Rings

Many algebraic structures have both an addition and a multiplication. So let's start to investigate what happens when we add that second operation.

Often we will have a structure that has two natural operations, usually that relate to each other via distributivity. So let's dive in and discuss such structures.

Definition. A *ring* is a non-empty set R together with two operations $+$ and $\cdot$ that satisfy:

- $(R, +)$ is an abelian group.
- R is associative under $\cdot$. (Also, we often omit the multiplication dot, writing ab instead of $a \cdot b$.)
- Multiplication distributes over addition: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Notice that we have to list both left- and right-distributivity as axioms for rings, since there is nothing that says our multiplication must be commutative. The term abelian is only used with groups, not rings, and if the multiplication is commutative we call the ring commutative. (The reason for this is that Abel studied permutations related to polynomial equations before there was a formalized theory about groups in the first place, so the specific structures that Abel studied were called Abelian systems, which were only then later identified to be a subclass of groups.)

Many of the most familiar sets that have two operations are rings.

Example. The integers $\mathbf{Z}$ are a ring, as are $\mathbf{Z}_n$ for any integer n, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ under the standard operations.

Example. $2\mathbf{Z}$ is also a ring, though this time there is no multiplicative identity.

Example. $\mathbf{R}[x]$, the set of all polynomials with real coefficients is a ring utilizing standard addition and multiplication of polynomials. We could also have other sets of coefficients (e.g. integers or complex), and we could also have polynomials in more than one variable.

All the rings mentioned so far have commutative multiplication. That is definitely not always the case!

Example. $M_{2,2}(\mathbf{R})$, the set of 2×2 matrices with regular matrix addition and multiplication is a ring. Of course, we could use other types of entries (integer, complex, $\mathbf{Z}_1 2$) and also obtain rings. And we could have larger square matrices as well.

Example. The *quaternions* are the set of all $a + bi + cj + dk$ where a, b, c, and d are real numbers. These are added by collecting like terms, and multiplied like polynomials, using the relationships $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, and $ki = j$.

Since the addition in a ring is a commutative group, we use additive notation for it. The additive identity in a ring is 0.

Lemma 1.
- $a0 = 0a = 0$ *for any* $a \in R$.
- $a(-b) = (-a)b = -(ab)$ *for any* $a, b \in R$.
- $(-a)(-b) = ab$ *for any* $a, b \in R$.

Proof. Note that $a0 = a(0+0) = a0 + a0$ and the result is obtained by additive cancellation. The same works for $0a = (0+0)a = 0a + 0a$.

Then $0 = a0 = a(b + (-b)) = ab + a(-b)$. Adding the opposite $-(ab)$ to both sides yields $a(-b) = -(ab)$. The other half is similar using $0b = (a + (-a))b$.

The third bullet comes from the second and the fact that the inverse of the inverse is the original element by uniqueness of inverses. □

Rings have several special sub-classes depending on them having several different "nice" properties. Here are a few.

Definition. If a ring has a multiplicative identity (which will usually be notated 1, though note that matrices often use I for the identity), it is called a *ring with unity*.

Be careful! Just because something acts like an identity for some elements doesn't make it an identity for all! For example, among 2×2 matrices, consider $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. If you multiply any matrix of the form $B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ on the left by A you will get B. But there are other matrices (e.g. with non-zero entries in the second column) for which A does not act as a left identity. Similarly, A acts as a right identity for any matrix with zero second row, but not for one that has a non-zero second row. The reason we can have "partial" identities like this is that we don't have inverses and cancellation.

Definition. In a ring that has a unity, all elements that have multiplicative inverses are called *units*.

Example. Consider 2×2 integer matrices. The identity matrix is the unity in this ring. The units are all integer matrices with determinant ± 1.

Now since $0a = 0$ for any a, unless the ring consists of just the element 0 (which is generally not considered interesting) the element 0 cannot have an inverse—0 is never a unit. But it is possible that all other elements have inverses.

Definition. A ring with unity in which each non-zero element is a unit is called a *division ring* (or sometimes a *skew field*).

Example. The real quaternions are a division ring. For note that $(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$. Since this is always a positive real numbers (unless all of a, b, c, and d are zero) we can find a multiplicative inverse for quaternions just like we did for complex numbers.

We won't run into many division rings that are not also commutative. They are actually kind of rare, and it is lucky we could produce one at all!

Definition. a commutative division ring is called a *field.*

The standard fields, where we can do addition, subtraction, multiplication, and division are $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $\mathbf{Z}_p$ where p is a prime. There are plenty of other fields, but these familiar examples show that fields are a useful thing to study.

A few paragraphs ago, we noted that "acting" like an identity for some elements was not good enough, because we didn't have cancellation. Let's examine this idea.

In any ring, non-zero elements a and b are called *zero divisors* if $ab = 0$. For example, in $\mathbf{Z}_12$ the elements 3 and 8 are zero divisors because their product is congruent to 0 modulo 12. Note that we should be more specific. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ while $BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. So there are left zero divisors and right zero divisors. Of course, in a commutative group it doesn't matter.

Lemma 2. *If a is not a left zero divisor and $ab = ac$ then $b = c$ (you can left-cancel elements that are not left zero divisors). Similarly, if a is not a right zero divisor and $ba = ca$ then $b = c$.*

Proof. If $ab = ac$ then $ab - ac = 0$ so by distributivity $a(b - c) = 0$. Since a is not a left zero divisor, $b - c = 0$ so $b = c$. A similar proof works on the other side. The proof is actually if and only if, because if a is a zero divisor, with $ab = 0$ but $b \neq 0$ then for any x, $ax = a(x + b)$ yet $x \neq x + b$. □

So in any ring with no zero divisors, the cancellation laws must hold for multiplication. An example where this might not be so obvious is multiplying polynomials. Clearly, since degree of polynomials adds upon multiplying the polynomials, there can't be any zero divisors. But then if $p(x)q(x) = p(x)r(x)$ we will have $q(x) = r(x)$. This will help with proving unique factorization of polynomials!

Note that a division ring cannot have any zero divisors, for if $ab = 0$ but $bb^{-1} = 1$ then $0 = 0b^{-1} = abb^{-1} = a1 = a$.

A commutative ring with no zero divisors is called an *integral domain.* Many texts (including ours) require integral domains to have a unity. So make sure you are aware of the exact definitions in use!

Example. Consider polynomials all of whose coefficients are even integers. This is an integral domain by some definitions, because there are no zero divisors. But there is no unity.

Every field is an integral domain, as a field is a division ring which cannot have zero divisors.

Now groups have subgroups. Naturally, rings will have subrings. A subring S of R is any subset that is a ring under the same operations. So $2\mathbf{Z} \subset \mathbf{Z}$ is a subring of $\mathbf{Z}$. SImilarly, $\mathbf{R}$ is a subfield of $\mathbf{C}$, and in turn contains subfield $\mathbf{Q}$, which then contains subring (not field!) $\mathbf{Z}$.

Lemma 3. *A nonempty subset $S \subset R$ is a subring if and only if it is closed under multiplication and subtraction.*

We use subtraction to avoid having the positive integers be a subring of the integers—they aren't even a subgroup under addition. The proof of the lemma is nearly trivial: the subtraction allows it to be an additive subgroup; the multiplicative closure allows it to be closed under multiplication, and associativity and distributivity are inherited.

Since addition is commutative, every subring is "normal." But quotients by any old subring don't quite work out. We'll have to wait and see what quotient rings mean. Especially because we can also take a ring without divison capablities and build them in, making a ring of quotients! Things will get confusing if we don't keep all our definitions straight!