Lecture 6

Ring homomorphisms

6.1 Goals

1. Understand the definition of a ring homomorphism
2. Understand the natural ring homomorphism from $\mathbb{C}$ to $M_2(\mathbb{R})$
3. Understand that ring homomorphisms can allow us to deduce a lot of interesting facts

6.2 $\mathbb{C}$ and $M_2(\mathbb{R})$ act on $\mathbb{R}^2$

At this point, we have seen that $\mathbb{C}$ acts on $\mathbb{R}^2$ by scaling and rotating. We have also seen that $M_2(\mathbb{R})$—the ring of 2-by-2 real matrices—acts on $\mathbb{R}^2$ by linear transformations. In the exercises, we have further seen that rotations (Exercise 4.5.1) and scaling (Exercise 4.5.9) are examples of linear transformations.

On the other hand, $\mathbb{C}$ and $M_2(\mathbb{R})$ feel very different. The former requires 2 real numbers to specify an element, so feels two-dimensional. The latter requires 4 real numbres to specify an element, so feels four-dimensional. Moreover, as rings, $\mathbb{C}$ is commutative while $M_2(\mathbb{R})$ definitely is not.

Is there a way to relate the fact that two seemingly different rings act in very similar ways?

6.3 Thinking of complex numbers as matrices

One can take a hint from Exercise 4.5.1, which represents rotation by θ as a matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

This matrix acts by taking the point $(1, 0)$ to the point $(\cos\theta, \sin\theta)$. In terms of complex numbers, it acts by taking the complex number 1 to the complex number $\cos\theta + i\sin\theta$. In other words, it seems like this matrix behaves like multiplication by the complex number $\cos\theta + i\sin\theta$.

Taking this hint from mother nature, we could see if the action by a complex number $a + bi$ acts like the action of the matrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

In fact, let's define a *function* from $\mathbb{C}$ to $M_2(\mathbb{R})$ as follows:

$$\rho : \mathbb{C} \to M_2(\mathbb{R}), \qquad a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Proposition 6.3.1. ρ is an injection.

The above proposition allows you think of $\mathbb{C}$ as "sitting inside" $M_2(\mathbb{R})$—more accurately, ρ "embeds" $\mathbb{C}$ into $M_2(\mathbb{R})$. So you can think of every complex number as a matrix. But that's just a statement about sets, and one can find many (meaningless) injections from $\mathbb{C}$ to $M_2(\mathbb{R})$. Here is a far more substantive statement about the "algebra" that ρ manifests:

Proposition 6.3.2. The function ρ satisfies the following properties:

(a) (ρ respects addition.) $\rho(z + z') = \rho(z) + \rho(z')$.

(b) (ρ respects multiplication.) $\rho(zz') = \rho(z)\rho(z')$.

(c) (ρ respects the multiplicative identity.) $\rho(1)$ is the multiplicative identity of $M_2(\mathbb{R})$.

Proposition 6.3.2 says that $\mathbb{C}$ can be made to sit inside $M_2(\mathbb{R})$ in an incredibly rich way. For example, (a) states that the embedding of $\mathbb{C}$ into

$M_2(\mathbb{R})$ "respects addition"—if you want to understand the addiction of two complex numbers, you can just as well understand the addition of matrices. And (b) states the same for multiplication.[1] The last item is also nice—it states that the complex number that "does nothing" when multiplied is also send to the matrix that does nothing when multiplying.

6.4 Ring homomorphisms

Before we delve into the Propositions, their proofs, and the consequences, let me introduce the terminology we'll use.

Definition 6.4.1. Let R and S be rings, and let $f : R \to S$ be a function. We will say that f is a *ring homomorphism* if the following are satisfied:

(a) For all $x, y \in R$, $f(x + y) = f(x) + f(y)$. If f satisfies this property, we say that f *respects addition.*

(b) For all $x, y \in R$, $f(xy) = f(x)f(y)$. If f satisfies this property, we say that f *respects multiplication.*

(c) Let 1_R and 1_S be the multiplicative identities of R and S, respectively. We ask that $f(1_R) = 1_S$. If f satisfies this property, we say that f *respects the multiplicative identity.*

Thus, Proposition 6.3.2 can be succinctly rephrased as: ρ is a ring homomorphism. Note that a ring homomorphism is *not* required to be an injection. ρ, being an injection, is a very special kind of ring homomorphism.

Remark 6.4.2. You may have seen the word "homomorphism" elsewhere. In general, you should think of a homomorphism as a kind of function that preserves some structure—and which structure you want to preserve depends on the context. Here, because we are studying rings, we want *ring* homomorphisms to preserve the structures that rings have.

Warning 6.4.3. Please try to never, ever use the adjective "homomorphic." This is despite the fact that the adjective "isomorphic" is commonly used in mathematics. (We will see this term later in the course.)

[1] This is kind of cool—I don't know whether you find matrix multiplication or complex multiplication more appealing, but (after applying ρ) one sees that one can phrase complex multiplication purely through matrix multiplication.

An astute reader will notice that there are *other* properties rings enjoy that are not mentioned in the definition of a ring homomorphism. For example, while the definition above requires that multiplicative identities be respected, how about additive identities? There seems to be no requirement that $f(0_R) = 0_S$. Likewise, how about additive inverses? Should we require that $f(-x) = -f(x)$ for all x? As it turns out, such equalities are *automatic* just by knowing that f is a ring homomorphism.

Proposition 6.4.4. Let $f : R \to S$ be a ring homomorphism. Then

1. $f(0_R) = 0_S$. In other words, f respects additive identities.
2. For every $x \in R$, $f(-x) = -x$. In other words, f respects additive inverses.

Proof. To prove the first claim, note that $0_R + 0_R = 0_R$ because 0_R is an additive identity. Applying f to both sides, we see that

$$f(0_R + 0_R) = f(0_R).$$

On the other hand, because f is a ring homomorphism (and hence respects addition), the lefthand side equals $f(0_R) + f(0_R)$. We thus conclude

$$f(0_R) + f(0_R) = f(0_R).$$

Now, whatever $f(0_R)$ is, it has some additive inverse because S is a ring. Call it s, and add s to both sides. We then have

$$\begin{align} s + f(0_R) + f(0_R) &= s + f(0_R) \tag{6.4.0.1} \\ (s + f(0_R)) + f(0_R) &= s + f(0_R) \tag{6.4.0.2} \\ 0_S + f(0_R) &= 0_S \tag{6.4.0.3} \\ & \tag{6.4.0.4} \end{align}$$

where the second line uses associativity, and the last line uses the definition of additive inverse in S. Now note that 0_S is the additive identity of S to change the lefthand side. We conclude

$$f(0_R) = 0_S$$

which is what we wanted to prove.

To prove the claim that f respects additive inverses, let $-x$ be the additive inverse to x, so that $-x + x = 0_R$. Applying f to both sides, and using the fact that f respects addition by hypothesis, we conclude

$$f(-x) + f(x) = f(0_R).$$

By the first part of our proposition, the righthand side is equal to 0_S, so we have

$$f(-x) + f(x) = 0_S.$$

Thus, $f(-x)$ precisely satisfies the property needed to be the additive inverse to $f(x)$. Of course, the usual notation for an additive inverse to *blah* is $-$*blah*, so we conclude

$$f(-x) = -f(x).$$

□

6.5 Our first examples of a proof that a function is a ring homomorphism

For practice, let's prove Proposition 6.3.2. (We'll leave it to you to verify Proposition 6.3.1 as Exercise 6.7.3.)

Proof of Proposition 6.3.2. Let $z, z' \in \mathbb{C}$ and write $z = a+bi$ and $z' = a'+b'i$.

Proof of (a): We must show that $\rho(z + z') = \rho(z) + \rho(z')$. We have:

$$\begin{aligned}
\rho(z + z') &= \rho((a + a') + (b + b')i) \\
&= \begin{pmatrix} a + a' & -(b + b') \\ b + b' & a + a' \end{pmatrix} \\
&= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \\
&= \rho(a + bi) + \rho(a' + b'i) \\
&= \rho(z) + \rho(z').
\end{aligned}$$

Proof of (b): We compute:

$$\begin{aligned}\rho(zz') &= \rho((aa' - bb') + (ab' + a'b)i) \\ &= \begin{pmatrix} aa' - bb' & -(ab' + a'b) \\ ab' + a'b & aa' - bb' \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \\ &= \rho(a + bi)\rho(a' + b'i) \\ &= \rho(z)\rho(z').\end{aligned}$$

Proof of (c): If $z = 1$, then $a = 1$ and $b = 0$, so

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

□

Remark 6.5.1 (The ingredients of proving that a function is a ring homomorphism)**.** You may often in life (or, more realistically, in this course) be asked to show that a particular function is a ring homomorphism. The ingredients going into such proofs are almost all the same:

1. An understanding of what addition is in both the domain and in the codomain.

2. An understanding of what multiplication is in both the domain and in the codomain.

3. An understanding of what the function in question does—e.g., how it is defined.

For example, to show above that $\rho(z + z') = \rho(z) + \rho(z')$, I had to do the following (and I could have done these in any order):

- Compute $z + z'$ so I understand the term inside the parentheses in $\rho(z + z')$.

- Compute $\rho(z + z')$ using my understanding of ρ.

- Perhaps by being clever, see that $\rho(z + z')$ is indeed a sum of two elements in the codomain. This is often the least trivial step, and requires an understanding of addition in the codomain.

- Compute $\rho(z)$ and $\rho(z')$, and show that their sum is the desired term.

Note that these steps only require knowledge of ρ and of the additions in $\mathbb{C}$ and $M_2(\mathbb{R})$, because the thing I'm trying to prove only involves these two things. To prove $\rho(zz') = \rho(z)\rho(z')$, one would have to use familiarity with multiplication, not addition.

6.6 Applications of ρ being a ring homomorphism

A ring homomorphism like ρ can give you a lot of information—both about the domain, and the codomain. Here are a few examples of data flowing in one direction: We learn a lot about certain matrices just by knowing things about $\mathbb{C}$.

Some terminology: Recall that a "corollary" is an immediate consequence of some other logical statement.

Corollary 6.6.1 (Of Proposition 6.3.2)**.** *Let A and B be matrices of the following form:*

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \qquad B = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}.$$

Then $AB = BA$.

Proof. Let $z = a + bi$ and $w = c + di$, so $A = \rho(z)$ and $B = \rho(w)$. We have that

$$AB = \rho(z)\rho(w) = \rho(zw) = \rho(wz) = \rho(w)\rho(z) = BA.$$

The middle equality uses the fact that multiplication in $\mathbb{C}$ is commutative. The two equalities adjacent to the middle use the fact that ρ is a ring homomorphism (so that ρ respects multiplication). □

Of course, one could have prove that $AB = BA$ by doing matrix computations, but there is something very satisfying about seeing this fact by only relying on more birds-eye-view truths: Because $\mathbb{C}$ can be made to embed inside $M_2(\mathbb{R})$ in a nice, algebraic way, and because multiplication in $\mathbb{C}$ is commutative, we've identified a bunch of matrices in $M_2(\mathbb{R})$ (the image of $\mathbb{C}$) which commute with each other.

Here is a far less trivial application. Before we state the result, let us set some notation:

Notation 6.6.2 (Polynomials of matrices)**.** Recall that given a matrix A and a real number λ, the notation λA represents the scaling of A by λ (Definition 3.3.10). More generally, we will often treat the number λ also as a diagonal matrix with entries λ along the diagonal (and zeroes elsewhere).

Finally, we also let A^k denote the matrix obtained by multiplying A by itself k times.

Example 6.6.3 (Polynomial equations of matrices)**.** In this way, an expression like

$$A^3 + \pi A^2 - \sqrt{2}$$

makes sense. For example, if

$$A = \begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}$$

then the above expression can be written out as

$$\begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix} + \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix} - \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

And we can ask someone to solve the matrix equation

$$A^3 + \pi A^2 - \sqrt{2} = 0$$

to find a matrix A so that the lefthand side equals the zero matrix.

Theorem 6.6.4. Fix any collection of real numbers $a_0, \ldots, a_n$. Then the matrix equation

$$a_n A^n + \ldots + a_2 A^2 + a_1 A + a_0 = 0$$

has a solution. In fact, one can find a matrix A satisfying this equation for which A is of the form

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Proof. Consider the polynomial equation

$$a_n z^n + \ldots + a_2 z^2 + a_1 z + a_0 = 0.$$

By the fundamental theorem of algebra, this equation has a complex number solution. Let $w = a + bi$ be one solution, and define A to be $\rho(w)$. Now, by applying ρ on both sides of the equation, we know that

$$\rho(a_n w^n + \ldots + a_2 w^2 + a_1 w + a_0) = \rho(0).$$

The righthand side of course simplifies to the zero matrix. The lefthand side simplifies as follows:

$$\begin{aligned}\rho(a_n w^n + \ldots + a_2 w^2 + a_1 w + a_0) &= \rho(a_n w^n) + \ldots + \rho(a_2 w^2) + \rho(a_1 w) + \rho(a_0)\\ &= \rho(a_n)\rho(w^n) + \ldots + \rho(a_2)\rho(w^2) + \rho(a_1)\rho(w) + \rho(a_0)\\ &= a_n\rho(w^n) + \ldots + a_2\rho(w^2) + a_1\rho(w) + a_0\\ &= a_n A^n + \ldots + a_2 A^2 + a_1 A + a_0\end{aligned}$$

The first equality is because ρ respects addition. The next equality is because ρ respects multiplication. The next one involves just writing out what ρ does to the complex number $a_n = a_n + 0i$, and interpreting multiplication by a diagonal matrix as scaling. The last equality uses the fact that ρ respects multiplication, so that $\rho(w^k) = \rho(w)^k = A^k$. □

Example 6.6.5. Is there some 2-by-2 real matrix satisfying the equation

$$A^3 + \pi A^2 - \sqrt{2} = 0?$$

Yes, there is. If you let w be the complex number satisfying the equation $w^3 + \pi w^2 - \sqrt{2} = 0$, then $\rho(w)$ is a matrix that satisfies the above equation (as shown in the above proof). Now, the above proof uses the fundamental theorem of algebra—this theorem tells you that such a w exists, but it doesn't tell you how to find it. Because of this, while we know that a solution exists, we don't have much access to what the solution actually is. That is for a different math course.

Regardless, isn't it incredibly powerful to *know* that a solution must exist? This is in great contrast to many problems in life, and in math, where we try to tackle problems without knowing even if there is a solution.

So far, none of our applications/results have relied on the fact that ρ is an injection. Here is one application that does:

Corollary 6.6.6. Let p be any real, degree n matrix polynomial. Then there are at least n matrices (counted with multiplicity) that satisfy the polynomial.

Proof. Think of p as a polynomial of a complex variable. The fundamental theorem of algebra exactly guarantees n roots (counted with multiplicity) to a degree n polynomial. Because ρ is an injection, distinct elements of $\mathbb{C}$ are sent to distinct elements of $M_2(\mathbb{R})$, concluding the proof. □

6.7 Exercises

Exercise 6.7.1. Let $f : \mathbb{C} \to \mathbb{C}$ be the function taking $a + bi$ to the complex number $a - bi$. Show that f is a ring homomorphism and a bijection.

Exercise 6.7.2. Let $f : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ be the function taking a matrix to its transpose.

(a) Show that f is not a ring homomorphism. (What is the one homomorphism property that f fails?)

(b) Consider the same function f, but now endow the codomain with the following multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a'a + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix}$$

while endowing the codomain with the usual matrix multiplication. Assuming that this makes the codomain a ring (it does, by the way) show that f now *is* a ring homomorphism.

Exercise 6.7.3. Prove Proposition 6.3.1.

Exercise 6.7.4. Let $\mathbb{Z}$ be the ring of integers, and consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(a) = 3a$. Say whether or not f is a ring homomorphism, providing a proof of your claim. If f is not a ring homomorphism, indicate all the ring homomorphism properties that are not satisfied.

Exercise 6.7.5. Let $\mathbb{Z}$ be the ring of integers, and consider the function $g : \mathbb{Z} \to \mathbb{Z}$ defined by $f(a) = a+9$. Say whether or not g is a ring homomorphism, providing a proof of your claim.If g is not a ring homomorphism, indicate all the ring homomorphism properties that are not satisfied.

Exercise 6.7.6. Let $\mathbb{Z}$ be the ring of integers, and consider the function $h : \mathbb{Z} \to \mathbb{Z}$ defined by $h(a) = 0$. Say whether or not h is a ring homomorphism, providing a proof of your claim. If h is not a ring homomorphism, indicate all the ring homomorphism properties that are not satisfied.

Exercise 6.7.7. (a) Find a 2-by-2 real matrix of the form

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

satisfying the matrix equation $A^2 = -1$.

(b) Can you find a matrix that is *not* of the above form, satisfying $A^2 = -1$?

(c) How many 2-by-2 matrices are there that satisfy the equation $A^2 = -1$?

Exercise 6.7.8. Fix a collection of matrices $C_0, \ldots, C_n$ of the form

$$C_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$$

for real numbers $a_0, b_0, a_1, b_1, \ldots, a_n, b_n$. Show that there exists a real, 2-by-2 matrix A satisfying the matrix equation

$$C_0 + C_1 A + C_2 A^2 + \ldots + C_n A^n = 0.$$

6.8 Extra Credit: Quaternions

In the last extra credit assignment, you saw that the famous cross product on $\mathbb{R}^3$ (along with the usual notion of addition) does not render $\mathbb{R}^3$ a ring. This does not *prove* that $\mathbb{R}^3$ has no ring structure compatible with its addition—but it really is a fact that $\mathbb{R}^3$ does not have such a ring structure that is also compatible with scaling by $\mathbb{R}$. The proof is inaccessible to us at the moment.

You may wonder if there is a ring structure on $\mathbb{R}^4$. Let's explore a candidate here.

Using the bijection $\mathbb{R}^4 \cong \mathbb{R} \times \mathbb{R}^3$, let us write an element of $\mathbb{R}^4$ as a pair

$$(t, \mathbf{x})$$

where $t \in \mathbb{R}$ is a real number and $\mathbf{x} = (x_1, x_2, x_3)$ is an element of $\mathbb{R}^3$. We can define the following operation on $\mathbb{R}^4$:

$$(t, \mathbf{x}) \cdot (t', \mathbf{x}') = (tt' - \mathbf{x} \cdot \mathbf{x}', \mathbf{x} \times \mathbf{x}' + t\mathbf{x}' + t'\mathbf{x}).$$

Here, $\mathbf{x} \cdot \mathbf{x}'$ is the dot product, while $\mathbf{x} \times \mathbf{x}'$ is the cross product, and $t\mathbf{x}'$ is scaling by a factor of t.

The set $\mathbb{R}^4$, endowed with the usual vector addition, and with this multiplication, is called the *quaternions*. Sometimes, we call the quaternions *Hamiltonians* after the mathematician who discovered them. For this reason, we often write $\mathbb{H}$ (instead of $\mathbb{R}^4$).

(a) Consider the elements

$$\mathbf{i} = (0, (1, 0, 0)), \qquad \mathbf{j} = (0, (0, 1, 0)), \qquad \mathbf{k} = (0, (0, 0, 1)), \qquad -\mathbf{1} = (-1, (0, 0, 0)).$$

Prove that the squares of $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ all equal $-\mathbf{1}$.

(b) Prove that $\mathbb{H}$ (the set of quaternions with the above multiplication and addition) forms a ring.

(c) Given a quaternion $(t, \mathbf{x})$, define its *conjugate* to be $(t, -\mathbf{x})$. By contemplating the product $(t, \mathbf{x}) \cdot (t, -\mathbf{x})$, prove that any non-zero element of $\mathbb{R}^4$ admits a multiplicative inverse. (By the way, the lingo is that the quaternions are hence a "division ring.")

(d) We've seen that there is an injective ring homomorphism from $\mathbb{C}$ to $M_2(\mathbb{R})$. Can you find an injective ring homomorphism from $\mathbb{H}$ to $M_4(\mathbb{R})$?