1 Basic Examples and Definitions

Next lecture

1.1 Preliminary Examples

A ring is just a set where you can add, subtract, and multiply. In some rings you can divide, and in others you can't. There are many familiar examples of rings, the main ones falling into two camps: "number systems" and "functions".

1. $\mathbb{Z}$: the integers $\ldots, -2, -1, 0, 1, 2, \ldots$, with usual addition and multiplication, form a ring. Note that we cannot always divide, since $1/2$ is no longer an integer.

2. Similarly, the familiar number systems $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings[1].

3. $2\mathbb{Z}$: the even integers $\ldots, -4, -2, 0, 2, 4, \ldots$.

4. $\mathbb{Z}[x]$: this is the set of polynomials whose coefficients are integers. It is an "extension" of $\mathbb{Z}$ in the sense that we allow all the integers, plus an "extra symbol" x, which we are allowed to multiply and add, giving rise to x^2, x^3, etc., as well as $2x, 3x$, etc. Adding up various combinations of these gives all the possible integer polynomials.

5. $\mathbb{Z}[x, y, z]$: polynomials in three variables with integer coefficients. This is an extension of the previous ring, too. In fact you can continue adding variables to get larger and larger rings.

6. $\mathbb{Z}/n\mathbb{Z}$: The integers mod n. These are equivalence classes of the integers under the equivalence relation "congruence mod n". If we just think about addition (and subtraction), this is exactly the cyclic group of order n, as discussed a long time ago. However, when we call it a ring, it means we are also using the operation of multiplication.

7. $C[0, 1]$: This is my notation for the set of all continuous real-valued functions on the interval $[0, 1]$. For example, $f(x) = 2x$ and $g(x) = \sin x$ are in $C[0, 1]$. They can be added and multiplied to give $(f + g)(x) = 2x + \sin x$ and $(fg)(x) = 2x \sin x$, which are also elements of $C[0, 1]$. This is a very large ring, since there are lots and lots of continuous functions. Notice also that the polynomials from example 2 are contained as a proper subset of this ring. We will see in a bit that they form a "subring".

8. $M_n(\mathbb{R})$ (non-commutative): the set of $n \times n$ matrices with entries in $\mathbb{R}$. These form a ring, since we can add, subtract, and multiply square matrices. This is the first example we've seen where the order of multiplication matters: AB is not always equal to BA (usually it's not).

9. $\mathbb{Q}[[x]]$: this ring consists of what are called "formal power series" with entries in $\mathbb{Q}$ (the rational numbers). A power series is just a polynomial with (possibly) infinitely many terms, such as you see in a calculus course. The word "formal" means that we don't care whether they converge or not, so that the series $\Sigma n! x^n$ is perfectly good, even though you never talk about it in calculus because it only converges when $x = 0$. Because of this possible non-convergence, we can't think of these power series as functions, and we think of the x as a "formal variable", rather than something for which we can substitute a numerical value. We are restricting the coefficients to be rational numbers for the sake of example, but you could just as well consider $\mathbb{Z}[[x]]$ or $\mathbb{R}[[x]]$.

[1] In fact they're **fields**, to be defined shortly.

10. $\mathbb{Z}[\{\frac{1}{p}\}_{p \text{ is prime}}]$: We take the integers, and adjoin all fractions of the form $\frac{1}{p}$, for each prime number p. But since we can multiply elements in a ring, we can also obtain such fractions as $\frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3}$. Since we can add, we can obtain, for instance, $\frac{5}{6} = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$. So you get more fractions than those with just primes in the denominator, and ones in the numerator. Which fractions do we get?

11. $\mathbb{R}[x]/(x^2 + 1)$. Here's some new notation. It means take the polynomial ring $\mathbb{R}[x]$ as above, and "divide out" by the polynomial x^2+1, meaning that this polynomial gets set to zero. So in this ring, the polynomial $(x+1)^2$ is the same as $2x$, since $(x+1)^2 = x^2+2x+1 = 2x+(x^2+1) = 2x+0 = 2x$. Another way of thinking about this is that x^2 is the same as -1. So there are never any powers of x larger than 1, since whenever we get to x^2 we just swap it out for -1. So every polynomial in here is going to have a constant term and an x term and that's it. This should remind you of the complex numbers, which each have a real part (the constant term) and an imaginary part (the x term), but usually when we work with complex numbers, we use the letter i instead of x. But it's essentially the same ring. Note that for complex numbers, we can always divide (except by zero, of course), so that shows that in this weird polynomial ring, we can divide as well, which is a bit strange, since in the usual polynomial ring we can almost never divide (since, for example, $\frac{1}{x}$ doesn't count as a polynomial). This is an example of a quotient ring, which is the ring version of a quotient group, and which is a very very important and useful concept.

12. Here's a really strange example. Consider a set S (finite or infinite), and let R be the set of all subsets of S. We can make R into a ring by defining the addition and multiplication as follows. For two subsets A, B, define $A + B = A \cup B \setminus A \cap B$ (sometimes people call this the symmetric difference, or "exclusive or"). Define subtraction by $-A = S \setminus A$ (the set-theoretic complement). Thus $A - B = (A \cup (S \setminus B)) \setminus (A \cap S \setminus B)$. This example shows you that addition and multiplication needn't be the usual operations we know from grade school. But luckily, in most of our examples, like above, they will be.

1.2 Definition of a Ring

As the preceding examples indicate, a ring is basically a set in which we have a way of adding, subtracting, multiplying, but not necessarily dividing[2] Of course, depending on the ring, the addition and multiplication may not seem like the ordinary operations we are used to. So here's the formal definition:

Definition 1.2.1. A **ring** is a set R endowed with two binary operations, usually denoted $+$ and $\cdot$, such that

- R1: R is an abelian group with respect to $+$
- R2: For any a, b, c in R, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of $\cdot$)
- R3: For any a, b, c in R, $a \cdot (b + c) = a \cdot b + a \cdot c$ (left-distributivity)
- R3': For any a, b, c in R, $(a + b) \cdot c = a \cdot c + b \cdot c$ (right-distributivity)

Most often we will also impose some additional conditions on our rings, as follows:

- R4: There exists an element, denoted 1, which has the property that $a \cdot 1 = 1 \cdot a = a$ for all a in R (multiplicative identity)
- R5: $a \cdot b = b \cdot a$ for all a, b in R (commutativity of $\cdot$)

Notice that since R forms an abelian group under $+$, the addition is *always* commutative, and that there is also an additive identity, which we will usually denote by 0. So axioms 4 and 5 impose

[2] We will see later that a ring in which we can always divide is called a *field*.

extra conditions on the multiplicative structure of R. A ring satisfying $R4$ is called a **ring with unity** (or sometimes a **unital ring**), where unity is just a fancy name for the multiplicative identity. A ring satisfying R5 is called a **commutative ring**.

As usual we use exponents to denote compounded multiplication; associativity guarantees that the usual rules for exponents apply. However, with rings (as opposed to multiplicative groups), we must use a little caution, since a^k may not make sense for $k < 0$, as a is not guaranteed to have an mulitplicative inverse.

In most of the examples above it is easy to see what the additive and multiplicative identities are. What are they for example 10?

The axioms are just a *minimal* list of properties of the addition and multiplication. Others can be deduced from these, e.g.,

Lemma 1.2.2. *Let R be a ring, with additive and multiplicative identities 0 and 1, respectively. Then for all a, b in R,*

1. $0a = a0 = 0$;
2. $(-a)b = a(-b) = -(ab)$;
3. $(-a)(-b) = ab$;
4. $(na)b = a(nb) = n(ab)$ *for any n in $\mathbb{Z}$.*

In 4, note that n is not to be thought of as an element of R: the notation na just means $a + \cdots + a$, where there are n copies of a in the sum.

Proof. 1. Exercise

2. To show that $(-a)b = -(ab)$ is to show that the element $(-a)b$ is the additive inverse of ab; so we add them together, and hope to get zero. So $(-a)b + ab = ((-a) + a)b = (0)b = 0$ (by 1). The equality of $a(-b)$ and $-(ab)$ is similar.

3. Exercise

4. $(na)b = (a + \cdots + a)b = (ab + \cdots + ab) = n(ab) = a(b + \cdots + b) = a(nb)$

□

Example 1.2.3. (The **zero ring**) The axiom R4 begs the question: can 0 and 1 be the same? The answer is yes, but in that case it turns out that there is only one element in our ring, which is 0 (which is equal to 1). We call this the zero ring, and sometimes write it just as 0. Here's the reason: suppose 1=0 in a ring, and now pick any element r in this ring. Since $r = 1 \cdot r = 0 \cdot r = 0$, we find that every element is 0.

1.3 Special elements in a ring

Here we pick out some types of elements that can occur in rings:

Definition 1.3.1. Let a be an element of a ring R. We say that a is:

1. a **unit** if a has a multiplicative inverse, i.e., if there exists an element b in R such that $ab = ba = 1$; in this case, a is also said to be **invertible**, and b the **inverse** of a (and vice versa);
2. a **zerodivisor** if $a \neq 0$ and there is a nonzero element b in R such that $ab = ba = 0$;
3. **nilpotent** if $a^k = 0$ for some $k \in \mathbb{N}$;
4. **idempotent** if $a^2 = a$.

Example 1.3.2. 1. In any ring 0 and 1 are (trivially) idempotent, and 0 is trivially nilpotent. 1 is always a unit ("unity is a unit")

2. In $\mathbb{Z}$, the units are ± 1, there are no zerodivisors, no nilpotent elements, and only 1 is idempotent.

3. In $\mathbb{Q}[x]$, the units are the nonzero constant polynomials, there are no zerodivisors, and no nontrivial idempotent or nilpotent elements.

4. In $M_n(\mathbb{R})$, the units are just the invertible matrices, which is just the multiplicative group $GL_n(\mathbb{R})$. There are plenty of zerodivisors: any strictly upper-triangular matrix multiplied by a strictly lower-triangular matrix is zero, so there are already lots of them. In fact, the zero-divisors are precisely the non-invertible matrices (except for 0, which never counts as a zerodivisor). This doesn't usually happen: rings can contain many elements that are neither units nor zerodivisors. Nilpotents must have 0 as their only eigenvalue. Idempotents must be diagonalizable and have 1 as their only eigenvalue.

5. In $\mathbb{Z}/n\mathbb{Z}$, the units are those classes $\overline{m}$ for which $\gcd(m, n) = 1$. The zerodivisors are those for which $\gcd(m, n) \neq 1$. This is another ring in which every nonzero element is either a unit or a zerodivisor, but again do not be tempted to believe that this holds for all rings!

Definition 1.3.3. A nonzero ring in which every nonzero element is a unit is called a **field**.

Fields include many familiar number systems, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$; $\mathbb{Z}$, on the other hand, is not a field.

2 Subrings; Homomorphisms

Previous lecture - Next lecture

IMPORTANT: FOR THE REMAINDER OF THESE LECTURES, ALL RINGS WILL BE ASSUMED COMMUTATIVE WITH UNITY, WITHOUT FURTHER MENTION, UNLESS EXPLICITLY STATED OTHERWISE.

In this lecture we will discuss how to easily get new rings out of other rings by finding rings inside others (subrings) or by "combining rings together", and also learn about homomorphisms, which just as for the groups, are the only types of functions which are of much interest in ring theory.

2.1 Subrings; Adjoining Elements

Definition 2.1.1. If R is a ring, and S is a subset of R we will say that S is a **subring** of R if

1. S is a subgroup of R under $+$.
2. S is closed under multiplication, and
3. 1 is in S.

We've seen subrings already: in yesterday's examples, $\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$, which is in turn a subring of $\mathbb{Z}[x, y, z]$, etc. Similarly, $\mathbb{Z}[\{\frac{1}{p}\}_{p \text{ is prime}}]$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, etc.

In general, there is a construction called **adjoining an element** defined as follows: start with a ring R, and add a new element x (of course, if x is already being used as the name of an element in R, then you'd better choose a different letter...). This x could be a "formal variable", or it could be a known element of some other ring containing R. We build a ring $R[x]$ (read aloud as "R adjoin x"), which contains all elements of R as well as the new element x. Since we allow addition and multiplication we must also include x^2, x^3, etc, as well as any product rx^k (and $x^r k$, if we want it to be commutative), where $r \in R$. Since we should be able to add, we also obtain sums of the form $a_0+a_1x+a_2x^2+\cdots+a_nx^n$, where the $a_i \in R$. Thus, as you can see, $R[x]$ is simply a polynomial ring with coefficients in R. But of course, the elements of R could be all sorts of things, in which case elements of $R[x]$ may not look like ordinary polynomials, which typically have some sorts of numbers $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ as their coefficients. Thus if you wanted, you could build a ring whose elements were polynomials with matrix coefficients.

The construction of $R[x]$ realizes R as a subring of a larger ring, and is in some sense the "smallest" way to do so, as we only added one element, and those which were forced upon us by the ring axioms.

Example 2.1.2.

1. The **Gaussian integers** are defined as the subring of $\mathbb{C}$ given by adjoining i to the integers, namely $\mathbb{Z}[i]$. They can be pictured as a square lattice in the complex plane. They contain $\mathbb{Z}$ as a proper subring.
2. Rings such as $\mathbb{Q}[\sqrt{2}]$, where we adjoin an irrational square root to the rational numbers, are of great importance in number theory. They are called **quadratic number fields**. Since $(\sqrt{2})^2 \in \mathbb{Q}$, we don't need any higher powers of the new element $\sqrt{2}$, so actually $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. In other words, if we think of this as some set of polynomial ring, where the "variable" is $\sqrt{2}$, then actually the only polynomials we need are linear.

2.2 Products of Rings

Definition 2.2.1. Let R and S be two rings. Their **product**, sometimes called the **direct product**, denoted $R \times S$, is the ring

$$R \times S = \{(r, s) \mid r \in R, s \in S\}$$

So as a set, $R \times S$ is just the Cartesian product. It's made into a ring by defining addition and multiplication componentwise:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2); \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1r_2, s_1s_2)$$

The zero element (additive identity) of this ring is just $(0, 0)$ - note that the first zero lives in R, but the second lives in S, so it's bad notation. The multiplicative identity is $(1, 1)$.

Inside $R \times S$, there is "a copy" of R, namely the set

$$R \times \{0\} = \{(r, 0) \mid r \in R\}$$

This is a subring of $R \times S$. It's not exactly the same as R, since things in $R \times \{0\}$ are still ordered pairs of things in R and S, whereas elements of R are not. But you can see that they're basically the same. In fancy jargon, R is "isomorphic" to $R \times \{0\}$.

Example 2.2.2.

1. Products of rings always have lots of zerodivisors. For example, in $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, if a, b are nonzero integers, then $(a, 0)$ and $(0, b)$ are nonzero elements whose product is zero, so they are zerodivisors.

2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a ring with 6 elements. So is $\mathbb{Z}/6$. Your intuition from our study of them as abelian groups may tell you that they are the same. We will see that they're **isomorphic** as rings, just as they were isomorphic as groups. But it's crucial that 2 and 3 are coprime: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not the same as $\mathbb{Z}/4\mathbb{Z}$, not least because they're not even the same as groups!

3. Products of rings also have nontrivial idempotents, which is a comparatively rare phenomenon. For instance, $\mathbb{Z}$ has no nontrivial idempotents, whereas $\mathbb{Z} \times \mathbb{Z}$ has the idempotents $(1, 0)$ and $(0, 1)$.

2.3 Homomorphisms

Just as with groups, when we study rings, we are only concerned with functions that "preserve the structure" of a ring, and these are called ring homomorphisms. Maybe you can guess what the definition should be, by analogy with the case of groups.

Definition 2.3.1. Let R and S be rings, and $\phi \colon R \to S$ be a function. We say ϕ is a **ring homomorphism** if, for all a, b in R,

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, and
3. $\phi(1) = 1$.

Note that in (3), the first 1 is in R, while the second 1 is in S.

Notice that we explicitly require that ϕ sends 1 to 1. What about the additive identity 0? Why don't we have to require that $\phi(0) = 0$? This is because, as we proved a while ago, since R and S are groups under addition, it follows automatically. But since neither R or S are groups under multiplication, we have to add in this condition separately.

Definition 2.3.2.

1. Let R and S be two rings. The set of all homomorphisms from R to S is denoted $\mathrm{Hom}(R, S)$.

2. A homomorphism is **injective** or **surjective** if it so as a map of sets (i.e., the usual definitions apply)

Example 2.3.3.

1. $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n + 1$ is not a ring homomorphism. It fails conditions 1,2, and 3.

2. In fact, there is only one ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$, the identity map, which sends each integer to itself. This is one of the reasons why $\mathbb{Z}$ is a very important ring.

3. The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which sends an integer m to its congruence class $\overline{m}$ mod n is a ring homomorphism.

4. $\mathrm{Ev}_a \colon \mathbb{Z}[x] \to \mathbb{Z}$ given by $\mathrm{Ev}_a(p(x)) = p(a)$ is a ring homomorphism, called the **evaluation map** at a. It means simply "plug in a". This type of homomorphism is ubiquitous, since polynomials can be viewed as functions, and for functions we just "plug in" an element. One can define the same sort of map with $\mathbb{Z}$ replaced by an arbitrary ring R.

5. The map $\mathbb{Z} \to \mathbb{Z}$ sending n to n^k is not a ring homomorphism unless $k = 1$. For example, if $k = 2$, then since $2 = 1^2 + 1^2 \neq (1+1)^2 = 4$, it is not additive.

6. If p is a prime, then the map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ which sends $[n]$ to $[n^p]$ *is* a ring homomorphism. In other words, when we work mod p, the pth power map is a ring homomorphism.[1] Contrast this with the example above.

7. If R is any ring, then there are lots of homomorphisms from $\mathbb{Z}[x]$ to R. All we have to do is pick an element r in R, and send x to r. The rest of the map is forced by the definition of homomorphism (see following proposition).

Proposition 2.3.4. *For any ring R, the set* $\mathrm{Hom}(\mathbb{Z}[x], R)$ *is in bijection with R.*

Proof. We will define a bijection from R to $\mathrm{Hom}(\mathbb{Z}[x], R)$. For each r in R, define a map f_r from $\mathbb{Z}[x]$ to R by

$$f_r(a_n x^n + \cdots + a_1 x + a_0) = a_n r^n + \cdots + a_1 r + a_0 \cdot 1$$

Since the term on the right is just various powers of r added together (remember that the a_i are integers), it makes sense as an element of R. Now we have to check some things: a) f_r is a homomorphism, b) the correspondence between the rs and f_rs is one-to-one, and c) it's onto.

To see that f_r is a homomorphism, it's convenient to write $f_r(p(x)) = p(r)$. This is just a shorthand notation for the formula above, where we've written $p(x)$ for $a_n x^n + \cdots + a_1 x + a_0$. Then

$$f_r(p(x) + q(x)) = p(r) + q(r) = f_r(p(x)) + f_r(q(x))$$

and

$$f_r(p(x)q(x)) = p(r)q(r) = f_r(p(x))f_r(q(x)),$$

which proves the first two properties. Finally, $f_r(1) = 1$, simply because there is nowhere to substitute r for x.

Now we have to show the one-to-one part. So suppose r and r' are two distinct elements of R. Then we get two maps f_r and $f_{r'}$ and we have to show they're different. Well, $f_r(x) = r$, and $f_{r'}(x) = r'$. Since these two homomorphisms send the polynomial x to different elements of R, they must be different homomorphisms, which establishes that the correspondence is one-to-one.

To show the correspondence is onto, suppose we start with a homomorphism f from $\mathbb{Z}[x]$ to R. We have to show it has the form f_r for some element r of R. First plug in the polynomial x to our map f. That gives us our element r. This r in turn gives rise to a map f_r. Now we have to show that f and the new f_r are the same map. By the definition of f_r, we have $f_r(p(x)) = p(r)$. And writing $p(x) = a_n x^n + \cdots + a_1 x + a_0$, we have

$$f(p(x) = f(a_n x^n + \cdots + a_1 x + a_0) = a_n f(x)^n + \cdots + a_1 f(x) + a_0 = a_1 r^n + \cdots + a_1 r + a_0 = p(r)$$

This shows that when applied to any polynomial $p(x)$, f and f_r give the same result, so they're the same homomorphism. Thus any given f can be written as f_r (where we choose r to be $f(x)$), so the correspondence is onto.

□

[1] In fact, since by Fermat's little theorem, $n^p \equiv n \mod p$, this map is none other than the identity map.

The proposition can be restated as follows: a homomorphism out of $\mathbb{Z}[x]$ is uniquely determined by where it sends x. An analogous statement is true for maps out of $\mathbb{Z}[x, y]$, etc.

The last part of the proof suggests why polynomial rings are so ubiquitous in ring theory: polynomials are built entirely out of addition and multiplication, and homomorphisms "pass through" addition and multiplication. So it is very easy to define homomorphisms on polynomials.

2.4 Isomorphisms

Just as for groups, bijective homomorphisms are called isomorphisms, and they tell us when two rings "have the same structure".

Definition 2.4.1. An **isomorphism** from a ring R to another ring S is a bijective homomorphism. If an isomorphism between R and S exists, then we say R and S are **isomorphic** and we write $R \cong S$.

There is an alternative way to characterize isomorphisms, using inverse functions.

Proposition 2.4.2. *Let $f\colon R \to S$ be a homomorphism. Then f is an isomorphism if and only if there exists a homomorphism $g\colon S \to R$ such that $g \circ f$ is the identity map on R and $f \circ g$ is the identity map on S.*

Proof. Exercise.

□

Example 2.4.3. Inside the matrix ring $M_2(\mathbb{R})$, there is a subring

$$R = \left\{ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\}.$$

Even though $M_2(\mathbb{R})$ is not a commutative ring, the subring R is commutative, and it is isomorphic to $\mathbb{Z}$, which is probably not surprising. To prove this, we define a map $\phi\colon \mathbb{Z} \to R$ by, for n in $\mathbb{Z}$,

$$\phi(n) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}.$$

First we check it's a homomorphism:

1. Additivity:

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

2. Multiplicativity:

$$\phi(mn) = \begin{pmatrix} mn & 0 \\ 0 & mn \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = \phi(m)\phi(n)$$

3. Finally, ϕ sends 1 in $\mathbb{Z}$ to 1 in R, the role of 1 in R being played by the identity matrix.

So ϕ is a homomorphism. To see that it's an isomorphism, we can either check injectivity and subjectivity, or go by the definition and produce an inverse. We'll go by the definition. The inverse is $\psi\colon R \to \mathbb{Z}$, given by

$$\psi \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = n.$$

This is one of those points where authors tend to say "it's obvious that ϕ and ψ are inverses", but I'll write out the details as a model for future reference. We need to check that $\psi(\phi(n)) = n$ and $\phi\left(\psi\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}\right) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$. Well,

$$\psi(\phi(n)) = \psi \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = n,$$

and

$$\phi\left(\left(\begin{array}{cc} n & 0 \\ 0 & n \end{array}\right)\right) = \phi(n) = \left(\begin{array}{cc} n & 0 \\ 0 & n \end{array}\right),$$

using only the definitions of the two maps.