Math 375
Week 6

6.1 Homomorphisms and Isomorphisms

DEFINITION 1 *Let G_1 and G_2 groups and let $\phi : G_1 \to G_2$ be a function. Then ϕ is a **group homomorphism** if for every $a,\ b \in G$ we have*

$$\phi(ab) = \phi(a)\phi(b).$$

REMARK 1 Notice that the operation on the left is occurring in G_1 while the operation on the right is occurring in G_2.

REMARK 2 Notice the similarity to the definition of a linear transformation from Math 204. I encourage you to look this up in your 204 text. This means that you can multiply before or after you apply the mapping ϕ and you will still get the same answer. This is great, you can't make a mistake here because the order of operations (mapping versus multiplication) does not matter.

EXAMPLE 1 Consider the following maps

a) Is the mapping $\phi : GL(n, \mathbf{R}) \to \mathbf{R}^*$ by $\phi(A) = \det A$ a homomorphism? Yes.

b) Let a be a fixed element of G. Is $\phi : G \to G$ by $g\phi = aga^{-1}$ a homomorphism? [Homework]

c) Is the mapping $f : \mathbf{R} \to \mathbf{R}^*$ by $f(x) = e^x$ a group homomorphism? Be careful: What are the group operations in each case?

d) Let a be a fixed element of G. Is $\phi : G \to G$ by $\phi(g) = ag$ a homomorphism? No.

e) Here's a silly example: Let G_1 and G_2 groups and let $\phi : G_1 \to G_2$ by $\phi(g) = e_2$ for all $g \in G$. Obviously, $\phi(ab) = e_2 = e_2e_2 = \phi(b)\phi(b)$, so this is a group homomorphism.

f) Recall that S_3 is the set of all permutations of the set By labelling the vertices of an equilateral triangle 1, 2, and 3 as usual, we can interpret the elements of D_3 as maps from S to S. Match up the elements of D_3 with their corresponding elements in S_3.

Example 2 **Extra Credit:** Label the vertices of a tetrahedron with 1, 2, 3, 4. Let G be the set of rotations and reflections of the tetrahedron. Write out each such rotation as an element of S_4. Do you get all elements of S_4 this way? See page 101 and 102 in your text. (It turns out that this pairing is a group homomorphism, indeed, an isomorphism.)

Theorem 2 ***(Basic Properties of Homomorphisms)*** *If $\phi : G_1 \to G_2$ is a group homomorphism, then*

- ***a)*** $\phi(e_1) = e_2$;
- ***b)*** $\phi(a^{-1}) = [\phi(a)]^{-1}$;
- ***c)*** $\phi(a^n) = [\phi(a\phi)]^n$ *for all* $n \in \mathbf{Z}$;
- ***d)*** *if* $|a| = n$, *then* $|\phi(a)|\Big| n$, *i.e.,* $|\phi(a)|\Big||a|$.

PROOF A Note that $\phi(e_1) = \phi(e_1e_1) = \phi(fe_1)\phi(e_1)$ so that by cancellation $e_2 = \phi(e_1)$. [Remember, this is all taking place in G_2.]

PROOF B We prove that something is an inverse by showing that it acts like an inverse. So

$$e_2 = \phi(e_1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}).$$

So $f(a^{-1})$ acts as the inverse to $f(a)$, i.e., $\phi(a^{-1}) = [\phi(a)]^{-1}$.

PROOF C Homework.

PROOF D Because $|a| = n$, then $a^n = e_1$. So

$$e_2 = \phi(e_1) = \phi(a^n) = [\phi(a)]^n.$$

By the Corollary on page 73, $|\phi(a)|\Big| n$.

Example 3 Suppose that $\phi : \mathbf{Z}_3 \to D_4$ is a homomorphism. Can $\phi(1) = r_{90}$?

SOLUTION No. Because the last part of the theorem we need $|\phi(1)|\Big||1|$ or but $|r_{90}| = 4 \not| 3 = |1|$.

Example 4 Let's continue with $\phi : \mathbf{Z}_3 \to D_4$. What can you say about this homomorphism?

SOLUTION Since the orders of elements in D_4 are either 1, 2, or 4, the only such order which divides $|1| = 3$ is 1. So, $\phi(1) = r_0$. But then part (b) of the theroem above, $\phi(2) = \phi(-1) = [\phi(1)]^{-1} = r_0^{-1} = r_0$. Of course, by part (a) of the theorem, $\phi(0) = r_0$. So every element in $\mathbf{Z}_3$ must be mapped to r_0. This is the silly example discussed above.

Let's prove something a bit more interesting about homomorphisms of (finite) cyclic groups. Suppose that $G =< a >$ is cyclic and $\phi : G \to H$

is a group homomorphism. Notice that ϕ is completely determined by where ϕ maps a. Because any element $g \in G$ is of the form $g = a^k$, so $\phi(g) = \phi(a^k) = [\phi(a)]^k$. Once we know what $\phi(a)$ is, we know what ϕ is. What are the choices for $\phi(a)$?

EXAMPLE 5 Her's the sort of thing I mean. Let's assume $\phi : \mathbf{Z}_8 \to \mathbf{Z}_4$ is a homomorphism. Suppose that $\phi(1_8) = 3_4$. Then the rest of ϕ is now completely determined because $\mathbf{Z}_8 =< 1_8 >$. We (because ϕ is a homomorphism)

$$\begin{aligned}
\phi(1_8) &\to 3_4 \\
\phi(2_8) = \phi(1_8 + 1_8) &\to 3_4 + 3_4 = 2_4 \\
\phi(3_8) = \phi(1_8 + 2_8) &\to 3_4 + 2_4 = 1_4 \\
\phi(4_8) = \phi(1_8 + 3_8) &\to 3_4 + 1_4 = 0_4 \\
\phi(5_8) = \phi(1_8 + 4_8) &\to 3_4 + 0_3 = 3_4 \\
\phi(6_8) = \phi(1_8 + 5_8) &\to 3_4 + 3_4 = 2_4 \\
\phi(7_8) = \phi(1_8 + 6_8) &\to 3_4 + 2_4 = 1_4 \\
\phi(0_8) = \phi(1_8 + 7_8) &\to 3_4 + 1_4 = 0_4
\end{aligned}$$

Or one could use $\phi(j_8) = \phi(j \cdot 1_8) \to j \cdot 3_4$ to get the same answers.

Ok, let's generalize finite case first.

LEMMA 3 *Let $G =< a >$ be a cyclic group of order n. Let $\phi : G \to H$ be a function such that $\phi(a^i) = \phi(a)^i$ for all i. If $|\phi(a)| \,\big|\, n$, then ϕ is a group homomorphism.*

PROOF Note from parts (c) and (d) of the previous theorem, if ϕ is a homomorphism, then these two properties must be true. This says that these two properties suffice to make ϕ a homomorphism when G is cyclic.

Let $|\phi(a)| = m$. Then we are given that $m \mid n$, so $n = md$ for some $d \in \mathbf{Z}$. Let $x, y \in G$. We must show that $\phi(xy) = \phi(x)\phi(y)$. But G is cyclic so $x = a^j$ and $y = a^k$ with $0 \le k, j < n$. Then $xy = a^j a^k = a^{j+k \bmod n}$. So

$$\phi(xy) = \phi(a^{j+k \bmod n}) = [\phi(a)]^{(j+k \bmod n) \bmod m}.$$

The mod m is necessary since $|\phi(a)| = m$. On the other hand,

$$\phi(x)\phi(y) = \phi(a^j)\phi(a^k) = [\phi(a)]^{j \bmod m}[\phi(a)]^{k \bmod m} = [\phi(a)]^{(j+k) \bmod m}.$$

So it all boils down to whether $(j + k \bmod n) \bmod m = (j + k) \bmod m$. By the division algorithm, we may write

$$j + k = qn + s \qquad 0 \le s < n.$$

So $(j+k \bmod n) \bmod m = s \bmod m$ Since $n = dm$, we have $j + k = qn + s = q(dm) + s = (qd)m + s$. But then $(j+k) \bmod m = s \bmod m$, too. So

$$\begin{aligned}\phi(xy) = [\phi(a)]^{(j+k \bmod n) \bmod m} &= [\phi(a)]^{s \bmod m}\\ &= [\phi(a)]^{(j+k) \bmod m}\\ &= [\phi(a)]^{j \bmod m}[\phi(a)]^{k \bmod m}\\ &= \phi(x)\phi(y).\end{aligned}$$

When G is an infinite cyclic group the proof is even easier.

Lemma 4 *Let $G =< a >$ be an infinite cyclic group. Let $\phi : G \to H$ be a function such that $\phi(a^i) = \phi(a)^i$ for all i. Then ϕ is a group homomorphism.*

Again, let $x, y \in G$. We must show that $\phi(xy) = \phi(x)\phi(y)$. But G is cyclic so $x = a^j$ and $y = a^k$ There are two cases. If $|\phi(a)| = \infty$, then by assumption

$$\phi(xy) = \phi(a^{j+k}) = [\phi(a)]^{j+k} = [\phi(a)]^j[\phi(a)]^k = \phi(x)\phi(y).$$

If $|\phi(a)| = n$, then by assumption

$$\begin{aligned}\phi(xy) = \phi(a^{j+k}) &= [\phi(a)]^{(j+k) \bmod n}\\ &= [\phi(a)]^{j \bmod n}[\phi(a)]^{k \bmod n} = \phi(x)\phi(y).\end{aligned}$$

Another crucial fact is that composites of homomorphisms are homomorphisms.

Lemma 5 *Let $\phi : G \to H$, and $\gamma : H \to K$ be group homomorphisms. Then so is the composite, $\gamma\phi : G \to K$.*

PROOF Let $a, b \in G$. Then since both maps are homomorphisms,

$$\begin{aligned}(\gamma\phi)(ab) = \gamma(\phi(ab)) &= \gamma(\phi(a)\phi(b))\\ &= \gamma((\phi(a))\gamma(f(b)) = [(\gamma\phi)(a)][(\gamma\phi)(b)].\end{aligned}$$

Definition 6 *If in addition a homomorphism $\phi : G_1 \to G_2$ is both injective and surjective then ϕ is called a* ***group isomorphism****. The two groups are said to be* ***isomorphic*** *and this is denoted by $G_1 \cong G_2$.*

REMARK Note that to prove two groups are isomorphic, we must (1) find a mapping $\phi : G_1 \to G_2$; (2) show that ϕ is injective; (3) show that ϕ is surjective; and (4) show that ϕ is a homomorphism.

Example

a) For homework, if G is a group and a is a fixed elelment of G, then the mapping $\phi : G \to G$ by $g\phi = aga^{-1}$ is an injective, surjective homomorphism. Thus ϕ is an isomorphism.

b) We saw that if G were a group and a was a fixed elelment of G, then the mapping $\phi : G \to G$ by $g\phi = ag$ was an injective and surjective. Let's check to see if it is an isomorhism. $(gh)\phi = agh$, while $(g\phi)(h\phi) = (ag)(ah)$. The two are not equal, and thus ϕ is not an isomorphism.

c) The simplest example is the identity mapping. Let G be a group and let $i_G : G \to G$ by $i_G(g) = g$. We know that i_G is injective and surjective and clearly

$$i_G(ab) = ab = i_G(a)i_G(b).$$

So i_G is an isomorphism and $G \cong G$. (In other words, $\cong$ is a reflexive relation. Is it an equivalence relation?)

d) Another important mapping for *abelian* groups is $\phi : G \to G$ by $g\phi = g^{-1}$. This map is injective: Let $a, b \in G$. Then

$$\phi(a) = \phi(b) \iff a^{-1} = b^{-1} \iff a = b.$$

ϕ is surjective: Let $c \in G$ (codomain). Find $a \in G$ so that $\phi(a) = c$. But

$$\phi(a) = c \iff a^{-1} = c \iff a = c^{-1}.$$

So why is abelian necessary here? When we chek the homomorphism property,

$$\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b).$$

But ths is only possible becuase the group is abelian. □

Lemma 7 *If $G_1 \cong G_2$ then $|G_1| = |G_2|$.*

PROOF There's a one-to-one onto map between the two sets. So counting the elements of one set simultaneously conts the elements of the other. ∎

Example 7 Can Q_8 be isomorphic to $\mathbf{Z}_{10}$? There is another reason that there is no isomorphism between these two groups.

Theorem 8 *Let $G = < a >$ be a cyclic group.*

a) *If $|G| = n$, then $\mathbf{Z}_n \cong G$.*

b) *If $|G| = \infty$, then $\mathbf{Z} \cong G$.*

PROOF In the first case, note that $G =< a >$. Define define $\phi : \mathbf{Z}_n \to G$ by $\phi(k) = a^k$ for any $k \in \mathbf{Z}_n$. The map is injective since

$$k\phi = \phi(j) \iff a^k = a^j \iff n \mid (j-k)$$

which by Theorem 4.1. But this means that $j = k \bmod n$. The map is surjective, obviously. Finally, it is a homomorphism by the lemma we proved earlier, since $n \mid n$.

In the second case, define $\phi : \mathbf{Z} \to G$ by $\phi(k) = a^k$. The map is injective since

$$\phi(j) = \phi(k) \iff a^k = a^j \iff k = j$$

by Theorem 4.1 since $|a| = \infty$. The map is surjective, obviously. Finally, it is a homomorphism si if $j, k \in \mathbf{Z}$, then

$$(j+k)\phi = a^{j+k} = a^j a^k = (j\phi)(k\phi). \quad \square$$

Example 8 $\{i, -1, -i, 1\} \cong \mathbf{Z}_4$ since both are cyclic of order four. What would the isomorphism apping ϕ be here?

Example 9 $\mathbf{Z}_6 \cong U(7)$ since both are cyclic of order 6. Use $\phi(1) \to 3$. ∎

Theorem 9 ***(Properties of Group Isomorphisms)*** *Let $\phi : G_1 \to G_2$ be a group isomorphism. Then in addition to the properties of the previous theorem:*

- ***a)*** *$\phi^{-1} : G_2 \to G_1$ is an isomorphism;*
- ***b)*** *$|a| = |\phi(a)|$;*
- ***c)*** *G_1 is cyclic if and only if G_2 is cyclic;*
- ***d)*** *$a, b \in G_1$ commute if and only if $\phi(a), \phi(b) \in G_2$ commute;*
- ***e)*** *G_1 is abelian if and only if G_2 is abelian.*
- ***f)*** *If $H \leq G_1$, then $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of G_2.*

(A) Since ϕ is an isomorphism, it is surjective and injective, so $\phi^{-1} : G_2 \to G_1$ exists and is injective and surjective. We only need to show that it is a group homomorphism. So take $g_2, h_2 \in G_2$. We must show that $\phi^{-1}(g_2h_2) = \phi^{-1}(g_2)\phi^{-1}(h_2)$. Let $\phi^{-1}g_2 = g_1$ and $\phi^{-1}(h_2) = h_1$. Then $\phi(g_1) = g_2$ and $\phi(h_1) = h_2$. Since ϕ is a homomorphism, $\phi(g_1h_1) = \phi(g_1)\phi(h_1) = g_2h_2$. Therefore,

$$\phi^{-1}(g_2h_2) = g_1h_1 = \phi^{-1}(g_2)\phi^{-1}(h_2).$$

(B) Both ϕ and ϕ^{-1} are homomorphisms. So we know that $|\phi(a)| \Big| |a|$ and $|\phi^{-1}(\phi(a)) = |a| \Big| |\phi(a)|$. Therefore, the orders are equal. (What happens if $|a| = \infty$?)

(C) Suppose $G_1 =< a >$ is cyclic. Then let $\phi(a) = b \in G_2$. We will show that $G_2 =< b >$. Let $g_2 \in G_2$. Because ϕ surjective, there is an element $g_1 \in G_1$ so that $\phi(g_1) = g_2$. But $G_1 =< a >$, so $g_1 = a^k$ for some $k \in \mathbf{Z}$. Therefore,

$$g_2 = \phi(g_1) = \phi(a^k) = [\phi(a)]^k = b^k.$$

Therefore G_2 is cyclic. If G_2 is cyclic, then so is G_1. Simply use the fact that ϕ^{-1} is an isomorphism.

(D) This is a homework problem.

(E) Follows from (g) and the fact that ϕ is onto.

(F) Use the one-step test. Let $x, y \in \phi(H)$. We must show that $xy^{-1} \in \phi(H)$. But there are elements in $a, b \in H$ so that $\phi(a) = x$ and $\phi(b) = y$. Moreover, since H is a subgroup, then $ab^{-1} \in H$. So

$$xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H),$$

since $ab^{-1} \in H$. ∎

Example

a) $\mathbf{Z}_6$ is not isomorphic D_3, even though both have the smae number of elements. [Give three different reasons!]

b) $\mathbf{Z}$ is not isomorphic to $\mathbf{R}$ since one is cyclic and the other is not. One has an element of order 2, the other does not.

c) $U(12)$ is not isomorphic to $\mathbf{Z}_4$ even though both are abelian and have the same number of elements. $U(12) = \{1, 5, 7, 11\}$ is not cyclic. However, $\mathbf{Z}_4 \cong < i > = \{i, -i, 1, -1\}$ since both are cyclic. $\mathbf{Z}_4$ is not isomorphic to V_4 since the latter is not cyclic. What about the group of motions of a rectangle? Of a rhombus? Is either isomorphic to $\mathbf{Z}_4$. Explain.

d) $\mathbf{C}^*$ is not isomorphic to $\mathbf{R}^*$. If ϕ were such an isomorphism, and $\phi(i) = x$, then $|x| = |\phi(i)| = |i| = 4$. But the only elements of finite order in $\mathbf{R}^*$ are 1 and -1 which have order 1 and 2, respectively.

e) $\mathbf{R}^*$ is not isomorphic to $\mathbf{R}$, because -1 in $\mathbf{R}^*$ has order 2 and no element in $\mathbf{R}$ has order 2. (Recall, however, that we know that $\mathbf{R}^+$ is isomorphic to $\mathbf{R}$; use $\phi = \ln x$.)

f) Show that D_{12} is not isomorphic to S_4. Both ahve order 24 and are not abelian. But the former has an element of order 12, while the later has no elements whose order is greater than 4.

g) Is D_4 isomorphic to Q_8? Find out by looking at their tables. (No. Check the number of elements of order 4 in each group. ∎

Theorem 10 ***(Cayley)*** *Every group is isomorphic to a group of permutations.*

See text. The result is interesting but very hard to use in practice, so we will ignore it temporarily.

Definition 11 *An isomorphism $\phi : G \to G$ from a group to itself is called an* ***automorphism****.*

Example 11 We have seen that for abelian groups the mapping $\phi : G \to G$ by $g\phi = g^{-1}$ is an isomorphism, hence it is an automorphism. Similarly, for any group G and any element $a \in G$, the mapping $\phi_a : G \to G$ by $\phi_a(g) = a^{-1}ga$ is an isomorphism. Hence ϕ_a is an automorphism. ϕ_a is called the **inner automorphism** of G induced by a. □

Let's look at a specfic example of an inner automorphism.

Example 12 Let $\alpha = (1,2,3) \in S_3$. What is the mapping $\phi_\alpha : S_3 \to S_3$? Well, $\alpha^{-1} = (3,2,1)$, so

$$\begin{aligned} x &\to \alpha^{-1}x\alpha \\ e = (1) &\to (3,2,1)(1)(1,2,3) = (1) \\ (1,2) &\to (3,2,1)(1,2)(1,2,3) = (2,3) \\ (1,3) &\to (3,2,1)(1,3)(1,2,3) = (1,2) \\ (2,3) &\to (3,2,1)(2,3)(1,2,3) = (1,3) \\ (1,2,3) &\to (3,2,1)(1,2,3)(1,2,3) = (1,2,3) \\ (3,2,1) &\to (3,2,1)(3,2,1)(1,2,3) = (3,2,1) \end{aligned}$$

Definition 12 *The set of all automorphisms of G is called $\mathrm{Aut}(G)$ and the set of all inner automorphisms is called $\mathrm{Inn}(G)$.*

Theorem 13 *Let G be a group. Then $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are also groups. They are both subgroups of S_G (the set of permutations of elements of G.*

Proof We'll show that $\mathrm{Aut}(G)$ is a subgroup of S_G. $\mathrm{Inn}(G)$ is less important at this point. $\mathrm{Aut}(G)$ is simply the set of injecitve, surjective maps from G to itself that are also group homomorphisms. Let $\alpha, \beta \in \mathrm{Aut}(G)$. Show that $\alpha\beta^{-1} \in \mathrm{Aut}(G)$. All we need to do is show that $\alpha\beta^{-1}$ is a homomorphism. But since β is an automorphism, it is an isomorphism so β^{-1} is an isomorphsim (why). So both α and β^{-1} are homomorphisms from G to G, hence so is there composite. ■