Queen Mary
University of London

MAS 305 Algebraic Structures II

Notes 3 Autumn 2006

Group homomorphisms

Definition Let G and H be groups, and let $\phi: G \to H$ be a function. Then ϕ is a *homomorphism* if $(g_1g_2)\phi = (g_1\phi)(g_2\phi)$ for all g_1, g_2 in G.

Note that we are writing homomorphisms as functions on the right. Also note that multiplication on the left-hand side of the equation is in G, while multiplication on the right-hand side is in H.

If ϕ is a homomorphism then $1_G\phi = 1_H$ and $g^{-1}\phi = (g\phi)^{-1}$ (proof: exercise).

A homomorphism which is a bijection is called an *isomorphism*. If there is an isomorphism from G to H then G is *isomorphic* to H, written $G \cong H$.

Definition If $\phi: G \to H$ is a homomorphism then the *image* of ϕ is $\{g\phi : g \in G\}$, which is written $\mathrm{Im}(\phi)$, and the *kernel* of ϕ is $\{g \in G : g\phi = 1_H\}$, which is written as $\ker(\phi)$.

Theorem If $\phi: G \to H$ is a homomorphism then

(a) $\mathrm{Im}(\phi)$ is a subgroup of H;

(b) $\ker(\phi)$ is a normal subgroup of G;

(c) $g_1\phi = g_2\phi$ if and only if g_1 and g_2 are in the same coset of $\ker(\phi)$, so there is a bijection between the set of cosets of $\ker(\phi)$ in G and $\mathrm{Im}(\phi)$.

Proof (a) $1_H = 1_G\phi \in \mathrm{Im}(\phi)$, so $\mathrm{Im}(\phi)$ is not empty.

If h_1 and h_2 are in $\mathrm{Im}(\phi)$ then there are g_1, g_2 in G with $h_1 = g_1\phi$ and $h_2 = g_2\phi$. Then $h_1^{-1}h_2 = (g_1\phi)^{-1}(g_2\phi) = (g_1^{-1})\phi(g_2\phi) = (g_1^{-1}g_2)\phi \in \mathrm{Im}(\phi)$.

Thus $\mathrm{Im}(\phi) \leqslant H$.

(b) $1_G\phi = 1_H$ so $1_G \in \ker(\phi)$, so $\ker(\phi)$ is not empty.

If g_1, g_2 are in $\ker(\phi)$ then $g_1\phi = g_2\phi = 1_H$ so $g_1^{-1}\phi = 1_H^{-1} = 1_H$ and $(g_1^{-1}g_2)\phi = (g_1^{-1})\phi(g_2\phi) = 1_H^2 = 1_H$, so $g_1^{-1}g_2 \in \ker(\phi)$.

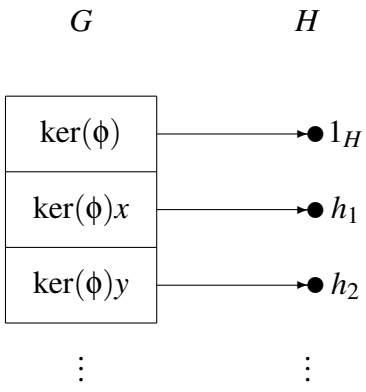
This shows that $\ker(\phi) \leqslant G$.

If $g \in \ker(\phi)$ and $x \in G$ then $(x^{-1}gx)\phi = (x^{-1})\phi(g\phi)(x\phi) = (x\phi)^{-1}1_H(x\phi) = 1_H$ so $x^{-1}gx \in \ker(\phi)$. Therefore $\ker(\phi) \trianglelefteq G$.

(c)

$$\begin{aligned} g_1\phi = g_2\phi &\iff (g_2\phi)(g_1\phi)^{-1} = 1_H \\ &\iff (g_2\phi)(g_1^{-1}\phi) = 1_H \\ &\iff (g_2g_1^{-1})\phi = 1_H \\ &\iff g_2g_1^{-1} \in \ker(\phi) \\ &\iff g_1 \text{ and } g_2 \text{ are in the same right coset of } \ker(\phi). \quad \square \end{aligned}$$

Part (c) of this theorem gives the bijection between right cosets of $\ker(\phi)$ in G and elements of $\mathrm{Im}(\phi)$ in H shown below. We know how to combine the latter using the group operation in H. Using the bijection, this gives a way of combining right cosets of $\ker(\phi)$ in G. We shall now show that we can define a group operation on the right cosets of a normal subgroup of G without knowing anything about another group H.



Definition If $K \trianglelefteq G$ then the *quotient group* G/K has as its elements the cosets of K in G, with binary operation $\circ$ defined by $Kx \circ Ky = Kxy$ for x, y in G.

Note that, since K is normal in G, we do not need to specify whether the cosets are right cosets or left cosets.

Theorem The above definition of $\circ$ is well defined, and $(G/K, \circ)$ is indeed a group.

Proof First we show that the definition of $\circ$ is not affected by which element of the coset we use in the definition.

Suppose that $Kx_1 = Kx_2$ and $Ky_1 = Ky_2$. Then $x_2 = kx_1$ and $y_2 = hy_1$ for some h, k in K. Hence $x_2y_2 = kx_1hy_1 = kx_1hx_1^{-1}x_1y_1$. But K is normal in G, so $x_1hx_1^{-1} \in K$, so $kx_1hx_1^{-1} \in K$. Therefore $Kx_2y_2 = Kx_1y_1$.

This shows that $\circ$ is well defined.

Next we have to check that the four group axioms are satisfied.

(a) Kxy is a coset of K, so $\circ$ is closed.

(b) Given x, y, z in G, we have $(Kx \circ Ky) \circ Kz = (Kxy) \circ Kz = K(xy)z = Kx(yz) = Kx \circ Kyz = Kx \circ (Ky \circ Kz)$, so $\circ$ is associative.

(c) K is the identity for $\circ$, because $K = K1_G$ and $K \circ Kx = K1_G \circ Kx = K(1_Gx) = Kx$, and, similarly, $Kx \circ K = Kx$.

(d) The inverse of Kx is Kx^{-1}, because $Kx \circ Kx^{-1} = K(xx^{-1}) = K1_G = K$ and $Kx^{-1} \circ Kx = K(x^{-1}x) = K1_G = K$.

Hence G/K is a group. $\square$

Theorem Let $K \trianglelefteq G$. The function $\theta: G \to G/K$ defined by $x\theta = Kx$ is a homomorphism from G onto G/K (called the *canonical homomorphism* for K) and its kernel is K.

Proof For all x, y in G, $x\theta \circ y\theta = Kx \circ Ky = Kxy = (xy)\theta$, so θ is a homomorphism. It is clear that θ is onto. Moreover, $x \in \ker(\theta) \iff x\theta = K \iff Kx = K \iff x \in K$. $\square$

Permutation groups

Here we develop an important homomorphism and use it to find a normal subgroup of S_n.

Definition A *transposition* is a permutation interchanging two objects and leaving the rest fixed.

Lemma Every permutation is a product of transpositions.

Proof Every permutation is a product of cycles, and $(1\,2\,3\,\ldots\,n) = (1\,2)(1\,3)\ldots(1\,n)$. $\square$

Lemma If the permutation h contains the cycle $(a_1\,a_2\,\ldots\,a_n)$ and the permutation g takes a_i to b_i for $i = 1, \ldots, n$ then $g^{-1}hg$ contains the cycle $(b_1\,b_2\,\ldots\,b_n)$.

Proof For $1 \leqslant i \leqslant n-1$, $b_i(g^{-1}hg) = a_ihg = a_{i+1}g = b_{i+1}$, and $b_ng^{-1}hg = a_nhg = a_1g = b_1$. $\square$

The following pictures illustrates the proof.

$$\begin{array}{rcccccc} h & = & (a_1 & a_2 & \ldots & a_n) & \ldots \\ & g & \downarrow & \downarrow & \ldots & \downarrow & \ldots \\ g^{-1}hg & = & (b_1 & b_2 & \ldots & b_n) & \ldots \end{array}$$

Definition The *cycle structure* of a permutation is the list of the lengths of its cycles, in non-descending order.

The previous lemma shows that $g^{-1}hg$ has the same cycle structure as h.

Example In S_9, if $h = (1\,4\,5)(2\,6\,7\,8)$ then the cycle structure of h is 1, 1, 3, 4. If $g = (1\,6\,3\,4\,9)(7\,8\,2)$ then $g^{-1}hg = (6\,9\,5)(7\,3\,8\,2)$, with the same cycle structure.

Definition In the symmetric group S_n, let $c(g)$ denote the number of cycles of the permutation g, including those cycles of length 1. Define $\text{sign}(g) = (-1)^{n-c(g)}$. Say that g is *even* if $\text{sign}(g) = +1$ and g is *odd* if $\text{sign}(g) = -1$.

Lemma Put $m(g)$ equal to the number of cycles of g which have even length. Then $\text{sign}(g) = (-1)^{m(g)}$.

Proof For each permutation g, we have

$$n = \sum_{\text{cycles of } g} (\text{length of cycle}).$$

So, modulo 2,

$$n = m(g) \times 0 + (c(g) - m(g)) \times 1,$$

so $n - c(g) = -m(g) = m(g) \bmod 2$, so $(-1)^{n-c(g)} = (-1)^{m(g)}$. $\square$

Example In S_9, $c(h) = 4$, so $\text{sign}(h) = (-1)^{9-4} = (-1)^5 = -1$. Also, $m(h) = 1$, so $\text{sign}(h) = (-1)^1 = -1$.

We are about to show that the function sign is a homomorphism. Untypically, this homomorphism is written as a function on the left rather than on the right.

Theorem The function sign is a homomorphism from S_n to the group $\{1,-1\}$ under multiplication.

Proof We need to show that $\text{sign}(gh) = \text{sign}(g)\,\text{sign}(h)$ for all permutations g and h.

First suppose that h is a transposition, say $h = (1\,2)$. Then $\text{sign}(h) = -1$. If 1 and 2 are in the same cycle of g then gh has two cycles in place of this, with the other cycles the same as those of g. If 1 and 2 are in different cycles of g, then gh unites these two cycles into one, leaving the other cycles the same as those of g. So $c(gh) = c(g) \pm 1$, so $\text{sign}(gh) = (-1)\,\text{sign}(g) = \text{sign}(g)\,\text{sign}(h)$.

In general, suppose that $h = h_1 h_2 \ldots h_s$ where the h_i are transpositions. Then $s-1$ applications of the previous step show that $\text{sign}(h) = (-1) \times (-1)^{s-1} = (-1)^s$ and s applications of the previous step show that $\text{sign}(gh) = \text{sign}(g) \times (-1)^s$. Hence $\text{sign}(gh) = \text{sign}(g) \times \text{sign}(h)$. $\square$

The kernel of sign is a normal subgroup of S_n, called the *alternating group* A_n. It consists of all the even permutations. By a preceding theorem, the number of cosets of A_n in S_n is equal to the size of $\text{Im}(\text{sign})$, which is equal to 2 if $n \geqslant 2$. That is, $|S_n : A_n| = 2$, so $|A_n| = n!/2$ if $n \geqslant 2$.

Linear groups

Homomorphisms also give us a powerful method of finding subgroups of general linear groups. Here are two examples.

First, consider the map ϕ from $(\mathbb{Z}, +)$ to $\text{GL}(2,\mathbb{R})$ defined by $n\phi = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. We have

$$(n\phi)(m\phi) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} = (n+m)\phi$$

for all integers n and m, so ϕ is a homomorphism. Therefore $\left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$ is a subgroup of $\text{GL}(2,\mathbb{R})$.

Secondly, consider the determinant map det from $\text{GL}(2,\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \times)$, which takes the 2×2 matrix M to its determinant $\det(M)$. It can be shown that $\det(AB) = (\det A)(\det B)$ for all 2×2 real matrices A and B, so det is a homomorphism. Therefore, the kernel of det is a normal subgroup of $\text{GL}(2,\mathbb{R})$. This normal subgroup consists of all the invertible real 2×2 matrices with determinant 1; it is called the *special linear group* $\text{SL}(2,\mathbb{R})$.

This can be generalized, by replacing $\mathbb{R}$ by any field F and replacing 2 by any positive integer n. The determinant map is still a homomorphism, and so $\text{GL}(n,F)$ has a normal subgroup $\text{SL}(n,F)$ consisting of the invertible $n \times n$ matrices with entries in F and determinant 1.

Isomorphism theorems

The next four theorems are collectively known as 'the isomorphism theorems'. Apart from the first one, there is no universal agreement about which one is which, or which results form part of which theorem.

First Isomorphism Theorem If G, H are groups and $\phi: G \to H$ is a homomorphism, then $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Proof Put $K = \ker(\phi)$. Define $\psi: G/K \to \mathrm{Im}(\phi)$ by $(Kx)\psi = x\phi$. The theorem just before the diagram shows that x and y are in the same coset of K if and only if $x\phi = y\phi$, so ψ is well defined and one-to-one. Obviously, ψ is onto. Furthermore,

$$\begin{aligned}
[(Kx)\psi][(Ky)\psi] &= (x\phi)(y\phi) \\
&= (xy)\phi \qquad \text{because } \phi \text{ is a homomorphism} \\
&= (Kxy)\psi \\
&= [(Kx)\circ(Ky)]\psi
\end{aligned}$$

and so ψ is a homomorphism. $\square$

From now on we shall write $Kx \circ Ky$ just as $(Kx)(Ky)$ when working in the quotient group G/K.

Lemma If $\phi_1: G_1 \to G_2$ and $\phi_2: G_2 \to G_3$ are group homomorphisms then $\phi_1\phi_2: G_1 \to G_3$ is a homomorphism.

Proof Exercise.

Correspondence Theorem Let $K \trianglelefteq G$. There is a bijection between the set of subgroups of G containing K and the set of subgroups of G/K. The bijection preserves inclusion. Normal subgroups of G containing K correspond to normal subgroups of G/K.

Proof Let $\theta: G \to G/K$ be the canonical homomorphism.

If $K \leqslant H \leqslant G$ and $h \in H$ then $Kh \subseteq H$, so H is a union of cosets of K. Let $H\psi$ be the set of these cosets, which is a subset of G/K. In fact, $H\psi = \{Kh : h \in H\} = \{h\theta : h \in H\} = H/K$. Since H is the union of the cosets in $H\psi$, it is clear that ψ is one-to-one. It is also clear that if $K \leqslant H_1 \leqslant H_2 \leqslant G$ then $H_1\psi \leqslant H_2\psi$, so ψ preserves inclusion.

Define $\tilde{\theta}: H \to G/K$ by $h\tilde{\theta} = h\theta$ for h in H. Then $\tilde{\theta}$ is a homomorphism, so $\mathrm{Im}(\tilde{\theta})$ is a subgroup of G/K. But $\mathrm{Im}(\tilde{\theta}) = H\psi$, so $H\psi \leqslant G/K$.

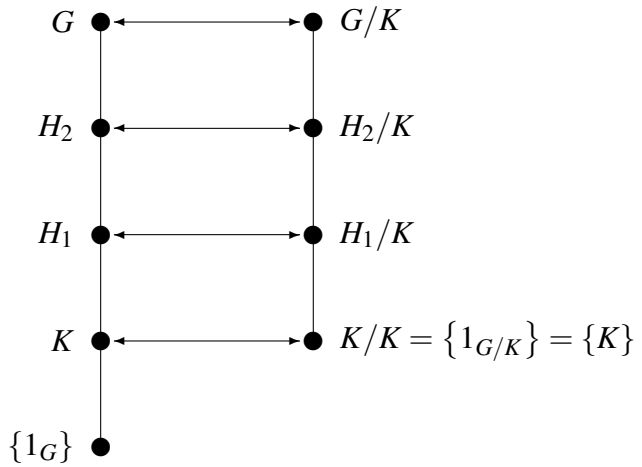
If $T \leqslant G/K$, put $\bar{T} = \{g \in G : g\theta \in T\}$. If $g \in K$ then

$$g\theta = K = \text{identity in } G/K \in T,$$

so $K \leqslant \bar{T}$ and $\bar{T}$ is not empty. If g_1 and g_2 are in $\bar{T}$ then $(g_1^{-1}g_2)\theta = (g_1\theta)^{-1}g_2\theta \in T$, because θ is a homomorphism, so $g_1^{-1}g_2 \in \bar{T}$. Hence $\bar{T} \leqslant G$. If the coset Kg is in T then $g \in \bar{T}$, so $T = \bar{T}\psi$. Hence ψ is onto, and so ψ is a bijection.

Finally, $H\psi \trianglelefteq G/K$ if and only if $(Kg)^{-1}(Kh)(Kg) \subseteq H$ for all g in G and all h in H. But $(Kg)^{-1}(Kh)(Kg) = K(g^{-1}hg)$. Since $K \subseteq H$, $K(g^{-1}hg) \subseteq H$ if and only if $g^{-1}hg \in H$. Moreover, $g^{-1}hg \in H$ for all g in G and all h in H if and only if $H \trianglelefteq G$. $\square$

I like to draw a Hasse diagram to represent a group. There is one dot for each subgroup that I am considering. If one subgroup is contained in another, there is a line, or series of lines, from the first to the second, in a generally upwards direction, possibly passing through other dots. The Correspondence Theorem says that the Hasse diagram for G/K is just the part of the Hasse diagram for G that is above K.



Second Isomorphism Theorem If K and N are normal subgroups of G with $K \leqslant N$ then $(G/K)/(N/K) \cong G/N$.

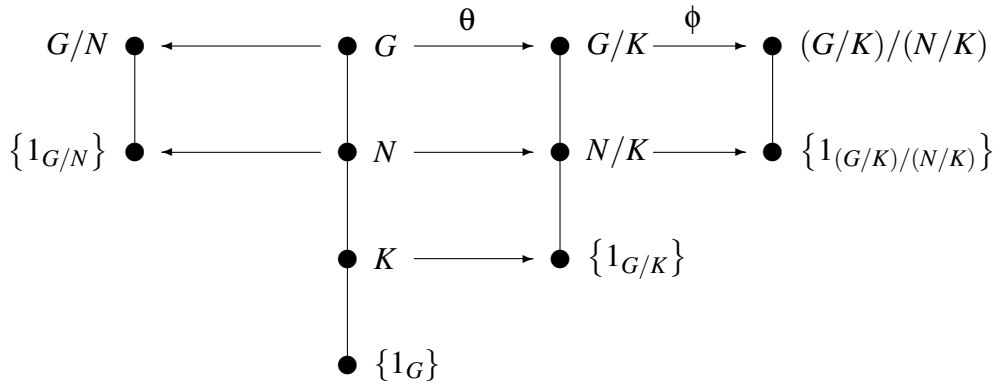
Proof Let θ be the canonical homomorphism from G onto G/K. The Correspondence Theorem shows that $N/K \trianglelefteq G/K$ and so we can indeed form the quotient group $(G/K)/(N/K)$. Let ϕ be the canonical homomorphism from G/K onto $(G/K)/(N/K)$. Then $\theta\phi$ is a homomorphism from G onto $(G/K)/(N/K)$, and

$$\begin{aligned}
\ker(\theta\phi) &= \{g \in G : g\theta\phi = \text{identity in } (G/K)/(N/K)\} \\
&= \{g \in G : g\theta \in \ker(\phi)\} \\
&= \{g \in G : g\theta \in N/K\} \\
&= N,
\end{aligned}$$

by the Correspondence Theorem.

Now the First Isomorphism Theorem gives

$$G/N = G/\ker(\theta\phi) \cong \mathrm{Im}(\theta\phi) = (G/K)/(N/K). \quad \square$$



This shows that it is legitimate to regard the part of the Hasse diagram for G that is above N as the Hasse diagram for G/N *whether or not* we take the intermediate step of regarding the part of the Hasse diagram for G that is above K as the Hasse diagram for G/K.

Third Isomorphism Theorem If G is a group, $K \trianglelefteq G$ and $H \leqslant G$, and KH is defined to be $\{kh : k \in K \text{ and } h \in H\}$ then

(a) KH is a subgroup of G containing K and H;

(b) $K \cap H$ is a normal subgroup of H;

(c) $KH/K \cong H/K \cap H$.

Proof We could prove parts (i) and (ii) be elementary means, but instead we prove them as a byproduct of proving part (iii).

Let θ be the canonical homomorphism from G onto G/K, and let $\tilde{\theta}$ be the restriction of θ to H. Then $\mathrm{Im}(\tilde{\theta})$ is a subgroup of G/K. But $\mathrm{Im}(\tilde{\theta}) = \{Kh : h \in H\}$, which, under the Correspondence Theorem, corresponds to the following subgroup of G containing K:

$$\begin{aligned}
\{g \in G : g\theta = Kh \text{ for some } h \text{ in } H\} &= \{g \in G : Kg = Kh \text{ for some } h \text{ in } H\} \\
&= \left\{g \in G : gh^{-1} \in K \text{ for some } h \text{ in } H\right\} \\
&= \{g \in G : g = kh \text{ for some } k \text{ in } K \text{ and some } h \text{ in } H\} \\
&= KH.
\end{aligned}$$

So KH is a subgroup of G containing K, and $\mathrm{Im}(\tilde{\theta}) = KH/K$. Obviously, KH contains H. This gives (i).

Moreover, $\ker(\tilde{\theta}) = \{h \in H : h\theta = \text{identity}\} = \ker(\theta) \cap H = K \cap H$, so $K \cap H$ is a normal subgroup of H. This gives (ii).

The First Isomorphism Theorem gives $H/K \cap H = H/\ker(\tilde{\theta}) \cong \mathrm{Im}(\tilde{\theta}) = KH/K$. $\square$

In any Hasse diagram, the convention is that if subgroups H and K are shown then so also is $K \cap H$, which is the largest subgroup contained in both of them. It is also conventional to show the smallest subgroup containing them both, which is just KH if either of them is normal in the whole group.

The following Hasse diagram depicts the Third Isomorphism Theorem. The parts of the diagram bettween KH and K, and between H and $H \cap K$, represent isomorphic groups.