Ring Theory Basics 1

P. Reany

April 22, 2025

Abstract

Just the very basic stuff for now.

> Emmy Noether's contributions to ring theory are monumental and have profoundly shaped modern mathematics. Her work on the theory of ideals in rings, particularly her publication "Idealtheorie in Ringbereichen," introduced the ascending-chain condition, which ensures that chains of ideals terminate after a finite number of steps. This concept laid the foundation for the classification of Noetherian rings, named in her honor, and significantly advanced abstract algebra.
> — Copilot

(At this point, I don't have many interesting quotes from famous mathematicians about rings. But I'm sure they're out there somewhere.)

1 From additive groups to rings

An example of a group is the set of integers $G = (\mathbb{Z}, +)$ under binary operation of addition, where 0 acts as the identity element of G. But we know that we can also multiply any two integers and get back another integer. Does this new structure have a special name? Yes, it's called a **ring** — the ring R of integers, which, to be precise, is $R = (\mathbb{Z}, +, \cdot)$, where, of course, some extra rules go along with this multiplication operation.

Definition: A **ring** R is a set of elements on which is defined a binary operator $+$, such that:

1) For any two elements of a and b of R, $a + b = b + a$ is an element of R [binary closure under addition].

2) For any three elements of a, b, c of G, $(a + b) + c = a + (b + c)$ [addition composition associativity].

3) There exists an element 0 of R, such that for any element of r, of R, $0 + r = r + 0 = r$ [0 being referred to the ring's additive identity element].

4) For every element r of R, there exists an element of $-r$, of R, such that $r + (-r) = (-r) + r = 0$ [$-r$ being referred to as the element's additive inverse element in R].

Thus, we see that every ring under only addition is an additive group, and every additive group is abelian. The rules governing multiplication in a ring are similar to those governing a group, except that ring elements do not necessarily have multiplicative inverses for each ring element. The ring of integers is like that. For example, its element 5 does not have a multiplicative inverse in the integers. The next ring up from the integers that contains multiplicative inverses for all its nonzero elements is the ring of rational numbers $(\mathbb{Q}, +, \cdot)$. And, of course, we are free to drop the $\cdot$ for multiplication in an expression, so long as the resulting expression is unambiguous.

Proceeding along, the rules governing ring multiplication are as follows:

1) For any two elements of a and b of R, ab and ba are elements of R [binary closure under multiplication].

2) For any three elements of a, b, c of R, $(ab)c = a(bc)$ [multiplicative composition associativity].

3) For any three elements of a, b, c of R, $a(b + c) = ab + ac$ [left multiplicative distributivity over addition].

4) For any three elements of a, b, c of R, $(b + c)a = ba + ca$ [right multiplicative distributivity over addition].

So, what about the existence of a multiplicative identity element in a ring? For the moment, let's use the symbol "1" to refer to the multiplicative identity element of a ring R, if the ring even has one. Then for every element r of R, $1r = r1 = r$.

Definition: A ring R is said to be **trivial** if it contains only the zero element; otherwise, it's said to be **nontrivial**.

Definition: A ring R with unitary element 1 is said to be **a ring with unity** or a **unital ring**.

Note: A ring R could be configured so that $0 = 1$, but nobody seems to want to deal with such a misfit, and neither do I here.

Definition: A ring R is said to be a **commutative** if for all a and b in R

$$ab = ba\,. \tag{1}$$

We reserve "abelian" for the commutivity of elements under addition and we reserve "commutative" for commutivity of elements under multiplication.

Definition: Every element of a unital ring R which has a multiplicative inverse is said to be a **unit** of the ring. So, if r is a unit of R then there exists some

element r' of R such that $rr' = r'r = 1$. I should point out that r and r' need not be distinct elements. If they are not, then r is its own multiplicative inverse, and $r^2 = 1$. Of course, both the unitary element 1 (if the ring has one) and 0 square to themselves.

Definition: A ring element is said to be an **idempotent** if it squares to itself.

Definition: I'll make powers formal here. The symbol r^n is an n-fold product of r with itself, where n is a positive integer. That is.

$$r^n \equiv r \cdot r \cdots r \,, \tag{2}$$

in which this product has n factors of the element r.

So, we see here one advantage of abstracting ring theory. Exponentiation by a positive integer has the same meaning whether the ring is the integers or a matrix ring or any other ring.

Definition: Let R be a unital ring. Denote by $R^\times$ as the subset of units of R.

Theorem: Let R be a unital ring. Then $R^\times$ is a multiplicative group under the multiplicative and associative operations defined in R. (Proof left to the reader.)

Definition: A **zero-divisor** of a ring R is a nonzero element r of R, such that, there exists some other nonzero element of R, r', such that

$$\text{either} \qquad rr' = 0 \qquad \text{or} \qquad r'r = 0 \,. \tag{3}$$

Definition: A nontrivial, commutative unital ring with no zero divisors is said to be a **integral domain.** The ring of integers is a good example.

Definition: A unital ring R in which every nonzero element is a unit is said to be a **division ring**. The meaning of this is simple: In such a ring, division is generally allowed.

Definition: A commutative, unital ring R in which every nonzero element has a multiplicative inverse is said to be a **field**. The sets of rational numbers, real numbers, and complex numbers are examples of fields.

It turns out that most rings of interest are unital, but let's look at a ring that has no multiplicative identity element. This is not difficult to do. Let's start with the integers $R = (\mathbb{Z}, +, \cdot)$ and then form a new ring by multiplying every element of R by the integer 2, which we'll denote as simply $2\mathbb{Z}$. So, what do the elements of $2\mathbb{Z}$ look like? They look like the set of even numbers, both positive, negative, and zero. But there is no number in $2\mathbb{Z}$ that can act as a multiplicative identity.

Definition: Let R be a ring. Let x be a nonzero element of R such that for some positive integer $n \geq 2$,

$$x^n = \mathbf{0} \,, \tag{4}$$

then element x is said to be **nilpotent** in R, and n is the smallest integer that satisfies (4).

Nilpotent elements are somewhat exotic in that you won't find examples of them in an integral domain or in field. But you can readily find them matrix rings, especially if they aren't highly specialized. Consider the matrix ring R of 2×2 matrices with integer entries. Let's examine the matrix

$$x = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \tag{5}$$

I leave it to the reader to confirm that $x^2 = \mathbf{0}$, where

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \tag{6}$$

and where $\mathbf{0}$ is the additive inverse of this ring.

Theorem: An integral domain D cannot contain a nilpotent element.

Proof: Assume the contrary. Let nonzero element $x \in D$ be nilpotent. Then, for some integer $n \geq 2$,

$$x^n = 0, \tag{7}$$

where n is the smallest positive integer satisfying this relation. Therefore,

$$x x^{n-1} = 0, \tag{8}$$

but this means that x and x^{n-1} play the roles of complementary zero divisors, which cannot exist in D by assumption. Therefore, x cannot be nilpotent.

The ring axioms (again):

For all $a, b, c \in R$,

a) $a + b = b + a$ for all $a, b \in R$

There exists a $0 \in R$ such that for all $a \in R$
b) $a + 0 = 0 + a = a$

For all $a, b, c \in R$
c) $(a + b) + c = a + (b + c)$
d) $(ab)c = a(bc)$
e) $c(a + b) = ca + cb$
f) $(a + b)c = ac + bc$

If R is unital (i.e., has a unitary element '1') then for all $a \in R$:
g) $1a = a1 = a$.