HOMOMORPHISMS

KEITH CONRAD

1. Introduction

In group theory, the most important functions between two groups are those that "preserve" the group operations, and they are called homomorphisms. A function $f\colon G \to H$ between two groups is a *homomorphism* when

$$f(xy) = f(x)f(y) \text{ for all } x \text{ and } y \text{ in } G.$$

Here the multiplication in xy is in G and the multiplication in $f(x)f(y)$ is in H, so a homomorphism from G to H is a function that transforms the operation in G to the operation in H.

In Section 2 we will see how to interpret many elementary algebraic identities as group homomorphisms, involving the groups $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{R}^\times$, $\mathbf{R}_{>0}$, $\mathbf{C}$, and $\mathbf{C}^\times$. Section 3 describes some homomorphisms in linear algebra and modular arithmetic. Section 4 gives a few important examples of homomorphisms between more abstract groups. Section 5 has examples of functions between groups that are not group homomorphisms. Finally, in Section 6 we discuss several elementary theorems about homomorphisms.

2. Familiar homomorphisms

The first homomorphisms we will see are at the level of precalculus, and include identities such as the following:

$$c(x+y) = cx + cy, \quad |xy| = |x||y|, \quad (xy)^2 = x^2y^2,$$
$$a^{x+y} = a^xa^y, \quad (xy)^c = x^cy^c, \quad \log_a(xy) = \log_a x + \log_a y,$$

Example 2.1. For each real number c, the formula $c(x+y) = cx + cy$ for all x and y in $\mathbf{R}$ says that the function $M_c\colon \mathbf{R} \to \mathbf{R}$ where $M_c(x) = cx$ is a group homomorphism.

Example 2.2. For all real numbers x and y, $|xy| = |x||y|$. Therefore the absolute value function $f\colon \mathbf{R}^\times \to \mathbf{R}_{>0}$, given by $f(x) = |x|$, is a group homomorphism. (We exclude 0, even though it works in the formula, in order for the absolute value function to be a homomorphism on a group.)

Example 2.3. For $x \in \mathbf{R}^\times$, let $s(x)$ be its sign: $s(x) = 1$ for $x > 0$ and $s(x) = -1$ for $x < 0$. Then $s(xy) = s(x)s(y)$ for all x and y in $\mathbf{R}^\times$, so $s\colon \mathbf{R}^\times \to \{\pm 1\}$ is a homomorphism.

Example 2.4. For all real numbers x and y, $(xy)^2 = x^2y^2$, so the squaring map $f\colon \mathbf{R}^\times \to \mathbf{R}^\times$ where $f(x) = x^2$ is a homomorphism. (We exclude 0 from the domain, even though $(xy)^2 = x^2y^2$ when x or y is 0, in order to have the domain be a multiplicative group.) The squaring map is also a homomorphism $\mathbf{R}^\times \to \mathbf{R}_{>0}$, $\mathbf{R}_{>0} \to \mathbf{R}^\times$, and $\mathbf{R}_{>0} \to \mathbf{R}_{>0}$.

A function is not determined completely just by how you compute it, but also by the set on which it is defined and the set in which its values are considered to lie. Therefore the four ways we described squaring as a homomorphism are *different* functions, hence different homomorphisms; squaring $\mathbf{R}^\times \to \mathbf{R}^\times$ is neither injective nor surjective, squaring $\mathbf{R}^\times \to \mathbf{R}_{>0}$ is surjective but not injective, squaring $\mathbf{R}_{>0} \to \mathbf{R}^\times$ is injective but not surjective, and squaring $\mathbf{R}_{>0} \to \mathbf{R}_{>0}$ is injective and surjective.

Example 2.5. Fix an integer n. For all real numbers x and y, $(xy)^n = x^n y^n$, so the n-th power map $f\colon \mathbf{R}^\times \to \mathbf{R}^\times$, where $f(x) = x^n$, is a homomorphism.

Example 2.6. For all positive numbers x and y, $\sqrt{xy} = \sqrt{x}\sqrt{y}$, so the square root function $f\colon \mathbf{R}_{>0} \to \mathbf{R}_{>0}$, where $f(x) = \sqrt{x}$, is a homomorphism.

Example 2.7. Fix a nonzero real number a. Since $a^{m+n} = a^m a^n$ for all integers m and n the function $f\colon \mathbf{Z} \to \mathbf{R}^\times$ where $f(n) = a^n$ satisfies $f(m+n) = f(m)f(n)$ for all m and n, so f is a homomorphism from the (additive) group $\mathbf{Z}$ to the (multiplicative) group $\mathbf{R}^\times$.

Example 2.8. Fix nonzero real numbers a and b and let $f\colon \mathbf{Z}^2 \to \mathbf{R}^\times$ by $f(m,n) = a^m b^n$. For all integer pairs (m,n) and (m',n'), we have

$$f((m,n)+(m',n')) = f(m+m', n+n') = a^{m+m'}b^{n+n'} = a^m a^{m'} b^n b^{n'}$$

and

$$f(m,n)f(m',n') = a^m b^n a^{m'} b^{n'}.$$

The two computations produce the same answer, so $f((m,n)+(m',n')) = f(m,n)f(m',n')$. Therefore f is a homomorphism from $\mathbf{Z}^2$ (an additive group) to $\mathbf{R}^\times$ (a multiplicative group).

This can be extended to any finite number of bases: for any $a_1, \dots, a_k$ in $\mathbf{R}^\times$ we get a homomorphism $f\colon \mathbf{Z}^k \to \mathbf{R}^\times$ by $f(m_1, \dots, m_k) = a_1^{m_1} \cdots a_k^{m_k}$.

Example 2.9. Fix a positive real number a. We can raise a not just to integral powers, but to arbitrary real powers (this is false for negative a). The equation $a^{x+y} = a^x a^y$, valid for all real numbers x and y, tells us that the exponential function with base a, sending x to a^x, defines a homomorphism $\mathbf{R} \to \mathbf{R}^\times$ and it is injective (that is, $a^x = a^y \Rightarrow x = y$). The values of the function a^x are positive, and if we view a^x as a function $\mathbf{R} \to \mathbf{R}_{>0}$ then this homomorphism is not just injective but also surjective provided $a \neq 1$.

Example 2.10. Fixing $c > 0$, the formula $(xy)^c = x^c y^c$ for positive x and y tells us that the function $f\colon \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ where $f(x) = x^c$ is a homomorphism.

Example 2.11. For $a > 0$ with $a \neq 1$, the formula $\log_a(xy) = \log_a x + \log_a y$ for all positive x and y says that the base a logarithm $\log_a\colon \mathbf{R}_{>0} \to \mathbf{R}$ is a homomorphism.

The functions $x \mapsto a^x$ and $x \mapsto \log_a x$, from $\mathbf{R}$ to $\mathbf{R}_{>0}$ and from $\mathbf{R}_{>0}$ to $\mathbf{R}$ respectively, are probably the most important examples of homomorphisms in precalculus. Let's turn now to some homomorphisms involving complex numbers.

Example 2.12. For a complex number $z = a + bi$, with real part a and imaginary part b, its complex conjugate is $\overline{z} = a - bi$. For all z and w in $\mathbf{C}$,

$$\overline{z+w} = \overline{z} + \overline{w} \quad \text{and} \quad \overline{zw} = \overline{z}\,\overline{w}. \tag{2.1}$$

To verify these, we give names to the real and imaginary parts of z and w and compute both sides. Writing z as $a + bi$ and w as $c + di$, we have

$$\overline{z+w} = \overline{(a+bi)+(c+di)} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i$$

and

$$\overline{z} + \overline{w} = (a-bi)+(c-di) = (a+c)-(b+d)i,$$

which both match. For multiplication,

$$\overline{zw} = \overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i$$

and

$$\overline{z}\,\overline{w} = (a-bi)(c-di) = (ac-bd)+(a(-d)+(-b)c)i = (ac-bd)-(ad+bc)i.$$

Therefore complex conjugation defines homomorphisms $\mathbf{C} \to \mathbf{C}$ and $\mathbf{C}^\times \to \mathbf{C}^\times$.

Example 2.13. For a complex number $z = a+bi$, its absolute value is $|z| = \sqrt{a^2+b^2}$. When z and w are any complex numbers, $|zw| = |z||w|$, which implies that the absolute value function on nonzero complex numbers is a homomorphism $\mathbf{C}^\times \to \mathbf{R}_{>0}$. (We have to exclude 0 from the function to have a homomorphism, even though the formula itself is true when z or w is 0.)

To verify $|zw| = |z||w|$, write $z = a+bi$ and $w = c+di$. Then

$$|zw| = |(a+bi)(c+di)| = |(ac-bd)+(ad+bc)i| = \sqrt{(ac-bd)^2+(ad+bc)^2}$$

and

$$|z||w| = \sqrt{a^2+b^2}\sqrt{c^2+d^2} = \sqrt{(a^2+b^2)(c^2+d^2)} = \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2}.$$

These don't visibly look the same, but their equality falls out if we calculate $|zw|$ a little further: underneath the square root,

$$(ac-bd)^2+(ad+bc)^2 = (a^2c^2 - \underline{2acbd} + b^2d^2) + (a^2d^2 + \underline{2adbc} + b^2c^2),$$

and the two underlined terms on the right cancel. We are left with the sum of four terms that also appear under the square root in $|z||w|$, so $|zw| = |z||w|$.

Here is a slicker way to see why $|zw| = |z||w|$. We had previously checked that complex conjugation is multiplicative (that is, $\overline{zw} = \overline{z}\,\overline{w}$). Since $a^2+b^2 = (a+bi)(a-bi)$, we can write $|z|^2 = z\overline{z}$. Then

$$|zw|^2 = zw\overline{zw} = zw\overline{z}\,\overline{w} = z\overline{z}w\overline{w} = |z|^2|w|^2 = (|z||w|)^2.$$

Since $|zw|$ and $|z||w|$ are nonnegative real numbers, from their squares being equal we know they must be equal.

Example 2.14. The two addition laws for the sine and cosine functions are

$$\sin(x+y) = \sin x\cos y + \cos x \sin y, \quad \cos(x+y) = \cos x\cos y - \sin x\sin y. \tag{2.2}$$

These two separate formulas are complicated, but if we package them together as the real and imaginary part of a single function with values in the complex numbers then (2.2) becomes cleaner: letting $f\colon \mathbf{R} \to \mathbf{C}^\times$ by $f(x) = \cos x + i\sin x$, (2.2) is the same as $f(x+y) = f(x)f(y)$. That is, if you calculate the real and imaginary parts of $f(x+y)$ and of $f(x)f(y)$, then equality of the real parts is the addition formula for cosine and equality of the imaginary parts is the addition formula for sine. Therefore the equations (2.2) tell us that f is a homomorphism from $\mathbf{R}$ to $\mathbf{C}^\times$. (The values of $f(x)$ are definitely not 0 because $|f(x)| = \sqrt{\cos^2 x + \sin^2 x} = 1$ for all x.)

3. Examples in linear algebra and modular arithmetic

Example 3.1. Fix an $m \times n$ matrix A. Using A we get a matrix transformation $f\colon \mathbf{R}^n \to \mathbf{R}^m$ by $f(\mathbf{x}) = A\mathbf{x}$. Both $\mathbf{R}^n$ and $\mathbf{R}^m$ are additive groups and the formula $A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y}$ says that f is a homomorphism.

Example 3.2. For any 2×2 real matrices A and B, $\det(AB) = \det(A)\det(B)$. If we restrict our attention to invertible matrices, whose determinants are nonzero, then we have a homomorphism $\det\colon \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$.

(The identity $\det(AB) = \det(A)\det(B)$ can be checked by writing $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, computing AB as a 2×2 matrix, then $\det(AB)$, and checking it equals $\det(A)\det(B)$. If you take a second course in linear algebra you may see slicker ways to understanding why the determinant is multiplicative.)

Example 3.3. In the group $\mathrm{Aff}(\mathbf{R}) = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbf{R}^\times, b \in \mathbf{R}\}$, the formula for multiplication is

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}. \tag{3.1}$$

The upper left matrix entry lies in the group $\mathbf{R}^\times$, and under multiplication in $\mathrm{Aff}(\mathbf{R})$ the upper left entries multiply together, so we get a homomorphism $f\colon \mathrm{Aff}(\mathbf{R}) \to \mathbf{R}^\times$ by $f\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = a$. That is, (3.1) tells us $f(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)) = ac = f\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)f\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)$.

Another way to think about this is that the upper left matrix entry in $\mathrm{Aff}(\mathbf{R})$ is the determinant: $\det\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = a$, so multiplicativity of f is a special case of the multiplicativity of determinants.

Some of the previous examples work with $\mathbf{Z}/(m)$ in place of $\mathbf{R}$ and $(\mathbf{Z}/(m))^\times$ in place of $\mathbf{R}^\times$.

Example 3.4. For each $c \in \mathbf{Z}$ let $M_c\colon \mathbf{Z}/(m) \to \mathbf{Z}/(m)$ by $M_c(x \bmod m) = cx \bmod m$. The algebraic formula $c(x+y) \equiv cx + cy \bmod m$ means M_c is a homomorphism.

Example 3.5. Fixing a positive integer n, the congruence $(xy)^n \equiv x^n y^n \bmod m$ for all x and y in $\mathbf{Z}$ implies that the n-th power map $(\mathbf{Z}/(m))^\times \to (\mathbf{Z}/(m))^\times$ is a homomorphism.

Here is what cubing ($x \mapsto x^3$) looks like on $(\mathbf{Z}/(15))^\times$ and $(\mathbf{Z}/(21))^\times$.

$a \bmod 15$	1	2	4	7	8	11	13	14
$a^3 \bmod 15$	1	8	4	13	2	11	7	14

$a \bmod 21$	1	2	4	5	8	10	11	13	16	17	19	20
$a^3 \bmod 21$	1	8	1	20	8	13	8	13	1	20	13	20

In the first table, cubing permutes the elements of $(\mathbf{Z}/(15))^\times$, while in the second table there are only 4 cubes and each cube arises 3 times.

Example 3.6. Fixing an integer $m \geq 1$, we *define* addition in $\mathbf{Z}/(m)$ by $\overline{a} + \overline{b} = \overline{a+b}$. That is, the addition on the left is defined to be given by the formula on the right. Thus the *reduction map* $\mathbf{Z} \to \mathbf{Z}/(m)$, where $a \mapsto \overline{a}\,(= a \bmod m)$, is a homomorphism by definition.

Example 3.7. We can reduce not only from $\mathbf{Z}$ to any $\mathbf{Z}/(m)$, but from any $\mathbf{Z}/(m)$ to $\mathbf{Z}/(d)$ where $d|m$: if $a \equiv b \bmod m$, so $m|(a-b)$, then $d|(a-b)$ too, so $a \equiv b \bmod d$. For instance, $19 \equiv 7 \bmod 6$ and also $19 \equiv 7 \bmod 3$. Let $r\colon \mathbf{Z}/(m) \to \mathbf{Z}/(d)$ by $r(a \bmod m) = a \bmod d$. This is a homomorphism:

$$\begin{aligned} r(a \bmod m + b \bmod m) &= r(a + b \bmod m) \\ &= a + b \bmod d \\ &= a \bmod d + b \bmod d \\ &= r(a \bmod m) + r(b \bmod m). \end{aligned}$$

Here we write $a \bmod m$ and $a \bmod d$ instead of $\overline{a}$ as in Example 3.6, because the latter notation is now ambiguous on account of the use of two moduli, m and d, in this setup.

Example 3.8. For positive integers m and d with $d|m$, the reduction map $\mathbf{Z}/(m) \to \mathbf{Z}/(d)$ is not just additive, but multiplicative:

$$\begin{aligned} r(a \bmod m \cdot b \bmod m) &= r(ab \bmod m) \\ &= ab \bmod d \\ &= a \bmod d \cdot b \bmod d \\ &= r(a \bmod m) r(b \bmod m). \end{aligned}$$

If we focus on invertible numbers, then reduction sends $(\mathbf{Z}/(m))^\times$ to $(\mathbf{Z}/(d))^\times$ since an integer relatively prime to m is also relatively prime to any factor of m. Thus the *reduction map* $(\mathbf{Z}/(m))^\times \to (\mathbf{Z}/(d))^\times$, where $a \bmod m \mapsto a \bmod d$, is a homomorphism.

Here are examples of reduction $(\mathbf{Z}/(15))^\times \to (\mathbf{Z}/(3))^\times$ and $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(7))^\times$, as tables.

$a \bmod 15$	1	2	4	7	8	11	13	14
$a \bmod 3$	1	2	1	1	2	2	1	2

$a \bmod 21$	1	2	4	5	8	10	11	13	16	17	19	20
$a \bmod 7$	1	2	4	5	1	3	4	6	2	3	5	6

In both tables, every value occurs the same number of times (4 times in the first table and 2 times in the second table). We saw this in the tables at the end of Example 3.5: each value of a homomorphism occurs equally often.

4. Other examples

Example 4.1. For any permutation $\sigma \in S_n$, its sign $\operatorname{sgn}(\sigma)$ is ± 1 and the formula $\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')$ for all σ and σ' in S_n tells us that $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ is a homomorphism.

Example 4.2. For any groups G and H there is always at least one homomorphism from G to H, namely the *trivial homomorphism* $f\colon G \to H$ where $f(x) = e_H$ for all $x \in G$. Every value of f is the identity element of H. Then $f(x)f(y) = e_He_H = e_H = f(xy)$. For some groups the only homomorphism between them is the trivial homomorphism (*e.g.*, $G = \mathbf{Z}/(3)$ and $H = \mathbf{Z}/(5)$).

Example 4.3. Let G be an *abelian* group and n be an integer (positive, negative, or 0). The formula

$$(gh)^n = g^n h^n$$

for all $g, h \in G$ says that the nth power map $G \to G$, where $g \mapsto g^n$, is a homomorphism from G to itself.

Warning: Power functions are usually not homomorphisms on nonabelian groups! For example, if D_4, we have $(rs)^3 = rs$ while $r^3s^3 = r^3s$, and $rs \neq r^3s$ because $r \neq r^3$, so $f(x) = x^3$ on D_4 is not a homomorphism. The exact same calculation goes through in D_m for any $m \geq 3$.

Example 4.4. In a group G, fix an element g. Its powers satisfy

$$g^{m+n} = g^m g^n$$

for all integers m and n, so we get a homomorphism $\mathbf{Z} \to G$ given by $n \mapsto g^n$ is a homomorphism. Note G doesn't have to be abelian here; the only values we meet are powers of g, and powers of a single element always commute with each other, whether or not the whole group is abelian.

Example 4.5. Fix an element g in a group G. Conjugation by g is a function $\gamma_g\colon G \to G$, given by $\gamma_g(x) = gxg^{-1}$, and it is a homomorphism:

$$\gamma_g(x)\gamma_g(y) = (gxg^{-1})(gyg^{-1}) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \gamma_g(xy).$$

While power functions on abelian groups might not be invertible (*e.g.*, squaring on $\mathbf{R}^\times$ is not invertible since $x^2 = (-x)^2$), conjugation on any group by any element is *always* invertible: just conjugate by the inverse element. Indeed,

$$\gamma_{g^{-1}}(\gamma_g(x)) = \gamma_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})g = g^{-1}gxg^{-1}g = x$$

for every $x \in G$, so γ_g and $\gamma_{g^{-1}}$ are inverses of each other.

5. Nonexamples

Nonexample 5.1. On the group $\mathrm{GL}_2(\mathbf{R})$, let $f(A) = A^2$, so $f\colon \mathrm{GL}_2(\mathbf{R}) \to \mathrm{GL}_2(\mathbf{R})$. For most A and B, $f(AB) \neq f(A)f(B)$. For instance, let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Then $AB = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, so $f(AB) = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right)$, while $f(A)f(B) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^2\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 5 & 2 \\ 2 & 1 \end{smallmatrix}\right)$.

Nonexample 5.2. On any group G the nth power map $G \to G$, where $x \mapsto x^n$, makes sense, but it usually is not a homomorphism when G is nonabelian. The previous example shows squaring on $\mathrm{GL}_2(\mathbf{R})$ is not a homomorphism. We saw after Example 4.3 that cubing on D_4, or on D_m for any $m \geq 3$, is not a homomorphism.

When $n = -1$ or 2, the nth power map is a homomorphism from G to G *only* when G is abelian:

$$(xy)^2 = x^2y^2 \iff xyxy = xxyy \iff yx = xy$$

and

$$(xy)^{-1} = x^{-1}y^{-1} \iff (xy)^{-1} = (yx)^{-1} \iff xy = yx.$$

Nonexample 5.3. While $\det(AB) = \det(A)\det(B)$ for all 2×2 real matrices A and B, the determinant $\mathrm{M}_2(\mathbf{R}) \to \mathbf{R}$ is not a homomorphism since $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{R}$ are not groups for multiplication.

Nonexample 5.4. For a 2×2 real matrix A, its exponential is defined by the infinite matrix series

$$\exp(A) := \sum_{n \geq 0} \frac{1}{n!}A^n = I_2 + A + \frac{1}{2}A^2 + \frac{1}{6}A^3 + \cdots.$$

It is true that $\exp(A)\exp(-A) = I_2$, so $\exp(A) \in \mathrm{GL}_2(\mathbf{R})$. Therefore the 2×2 matrix exponential is a function $\mathrm{M}_2(\mathbf{R}) \to \mathrm{GL}_2(\mathbf{R})$, from an additive group to a multiplicative group. This is analogous to the classical exponential function being a function $\mathbf{R} \to \mathbf{R}^\times$. However, the matrix exponential is *not* a homomorphism: $\exp(A+B)$ is usually *not* equal to $\exp(A)\exp(B)$. As a specific example, if $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ then $\exp(A) = \left(\begin{smallmatrix} e & e \\ 0 & e \end{smallmatrix}\right)$, $\exp(B) = \left(\begin{smallmatrix} e & 0 \\ e & e \end{smallmatrix}\right)$, so $\exp(A)\exp(B) = \left(\begin{smallmatrix} 2e^2 & e^2 \\ e^2 & e^2 \end{smallmatrix}\right)$, but $\exp(A+B) = \left(\begin{smallmatrix} (e^3+e)/2 & (e^3-e)/2 \\ (e^3-e)/2 & (e^3+e)/2 \end{smallmatrix}\right)$.

Nonexample 5.5. In Example 3.3 we saw that the function $f\colon \mathrm{Aff}(\mathbf{R}) \to \mathbf{R}^\times$ by $f\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = a$ is a homomorphism. However, the function $f\colon \mathrm{Aff}(\mathbf{R}) \to \mathbf{R}$ by $f\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) = b$ is not a homomorphism. Indeed, from the multiplication formula (3.1) we have $f(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)) = ad+b$, while $f\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)+f\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = b + d$. These don't match in general (anytime $d \neq 0$ and $a \neq 1$).

6. A few theorems about homomorphisms

Theorem 6.1. *Let $f\colon G \to H$ be a group homomorphism.*

1. *$f(e_G) = e_H$, i.e., the identity in G goes to the identity in H.*
2. *For all $x \in G$, $f(x^{-1}) = f(x)^{-1}$.*
3. *For all $n \in \mathbf{Z}$ and $x \in G$, $f(x^n) = f(x)^n$.*

Proof. 1) Apply f to both sides of the equation $e_Ge_G = e_G$. We get $f(e_G)f(e_G) = f(e_G)$. Cancel $f(e_G)$ from both sides to get $f(e_G) = e_H$.

2) Apply f to both sides of the equation $xx^{-1} = e_G$ to get $f(x)f(x^{-1}) = f(e_G) = e_H$. Therefore $f(x)$ is the inverse of $f(x^{-1})$.

3) We will prove this for $n \geq 1$ by induction. That $f(x^n) = f(x)^n$ when $n = 1$ is obvious. Assuming $f(x^n) = f(x)^n$ for some $n \geq 1$, we get $f(x^{n+1}) = f(x^nx) = f(x^n)f(x) = f(x)^nf(x) = f(x)^{n+1}$; the 3rd equality at the end used the induction hypothesis.

For $n = 0$ the identity $f(x^n) = f(x)^n$ is the same as $f(e_G) = e_H$, which is true by the first part of the theorem. For $n < 0$, write $n = -N$ with $N \geq 1$. Then

$$f(x^n) = f(x^{-N}) = f((x^N)^{-1}) = f(x^N)^{-1} = (f(x)^N)^{-1} = f(x)^{-N} = f(x)^n,$$

where we used the proved case of positive exponents and exponent -1 in the calculation. □

Example 6.2. For an exponential function $x \mapsto a^x$, which is a homomorphism $\mathbf{R} \to \mathbf{R}_{>0}$, Theorem 6.1 becomes the known identities $a^0 = 1$, $a^{-x} = (a^x)^{-1}$, and $a^{nx} = (a^x)^n$ (note that in an *additive* group such as $\mathbf{R}$, the abstract multiplicative notation x^n becomes nx).

Example 6.3. For a logarithm function $x \mapsto \log_a x$, which is a homomorphism $\mathbf{R}_{>0} \to \mathbf{R}$, Theorem 6.1 becomes the identities $\log_a(1) = 0$, $\log_a(1/x) = -\log_a x$, and $\log_a(x^n) = n\log_a x$.

Corollary 6.4. *If $f\colon G \to H$ is a homomorphism and $x \in G$ has order n, then $f(x)$ has order dividing n.*

Proof. Since x has order n, $x^n = e_G$. Applying f to both sides, $f(x)^n = e_H$, so the order of $f(x)$ divides n. □

Example 6.5. In the second table of Example 3.8 we see the effect of the reduction homomorphism $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(7))^\times$. The number 11 mod 21 has order 6, while 11 mod 7 reduces to 4, which has order 3. The number 8 mod 21 has order 2 , while 8 mod 7 it reduces to 1, which has order 1.

Theorem 6.6. *The composition of homomorphisms is a homomorphism: if $f_1\colon G_1 \to G_2$ and $f_2\colon G_2 \to G_3$ are homomorphisms, then the composite function $f_2 \circ f_1\colon G_1 \to G_3$ is a homomorphism.*

Proof. This is *straightforward*: for all x and y in G_1, we have

$$(f_2 \circ f_1)(xy) = f_2(f_1(xy)) = f_2(f_1(x)f_1(y)) = f_2(f_1(x))f_2(f_1(y)) = (f_2 \circ f_1)(x)(f_2 \circ f_1)(y).$$

□

Example 6.7. The function $f\colon \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}_{>0}$ where $f(A) = |\det A|$ is a homomorphism since it is the composition of the determinant $\det\colon \mathrm{GL}_2(\mathbf{R}) \to \mathbf{R}^\times$ and absolute value $|\cdot|\colon \mathbf{R}^\times \to \mathbf{R}_{>0}$, which are both homomorphisms.

For a function $f\colon X \to Y$, the *image* of a subset $A \subset X$ is $f(A) := \{f(a) : a \in A\}$, and the *inverse image* of a subset $B \subset Y$ is $f^{-1}(B) := \{x \in X : f(x) \in B\}$.

Example 6.8. Let $f\colon \mathbf{R} \to \mathbf{R}$ by $f(x) = x^2 + 1$. (This is not a homomorphism, just a function.) Then $f(\{4,8\}) = \{17,65\}$, $f^{-1}(\{5\}) = \{2,-2\}$, $f([1,3]) = [2,10]$, $f^{-1}([2,10]) = [1,3] \cup [-3,-1]$, and $f^{-1}(1/2) = \emptyset$.

Theorem 6.9. *Let $f\colon G \to H$ be a homomorphism of groups.*

(1) *The image of a subgroup of G is a subgroup of H. In particular, $f(G)$ is a subgroup of H.*
(2) *The inverse image of a subgroup of H is a subgroup of G.*

Proof. 1) Let K be a subgroup of G, so $f(K) = \{f(k) : k \in K\}$. Showing this is a subgroup of H is a *straightforward* calculation using definitions:

- The identity of H is in $f(K)$ since $e_H = f(e_G)$ and $e_G \in K$.
- Pick any two elements of $f(K)$. They have the form $f(k)$ and $f(k')$ for some k and k' in K. Then their product is $f(k)f(k') = f(kk')$, and $kk' \in K$ since K is a subgroup of G. Thus $f(k)f(k') \in f(K)$.
- Pick any element of $f(K)$. It has the form $f(k)$ for some $k \in K$. Its inverse is $f(k)^{-1} = f(k^{-1})$, and $k^{-1} \in K$ since K is a subgroup of G. Therefore $f(k)^{-1} \in f(K)$.

2) Choose a subgroup L of H. To see that $f^{-1}(L)$ is a subgroup of G we just check the definitions.

- Since $f(e_G) = e_H \in L$, we get $e_G \in f^{-1}(L)$.
- Pick any two elements of $f^{-1}(L)$, say x and y. That means $f(x) \in L$ and $f(y) \in L$. Since L is a subgroup of H, $f(x)f(y) \in L$, so $f(xy) \in L$. Therefore $xy \in f^{-1}(L)$.
- Pick any element of $f^{-1}(L)$, say x. Then $f(x) \in L$. Since $f(x^{-1}) = f(x)^{-1}$, and L is a subgroup of H, we have $f(x)^{-1} \in L$. Therefore $f(x^{-1}) \in L$, so $x^{-1} \in f^{-1}(L)$.

□

Example 6.10. By Example 3.5, cubing $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(21))^\times$ has image $\{1, 8, 13, 20 \bmod 21\}$, and this is a subgroup of $(\mathbf{Z}/(21))^\times$.

Example 6.11. By Example 3.5, cubing $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(21))^\times$ on the subgroup $\langle 2 \bmod 21\rangle = \{1, 2, 4, 8, 16, 11\}$ has image $\{1, 8 \bmod 21\}$, and this is a subgroup of $(\mathbf{Z}/(21))^\times$.

Example 6.12. In $(\mathbf{Z}/(21))^\times$, $\langle 20 \bmod 21\rangle = \{1, 20\}$. By Example 3.5, the inverse image of $\{1, 20\}$ under the cubing map $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(21))^\times$ is $\{x : x^3 \equiv 1 \text{ or } 20 \bmod 21\} = \{1, 4, 5, 16, 17, 20\} = \langle 5\rangle$, and this is a subgroup of $(\mathbf{Z}/(21))^\times$.

7. The kernel of a homomorphism

There is no simple test for showing a homomorphism is surjective in general, but here is a very important way to show a homomorphism is injective.

Theorem 7.1. *A homomorphism $f\colon G \to H$ is injective if and only if the unique solution to $f(x) = e_H$ is e_G.*

The condition in this theorem is saying that when a homomorphism takes the value e_H just once (necessarily at $x = e_G$) then there is at most one way it takes any other value.

Proof. First suppose f is injective. The condition $f(x) = e_H$ is the same as $f(x) = f(e_G)$, and by injectivity of f this equality implies $x = e_G$.

Now suppose the only solution to $f(x) = e_H$ is $x = e_G$. To show f is injective, suppose $f(g) = f(g')$. Because f is a homomorphism, we can rewrite the condition $f(g) = f(g')$ in the form $f(\text{something}) = e_H$:

$$f(g) = f(g') \Longrightarrow f(g)f(g')^{-1} = e_H \Longrightarrow f(g)f((g')^{-1}) = e_H \Longrightarrow f(g(g')^{-1}) = e_H.$$

Therefore $g(g')^{-1} = e_G$, so $g = g'$. □

We can see Theorem 7.1 at work in the tables at the end of Example 3.5: cubing on $(\mathbf{Z}/(15))^\times$ is injective and 1 occurs as a value just once, while cubing on $(\mathbf{Z}/(21))^\times$ is not injective and 1 appears as a value several times. Similarly, the reduction homomorphisms $(\mathbf{Z}/(15))^\times \to (\mathbf{Z}/(3))^\times$ and $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(7))^\times$ in the tables at the end of Example 3.8 are not injective and 1 appears as a value of each homomorphism multiple times.

Knowing how the identity appears as the value of a homomorphism is important, and gets the following name.

Definition 7.2. The *kernel* of a group homomorphism $f\colon G \to H$ is the set of elements in G sent to the identity:

$$\ker f = \{x \in G : f(x) = e_H\}.$$

Example 7.3. The squaring map $\mathbf{R}^\times \to \mathbf{R}^\times$ has kernel $\{\pm 1\}$. This is the solution set to $x^2 = 1$.

Example 7.4. From tables in Example 3.5, cubing $(\mathbf{Z}/(15))^\times \to (\mathbf{Z}/(15))^\times$ has trivial kernel $\{1\}$ and cubing $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(21))^\times$ has kernel $\{1, 8, 13, 20 \bmod 21\}$.

Example 7.5. From tables in Example 3.8, the reduction homomorphism $(\mathbf{Z}/(15))^\times \to (\mathbf{Z}/(3))^\times$ has kernel $\{1, 4, 7, 13 \bmod 15\}$ and reduction $(\mathbf{Z}/(21))^\times \to (\mathbf{Z}/(7))^\times$ has kernel $\{1, 8 \bmod 21\}$.

Example 7.6. The sign homomorphism $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ has kernel A_n, the alternating group on n letters.

Example 7.7. The homomorphism $\operatorname{Aff}(\mathbf{R}) \to \mathbf{R}^\times$ from Example 3.3, where $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mapsto a$, has kernel $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \mathbf{R}\}$.

Most homomorphisms from precalculus have trivial kernel, so the kernel is not something interesting at that level. But it is something that is met in linear algebra, under a different name:

Example 7.8. For an $m \times n$ matrix A, the homomorphism $f\colon \mathbf{R}^n \to \mathbf{R}^m$ where $f(\mathbf{x}) = A\mathbf{x}$ has kernel $\{\mathbf{x} \in \mathbf{R}^n : A\mathbf{x} = \mathbf{0}\}$. In linear algebra this kernel is known as the *null space* of A.

Here is a kernel of a homomorphism that is related to periodicity of the trigonometric functions.

Example 7.9. The homomorphism $\mathbf{R} \to \mathbf{C}^\times$ from Example 2.14, where $x \mapsto \cos x + i \sin x$, has kernel

$$\{x \in \mathbf{R} : \cos x + i \sin x = 1\} = \{x \in \mathbf{R} : \cos x = 1 \text{ and } \sin x = 0\} = 2\pi\mathbf{Z},$$

the integral multiples of 2π.

Theorem 7.10. *The kernel of a homomorphism $f\colon G \to H$ is a subgroup of G.*

Proof. This is a *straightforward* calculation using definitions:

- Since $f(e_G) = e_H$, $e_G \in \ker f$.
- For all x and y in $\ker f$, $f(xy) = f(x)f(y) = e_H e_H = e_H$, so $xy \in \ker f$.
- For all $x \in \ker f$, $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in \ker f$.

Theorem 7.10 is a special case of part 2 of Theorem 6.9, since $\ker f = \{x \in G : f(x) = e_H\} = f^{-1}(\{e_H\})$, which is the inverse image of the trivial subgroup of H. □

Theorem 7.11. *If $f\colon G \to H$ is a homomorphism with kernel K, then $f(x) = f(y)$ if and only if $y = xk$ for some $k \in K$.*

Proof. Suppose $f(x) = f(y)$. We want to show $y = xk$ for some $k \in K$. Necessarily $k = x^{-1}y$, so we want to show $x^{-1}y \in K$. This is a direct calculation: $f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) = e_H$.

Conversely, suppose $y = xk$ where $k \in K$. Then $f(y) = f(xk) = f(x)f(k) = f(x)$. □

Example 7.12. The squaring function $\mathbf{R}^\times \to \mathbf{R}^\times$ has kernel ± 1, and Theorem 7.11 in this instance says something familiar: $x^2 = y^2$ in $\mathbf{R}^\times$ if and only if $y = \pm x$. The way this is seen in school is

$$x^2 = y^2 \iff y^2 - x^2 = 0 \iff (y+x)(y-x) = 0 \iff y + x = 0 \text{ or } y - x = 0 \iff y = \pm x.$$

This is *not* the way the proof of Theorem 7.11 works. Instead, that proof in this instance would use only multiplication and division: for nonzero real numbers x and y,

$$x^2 = y^2 \iff \frac{y^2}{x^2} = 1 \iff \left(\frac{y}{x}\right)^2 = 1 \iff \frac{y}{x} = \pm 1 \iff y = \pm x.$$