MATH 436 Notes: Homomorphisms.

Jonathan Pakianathan

September 23, 2003

1 Homomorphisms

Definition 1.1. *Given monoids M_1 and M_2, we say that $f : M_1 \to M_2$ is a homomorphism if*
(A) $f(ab) = f(a)f(b)$ for all $a, b \in M_1$
(B) $f(e_1) = e_2$ where e_i is the identity element in M_i, $i = 1, 2$.

Basically a homomorphism of monoids is a function between them that preserves all the basic algebraic structure of a monoid: the binary operation and the identity.

The function $f : \mathbb{N} \to \mathbb{N}$ given by $f(n) = 0$ for all $n \in \mathbb{N}$ is not a homomorphism of the monoid $(\mathbb{N}, \cdot)$ to itself even though condition (A) is satisfied. This is because 1 is the identity for multiplication and $f(1) = 0$ so condition (B) is not satisfied. Thus functions satisfying (A), do not automatically satisfy (B) when dealing with monoids.

The situation with groups is somewhat different!

Definition 1.2. *Given groups G_1, G_2 a function $f : G_1 \to G_2$ is called a homomorphism if $f(ab) = f(a)f(b)$ for all $a, b \in G_1$.*

One might question this definition as it is not clear that a homomorphism actually preserves all the algebraic structure of a group: It is not apriori obvious that a homomorphism preserves identity elements or that it takes inverses to inverses. The next proposition shows that luckily this is not actually a problem:

Proposition 1.3. *If $f : G_1 \to G_2$ is a homomorphism between groups then:*
(1) $f(e_1) = e_2$ where e_i is the identity element of G_i, $i = 1, 2$.
(2) $f(x^{-1}) = (f(x))^{-1}$ for all $x \in G_1$. Thus f takes inverses to inverses.

Proof. (1): We compute $f(e_1) = f(e_1e_1) = f(e_1)f(e_1)$. Multiplying both sides of this equation by $f(e_1)^{-1}$ on the left we see that $e_2 = f(e_1)$ as desired. (2): We compute using (1) that $e_2 = f(e_1) = f(xx^{-1}) = f(x)f(x^{-1})$. Thus $e_2 = f(x)f(x^{-1})$ for all $x \in G_1$. Multiplying both sides of this equation by $f(x)^{-1}$ on the left we find $f(x)^{-1} = f(x^{-1})$ for all $x \in G_1$ as desired. $\square$

There are various special names for homomorphisms with certain properties which we define next:

Definition 1.4. *Let $f : M_1 \to M_2$ be a homomorphism of monoids (or groups). Then:*
(a) If f is injective we call it a monomorphism. We typically write $f : M_1 \hookrightarrow M_2$ in this case.
(b) If f is surjective we call it an epimorphism. We typically write $f : M_1 \twoheadrightarrow M_2$ in this case.
(c) If f is bijective we call it an isomorphism. We typically write $f : M_1 \xrightarrow{\cong} M_2$ in this case. Note in this case f sets up a one-to-one correspondence between the points of M_1 and the points of M_2 in such a way that the operation in M_1 then corresponds to the operation in M_2. We say M_1 and M_2 are isomorphic, denoted $M_1 \cong M_2$ and we regard them as the same monoid (group) in different disguises.
(d) A homomorphism $f : M \to M$ of a monoid (group) M back to itself is called an endomorphism of M.
(e) A bijective endomorphism of M is called an automorphism of M.

We consider some examples:

Example 1.5. *Let $det : Mat_n(\mathbb{R}) \to \mathbb{R}$ be the determinant function. Since $det(\mathbb{AB}) = det(\mathbb{A})det(\mathbb{B})$ and $det(\mathbb{I}) = 1$ in general, we see that*

$$det : Mat_n(\mathbb{R}) \to (\mathbb{R}, \cdot)$$

is a homomorphism of monoids where $Mat_n(\mathbb{R})$ is a monoid under matrix multiplication.

The determinant function restricts to also give a homomorphism of groups $det : GL_n(\mathbb{R}) \to (\mathbb{R}^\times, \cdot)$ where $(\mathbb{R}^\times, \cdot)$ denotes the group of nonzero real numbers under multiplication. It is easy to check that det is an epimorphism which is not a monomorphism when $n > 1$.

Let $tr : Mat_n(\mathbb{R}) \to \mathbb{R}$ be the trace function. Since $tr(\mathbb{A} + \mathbb{B}) = tr(\mathbb{A}) + tr(\mathbb{B})$ we see that the trace gives a homomorphism $tr : (Mat_n(\mathbb{R}), +) \to$

$(\mathbb{R}, +)$ *where* $Mat_n(\mathbb{R})$ *and* $\mathbb{R}$ *are considered groups under addition. Again, it is easy to check that* tr *is an epimorphism which is not a monomorphism when* $n > 1$.

Example 1.6. *Let* A *be an alphabet and let* $W(A)$ *be the monoid of finite words on this alphabet under the operation of concatenation. Define* $L : W(A) \to \mathbb{N}$ *by* $L(w) =$*length of the word* w. *Thus if* A *is the standard roman alphabet,* $L(cat) = 3$. *It is clear* $L(\hat{e}) = 0$ *where* $\hat{e}$ *is the empty word and it is also easy to check that* $L(w_1 \star w_2) = L(w_1) + L(w_2)$ *and so* $L : W(A) \to (\mathbb{N}, +)$ *is a homomorphism of monoids. It is called the length homomorphism. If* $|A| \geq 2$ *then it is easy to check that the length homomorphism is an epimorphism but not a monomorphism. For example if* $a, b \in A$ *are distinct then* $L(ab) = L(ba) = 2$ *but* $ab \neq ba \in W(A)$.

Example 1.7. *Let* $I : \Sigma_n \to \Sigma_{n+1}$ *be defined as follows: For* $\sigma \in \Sigma_n$ *we set:*

$$I(\sigma)(j) = \begin{cases} \sigma(j) \text{ when } 1 \leq j \leq n \\ n+1 \text{ when } j = n+1. \end{cases}$$

Basically I *takes a permutation* σ *of* $\{1, 2, \ldots, n\}$ *and extends it to a permutation of* $\{1, 2, \ldots, n, n+1\}$ *by just sending* $n+1$ *to itself. It is a simple exercise left to the reader to show that* I *is a monomorphism. Thus it induces an isomorphism between* Σ_n *and its image* $Im(I) \subseteq \Sigma_{n+1}$. *We often view* $Im(I)$ *as a copy of* Σ_n *sitting within* Σ_{n+1}.

The following is a basic fact about homomorphisms:

Theorem 1.8. *(a) Let* $f : M_1 \to M_2$, $g : M_2 \to M_3$ *be homomorphisms of monoids (groups) then* $g \circ f : M_1 \to M_3$ *is also a homomorphism.*
(b) The identity map $1_M : M \to M$ *is a homomorphism.*
(c) If S *is a monoid (group) then* $End(S) = \{f : S \to S | f \text{ an endomorphism }\}$ *is a submonoid of* $M(S)$, *the monoid of functions with domain and codomain* S. $End(S)$ *is called the monoid of endomorphisms of* S.
(d) If S *is a monoid (group) then* $Aut(S) = \{f : S \to S | f \text{ an automorphism }\}$ *is the group of units of* $End(S)$. *It is a subgroup of* $\Sigma(S)$, *the group of permutations on* S. $Aut(S)$ *is called the group of automorphisms of* S.

Proof. (a): We compute

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$$

and also $(g \circ f)(e_1) = g(f(e_1)) = g(e_2) = e_3$ and so $g \circ f$ is a homomorphism of monoids (groups).
(b): $1_M(ab) = ab = 1_M(a)1_M(b)$ and $1_M(e) = e$ so 1_M is a homomorphism of monoids (groups).
(c): By (a) and (b), it follows that $End(S)$ is a monoid under composition of functions and that it is a submonoid of $M(S) = \{f : S \to S\}$.
(d): Also follows directly as in (c). □

Before we can calculate a basic example of $End(G)$ or $Aut(G)$ we record a basic fact:

Proposition 1.9. *If $G =< S >$ for some subset S of G and $f_1, f_2 : G \to H$ are two homomorphisms to another group such that they agree on S, i.e., $f_1(s) = f_2(s)$ for all $s \in S$, then $f_1 = f_2$. In other words a homomorphism is uniquely determined by what is does on a generating set.*

Proof. Take $g \in G$. Since S generates G we have $g = s_1^{\pm 1} s_2^{\pm 1} \dots s_k^{\pm 1}$ for some elements $s_j \in S$. We then compute:

$$\begin{aligned} f_1(g) &= f_1(s_1^{\pm 1} \dots s_k^{\pm 1}) \\ &= f_1(s_1)^{\pm 1} \dots f_1(s_k)^{\pm 1} \text{ as } f_1 \text{ is a homomorphism} \\ &= f_2(s_1)^{\pm 1} \dots f_2(s_k)^{\pm 1} \text{ as } f_1 \text{ and } f_2 \text{ agree on } S \\ &= f_2(g) \text{ as } f_2 \text{ is a homomorphism.} \end{aligned}$$

Thus $f_1(g) = f_2(g)$ for all $g \in G$ and so $f_1 = f_2$ and we are done. □

Proposition 1.10. *Let $(\mathbb{Z}, +)$ be the group of integers under addition. Then $End((\mathbb{Z}, +)) = \{f_m | m \in \mathbb{Z}\}$ where $f_m : \mathbb{Z} \to \mathbb{Z}$ is multiplication by m, given by $f_m(n) = mn$ for all $n \in \mathbb{Z}$. Thus $Aut((\mathbb{Z}, +)) = \{f_{-1}, f_1\}$.*

Furthermore the monoid $End((\mathbb{Z}, +))$ is isomorphic to $(\mathbb{Z}, \cdot)$, the monoid of integers under multiplication. $Aut((\mathbb{Z}, +))$ is thus isomorphic to the 2-element group of units of this monoid, i.e., $\{-1, 1\}$.

Proof. Each f_m is an endomorphism of $(\mathbb{Z}, +)$ as $f_m(n + n') = m(n + n') = mn + mn' = f_m(n) + f_m(n')$. Suppose g is some other endomorphism of $\mathbb{Z}$, then $g(1) = m$ for some $m \in \mathbb{Z}$. However $f_m(1) = m$ also and $(\mathbb{Z}, +) =< 1 >$ so by Proposition 1.9 we have that $g = f_m$ since they agree on the generating set.

Thus this shows $End((\mathbb{Z}, +)) = \{f_m | m \in \mathbb{Z}\}$. It is easy to check that the only $f_m : \mathbb{Z} \to \mathbb{Z}$ that are bijections are f_{-1} and f_1 so $Aut((\mathbb{Z}, +)) = \{f_1, f_{-1}\}$.

Finally define $\theta : (\mathbb{Z}, \cdot) \to End((\mathbb{Z}, +))$ by $\theta(m) = f_m$. Since $f_m \circ f_k = f_{mk}$ and $f_1 = 1_{\mathbb{Z}}$ it follows that θ is a homomorphism of monoids. It is trivial to check that it is a bijection and so induces an isomorphism between $(\mathbb{Z}, \cdot)$ and $End((\mathbb{Z}, +))$. This completes the proof. □

The following is an important concept for homomorphisms:

Definition 1.11. *If $f : G \to H$ is a homomorphism of groups (or monoids) and e' is the identity element of H then we define the kernel of f as $ker(f) = \{g \in G | f(g) = e'\}$.*

The kernel can be used to detect injectivity of homomorphisms as long as we are dealing with groups:

Theorem 1.12 (Kernels detect injectivity). *Let $f : G \to H$ be a homomorphism of groups. Then f is injective if and only if $ker(f) = \{e\}$.*

Proof. $\implies$**:** If f is injective then as $f(e) = e'$ we conclude that $ker(f) = f^{-1}(\{e'\}) = \{e\}$ as no more than one element can be sent to the output e'. $\impliedby$**:** Now suppose we know $ker(f) = \{e\}$ and $f(g_1) = f(g_2)$. Then we may compute $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = e'$. Thus $g_1 g_2^{-1} \in ker(f)$ and so $g_1 g_2^{-1} = e$. Hence $g_1 = g_2$. Thus we see f is injective. □

The argument above used inverses in the proof. It turns out that indeed it does not apply to monoids. For example consider the length homomorphism $L : W(A) \to (\mathbb{N}, +)$. Then $ker(L) = \{\hat{e}\}$ as only the empty word $\hat{e}$ has length 0. However L is not injective, for example if A is the standard roman alphabet then $L(cat) = L(dog) = 3$ so L is clearly not injective even though its kernel is trivial. Thus we must be careful when dealing with monoids and check injectivity directly.

Example 1.13. *Given a group G and a normal subgroup $N \trianglelefteq G$ we have seen that we may form the quotient group G/N. There is a canonical map $\phi_N : G \to G/N$ defined by $\phi_N(g) = gN$ for all $g \in G$. Since $\phi_N(gh) = ghN = gN \star hN = \phi_N(g) \star \phi_N(h)$ we see that this map is a homomorphism. We shall call it the canonical quotient homorphism. Note $ker(\phi_N) = \{g \in G | gN = eN\} = N$, and that ϕ_N is an epimorphism.*

The following is a fundamental theorem about the images and kernels of homomorphisms:

Theorem 1.14. *Let G, H be groups and $f : G \to H$ be a homomorphism. Then $Im(f) \leq H$ and $ker(f) \trianglelefteq G$.*

Proof. Let $x, y \in ker(f)$ then we compute $f(xy) = f(x)f(y) = ee = e$ and $f(x^{-1}) = f(x)^{-1} = e^{-1} = e$. Thus we conclude that $xy, x^{-1} \in ker(f)$ and thus see that $ker(f)$ is a subgroup of G.

On the other hand for $g \in G$ and $x \in ker(f)$ we compute $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)ef(g)^{-1} = e$ and so $gxg^{-1} \in ker(f)$ also. Thus we conclude $gker(f)g^{-1} \subseteq ker(f)$ for all $g \in G$. Replacing g with g^{-1} we find $g^{-1}ker(f)g \subseteq ker(f)$ for all $g \in G$ and hence after left multiplying by g and right multiplying by g^{-1} we see $ker(f) \subseteq gker(f)g^{-1}$. Since we have previously seen the reverse inclusion, we conclude $gker(f)g^{-1} = ker(f)$ from which it follows $gker(f) = ker(f)g$ for all $g \in G$ and hence we see $ker(f)$ is a normal subgroup of G.

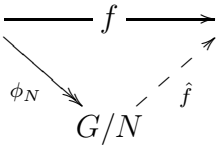
Finally the identities $f(x)f(y) = f(xy)$ and $f(x)^{-1} = f(x^{-1})$ show that $Im(f)$ is a subgroup of H.

□

2 Isomorphism Theorems

We now discuss the all important fundamental isomorphism theorems of group theory! Before we do that we address a fundamental factorization theorem:

Theorem 2.1 (Factoring a homomorphism). *Let $f : G \to H$ be a homomorphism of groups and let $N \trianglelefteq G$ be a normal subgroup of the domain group.*

Then there is a homomorphism $\hat{f} : G/N \to H$ making the following diagram commute: 

if and only if $N \subseteq ker(f)$.

In the case where $\hat{f}$ exists it is given by the formula $\hat{f}(gN) = f(g)$ for all $g \in G$. Furthermore $Im(\hat{f}) = Im(f)$ and $ker(\hat{f}) = ker(f)/N$.

Proof. $\implies$: Suppose a homomorphism $\hat{f}$ exists such that the diagram commutes, i.e., $\hat{f} \circ \phi_N = f$. Then for $n \in N$ we calculate $f(n) = \hat{f}(\phi_N(n)) = \hat{f}(nN) = \hat{f}(eN) = e'$ where the final equality follows as $\hat{f}$ is a homomorphism

and hence must take identity element to identity element. Thus $n \in ker(f)$ for all $n \in N$ and so $N \subseteq ker(f)$.
$\Longleftarrow$: Now suppose $N \subseteq ker(f)$. We attempt to define a function $\hat{f} : G/N \to H$ to make the diagram commute. This forces the definition $\hat{f}(gN) = f(g)$. We must check to see that this is well-defined!

If $g_1N = g_2N$ we have $g_1 = g_2n$ for some $n \in N$. Then we calculate $\hat{f}(g_1N) = f(g_1) = f(g_2n) = f(g_2)f(n) = \hat{f}(g_2N)f(n)$. However since $N \subseteq ker(f)$ we have $f(n) = e'$ and so $\hat{f}(g_1N) = \hat{f}(g_2N)$. This shows that $\hat{f}$ is a well-defined function. It is then trivial to verify that it is a homomorphism and that it makes the diagram commute.

Finally in the case that $\hat{f}$ exists, we have seen that we must have $\hat{f}(gN) = f(g)$ for all $g \in G$ in order for the diagram to commute. This clearly shows that $Im(f) = Im(\hat{f})$. We compute $ker(\hat{f}) = \{gN|\hat{f}(gN) = e'\} = \{gN|f(g) = e'\} = \{gN|g \in ker(f)\} = ker(f)/N$. Thus we are done. □

A direct corollary of this factorization theorem is the First Isomorphism Theorem:

Theorem 2.2 (First Isomorphism Theorem). *Let $f : G_1 \to G_2$ be a homomorphism. Then there is a monomorphism $\hat{f} : G_1/ker(f) \hookrightarrow G_2$ that makes the following diagram commute:*

Thus

$$G_1/ker(f) \cong Im(f).$$

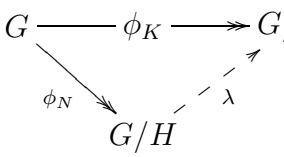
Furthermore $f = \hat{f} \circ \phi$ where ϕ is an epimorphism and $\hat{f}$ is a monomorphism.

Proof. Applying the case $N = ker(f)$ in Theorem 2.1 we find a homomorphism $\hat{f} : G_1/ker(f) \to G_2$ making the diagram commute. From the same theorem, we know $ker(\hat{f}) = ker(f)/ker(f) = (eker(f))$ and so is trivial. Thus $\hat{f}$ is a monomorphism. Since $Im(\hat{f}) = Im(f)$ we conclude $\hat{f} : G_1/ker(f) \to Im(f)$ is an isomorphism of groups. This completes the proof. □

The First Isomorphism Theorem itself gives the Second Isomorphism Theorem:

Theorem 2.3 (Second Isomorphism Theorem). *Let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K.$$

Proof. Consider the following diagram: 

. The homomorphism λ exists by Theorem 2.1 as $ker(\phi_K) = K$ contains H. Also by the factorization theorem we see that λ is onto and that $ker(\lambda) = K/H$ and hence $K/H \trianglelefteq G/H$. Finally by the First Isomorphism Theorem, λ induces an isomorphism $(G/H)/(K/H) \cong G/K$.

□

The third isomorphism theorem involves $HK = \{hk | h \in H, k \in K\}$ and so we discuss that first:

Example 2.4. *If $G = \Sigma_3$, $H =< (1,2) >= \{e, (1,2)\}$, $K =< (2,3) >= \{e, (2,3)\}$ then $HK = \{e, (1,2), (2,3), (1,2,3)\}$. Thus since $|HK|$ does not divide $|G|$ we can conclude that HK is not a subgroup of G even though H and K are.*

From the last example, we see that in general the product HK of two subgroups H and K need not itself be a subgroup. We next find extra conditions on H and K that ensure HK is a subgroup.

Proposition 2.5. *Let H and K be subgroups of a group G. Then HK is a subgroup if and only if $HK = KH$. We say that the subgroups H and K permute each other in this case.*

Proof. $\Longrightarrow$: If HK is a subgroup then it must contain its inverses so $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ as $K, H \leq G$.
$\Longleftarrow$: On the other hand if $HK = KH$ then we may check that HK is a subgroup. It contains inverses by computing as above that $(HK)^{-1} = KH$ and using that $KH = HK$. To show that it is closed we compute: $(HK)(HK) = (HK)(KH) = H(KK)H = HKH = (HK)H = (KH)H = K(HH) = KH = HK$. (Here we have used $KK = K$ which follows as $KK \subseteq K$ since K is a subgroup and $K = Ke \subseteq KK$.) Thus we see that $HK \leq G$. □

The following is an important special case of the previous Proposition:

Corollary 2.6. *If $H \leq G$ and $K \trianglelefteq G$ then HK is a subgroup of G.*

Proof. Since K is normal in G we have in particular $hK = Kh$ for all $h \in H$. Thus we conclude $HK = \cup_{h \in H} hK = \cup_{h \in H} Kh = KH$ and so HK is a subgroup of G by Proposition 2.5. □

We are now ready for the Third Isomorphism Theorem:

Theorem 2.7 (Third Isomorphism Theorem). *If $H \leq G$ and $K \trianglelefteq G$ then $HK \leq G$, $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$. Furthermore*

$$HK/K \cong H/(H \cap K).$$

Thus in the case when G is finite, we have $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. Consider the canonical quotient homomorphism $\phi : G \to G/K$. We may restrict this homomorphism to the domain H and we get the following commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G/K \\ \uparrow & & \uparrow \\ H & \xrightarrow{\phi|_H} & \phi(H) \end{array}$$

where the vertical arrows are inclusions. Since $ker(\phi) = K$ it is easy to see that $ker(\phi|_H) = H \cap K$ and hence $H \cap K \trianglelefteq H$ as kernels are normal. Thus the first isomorphism theorem applied to $\phi|_H$ gives $\phi(H) \cong H/(H \cap K)$.

On the other hand we may look at the full preimage $S = \phi^{-1}(\phi(H))$. Since it is the preimage of a subgroup under a homomorphism, we know $S \leq G$ and furthermore it is easy to see that $K = ker(\phi) \trianglelefteq S$.

Then ϕ restricts to an epimorphism $S \twoheadrightarrow \phi(H)$ which has kernel K so that the first isomorphism theorem gives $S/K \cong \phi(H)$ and hence that $S/K \cong H/(H \cap K)$.

To finish the proof of the theorem, it remains to show that $S = HK$. Well, $S = \phi^{-1}(\phi(H)) = \{g \in G | \phi(g) = \phi(h) \text{ for some } h \in H\}$. However $\phi(g) = \phi(h)$ gives $gK = hK$ and so $g = hk$ for some $k \in K, h \in H$. Thus $S = HK$ as desired.

The final counting formula follows as $|G/N| = |G : N| = \frac{|G|}{|N|}$ in general. □

As we go on, the last 3 isomorphisms will be fundamental tools in our analysis.

[To be continued....]