MATH 417 –FIFTH WEEK

BRUCE REZNICK
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

September 21, 2020, in advance

There is a lot of material in section 9 of the book on cycles and permutations, and section 10 on cosets, and I think we've covered most of it already.

One topic I'm going to mention but not have on homework or exams is the idea of even and odd permutations. This is based on counting transpositions, and the "real" proof of it requires matrices. Since linear algebra isn't a prerequisite, I can't give the full proof, but I'd like to sketch it anyway.

A transposition is a permutation $\pi \in S_n$ with the property that $\pi(k) = k$ for $n-2$ of the elements in $\{1, \ldots, n\}$, and for $i \neq j$, $\pi(i) = j$ and $\pi(j) = i$. Examples include the μ_j's in S_3. The cycle representation for π consists of the cycle (ij), and everything else a singleton. For example, with $n = 5$,

$$\pi_5 = \begin{pmatrix} 12345 \\ 15342 \end{pmatrix} = (25) = (25)(1)(3)(4),$$

Two comments on notation. Since (i) doesn't do anything, we often don't write it. Also, Fraleigh puts commas in his cycles. I don't.

I mentioned in passing a few days ago that any cycle can be written as a product of transpositions: if the x_i's are all different, then

$$(x_1 x_n)(x_1 x_{n-1}) \cdots (x_1 x_3)(x_1 x_2) = (x_1 x_2 x_3 \cdots x_{n-1} x_n)$$

But there are many ways to write permutations as products. For example,

$$(12)(13)(14)(13) = (12)(34).$$

We call a permutation an *even* permutation if it is a product of an even number of transpositions and an *odd* permutation if it is a product of an odd number of transpositions.

The obvious and crucial question would be: is this well-defined? Could you write the same permutation as a product of an even number of transpositions and as a product of an odd number of transpositions? The answer is no, and there are two proofs in the book. What I'll give you is the most fundamental proof; this is "culture".

The *permutation matrix* M_π associated to $\pi \in S_n$ is an $n \times n$ matrix $[a_{ij}]$ so that $a_{ij} = 1$ if $j = \pi(i)$ and $a_{ij} = 0$ otherwise. For example, for the D_4 element $\mu_1 = (12)(34)$,

$$M_{\mu_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

I won't go into details, but if you define $G = \{M_\pi, \pi \in S_n\}$ with the operation of matrix multiplication, you get a group, and $\Phi(\pi) = M_\pi$ defines an isomorphism. Big deal, right?

But here's the thing. If you know row reduction, you can very easily persuade yourself that the determinant $\det(M_\pi)$ is always equal to ± 1.

If you know matrices, you know that $\det(M_1 M_2) = \det(M_1)\det(M_2)$. It is not hard to show that if τ is a transposition, then $\det(M_\tau) = -1$. Thus if π is a product of k transpositions, then $\det(M_\pi) = (-1)^k$.

So an alternative definition of an even permutation π is one for which $\det(M_\pi) = 1$, and an odd permutation π is one for which $\det(M_\pi) = -1$.

There is an important subgroup of S_n, for $n \geq 2$, called the *alternating subgroup* A_n and consisting of the even permutations in S_n: $|A_n| = n!/2$.

As noted in the book, A_4 is a group of order 12, and even though $6 \mid 12$, A_4 does not have a subgroup of order 6. Thus, Lagrange's Theorem can't be an iff statement.

I'd like to move onto a new topic which we've seen instances of. Suppose $(G, *_G)$ and $(H, *_H)$ are both groups. They might even be the same, it doesn't matter. They can be finite or infinite, abelian or not abelian. We define the *direct product* as follows: the elements come from a Cartesian product

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

and we define the operation $*_{G\times H}$ in the simplest way possible: if $g_i \in G$ and $h_i \in H$, then

$$(g_1, h_1) *_{G\times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

THEOREM Using the definitions given above, $G \times H$ is a group.

PROOF What do we have to prove? First that the operation is a binary operation. But if $(g_1, h_1), (g_2, h_2) \in G \times H$, then $g_1, g_2 \in G \implies g_1 *_G g_2 \in G$, because G is a group, and $h_1, h_2 \in H \implies h_1 *_H h_2 \in H$, so the product is in $G \times H$.

Next there is the identity, but G and H are groups, so they have identity elements e_G and e_H, and so for every $(g,h) \in G \times H$,

$$(g,h) *_{G\times H} (e_G, e_H) = (g *_G e_G, h *_H e_h) = (g,h) = (e_G, e_H) *_{G\times H} (g,h).$$

Inverses are handled the same way: suppose $g \in G, h \in H$, then there exist $g^{-1} \in G, h^{-1} \in H$ and

$$(g,h) *_{G\times H} (g^{-1}, h^{-1}) = (g *_G g^{-1}, h *_H eh^{-1}) = (e_G, e_H) = e_{G\times H}.$$

Finally, associativity is verified for each component separately, since G and H are themselves associative.

$$((g_1,h_1) *_{G\times H} (g_2,h_2)) *_{G\times H} (g_3,h_3) =$$
$$(g_1 *_G g_2, h_1 *_H h_2) *_{G\times H} (g_3,h_3) = ((g_1 *_G g_2) *_G g_3, (h_1 *_H h_2) *_H h_3)$$
$$= (g_1 *_G (g_2 *_G g_3), h_1 *_H (h_2 *_H h_3))$$
$$= (g_1,h_1) *_{G\times H} ((g_2,h_2) *_{G\times H} (g_3,h_3)).$$

So this is a group. If G and H are both finite groups, then $|G \times H| = |G| \cdot |H|$; if they are both abelian, then so is $G \times H$.

We can generalize this and consider the direct product $G_1 \times G_2 \times \cdots \times G_s$ in exactly the same way. Yes, it's associative. We won't talk about this except at the end of class today.

What about subgroups?

THEOREM If $G_1 < G$ and $H_1 < H$, then

$$\{(g,h) \ : \ g \in G_1, h \in H_1\}$$

is a subgroup of $G \times H$. (It is customarily called $G_1 \times H_1$.)

PROOF The proof is simple. We have the same operation as before, and for $g_1, g_2 \in G_1$ and $h_1, h_2 \in H_1$

$$(g_1,h_1) *_{G\times H} (g_2,h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

Since G_1 is a subgroup, $g_1 *_G g_2 \in G_1$; since H_1 is a subgroup, $h_1 *_H h_2 \in H_1$, so $G_1 \times H_1$ closed under the operation.

Also, $e_G \in G_1$ and $e_H \in H_1$ so $(e_G, e_H) = e_{G\times H} \in G_1 \times H_1$, and $(g^{-1}, h^{-1}) \in G_1 \times H_1$, so we've satisfied all the criteria, and $G_1 \times H_1$ is a subgroup. Is it the only kind of subgroup?

Time for some examples. It is not hard to show that $G \times \{e\}$ and $\{e\} \times G$ are both isomorphic to G, so they are not interesting.

The smallest nontrivial group is C_2. What happens if we take $G \times H$, when G and H are each cyclic groups of order 2? It is a group of order $2 \times 2 = 4$, so we should know it.

Let's be more specific and overly careful with notation. Look at

$$\{e_G, a\} \times \{e_H, b\}$$

where $a *_G a = e_G$ and $b *_H b = e_H$. So there are four elements

$$\{(e_G, e_H), (a, e_H), (e_G, b), (a, b)\}$$

Multiplication is by component: for example

$$(a, e_H) *_{G\times H} (a, b) = (a *_G a, e_H *_H b) = (e_G, b).$$

We can finish the multiplication table, and I think you'll recognize it.

$G \times H$	(e_G, e_H)	(a, e_H)	(e_G, b)	(a, b)
(e_G, e_H)	(e_G, e_H)	(a, e_H)	(e_G, b)	(a, b)
(a, e_H)	(a, e_H)	(e_G, e_H)	(a, b)	(e_G, b)
(e_G, b)	(e_G, b)	(a, b)	(e_G, e_H)	(a, e_H)
(a, b)	(a, b)	(e_G, b)	(a, e_H)	(e_G, e_H)

Yes, this is V, in its true colors as $C_2 \times C_2$. Let's look at the subgroups. Since G and H are cyclic groups of order 2, they have no proper subgroups, so the subgroups of G are $\{e_G\}$ and $\{e_G, a\}$ and the subgroups of H are $\{e_H\}$ and $\{e_H, a\}$.

This gives four subgroups of $G \times H$

$$\{(e_G, e_H)\}, \{(e_G, e_H), (a, e_H)\}, \{(e_G, e_H), (e_G, b)\}, G \times H.$$

To make this more familiar, let's apply the isomorphism to V which takes

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto X, (e_G, b) \mapsto Y, (a, b) \mapsto Z.$$

Then the four subgroups are $\{I\}$, $\{I, X\}$,$\{I, Y\}$. $\{I, X, Y, Z\}$.

One subgroup is missing: $\{I, Z\}$ or $\{(e_G, e_H), (a, b)\}$. This is a subgroup which does not come from a product of subgroups of G and H.

We've seen other instances of this: $(\mathbb{Z}/m\mathbb{Z}, \oplus) \times (\mathbb{Z}/n\mathbb{Z}, \oplus)$, when $m = 2$ and $n = 3, 4$. You looked at some subgroups of these too.

I wanted to finish with two nice theorems about the direct product of cyclic groups, which show the deep connection with number theory.

THEOREM If $gcd(m, n) = 1$, then $C_m \times C_n$ is isomorphic to C_{mn}.

Two remarks: when $m = n = 2$, the condition fails ($gcd(2, 2) = 2$) and $C_2 \times C_2$ is isomorphic to V, which is *not* isomorphic to C_4.

We have seen that $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/3\mathbb{Z}, \oplus)$ has an element of order 6, and so is isomorphic to C_6, which is isomorphic to $(\mathbb{Z}/6\mathbb{Z}, \oplus)$.

We need a lemma which we might have done already, but is worth repeating:

LEMMA If $gcd(m, n) = 1$, then $lcm(m, n) = mn$: if $m \mid t$ and $n \mid t$, then $mn \mid t$.

PROOF Suppose $m \mid t$, then we can write $t = ma$ for some $a \in \mathbb{Z}$. But now we have $n \mid ma$, and since $gcd(m, n) = 1$, one of our first

results was that this implies that $n \mid a$, so $a = nb$ for some $b \in \mathbb{Z}$, Putting this together,

$$t = ma = mnb$$

That is, $mn \mid t$. □

PROOF OF THEOREM Let's write

$$G = C_m = \langle a \rangle = \{e_G, a, a^2, \ldots, a^{m-1}\}, \quad a^m = e_G,$$
$$H = C_n = \langle b \rangle = \{e_H, b, b^2, \ldots, b^{n-1}\}, \quad b^n = e_H.$$

The elements of $C_m \times C_n$ are $\{(a^j, b^k)\}$, with j taken mod m and k taken mod n, and the combined operation is clear:

$$(a^j, b^k)(a^r, b^s) = (a^{j+r}, b^{k+s}).$$

It follows that the powers of (a, b) are straightforward:

$$(a, b)^t = (a^t, b^t).$$

What is the order of (a, b)?

$$(a, b)^t = e_{G\times H} \iff (a^t, b^t) = (e_G, e_H) \iff$$
$$a^t = e_G, b^t = e_H \iff m \mid t, n \mid t \iff mn \mid t.$$

This last equivalence is the lemma, because $gcd(m, n) = 1$.

It follows that

$$\{e_{G\times H}, (a, b), (a, b)^2, \ldots, (a, b)^{mn-1}\}$$

are distinct and $(a, b)^{mn} = e_{G\times H}$. That is,

$$C_m \times C_n = \langle (a, b) \rangle$$

is a cyclic group of order mn. □

This is what we found for $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/3\mathbb{Z}, \oplus)$.

What happened for $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/4\mathbb{Z}, \oplus)$ is different. Here, we can take the generators of the factors as $[1]_2$ and $[1]_4$, and $([1]_2, [1]_4)^4 = ([4]_2, [4]_4) = ([0]_2, [0]_4)$ is the identity. In fact, for any element of this group of order 8,

$$([i]_2, [j]_4)^4 = ([4i]_2, [4j]_4) = ([0]_2, [0]_4),$$

so there is no element of order 8, and so the group is not cyclic.

THEOREM If $gcd(m, n) = g > 1$, then $C_m \times C_n$ is not cyclic.

PROOF Write $m = gm'$ and $n = gn'$ and let $T = gm'n' = mn/g$; $T < mn$. (This is also equal to $lcm(m, n)$, but we don't need that here.) Let (a^j, b^k) be any element of the group. Then recalling the definitions of m' and n', we get

$$(a^j, b^k)^T = (a^{jgm'n'}, b^{kgm'n'}) = (a^{jmn'}, b^{knm'}) =$$
$$((a^m)^{jn'}, (b^n)^{km'}) = (e_G^{jn'}, e_H^{km'}) = e_{G\times H}.$$

Since $|C_m \times C_n| = mn > T$, this means that there is no element which generates the entire group, so it isn't cyclic. □

Final note: we won't prove it in this class, and Fraleigh doesn't prove it in the book, but one of the reasons this sort of thing is studied is the Fundamental Theorem of Abelian Groups: every finite abelian group can be written as a product of cyclic groups whose orders are each the power of a prime.

To be precise, suppose G is a finite abelian group of order

$$n = p_1^{a_1} \dots p_s^{a_s}$$

Then for each k, $1 \le k \le s$, there is a group

$$G_k = C_{p_k^{b_{k1}}} \times \cdots \times C_{p_k^{b_{km}}}, \quad \sum_\ell b_{k\ell} = a_k$$

and G is isomorphic to

$$G_1 \times G_2 \cdots \times G_s.$$

September 21, 2020, in class

There seems to be some confusion in the way I presented the subgroups of $C_2 \times C_2$, so I'd like to run through it again.

We had

$$\{e_G, a\} \times \{e_H, b\}$$

where $a *_G a = e_G$ and $b *_H b = e_H$. So there are four elements

$$\{(e_G, e_H), (a, e_H), (e_G, b), (a, b)\}$$

Each group has two subgroups. I'll call them

$$G_1 = \{e_G\}, G_2 (= G) = \{e_G, a\}, \quad H_1 = \{e_H\}, H_2 (= H) = \{e_H, b\}$$

This gives four subgroups of $G \times H$:

$$G_1 \times H_1 = \{(e_G, e_H)\}$$
$$G_2 \times H_1 = \{(e_G, e_H), (a, e_H)\}$$
$$G_1 \times H_2 = \{(e_G, e_H), (e_G, b)\},$$
$$G_2 \times H_2 = G \times H.$$

My point was only that $G \times H$ has one more subgroup which is not of that form: $\{(e_G, e_H), (a, b)\}$.

Under the familiar isomorphism to V which takes

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto X, (e_G, b) \mapsto Y, (a, b) \mapsto Z.$$

these five subgroups are, in order, $\{I\}$, $\{I, X\}$,$\{I, Y\}$. $\{I, X, Y, Z\}$, $\{I, Z\}$.

There is nothing special about Z! It is just the image of (a, b) under the isomorphism. Remember that X, Y, Z are somehow equivalent to each other, and

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto Y, (e_G, b) \mapsto Z, (a, b) \mapsto X.$$

is also an isomorphism.

This leads to another important piece of terminology. Suppose G is a group. An isomorphism of G to itself is called an *automorphism*. To distinguish these, I'll use the letter Ψ, rather than Φ. (Personal choice, not in the book. Automorphisms aren't in the book this early, except as a homework problem.)

Every group has an automorphism! Define Ψ_0 on G by: $\Psi_0(g) = g$ for all g. Then Ψ_0 is a bijection and $\Psi_0(g) * \Psi_0(h) = \Psi_0(g * h)$.

Remember that automorphisms are isomorphisms, so we can specialize our early results, which I'll quickly review;

$$\Psi(e) = e, \quad \Psi(g^{-1}) = (\Psi(g))^{-1}.$$

Suppose now that $G = C_n$, a cyclic group. It turns out that the automorphisms of C_n depend very much on the properties of n as an integer. THEOREM If $G = C_n$, then G has $\phi(n)$ different automorphisms, given by

$$x \in G \implies \Psi(x) = x^k, \quad gcd(k, n) = 1.$$

PROOF Suppose Ψ is an automorphism of $G = \langle a \rangle$. Since $\Psi(a) \in G$, there is a k so that $\Psi(a) = a^k$. It follows that

$$\Psi(a^2) = \Psi(a)\Psi(a) = a^k a^k = a^{2k}, \Psi(a^3) = \Psi(a)\Psi(a) = a^{2k}a^k = a^{3k}$$

and so on, so $\Psi(a^i) = a^{ik}$. It is now easy to check that $\Psi(a^i)\Psi(a^j) = \Psi(a^{i+j})$. The only condition we need to look at is that Ψ be a bijection, in other words,

$$\{e, a^k, a^{2k}, \ldots, a^{(n-1)k}\} = \{e, a, a^2, \ldots, a^{n-1}\}$$

This will happen if and only if the order of a^k in G is equal to n. But we have seen that this order is $\frac{n}{gcd(n,k)}$, so we get an automorphism if and only if $gcd(n, k) = 1$. If you didn't want to use the that theorem, you could say this: if there is an automorphism, there must be an r so that $a^{rk} = a$; that is, $rk \equiv 1 \mod n$, and this implies $gcd(k, n) = 1$. And, if $a^{rk} = a$, $(\Psi(a^r) = a)$, then $a^{(ir)k} = a^i$, or $\Psi(a^{ir}) = a^i$.

What are the automorphisms of $V = \{I, X, Y, Z\}$? If Ψ is an automorphism, then $\Psi(I) = I$, and it is easy to check that if

$$\{\Psi(X), \Psi(Y), \Psi(Z)\} = \{X, Y, Z\},$$

then Ψ will be an automorphism, so there are 3! different automorphisms.

It is not hard to show that for any group G, the set of automorphisms forms a group under composition. It is often called $Aut(G)$. I will only talk about this if there is class interest!

The last topic today is the subgroups of $C_2 \times C_4$. To simplify notation, write $C_2 = \{e, a\}$ and $C_4 = \{e, b, b^2, b^3\}$, where $a^2 = e$ and $b^4 = e$ (The identities are technically different.) If you prefer, you can make $a = [1]_2$ and $b = [1]_4$ as an arithmetic version of this

Then the elements of the group are

$$\{(e,e),(e,b),(e,b^2),(e,b^3),(a,e),(a,b),(a,b^2),(a,b^3)\}$$

What is the order of (a^j, b^k)? It's the smallest r so that

$$a^{jr} = e, b^{kr} = e \iff jr \equiv 0 \mod 2 \qquad kr \equiv 0 \mod 4.$$

It isn't terrible hard to see that (e,e) has order 1, (e,b^2),(a,e),(a,b^2) all have order 2, and the other elements: (e,b), (e,b^3), (a,b), (a,b^3) all have order 4. It follows that the subgroups of shape $\langle x \langle$ are:

$$\{(e,e)\},\{(e,e),(e,b^2)\},\{(e,e),(a,e)\},\{e,e),(a,b^2)\}$$
$$\{(e,e),(e,b),(e,b^2),(e,b^3)\},\{(e,e),(a,b),(e,b^2),(a,b^3)\}$$

A subgroup of $C_2 \times C_4$ will have order dividing $|C_2 \times C_4| = 8$, and so be 1,2,4,8. The only subgroup of order 1 is (e,e), and the only subgroup of order 8 is the whole group. Furthermore, if H is a subgroup of order 2, then it has to look like $\{(e,e), x\}$, where x has order 2, so it's in the list above. In the remaining case, H has order 4. If it has an element of order 4, then that's H, and it's in the list.

What's left? There are four elements of order less than four, and this is the only possibility. You've already proved that

$$\{(e,e),(e,b^2),(a,e),(a,b^2)\}$$

is a subgroup!

WORKSHEET PROBLEM

For a change, this one is a bit more theoretical. It's not hard if you follow the definitions carefully.

1. Prove that in any group, for any $g, h \in G$,

$$(gh)^{-1} = h^{-1}g^{-1}$$

Hint: Consider the product $(gh)(h^{-1}g^{-1})$ and apply associativity.

2. Suppose G is an *abelian* group and define $\Psi(g) = g^{-1}$. Prove that Ψ is an automorphism of G.

That is: prove that Ψ is a bijection and $\Psi(gh) = \Psi(g)\Psi(h)$ for all $g, h \in G$.

WORKSHEET SOLUTIONS

1. By associativity,

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.$$

2. If $g \in G$, then $g = (g^{-1})^{-1}$, hence $\Psi(g^{-1}) = g$, so Ψ is onto or surjective. If $\Psi(g) = \Psi(h)$, then $g^{-1} = h^{-1}$, so $g = (g^{-1})^{-1} = (h^{-1})^{-1} = h$, so Ψ is one-to-one or injective. Thus Ψ is a bijection.

Finally, since G is an abelian group,

$$\Psi(gh) = h^{-1}g^{-1} = g^{-1}h^{-1} = \Psi(g)\Psi(h).$$

Bonus. Suppose we don't know anything about G, but Ψ is an automorphism, then

$$\Psi(gh) = \Psi(g)\Psi(h) \implies h^{-1}g^{-1} = g^{-1}h^{-1}$$
$$\implies (h^{-1}g^{-1})^{-1} = (g^{-1}h^{-1})^{-1} \implies gh = hg.$$

So, if Ψ is an automorphism, then G is abelian.

September 23, 2020, in advance

We briefly talked about automorphisms on Monday, which are a special kind of isomorphism. Today, I want to talk about a generalization, the homomorphism. An isomorphism between two groups is a kind of mirror image. A homomorphism is more of a shadow. In addition, it has an unexpected connection with cosets.

Suppose $(G, *_G)$ and $(H, *_H)$ are two groups. The map $\phi : G \to H$ is called a *homomorphism* if, for all $g_1, g_2 \in G$, we have

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

We do not care about one-to-one or onto; if ϕ is a bijection between G and H, then it is also an isomorphism, but we do not assume this.

There is always a homomorphism between any two groups, but it might not be very interesting – if $\phi(g) = e_H$ for every $g \in G$, then ϕ is a homomorphism, because $e_h *_H e_H = e_H$.

If $G_1 < G$ is a subgroup of G, there is always a homomorphism from $G_1 \to G$ called the *inclusion* homomorphism, defined by $\phi(g) = g$. This isn't so interesting either.

Related to every homomorphism are two sets, which we'll later show are groups. The first is $Im(\phi) \subseteq H$, or the *image* of ϕ:

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

The second is $Ker(\phi) \subseteq G$, or the *kernel* of ϕ. (I'm not sure why it's called the kernel.) In matrix theory, this is the nullspace

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

It will turn out that, not only is $Ker(\phi)$ a subgroup of G, but its cosets have a particularly nice property. More later.

First a few examples. Let $G_1 = (\mathbb{Z}/2\mathbb{Z}, \oplus)$ and $G_2 = (\mathbb{Z}/6\mathbb{Z}, \oplus)$. (Equivalently, G_1 is the cyclic group $C_2 = \langle a \rangle, a^2 = e$ and G_2 is the cyclic group $C_6 = \langle b \rangle, b^6 = e$.)

Define $\phi_1 : G_1 \to G_2$ as follows:

$$\phi_1([0]_2) = [0]_6, \quad \phi_1([1]_2) = [3]_6.$$

Since $[0]_2 \mapsto [0]_6$, the only thing you need to check is

$$\begin{aligned}\phi_1([1]_2 + [1]_2) = \phi_1([2]_2) = \phi_1([0]_2) = [0]_6 \\ = [3]_6 + [3]_6 = \phi_1([1]_2) + \phi_1([1]_2).\end{aligned}$$

So ϕ_1 is a homomorphism. We have $Im(\phi) = \{[0]_6, [3]_6\}$ and $Ker(\phi) = \{[0]_2\}$. Alternatively, $\phi(e) = e, \phi(a) = b^3, Im(\phi) = \{e, b^3\}, Ker(\phi) = \{e\}$.

Now define an unrelated homomorphism $\phi_2 : G_2 \to G_1$ as follows

$$\begin{aligned}\phi_2([0]_6) = \phi_2([2]_6) = \phi_2([4]_6) = [0]_2; \\ \phi_2([1]_6) = \phi_2([3]_6) = \phi_2([5]_6) = [1]_2.\end{aligned}$$

That is, $\phi_2([i]_6) = [i]_2$. You should try to persuade yourself that this is a homomorphism, and we'll soon have an explanation why it always works.

The operation is "well-defined": $i \equiv j \mod 6 \implies i \equiv j \mod 2$. (This would not work with 6 replaced by 5: $\phi([i]_5) = [i]_2$ isn't even a function, because $[0]_5 = [5]_5$, but $[0]_2 \neq [5]_2$.)

We have $Im(\phi) = \{[0]_2, [1]_2\}$ and $Ker(\phi) = \{[0]_6, [2]_6, [4]_6\}$. In the other version

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

$Im(\phi) = \{e, a\}$, $Ker(\phi) = \{e, b^2, b^4\}$.

Here is a more general and completely typical example of a homomorphism. Suppose G and H are groups and consider the direct product $G \times H$. Define the *projection* maps $\phi_G : G \times H \to G$ and $\phi_H : G \times H \to H$ by:

$$\phi_G((g, h)) = g, \qquad \phi_H((g, h)) = h.$$

You are just taking the first (or second) component of the ordered pair. These are homomorphisms immediately from the definition of

$$(g_1, h_1) *_{G \times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

In this case, $Im(\phi_G) = G, Ker(\phi_G) = \{(e_G, h) : h \in H\}$, and similarly for ϕ_H. Always remember that the kernel is in the group you start with and the image is in the group you end with.

Two more examples: suppose $G = \mathbb{Z}$ and $H = \mathbb{Z}/n\mathbb{Z}$ as usual. Define ϕ by

$$\phi(m) = [m]_n$$

In other words, we map the integer m to m mod n. What is $Im(\phi)$? It's all of H, because $\phi(j) = [j]_n$ for $0 \leq j \leq n-1$, so we get everything. What is $Ker(\phi)$? Unpack this: what gets mapped to the identity in H; namely, $[0]_n$? It's the integers which are $\equiv 0$ mod n. That is, $Ker(\phi) = n\mathbb{Z}$.

Suppose $n \mid r$, and to be precise, $r = dn$. Then there is a homomorphism $\phi : \mathbb{Z}/(dn)\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, defined by $\phi([a]_{dn}) = [a]_n$. First, we have to check that this is "well-defined":

$$[a]_{dn} = [b]_{dn} \implies dn \mid b - a \implies (b - a) = dns$$
$$\implies n \mid b - a \implies [a]_n = [b]_n$$

Once you know that this is well-defined, you only have to check the operation:

$$\phi([a]_{dn} + [b]_{dn}) = \phi([a + b]_{dn}) = [a + b]_n$$
$$= [a]_n + [b]_n = \phi([a]_{dn}) + \phi([b]_{dn}).$$

This is ϕ_2 above with $dn = 6$ and $n = 2$.

Now, a (probably unsurprising) general result.

THEOREM If ϕ is a homomorphism from G to H, then $\phi(e_G) = e_H$, and for every $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

PROOF Since ϕ is a homomorphism, and e_G and e_H are the respective identities,

$$e_H *_H \phi(e_G) = \phi(e_G) = \phi(e_G *_G e_G) = \phi(e_G) *_H \phi(e_G).$$

By cancellation, $e_H = \phi(e_G)$. But now for $g \in G$,

$$e_H = \phi(e_G) = \phi(g *_G g^{-1}) = \phi(g) *_H \phi(g^{-1});$$

that is, $\phi(g)$ and $\phi(g^{-1})$ are inverses in H.

Using this information, we can quickly establish that $Im(\phi)$ and $Ker(\phi)$ are groups.

THEOREM If $\phi : G \to H$ is a homomorphism, then $Im(\phi)$ is a subgroup of H.

PROOF Since $e_H = \phi(e_G)$, $Im(\phi)$ contains the identity. If $h_1, h_2 \in Im(\phi)$, then there exist $g_1, g_2 \in G$ so that $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$, hence

$$h_1 *_H h_2 = \phi(g_1) *_H \phi(g_2) = \phi(g_1 *_G g_2) \in Im(\phi).$$

Thus, $Im(\phi)$ is closed under $*_H$. Finally, if $h \in Im(\phi)$, then $h = \phi(g)$, so $h^{-1} = \phi(g^{-1}) \in Im(\phi)$: that is, $Im(\phi)$ contains inverses. □

THEOREM If $\phi : G \to H$ is a homomorphism, then $Ker(\phi)$ is a subgroup of H.

PROOF First, $\phi(e_G) = e_H \in Ker(\phi)$. If $g_1, g_2 \in Ker(\phi)$, then $\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) = e_H *_H e_H = e_H$, so $g_1 *_G g_2 \in Ker(\phi)$ as well. Finally, if $g \in Ker(\phi)$, then $\phi(g^{-1}) = (\phi(g))^{-1} = e_H^{-1} = e_H$, so $g^{-1} \in Ker(\phi)$. $\square$

Not only is $Ker(\phi)$ a subgroup of G, but its cosets have a very special property. In the following, I write $K = Ker(\phi)$ and will no longer explicitly write $*_G$ and $*_H$; the correct subscript always can be found by context.

THEOREM Suppose $\phi : G \to H$ is a homomorphism with kernel K. Then for $a \in G$,

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

In other words, the left coset aK and the right coset Ka are equal to the preimage of $\phi(a)$; those elements in G which are mapped to $\phi(a)$.

PROOF If $x \in aK$, then $x = ak$, for some $k \in K$. Since ϕ is a homomorphism,

$$\phi(x) = \phi(ak) = \phi(a)\phi(k) = \phi(a)e_H = \phi(a).$$

(If $x \in Ka$, then $x = ka$, and the same proof goes through.)

Conversely, if $\phi(x) = \phi(a)$, then we can write $x = a(a^{-1}x)$, and

$$\phi(a) = \phi(x) = \phi(a(a^{-1}x)) = \phi(a)\phi(a^{-1}x) \implies \phi(a^{-1}x) = e_H$$

Thus, $a^{-1}x \in Ker(\phi) = K$, so $x \in aK$. Similarly, we can write $x = (xa^{-1})a$, show that $xa^{-1} \in K$, so $x \in Ka$. $\square$

The coset decomposition of G by K is determined by the values taken by ϕ. The fact that $aK = Ka$ for all a will be very significant!

Let's return to two of the examples. We had $\phi_2 : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ by

$$\phi_2([0]_6) = \phi_2([2]_6) = \phi_2([4]_6) = [0]_2;$$
$$\phi_2([1]_6) = \phi_2([3]_6) = \phi_2([5]_6) = [1]_2.$$

As previously noted, K $= Ker(\phi_2) = \{[0]_6, [2]_6, [4]_6\}$, and the cosets of K are

$$[0]_6 + K = \{[0]_6, [2]_6, [4]_6\} = \phi_2^{-1}(0),$$
$$[1]_6 + K = \{[1]_6, [3]_6, [5]_6\} = \phi_2^{-1}(1).$$

We also had $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(m) = [m]_n$, and saw that $Ker(\phi) = n\mathbb{Z}$. The cosets are $i + n\mathbb{Z} = [i]_n = \{m : m \equiv i \mod n\}$, as we've already seen.

Now a very important definition: if $G_1 \leq G$ is a subgroup, then G_1 is called a *normal* subgroup if $aG_1 = G_1a$ for every $a \in G$ (in words, "if every left coset of G_1 is also a right coset.") This does *not* mean that $ag = ga$ for every $g \in G_1$, but it does mean that the cosets are equal *as sets*.

The symbol for being a normal subgroup is $G_1 \trianglelefteq G$.

There are now three cases in which we know that $G_1 \trianglelefteq G$.

(i) If G is abelian, then $ag = ga$, so $aG_1 = G_1a$, element by element.

(ii) We just proved that if $\phi : G \to H$ is a homomorphism, then $Ker(\phi) \trianglelefteq G$.

What we will prove soon is the converse: if $G_1 \trianglelefteq G$, then there exists a group H and a homomorphism $\phi : G \to H$ so that $Ker(\phi) = G_1$. The group H will actually consist of the cosets of G_1.

(iii) There is one more case of normal subgroups that we've already discussed. Suppose $G_1 \leq G$ and $[G : G_1] = 2$. We've already seen a description of the two cosets of G_1:

$$G = eG_1 \cup aG_1 \implies aG_1 = G \setminus G_1;$$
$$G = G_1e \cup G_1a \implies G_1a = G \setminus G_1 \implies G_1a = aG_1.$$

The left cosets and the right cosets are each $\{G_1, G \setminus G_1\}$.

Can we find a homomorphism of G whose kernel is G_1? Sure! Let $H = C_2 = \{e, u\}, u^2 = e$ and define:

$$\phi(g) = e \quad \text{if } g \in G_1, \qquad \phi(g) = a \quad \text{if } g \notin G_1$$

Write $G = G_1 \cup aG_1 = G_1 \cup G_1a$.

If $g_1, g_2 \in G_1$, then $g_1g_2 \in G_1$, and

$$e = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = ee. \qquad \checkmark$$

If $g_1 \in aG_1$ and $g_2 \in G_1$, then $g_1 = ag_3$, with $g_3 \in G_1$, so $g_1g_2 = (ag_3)g_2 = a(g_3g_2) \in aG_1$ and

$$u = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = ue. \qquad \checkmark$$

If $g_1 \in G_1$ and $g_2 \in aG_1 = G_1a$, then $g_2 = g_3a$, with $g_3 \in G_1$, so $g_1g_2 = g_1(g_3a) = (g_1g_3)a \in G_1a = aG_1$ and

$$u = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = eu. \qquad \checkmark$$

Finally, if $g_1 \in G_1a$ and $g_2 \in G_1a = aG_1$, then $g_1 = g_3a$ and $g_2 = ag_4$, with $g_3, g_4 \in G_1$, so

$$u^2 = e = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = uu. \qquad \checkmark$$

You can also think of the multiplication table as being divided in two, with all the elements of G_1 in the left half and upper half, and the elements of aG_1 in the right half and lower half, and you get blocks like we've seen with S_3 and D_4.

It is helpful to have the following small result:

LEMMA If $a \in G$, $L = \{e, a\}$ is a normal subgroup of G if and only if $a^2 = e$ and, for every $g \in G$, $ag = ga$.

PROOF The condition $a^2 = e$ is necessary and sufficient for $\{e, a\}$ to be a subgroup, because by closure, $a^2 \in L$, and $a^2 = a = ae$ is impossible.

Now for $g \in G$, consider the left coset $gL = \{g, ga\}$ and the right coset $Lg = \{g, ag\}$. If these are equal, then $ga = ag$.

Conversely, if $ga = ag$ for all g, then every left coset of L is a right coset. □

Since every subgroup of an abelian group is normal, it's interesting to look at non-abelian groups. So far, we only know two of these: S_3 and D_4.

Through the miracle of cut and paste, here is S_3 again:

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$
$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$
$$\mu_2 = \begin{pmatrix}123\\321\end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix}123\\213\end{pmatrix} = (12)(3).$$

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

We've already seen that the proper subgroups of S_3 are $\{\rho_0, \rho_1, \rho_2\}$, which has order $3 = \frac{6}{2}$, and so is normal, and $\{\rho_0, \mu_1\}$, $\{\rho_0, \mu_2\}$, $\{\rho_0, \mu_3\}$, which have order 2.

In the first case, the cosets of $\{\rho_0, \rho_1, \rho_2\}$ are itself and the remaining elements $\{\mu_1, \mu_2, \mu_3\}$. As a reminder, in a normal subgroup, a left and a right coset are considered equal, even if the products aren't equal as you go along:

$$(\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2) = (\mu_1, \mu_2, \mu_3)$$
$$(\rho_0\mu_1, \rho_1\mu_1, \rho_2\mu_1) = (\mu_1, \mu_3, \mu_2).$$

We actually already know a homomorphism from $S_3 \to C_2 = \{e, a\}$, defined by

$$\phi(\rho_i) = e, \qquad \phi(\mu_i) = a,$$

Since $\rho_i\rho_j = \rho_k$, $\mu_i\mu_j = \rho_\ell$, $\rho_i\mu_j = \mu_m$, $\mu_i\rho_j = \mu_n$, we have that ϕ is a homomorphism. As an interpretation, if you think of S_3 as a symmetry

of the triangle, the μ_i's flip the front and the back, and the ρ_i's don't and a is the motion of the flip.

You may also vaguely remember that for the subgroups of order two, the left and right cosets are different. Here is an example with $G_1 = \{\rho_0, \mu_3\}$ and $a = \rho_1$:

$$aG_1 = \{\rho_1\rho_0, \rho_1\mu_3\} = \{\rho_1, \mu_2\}$$
$$G_1a = \{\rho_0\rho_1, \mu_3\rho_1\} = \{\rho_1, \mu_1\}.$$

These are different, so by our theorem, there is no homomorphism whose kernel is exactly $G_1 = \{\rho_0, \mu_3\}$. (Or, by (iv), because $\rho_1\mu_3 \neq \mu_3\rho_1$.)

I'll talk about D_4 in class, but here's something to think about. We already have found three subgroups of D_4 of order $4 = \frac{8}{2}$, and so they are normal. The question is: what is another way of describing these groups in terms of the motions of the square. We already know that $\{\rho_0, \rho_1, \rho_2, \rho_3\}$ represents the rotations, that keep the front and back in place. Can you describe the other two?

September 23, 2020, in class

Comments on the homework, taken from my email! The main issue seems to be cosets in problem 2. I'll quote "$G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, so the elements of G are $([i]_6, [j]_8)$, where $0 \leq i \leq 5$, $0 \leq j \leq 7$. Let $H = \{([0]_6, [0]_8), ([0]_6, [4]_8), ([3]_6, [0]_8), ([3]_6, [4]_8)\}$ be a subgroup of G." The operation is component-wise addition.

I won't give you a left coset, but I will give you a right coset. Just pick an element from G and combine it with the group. I'll pick $([4]_6, [7]_8)$ for the element. Then

$$H + ([4]_6, [7]_8) =$$
$$\{([0]_6, [0]_8) + ([4]_6, [7]_8), ([0]_6, [4]_8) + ([4]_6, [7]_8),$$
$$([3]_6, [0]_8) + ([4]_6, [7]_8), ([3]_6, [4]_8) + ([4]_6, [7]_8)\} =$$
$$\{([4]_6, [7]_8), ([4]_6, [11]_8), ([7]_6, [7]_8), ([7]_6, [11]_8)\} =$$
$$\{([4]_6, [7]_8), ([4]_6, [3]_8), ([1]_6, [7]_8), ([1]_6, [3]_8)\}.$$

This is also $H + ([1]_6, [3]_8)$. The last remark is based on the fact that $a \in Ha$ (or aH) for every coset. If H is a subgroup, then $e \in H$ and if $H = \{e, h_2, \ldots, h_n\}$ then

$$aH = \{ae, \ldots, ah_n\}$$

But different elements give the same coset. We have $ah_i \in aH$.

What is the left coset associated to ah_i?

$$(ah_i)H = \{ah_ie, ah_ih_1, \ldots, ah_ih_n\}$$

On the one hand, we can quote a theorem that $ah_i \in aH \cap (ah_i)H$, so that $aH = (ah_i)H$. Or we can give the proof of the theorem in this case. We see that $ah_ih_j \in aH$, so $(ah_i)H \subseteq aH$, but also $ah_j = (ah_i)(h_i^{-1}h_j)$, so $aH \subseteq (ah_i)H$.

I'd like to redo that botched example, as also a review of subgroups, cosets and homomorphisms.

Suppose $K < G$ and $[G : K] = 2$, which means that, if G is a finite group, $|K| = \frac{1}{2}|G|$, and in any case, that G can be written as a disjoint union of two cosets of K. Suppose $a \in G \setminus K$; that is, $a \in G$, $a \notin K$. Since $a \notin K$ and $a = ae \in aK$ and $a = ea \in Ka$, the left coset aK and the right coset Ka are different from K, and by an earlier result, disjoint from K. Thus we can write

$$G = K \cup aK, \quad G = K \cup Ka, \quad (\implies aK = Ka = G \setminus K).$$

One thing I didn't mention but should have is this: $a^2 \in G$, because G is closed under its operation. If $a^2 \in aK$, then $a^2 = ak$ for some $k \in K$. But this implies that $a = k \in K$, which is impossible. Therefore, $a^2 \in K$.

I now want to look at where products of elements go. There are four cases: (i) $gh, g \in K, h \in K$, (ii) $gh, g \in K, h \in aK = Ka$, (iii) $gh, g \in aK = Ka, h \in K$, (iv) $gh, g \in aK = Ka, h \in aK = Ka$.

For (i), if $g, h \in K$, then $gh \in K$ because K is a subgroup.

For (ii), write $h = ka, k \in K$, then $gh = g(ka) = (gk)a \in Ka$, because $g, k \in K$.

For (iii), write $g = ak, k \in K$, then $gh = (ak)h = a(kh) \in aK$, because $k, h \in K$.

For (iv), write $g = k_1a, k_1 \in K$ and $h = ak_2, k_2 \in K$. Then $gh = (k_1a)(ak_2) = k_1a^2k_2$ is a product of three elements in K, so $gh \in K$.

This pattern is one we have seen in S_3, where K consists of the ρ_i's and aK consists of the μ_i's.

Now (and only now) will I define a homomorphism: Let $C_2 = \{e, u\}$ be a cyclic group of order 2, so $u^2 = e$, and define $\phi : G \to C_2$ by $\phi(x) = e$ if $x \in K$ and $\phi(x) = u$ if $x \in aK = Ka$. I need to check that $\phi(gh) = \phi(g)\phi(h)$ for $g, h \in K$ and there are the four cases noted above.

In (i), $g, h, gh \in K$, so $\phi(g) = e, \phi(h) = e, \phi(gh) = e$.

In (ii), $g \in K, h \in Ka, gh \in Ka$, so $\phi(g) = e, \phi(h) = u, \phi(gh) = u$.

In (iii), $g \in aK, h \in K, gh \in aK$, so $\phi(g) = u, \phi(h) = e, \phi(gh) = u$.

In (iv), $g \in aK, h \in Ka, gh \in K$, so $\phi(g) = u, \phi(h) = u, \phi(gh) = e$.

Since $u^2 = e$, ϕ has been shown to be a homomorphism, and

$$Ker(\phi) = \{x \in G \mid \phi(x) = e\} = K.$$

This is what we wanted. We will have a more general version of this construction in a short while (not today).

The other topic I wanted to talk about involved the subgroups of D_4 of order four. As a reminder, here are the elements in the group:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4) \quad \rho_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = (1234),$$

$$\rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24) \quad \rho_3 = \begin{pmatrix}1234\\4123\end{pmatrix} = (1432),$$

$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$

$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3),$$

One of the subgroups of order four is

$$\{\rho_0, \rho_1, \rho_2, \rho_3\} = \langle\rho_1\rangle = \langle\rho_3\rangle.$$

This group can be interpreted as the rotations of the square, or the motions which keep the front to the front.

The other subgroups are isomorphic to V: $\{\rho_0, \rho_2, \mu_1, \mu_2\}$ and $\{\rho_0, \rho_2, \delta_1, \delta_2\}$. Can these be understood in terms of motions? Let me put the squares in the first case.

$$\rho_0 = \begin{matrix}1&2\\4&3\end{matrix} \quad \rho_2 = \begin{matrix}3&4\\2&1\end{matrix} \quad \mu_1 = \begin{matrix}2&1\\3&4\end{matrix} \quad \mu_2 = \begin{matrix}4&3\\1&2\end{matrix}$$

Can you see the common feature of these rotations?

What I see is that the horizontal edges (12 and 34) stay horizontal, and the vertical edges stay vertical. In the other coset,

$$\rho_1 = \begin{matrix}4&1\\3&2\end{matrix} \quad \rho_3 = \begin{matrix}2&3\\1&4\end{matrix} \quad \delta_1 = \begin{matrix}3&2\\4&1\end{matrix} \quad \delta_2 = \begin{matrix}1&4\\2&3\end{matrix}$$

the horizontal edges all go vertical, and the vertical edges go horizontal.

What do you see in the third subgroup?

$$\rho_0 = \begin{matrix}1&2\\4&3\end{matrix} \quad \rho_2 = \begin{matrix}3&4\\2&1\end{matrix} \quad \delta_1 = \begin{matrix}3&2\\4&1\end{matrix} \quad \delta_2 = \begin{matrix}1&4\\2&3\end{matrix}$$

What I see is that the diagonals are preserved: (13) stay in the (13) positions and (24) in the (24) positions.

In the coset, the diagonals are flipped.

$$\rho_1 = \begin{matrix} 4 & 1 \\ 3 & 2 \end{matrix} \qquad \rho_3 = \begin{matrix} 2 & 3 \\ 1 & 4 \end{matrix} \qquad \mu_1 = \begin{matrix} 2 & 1 \\ 3 & 4 \end{matrix} \qquad \mu_2 = \begin{matrix} 4 & 3 \\ 1 & 2 \end{matrix}$$

WORKSHEET QUESTION

1. Suppose $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ is a homomorphism. We know that $\phi([0]_6) = [0]_4$. There are four possible choices for $\phi([1]_6)$:

(a) $\phi_0([1]_6) = [0]_4$,
(b) $\phi_1([1]_6) = [1]_4$,
(c) $\phi_2([1]_6) = [2]_4$,
(d) $\phi_3([1]_6) = [3]_4$,

Show that ϕ_0 and ϕ_2 are homomorphisms and, using the property of homomorphisms, write out $\phi_0([a]_6)$ and $\phi_2([a]_6)$. Determine the images and kernels.

Also, by considering the equation

$$[1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6 = [0]_6,$$

show that ϕ_1 and ϕ_3 are not homomorphisms

WORKSHEET SOLUTION

(a) We have already seen ϕ_0: $\phi_0([a]_6) = [0]_4$ for all a, so the kernel is $\mathbb{Z}/6\mathbb{Z}$ and the image is $\{[0]_4\}$.

(c) Here, we have $\phi_2([0]_6) = [0]_4$ and $\phi_2([1]_6) = [2]_4$, additivity implies that $\phi_2([2]_6) = [0]_4$, $\phi_2([3]_6) = [2]_4$, $\phi_2([4]_6) = [0]_4$, $\phi_2([5]_6) = [2]_4$. In words (though this wasn't asked), $\phi_2([a]_6) = [2a]_4$. The kernel is $\{[0]_6, [2]_6, [4]_6\}$ and the image is $\{[0]_4, [2]_4\}$

(b) and (d) The problem is that if ϕ is a homomorphism, then

$$\begin{aligned} \phi([0]_6) &= \phi([1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6 + [1]_6) \\ &= \phi([1]_6) + \phi([1]_6) + \phi([1]_6) + \phi([1]_6) + \phi([1]_6) + \phi([1]_6) \\ &= 6\phi([1]_6). \end{aligned}$$

And if $\phi = \phi_1([1]_6 = [1]_4$, then $[0]_4 \neq 6[1]_4 = [6]_4$. Similarly, if $\phi = \phi_3([1]_6 = [3]_4$, then $[0]_4 \neq 6[3]_4 = [18_4$.

Yes, there's a general theorem lurking here.

September 25, 2020, in advance

A couple more general things about homomorphisms.

THEOREM If $\phi : G \to H$ is a homomorphism from the group G to the group H, then for $n \geq 2$ and $g_j \in G$,

$$\phi(g_1 *_G g_2 *_G \cdots *_G g_n) = \phi(g_1) *_H \phi(g_2) *_H \cdots *_H \phi(g_n).$$

PROOF The proof is by induction on n. The base case is $n = 2$, and comes from the definition of homomorphism. Assuming the result

is true for n, then

$$\phi(g_1 *_G g_2 *_G \cdots *_G g_n *_G g_{n+1}) =$$
$$\phi((g_1 *_G g_2 *_G \cdots *_G g_n) *_G g_{n+1}) =$$
$$\phi(g_1 *_G g_2 *_G \cdots *_G g_n) *_H \phi(g_{n+1})$$
$$= (\phi(g_1) *_H \phi(g_2) *_H \cdots *_H \phi(g_n)) *_H \phi(g_{n+1})$$
$$= \phi(g_1) *_H \phi(g_2) *_H \cdots *_H \phi(g_n) *_H \phi(g_{n+1}). \quad \square$$

There is a bit of confusion about the relationship between isomorphisms and homomorphisms, so here is the connection.

THEOREM If $\phi : G \to H$ is a homomorphism from the group G to the group H, then ϕ is an isomorphism if and only if $Ker(\phi) = \{e_G\}$ and $Im(\phi) = H$.

PROOF For ϕ to be an isomorphism, it needs to be a bijection from G to H and satisfy $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

The second criterion is automatic with a homomorphism. Also, by definition, ϕ is onto if and only if $Im(\phi) = G$. If ϕ is one-to-one, then, since $\phi(e_G) = e_H$, it must be the only element that goes to e_H; that is, $Ker(\phi) = \{e_G\}$.

Conversely, suppose $Ker(\phi) = \{e_G\}$ and $\phi(g_1) = \phi(g_2) \in H$. Then $\phi(g_1^{-1}) = \phi(g_1)^{-1} \in H$, and

$$\phi(g_1^{-1} *_G g_2) = \phi(g_1^{-1}) *_H \phi(g_2) =$$
$$\phi(g_1)^{-1} *_H \phi(g_2) = \phi((g_1)^{-1}) *_H \phi(g_1) = e_H,$$

so $g_1^{-1} *_G g_2 \in Ker(\phi)$. Thus $g_1^{-1} *_G g_2 = e_G$, and so, by multiplying on the left by g_1, we get $g_2 = g_1$. That is, $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$, so ϕ is injective, or one-to-one. $\square$

Suppose $\phi : G \to H$ is a homomorphism. Then it is relatively easy to show that ϕ preserves the subgroup structures of both G and H.

THEOREM If $G_1 < G$, then

$$\phi(G_1) := \{\phi(g) \ : \ g \in G_1\}$$

is a subgroup of H.

PROOF We know the drill. Since $e_G \in G_1$, $\phi(e_G) = e_H \in \phi(G_1)$. If $h_1, h_2 \in \phi(G_1)$, then there exist $g_1, g_2 \in G_1$ so that $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$. Since G_1 is a subgroup, $g_1 *_G g_2 \in G_1$, so $\phi(G_1)$ contains

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) = h_1 *_H h_2,$$

thus $\phi(G_1)$ is closed under the operation of H. Finally, if $h \in \phi(G_1)$, then $h = \phi(g)$ for some $g \in G_1$. Thus $\phi(g^{-1}) = (\phi(g))^{-1} \in \phi(G_1)$. $\square$

THEOREM If $H_1 \leq Im(\phi)$, then the inverse image of H_1

$$\phi^{-1}(H_1) := \{g \in G \mid \phi(g) \in H_1\}$$

is a subgroup of G.

PROOF. Again, H_1 is a subgroup, so $e_H \in H_1$ and $\phi(e_G) = e_H$ implies that $e_G \in \phi^{-1}(H_1)$. If $g_1, g_2 \in \phi^{-1}(H_1)$, then $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$, with $h_1, h_2 \in H_1$. Since $h_1 *_H h_2 \in H_1$ and $\phi(g_1 *_G g_2) = h_1 *_H h_2 \in H_2$, it follows that $g_1 *_G g_2 \in \phi^{-1}(H_1)$. And if $g \in \phi^{-1}(H_1)$, then $\phi(g) \in H_1$, so $\phi(g)^{-1} = \phi(g^{-1}) \in H_1$, so $g^{-1} \in \phi^{-1}(H_1)$. □

The next theorem is one you will probably think is obvious, but it needs to be written. It's kind of boring, to be sure.

THEOREM If G, H, K are groups and $\phi_1 : G \to H$ is a homomorphism and $\phi_2 : H \to K$ are both homomorphisms, then the composition map $\phi : G \to K$ defined by $\phi(g) = \phi_2(\phi_1(g))$ is also a homomorphism.

PROOF For clarity, if $g \in G$, then $\phi_1(g) \in H$ so $\phi_2(\phi_1(g)) \in K$. All we have to do is check that products go through. This will be true because the intermediate maps are homomorphisms. For $g_1, g_2 \in G$,

$$\begin{aligned}\phi(g_1 *_G g_2) &= \phi_2(\phi_1(g_1 *_G g_2)) = \phi_2(\phi_1(g_1) *_H \phi_1(g_2)) \\ &= \phi_2(\phi_1(g_1)) *_K \phi_2(\phi_1(g_2)) = \phi(g_1) *_K \phi(g_2).\end{aligned}$$

Thus, ϕ is a homomorphism. □

As a remark, this result can be generalized to chain homomorphisms with more than three groups by an even-more boring induction that will be omitted.

COROLLARY Suppose G_1 and G_2 are groups with an isomorphism $\Phi_G : G_1 \to G_2$ and H_1 and H_2 are groups with an isomorphism $\Phi_H : H_1 \to H_2$. Suppose also that $\phi : G_1 \to H_1$ is a homomorphism, then there is an *induced* homomorphism $\phi' : G_2 \to H_2$, defined for $g \in G_2$

$$\phi'(g) = \Phi_H(\phi(\Phi_G^{-1}(g))).$$

PROOF Yes, I know this looks horrible, but let's keep track of things: $g \in G_2$ so $\Phi_G^{-1}(g) \in G_1$ (notice that $\Phi_G : G_1 \to G_2$ is a bijection, so it has an inverse $\Phi_G^{-1} : G_2 \to G_1$.) Once we know that $\Phi_G^{-1}(g) \in G_1$, then we can apply our homomorphism $\phi : G_1 \to H_1$ and $\phi(\Phi_G^{-1}(g)) \in H_1$. The last function is Φ_H which takes this to H_2. This is then an example of the last theorem, with a composition of three homomorphisms. □

By switching the indices, any homomorphism $\tilde{\phi} : G_2 \to H_2$ can be made to induce a homomorphism $\tilde{\phi}' : G_1 \to H_1$.

Why do we do this?

We have talked about homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$, but these are isomorphic to the cyclic groups C_n and C_m respectively, and

I'd rather talk about homomorphisms with the cyclic groups, because later in the semester we'll be talking about *ring* homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$, and it can get confusing otherwise.

This turns out to be a number-theoretic question. What are the possible homomorphisms from one cyclic group to another? To be specific, suppose $G = C_n = \langle a\rangle, a^n = e_G$ and $H = C_m = \langle b\rangle, b^m = e_H$.

In any case, we know that $\phi(e_G) = e_H$. Define ϕ_k by $\phi_k(a) = b^k$, where $0 \le k \le m-1$. (Since $\phi(a) \in H$, it has to be a power of b.) Then the property of homomorphisms implies that

$$\phi_k(a^2) = \phi_k(aa) = \phi_k(a)\phi_k(a) = b^k b^k = b^{2k},$$
$$\phi_k(a^3) = \phi_k(a^2a) = \phi_k(a^2)\phi_k(a) = b^{2k}b^k = b^{3k},$$

and so on. It is easy to establish by induction that

$$\phi_k(a^r) = b^{kr} \implies \phi_k(a^r * a^s) = \phi_k(a^{r+s})$$
$$= b^{k(r+s)} = \phi_k(a^r)\phi_k(a^s).$$

So we're fine, except that we have to check that we actually have a well-defined map. That is, is it true that

$$a^r = a^s \implies \phi(a^r) = \phi(a^s) \iff b^{kr} = b^{ks}?$$

Now $a^r = a^s \iff r \equiv s \mod n \iff n \mid s-r$, and $b^{kr} = b^{ks} \iff kr \equiv ks \mod m \iff m \mid ks - kr = k(s-r)$. This is a number-theory problem. When does $n \mid s-r$ imply $m \mid k(s-r)$?

The hypothesis is that $n \mid s-r$; that is, $s - r = nt$ for some integer t. The conclusion is

$$m \mid k(s-r) = knt$$

for all t. In particular, it holds for $t = 1$; that is, $m \mid kn$, and if $m \mid kn$, then $m \mid knt$ for all t.

Putting this together, we have now proved

THEOREM The homomorphisms from C_n to C_m are given precisely by $\phi(a^r) = b^{kr}$, under the condition that $m \mid kn$.

For example, if $n = 6$ and $m = 4$, the choice for k is $k \in \{0, 1, 2, 3\}$, and we want to know when $4 \mid 6k$.

Since C_k is isomorphic to $\mathbb{Z}/k\mathbb{Z}$, this will also tell us all homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. We saw in Wednesday's Worksheet Problem with $n = 6$ and $m = 4$, that a homomorphism exists for $k = 0, 2$ and not $k = 1, 3$.

There is one special case with an interesting result.

COROLLARY If $gcd(m,n) = 1$, then the only homomorphism from C_n to C_m is the trivial one.

PROOF As we've seen, $\phi(a^r) = b^{kr}$, but we need $m \mid kn$. Since $gcd(m,n) = 1$, a property of relatively prime integers is that $m \mid kn \implies m \mid k$, so $k = um$, and for every r,

$$\phi(a^r) = b^{kr} = b^{umr} = (b^m)^{ur} = e_H^{ur} = e_H$$

In other words, the only homomorphism maps everything to the identity. □

The full story is a bit messy.

COROLLARY Suppose $gcd(m,n) = g$, then the homomorphisms from C_n to C_m are given precisely by $\phi(a^r) = b^{kr}$, under the condition that k is a multiple of m/g. There are exactly g such homomorphisms.

PROOF Write $m = gm'$ and $n = gn'$, where $gcd(m',n') = 1$. The condition $m \mid kn$ is equivalent to

$$\frac{kn}{m} \in \mathbb{Z} \iff \frac{kgn'}{gm'} \in \mathbb{Z} \iff \frac{kn'}{m'} \in \mathbb{Z} \iff m' \mid kn'.$$

But $gcd(m',n') = 1$, so this last condition is that k is a multiple of

$$m' = \frac{m}{g} = \frac{m}{gcd(m,n)}.$$

Since $0 \le k < m$ and $k = im'$, $0 \le im' < m = gm'$, so $0 \le i < g$ and $i \in \{0, 1, \ldots, g-1\}$. □

On the last Worksheet, k is a multiple of $\frac{4}{gcd(4,6)} = 4/2 = 2$, as we saw. If we had wanted homomorphisms from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/6\mathbb{Z}$ instead, then k must be a multiple of $\frac{6}{gcd(6,4)} = 6/2 = 3$: $k = 0, 3$.

The final topic will continue on Monday. Suppose that A and B are subsets of a group $(G, *)$, which might be finite or infinite. The *set product* $A * B$ is defined as

$$A = \{a_i\}, \quad B = \{b_i\} \implies A * B = \{a_j * b_k\}.$$

Usually, G will be finite, but there will be one simple and important exception later.

Suppose now that G is a group and $N \trianglelefteq G$ is a normal subgroup: for every $a \in G$, $aN = Na$; that is, every left coset is a right coset.

LEMMA If $N \trianglelefteq G$ is a normal subgroup, then for every $g \in G$ and $x \in N$, there exists $y \in N$ so that $g*x = y*g$; that is, $g*x*g^{-1} = y \in N$.

PROOF Consider the coset gN. By hypothesis, $g * x \in gN$, but $gN = Ng$, so $g*x \in Ng$. This means that $g*x = y*g$ for some $y \in N$.

We can solve for y by multiplying by g^{-1} on the right: $(g*x)*g^{-1} = (y*g)*g^{-1} = y*(g*g^{-1}) = y \in N$. $\square$

If G is abelian, then $y = g*x*g^{-1} = g*g^{-1}*x = x$, and this is no big deal. Matrix fans will recognize conjugation.

THEOREM Under the definition of set products, if $N \trianglelefteq G$ and aN and bN are two cosets of N, then $(aN)*(bN) = (a*b)N$.

(This is an amazing theorem. If $|N| = t$, then aN and bN each have t elements, and we'd expect t^2 products, not t. Please note n is a group element, not a natural number!)

PROOF If $x \in (a*b)N$, then $x = (a*b)*n$ for some $n \in N$. Thus $x = (a*e_G)*(b*n) \in (aN)*(bN)$. This shows that $(a*b)N \subseteq (aN)*(bN)$.

To prove the other direction, suppose $x \in (aN)*(bN)$. Then there exist $n_1, n_2 \in N$ so that $x = (a*n_1)*(b*n_2)$. By the Lemma, $n_1*b = b*n_3$ for some $n_3 \in N$, and we then use associativity:

$$\begin{aligned}(a*n_1)*(b*n_2) &= a*(n_1*b)*n_2 = a*(b*n_3)*n_1 \\ &= (a*b)*(n_3*n_1) \in (a*b)N \quad \square\end{aligned}$$

Here is an example from a friendly group. Let $G = C_6 = \langle a \rangle$, $a^6 = e$ and let $N = \langle a^3 \rangle = \{e, a^3\}$. Since G is abelian and N is a subgroup, it is a normal subgroup. The cosets of N are:

$$N = a^3N = \{e, a^3\},\ aN = a^4N = \{a, a^4\},\ a^2N = a^5N = \{a^2, a^5\}.$$

I won't do all the products, but I hope you can see that

$$N*aN = \{a, a^4, a^4, a^7\} = \{a, a^4, a^4, a\} = \{a, a^4\} = aN$$

and

$$aN*a^2N = \{a^3, a^6, a^6, a^9\} = \{a^3, e, e, a^3\} = \{e, a^3\} = a^3N = N$$

The next step is to prove that this definition can be used to define a group whose elements consist of the cosets of N with the operation done above. That will have to wait for Monday.

Back to D_4:

$$\rho_0 = \begin{pmatrix}1234\\1234\end{pmatrix} = (1)(2)(3)(4) \quad \rho_1 = \begin{pmatrix}1234\\2341\end{pmatrix} = (1234),$$
$$\rho_2 = \begin{pmatrix}1234\\3412\end{pmatrix} = (13)(24) \quad \rho_3 = \begin{pmatrix}1234\\4123\end{pmatrix} = (1432),$$
$$\mu_1 = \begin{pmatrix}1234\\2143\end{pmatrix} = (12)(34), \quad \mu_2 = \begin{pmatrix}1234\\4321\end{pmatrix} = (14)(23),$$
$$\delta_1 = \begin{pmatrix}1234\\3214\end{pmatrix} = (13)(2)(4), \quad \delta_2 = \begin{pmatrix}1234\\1432\end{pmatrix} = (1)(24)(3),$$

You may recall that we found that $N = \{\rho_0, \rho_2\}$ is a normal subgroup of D_4 and we had a special version of the multiplication table of D_4.

D_4	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_2	ρ_1	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_2	ρ_2	ρ_0	ρ_3	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_1	ρ_1	ρ_3	ρ_2	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_3	ρ_3	ρ_1	ρ_0	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	μ_2	δ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	μ_1	δ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	δ_2	μ_1	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	δ_1	μ_2	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

The cosets of N are N, $\rho_1 N$, $\mu_1 N$, $\delta_1 N$ and the elements in the products of the cosets occupy the 2×2 blocks of the 8×8 multiplication table. This is what the products look like

$\circ$	N	$\rho_1 N$	$\mu_1 N$	$\delta_1 N$
N	N	$\rho_1 N$	$\mu_1 N$	$\delta_1 N$
$\rho_1 N$	$\rho_1 N$	N	$\delta_1 N$	$\mu_1 N$
$\mu_1 N$	$\mu_1 N$	$\delta_1 N$	N	$\rho_1 N$
$\delta_1 N$	$\delta_1 N$	$\mu_1 N$	$\rho_1 N$	N

Each entry above represents a 2×2 square. If the coset is $\{x, y\}$, then the square is one of the following two entries

$$\begin{pmatrix}\text{x y}\\\text{y x}\end{pmatrix} \quad \text{or} \begin{pmatrix}\text{y x}\\\text{x y}\end{pmatrix}.$$

This sure looks like V to me.

September 25, 2020, in class

All I have for you today is one example. What happens with multiplication when you take the cosets of a subgroup that *isn't* normal?

Since every subgroup of an abelian group is normal, we don't have much choice. We only know two non-abelian groups: S_3 and D_4.

As a reminder:

$$\rho_0 = \begin{pmatrix}123\\123\end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix}123\\231\end{pmatrix} = (123),$$
$$\rho_2 = \begin{pmatrix}123\\312\end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix}123\\132\end{pmatrix} = (1)(23),$$
$$\mu_2 = \begin{pmatrix}123\\321\end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix}123\\213\end{pmatrix} = (12)(3).$$

Let's take one of the subgroups of order two: $H = \{\rho_0, \mu_1\}$ and calculate the left cosets. Here they are:

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

What happens when we take the products?

$$\rho_0 H \rho_0 H = \{\rho_0^2, \rho_0\mu_1, \mu_1\rho_0, \mu_1^2\} = \{\rho_0, \mu_1, \mu_1, \rho_0\}$$
$$= \{\rho_0, \mu_1\} = \rho_0 H.$$

But that's the "easy one", because we are multiplying within a subgroup.

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

This is not a coset! It happens to be the union of two cosets.

I'll do one more:

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

Again, there are four different elements, and this is not a coset.

If you find this interesting, you could try to compute the other products.