MATH 417 –SIXTH WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

September 28, 2020, in advance

We're going to continue with two of the main ideas from last week. Suppose $K \leq G$ is a subgroup, then K is a normal subgroup ($K \trianglelefteq G$) if $aK = Ka$ for every $a \in G$. By this, we mean that the sets are equal.

We've also proved that the cosets of a normal subgroup have a remarkable property: $aK * bK = (a * b)K$. This means that we can take the operation for the group and apply it to the cosets, and it makes sense. A typical element in aK is $a * k_1$ for some $k_1 \in K$ and a typical element in bK is $b * k_2$ for some $k_2 \in K$. (Just to be clear here: it might be the case that $k_1 = k_2$, but they don't have to be equal.) A typical element in $aK * bK$ is then $(a * k_1) * (b * k_2)$, and we proved that this can be re-written as $(a * b) * k_0$ for some $k_0 \in K$, and so this element is also in $(a * b)K$. The crucial part of the argument here is that $aK = Ka$, so $x * k_1 \in aK = Ka$ implies that $x * k_1 = k_2 * x$ for some $k_2 \in K$ and $k_3 * y \in Ka = aK$ implies that $k_3 * y = y * k_4$ for some $k_4 \in K$ We'll need this later today.

Every subgroup of an abelian group is a normal subgroup, because the operation is commutative. Also, if $[G : K] = 2$, then $K \trianglelefteq G$. Thus, even though S_3 is not abelian, the subgroup $\{\rho_0, \rho_1, \rho_2\}$ is a normal subgroup, because it has $|S_3|/2 = 6/2 = 3$ elements.

The other big idea from last week was the homomorphism. Suppose G and H are groups. Then ϕ is a homomorphism, if it is a map from $G \to H$ with the property that for $g, g; \in G$,

$$\phi(g *_G g') = \phi(g) *_H \phi(g').$$

Associated to each homomorphism are two important sets which we proved were groups, the kernel and the image

$$Ker(\phi) = \{g \in G \mid \phi(g) = e_H\} \subseteq G, \quad Im(\phi) = \{\phi(g) \mid g \in G\} \subseteq H.$$

As we have seen, an isomorphism is a homomorphism from $G \to H$ with the additional conditions that $Ker(\phi) = \{e_G\}$ and $Im(\phi) = H$.

The fact combining these two ideas is that for any homomorphism ϕ from $G \to H$ the kernel is a normal subgroup: $K = Ker(\phi) \trianglelefteq G$. The cosets of K have two descriptions: as a coset, and as the preimage of

an element from $Im(\phi)$:

$$aK = \{g \in G \mid \phi(g) = \phi(a)\}$$

One goal today is to prove the converse: that if $K \trianglelefteq G$, then there is a "natural" way to find a group H and a homomorphism ϕ from $G \to H$ such that $Ker(\phi) = K$.

As a simple example, suppose the group G is given and $K = \{e_G\}$. Then we could take $H = G$ and define $\phi(g) = g$ for $g \in G$. Then

$$Ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$$

by the definition above, but $\phi(g) = g$ and $H = G$, so

$$Ker(\phi) = \{g \in G \mid g = e_G\} = \{e_G\}.$$

Time for new material. We need to return to normal subgroups. Suppose $K \trianglelefteq G$. Consider the set of cosets $\{aK\}$. The name of this set is G/K. It is usually called a *quotient* group or a *factor* group.

We have already seen this in one case. Look at the group $G = \mathbb{Z}$, and the normal subgroup $K = n\mathbb{Z}$. (It's normal because G is abelian.) We have already seen the cosets of K in G: these are $\{[a]_n\}$, and I've been calling this $\mathbb{Z}/n\mathbb{Z}$ all semester. Now you know why!

Define an operation $*_H$ on $H = G/K$ by

$$aK *_H bK = (a *_G b)K.$$

(Yes, I know it's confusing, because it's basically the same operation on both sides, but it is on different objects.)

THEOREM Under these circumstances, $(G/K, *_{G/K})$ is a group

PROOF The first thing I need to show is that the operation is well-defined. What do I mean here? Suppose $aK = a'K$ and $bK = b'K$; that is, the cosets are defined differently but are the same sets. Then I want to prove that

$$aK *_{G/K} bK = a'K *_{G/K} b'K$$

That is, $(a *_G b)K = (a' *_G b')K$ as cosets. Since these are both cosets and $a' *_G b' \in (a' *_G b')K$ ($e_G \in K$), if $a' *_G b' \in (a *_G b)K$, then the two cosets have an element in common and so are equal.

This isn't so hard. We've already seen that $xK = yK$ if and only if $y = x *_G k$ for some $k \in K$. So $a' = a *_G k_1$ and $b' = b *_G k_2$ for some $k_1, k_2 \in K$. Thus

$$a' *_G b' = (a *_G k_1) *_G (b *_G k_2) = a *_G (k_1 *_G b) *_G k_2 =$$
$$a *_G (b *_G k_3) *_G k_2 = (a *_G b) *_G (k_3 *_G k_2)$$

Since $k_3 *_G k_2 \in K$, this shows that $a' *_G b' \in (a *_G b)K$.

We have a set and an operation. What's left? Identity, inverses and associativity. These are much easier!

Recall that $K = e_G K \in G/K$, so for every $aK \in G/K$,

$$(e_G K) *_{G/K} aK = (e_G *_G a)K = aK, aK *_{G/K} e_G K = (a *_G e_G)K = aK,$$

so K is the identity. We now have

$$(a^{-1}K) *_{G/K} aK = (a^{-1} * a)K = e_G K = K,$$

so the inverse of the coset aK is the coset $a^{-1}K$. Finally, and I'm not looking forward to this, for any three cosets aK, bK, cK,

$$(aK *_{G/K} bK) *_{G/K} cK = (a *_G b)K *_{G/K} cK = ((a *_G b) *_G c)K$$
$$aK *_{G/K} (bK *_{G/K} cK) = aK *_{G/K} (b *_G c)K = (a *_G (b *_G c))K.$$

Since G is a group, it is associative, so $(a *_G b) *_G c = a *_G (b *_G c)$, and so we have associativity here. □

We've already seen some examples. I'd like to write out a case I started to talk about last week. Let $G = S_3$ and let $K = \langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$, which is a cyclic subgroup of order 3. In this case, the group G/K consists of the two cosets of K

$$K = \{\rho_0, \rho_1, \rho_2\},\ \mu_1 K = \{\mu_1, \mu_2, \mu_3\}.$$

And taking the operation of multiplication as defined, here is the multiplication table of G/K, which is evidently isomorphic to C_2

G/K	$\{\rho_0, \rho_1, \rho_2\}$	$\{\mu_1, \mu_2, \mu_3\}$
$\{\rho_0, \rho_1, \rho_2\}$	$\{\rho_0, \rho_1, \rho_2\}$	$\{\mu_1, \mu_2, \mu_3\}$
$\{\mu_1, \mu_2, \mu_3\}$	$\{\mu_1, \mu_2, \mu_3\}$	$\{\rho_0, \rho_1, \rho_2\}$

A natural question suggested by the notation is that maybe, if we know K and G/K, we can "recover" G. It is true that $|G/K| = |G|/|K|$. Thus, if we take the product of the two groups $K \times G/K$, we get a group that has $|G|$ elements. However, there is no guarantee that it is isomorphic to G. In this case K is isomorphic to C_3 and S_3/K is isomorphic to C_2 and so $K \times S_3/K$ is isomorphic to $C_3 \times C_2$. Since $gcd(2, 3) = 1$, it follows that $C_3 \times C_2$ is isomorphic to $C_{2\cdot 3} = C_6$. Thus, in this example $K \times S_3/K$ is isomorphic to C_6 and is not isomorphic to S_3.

Let's throw homomorphisms back into the mix. Suppose $K \trianglelefteq G$ is a normal subgroup of G. Define the homomorphism ϕ_K from $G \to G/K$ by $\phi_K(g) = gK$. Let's check that it's a homomorphism. It takes an element of G and maps it to an element of G/K. What about the product?

$$\phi_K(g_1 *_G g_2) = (g_1 *_G g_2)K = g_1 K *_{G/K} g_2 K = \phi_K(g_1) *_{G/K} \phi_K(g_2).$$

So all is fine.

What is the kernel of ϕ_K? We have, from the definition, and the fact that $e_{G/K} = K$, that $Ker(\phi_K)$ is

$$\{g \in G \mid \phi_K(g) = e_{G/K} = K\} = \{g \in G \mid gK = K\} = K$$

Thus, ϕ_K is a homomorphism whose kernel is K, as promised.

What is the image of ϕ_K?

$$Im(\phi_K) = \{gK \mid g \in G\} = G/K$$

One final twist, which is the sort of thing you might see in graduate mathematics. Suppose we started with a homomorphism ϕ from $G \to H$ and $K = \ker(\phi)$.

A subtle but important point: ϕ and ϕ_K are not the same homomorphism! We have ϕ mapping $G \to H$ and ϕ_K mapping $G \to G/K$, so the images are different. But there is a natural connection. Remember that K is defined by ϕ and we know that $aK = \{g \in G \mid \phi(g) = \phi(a)\}$. So let us define a map $\alpha : G/K \to H$ in the only way we could: $\alpha(aK) = \phi(a) \in Im(\phi) \subseteq H$, which we know is well-defined.

THEOREM With the above definitions, α is an isomorphism from G/K to $Im(\phi)$ and $\phi(g) = \alpha(\phi_K(g))$.

PROOF Let's first do the formula. We have $\alpha(\phi_K(g)) = \alpha(gK) = \phi(g)$. OK, that's good. Now we have to prove that α is an isomorphism. Is it one-to-one?

$$\alpha(aK) = \alpha(bK) \iff \phi(a) = \phi(b) \iff aK = bK.$$

Is it onto? If $h \in Im(\phi)$, then there exists $g \in G$ so that $\phi(g) = h$, and so $\alpha(gK) = h$, so yes, α is onto.

Thus α is a bijection. Finally, we have to check the operation, and use the definitions and the fact that

$$\alpha(aK *_{G/K} bK) = \alpha((a * Gb)K) = \phi(a * Gb) =$$
$$\phi(a) *_H \phi(b) = \alpha(aK) *_H \alpha(bK).$$

We've checked everything, so α is an isomorphism. □

This is called the "Fundamental Homomorphism Theorem"

Let me work it out in another somewhat familiar case. Suppose $G = C_6 = \langle a \rangle, a^6 = e_G$ and $H = C_4 = \langle b \rangle, b^4 = e_H$ and define ϕ by $\phi(a) = b^2$. What we found was that

$$\phi(e) = \phi(a^2) = \phi(a^4) = e_h, \quad \phi(a) = \phi(a^3) = \phi(a^5) = b^2$$

Thus, $K = Ker(\phi) = \{e_G, a^2, a^4\}$ and $Im(\phi) = \{e_H, b^2\}$. So G/K consists of the two cosets $\{K, aK\}$:

$$K = \{e_G, a^2, a^4\}, \quad aK = \{a, a^3, a^5\}$$

Thus, G/K is a cyclic group of order 2, as is $Im(\phi) \subset H$. Here is a picture of the Fundamental Homomorphism Theorem, as it applies to the elements of G, with $g \mapsto \phi_K(g) \mapsto \alpha(\phi_K(g))$:

$$e_G \mapsto K \mapsto e_H,$$
$$a \mapsto aK \mapsto b^2,$$
$$a^2 \mapsto K \mapsto e_H,$$
$$a^3 \mapsto aK \mapsto b^2,$$
$$a^4 \mapsto K \mapsto e_H,$$
$$a^5 \mapsto aK \mapsto b^2.$$

There is one more topic in Section 13 that I wanted to mention: a family of isomorphisms for any group, which is interesting only when the group is *not* abelian.

Given a group G and a fixed element $g \in G$. We define i_g or *conjugation by* g to be the map defined by

$$i_g(x) = gxg^{-1}.$$

(This is the book's notation, so I should keep it; I'm working with only one group here, so it's ok to use the juxtaposition ab for the operation $a *_G b$.)

THEOREM For a group G and $g \in G$, i_g is an automorphism of G.

PROOF We have to prove that $i_g : G \to G$ is one-to-one, onto and a homomorphism. First,

$$i_g(x) = i_g(y) \iff gxg^{-1} = gyg^{-1} \iff x = y.$$

The last $\iff$ comes from left cancellation and then right cancellation. Thus, i_g is one-to-one. It is also easy to check that

$$i_g(g^{-1}xg)) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = x.$$

so i_g is onto. Finally,

$$i_g(xy) = g(xy)g^{-1} = (gx)(g^{-1}g)(yg^{-1}) =$$
$$(gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y),$$

so it's a homomorphism as well. □

Any automorphism which can be defined as a conjugation by g is called an *inner automorphism*.

One limitation with this is that if G is an abelian group, then

$$i_g(x) = gxg^{-1} = xgg^{-1} = xe_G = x,$$

so i_g is the identity.

What happens with our favorite non-abelian group S_3? Here's a start. What is i_{ρ_0}? Well, ρ_0 is the identity, so $\rho_0 x \rho_0^{-1} = x$. This is just the identity.

I'll stop today after looking at i_{ρ_1}, noting that $\rho_1^{-1} = \rho_2$

$$\begin{aligned} i_{\rho_1}(\rho_0) &= \rho_1\rho_0\rho_2 = \rho_0, \\ i_{\rho_1}(\rho_1) &= \rho_1\rho_1\rho_2 = \rho_1, \\ i_{\rho_1}(\rho_2) &= \rho_1\rho_2\rho_2 = \rho_2, \\ i_{\rho_1}(\mu_1) &= \rho_1\mu_1\rho_2 = \rho_1\mu_3 = \mu_2, \\ i_{\rho_1}(\mu_2) &= \rho_1\mu_2\rho_2 = \rho_1\mu_1 = \mu_3, \\ i_{\rho_1}(\mu_3) &= \rho_1\mu_3\rho_2 = \rho_1\mu_2 = \mu_1 \end{aligned}$$

So what happens here is this: ρ_0, ρ_1, ρ_2 don't change under i_{ρ_1}, but the flips are cycled: $\mu_1 \mapsto \mu_2 \mapsto \mu_3 \mapsto \mu 1$.

Can this be explained? Let me put the pictures of the rotations of S_3 back up:

$$\rho_0 = \begin{matrix} 1 & 2 \\ & 3 \end{matrix}, \quad \rho_1 = \begin{matrix} 3 & 1 \\ & 2 \end{matrix}, \quad \rho_2 = \begin{matrix} 2 & 3 \\ & 1 \end{matrix};$$

$$\mu_1 = \begin{matrix} 1 & 3 \\ & 2 \end{matrix}, \quad \mu_2 = \begin{matrix} 3 & 2 \\ & 1 \end{matrix}, \quad \mu_3 = \begin{matrix} 2 & 1 \\ & 3 \end{matrix}.$$

Suppose that, rather than acting on the permutations, I acted on the *set*, and I renamed 1 as 2, renamed 2 as 3 and renamed 3 as 1. Call the action F, with the understanding that $F(\rho_0)$ represents the new names.

$$F(\rho_0) = \begin{matrix} 2 & 3 \\ & 1 \end{matrix}, \quad F(\rho_1) = \begin{matrix} 1 & 2 \\ & 3 \end{matrix}, \quad F(\rho_2) = \begin{matrix} 3 & 1 \\ & 2 \end{matrix};$$

$$F(\mu_1) = \begin{matrix} 2 & 1 \\ & 3 \end{matrix}, \quad F(\mu_2) = \begin{matrix} 1 & 3 \\ & 2 \end{matrix}, \quad F(\mu_3) = \begin{matrix} 3 & 2 \\ & 1 \end{matrix}.$$

So what does $F(\rho_1)$ so? What used to be in the 1 position is now in the 2 position, what used to be in the 2 position is now in the 3 position and what used to be in the 3 position is now in the 1 position, so as a permutation, $F(\rho_1) = \rho_1$. Similarly, $F(\rho_2) = \rho_2$.

What about $F(\mu_1)$. What used to be in the 1 position is now in the 3 position, what used to be in the 2 position is now in the 2 position and what used to be in the 3 position is now in the 1 position, so as a permutation, $F(\mu_1) = \mu_2$.

If you go through everything, you'll discover that $F(x) = i_{\rho_1}(x)$. There are $3! = 6$ ways to permute the labels, and each one corresponds to one of these inner automorphisms.

September 28, 2020, in class

I got some very good questions after Sunday night's talk, and I'd like to give you all the answers I gave your classmates when they wrote. If you have follow-ups, it's hard for me to see you all on screen-share, so put it into the Chat.

First: what's going on with "well-defined"? What are we checking?

What we're doing is that sometimes on a map f from G to H, the same object in G might have different names. (This applies whether G is a group or another kind of object.) For example $[1]_6 = [7]_6$, or you could have $aK = bK$ for a subgroup K. What mathematicians mean by a "well-defined" map f is that, however you name the object, the image under f is the same.

Second: When we talk about a homomorphism becoming an isomorphism and that $Ker(\phi) = \{eH\}$ and $Im(\phi) = H$, does $Ker(\phi) = \{eH\}$ tell us that the relationship is injective and $Im(\phi) = H$ tell us that the map is surjective?

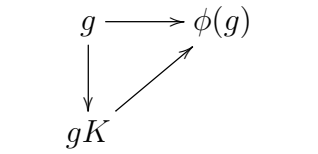
Exactly!

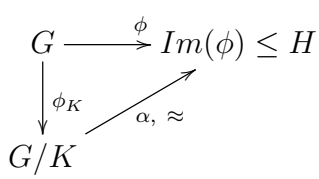
Third: Why did we look at $6/3 = 2$ or $6/2 = 3$ in the context of cosets and S_3?

There are three parameters: the order of a group, the order of a subgroup, and the number of cosets, and these are related by the equation $|G| = |H| \cdot [G : H]$, so if you know two of them, you know the third.

Fourth: Could you also go over exactly was the Fundamental Homomorphism Theorem is?

There are two things about it. One is that any homomorphism ϕ from $G \to H$ can be split up into a composition of two maps. The other is that one of the maps is an isomorphism. I put some diagrams on the next frame.





If you've ever seen diagrams like these in a classroom when you walk in, that's all they mean. Lots of mathematicians use diagrams like these in their research. I don't, and I had to google how to write them in LaTeX.

The other question had to do with automorphisms and inner automorphisms, and that fit in well with the material I had already planned to present.

Recall that an automorphism Φ of G is an isomorphism of G to itself and this means that it is a homomorphism of $G \to G$ which is injective and surjective. An automorphism can be thought of as an "internal symmetry" of a group.

One trivial automorphism of any group G is the identity map: $\Phi(g) = g$, but since any group has it, it's not very illuminating. Here's another example

THEOREM If G is an abelian group, then $\Phi(g) = g^{-1}$ is an automorphism.

PROOF. It's easily shown to be injective and surjective (check if you don't see these!) and $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \phi(g)\phi(h)$, where the key step in the middle comes from the assumption that G is abelian. $\square$.

For example, if $G = \mathbb{Z}/n\mathbb{Z}$, then $\phi([a]_n) = [-a]_n = [n-a]_n$ is an automorphism.

As noted yesterday, a general class of automorphisms comes from conjugation. If G is any group and $g \in G$ is fixed, define a map $i_g : G \to G$ by

$$i_g(x) = gxg^{-1}.$$

We saw that it is an isomorphism, but it isn't interesting for an abelian group, because then $i_g(x) = x$ for every x and i_g is the identity map.

An automorphism that is defined in this way is called an "inner" automorphism; every other automorphism is an "outer" automorphism. So the map $x \to x^{-1}$ in an abelian group is an outer automorphism.

What happens with our favorite non-abelian group S_3? Here's a start. What is i_{ρ_0}? Well, ρ_0 is the identity, so $\rho_0 x \rho_0^{-1} = x$. This is just the identity.

Here is i_{ρ_1}, noting that $\rho_1^{-1} = \rho_2$

$$\begin{aligned} i_{\rho_1}(\rho_0) &= \rho_1\rho_0\rho_2 = \rho_0, \\ i_{\rho_1}(\rho_1) &= \rho_1\rho_1\rho_2 = \rho_1, \\ i_{\rho_1}(\rho_2) &= \rho_1\rho_2\rho_2 = \rho_2, \\ i_{\rho_1}(\mu_1) &= \rho_1\mu_1\rho_2 = \rho_1\mu_3 = \mu_2, \\ i_{\rho_1}(\mu_2) &= \rho_1\mu_2\rho_2 = \rho_1\mu_1 = \mu_3, \\ i_{\rho_1}(\mu_3) &= \rho_1\mu_3\rho_2 = \rho_1\mu_2 = \mu_1 \end{aligned}$$

So what happens here is this: ρ_0, ρ_1, ρ_2 don't change under i_{ρ_1}, but the flips are cycled: $\mu_1 \mapsto \mu_2 \mapsto \mu_3 \mapsto \mu_1$.

Can this be explained? Let me put the pictures of the rotations of S_3 back up:

$\rho_0 =$ 1 2 / 3 , $\rho_1 =$ 3 1 / 2 , $\rho_2 =$ 2 3 / 1 ;

$\mu_1 =$ 1 3 / 2 , $\mu_2 =$ 3 2 / 1 , $\mu_3 =$ 2 1 / 3 .

Suppose that, rather than acting on the permutations, I acted on the *labels*, and renamed 1 as 2, renamed 2 as 3 and renamed 3 as 1. Call the action F, with the understanding that $F(\rho_0)$ represents the new names.

That should be an automorphism; it's some kind of symmetry on the group S_3.

$F(\rho_0) =$ 2 3 / 1 , $F(\rho_1) =$ 1 2 / 3 , $F(\rho_2) =$ 3 1 / 2 ;

$F(\mu_1) =$ 2 1 / 3 , $F(\mu_2) =$ 1 3 / 2 , $F(\mu_3) =$ 3 2 / 1 .

So what does $F(\rho_1)$ do? What used to be in the 1 position is now in the 2 position, what used to be in the 2 position is now in the 3 position and what used to be in the 3 position is now in the 1 position, so as a permutation, $F(\rho_1) = \rho_1$. Similarly, $F(\rho_2) = \rho_2$.

What about $F(\mu_1)$? What was in the 1 position is now in the 3 position, what was in the 2 position is now in the 2 position and what was in the 3 position is now in the 1 position, so $F(\mu_1) = \mu_2$. Similarly, $F(\mu_2) = \mu_3$ and $F(\mu_3) = \mu_1$.

If you go through everything, you'll discover that $F(x) = i_{\rho_1}(x)$.

And notice that ρ_1 takes $1 \to 2 \to 3 \to 1$ too.

WORKSHEET PROBLEM

1. For the group $G = S_3$, compute the conjugation by μ_1. That is, compute

$$i_{\mu_1}(x) = \mu_1 x \mu_1^{-1} = \mu_1 x \mu_1, \quad \text{for } x \in S_3.$$

Give an "interpretation" for this automorphism in terms of labels.

I'll leave the multiplication table up for your convenience, and you can do your work before you go to the breakout rooms, and then talk about it there.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

WORKSHEET SOLUTION

Here's what I get:

$$\begin{aligned}
i_{\mu_1}(\rho_0) &= \mu_1\rho_0\mu_1 = \mu_1\mu_1 = \rho_0,\\
i_{\mu_1}(\rho_1) &= \mu_1\rho_1\mu_1 = \mu_1\mu_3 = \rho_2,\\
i_{\mu_1}(\rho_2) &= \mu_1\rho_2\mu_1 = \mu_1\mu_2 = \rho_1,\\
i_{\mu_1}(\mu_1) &= \mu_1\mu_1\mu_1 = \mu_1\rho_0 = \mu_1,\\
i_{\mu_1}(\mu_2) &= \mu_1\mu_2\mu_1 = \mu_1\rho_2 = \mu_3,\\
i_{\mu_1}(\mu_3) &= \mu_1\mu_3\mu_1 = \mu_1\rho_1 = \mu_2
\end{aligned}$$

The interpretation is that the label 1 is fixed and the labels 2 and 3 are reversed. Hmm. That's what μ_1 does as well.

THEOREM Suppose $\alpha, \beta \in S_n$, then $i_\beta(\alpha) \in S_n$ is the permutation which takes $\beta(j)$ to $\beta(\alpha(j))$.

PROOF Let's just write it out: $i_\beta(\alpha) = \beta\alpha\beta^{-1}$, so

$$i_\beta(\alpha)(\beta(j)) = \beta(\alpha(\beta^{-1}(\beta(j)))) = \beta(\alpha(j))$$

For example, let $n = 4$ and think of elements in D_4. Let $\alpha = \rho_1 = (1234)$ and $\beta = \mu_1 = (12)(34)$. Then

$$\begin{gathered}
\pi := i_{\mu_1}(\rho_1) = \mu_1\rho_1\mu_1^{-1} = (12)(34)(1234)(12)(34) :\\
1 \to 2 \to 3 \to 4, \quad 2 \to 1 \to 2 \to 1,\\
3 \to 4 \to 1 \to 2, \quad 4 \to 3 \to 4 \to 3\\
= (1432).
\end{gathered}$$

So $\pi(\beta(j)) = \beta(\alpha(j))$ Can we check this? I'll do it for $j = 1, 2$:

$$\alpha(1) = 2,\ \beta(2) = 1, \quad \beta(1) = 2,\ \pi(2) = 1,$$
$$\alpha(2) = 3,\ \beta(3) = 4, \quad \beta(2) = 1,\ \pi(1) = 4.$$

September 30, 2020, in advance

Today a few more comments about automorphisms and then another nice group.

Recall that if G is a group, then an automorphism Φ is a bijection from G to itself that preserves the operation: for $g, h \in G$,

$$\Phi(gh) = \Phi(g)\Phi(h)$$

I talked about the automorphisms of V, and now I'd like to be precise. We have $V = \{I, X, Y, Z\}$, where I is the identity and $X^2 = Y^2 = Z^2 = I$ and $XY = YX = Z$, $XZ = ZX = Y$ and $YZ = ZY = X$.

If Φ is an automorphism, then it has to take the identity to the identity, so $\Phi(I) = I$. Suppose π is any permutation of $\{X, Y, Z\}$; that is, $\{\pi(X), \pi(Y), \pi(Z)\} = \{X, Y, Z\}$, then the map defined by

$$\Phi(I) = I, \quad \Phi(X) = \pi(X), \quad \Phi(Y) = \pi(Y), \quad \Phi(Z) = \pi(Z)$$

is an automorphism.

From its definition, Φ is a bijection of $\{I, X, Y, Z\}$ to itself. Now we have to check the operation: $\Phi(uv) = \Phi(u)\Phi(v)$ for all choices of $u, v \in V$.

Since $\Phi(I) = I$, this is automatic when one of u, v equals I. Otherwise, suppose $u = v \in \{X, Y, Z\}$. Then

$$\Phi(u^2) = \Phi(I) = I; \quad \Phi(u)\Phi(u) = (\pi(u))^2 \in \{X^2, Y^2, Z^2\} = \{I\},$$

so $\Phi(u^2) = (\Phi(u))^2$ as we wanted. Finally, suppose $u \neq v$, $u, v \in \{X, Y, Z\}$. If we write w as the third element, so that $\{u, v, w\} = \{X, Y, Z\}$, then $w = uv$, and we need to show that

$$\pi(w) = \Phi(w) = \Phi(uv) = \Phi(u)\Phi(v) = \pi(u)\pi(v).$$

But $\{\pi(X), \pi(Y), \pi(Z)\} = \{X, Y, Z\}$, so no matter which π we choose, this equation will be correct.

Now I would like to talk generally about automorphisms. Fix a group G.

LEMMA If Φ is an automorphism of G, then so is Φ^{-1}.

PROOF Since $\Phi : G \to G$, its inverse is defined: $\Phi^{-1} : G \to G$. We need to check the operation. This is just "symbol-pushing". We need to show that, for every $g_1, g_2 \in G$,

$$\Phi^{-1}(g_1 g_2) = \Phi^{-1}(g_1)\Phi^{-1}(g_2).$$

To prove this, write $h_1 = \Phi^{-1}(g_1)$ and $h_2 = \Phi^{-1}(g_2)$ (we can do this because Φ is surjective.) Then what we need to prove is that

$$\Phi^{-1}(\Phi(h_1)\Phi(h_2)) = \Phi^{-1}(\Phi(h_1))\Phi^{-1}(\Phi(h_2)) = h_1 h_2.$$

But Φ is an automorphism, so $\Phi(h_1)\Phi(h_2) = \Phi(h_1 h_2)$, and this becomes

$$\Phi^{-1}(\Phi(h_1 h_2)) = h_1 h_2,$$

which is true by definition. $\square$.

Suppose now that Φ_1 and Φ_2 are two automorphisms of G. Then we can compose them. For $g \in G$, let

$$\Phi(g) = \Phi_1(\Phi_2(g))$$

THEOREM The composition map Φ is also an automorphism of G.

PROOF Since Φ_1 and Φ_2 are bijections, their composition is also a bijection. Here's a quick proof. First, injection

$$\Phi(g) = \Phi(h) \iff \Phi_1(\Phi_2(g)) = \Phi_1(\Phi_2(h))$$
$$\iff \Phi_2(g) = \Phi_2(h) \iff g = h.$$

(This uses the facts that Φ_1 and Φ_2 are both injective.)

For surjectivity, suppose $g_0 \in G$. Then by the surjectivity of Φ_1 and Φ_2, there exists $g_1 \in G$ so that $\Phi_1(g_1) = g_0$ and there exists $g_2 \in G$ so that $\Phi_2(g_2) = g_1$, hence

$$\Phi(g_2) = \Phi_1(\Phi_2(g_2)) = \Phi_1(g_1) = g_0.$$

That is, Φ is surjective and so it's a bijection.

The other part is showing that Φ is a homomorphism, but we just proved last week that the composition of two homomorphisms is a homomorphism last week, except that we had one from G to H and another one from H to K. Apply that result, but assume $K = H = G$. $\square$

The set of automorphisms of a group G is denoted $Aut(G)$, and called the *automorphism group* of G.

THEOREM Under the operation of composition:

$$(\Phi_1 * \Phi_2)(g) := \Phi_1(\Phi_2(g)) \quad \text{for } g \in G,$$

$Aut(G)$ is a group.

PROOF We have just shown that if $\Phi_1, \Phi_2 \in Aut(G)$ implies that $\Phi_1 * \Phi_2 \in Aut(G)$, so $*$ is a binary operation.

The identity map $\Phi_0(g) = g$ is the trivial automorphism, and so is in $Aut(G)$. It also has the pleasant composition property that $\Phi * \Phi_0 = \Phi_0 * \Phi = \Phi$ for $\Phi \in Aut(G)$, so it is the identity element.

By the lemma, $\Phi \in Aut(G)$, then $\Phi^{-1} \in Aut(G)$ and by the definition of the operation,

$$(\Phi * \Phi^{-1})(g) = \Phi(\Phi^{-1}(g)) = g = \Phi_0(g),$$

so the functional inverse is the inverse in $Aut(G)$.

Finally, we need to check associativity. As usual, for any $\Phi_j \in Aut(G)$ and $g \in G$,

$$((\Phi_1 * \Phi_2) * \Phi_3)(g) = (\Phi_1 * \Phi_2)(\Phi_3(g)) = \Phi_1(\Phi_2(\Phi_3(g)))$$
$$(\Phi_1 * (\Phi_2 * \Phi_3))(g) = \Phi_1(\Phi_2(\Phi_3(g))) = ((\Phi_1 * \Phi_2) * \Phi_3)(g).$$

Thus, Aut(G) is a group. □

We can combine a lot of what we've done this semester into one theorem.

THEOREM Let $G = C_n$. Then $Aut(G)$ is isomorphic to $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$, so

$$|Aut(C_n)| = \phi(n),$$

where ϕ is the Euler phi-function.

PROOF Write $G = \langle a \rangle, a^n = e$. If $\Phi \in Aut(G)$, then $\Phi(e) = e$. Since $\Phi(a) \in G$, we have $\Phi(a) = a^k$ for some $k \in \{0, \ldots, n-1\}$. We know that for every k, Φ is a homomorphism defined by

$$\Phi_k(a^r) = a^{kr}$$

(Take our result about homomorphisms from C_n to C_m with $m = n$; we need k to be divisible by $n/gcd(n,n) = n/n = 1$, which is no condition at all.)

What we need to check is whether Φ_k is a bijection. If Φ_k is a bijection, then there exists $g = a^s \in C_n$ so that $a = \Phi_k(a^s) = a^{ks}$. This implies that $ks \equiv 1 \mod n$, which implies that $gcd(k,n) = 1$, and s is just the inverse of k mod n. And if $gcd(k,n) = 1$, such an s exists.

So far, we've shown that there is $g \in C_n$ so that $\Phi_k(g) = a$ if and only if $gcd(k,n) = 1$. But if $\Phi_k(g) = a$, then $\Phi_k(g^i) = \Phi_k(a^{si}) = a^i$. To expand that out a bit:

$$\Phi_k(a^{si}) = a^{ski} = (a^{sk})^i = a^i.$$

Therefore,

$$Aut(C_n) = \{\Phi_k \mid gcd(k,n) = 1\}$$

How do these combine? Suppose $\Phi_j, \Phi_k \in Aut(C_n)$. Then

$$(\Phi_j * \Phi_k)(a) = \Phi_j(\Phi_k(a)) = \Phi_j(a^k) = (a^k)^j = a^{jk} = \Phi_{jk}(a).$$

That is, $\Phi_j * \Phi_k = \Phi_{jk}$, and $gcd(j,n) = gcd(k,n) = 1$.

This looks a great deal like $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$! To make this precise, define $\Psi : Aut(C_n) \to ((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ in the only reasonable way:

$$\Psi(\Phi_k) = [k]_n.$$

The previous discussions have hopefully made it clear that Ψ is a bijection: $\Phi_k \in Aut(C_n)$ if and only if $[k]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, so all we have to check is the operation, and

$$\Psi(\Phi_j * \Phi_k) = \Psi(\Phi_{jk}) = [jk]_n = [j]_n[k]_n = \Psi(\Phi_j) \odot \Psi(\Phi_k).$$

Thus, Ψ is the desired isomorphism.

Since $(\mathbb{Z}/n\mathbb{Z})^*$ has $\phi(n)$ elements, where ϕ is the Euler phi function, if follows that $|Aut(C_n)| = |(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. □

As a remark, lots of times, isomorphisms are easy to check, once you understand the groups involved.

Let's do a few examples here, for $n = 11$ and $n = 12$.

First, since 11 is prime, $\phi(11) = 11 - 1 = 10$ and all possible non-trivial homomorphisms from $C_{11} = \langle a \rangle, a^{11} = e$ to itself are automorphisms:

$$\Phi_k(a) = a^k, \qquad a \in \{1,2,3,4,5,6,7,8,9,10\}.$$

As we have seen, $[2]_{11}$ is a generator of $((\mathbb{Z}/11\mathbb{Z})^*, \odot)$; that is, the powers of $[2]_{11}$ give the entire group. I list $[2^i]_{11}$ below:

$$[1]_{11}, [2]_{11}, [4]_{11}, [8]_{11}, [5]_{11}, [10]_{11}, [9]_{11}, [7]_{11}, [3]_{11}, [6]_{11}.$$

By the isomorphism, the powers of Φ_2 generate $Aut(C_{11})$:

$$\Phi_1, \Phi_2, \Phi_4, \Phi_8, \Phi_5, \Phi_{10}, \Phi_9, \Phi_7, \Phi_3, \Phi_6.$$

Powers here mean under composition, so $\Phi_8 = \Phi_2^3$ means that

$$\Phi_2(\Phi_2(\Phi_2(a))) = \Phi_2(\Phi_2(a^2)) = \Phi_2(a^4) = a^8 = \Phi_8(a).$$

On the other hand, we saw about a month ago that $\phi(12) = 4$ and $((\mathbb{Z}/12\mathbb{Z})^*, \odot)$ is isomorphic to V. To be specific, the elements of $(\mathbb{Z}/12\mathbb{Z})^*$ are:

$$[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}.$$

What does $Aut(C_{12})$ look like?

$$\Phi_k(a) = a^k, \qquad a \in \{1, 5, 7, 11\}.$$

As a review, the reason that, say $\Phi_{10} \notin Aut(C_{12})$ is that the image of Φ_{10}, that is, $\{\Phi_{10}(a^k)\}$, consists of

$$\{e, a^{10}, a^8, a^6, a^4, a^2\}$$

Since $a \notin Im(\Phi_{10})$, the map Φ_{10} is not a surjection, and can't be an automorphism.

A check that $Aut(C_{12}) \approx V$: since $\Phi_j * \Phi_k = \Phi_{jk} = \Phi_{(jk \mod 12)}$,

$$\begin{gathered}
\Phi_1 * \Phi_k = \Phi_k * \Phi_1 = \Phi_k, \\
(\Phi_5)^2 = \Phi_{25} = \Phi_1, \\
(\Phi_7)^2 = \Phi_{49} = \Phi_1, \\
(\Phi_{11})^2 = \Phi_{121} = \Phi_1, \\
\Phi_5 * \Phi_7 = \Phi_7 * \Phi_5 = \Phi_{35} = \Phi_{11}, \\
\Phi_5 * \Phi_{11} = \Phi_{11} * \Phi_5 = \Phi_{55} = \Phi_7, \\
\Phi_7 * \Phi_{11} = \Phi_{11} * \Phi_7 = \Phi_{77} = \Phi_5.
\end{gathered}$$

The final topic for today is another interesting group, the generalization of V to "three dimensions". For our purposes, let $C_2 = (\mathbb{Z}/2\mathbb{Z}, \oplus)$, so the components are $[0]_2$ or $[1]_2$

$$C_2 \times C_2 \times C_2 = \{([i]_2, [j]_2, [k]_2)\}, \qquad i, j, k \in \{0, 1\}.$$

Let's write $([i]_2, [j]_2, [k]_2)$ as ijk, so the $8 = 2^3$ elements are:

$$000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111.$$

Addition is component-wise mod 2 and commutative, so for example, $011 + 101 = 112 = 110$. The identity is 000, and

$$([i]_2,[j]_2,[k]_2)+([i]_2,[j]_2,[k]_2)=$$
$$([2i]_2,[2j]_2,[2k]_2)=([0]_2,[0]_2,[0]_2),$$

so every element has order two.

The order of this group is 8, so subgroups might have order 1,2,4 or 8, and proper subgroups would have order 2 or 4. Any subgroup of order 2 would have to look like $\{000, ijk\}$ and there are $7 = 2^3 - 1$ ways to pick ijk, so there are 7 subgroups of order 2.

Let's write $000 = e$, because it's the identity, and suppose H is a subgroup of order 4. Suppose $e, x, y \in H$ are different. Then we have to have $x + y \in H$, but then we actually get a subgroup: $x + (x + y) = (x + y) + x = y$, etc.,

$$H = \{e, x, y, x + y\},$$

which you won't be shocked to learn is isomorphic to V.

How many different subgroups of order 4 are there? At first glance, you might count them this way: there are 7 choices for x (not e) and then 6 choices for y (not e or x), so you might think there are $7 \cdot 6 = 42$ subgroups, but that is over-counting! For example, $\{e, x, y, x+y\}$ gives you the same set as $\{e, y, x, y + x\}$.

If you started with $x + y$ and y you'd get $(x + y) + y = x$. In fact, each subgroup arises in six different ways, and there are seven different subgroups, presented with an "external" definition.

$$H_1 = \{000,\ 001,\ 010,\ 011\} = \{ijk \mid i = 0\}$$
$$H_2 = \{000,\ 001,\ 100,\ 101\} = \{ijk \mid j = 0\}$$
$$H_3 = \{000,\ 001,\ 110,\ 111\} = \{ijk \mid i = j\}$$
$$H_4 = \{000,\ 010,\ 100,\ 110\} = \{ijk \mid k = 0\}$$
$$H_5 = \{000,\ 010,\ 101,\ 111\} = \{ijk \mid i = k\}$$
$$H_6 = \{000,\ 011,\ 100,\ 111\} = \{ijk \mid j = k\}$$
$$H_7 = \{000,\ 011,\ 101,\ 110\} = \{ijk \mid i + j + k \equiv 0 \mod 2\}.$$

A couple of final remarks. If you think of $\{ijk\}$ as the point $(i, j, k) \in \mathbb{R}^3$, then C_2^3 can be thought of as the vertices of a unit cube, and six of these subgroups are the intersections of the cube with a plane that passes through the origin: $x = 0$, $y = 0$, $x = y$, $z = 0$, $x = z$, $y = z$.

If you draw it out, the vertices of H_7 don't lie in the plane, but they form a regular tetrahedron, taken from alternate vertices of the cube.

The other thing I want to say is that we can look at the H_i's and take out 000 and just look at these as seven sets, and for convenience, I'll look at the remaining numbers as if they were in binary, so, for example, $101 \to 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 5$.

$$\begin{aligned}
S_1 &= \{001,\ 010,\ 011\} = \{1, 2, 3\} \\
S_2 &= \{001,\ 100,\ 101\} = \{1, 4, 5\} \\
S_3 &= \{001,\ 110,\ 111\} = \{1, 6, 7\} \\
S_4 &= \{010,\ 100,\ 110\} = \{2, 4, 6\} \\
S_5 &= \{010,\ 101,\ 111\} = \{2, 5, 7\} \\
S_6 &= \{011,\ 100,\ 111\} = \{3, 4, 7\} \\
S_7 &= \{011,\ 101,\ 110\} = \{3, 5, 6\}
\end{aligned}$$

Notice that each number is in three sets and each set has three numbers. Every pair of numbers is in exactly one set, and any two sets contain exactly one number in common.

You can think of each S_j as a "line" and each number as a "point". There is exactly one line containing any two points and any two lines intersect in exactly one point.

It is called the *Fano plane* and is a finite projective plane "of order 2". You won't see these terms again in this class this semester!

September 30, 2020, in class

I'll start again from the inbox, with answers to questions.

1. When you were talking about the isomorphisms of V, and the permutation $\{\pi(X), \pi(Y), \pi(Z)\}$, Permutation is just the reordering of the elements in a set, right?

Exactly. Two permutations are $\pi(X) = Y, \pi(Y) = X, \pi(Z) = Z$ and $\pi(X) = Y, \pi(Y) = Z, \pi(Z) = X$.

2. When we took into account u does not equal to v, why did we include a third element and compare the third element? Is it because u, v are already two elements of the set $\{X, Y, Z\}$?

This was because $X * Y = Z, Z * X = Y$, etc for all choices, so if the three elements are $\{u, v, w\}$, then $u * v = w$.

3. Is homomorphism the general concept and then isomorphism a special case of homomorphism and automorphism a special case of isomorphism?

Yes.

4. When we are proving that a function map is an automorphism, do we need to prove that it is a homomorphism first, then that it is injective to itself, and surjective to itself?

Not always. The order of proof doesn't matter. If you see that a map it isn't surjective, for example, then it can't be an automorphism, and you don't have to do anything else.

But an automorphism is a special kind of isomorphism, and the map in an isomorphism has to be a bijection, so at some point you have to prove that it is one-to-one and onto.

5. Why does $\phi(12) = 4$ and why did we do $\phi(11) = 11 - 1 = 10$? Is it related to the numbers that are relatively prime to n?

Yes, $\phi(n)$ is the number of integers less than n which are relatively prime to n. The formula is that if p is a prime, $\phi(p^k) = p^k - p^{k-1}$, and if n is given in terms of its prime factorization,

$$n = p_1^{k_1} \cdots p_r^{k_r} \implies$$
$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

We have $11 = 11^1$ and $\phi(11) = 11 - 1$; $12 = 2^2 \cdot 3$, so $\phi(12) = (2^2 - 2^1)(3 - 1) = (4 - 2)(3 - 1) = 2 \cdot 2 = 4$.

6. For the exam, what sections of the book should I focus my studying on?

The material is mostly from sections 4,5,6,8,9,10,11,13,14, but the main thing to do is to look at the sort of questions that have been on the homework and in the worksheet questions. I will have by Monday a list of vocabulary, ideas and theorems that you should know for the exam

Remember that $Aut(G)$, the set of automorphisms of G is a group. We gave one general construction of automorphisms, the conjugations: i_g given by $i_g(x) = gxg^{-1}$; these are called inner automorphisms. Let $Aut_I(G) = \{i_g \mid g \in G\}$.

As always, $Aut_I(G)$ is the *set* of all inner automorphisms, if $i_g = i_h$, then it's only counted once in the set; if G is abelian, we've already seen that $Aut_I(G)$ consists of the identity map

THEOREM The set of inner automorphisms $Aut_I(G)$ is a subgroup of $Aut(G)$.

PROOF The proof is pretty fast. We have

$$(i_g * i_h)(x) = i_g(i_h(x)) = i_g(hxh^{-1}) = g(hxh^{-1})g^{-1}$$
$$= (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = i_{gh}(x).$$

so $Aut_I(G)$ is closed under $*$. For all x, $i_e(x) = exe^{-1} = x$, so the identity element in $Aut(G)$ is contained in $Aut_I(G)$. And from the above $i_g * i_{g^{-1}} = i_e$, so it contains inverses as well. □

WORKSHEET PROBLEM

Let $G = S_3 \times (\mathbb{Z}/2\mathbb{Z}, \oplus)$. That is, the elements of G consist of the ordered pairs (g, h), where $g \in S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ and $h \in \{[0]_2, [1]_2\}$, with the respective operations on each component:

$$(\rho_1, [1]_2) * (\mu_1, [1]_2) = (\rho_1\mu_1, [1]_2 \oplus [1]_2) = (\mu_3, [0]_2), \quad \text{etc.}$$

1. Determine $H = \langle(\rho_1, [1]_2)\rangle$, explain (quickly!) why it is a normal subgroup, and give a homomorphism ϕ from H to $C_2 = \langle a\rangle, a^2 = e$ for which $Ker(\phi) = H$.

2. "Extra credit". Find a subgroup of S_5 which is isomorphic to H.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Let's start by taking the powers of $x = (\rho_1, [1]_2)$

$$\begin{aligned}
x^2 &= x * x = (\rho_1\rho_1, [1]_2 + [1]_2) = (\rho_2, [0]_2),\\
x^3 &= x * x^2 = (\rho_1\rho_2, [1]_2 + [0]_2) = (\rho_0, [1]_2),\\
x^4 &= x * x^3 = (\rho_1\rho_0, [1]_2 + [1]_2) = (\rho_1, [0]_2),\\
x^5 &= x * x^4 = (\rho_1\rho_1, [1]_2 + [0]_2) = (\rho_2, [1]_2),\\
x^6 &= x * x^5 = (\rho_1\rho_2, [1]_2 + [1]_2) = (\rho_0, [0]_2),
\end{aligned}$$

So $x^6 =$ e and $H = \langle x\rangle$ is a cyclic group of order 6. Since $|S_3 \times C_2| = 6 \times 2 = 12$, $[G : H] = 12/6 = 2$ and H is normal.

Write $G = H \cup uH$, then ϕ would have to be defined as

$$\begin{aligned}
\phi((g, h)) &= e, \quad \text{if } (g, h) \in H,\\
\phi((g, h)) &= a, \quad \text{if } (g, h) \in uH \qquad \text{or } (g, h) \notin H.
\end{aligned}$$

2. Notice that the first and second component have nothing to do with each other, and I'd make the association $\Phi(x) = (123)(45)$, which

has a cycle of order three and a cycle of order two that don't interact.

$$\Phi(x^0) = \Phi((\rho_0, [0]_2)) = (1)(2)(3)(4)(5),$$
$$\Phi(x^1) = \Phi((\rho_1, [1]_2)) = (123)(45),$$
$$\Phi(x^2) = \Phi((\rho_2, [0]_2)) = (132)(4)(5),$$
$$\Phi(x^3) = \Phi((\rho_0, [1]_2)) = (1)(2)(3)(45),$$
$$\Phi(x^4) = \Phi((\rho_1, [0]_2)) = (123)(4)(5),$$
$$\Phi(x^5) = \Phi((\rho_2, [1]_2)) = (132)(45).$$

You should check that Φ is an isomorphism from H to $\langle (123)(45) \rangle$; that is, from one cyclic group of order six to another one.

In the same way, H is isomorphic to $\langle (123456) \rangle \subset S_6$.

October 2, 2020, in advance

Now we move on to the second main topic of this course, rings. This is an overview, and since we won't have homework due on this for two weeks, I'll just give mostly definitions. There are a lot of them.

A *ring* R is a set which has two binary operations – $+$ and $\cdot$ – which fulfill the following rules:

The rings, under $+$, are an abelian group. So:

(i) $a, b \in R \implies a + b = b + a \in R$;

(ii) There exists an additive identity element, called 0_R, so that, for all $a \in A$, $a + 0_R = 0_R + a = a$;

(iii) Every $a \in R$ has an inverse, called $-a$ so that $a \in A$, $a + (-a) = (-a) + a = 0_R$;

(iv) Associativity: $a, b, c \in R \implies (a + b) + c = a + (b + c) \in R$;

The rings, under $\cdot$, have very few rules:

(v) $a, b \in R \implies a \cdot b \in R$;

(vi) Associativity: $a, b, c \in R \implies (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

The two operations are linked by the distributive law, both on the left and the right.

(vii) Distributivity: $a, b, c \in R \implies a \cdot (b+c) = a \cdot b + a \cdot c), (a+b) \cdot c = a \cdot c + b \cdot c$.

What isn't spoken of is not necessarily there. We do not assume that multiplication is commutative. We do not assume that there is a multiplicative identity. We do not assume that all elements have multiplicative inverses!

If the ring R satisfies the additional condition

(viii) $a, b \in R \implies a \cdot b = b \cdot a \in R$

Then it is called a *commutative ring*. Most of the rings we will deal with in the class are commutative rings. The most natural example of

a non-commutative ring is

$$M_n(\mathbb{R}) := \{\text{the set of all. } n \times n \text{ matrices with real coefficients}\}.$$

For matrices with integer coefficients, we'd have $M_n(\mathbb{Z})$, etc.

If the ring R satisfies the additional condition

(ix) There exists a multiplicative identity element, written 1_R, so that, for all $a \in A$, $a \cdot 1_R = 1_R \cdot a = a$.

then it is called a *ring with unity*. (Fraleigh calls the element "unity".) If both (viii) and (ix) are satisfied, it is a *commutative ring with unity*.

There are more definitions, but I'd like to give you some familiar examples.

The real numbers $\mathbb{R}$ with the usual operations are a commutative ring with unity $1_R = R$ and $0_R = 0$. Addition is an abelian group, multiplication is associative and the distributive laws hold. All non-zero elements of $\mathbb{R}$ have the usual multiplicative inverse x^{-1}.

The rational numbers $\mathbb{Q}$ with the usual operations are a commutative ring with unity for the same reason. All non-zero elements of $\mathbb{Q}$ have the usual multiplicative inverse x^{-1}.

The integers $\mathbb{Z}$ with the usual operations are a commutative ring with unity. The only elements of $\mathbb{Z}$ which have a multiplicative inverse *in* $\mathbb{Z}$ are $\{-1, 1\}$. (For example $\frac{1}{2} \cdot 2 = 1$, but $\frac{1}{2} \notin \mathbb{Z}$.)

Let's look at $2\mathbb{Z}$, under the usual operations. We've already looked at this under addition and persuaded ourselves that it's an abelian group. The associative and distributive laws are "inherited" from $\mathbb{R}$, so this is a ring. It is commutative, but it doesn't have an identity! We have

$$2\mathbb{Z} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\},$$

and the only possible multiplicative identity is 1, but $1 \notin 2\mathbb{Z}$. This is true for $n\mathbb{Z}$ for every integer n, so $1_{2\mathbb{Z}}$ does not exist.

Another friend from our group days is a candidate for a ring, and this combines $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ and $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ into one object.

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \dots, [n-1]_n\}, \quad [a]_n + [b]_n = [a+b]_n,\ [a]_n \cdot [b]_n = [ab]_n$$

The difference here is that we do not limit multiplication to those $[k]_n$ with $gcd(k, n) = 1$.

For example, cut and pasting from the first week, with $n = 4$,

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is a commutative ring with unity $[1]_4$ and additive identity $[0]_4$. But notice something unexpected here $[2]_4 \cdot [2]_4 = [0]_4$. We can have the product of two non-zero elements equal to zero. This leads to an important definition

If $a, b \in R$ and $a \neq 0, b \neq 0$, but $ab = 0$, then a and b are called *zero divisors*. It is not very hard to show that with the definitions given so far, $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is prime.

An *integral domain* is a commutative ring with unity $1_R \neq 0_R$ which has no zero divisors. Think of $\mathbb{Z}$ as the natural example. (The condition $1_R \neq 0_R$ is a technicality we'll deal with later.)

Another familiar ring is the *ring of polynomials* over a ring R, which is written $R[x]$. So, for example $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients and $\mathbb{R}[x]$ is the ring of polynomials with real coefficients. One fun thing is that if we look at polynomials with coefficients in $\mathbb{Z}/n\mathbb{Z}$, then it is possible that we no longer have unique factorization: for example

$$x^2 + 7 = (x+1)(x+7) = (x+3)(x+5)$$

if we are only looking mod 8, because $(x+1)(x+7) = x^2 + 8x + 7$ and $(x+3)(x+5) = x^2 + 8zx + 15$, and both of these reduce to $x^2 + 7$ mod 8. To be precise, the equation above is really

$$[1]_8x^2+[0]_8x+[7]_8 = ([1]_8x+[1]_8)([1]_8x+[7]_8) = ([1]_8x+[3]_8)([1]_8x+[5]_8)$$

We will have *a lot* on situations like these later in the semester.

One more piece of notation, if R is a ring with unit 1_R, $a \in R$ is called a *unit* if there exists $b \in R$ so that $ab = 1_R$. The set of units in a ring is written as $U(R)$ or R^*. (This is where I got the notation $(\mathbb{Z}/n\mathbb{Z})^*$.)

LEMMA If R is a ring, then $0_R \cdot x = 0_R$ for every $x \in R$. In particular, 0_R is not a unit.

PROOF. We have from the distributive law that

$$\begin{gathered} 0_R \cdot x = (0_R + 0_R) \cdot x = 0_R \cdot x + 0_R \cdot x \implies \\ -(0_R \cdot x) + 0_R \cdot x = -(0_R \cdot x) + (0_R \cdot x + 0_R \cdot x) \implies \\ -(0_R \cdot x) + 0_R \cdot x = (-(0_R \cdot x) + 0_R \cdot x) + 0_R \cdot x) \implies \\ 0_R = 0_R + 0_R \cdot x \implies 0_R = 0_R \cdot x \end{gathered}$$

If $U(R) = R \setminus \{0_R\}$, then R is called a *division ring*. If a division ring is commutative, it is called a *field*. We will see that $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ are fields, as is $\mathbb{Z}/p\mathbb{Z}$ when p is prime.

What are the units in $\mathbb{R}[x]$? Let's talk informally about polynomials, there will be a formal definition later, but it does coincide with what

you are familiar with, and both addition and multiplication are what you expect.

Well, when can we have polynomials p, q so that $p(x)q(x) = 1_{\mathbb{R}[x]}$? First of all what is $1_{\mathbb{R}[x]}$? If a polynomial is

$$p(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_j \in \mathbb{R},$$

and multiplication is what you expect, and $q(x) = 1$ is the constant polynomial, then $p(x)q(x) = q(x)p(x) = p(x)$ for all p, so $q(x) = 1_{\mathbb{R}[x]}$ is the constant polynomial.

Repeating the question, when can we have polynomials p, q so that $p(x)q(x) = 1$, where 1 is the constant polynomial. If you think about degrees (we'll do this formally later), p and q both have to be non-zero constant polynomials (degree zero), so

$$U(\mathbb{R}[x]) = \{a_0 \mid a_0 \neq 0\}$$

and can be put into one-to-one correspondence with $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Finally, yes there are ring homomorphisms too. Suppose R and R' are two rings. A map $\phi : R \to R'$ is called a ring homomorphism if for all $a, b \in R$, we have

$$\phi(a + b) = \phi(a) + \phi(b), \qquad \phi(ab) = \phi(a)\phi_b$$

where the operations on a, b are the operations in R and those on $\phi(a), \phi(b)$ are the operations in R'. Yes, we have kernels and images and isomorphisms and automorphisms. All in due time.

I wanted to mention one non-intuitive homomorphism on $\mathbb{R}[x]$. We have polynomials as objects, we can add them and multiply them in the familiar way as objects. But they are also functions, and we can evaluate them. Suppose $a \in \mathbb{R}[x]$, the *evaluation homomorphism at* t, ϕ_c, which is a homomorphism from $\mathbb{R}[x] \to \mathbb{R}$ is defined by

$$\phi_c(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1c + \cdots + a_nc^n; \qquad \phi_c(p) = p(c).$$

As a small hint of further developments, what ought $Ker(\phi_t)$ be. I haven't given all the formal definitions, but

$$Ker(\phi_c) = \{p(x) \ : \ \phi_c(p(x)) = 0_{\mathbb{R}}\} = \{p(x) \ : \ p(c) = 0\},$$

so the kernel is the set of polynomials which vanish at $x = c$. You probably know that, in this case, this condition is equivalent to being able to factor $p(x) = (x - c)q(x)$. We will look at some polynomial rings in which this is not the case.

October 2, 2020, in class

Before I repeat the frames with the overview (yes, basically unchanged)

I'd like to answer a few questions I've gotten overnight.

1. An extremely alert student noted that on frames from Sept. 9 (Day 7), I multiplied permutations in the wrong order. This was corrected on Sept. 11 (Day 8), so keep that in mind when studying.

2. A student writes to ask whether "generators" will be on the test. What I said was:

Yes, they might be on the test. I might give you a cyclic group and one generator and ask you to find another generator, but it won't involve large numbers: for example, I wouldn't ask you to decide if $[2]_{37}$ is a generator of $((\mathbb{Z}/37\mathbb{Z})^*, \odot)$.

3. Another student asked about the nature of the first exam, so I think it's worthwhile to put this all in one place.

a. I will email you the exams on Thursday night (10/8). They will be due back to me by 11:59PM on Saturday night (10/10). I will try to acknowledge receipt with reasonable speed, depending on the time of day.

b. My intention is that this test would be the same length as a typical hour exam, with a median time to finish around 45 minutes.

c. There will be no class on Friday 10/9.

d. There will be multiple equivalent variations on the problems of the exam, sent to different people.

e. I will ask you to block out a **consecutive** period of time to work on the test. If you take more than two hours, please indicate that on your paper.

f. It is very important to show your work and explain your steps.

g. As always, read the problems carefully.

h. The exam is open book, open notes and open to the class notes I've been providing. You may use a calculator, but it shouldn't be necessary.

i. **This is a non-collaborative exam. Please do not talk to anyone else about the test unless you know that everyone in the conversation has taken it.**

j. Despite the relaxed nature of these rules, I am attaching a link to §1-402 of the Student Code regarding Academic Integrity. I've read it, and I hope you have too.

https://studentcode.illinois.edu/article1/part4/1-402/

Here are the frames again. Please let me know if you have questions or if I missed something.

Number theory topics: $\mathbb{Z}, \mathbb{Q}$, divisibility, $m \mid n$, congruence mod n, $a \equiv b \mod n$, $[a]_n$, prime numbers, gcd, $gcd(m, n)$, relatively prime integers, the existence of prime factorization, Euclidean Algorithm. Know what the Euler phi function $\phi(n)$ means, but you won't have to calculate it. Know that $gcd(m, n) = g$ implies that there exist integers

r, s so that $g = mr+ns$ (findable through the EA) and if $gcd(m, n) = 1$ and $n \mid mr$, then $n \mid r$.

Group Theory Vocabulary: commutative, associative, binary operations, the definition of a group, and an identity and inverses in a group, abelian groups, cyclic groups ($C_n = \langle a \rangle, a^n = e$ or $(\mathbb{Z}/n\mathbb{Z}, \oplus)$), the symmetric group S_n in general, and in more detail S_3, the Klein group V and the dihedral group D_4.

More Group Theory: subgroups, $H \leq G$, the order of a group $|G|$, the order of an element in a group, isomorphisms, homomorphisms (plus kernel $Ker(\phi)$ and image $Im(\phi)$), left and right cosets of a subgroup, normal subgroup $H \trianglelefteq G$ and what that means, direct product of two groups $G \times H$, factor groups as a result of a normal subgroup, G/H consisting of the cosets of H. If $\phi : G \to H$ is a homomorphism, then $K = Ker(\phi) \trianglelefteq G$ and G/K is isomorphic to $Im(\phi)$.

More things to be able to do: Read a group multiplication table. If you know G and H, you should be able to work with $G \times H$ and if $gcd(m, n) = 1$, you should know that $C_m \times C_n \approx C_{mn}$. How to decide if a subset H of G is a subgroup, how to find the subgroups of cyclic groups and the connection with gcd, Lagrange's Theorem. How to compute the orders of elements in cyclic groups and in direct products.

With permutations, know cycles and transpositions. Write permutations in multiple ways, for example if $\pi : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ and $\pi(1) = 2, \pi(2) = 4, \pi(3) = 3, \pi(4) = 1$, then we might write this as:

$$\pi : 1 \mapsto 2 \mapsto 4 \mapsto 1, 3 \mapsto 3,$$

$$\pi = (124)(3), \quad \pi = (124), \qquad \pi = \begin{pmatrix} 1234 \\ 2431 \end{pmatrix}$$

Know how to multiply permutations in the right order.

Not on this test $\phi(n)$ (except incidentally as $|((\mathbb{Z}/n\mathbb{Z})^*, \odot)|$), repeating decimals as such, Cayley's Theorem, odd/even permutations, the book's theorem on the classification of finite abelian groups. What we've done this week on $Aut(G)$, i_g, etc.

Send me an email if there's something I missed.