# Rings

Modern Algebra I is primarily the study of finite groups, and a general theme is that of *symmetry*. If there is any theme to Modern Algebra II, it is most likely that of *factorization*. Despite the formal similarity between groups and rings, ring theory has a very different flavor than group theory. Also, aside from a general level of conceptual sophistication, we shall use very little of group theory in this course until the very end, when we study Galois theory.

## 1 Basic definitions

**Definition 1.1.** A *ring* $R = (R, +, \cdot)$ consists of a set $R$ together with two binary operations $+$ and $\cdot$ on $R$ such that:

1. The set $R$ together with the binary operation $+$, i.e. the binary structure $(R, +)$, is an abelian group.
2. The binary operation $\cdot$ is associative. We usually write $rs$ for $r \cdot s$.
3. The left and right distributive laws hold: for all $r, r, t \in R$,

$$(r + s)t = rt + st;$$
$$t(r + s) = tr + ts.$$

As with groups, we shall usually just write $R$ instead of $(R, +, \cdot)$, with the operations $+$ and $\cdot$ usually clear from the context. We write $0$ for the additive identity of $R$ and $-r$ for the additive inverse of $r$.

Before giving some of the very many examples of rings, we record some easy consequences (mostly without proof) of the axioms for a ring $R$:

1. For all $r \in R$, $0r = r0 = 0$. This follows by the usual argument, that

$$0r = (0 + 0)r = 0r + 0r,$$

and by (additive) cancellation, and similarly for $r0$.

2. For all $r, s \in R$,
$$(-r)s = r(-s) = -rs,$$
and hence
$$(-r)(-s) = rs.$$

3. The generalized distributive law holds: given two sums $\sum_{i=1}^{n} r_i$ and $\sum_{j=1}^{m} s_j$, where the $r_i, s_j \in R$, then
$$\left(\sum_{i=1}^{n} r_i\right)\left(\sum_{j=1}^{m} s_j\right) = \sum_{i,j} r_i s_j.$$
For example,
$$(r_1 + r_2)(s_1 + s_2) = r_1 s_1 + r_1 s_2 + r_2 s_1 + r_2 s_2.$$

4. The "laws of exponents" for the additive group $(R, +)$ say that, for all $n, m \in \mathbb{Z}$ and $r \in R$,
$$(n + m) \cdot r = (n \cdot r) + (m \cdot r), \text{ and } n \cdot (m \cdot r) = (nm) \cdot r,$$
where $n \cdot r$ means $r$ added to itself $n$ times, for $n > 0$. More precisely, we define $n \cdot r$ inductively by: $1 \cdot r = r$, and $(n + 1) \cdot r = (n \cdot r) + r$. For $n = 0$, we set $0 \cdot r = 0$, and for $n < 0$, we set $n \cdot r = -((-n) \cdot r)$. Note that this $\cdot$ is **not** the same as multiplication in $R$. Then there is an additional property for rings: for all $n \in \mathbb{Z}$ and $r, s \in R$,
$$(n \cdot r)s = r(n \cdot s) = n \cdot (rs).$$

5. For $n > 0$, $n \in \mathbb{Z}$, define $r^n$ as the product of $r$ with itself $n$ times. More precisely, we define $r^n$ inductively as follows: $r^1 = r$, and $r^{n+1} = r^n r$. Then we have the usual "laws of exponents:"
$$r^n r^m = r^{n+m} \text{ and } (r^n)^m = r^{nm}.$$
These can be proved by induction.

We shall usually narrow the class of rings we consider as follows:

**Definition 1.2.** Let $R$ be a ring.

1. The ring $R$ is *commutative* if multiplication is commutative, i.e. if, for all $r, s \in R$, $rs = sr$.

2. The ring $R$ is a *ring with unity* if there exists a multiplicative identity in $R$, i.e. an element, almost always denoted by 1, such that, for all $r \in R$, $r1 = 1r = r$. The usual argument shows that such an element is unique: if $1'$ is another, then $1 = 1'1 = 1'$. In this case, it is easy to check that the element $n \cdot r$ defined above is actually equal to $(n \cdot 1)r$.

3. If $R$ is a ring with unity 1, then a *unit* of $R$ is an element $r \in R$ such that $r$ has a multiplicative inverse, i.e. there exists an $r' \in R$ such that $rr' = r'r = 1$. (Unfortunately, it is easy to confuse the terms unity and unit.) If $r$ has a multiplicative inverse, then the inverse is unique, if it exists, by the usual argument and using associativity: if $r''$ is another such element, then

$$r'rr'' = (r'r)r'' = 1r'' = r'' = r'(rr'') = r'1 = r'.$$

(This also shows as usual that if $r$ has a left and a right multiplicative inverse then they are equal and $r$ is a unit.) We also say that $r$ is *invertible* and denote its unique multiplicative inverse by $r^{-1}$. An argument which should be familiar from Modern Algebra I is that, if we let

$$R^* = \{r \in R : R \text{ is a unit}\},$$

then $(R^*, \cdot)$ is a group. In particular, the product of two units is a unit and the inverse of a unit is a unit (with $(r^{-1})^{-1} = r$.)

4. The ring $R$ is a *division ring* or *skew field* if $R$ is a ring with unity 1, $1 \neq 0$ (this is easily seen to be equivalent to the hypothesis that $R \neq \{0\}$), and $R^* = R - \{0\}$, i.e. every nonzero element of $R$ has a multiplicative inverse. A *field* is a commutative division ring.

Let $R$ be a ring. If we try to compute $(r + s)^2$, we don't necessarily get the "expected" answer. However, if $R$ is commutative, then

$$(r + s)^2 = r^2 + rs + sr + s^2 = r^2 + rs + rs + s^2 = r^2 + 2 \cdot rs + s^2.$$

More generally, for a commutative ring $R$ and a positive integer $n$, we have:

**Theorem 1.3** (Binomial Theorem)**.** *For all $r, s \in R$,*

$$(r + s)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot r^{n-i} s^i.$$

This can be proved by adapting the usual inductive proof to our more abstract setting. Here, the end terms are $r^n s^0$ and $r^0 s^n$, which we set equal to $r^n$ and $s^n$ respectively. For a ring $R$ with unity, not necessarily commutative, we define $r^0 = 1$ for all $r \in R$, although the binomial theorem holds even if $R$ does not have unity.

## 2 Examples

Rings are ubiquitous in mathematics. We list some important examples.

1. There are the familiar examples of numbers: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. These are all commutative rings with unity. Here, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields, but $(\mathbb{Z})^* = \{\pm 1\}$. A related example is $n\mathbb{Z} = \langle n \rangle$, the cyclic subgroup of $\mathbb{Z}$ generated by $n$. It is an additive group, and multiplication is a well-defined binary operation since

$$(nk_1)(nk_2) = n^2(k_1 k_2) = n(nk_1 k_2) \in n\mathbb{Z}.$$

   Note that, if $n > 1$, $n\mathbb{Z}$ is **not** a ring with unity.

2. As we saw in Modern Algebra I, $\mathbb{Z}/n\mathbb{Z}$ is a finite commutative ring with unity for all positive integers $n$. In the case, the group of units is the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ $n = p$ is a prime number. In this case, we will usually use the notation $\mathbb{F}_p$ for the ring $\mathbb{Z}/p\mathbb{Z}$, thought of as a field. These are the first cases of finite fields. Later in the course, we shall describe all finite fields.

3. Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices with entries in $\mathbb{R}$. Then we can both add and multiply elements of $M_n(\mathbb{R})$, and the left and right distributive laws hold: for all $A, B, C \in M_n(\mathbb{R})$,

$$(A + B)C = AC + BC \text{ and } C(A + B) = CA + BA.$$

   Thus $M_n(\mathbb{R})$ is a ring, and it is not commutative as soon as $n \geq 2$. It does have unity, the identity matrix $I$. The units in $M_n(\mathbb{R})$ form the group $GL_n(\mathbb{R})$ of invertible $n \times n$ matrices with entries in $\mathbb{R}$. We can consider matrices with entries in other rings as well, for example $M_n(\mathbb{C})$, $M_n(\mathbb{Q})$, or even $M_n(\mathbb{Z})$. In fact, in order to be able to define matrix multiplication, we just need to be able to add and multiply the entries, and this will satisfy the usual properties (e.g. matrix multiplication is associative and distributes over matrix addition) as long as

addition and multiplication have these properties. So, for every ring $R$, the set $M_n(R)$ of $n \times n$ matrices with coefficients in $R$ is a ring under matrix addition and multiplication. If $R$ is a ring with unity, then so is $M_n(R)$, where the unity is the $n \times n$ identity matrix. For example, for every positive integer $k$, $M_n(\mathbb{Z}/k\mathbb{Z})$ is a finite ring (of order $k^{n^2}$), and it is not commutative if $n > 1$ and $k \neq 1$.

4. There are trivial examples of rings. For example, the *zero ring* $R$ is the ring $\{0\}$, with the unique binary operations $(0+0 = 0, 0 \cdot 0 = 0)$. More generally, if $A$ is an abelian group, then we can define a multiplication on $A$ by the rule that $a \cdot b = 0$ for all $a, b \in A$. Then it is easy to check that $A$ is a (commutative) ring with this definition of multiplication, but it is not a ring with unity unless $A = \{0\}$.

5. Rings of functions arise in many areas of mathematics. For example, the set $\mathbb{R}^{\mathbb{R}}$ of all real-valued functions $f\colon \mathbb{R} \to \mathbb{R}$ is a ring under pointwise addition and multiplication: given two functions $f$ and $g$, we define the "pointwise sum" $f + g$ and the "pointwise product" $fg$ by:
$$(f + g)(x) = f(x) + g(x); \qquad (fg)(x) = f(x)g(x).$$
Clearly, if $X$ is any set and $R$ is a ring, then the set $R^X$ of all functions from $X$ to $R$ becomes a ring under pointwise addition and multiplication as well.

   Often, we don't look at all functions from, say, $\mathbb{R}$ to itself but at interesting subsets. For example, let $C^0(\mathbb{R})$ be the set of all **continuous** functions from $\mathbb{R}$ to $\mathbb{R}$. Then $C^0(\mathbb{R})$ is a ring via pointwise addition and multiplication. This fact doesn't follow from pure thought: the content of this statement is that the sum of two continuous functions is continuous and the product of two continuous functions is continuous. Similarly, the set $C^\infty(\mathbb{R})$ of all functions from $\mathbb{R}$ to $\mathbb{R}$ with derivatives of all orders is a ring via pointwise addition and multiplication.

   Note that, if $R$ is a commutative ring, then $R^X$ is commutative: the pointwise product $fg$ is equal to $gf$, since, for all $x \in X$, $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$. Also, if $R$ is a ring with unity, then so is $R^X$: the constant function 1, i.e. the unique function from $X$ to $R$ whose value at every $x \in X$ is 1, is a unity under pointwise multiplication.

6. Given two rings $R_1$ and $R_2$, the Cartesian product $R_1 \times R_2$ is a ring under componentwise addition and multiplication: given $(r_1, r_2), (s_1, s_2) \in$

$R_1 \times R_2$, we define

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2);$$
$$(r_1, r_2) \cdot (s_1, s_2) = (r_1 s_1, r_2 s_2).$$

Then $R_1 \times R_2$ is commutative if $R_1$ and $R_2$ are commutative, and it is a ring with unity if $R_1$ and $R_2$ both have unity; in fact, the unity in $R_1 \times R_2$ is then necessarily $(1, 1)$.

7. There are many interesting rings which are subsets of $\mathbb{C}$ defined by special numbers. For example, define the *Gaussian integers* $\mathbb{Z}[i]$ by

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Addition and multiplication are given by the usual addition and multiplication of complex numbers, and multiplication defines a binary operation on $\mathbb{Z}[i]$ because $\mathbb{Z}[i]$ is closed under multiplication:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

The ring $\mathbb{Z}[i]$ is a commutative ring with unity, but is not a field. In fact $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$ and hence is a cyclic group of order 4. There is no reason to just look at integer coefficient $a, b$. We could also take $a, b$ to be rational. In this case, for reasons we will explain later, we use the notation $\mathbb{Q}(i)$ instead:

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

In this case, many of you have probably seen in high school that $\mathbb{Q}(i)$ is a field. In fact, given $a+bi \in \mathbb{Q}(i)$, where not both $a, b$ are 0, we find a multiplicative inverse for $a + bi$ by "rationalizing the denominator:"

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{1}{a^2 + b^2} \cdot (a - bi) = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

A similar construction works with $\sqrt{2}$: define

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

As before, $\mathbb{Z}[\sqrt{2}]$ is closed under multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

The ring is a commutative ring with unity, but is still not a field. For example, 2, 3, $\sqrt{2}$ have no multiplicative inverses in this ring. However, there are **lots** of units! For example, since

$$(1+\sqrt{2})(1-\sqrt{2}) = 1-2 = -1,$$

we see that $(1+\sqrt{2})^{-1} = -(1-\sqrt{2}) = -1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. It is easy to see that $1+\sqrt{2}$ has infinite order in $\mathbb{Z}[\sqrt{2}]$: since the absolute value $|1+\sqrt{2}|$ is greater than 1, no positive power of $1+\sqrt{2}$ can be 1. Thus $(\mathbb{Z}[\sqrt{2}])^*$ contains the infinite cyclic subgroup

$$\langle 1+\sqrt{2}\rangle = \{(1+\sqrt{2})^n : n \in \mathbb{Z}\}.$$

As before we can consider $\mathbb{Q}$ coefficients and define

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}.$$

This is again a field by rationalizing denominators:

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{1}{a^2-2b^2}\cdot(a-b\sqrt{2}) = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

Note that the denominator $a^2-2b^2$ is nonzero as long as at least one of $a,b$ are nonzero; this is equivalent to the statement that $\sqrt{2}$ is irrational.

For a final example of this type, consider instead $\mathbb{Z}[\sqrt[3]{2}]$. We can't just take complex numbers of the form $a+b\sqrt[3]{2}$, because (as we will see more carefully much later) the number $(\sqrt[3]{2})^2$ is not of the form $a+b\sqrt[3]{2}$. Thus we need **three** coefficients, and define

$$\mathbb{Z}[\sqrt[3]{2}] = \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 : a,b,c \in \mathbb{Z}\}.$$

With this definition, it should be intuitively clear (if a little tedious to write out) that $\mathbb{Z}[\sqrt[3]{2}]$ is closed under multiplication and hence is a ring. For example,

$$(\sqrt[3]{2})^2(\sqrt[3]{2})^2 = (\sqrt[3]{2})^4 = 2\sqrt[3]{2}.$$

Likewise we define $\mathbb{Q}(\sqrt[3]{2})$ via

$$\mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 : a,b,c \in \mathbb{Q}\}.$$

In this case, it is still true that $\mathbb{Q}(\sqrt[3]{2})$ is a field, but it is far from obvious: given $a, b, c \in \mathbb{Q}$, not all 0, we have to find a way to rationalize the denominator of the expression

$$\frac{1}{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2}.$$

We will describe several different ways to think about this over the course of the semester.

8. The *quaternions* are an interesting example of a division ring which is not a field. Let $\mathbb{H} = \mathbb{R}^4$, with basis 1, $i$, $j$, $k$. Thus an element of $\mathbb{H}$ is uniquely written as $\alpha = x_0 + x_1 i + x_2 j + x_3 k$. We view $\mathbb{R}$ as a subset of $\mathbb{H}$ by identifying $t$ with $t \cdot 1$. Two quaternions are multiplied by the following rules: if $t = t1$, then $it = ti$ and similarly for $j$, $k$. Otherwise, $i^2 = j^2 = k^2 = -1$, and $ij = k = -ji$, $jk = i = -kj$, and $ki = j = -ik$. Then we expand out by the usual rules for distributivity. It is a little painful to check that multiplication is associative and left and right distributes over addition, but one can identify $\mathbb{H}$ with a subset of $M_2(\mathbb{C})$, or $M_4(\mathbb{R})$, with the inherited operations of addition and matrix multiplication, and use this to prove associativity and left and right distributivity. Then (homework) $\mathbb{H}$ is a division ring, but it is clearly not commutative. It is interesting for many reasons, but one of the most important ones is the following fact: if $R$ is a division ring containing the real numbers $\mathbb{R}$, and $R$ is finite dimensional over $\mathbb{R}$ in a natural way, then $R$ is essentially $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

9. A fundamental class of rings are *polynomial rings*. We will use the notation $\mathbb{R}[x]$ to denote the set of all polynomials with real coefficients:

$$\mathbb{R}[x] = \left\{ \sum_{i=0}^{N} a_i x^i : a_i \in \mathbb{R} \right\}.$$

Here, however, we write $1x = x$, and we agree that adding terms of the form $0x^k$ does not affect the polynomial. The sets $\mathbb{C}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ of polynomials with coefficients in $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$ respectively are defined similarly. More generally, let $R$ be a commutative ring with unity. Then a *polynomial with coefficients in* $R$ is an expression $f(x)$ of the form $\sum_{i=0}^{N} a_i x^i$ with $a_i \in R$. We define $R[x]$ to be the set of all polynomials with coefficient in $R$. To avoid the issue with terms of the form $0x^k$, we can simply identify the polynomial $f(x)$ with the infinite sequence

of coefficients $(a_0, a_1, \dots)$, where $a_i \in R$ and $a_i = 0$ for all $i > N$. The largest $d$ (possibly 0) such that $a_d \neq 0$ is called the *degree* of $f(x)$ and written $\deg f(x)$. Here, the degree of a "constant polynomial" $a_0$ is 0, but the degree of the zero polynomial 0 is **undefined** (some people define it to be $-\infty$).

Addition of polynomials is defined by adding coefficients, so that

$$\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i.$$

Multiplication of polynomials is given by the formula

$$\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = \sum_i c_i x^i,$$

where $c_k = \sum_{i+j=k} a_i b_j$. It is the formula forced on us by requiring that $x^i a = a x^i$, $x^i x^j = x^{i+j}$, and distributivity. With these definitions, a somewhat tedious argument (which we shall discuss in more detail shortly) shows that $R[x]$ is a commutative ring with unity.

In precalculus and calculus, polynomials with real coefficients define functions (polynomial functions) from $\mathbb{R}$ to $\mathbb{R}$ and we can identify the polynomial with the function that it defines. For a general ring, it turns out that this is not quite the case. We will discuss later the many ways in which polynomials can be used to define functions, but for the moment we can just think of them as formal objects.

## 3 A few more general definitions

Many of the basic definitions of group theory have straightforward generalizations to rings.

**Definition 3.1.** Let $R_1$ and $R_2$ be two rings. A *homomorphism* $f\colon R_1 \to R_2$ is a function (not necessarily injective or surjective) such that, for all $r, s \in R_1$,

$$f(r+s) = f(r) + f(s);$$
$$f(rs) = f(r)f(s).$$

An *isomorphism* $f\colon R_1 \to R_2$ is a homomorphism which is a bijection. If $R_1 = R_2$, then an isomorphism from $R_1$ to itself is called an *automorphism*

of $R_1$. For example, the identity is an automorphism. Two rings $R_1$ and $R_2$ are *isomorphic* if there exists an isomorphism $f\colon R_1 \to R_2$. **In this course, unless otherwise specified, a homomorphism is always understood to mean a ring homomorphism and similarly for isomorphisms.**

**Example 3.2.** If $R_1$ and $R_2$ are any rings and we define $f(r) = 0$ for all $r$, then $f$ is a homomorphism under the above definition. However, we shall shortly modify the definition so that such an $f$ is **not** allowed.

For a more interesting example, the natural projection homomorphism $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism. For $R = \mathbb{C}$, complex conjugation is an automorphism: if we set $f(z) = \bar{z}$, then the well-known identities $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$ imply that $f$ is an automorphism (it is a bijection with inverse equal to $f$). Conjugation also defines automorphisms $\mathbb{Z}[i] \to \mathbb{Z}[i]$ and $\mathbb{Q}(i) \to \mathbb{Q}(i)$. A similar construction works for $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Q}(\sqrt{2})$, by defining

$$f(a + b\sqrt{2}) = a - b\sqrt{2}.$$

(However, aside from the zero homomorphism, the only other automorphism of $\mathbb{Z}[\sqrt[3]{2}]$ or of $\mathbb{Q}(\sqrt[3]{2})$ is the identity.)

**Definition 3.3.** Let $S$ be a ring. A *subring* of $S$ is a subset $R$ such that

1. $R$ is an (additive) subgroup of $S$, i.e. a subgroup of $(S, +)$.
2. $R$ is closed under multiplication.

In this case, $R$ is a ring as well, with the inherited operations (since multiplication becomes a well-defined binary operation which is automatically associative and left and right distributes over addition). We write $R \leq S$ is $R$ is a subring of $S$.

As has already been implicit in our list of examples of rings, many rings arise as subrings of other rings. Here are some examples:

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. But also $\mathbb{Z} \leq \mathbb{Z}[i] \leq \mathbb{Q}(i) \leq \mathbb{C}$, and $\mathbb{Z} \leq \mathbb{Z}[\sqrt{2}] \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{R}$.
2. $n\mathbb{Z} \leq \mathbb{Z}$. (We will modify the definition shortly to disallow this example.)
3. The trivial ring $\{0\}$ is a subring of every ring $R$. (As with homomorphisms, we will shortly disallow this example.)

4. Given two rings $R_1$, $R_2$, the subsets $R_1 \times \{0\}$ and $\{0\} \times R_2$ are subrings of $R_1 \times R_2$.

5. $\mathbb{R} \leq \mathbb{H}$.

6. If $R$ is a commutative ring with unity, then $R \leq R[x]$ in the obvious way, as the subset of "constant polynomials," i.e. the set of polynomials of degree 0 union $\{0\}$.

**Basic Conventions**: (i) If $R_1$ and $R_2$ are two rings with unity, and $f\colon R_1 \to R_2$ is a homomorphism, we **also require** that $f(1) = 1$. Thus, with this convention, the zero homomorphism is no longer allowed to be a homomorphism from one ring with unity to another. Note that, in this case, if $r$ is a unit of $R$, so that there exists an $r^{-1} \in R$ with $rr^{-1} = 1$, then $f(1) = 1 = f(rr^{-1}) = f(r)f(r^{-1})$. Thus, if $r$ is a unit, then so is $f(r)$, and in fact $(f(r))^{-1} = f(r^{-1})$.
(ii) If $S$ is a ring with unity 1 and $R$ is a subring of $S$, then we **also require** that $1 \in R$. Thus, $R$ is also a ring with unity and it has the **same** unity as $S$. For example, $\{0\}$ is no longer allowed to be a subring of a ring $S$ with unity unless $S = \{0\}$ also. Likewise, $n\mathbb{Z}$ is **not** allowed to be a subring of $\mathbb{Z}$ for $n > 1$. For another, slightly more complicated example, if $R_1$ and $R_2$ are two nonzero rings with unity, then the "subring" $R_1 \times \{0\}$ is not, in this new sense, a subring of $R_1 \times R_2$: it has the unity $(1, 0)$, which is **not** the same as the unity $(1, 1)$ of $R_1 \times R_2$. However, most of the examples in our list of subrings still have the property that they contain the unity, and so are subrings in this new sense.

One simple remark that we shall use frequently is the following:

**Proposition 3.4.** *Ler $R$ and $S$ be rings and let $f\colon R \to S$ be a homomorphism. Then $\operatorname{Im} R = f(R)$ is a subring of $S$.*

*Proof.* From Modern Algebra I, we know that $f(R)$ is a subgroup of $(S, +)$. It is closed under multiplication since, if $f(r_1), f(r_2) \in f(R)$, then

$$f(r_1)f(r_2) = f(r_1(r_2) \in f(R).$$

Finally, if both of $R$, $S$ are rings with unity, then the assumption that $f(1) = 1$ implies that $1 \in f(R)$. □

**For the rest of this course, unless otherwise stated, all rings $R$ will be commutative rings with unity 1, all subrings of $R$ have to contain the unity 1, and all homomorphisms $f\colon R \to S$ satisfy $f(1) = 1$.**