elements of order 5, and they all intersect trivially), which already gives too many elements in G. Thus at least one of n_3 or n_5 is 1, so at least one of P or Q is normal in G. Then PQ is a subgroup of G of order $|PQ| = |P||Q| = 15$ (since $P \cap Q = 1$), and the first Warm-Up shows that $PQ \cong \mathbb{Z}/15\mathbb{Z}$.

Now, here is what the book says: since at least one of P or Q is normal in PQ, both P and Q are *characteristic* subgroups of PQ, so both P and Q are normal in PQ, which implies that $PQ \cong P \times Q$ is $\mathbb{Z}/15\mathbb{Z}$. We have not spoken about characteristic subgroups before, so here is a definition: H is a characteristic subgroup of G if it is invariant under every automorphism of G, i.e. if $\phi \in \text{Aut}(G)$, then $\phi(H) = H$. (The fact that characteristic subgroups are always normal comes from considering the automorphisms of G induced by conjugation by elements of G.) The notion of a characteristic subgroup, however, is not we will really need going forward, and indeed I think the book's use of this concept here is confusing. In particular, the fact that here both P and Q are characteristic in PQ is not a general type of phenomena for products of subgroups, and is unique to the circumstances of this type of problem. The point is that in this case, even though P is not the only Sylow 3-subgroup of G, it *is* the only Sylow 3-subgroup of PQ! Indeed, the number n_p of Sylow 3-subgroups of PQ has to be congruent to 1 mod 3 and divide 15 (instead of 30 as before), and $n_2 = 1$ is now the only possibility. This is why both P and Q are normal in PQ *in this particular instance*, so $PQ \cong P \times Q$. I do not know what benefit the book gets from phrasing this in terms of characteristic subgroups, but cést la vie.

Automorphisms of normal Sylows. Even if the book's approach to the second Warm-Up above is not necessarily the quickest way towards a proof, it does have the benefit of introducing the use of automorphisms, in that case via the concept of a characteristic subgroup. This was not so crucial in that specific problem, but now we outline the way in which automorphisms *will* be crucial in applications of Sylow Theory in general.

Suppose G is a group with a unique (equivalently normal) Sylow p-subgroup P. The fact that P is normal guarantees that conjugating P by elements of G still produces elements of P, so that the map $g : P \to P$ induced by such a conjugation can be viewed as an *automorphism* of P. That is, normality of P gives a homomorphism

$$G \to \text{Aut}(P)$$

which sends $g \in G$ to the automorphism which sends $p \in P$ to $gpg^{-1} \in P$. The point is that if we know something about the structure of this automorphism group $\text{Aut}(P)$, we can derive information about the homomorphism $G \to \text{Aut}(P)$ and thereby understand something more about how elements of G relate to those of P. Even better: conjugating by elements of any subgroup $Q \leq G$ (for instance, a Sylow q-subgroup) also gives a homomorphism $Q \to \text{Aut}(P)$, which says something about the commutativity or lack thereof between elements of Q and elements of P.

Example. Here is a first example of putting this idea into action. Suppose G is a group of order $231 = 3 \cdot 7 \cdot 11$. We claim that every element of G of order 11 commutes with every other element of G, and hence must be contained in the center $Z(G)$. The structure of a certain automorphism group here will be key.

Since n_{11} must divide $3 \cdot 7 = 21$ and is congruent to 1 mod 11, the only possibility is $n_{11} = 1$. Thus there is a normal Sylow 11-subgroup of G; call it $P \cong \mathbb{Z}/11\mathbb{Z}$. Since P is normal, conjugation by elements of P gives an automorphism of P, so we have a homomorphism

$$\phi : G \to \text{Aut}(P).$$

Now, we previously determined the structure of the automophism group of a cyclic group, with the result being $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. (This comes from the fact that only those elements in

$(\mathbb{Z}/n\mathbb{Z})^\times$ can serve as generators of $\mathbb{Z}/n\mathbb{Z}$. Check earlier in these notes for more details.) Thus in our case we have

$$\operatorname{Aut}(P) \cong \operatorname{Aut}(\mathbb{Z}/11\mathbb{Z}) \cong (\mathbb{Z}/11\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z},$$

and so ϕ above maps G into a group of order 10. The image of ϕ must thus have order dividing 10 and dividing $|G| = 231$ (by the First Isomorphism Theorem), so since 10 and 231 are relatively prime we get that $\phi(G)$ has order 1, and is thus trivial.

But saying that ϕ is trivial means that $\phi(g)$ is the identity automorphism for every $g \in G$, so that the automorphism of P induced by conjugation by g is the identity:

$$gpg^{-1} = p \text{ for all } p \in P.$$

This means that each $p \in P$ commutes with all $g \in G$, so $P \leq Z(G)$. Every element of G of order 11 is contained in some Sylow 11-subgroup, so every such element is in $Z(G)$ as claimed.

Another example. Let us consider one final example. Previously we considered those groups G of order $|G| = pq$ with $p < q$ primes where $p \nmid q - 1$ (G is cyclic in this case), and now we consider the case where p does divide $q - 1$. Following the same logic as before, there is a unique normal Sylow q-subgroup Q, and the number of Sylow p-subgroups is either $n_p = 1$ or $n_p = q$. In this case, however, $n_p = q$ is possible since q is congruent to 1 mod p because $p \mid q - 1$. If $n_p = 1$, then the same reasoning as before applies and G will be cyclic.

Now consider the case where $n_p = q$, and let P be a Sylow p-subgroup of G. We show that in this case there can only be *at most* $p - 1$ candidates for G, which will necessarily be non-abelian since they have non-normal Sylow subgroups. (In fact, all of these "at most" $p - 1$ candidates will be isomorphic to each other, so that there is actually only *one* group in this case, but we will save this fact for later after we have discussed semidirect products.) As in the previous example, normality of Q says that conjugating by elements of G gives an automorphism of Q, so in particular we consider conjugating only by elements of P to get a homomorphism

$$\phi : P \to \operatorname{Aut}(Q).$$

(To be clear, for $x \in P$, $\phi(x)$ is the automorphism of Q which sends $y \in Q$ to $xyx^{-1} \in Q$.) Since $Q \cong \mathbb{Z}/q\mathbb{Z}$ since $|Q| = q$ is prime, we have that

$$\operatorname{Aut}(Q) \cong \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}.$$

The image $\phi(P)$ of ϕ thus has order dividing $q - 1$ and $|P| = p$. Since p is prime, this gives the possibilities $|\phi(P)| = 1$ or p. (The latter is allowed since p does divide $q - 1$ in this example.) But if $|\phi(P)| = 1$, then ϕ is trivial, meaning that $\phi(x)$ is the identity automorphism for all $x \in P$:

$$xyx^{-1} = y \text{ for all } y \in Q.$$

This would imply that elements of P commute with those of Q, so $G = PQ$ (note $|PQ|$ is still $pq = |G|$ in this case) would be abelian. This is not true in this case, so $|\phi(P)| = p$ instead.

Thus $\phi(P)$ is cyclic (and ϕ induces an isomorphism between G and $\phi(G)$), generated by any element of $\operatorname{Aut}(Q) \cong \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$ of order p. Now, to be clear, the isomorphism between $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$ and $\operatorname{Aut}(Q)$ sends the "multiplication by k" map (for $k \in (\mathbb{Z}/q\mathbb{Z})^\times$) to the "$k$-th power" map $y \mapsto y^k$, which is a homomorphism of Q since Q is abelian. Hence, the possible generators of $\phi(P) \leq \operatorname{Aut}(Q)$ can be explicitly described as being the k-th power maps for those $k \in (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$ of order p, of which there are $p-1$ many in total. (The elements of order p in $\mathbb{Z}/(q-1)\mathbb{Z}$

are $\ell(q-1)/p$ for $\ell = 1, \dots, p-1$.) Pick generators x of P and y of Q. Then $\phi(x) \in \phi(G) \leq \operatorname{Aut}(Q)$ is one of these k-th power maps, meaning that

$$xyx^{-1} = y^k \text{ for some } k \in (\mathbb{Z}/q\mathbb{Z})^\times \text{ of order } p.$$

But this fully determines G, which can now be given in terms of generators and relations as:

$$G = \langle x, y \mid x^p = 1 = y^q, xyx^{-1} = y^k \rangle$$

for one of the values of k above. Since there are $p-1$ choices for k, this at first glance gives at most $p-1$ possibilities for G as claimed. (As stated before, we will later show that in fact these are all actually isomorphic to each other. Note that when $p = 2$, we can immediately see that we only get one such group—the dihedral group—since $p - 1 = 1$ in this case: $q - 1 \in (\mathbb{Z}/q\mathbb{Z})^\times$ is the only element of order 2, so the defining relation in the presentation above becomes $xyx^{-1} = y^{q-1}$, which is precisely the defining relation of D_{2q} with x playing the role of s and y the role of r.)

Lecture 26: Semidirect Products

Warm-Up. We go back to considering groups G of order 12. Previously we argued that in the case where the Sylow 2- and 3-subgroups are unique, hence normal, G is abelian and isomorphic to either $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, while in the case where there are four Sylow 3-subgroups, G is isomorphic to A_4. That leaves the case there are three Sylow 2-subgroups (so G is necessarily non-abelian) and only one Sylow 3-subgroup. We claim that, for now, there are at most four possibilities for G. (We will see later that there are actually only two: D_{12} and a group we have yet to describe.)

Let P be a Sylow 2-subgroup (of order 4) and Q the Sylow 3-subgroup (of order 3). Then Q is normal in G, so conjugation by elements of P gives automorphism of Q:

$$\phi : P \to \operatorname{Aut}(Q),\ \ \phi(x) = \text{conjugation by } x \text{ for } x \in P.$$

In order to obtain a non-abelian group, this map ϕ must be nontrivial since otherwise elements of P would commute with elements of Q, in which case $G = PQ \cong P \times Q$ would be abelian. We previously classified groups of order p^2 for p prime, so that in this case P of order $4 = 2^2$ is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $\operatorname{Aut}(Q) \cong \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$, we thus seek to classify nontrivial homomorphisms

$$\phi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^\times \quad \text{ and } \quad \phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^\times.$$

In the first case, ϕ is determined by the value of $\phi(1)$. In order for ϕ to be nontrivial, $\phi(1)$ should not be 1, so it must be $\phi(1) = 2$. Thus we only get one possible group G in this case: if x generates P and y generates Q, then $\phi(1) = 2$ means that conjugation by x should act as the "second-power" map, so that $xyx^{-1} = y^2$ and thus $G = PQ$ has presentation

$$G = \langle x, y \mid x^4 = 1 = y^3, xyx^{-1} = y^2 \rangle.$$

(This is actually not a group we have come across before!) In the case where $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a homomorphism

$$\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^\times$$

is determined by $\phi(1, 0)$ and $\phi(0, 1)$. Since $(\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$, the non-trivial possibilities are:

$$\phi(1,0) = 1, \phi(0,1) = 2 \quad \phi(1,0) = 2, \phi(0,1) = 1 \quad \phi(1,0) = 2, \phi(0,1) = 2.$$

(Having $\phi(1,0) = 1 = \phi(0,1)$ yields the trivial homomorphism, which gives G abelian.) Thus there are at most three groups we get in this case, so four overall. (Again, we will see that the three we get here are actually all isomorphic—it is D_{12}!—so there are actually only two distinct groups in the case where $n_2 = 3$ and $n_3 = 1$.)

Rethinking products of subgroups. In many of the recent examples we have looked at ($|G| = pq$ and $|G| = 12$ for instance, and some others), we have come across the following setup: a group G with a normal Sylow subgroup Q and some other subgroup P such that $Q \cap P = 1$ and $G = QP$. Let us consider this scenario in a bit more detail, since it is the prototype for the notion of a *semidirect product* of groups, which is the final tool we need to carry out classifications.

If $Q \cap P = 1$, then when writing an element of $G = QP$ in the form yx with $y \in Q$ and $x \in P$, we see that there is a unique way of doing so: if $yx = y'x'$ are two such expressions, then $x(x')^{-1} = y^{-1}y'$ is in both P and Q, and hence must be 1, which implies $x = x'$ and $y = y'$. Thus to get a handle on the entire structure of $G = QP$, we need only understand the group multiplication better. In particular, if y_1x_1 and y_2x_2 are two elements of QP (with $y_i \in Q, x_i \in P$), we seek to write their product in the form required of elements of QP. Note that:

$$(y_1x_1)(y_2x_2) = (yx_1y_2x_1^{-1})(x_1x_2)$$

after inserting $1 = x_1^{-1}x_1$ in between y_2 and x_2. But this is the form we want: since Q is normal, $x_1y_2x_1^{-1} \in Q$, so $y_1x_1y_2x_1^{-1}$ is indeed in Q and x_1x_2 is in P. If we consider the action of P on Q by conjugation, we can $x_1y_2x_1^{-1}$ as $x_1 \cdot y_2$, so that the above product looks like

$$(y_1x_1)(y_2x_2) = (y_1[x_1 \cdot y_2])(x_1x_2).$$

The point is that, as a set, we can think of QP as $Q \times P$, since we can "separate" the elements of Q from those of P due to the uniqueness of an expression yx with $y \in Q, x \in P$. Under this identification $QP = Q \times P$ (not literally an equality), the multiplication above tells us how to interpret the group operation on QP as an operation on $Q \times P$ instead: the Q-component is $y_1[x_1 \cdot y_2]$ and the P-component is x_1x_2.

Semidirect Products. Thus, we make the following general definition. Let Q and P be groups (not assumed a priori to be subgroups of any larger group) with an action of P on Q by automorphisms; equivalently a homomorphism $\phi : P \to \text{Aut}(Q)$. The *semidirect product* determined by ϕ is the group whose underlying set is $Q \times P$, and whose group operation is given by

$$(y_1, x_1)(y_2, x_2) := (y_1[x_1 \cdot y_2], x_1x_2).$$

That this does define a group structure is a straightforward (but non-trivial!) check, and was actually carried out in the Discussion 2 Problems handout. (Of course, back then we had no context for this construction. Also, back then we wrote the product as $P \times Q$ instead of $Q \times P$, which requires a slight adjustment to the definition of the multiplication; the two constructions, however, are easily seen to be isomorphic. The fact that P acts by automorphisms is crucial to verifying the associativity of the multiplication above. The inverse of (y, x) is $(x^{-1} \cdot y^{-1}, x^{-1})$.) The semidirect product is denoted by $Q \rtimes_\phi P$ (it depends on the action ϕ), or simply $Q \rtimes P$ if the action is clear from context.

In the case of $G = QP$ from before, we see thus see that with the action of P on Q being the conjugation action, the resulting semidirect product $Q \rtimes P$ is indeed isomorphic to QP. (After all, this is what motivated the definition of a general semidirect product!) But in fact, this scenario always holds, and all semidirect products arise in this way: set $G = Q \rtimes P$ (recall that in the general construction Q, P can be unrelated groups which are not assumed to be subgroups of an already existing group), so that we can identity Q with the subgroup $Q \times \{e_P\}$ and P with the subgroup $\{e_Q\} \times P$. Then you can verify that Q is normal in G and $Q \cap P$ is trivial. Conjugating an element of Q by an element of P in $G = Q \rtimes P$ looks the following:

$$(e_Q, x)(y, e_P)(e_Q, x)^{-1} = (x \cdot y, x)(e_Q, x^{-1}) = (x \cdot y, e_P)$$

(so lo and behold $Q \cong Q \times e_P$ is indeed normal!), which shows that the original action $x \cdot y$ corresponds precisely to conjugation in the semidirect product, just as expected from the $G = QP$ case. Thus, thinking of semidirect products as taking place *within* an existing group $G = QP$ with a conjugation action or as $Q \rtimes P$ with any action by automorphisms are equivalent. (Often the terms *inner* and *outer* semidirect products are used to distinguish between these scenarios.)

Note also that the usual direct product $Q \times P$ is a special case: when P acts trivially on Q (equivalently $P \to \mathrm{Aut}(Q)$ is trivial), then

$$(y_1, x_1)(y_2, x_2) = (y_1[x_1 \cdot y_2], x_1x_2) = (y_1y_2, x_1x_2)$$

is the usual group structure on $Q \times P$. This corresponds precisely to what we have seen in $G = QP$ when *both* Q and P are normal, so that $QP \cong Q \times P$.

Example. Consider the usual action of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$ by matrix multiplication. If we consider $\mathbb{R}^n$ as a group under vector addition, this is an action by automorphisms. (This just says that linear transformations preserve addition.) Thus we get a semidirect product $\mathbb{R}^n \rtimes GL_n(\mathbb{R})$ whose group operation is:

$$(\mathbf{b}, A)(\mathbf{c}, B) = (\mathbf{b} + A\mathbf{c}, AB).$$

This semidirect is called the n-dimensional *general affine group*, and is the group of so-called invertible *affine transformations* of $\mathbb{R}^n$, which are functions $T : \mathbb{R}^n \to \mathbb{R}^n$ of the form $T(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ for a fixed invertible matrix A and fixed vector $\mathbf{b}$. (So, affine transformations are compositions of linear transformations with translations. The defining data $A, \mathbf{b}$ of an affine transformation corresponds precisely to $(\mathbf{b}, A) \in \mathbb{R}^n \times GL_n(\mathbb{R})$.) The point is that composing two affine transformation $T(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ and $S(\mathbf{x}) = B\mathbf{x} + \mathbf{c}$ gives:

$$TS(\mathbf{v}) = T(B\mathbf{x} + \mathbf{c}) = A(B\mathbf{x} + \mathbf{c}) + \mathbf{b} = AB\mathbf{x} + [A\mathbf{c} + \mathbf{b}],$$

where if we "isolate" the $\mathbb{R}^n$-component $\mathbf{b} + A\mathbf{c}$ from the $GL_n(\mathbb{R})$-component AB, we get precisely the semidirect product element $(\mathbf{b} + A\mathbf{c}, AB)$. So, the semidirect group operation in this case encodes composition of affine transformations.

Revisiting dihedral groups. Consider now the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/n\mathbb{Z}$ where the non-identity element of $\mathbb{Z}/2\mathbb{Z}$ acts by inversion: $1 \cdot x = -x$, or in other words where $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ sends the generator 1 of the domain to the automorphism which send everything in $\mathbb{Z}/n\mathbb{Z}$ to its inverse. The semidirect product $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ has the group operation given explicitly by:

$$(a, b)(c, d) = (a + (-1)^b c, b + d)$$

since $(-1)^b c = c$ when $b = 0$ and $(-1)^b c = -c$ when $b = 1$.

We claim that this is actually describing D_{2n}! This was shown back in the Discussion 2 Problems where semidirect products were first introduced, but here is the idea anyway. Identify the generator of $\mathbb{Z}/2\mathbb{Z}$ with $s \in D_{2n}$ and the generator of $\mathbb{Z}/n\mathbb{Z}$ with $r \in D_{2n}$. Then we have

$$(0, s)(r, 0)(0, s)^{-1} = (r^{-1}, s)(0, s^{-1}) = (r^{-1}, 0),$$

which says that $srs^{-1} = r^{-1}$. (Recall, after all, that the action $\mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ should simply correspond to conjugation in the semidirect product, so since we said that conjugation by $s \in \mathbb{Z}/2\mathbb{Z}$ should act as inversion, we should expect $srs^{-1} = r^{-1}$.) The elements of $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, written simply as elements in the product $(\mathbb{Z}/n\mathbb{Z})(\mathbb{Z}/2\mathbb{Z})$ where $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ are viewed as subgroups of $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, are of the form $r^i s^x$ where $i = 1, \ldots, n$ and $x = 0, 1$, which precisely correspond to the elements of D_{2n}. Using $srs^{-1} = r^{-1}$, and noting $s^{-1} = s$, we get the following presentation for $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$:

$$\langle r, s \mid r^n = 1 = s^2, srs = r^{-1} \rangle,$$

which is indeed the standard presentation of D_{2n}, so $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{2n}$ as claimed.

Lecture 27: Classifying Groups

Warm-Up 1. We show that there are four homomorphisms $\mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$, and that they give rise to non-isomorphic semidirect products $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. (Honestly, this is much more than a "Warm-Up", since we will see in a bit that this amounts to classifying all groups of order 30.) First, we claim that

$$\text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z}).$$

(More generally, $\text{Aut}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/m\mathbb{Z})$ when n and m are relatively prime.) Given $f \in \text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$, the point is that $f(1,0)$ must actually be an element of $\mathbb{Z}/3\mathbb{Z} \times 0$ and $f(0,1)$ must be an element of $0 \times \mathbb{Z}/5\mathbb{Z}$. Indeed, $(1,0)$ has order 3 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, so $f(0,1)$ have have order 3 as well. But this rules out anything like

$$f(1,0) = (a, \text{nonzero}),$$

since no nonzero element of $\mathbb{Z}/5\mathbb{Z}$ has order dividing 3. Similarly, $(0,1)$ has order 5 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, so $f(0,1)$ must have order 5 as well, and hence must be of the form $f(0,1) = (0,b)$ since no nonzero element of $\mathbb{Z}/3\mathbb{Z}$ has order dividing 5. Thus f acting on $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times 0$ produces something in $\mathbb{Z}/3\mathbb{Z}$, and similarly for f acting on $\mathbb{Z}/5\mathbb{Z} \cong 0 \times \mathbb{Z}/5\mathbb{Z}$, so that the behavior of f can be "separated" into its behavior on $\mathbb{Z}/3\mathbb{Z}$ and its behavior on $\mathbb{Z}/5\mathbb{Z}$:

$$\text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \to \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z}) \text{ defined by } f \mapsto (f|_{\mathbb{Z}/3\mathbb{Z}}, f|_{\mathbb{Z}/5\mathbb{Z}}),$$

where $f|_A$ denotes the restriction of f to the subgroup A, is an isomorphism. (In other words, an automorphism of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ does not "mix up" terms between the factors.)

Since $\text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$ and $\text{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$, we can now get to work. A homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z})$ is determined by $\phi(1)$, which must be an element of order dividing 2. Both elements of $\text{Aut}(\mathbb{Z}/3\mathbb{Z})$ have order dividing 2, but only $1, 4 \in \text{Aut}(\mathbb{Z}/5\mathbb{Z})$ do (recall that by $k \in \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ we mean the map which is "multiplication by k"), so we get four possibilities:

$$\phi(1) = (1,1), (2,1), (1,4), (2,4) \in \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z}).$$

To be even clearer: $1 \in \text{Aut}(\mathbb{Z}/3\mathbb{Z})$ or $\text{Aut}(\mathbb{Z}/5\mathbb{Z})$ denotes the identity map id (multiply by 1) and both $2 = -1 \in \text{Aut}(\mathbb{Z}/3\mathbb{Z})$ and $4 = -1 \in \text{Aut}(\mathbb{Z}/5\mathbb{Z})$ denote inversion inv (multiply by -1), so the four possibilities are:

$$\phi(1) = (id, id), (inv, id), (id, inv), (inv, inv).$$

The four semidirect product multiplications on $(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$ are then explicitly given by:

$$\begin{aligned}
&(id, id): && ([a,b],x)([c,d],y) = ([a+c, b+d], x+y)\\
&(inv, id): && ([a,b],x)([c,d],y) = ([a+(-1)^x c, b+d], x+y)\\
&(id, inv): && ([a,b],x)([c,d],y) = ([a+c, b+(-1)^x d], x+y)\\
&(inv, inv): && ([a,b],x)([c,d],y) = ([a+(-1)^x c, b+(-1)^x d], x+y)
\end{aligned}$$

The $(-1)^x$ term tells us whether or not we should invert. Note we can already tell that the first case gives the abelian group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$; indeed, this is expected since in this case $\mathbb{Z}/2\mathbb{Z}\to\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})$ is trivial, so the semidirect product will be the ordinary direct product.

To show that the other three semidirect products (which are necessarily non-abelian) give non-isomorphic groups, we determine the number of elements of order 2 in each. Using the multiplications above we can compute the following squares:

$$\begin{aligned}
&(inv, id): && ([a,b],x)^2 = ([a+(-1)^x a, 2b], 2x)\\
&(id, inv): && ([a,b],x)^2 = ([2a, b+(-1)^x b], 2x)\\
&(inv, inv): && ([a,b],x)^2 = ([a+(-1)^x a, b+(-1)^b], 2x)
\end{aligned}$$

Since $x\in\mathbb{Z}/2\mathbb{Z}$, we always have $2x=0$ so the third component tells us nothing. For the (inv, id) case, $2b\in\mathbb{Z}/5\mathbb{Z}$ is zero if and only if $b=0$. Also, if $x=0$ here, then $a+(-1)^x a = 2a\in\mathbb{Z}/3\mathbb{Z}$ is zero if and only if $a=0$, so the only element whose square is zero when $x=0$ is $([0,0],0)$, which is just the identity. However, if $x=1$, then $a+(-1)^x a = a-a=0$ for all $a\in\mathbb{Z}/3\mathbb{Z}$, so anything of the form

$$([a,0],1)\in(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$$

has order 2. There are three choices for a, so this gives 3 elements of order 2 in the (inv, id) case.

In the (id, inv) case, similar reasoning shows that there are no elements of order 2 when $x=0$, and when $x=1$ we have $2a=0\in\mathbb{Z}/3\mathbb{Z}$ if and only if $a=0$ but $b+(-1)^x b = b-b=0$ for all $b\in\mathbb{Z}/5\mathbb{Z}$, so anything of the form

$$([0,b],1)\in(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$$

has order 2 in this case, and there are 5 such elements. Finally, in the (inv, inv) case, for $x=1$ we have that $a+(-1)^x a$ and $b+(-1)^x b$ are always zero, so

$$([a,b],1)\in(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})\rtimes\mathbb{Z}/2\mathbb{Z}$$

all have order 2, and there are 15 such elements. Thus, we conclude that the four semidirect products arising from $\mathbb{Z}/2\mathbb{Z}\to\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})$ are all non-isomorphic. (The abelian case $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ only has one element of order 2.)

Warm-Up 2. But lest you believe that semidirect products can *never* be isomorphic, here is a general scenario under which they are. Let $\phi: P\to\operatorname{Aut}(Q)$ be a homomorphism. If $f\in\operatorname{Aut}(P)$, then we get another action of P on Q via the homomorphism $\phi\circ f: P\to\operatorname{Aut}(Q)$ which precomposes with f, so that $p\cdot q$ under this new action is $f(p)\cdot q$ under the old. We claim that these two actions of P on Q give isomorphic semidirect products.

Indeed, define a map $\Psi: Q\rtimes_{\phi\circ f}P\to Q\rtimes_\phi P$ by $\Psi(q,p)=(q,f(p))$. This is bijective because $f: P\to P$ is bijective. Moreover, we have:

$$\Psi((q_1,p_1)(q_2,p_2)) = \Psi(q_1\overbrace{[f(p_1)\cdot q_2]}^{\text{using }\phi\circ f}, p_1p_2)$$

$$\begin{aligned}&= (q_1[f(p_1) \cdot q_2], f(p_1 p_2))\\ &= (q_1[f(p_1) \cdot q_2], f(p_1)f(p_2))\\ &= (q_1, f(p_1))(q_2, f(p_2))\\ &= \Psi(q_1, p_1)\Psi(q_2, p_2),\end{aligned}$$

so Ψ preserves multiplication, and is thus an isomorphism. Hence $Q \rtimes_{\phi\circ f} P \cong Q \rtimes_\phi P$ as claimed. We will make use of this fact in a bit.

Classifying groups. Now we come back to the problem of classifying groups, armed with the notion of a semidirect product. Recall the following general type of setup: if a finite group G has a normal Sylow subgroup Q (for some prime), and a subgroup P for which $G = QP$ and $Q \cap P = 1$ (equivalently $|P| = |G|/|Q|$), then G is a semidirect product of Q and P. Thus if we can classify all such semidirect products, with maps $P \to \text{Aut}(Q)$, we can completely understand the structure of G. (There is a limitation to how far this can get us, since a group in general might not have *any* normal Sylow subgroups, so that not all groups can be described via semidirect products, but it will get us quite far anyway. We will say something later about the problem of understanding which groups are indeed obtainable as semidirect products.)

Groups of order 30. We classify all groups of order 30, which we now argue was done in the first Warm-Up. Indeed, if $|G| = 30$, we know from a previous Warm-Up that G has $\mathbb{Z}/15\mathbb{Z}$ as a subgroup. This subgroup has index 2, and so is normal in G. Pick an element (using Cauchy's Theorem) $x \in G$ of order 2. Then conjugation by x gives a homomorphism

$$\langle x\rangle \cong \mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \cong \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \times \text{Aut}(\mathbb{Z}/5\mathbb{Z}).$$

Since $\mathbb{Z}/2\mathbb{Z} \cap \mathbb{Z}/15\mathbb{Z} = 1$, $G = (\mathbb{Z}/2\mathbb{Z})(\mathbb{Z}/15\mathbb{Z})$, so that G is a semidirect product of $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$. The first Warm-Up then shows that there are four different possibilities for G: one abelian group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}$, and three non-abelian groups $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, characterized by having $3, 5$, or 15 elements of order 2.

But actually, in this case we can give descriptions of these three non-abelian possibilities in terms of better known groups. Indeed, D_{30}, $\mathbb{Z}/3\mathbb{Z} \times D_{10}$, and $\mathbb{Z}/5\mathbb{Z} \times D_6$ all have order 30, are non-abelian, and non-isomorphic, so these must be the three semidirect products we computed before. To see which is which, we count elements of order 2:

- D_{30} has 15 elements of order 2, so D_{30} is the semidirect product in the $\phi(1) = (inv, inv)$ case,
- $\mathbb{Z}/3\mathbb{Z} \times D_{10}$ has 5 elements of order 2, so this is the $\phi(1) = (id, inv)$ case, and
- $\mathbb{Z}/5\mathbb{Z} \times D_6$ has 3 elements of order 2, so this is the $\phi(1) = (inv, id)$ case.

We can also determine this as follows. First, recall from last time that $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ with $1 \in \mathbb{Z}/2\mathbb{Z}$ acting by inversion is isomorphic to D_{2n} in general. In the $\phi(1) = (id, inv)$ case above, the point is that this says 1 acts trivially on the $\mathbb{Z}/3\mathbb{Z}$ factor of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, so that $\mathbb{Z}/3\mathbb{Z}$ will then commute with everything else and we can "break off" a $\mathbb{Z}/3\mathbb{Z}$ factor from the semidirect product; but 1 acts by inversion on the $\mathbb{Z}/5\mathbb{Z}$ factor of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, so this portion of the semidirect product gives $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{10}$, which is why we get $\mathbb{Z}/3\mathbb{Z} \times D_{10}$ in this case. Similarly, in the $\phi(1) = (inv, id)$ case, we act trivially on the $\mathbb{Z}/5\mathbb{Z}$ factor—so this "breaks off"—but by inversion on the $\mathbb{Z}/3\mathbb{Z}$ factor, so we get

$$\mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z} \times D_6$$

in tis case. Finally, in the $\phi(1) = (inv, inv)$ case we act by inversion on both factors, which is equivalent to acting by inversion on $\langle(1, 1)\rangle \cong \mathbb{Z}/15\mathbb{Z}$, so we get $\mathbb{Z}/15\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{30}$.

To summarize, there are four groups of order 30: $\mathbb{Z}/30\mathbb{Z}$, D_{30}, $\mathbb{Z}/3\mathbb{Z} \times D_{10}$, and $\mathbb{Z}/5\mathbb{Z} \times D_6$. The point is that the use of semidirect products gives us a way to prove that this list is complete.

Groups of order 12. Next we classify groups of order 12, for which we did the bulk of the work before. Let us recall what we know, based on the numbers of Sylow subgroups:

- when $n_2 = 1$ and $n_3 = 1$, we have $G \cong \mathbb{Z}/12\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$,
- when $n_3 = 4$, we have $G \cong A_4$ (this was a good argument, go back and look at it!); and
- when $n_2 = 3$ and $n_3 = 1$, G is a semidirect product $Q \rtimes P$ where Q is the normal Sylow 3-subgroup and P is a Sylow 2-subgroup. (We did not use the phrase "semidirect product" in this case previously, but this is precisely what we had: $G = QP$, Q normal, and $Q \cap P = 1$.)

Moreover, in this last case we also previously described all possible homomorphisms $P \to \operatorname{Aut}(Q)$, depending on whether $P \cong \mathbb{Z}/4\mathbb{Z}$ or $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which are the only possibilities for $|P| = 4$: when $P \cong \mathbb{Z}/4\mathbb{Z}$, there is only one homomorphism $1 \mapsto 2 = inv$ (we previously called this is the "second power" map, which is the same as inversion in $Q \cong \mathbb{Z}/3\mathbb{Z}$); and when $P \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we obtained three homomorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$, and so at most three possible semidirect products, which we will now show to all be isomorphic.

Recall that the possible nontrivial homomorphisms $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$ are given on generators by:

$$\phi_1(1,0) = inv, \phi_1(0,1) = id \qquad \phi_2(1,0) = id, \phi_2(0,1) = inv \qquad \phi_3(1,0) = inv, \phi_3(0,1) = inv.$$

(Again, we previously denoted *id* by 1 and *inv* by 2.) We now make use of the second Warm-Up: if we can show that the second and third of these are obtained from the first by precomposing with some automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we will know that they give isomorphic semidirect products. If we think of elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are column vectors $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ where $x, y \in \mathbb{Z}/2\mathbb{Z}$, then the automorphisms correspond precisely to invertible matrices with entries in $\mathbb{Z}/2\mathbb{Z}$:

$$\operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong GL_2(\mathbb{Z}/2\mathbb{Z}).$$

(We will consider these types of matrices, and ones with other types of entries, in more detail next quarter in the context of *rings* and *modules*.) Now, we have:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Thus for $f \in \operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ given by this specific matrix, we have:

$$\phi_1(f(1,0)) = \phi_1(1,1) = \phi(1,0)\phi(0,1) = id \cdot inv = inv \quad \text{and} \quad \phi_1(f(0,1)) = \phi_1(1,0) = inv.$$

Hence $\phi_1 \circ f = \phi_3$, so $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi_1} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi_3} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Since

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

for g the automorphism given by this matrix we have:

$$\phi_1(g(1,0)) = \phi_1(0,1) = id \quad \text{and} \quad \phi_1(g(0,1)) = \phi_1(1,1) = inv.$$

Thus $\phi_1 \circ g = \phi_2$, so $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi_1} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi_2} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Hence, as claimed, all semidirect products arising from nontrivial $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$ are isomorphic.

The group we get in this case is actually D_{12}, and here is one way of seeing this. Take the ϕ_1 case. The second $\mathbb{Z}/2\mathbb{Z}$ factor in the domain acts trivially, and so commutes with the $\mathbb{Z}/3\mathbb{Z}$ factor in $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. If we take $x \in \mathbb{Z}/3\mathbb{Z}, y \in \mathbb{Z}/2\mathbb{Z}, z \in \mathbb{Z}/2\mathbb{Z}$ to be generators of the three factors, then we have:

$$xz = zx \quad \text{and} \quad yxy^{-1} = x^{-1},$$

where the second relation comes from having the first $\mathbb{Z}/2\mathbb{Z}$ factor act by inversion on $\mathbb{Z}/3\mathbb{Z}$. But these two together imply:

$$y(xz)y^{-1} = (yxy^{-1})(yzy^{-1}) = x^{-1}z^{-1} = (zx)^{-1} = (xz)^{-1},$$

where we have used the fact that $yzy^{-1} = z$ since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is abelian, and that $z^{-1} = z$. The element $xz \in (\mathbb{Z}/3\mathbb{Z})(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ has order 6 since $|x| = 3$ and $|z| = 2$, so since $y \in \mathbb{Z}/2\mathbb{Z}$ acts by inversion on this element $xz \in \mathbb{Z}/6\mathbb{Z}$, we can characterize $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ instead as $\mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ with the inversion action, which is precisely D_{12}.

The group we got in the $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ case, with $1 \in \mathbb{Z}/4\mathbb{Z}$ acting on $\mathbb{Z}/3\mathbb{Z}$ by inversion, is a brand new group we have not come across before, in the sense that it cannot be described in terms of other groups we have seen: $D_{2n}, S_n, A_n, \mathbb{Z}/n\mathbb{Z}$, etc. The group operation in this semidirect product is explicitly given (in additive form) by:

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Alternatively, in multiplicative form with $\mathbb{Z}/4\mathbb{Z} = \langle x \rangle$ and $\mathbb{Z}/3\mathbb{Z} = \langle y \rangle$, we have $xyx^{-1} = y^{-1}$ ($x = 1$ acts by inversion), so this group has presentation

$$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} = \langle x, y \mid x^4 = 1 = y^3, xyx^{-1} = y^{-1} = y^2 \rangle,$$

which had already derived previously. If you want an even more concrete description, it turns out that we can realize this group as the subgroup of $GL_2(\mathbb{C})$ generated by

$$x = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \text{ and } y = \begin{bmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{bmatrix},$$

where $e^{2\pi/3} = \cos(2\pi/3) + i\sin(2\pi/3)$ and $e^{-2\pi/3} = \cos(2\pi/3) - i\sin(2\pi/3)$. You can check this by verifying that these satisfy the relations in the presentation above.

To summarize, there are five groups of order 12: $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, A_4, D_{12}, and $\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}$ with $1 \in \mathbb{Z}/4\mathbb{Z}$ acting on $\mathbb{Z}/3\mathbb{Z}$ by inversion.

Lecture 28: More Classifications

Warm-Up. We finish the classification of groups of order pq, where $p < q$ are primes. Let us refresh our memory of what we know:

- when $p \nmid q - 1$, the only possibility is $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/qp\mathbb{Z}$;
- when $p \mid q - 1$, $G = QP$ where Q is the normal Sylow q-subgroup and P a Sylow p-subgroup. If P is also normal, then $G \cong Q \times P \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/qp\mathbb{Z}$ is again cyclic.
- when $p \mid q - 1$ and P in the notation above is not normal, the structure of G is determined by the relation $xyx^{-1} = y^k$ where $P = \langle x \rangle$, $Q = \langle y \rangle$, and $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ has order p.

There are $p-1$ elements of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$, giving at most $p-1$ possibilities for G in the last case, but we will now show that these are actually all isomorphic.

First, let us recast everything above in the language of semidirect products. In any case above we have $G = QP$, where Q is the normal Sylow q-subgroup and P a Sylow p-subgroup (note $Q \cap P = 1$), so G is always isomorphic to a semidirect product $Q \rtimes P$ for some action $\phi : P \to \operatorname{Aut}(Q)$. In the case where $p \nmid q-1$, this action must be trivial since $|\phi(P)|$ divides both $|P| = p$ and $|\operatorname{Aut}(Q)| = |(\mathbb{Z}/q\mathbb{Z})^\times| = q-1$, so that $\phi(P) = 1$. Hence the semidirect product is a direct product in this case. If $p \mid q-1$, $\phi(P)$ is either trivial (giving again $G \cong Q \times P$), or a cyclic subgroup of $\operatorname{Aut}(Q)$ of order p, so $\phi(x)$ (where x generates P) is, as stated above, one of $p-1$ elements of order p in $\operatorname{Aut}(Q)$, and $G \cong Q \rtimes P$ is the corresponding semidirect product.

Take k to be a generator of $\phi(P)$ as a cyclic subgroup of order p in $\operatorname{Aut}(Q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$. Then the other elements of order p are k^t for $t = 1, \ldots, p-1$. As an element of $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, k denotes the "multiplication by k", whereas in multiplicative form in $\operatorname{Aut}(Q)$ instead, this is the "k-th power" map. This gives that the action of $P = \langle x \rangle$ on $Q = \langle y \rangle$ is determined by

$$xyx^{-1} = y^k.$$

(This is just what we had said previously when we considered this problem.) For a different choice of an element $\phi(x)$ of order p, we have $\phi(x) = k^t$ (the "k^t-th power" map) for some $t = 1, \ldots, p-1$, so the semidirect product in this case is determined by the relation

$$xyx^{-1} = y^{k^t}.$$

If ϕ_1 denotes the first map $P \to \operatorname{Aut}(Q)$ where $\phi_1(x) = k$ and ϕ_2 the second where $\phi(x) = k^t$, then for the automorphism $f \in \operatorname{Aut}(P)$ given by the t-th power map, we have:

$$\phi_1(f(x)) = \phi_1(x^t) = \phi_1(x)^t = k^t = \phi_2(x),$$

so that $\phi_2 = \phi_1 \circ f$. Thus by the second Warm-Up from last time, ϕ_2 and ϕ_1 determine isomorphic semidirect products $Q \rtimes P$, so we conclude that all of the nontrivial choices for $P \to \operatorname{Aut}(Q)$ give the same nonabelian group $G \cong Q \rtimes P$. In terms of generators and relations

$$\langle x, y \mid x^p = 1 = y^q, xyx^{-1} = y^k \rangle \text{ v.s. } \langle x, y \mid x^p = 1 = y^q, xyx^{-1} = y^{k^t} \rangle,$$

the isomorphism comes from using x^t (also of order p) as a generator in the first case instead of x: the defining relation $xyx^{-1} = y^k$ in the first then becomes the defining relation $(x^t)y(x^t)^{-1} = y^{k^t}$ in the second, so the two presentations give the same group.

To summarize: when $p \nmid q-1$ ($p < q$ primes), the only group of order pq is $\mathbb{Z}/pq\mathbb{Z}$; whereas when $p \mid q-1$, there is one abelian group $\mathbb{Z}/pq\mathbb{Z}$ of order pq and one non-abelian group $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ where $1 \in \mathbb{Z}/p\mathbb{Z}$ acts on $\mathbb{Z}/q\mathbb{Z}$ by multiplication by an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$. Note when $p = 2$ that this non-abelian group $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is precisely D_{2q}, since here $1 \in \mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{Z}/q\mathbb{Z}$ by inversion because the only element of order 2 in $(\mathbb{Z}/q\mathbb{Z})^\times$ is $q-1 = -1$.

Groups of order 18. Let us now classify all groups G of order 18. (We will have to make use of some more advanced linear algebra here, namely linear algebra over what are called *finite fields*. Indeed, one reason to look at this example is to get a sense for some of things we will be looking at next quarter, such as the notion of a finite field and what it means to do linear algebra over them.) Since $18 = 2 \cdot 3^2$, there is a unique/normal Sylow 3-subgroup Q of order 9. (On the homework you will classify groups of order pq^2 with $p < q$ primes where $p \nmid q-1$. In this case, 2 does divide

$3-1$, so this example is not covered by the problem on the homework.) If $P \cong \mathbb{Z}/2\mathbb{Z}$ is a Sylow 2-subgroup, then $G = QP$ ($Q \cap P = 1$ since they have relatively prime orders) so we get

$$G \cong Q \rtimes \mathbb{Z}/2\mathbb{Z} \text{ for some action } \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(Q).$$

Now, $|Q| = 9 = 3^2$, so there are two possibilities for Q: $Q \cong \mathbb{Z}/9\mathbb{Z}$ or $Q \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. (Again, we classified groups of prime-squared order earlier after discussing the class equation.) First we consider the case $Q \cong \mathbb{Z}/9\mathbb{Z}$. But this is very similar to what we have done in other examples: the only element of order 2 in $\operatorname{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ is $8 = -1$, so $\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/9\mathbb{Z})$ is either trivial or the action where $1 \in \mathbb{Z}/2\mathbb{Z}$ acts by inversion, and hence we get $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{18}$ as the possibilities for G in this case.

Now consider $Q \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, so that we need to understand homomorphisms

$$\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}).$$

Thinking about elements of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ as 2-dimensional column vectors with entries in $\mathbb{Z}/3\mathbb{Z}$ shows that we can obtain automorphisms via invertible 2×2 matrices with entries in $\mathbb{Z}/3\mathbb{Z}$, and in fact all automorphisms arise in this way:

$$\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong GL_2(\mathbb{Z}/3\mathbb{Z}).$$

(As stated earlier, this—and some concepts which follow—is the kind of thing we will be able to make clear next quarter.) So, the possible maps $\phi : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ are determined by $\phi(1) \in GL_2(\mathbb{Z}/3\mathbb{Z})$ being a matrix of order dividing 2. But of course, different choices of such matrices could give rise to isomorphic semidirect products, so we need to understand when precisely that happens. Here is a fact: ϕ_1, ϕ_2 give isomorphic semidirect products in this case if and only if $\phi_1(1), \phi_2(1) \in GL_2(\mathbb{Z}/3\mathbb{Z})$ are conjugate matrices. We will not prove this here, but is something which can be done using no more than we already know.

Given this, we must thus understand what conjugacy classes in $GL_2(\mathbb{Z}/3\mathbb{Z})$ look like. And here is where linear algebra comes in: the conjugacy class of a matrix is characterized by its so-called *Jordan normal form*. We will not develop nor define this concept at this point, but will do so next quarter. (In the case of matrices with entries in $\mathbb{R}$ or $\mathbb{C}$, Jordan normals forms are covered in Math 334, the course in abstract linear algebra.) We will say, however, that one class of Jordan normal forms is given by the set of diagonal matrices (Jordan normal forms are related to the notion of diagonalizability), which is all we need for our purposes. The fact is that any matrix in $GL_2(\mathbb{Z}/3\mathbb{Z})$ of order dividing 2 is conjugate to exactly one of the following:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

So, we get the possible semidirect products $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ by considering the actions determined by each of these. Note something special here: the action $\phi : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ determined by each of these has $\mathbb{Z}/2\mathbb{Z}$ acting on each factor of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ independently of one another, due to the fact that these matrices are diagonal. In other words, taking each of these times a vector $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$ in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ does not "mix up" the a and b coordinates. In general, a matrix *can* mix these up, such as in $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right] = \left[\begin{smallmatrix} a+2b \\ 2a \end{smallmatrix}\right]$, so that a general action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ might *not* have $\mathbb{Z}/2\mathbb{Z}$ acting independently on each factor, but the point is that all such actions will determine the same semidirect product as one where $\mathbb{Z}/2\mathbb{Z}$ *does* act independently on each factor.

For $\phi(1) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, the action $\phi : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ is trivial, so G is abelian and isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ in this case. For $\phi(1) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right]$, we have that

$\mathbb{Z}/2\mathbb{Z}$ acts trivially on the first factor of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ but by inversion ($2 = -1$ in $\mathbb{Z}/3\mathbb{Z}$) on the second since:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ 2b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix}.$$

The fact that $\mathbb{Z}/2\mathbb{Z}$ acts trivially on the first factor says that the first $\mathbb{Z}/3\mathbb{Z}$ factor commutes with everything else (it already commutes with the second $\mathbb{Z}/3\mathbb{Z}$ factor in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$), so we can "break off" a $\mathbb{Z}/3\mathbb{Z}$ factor from all of G: $G \cong \mathbb{Z}/3\mathbb{Z} \times (\text{something})$. We are left with $\mathbb{Z}/2\mathbb{Z}$ acting on the second $\mathbb{Z}/3\mathbb{Z}$ by inversion, and this gives D_6, so overall:

$$G \cong \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \times D_6.$$

That leaves the case where $\phi(1) = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$, where $\mathbb{Z}/2\mathbb{Z}$ acts on each factor of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by inversion. This semidirect product $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to a group which can be described in simpler terms using more familiar groups, so the semidirect product description is the best we can do! Explicitly, the semidirect product multiplication is:

$$([a, b], x)([c, d], y) = ([a + (-1)^x c, b + (-1)^x d], x + y).$$

Written instead in multiplicative form with $\mathbb{Z}/2\mathbb{Z} = \langle x \rangle$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \langle y \rangle \times \langle z \rangle$, this can be characterized by the relations

$$xyx^{-1} = y^{-1} \quad \text{and} \quad xzx^{-1} = z^{-1}.$$

Thus this group has presentation $\langle x, y, z \mid x^2 = y^3 = z^3 = 1, yz = zy, xyx^{-1} = y^{-1}, xzx^{-1} = z^{-1} \rangle$.

In summary, there are five groups of order 18: $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, D_{18}, $\mathbb{Z}/3\mathbb{Z} \times D_6$, and the semidirect product $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ where $1 \in \mathbb{Z}/2\mathbb{Z}$ acts on each factor by inversion.

Groups of order 8. We finish with the classification of groups of order 8. This requires—for the final group at least—a different approach than what we've used so far since the final group we'll give is *not* obtainable as a semidirect product. Indeed, note that Sylow theory is completely useless here since the only Sylow subgroup of a group G of order $8 = 2^3$ is the entire group itself!

So, instead we argue by considering orders of elements. Any element of G will have order $1, 2, 4$, or 8. If there is an element of order 8, then $G \cong \mathbb{Z}/8\mathbb{Z}$. If all non-identity elements have order 2, then for three such elements x, y, z we have that the subgroups they generate have pairwise trivial intersections, so

$$G = \langle x \rangle \langle y \rangle \langle z \rangle \cong \langle x \rangle \times \langle y \rangle \times \langle z \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

That leaves the case where there is an element x of order 4, and no element of order 8. Note that x^2 then has order 2. If there is some other element y of order 2, then $\langle x \rangle \cap \langle y \rangle = 1$ so $G = \langle x \rangle \langle y \rangle$. Since $\langle x \rangle$ is normal in G (it has index 2), in this case we do get G as a semidirect product $\langle x \rangle \rtimes \langle y \rangle$. There are two homomorphisms $\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/4\mathbb{Z})$, where $1 \in \mathbb{Z}/2\mathbb{Z}$ acts trivially or by inversion, so we get either $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_8$.

Thus finally we are left with the case where x^2 (where $|x| = 4$ as above), is the only element of order 2. Then all of the elements y not in $\langle x \rangle$ must have order 4. We then have $x^2 = y^2$ and that yxy^{-1} must be an element of order 4 in $\langle x \rangle$ (this subgroup is still normal), so we have

$$yxy^{-1} = x \quad \text{or} \quad yxy^{-1} = x^3.$$

If all such y satisfy the first relation, then x commutes with all elements not in $\langle x \rangle$, which implies that x is in the center of G. Then $Z(G)$ has order 4 or 8, both of which imply G is abelian:

$|Z(G)| = 8$ immediately gives $Z(G) = G$, whereas $|Z(G)| = 4$ implies $G/Z(G) \cong \mathbb{Z}/2\mathbb{Z}$ is cyclic, which implies that G is abelian. But all the abelian cases were already worked out above ($\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; this probably depends on the fact that all finite abelian groups are products of cyclic groups, which we will finally prove next time), so we are left with the case where one y of order 4 satisfies $yxy^{-1} = x^3$. Our group then has presentation

$$G = \langle x, y \mid x^4 = 1 = y^4, yxy^{-1} = x^3 \rangle$$

(the other elements of order 4 are xy and $(xy)^{-1}$), which in fact describes Q_8! Indeed, we can take $x = i$ and $y = j$, and verify that $i^4 = 1 = y^4$ and $jij^{-1} = -i = i^3$ to see that this is the case. The quaternion group Q_8 is, in fact, a group which is not obtainable as a semidirect product, except for something silly like $Q_8 \rtimes \{e\}$ or $\{e\} \rtimes Q_8$. (We will say something about why next time.)

To summarize, there are five groups of order 8: three $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ abelian and two D_8, Q_8 non-abelian.

Lecture 29: Finitely Generated Abelian

Warm-Up. We list all groups of order at most 15, which by now we have fully classified. Let us record the list in the table below, where in the final column we recall some of the techniques used in the classification:

order	groups	techniques
1	$\{e\}$	:)
2	$\mathbb{Z}/2\mathbb{Z}$	Lagrange
3	$\mathbb{Z}/3\mathbb{Z}$	Lagrange
4	$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	class equation
5	$\mathbb{Z}/5\mathbb{Z}$	Lagrange
6	$\mathbb{Z}/6\mathbb{Z}, S_3 \cong D_6$	G acting on cosets
7	$\mathbb{Z}/7\mathbb{Z}$	Lagrange
8	$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_8, Q_8$	semidirect, brute force
9	$\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	class equation
10	$\mathbb{Z}/10\mathbb{Z}, D_{10}$	$\|G\| = pq$
11	$\mathbb{Z}/11\mathbb{Z}$	Lagrange
12	$\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_{12}, A_4, \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	G acting on Sylows
13	$\mathbb{Z}/13\mathbb{Z}$	Lagrange
14	$\mathbb{Z}/14\mathbb{Z}, D_{14}$	$\|G\| = pq$
15	$\mathbb{Z}/15\mathbb{Z}$	$\|G\| = pq$

By "Lagrange" we mean the use of Lagrange's Theorem to show that any group of prime order is cyclic; by "class equation" we mean the use of the class equation to show that any group of prime-power order has a nontrivial center, which then leads to the classification of groups of prime-squared order; by "semidirect" we mean the use of semidirect products; by "$|G| = pq$" we mean the classification of groups of order a product of two distinct primes; by "G acting on something" we mean the action of G on cosets by left multiplication (in the order 6 case) or on Sylow subgroups by conjugation (in the order 12 case), which leads to a map $G \to S_n$; and by "brute force" we mean the brute force computation which constructs Q_8 in the order 8 case. Of course, this list of techniques is not exclusive, so that one technique might also show up elsewhere (such as the use of semidirect products in the $|G| = pq$ case or the order 12 case), and is only meant to highlight some important ideas.

We stop at order 15 because the order 16 case is where things get more complicated: there are 14 (!) non-isomorphic groups of order 16. Part of the reason why this is more complicated is because the Sylow Theorems are of no use here: the only Sylow subgroup of a group of order $16 = 2^4$ is the entire group itself, so nothing can be said from Sylow theory alone. The same was true in the order $8 = 2^3$ case, and as there the order 16 case requires many more brute force computations. I completely believe it is possible to work them all out by hand using the tools you have available so far, but certainly it would involve a lot of work. After order 16 things calm down again for a bit: $17, 19$ and 23 are all prime; we did order 18 (and 30) previously; order 20 is on the homework, and orders 21 and 22 are covered by $|G| = pq$. Then with order 24 we again get a large number of possibilities—15 in this case—which involves a lot more work. And so on, we can keep going, classifying many groups along the way, up to order 60 when we hit our first nonsolvable group A_5. As a general comment, there exist many more tools we can use to classify even more groups, but not ones we will discuss in this course.

What are semidirect products? Apart from the failure of the Sylow Theorems to give much meaningful information (such as in the orders 8 and 16 cases), another main reason why the problem of classifying groups becomes harder in general is the fact that not every group is obtainable as a "non-silly" semidirect product. (By a "silly" semidirect product we mean something like

$$G \cong G \rtimes \{e\} \cong \{e\} \rtimes G$$

with trivial actions of $\{e\}$ on G or G on $\{e\}$, so by a "non-silly" one we mean not one of these, so one which uses *proper, nontrivial* subgroups of G.) Let us say a bit more about this. If $G \cong Q \rtimes P$ where $Q \trianglelefteq G$ and $P \leq Q$ with $G = QP$ and $Q \cap P = 1$, then the Second Isomorphism Theorem gives $(Q \rtimes P)/Q \cong P/(Q \cap P) \cong P$. Thus, $G \cong Q \rtimes P$ fits into the following sequence:

$$Q \hookrightarrow Q \rtimes P \twoheadrightarrow P.$$

(Recall that the $\hookrightarrow$ denotes an injecion, and the $\twoheadrightarrow$ a surjection.)

We briefly saw such sequences earlier, in the context of constructing finite groups from simple groups via a composition series. In general, we referred to the problem of constructing G from such a sequence

$$Q \hookrightarrow G \twoheadrightarrow P$$

as an *extension problem*, and now we are saying that semidirect products provide one type of solution to such a problem. But, semidirect products provide a special type of solution: if G in the sequence above is in fact isomorphic to a semidirect product $Q \rtimes P$, then $P \cong G/Q$ is itself (isomorphic to) a subgroup of G. Said another way, in this case there is a map $P \to G$ whose composition with the map $G \twoheadrightarrow P$ in the sequence is the identity on P (which forces $P \to G$ to be injective), and via this map $P \to G$ we can realize P as a subgroup of G. When such a map $P \to G$ exists, we say that the sequence above *splits*. The fact is that the converse is true: if the sequence $Q \hookrightarrow G \twoheadrightarrow P$ splits, then $G \cong Q \rtimes P$ for the action of P on Q by conjugation given by the realization of $P \cong G/Q$ as a subgroup of G via the splitting.

Thus, G is a "non-silly" semidirect product if and only if it fits in the middle of a sequence with nontrivial groups which splits. The problem of determining when a sequence splits is a hard one in general, and indeed amounts to the same problem as that of building finite groups out of simple groups. Consider now the example of Q_8. In this case, the only possible nontrivial normal subgroups Q of G in the relevant sequence are $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, so the only possible sequences are of the form

$$\mathbb{Z}/4\mathbb{Z} \hookrightarrow Q_8 \twoheadrightarrow Q_8/(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \hookrightarrow Q_8 \twoheadrightarrow Q_8/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

(The $\mathbb{Z}/4\mathbb{Z}$ in the first sequence is obtained by any of $\langle i \rangle, \langle j \rangle, \langle k \rangle$, and the $\mathbb{Z}/2\mathbb{Z} \leq Q_8$ in the second sequence is $\langle -1 \rangle$. The quotient $Q_8/\langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is generated by i and j.) However, neither of these sequences split: if the first did split, we would have $Q_8 \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, but the only possible such semidirect products are $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and D_8 since the only actions $\mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/4\mathbb{Z})$ are the trivial one and the one where 1 acts by inversion; whereas if the second sequence split, there would be a subgroup of Q_8 isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which there is not. Thus Q_8 cannot be expressed a semidirect product of proper, nontrivial groups. In fact, Q_8 was not the first group in our list of groups of order at most 15 above which is not a semidirect product: $\mathbb{Z}/4\mathbb{Z}$ is also not a semidirect product, since the only semidirect product form which could work is $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, and the only such semidirect product is actually $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Finitely generated abelian groups. And now we move towards our final result of the quarter: the classification of finite abelian groups. We have made mention of this result in previously, where the fact is that any finite abelian group is a direct product of cyclic groups. In fact, we will phrase the result we want in the more general setting of *finitely generated* abelian groups, of which finite abelian groups are a special case. (Actually, we will only prove the finite case at this point, and will leave the general finitely generated case to next quarter where it will be a consequence of some more general "linear algebraic" result.)

Recall that an abelian group G is finitely generated if there exist finitely many $x_1, \ldots, x_n \in G$ such that $G = \langle x_1, \ldots, x_k \rangle$. Concretely, this means that anything in G is of the form $n_1x_1 + \cdots + n_kx_k$ where each $n_i \in \mathbb{Z}$:

$$G = \{n_1x_1 + \cdots + n_kx_k \mid n_i \in \mathbb{Z}\}.$$

Here we use the convention (which will be in effect next quarter as well) that we use additive notation when working with abelian groups (since addition in any way, shape, or form is always assumed to be commutative, whereas multiplication is not), and that n_1x_1 is assumed to be the result of adding $-x_1$ to itself $|n_1|$ (absolute value) times when n_1 is negative. (It is no coincidence that this looks similar to "linear combination" or "span" notation from linear algebra, as we will see next quarter.) Now, given these generators $x_1, \ldots, x_k \in G$ we can construct a surjective homomorphism

$$\phi : \mathbb{Z}^k \twoheadrightarrow G$$

by sending $(n_1, \ldots, n_k) \mapsto n_1x_1 + \cdots + n_kx_k$. ($\mathbb{Z}^k$ is the product of k-copies of $\mathbb{Z}$.) Then by the First Isomorphism Theorem we have:

$$G \cong \mathbb{Z}^k / \ker \phi,$$

so that a finitely generated abelian group is a quotient of $\mathbb{Z}^k$ for some k. Conversely, if there exists a surjective map $\mathbb{Z}^k \to G$—or equivalently if G is a quotient of some $\mathbb{Z}^k$—then G will be finitely generated abelian with generators given by the images $\phi(e_i)$ where e_i is the "vector" with 1 in the i-th location and zeroes elsewhere.

Structure Theorem. The *structure theorem for finitely generated abelian groups* then classifies finitely generated abelian groups G as being products of cyclic groups. But we can be more precise about what this product structure looks like, and in fact there are two commonly used versions:

- $G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z}$ for some $r \geq 0$ and prime-powers $p_i^{k_i}$, and
- $G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$ for some $r \geq 0$ and d_i such that $d_i \mid d_{i+1}$ for each i.

To be clear, any G will admit *both* such expressions, and there is a uniqueness statement attached to each. The first expression is called the *primary factor decomposition* of G, and the second is called the *invariant factor decomposition* of G, with $d_1, \ldots, d_\ell$ called the *elementary divisors* of G. Note that the primes showing up in the primary factor decomposition are not assumed to be distinct. The $\mathbb{Z}^r$ is present (meaning $r > 0$) when G is infinite, so $r = 0$ if and only if G is finite.

We will prove this structure theorem (at least the existence part) next time in the case where G is finite. The general version will be derived next quarter as a consequence of what's called the "structure theorem for finitely generated modules over a principal ideal domains" (we will see later what all of these terms mean), of which finitely generated abelian groups are a key example. But here is a hint at how the proof works in the general case: recall that G is finitely generated abelian if and only if $G \cong \mathbb{Z}^k/K$ for some $K \leq \mathbb{Z}^k$; the proof then works by determining the structure of any $K \leq \mathbb{Z}^k$ and then from here the structure of $\mathbb{Z}^k/K$.

Examples. Let us see some examples of the two forms of the structure theorem in action in the case where G has order 72. Consider for instance $\mathbb{Z}/72\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. In this case, $\mathbb{Z}/72\mathbb{Z}$ is the invariant factor form (only one factor here) of this group, and $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ is the primary factor form (8 and 9 are prime powers):

primary	invariant
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/72\mathbb{Z}$.

Next, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ since $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z}$:

primary	invariant
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.

(Note $2, 4, 9$ are all prime powers, and $2 \mid 36$.) As another example, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ using $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ twice, so:

primary	invariant
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

The remaining abelian groups of order 72 are:

primary	invariant
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

Rank and torsion. Let us note two more things. In the decompositions

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z} \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z},$$

the exponent $r \geq 0$ is unique. This number r is called the *rank* of G, and is in a sense analogous to the notion of dimension in linear algebra. Rank zero corresponds to the finite case, so that the $\mathbb{Z}^r$ factor encodes the "infinite" part of G. (This is also called the *free* part of G, for reasons to be made clear later.) Any element contained only in the free part has infinite order, so the elements of finite order are encoded completely by the $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z} \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$ factors. Previously on the homework we referred to the subgroup of G consisting of elements of finite order as the *torsion* subgroup of G, so the point is that the "primary" and "invariant" factors $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z} \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z}$ encode the torsion part of G.

Thus, the structure theorem essentially says that a finitely generated abelian group can be "broken" down into its free and torsion parts, and moreover the torsion part can be written in one of two "nice" ways as a product of finite cyclic groups. We have been harping on this point quite a bit, but will mention once more that this all fits in a general setting in module theory, where much of the reasons for why these decompositions are useful will be made clear. (The answer, essentially, is that they correspond to certain *normal forms* of matrices.)

Lecture 30: Back to Free Groups

Warm-Up. We show that any finite abelian group G is a product of groups of prime-power order. This is actually fairly quick: suppose $|G| = p_1^{k_1} \cdots p_m^{k_m}$ is the prime factorization of the order of G, and let $A_1, \ldots, A_m$ be the Sylow subgroups of G, where $|A_i| = p_i^{k_i}$. Since G is abelian, each A_i is normal in G, and the A_i have pairwise trivial intersections since they have relatively-prime orders. Since $|G| = p_1^{k_1} \cdots p_m^{k_m} = |A_1| \cdots |A_m|$, we thus have $G = A_1 \ldots A_m \cong A_1 \times \cdots \times A_m$ as desired.

Finite abelian groups. We now show that any finite abelian group is a product of cyclic groups, proving the finite case of the finitely generated abelian structure theorem from last time, or at least the existence part of that theorem. (We save the uniqueness for the general theorem next quarter.) By the Warm-Up, we are reduced to the case where $|G| = p^k$ has prime-power order. (If each A_i above is a product of cyclic groups, so is G.) Let $x \in G$ be an element of maximal order. Then $\langle x \rangle$ is nontrivial and normal in G, and $G/\langle x \rangle$ is also finite and abelian. By induction, we may assume that $G/\langle x \rangle$ is a product of cyclic groups:

$$G/\langle x \rangle \cong \langle \overline{y_1} \rangle \times \cdots \times \langle \overline{y_t} \rangle$$

for some $y_1, \ldots, y_t \in G$. Denote the order $\overline{y_i}$ in $G/\langle x \rangle$ by p^{m_i}, which divides the order of y_i in G.

We claim that we can assume y_i has order exactly p^{m_i} in G. To see this, note that since $\overline{y_i}$ has order p^{m_i} in $G/\langle x \rangle$, we have

$$y_i^{p^{m_i}} = x^s \text{ in } G$$

for some $s \in \mathbb{N}$. If p does not divide s, then $|x^s| = |x|$ (the order of x^s is $|x|/gcd(s, |x|)$ and $gcd(s, |x|) = 1$ since $|x|$ is a power of p), so

$$e = (x^s)^{|x|} = (y_i^{p^{m_i}})^{|x|} = y_i^{|x|p^{m_i}},$$

which means that y_i has order larger than $|x|$, contradicting the choice of $x \in G$. Thus p does divide s, so $s = ap^b$ for some $a, b \in \mathbb{N}$. Then

$$y_i^{p^{m_i}} = x^{ap^b} \implies y_i^{p^{m_i}} x^{-ap^b} = (y_i x^{-ap^{b-m_i}})^{p^{m_i}} = e.$$

If $y_i x^{-ap^{b-m_i}}$ had order in G smaller than p^{m_i}, reversing the computation above shows there would be a smaller power of p such that $y_i^{p^n}$ is equal to a power of x, which contradicts the assumption that p^{m_i} is the order of $\overline{y_i}$ in $G/\langle x \rangle$. Thus $y_i x^{-ap^{b-m_i}} \in \langle \overline{y_i} \rangle$ has the same order p^{m_i} in G as $\overline{y_i}$ has in $G/\langle x \rangle$, so by replacing y_i with this element we may assume that y_i has the same order as $\overline{y_i}$.

The subgroups $\langle y_1 \rangle, \ldots, \langle y_t \rangle$ have pairwise trivial intersection since the cosets their generators determine have pairwise trivial intersection (since $\langle \overline{y_1} \rangle \cdots \langle \overline{y_t} \rangle \cong \langle \overline{y_1} \rangle \times \cdots \times \langle \overline{y_t} \rangle$ by the choice of the y_i's), and each $\langle y_i \rangle$ has trivial intersection with $\langle x \rangle$ since $y_i^k \in \langle x \rangle$ first when k is the order of $\overline{y_i}$ in $G/\langle x \rangle$, which is the same as the order of y_i in G meaning that $y_i^k = e$. Thus, putting it all together gives:

$$|G| = |\langle x \rangle||G/\langle x \rangle| = |\langle x \rangle||\langle \overline{y_1} \rangle \times \cdots \times \langle \overline{y_t} \rangle|$$

$$\begin{aligned} &= |\langle x\rangle||\langle\overline{y_1}\rangle|\cdots|\langle\overline{y_t}\rangle| \\ &= |\langle x\rangle||\langle y_1\rangle|\cdots|\langle y_t\rangle|, \end{aligned}$$

which implies that $G = \langle x\rangle\langle y_1\rangle\cdots\langle y_t\rangle \cong \langle x\rangle \times \langle y_1\rangle \times \cdots \times \langle y_t\rangle$, so G is a product of cyclic groups. (Phew! Since $\langle x\rangle$ and each $\langle y_i\rangle$ has prime-power order, this gives the "primary factor decomposition" form of G, but, as we saw in some examples last time, from this it is straightforward to work out the "invariant factor decomposition" form of G.)

Back to finitely generated. So, any finite abelian group is indeed a product of cyclic groups. But, as we saw, the proof is not for the faint of heart, and involves some brute-force computations with quotients and orders. The proof in the general finitely generated case is even tougher, at least until we have some better language to use in which to phrase it. As we saw last time, the proof works by writing G as a quotient $\mathbb{Z}^\ell/K$ of $\mathbb{Z}^\ell$ for some subgroup $K \leq \mathbb{Z}^l$, and then determining the structure of K and of $\mathbb{Z}^\ell/K$. Here is the key fact which makes this work:

> Any subgroup of a finitely generated abelian group is itself finitely generated!

In the case at hand, once we know $K \leq \mathbb{Z}^\ell$ is finitely generated, we can pick generates $d_1, \ldots, d_s \in K$ and then determine the structure of $\mathbb{Z}^\ell/K$ using the First Isomorphism Theorem.

The fact that a subgroup of a finitely generated abelian group is itself finitely generated is highly non-obvious and non-trivial, and indeed is not true in the non-abelian case in general. We will give an example of how this can fail shortly, so the fact that we are working with *abelian* groups here is absolutely crucial. Showing that a subgroup of a finitely generated abelian group is finitely generated comes down to a linear algebraic type of computation, and indeed this fact should be thought of as analogous to the fact in linear algebra that any subspace of a finite-dimensional space is itself finite-dimensional,

Back to free groups. To give an example where a subgroup of a finitely generated group need not be finitely generated, we return to the setting of free groups. Recall that the free group on a set S is the group F_S consisting of "words" of elements in S and their inverses with group operation given by concatenation. The key point is that there are no non-trivial relations among the generators in S. Let $F_2 = \langle x, y\rangle$ be the free group on two generators and let H be the subgroup generated by elements of the form y^nxy^{-n}:

$$H = \langle y^nxy^{-n} \mid n \in \mathbb{Z}\rangle.$$

Then in fact H is *not* finitely generated! To be clear, the generating elements y^nxy^{-n} are infinite in number, and we can show that there are no nontrivial relations among these, so that this particular generating set cannot be cut down to a finite generating set. However, this is still not enough to show that H is not finitely generated, since we would have to also show that *no* finite subset of H—possibly consisting of elements apart form the y^nxy^{-n} alone—can generate H either. This is hard to prove using group theory alone, and amounts to a big, brute-force, and difficult computation.

Here is another seemingly "obvious" looking fact that is also highly non-trivial: any subgroup of a free group is itself free. In this context, to say that a group is *free* just means that it has a generating set whose elements satisfy no non-trivial relations among each other. More precisely, $H \leq F_S$ is free if there exists a set T such that $H \cong F_T$. (You can view the fact that any subgroup of a free is free as an analog of the fact that any vector space has a basis. The "no nontrivial relations" is an analog of linear independence.) Producing the free generating set T for which $H \cong F_T$ is challenging to do in general, and again amounts to a big brute-force computation.

The upshot is that questions dealing with free groups are actually difficult to address directly using group theory alone, so the fact that the analogous questions about free *abelian* groups (such as the fact that any subgroup of a finitely generated one is still finitely generated) are easier to handle really speaks to the benefit of having the abelian assumption. (A *free abelian group* is an abelian group which satisfies a similar notion of "freeness", namely that it has a generating set whose elements satisfy no nontrivial relations, apart from the ones needed to say the group is abelian. The "free abelian group on n generators" for instance is $\mathbb{Z}^n$.) The study of free groups in general requires moving beyond group theory, and we will finish this quarter with a brief introduction to some of the key tools in this area: fundamental groups.

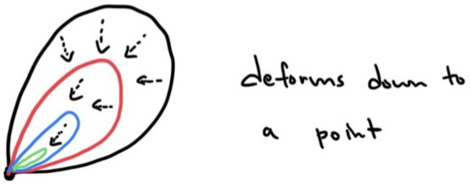
But before moving on, we clarify that free groups are indeed important within group theory itself, if for no other reason that free groups can be used to describe *all* groups. Just as a finitely generated abelian group is a quotient of some $\mathbb{Z}^\ell$, it is true that any group whatsoever is a quotient of a free group! Indeed, let G be a group and let F_G be the free group generated by the elements of G. (To be clear, even if elements of G satisfy some relations within G, they do not satisfy any non-trivial relations in F_G.) The map $F_G \to G$ sending a "word" $g_1 g_2 \dots g_k$ to its actual value in G as a product computed using the multiplication of G is a surjective homomorphism, so the First Isomorphism Theorem gives:

$$G \cong F_G/K, \text{ where } K \text{ is the kernel of } F_G \to G.$$

(As a consequence, this shows that any group has a presentation: elements of G give the generators, and elements of the kernel K the relations.) Thus, if we knew everything there was to know about free groups (including K, which, as a subgroup of a free group, is free itself), we would everything there was to know about all groups. Of course, knowing everything there is to know about free groups is an intractable problem, but this at least highlights the role which free groups play in group theory in general.

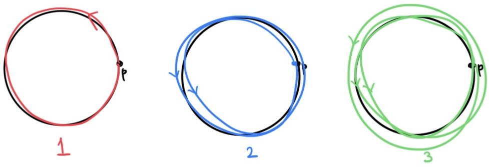
Fundamental groups. As mentioned above, fundamental groups are examples of groups which on the one hand show up the study of free groups, but in fact are used much more broadly in geometry and topology. They belong to the subject of *algebraic topology*, which deals with the use of algebraic constructions (groups, rings, and modules—the latter two of which we will see next quarter) to study geometric and topological spaces. The fundamental group is introduced in the second quarter of the undergraduate topology course MATH 344-2, but here is a quick overview.

Given some space X (we will not clarify what we mean by "space" here, and just naively think of a space as being some type of geometric object like a plane, sphere, or whatever), we can construct a group out of the *loops* in X, which are paths which begin and end at the same point. We make the declaration that two loops are thought of as being the "same" if one can be deformed into the other. (We will not define what we mean by "deform" more formally, and again rely on pure intuition. What we are really doing is defining an equivalence relation on the set of loops, and considering its equivalence classes.) For instance, every loop in the plane $\mathbb{R}^2$ can be deformed to a point, which we think of as being a constant loop:



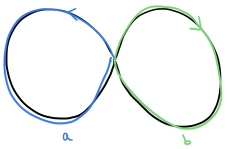
Fix $x_0 \in X$, and set $\pi_1(X, x_0)$ to be the set of (equivalence classes of) loops in this sense. Together with the operation of "concatenation of paths", where in a product $\gamma_1\gamma_2$ we follow one loop and then the other, $\pi_1(X, x_0)$ becomes a group called the *fundamental group* of X based at x_0. The identity element is the constant loop at x_0, and the inverse of γ is visually the same loop but traversed in the opposite direction. (So, all loops we consider are oriented with a particular direction. Showing that going around γ one way followed by the other way does produce the identity requires the formal definition of what "deform" means. Also, for nice enough spaces the basepoint x_0 can essentially be ignored since different choices give rise to isomorphic fundamental groups.)

Here are some examples. First, since all loops in $\mathbb{R}^2$ (no matter the point x_0 we take) can be deformed to the constant loop, we find that $\pi_1(\mathbb{R}^2, x_0) = 1$ is trivial. Next consider a circle S^1 (standard notation for the unit circle in $\mathbb{R}^2$):



The loop which goes around the circle once cannot be deformed to the constant loop, so this fundamental group $\pi_1(S^1, p)$ is definitely non-trivial. It turns out that looping around the circle twice, or three times, four times, etc produces all distinct elements in the fundamental group, so that $\pi_1(S^1, p)$ is in fact isomorphic to $\mathbb{Z}$! The integer which corresponds to a loop under this isomorphism keeps track of how many times it wraps around the circle, with negative integers corresponding to wrapping around in the opposite direction. It is true that all other loops can be deformed into one of these, so that we get exactly $\mathbb{Z}$ as the fundamental group.

Finally, consider a figure eight:



As in the case of the circle, it turns out that the only thing which matters in the fundamental group is how many times a loop wraps around each "leaf" of the figure eight. If we take a be the loop which arounds the left leaf once and b the loop which wraps around the right leaf once, then any element in the fundamental group looks like a word *aabbbaababababbbababbab*, so that the fundamental group of the figure eight is the free group $\langle a, b\rangle$ on two generators! (Note that order matters: wrapping around the left leaf and then the right is different than wrapping around the right and the left, so $ab \neq ba$.) In general, if we "glue" n circles together at a single point, the fundamental group of the resulting space will be the free group on n generators.

Geometric group theory. And thus we see free groups enter the realm of fundamental groups and geometry/topology. This then leads to the fact that questions about free groups can be recast as questions about certain spaces, such as ones obtained by gluing circles together. Subgroups of fundamental groups correspond to what are called "covering spaces" of a space, so the claims that any subgroup of a free groups is free, or that the subgroup $\langle y^nxy^{-n} \mid n \in \mathbb{Z}\rangle$ of $F_2 = \langle x, y\rangle$ is not finitely generated, can be rephrased as questions about covering spaces instead. This allows for the use of geometry/topology to study group theory, where there are new tools available and make old, seemingly difficult problems much easier to handle. This is the topic of the subject known as *geometric group theory*, and it is here that we will conclude our quarter. Thanks for reading!