RINGS

TIM SMITS

Rings are objects which abstract the nice properties that addition and multiplication have in the integers.

1. Basic definitions and examples

Definition 1.1. A **ring** is a set R with binary operations $+, \cdot$ called addition and multiplication that satisfy the following axioms for all $a, b, c \in R$:

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$ and $(ab)c = a(bc)$.
3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
4. There is an element $0 \in R$ with the property $a + 0 = a$.
5. For any a, there is an element $-a \in R$ such that $a + (-a) = 0$.
6. There is an element $1 \in R$ such that $a \cdot 1 = a$.

Note that the definition of a ring does *not* require that multiplication be commutative. A ring that satisfies $ab = ba$ for all $a, b \in R$ is called a **commutative ring**.

Some algebra textbooks do not require that a ring have a multiplicative identity, and instead call our definition a "ring with identity". This is very bad – for various reasons, it ends up being better to think of not having an identity element as something *missing* from a ring instead of something *added* to a ring. There are a few arguments for not including a multiplicative identity as part of the definition of a ring, but at the end of the day, objects that behave like rings without identity are much better labeled under different terms. See for example, [1] or [2] for a more in depth discussion.

Definition 1.2. A **subring** of a ring R is a subset $S \subset R$ such that the operations $+, \cdot$ of R make S a ring with multiplicative identity the same as that of R.

Rings are defined in such a way that make all the basic arithmetic properties of the integers carry over.

Proposition 1. *Let R be a ring.*

1. $a0 = 0a = 0$ *for all* $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$.
3. $(-a)(-b) = ab$ *for all* $a, b \in R$.
4. $-a = (-1)a$ *for all* $a \in R$.

Proof. Exercise. □

We'll start off by listing a standard collection of rings that we'll be using to later to illustrate the differences that can arise in ring structures.

Example 1.3. We've already studied two examples of a ring in depth: the integers $\mathbb{Z}$ are the most basic example of a commutative ring, and the integers mod n, $\mathbb{Z}/n\mathbb{Z}$, also form

a commutative ring for any $n > 1$. Note that neither $\mathbb{Z}$ nor $\mathbb{Z}/n\mathbb{Z}$ have any non-trivial subrings: any subset of $\mathbb{Z}$ that contains 1 and is also closed under addition contains all positive integers. Since a subring also contain inverses, it contains all negative integers as well, and must contain 0, and therefore such a subset is actually all of $\mathbb{Z}$. Similarly, any subset of $\mathbb{Z}/n\mathbb{Z}$ that contains $[1]$ and is closed under addition contains $[1], [2], \ldots, [n-1], [n]$ which gives us all of $\mathbb{Z}/n\mathbb{Z}$.

Example 1.4. The trivial ring (or zero ring) is the set $\{0\}$ with operations defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$. Note that in this ring, the additive and multiplicative identity are equal!

Example 1.5. The rational numbers $\mathbb{Q}$, and the real numbers $\mathbb{R}$ are both familiar commutative rings. More generally, if F is any field, then F is also a commutative ring.

Example 1.6. If R is any ring, then the set of polynomials with coefficients in R and the variable T, $R[T]$, has a ring structure given by the usual addition and multiplication of polynomials. The additive identity is the zero polynomial $p(T) = 0$ and the multiplicative identity is the polynomial $p(T) = 1$. Note that $R[T]$ is commutative if and only if R is commutative.

Example 1.7. If R is any ring, then the set of formal power series with coefficients in R and the variable T, $R[[T]]$, has the structure of a ring. Here, a typical element of $R[[T]]$ is an expression of the form $f(T) = \sum_{n=0}^{\infty} a_n T^n$. The sum of two power series $f(T) = \sum_{n=0}^{\infty} a_n T^n$ and $g(T) = \sum_{n=0}^{\infty} b_n T^n$ is defined by $(f+g)(T) = \sum_{n=0}^{\infty}(a_n + b_n)T^n$ and the product is given by $(fg)(T) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) T^n$.

Example 1.8. If R is any ring, then the set $M_n(R)$ of $n \times n$ matrices with coefficients in R with the usual addition and multiplication of matrices forms a ring. Here the additive identity is the zero matrix, and the multiplicative identity the identity matrix (hence the names). $M_n(R)$ is our first interesting example of a non-commutative ring: if E_{ij} is the matrix with (i, j)-th entry equal 1 and 0 everywhere else, then $E_{11}E_{21} = 0$, while $E_{21}E_{11} = E_{21}$.

Example 1.9. Let $C(\mathbb{R})$ denote the set of functions $f : \mathbb{R} \to \mathbb{R}$ that are continuous. Then with operations given by pointwise addition and multiplication of functions, then $C(\mathbb{R})$ has the structure of a commutative ring with zero element the function $f(x) = 0$ and multiplicative identity $f(x) = 1$.

Example 1.10. For any squarefree integer D, let $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$. Then with operations given by $(a+b\sqrt{D})+(a'+b'\sqrt{D}) = (a+a')+(b+b')\sqrt{D}$ and $(a+b\sqrt{D})(a'+b'\sqrt{D}) = (aa' + bb'd) + (ab' + ba')\sqrt{D}$, we have that $\mathbb{Z}[\sqrt{D}]$ forms a commutative ring with additive and multiplicative identity elements given by 0 and 1 respectively. We see that $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{C}$. In the particular case that $D = -1$, the ring $\mathbb{Z}[i]$ is called the ring of **Gaussian integers**. The Gaussian integers are a subring of the field $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ that have a role analogous to the usual integers $\mathbb{Z}$ sitting inside of $\mathbb{Q}$.

We'll now give an easy criterion for determining when a subset of a ring forms a subring.

Proposition 2 (Subring test)**.** *Let $S \subset R$ be a subset such that:*

1. $1 \in S$.
2. $a - b \in S$ *for all* $a, b \in S$.

3. $ab \in S$ *for all* $a, b \in S$.

Then S *is a subring of* R.

Proof. We have $a - a = 0 \in S$. Since $1 \in S$, we then have $0 - 1 = -1 \in S$. As S is closed under multiplication, we have $a \cdot -1 = -a \in S$ for all $a \in S$. Therefore, we have $a - (-b) = a + b \in S$ for all $a, b \in S$, which says that S is closed under $\cdot$ and $+$. We're now done, because the relevant expressions in axioms $1, 2, 3$ live not only in S, but in R, where we know they satisfy the axioms. □

Example 1.11. Given two rings R, S, the **product ring** $R \times S$ is defined as a set by $R \times S = \{(r, s) : r \in R, s \in S\}$ with operations of addition and multiplication performed component-wise. The additive identity is given by $(0_R, 0_S)$ and the multiplicative identity is given by $(1_R, 1_S)$. If R is ring and $A, B \subset R$ are two subrings, then using the subring test one can check that $A \cap B$ is another subring of R.

There's no axiom that says an element in a ring must have a multiplicative inverse. Indeed, we've seen that in $\mathbb{Z}/n\mathbb{Z}$ that it's possible to have non-zero elements $[a]$ with $[a][b] = [0]$, which we called zero divisors. We carry this terminology over to the general ring setting.

Definition 1.12. Let R be a ring. A non-zero element $a \in R$ is called a **unit** if it has a multiplicative inverse, i.e. there is a non-zero element $b \in R$ with $ab = ba = 1$. The set of all units of R is denoted $R^\times$. A non-zero element $a \in R$ is called a **zero divisor** if there is a non-zero element $b \in R$ with $ab = 0$.

In the definition of unit above, it's important to remember that a unit is an element with a *two-sided* inverse. If a has both a left and right inverse, then necessarily they are the same: if $ab = 1$ and $ca = 1$, then multiplying by c says $b = c$. It's possible for an element to have a right sided inverse but no left sided inverse, but we don't want to call these things units. Also, note that it's not possible for an element $a \neq 0$ of a ring R to be both a zero divisor and a unit: if $ab = 1$ for some $b \in R$ and $ac = 0$ for some $c \in R$, multiplying the second equation by b says that $a = 0$, a contradiction. When a ring has no zero divisors, we give it a special name:

Definition 1.13. A commutative ring R is called an **integral domain** if R has no zero divisors. That is, for $a, b \in R$, $ab = 0$ means $a = 0$ or $b = 0$.

Integral domains are nice because they are rings in which the cancellation property holds.

Proposition 3. *Let* R *be an integral domain. Then if* $ab = ac$ *for some* $a, b, c \in R$ *with* $a \neq 0$*, we have* $b = c$.

Proof. $ab = ac$ means $a(b - c) = 0$. Since $a \neq 0$ and R is an integral domain, we must have $b - c = 0$, i.e. $b = c$. □

Example 1.14. $\mathbb{Z}$ is an integral domain, and $\mathbb{Z}^\times = \{-1, 1\}$, as these are the only integers a that have $ax = 1$ solvable in $\mathbb{Z}$. Note that every non-zero integers *is* a unit inside the larger ring $\mathbb{Q}$, which says that being a unit is a property of which ring the element is viewed as living in.

Example 1.15. We've seen that $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : (a, n) = 1\}$. In particular, we've also seen that every element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime, because this is equivalent to saying that $(a, n) = 1$ for $1 \leq a \leq n - 1$.

Example 1.16. A unit in $M_n(R)$ is a non-zero matrix A with $AB = BA = I_n$ for some non-zero matrix B, i.e. an invertible matrix. The set of units in $M_n(R)$ is denoted $\mathrm{GL}_n(R)$. When $R = F$ is a field, linear algebra tells us that a matrix is invertible if and only if it's determinant is non-zero. Also recall that if $AB = I_n$ for some matrices A, B then actually $BA = I_n$ as well, so having a one-sided inverse is the same as having a two-sided inverse. Note that our previous example says that E_{11} is a zero divisor for $n > 1$.

Example 1.17. In $\mathbb{Z}[i]$, let $a + bi$ be non-zero. Then notice that $(a + bi)(a - bi) = a^2 + b^2$, and that $a^2 + b^2 \neq 0$. The inverse of $a + bi$ inside the field $\mathbb{Q}(i)$ is then given by $\frac{a-bi}{a^2+b^2}$. Now, the multiplicative inverse of an element must be unique, and the inverse of $a + bi$ inside $\mathbb{Z}[i]$ is still a multiplicative inverse in $\mathbb{Q}(i)$. This means that $a + bi$ is a unit in $\mathbb{Z}[i]$ if and only if $\frac{a-bi}{a^2+b^2}$ lives in $\mathbb{Z}[i]$. Since $a \leq a^2 + b^2$ and $b \leq a^2 + b^2$, we see the only way that $\frac{a}{a^2+b^2}$ and $\frac{b}{a^2+b^2}$ are integers is when $a^2 + b^2 = 1$. This equation has integer solutions given by $(a, b) = (\pm 1, 0), (0, \pm 1)$, so that $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$.

The following result is sometimes useful.

Proposition 4. *Let R be a finite, integral domain. Then R is a field.*

Proof. Let $a \in R$ be non-zero. Define a function $f : R \to R$ by $f(x) = ax$. I claim that f is injective. Suppose that $f(x) = f(y)$ for some $x, y \in R$. Then $ax = ay$, so $a(x - y) = 0$. Since R is an integral domain and $a \neq 0$, the cancellation property says that $x - y = 0$, i.e. $x = y$. Since f is an injective map from a finite set to itself, f must be bijective, and in particular, surjective. Then by definition of surjectivity, there is some element $b \in R$ such that $f(b) = 1$, i.e. $ab = 1$. Since R is commutative, $ba = 1$, so we are done. □

2. Ring homomorphisms

In order to study rings, we must study structure preserving maps between them.

Definition 2.1. Let R and S be rings. A **ring homomorphism** $f : R \to S$ is a map satisfying the following:

(i) $f(1_R) = 1_S$
(ii) $f(x + y) = f(x) + f(y)$ for all $x, y \in R$
(iii) $f(xy) = f(x)f(y)$ for all $x, y \in R$.

A bijective ring homomorphism is called an **isomorphism**. If there is an isomorphism between two rings R and S we say that R and S are **isomorphic** and write $R \cong S$.

Attached to a ring homomorphism are two special subsets of R and S:

Definition 2.2. Let $f : R \to S$ be a ring homomorphism. The **kernel** of f, $\ker(f)$ is defined by $\ker(f) = \{x \in R : f(x) = 0\}$. The **image** of f, $\mathrm{Im}(f)$, is defined by $\mathrm{Im}(f) = \{f(x) : x \in \mathbb{R}\}$.

Proposition 5. *Let $f : R \to S$ be a ring homomorphism. Then $\mathrm{Im}(f)$ is a subring of S. If f is injective, then $R \cong \mathrm{Im}(f)$.*

Proof. Note that $f(1_R) = 1_S$ so $1_S \in \mathrm{Im}(f)$. Now suppose that $x, y \in \mathrm{Im}(f)$. Then we can write $x = f(a)$ and $y = f(b)$ for some $a, b \in R$. We then see that $x - y = f(a) - f(b) = f(a - b)$, so $x - y \in \mathrm{Im}(f)$ and $xy = f(a)f(b) = f(ab)$ because f is a ring homomorphism. The subring test then says that $\mathrm{Im}(f)$ is a subring of S. If f is injective, then by restricting the co-domain

we can consider f as a map $f : R \to \mathrm{Im}(f)$ instead. This map is now obviously a bijective ring homomorphism, so $R \cong \mathrm{Im}(f)$. □

The image of f is a subring of S, but the kernel of f is *not* a subring of R, because the definition requires that $f(1_R) = 1_S$, so $1_R \notin \ker(f)$. Part of our reason for requiring that rings have a multiplicative identity is because we *don't* want kernels to be subrings – they are an example of a different type of object, called an *ideal*, which we will study more in depth later.

Example 2.3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a ring homorphism. Since $n = n \cdot 1$ and $f(1) = 1$ by definition, we have $f(n) = nf(1) = n$, i.e. f is the identity map. The identity map is obviously a ring homomorphism, so this says there is a single ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$. More generally, there is a single ring homorphism from $\mathbb{Z}$ to any ring R: if $f : \mathbb{Z} \to R$ is a homomorphism, we again have $f(1) = 1_R$ so $f(n) = n \cdot 1_R$, where the latter denotes repeated addition of 1_R a total of n times. It's once more fairly easy to see that this map actually is a ring homomorphism, so there is is a unique ring homorphism from $\mathbb{Z}$ into any ring.

Example 2.4. Let $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$. This is defined by $f(n) = n \cdot [1] = [n]$. This map is called the **natural projection** map. f is clearly surjective, so $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$. The kernel of f is all integers n with $[n] = [0] \in \mathbb{Z}/n\mathbb{Z}$, i.e. $\ker(f) = \{nk : k \in \mathbb{Z}\}$.

Example 2.5. Let $f : R \to R[x]$ be defined by $f(r) = r$ for $r \in R$, where the latter is viewed as the constant polynomial $p(x) = r \in R[x]$. It's easy to see that f is a ring homomorphism, with $\ker(f) = \{0\}$. In general, if $R \subset S$ is a subring, then the map $f : R \to S$ given by $f(r) = r$ is a ring homomorphism called the **natural inclusion**.

Example 2.6. Let $c \in R$ and define $f_c : R[x] \to R$ by $f_c(p(x)) = p(c)$. This is a ring homomorphism: if $p(x) = 1$, then $f_c(p(x)) = p(c) = 1$, and for $p, q \in R[x]$ we have $f_c((pq)(x)) = (pq)(c) = p(c)q(c) = f_c(p(x))f_c(q(x))$ and $f_c((p + q)(x)) = (p + q)(c) = p(c) + q(c) = f_c(p(x)) + f_c(q(x))$ because of how polynomial addition and multiplication is defined. This homomorphism is called the **evaluation** map. Note that f is surjective, so $\mathrm{Im}(f_c) = R$, and $\ker(f_c) = \{p(x) \in R[x] : p(c) = 0\}$ is the set of all polynomials that vanish at c.

Example 2.7. Let $f : R \to S$ be a ring homomorphism, and let $x \in R^\times$. Then by definition, there is $y \in R$ with $xy = yx = 1_R$, so $f(x)f(y) = f(xy) = f(1_R) = f(yx) = f(y)f(x) = 1_S$ says that $f(x) \in S^\times$. That is, units map to units under ring homomorphisms. This is hopefully unsurprising, because homomorphisms preserve ring structure – if $r \in R$ satisfies some sort of algebraic relation in terms of $+$ and $\cdot$, then so must $f(r) \in S$!.

Example 2.8. Our first example tells us the ring homomorphism $i : \mathbb{Z} \to \mathbb{Q}$ is the inclusion map, but there is no ring homomorphism $f : \mathbb{Q} \to \mathbb{Z}$. To see this, note $f(1) = 1$, so $f(n) = n$ for any $n \in \mathbb{Z}$. Then $1 = 2 \cdot \frac{1}{2}$, so $1 = f(1) = f(2 \cdot \frac{1}{2}) = 2f(\frac{1}{2})$, which is obviously impossible in $\mathbb{Z}$.

Example 2.9. A **ring endomorphism** is a ring homomorphism $f : R \to R$ for a ring R. The set of ring endomorphisms of R is denoted $\mathrm{End}(R)$. Then $\mathrm{End}(R)$ has the structure of a ring under the operations $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(g(x))$ for $x \in R$, i.e. addition is pointwise and multiplication is composition (you should verify that the

composition of two homomorphisms is still a homomorphism!). Our first example shows that $\mathrm{End}(\mathbb{Z}) = \{\mathrm{id}_{\mathbb{Z}}\}$ is a ring with 1 element, i.e. $\mathrm{End}(\mathbb{Z}) \cong \{0\}$.

There's an easy way to check if a ring homomorphism is injective or surjective by translating these set theoretic statements into the language of images and kernels:

Proposition 6. *Let $f : R \to S$ be a ring homomorphism. Then f is injective if and only if $\ker(f) = \{0\}$. Similarly, f is surjective if and only if $\mathrm{Im}(f) = S$.*

Proof. First, suppose that f is injective. Since $f(0) = 0$, if $x \in \ker(f)$ we have $f(x) = 0 = f(0)$, so the injectivity of f says that $x = 0$. Now suppose that $\ker(f) = \{0\}$, and that $f(x) = f(y)$. Since f is a ring homomorphism, this says $f(x-y) = 0$, so that $x-y \in \ker(f)$. This then means that $x - y = 0$, so that $x = y$, which proves that f is injective. The latter statement is obvious, since the image of f in the ring theoretic sense is the same as in the set theoretic sense. □

Example 2.10. The complex number i satisfies the algebraic relation $i^2 = -1$. In the ring $M_2(\mathbb{R})$, there is a matrix $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ with the property that $A^2 = -I_2$. We can naturally associate any real number a to a diagonal matrix in $M_2(\mathbb{R})$, so this suggests we define a map $f : \mathbb{C} \to M_2(\mathbb{R})$ by $f(a+bi) = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. One can verify that f is an injective ring homomorphism, so that $\mathbb{C} \cong \mathrm{Im}(f)$ can be identified with a subring of $M_2(\mathbb{R})$!.

References

[1] https://math.mit.edu/~poonen/papers/ring.pdf
[2] https://kconrad.math.uconn.edu/blurbs/ringtheory/ringdefs.pdf