We now begin to develop the abstract part of abstract algebra.

We want to identify the common algebraic properties that the sets \( \mathbb{Z}_n, k\mathbb{Z} \) for an integer \( k \geq 2 \), \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \), and the set \( M(\mathbb{R}) \) of all \( 2 \times 2 \) real-valued matrices have, and do this in a minimal way.

**Definition.** A ring is a nonempty set \( R \) equipped with two operations, usually written as addition \( a + b \) and multiplication \( ab \), that satisfy the following axioms.

1. If \( a \in R \) and \( b \in R \), then \( a + b \in R \).
2. For all \( a, b, c \in R \), we have \( a + (b + c) = (a + b) + c \).
3. For all \( a, b \in R \), we have \( a + b = b + a \).
4. There exists an element \( 0_R \in R \) such that for all \( a \in R \) we have \( 0_R + a = a = a + 0_R \).
5. For each \( a \in R \) the equation \( a + x = 0_R \) has a solution \( x \in R \).
6. If \( a \in R \) and \( b \in R \), then \( ab \in R \).
7. For all \( a, b, c \in R \), we have \( a(bc) = (ab)c \).
8. For all \( a, b, c \in R \), we have \( a(b + c) = ab + ac \) and \( (a + b)c = ac + bc \).

We did not put as an axiom of a ring the commutativity of multiplication because \( M(\mathbb{R}) \) does not satisfy this.

**Definition** A commutative ring is a ring \( R \) that satisfies

9. For all \( a, b \in R \) we have \( ab = ba \).

We did not put as an axiom of a ring the existence of a multiplicative identity because the set \( 2\mathbb{Z} \) does not have a multiplicative identity.

**Definition** A ring with identity is a ring \( R \) that satisfies

10. There exists an element \( 1_R \) in \( R \) such that for all \( a \in R \) we have \( 1_R a = a = a 1_R \).

**Examples.** The sets \( \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are all commutative rings with identity.

The set \( M(\mathbb{R}) \) is a noncommutative ring with identity.

The set \( k\mathbb{Z} \) for each integer \( k \geq 2 \) is a commutative ring without identity.

**Examples**

(a) Is the set \( R \) of odd integers a ring? If not which axiom fails?

Well, Axiom (1) fails because odd plus odd is not odd.

(b) Is the vector space \( \mathbb{R}^3 \) equipped with the usual addition and the cross product for multiplication a ring?

The addition satisfies Axioms (1) through (5), and the cross product satisfies Axiom (6).

But for the cross product applies the standard basis vectors \( i, j, \) and \( k \), we have

\[ i \times (i \times k) = i \times (-j) = -k \]
and

\[(i \times i) \times k = 0 \times k = 0\]

which are not equal, and so Axiom (7) fails, that is, the cross product is not associative.

(c) Is the set \(M(\mathbb{R})\) with the usual addition but with the multiplication

\[AB = B^T AB\]
a ring? Which axioms fails?

Well, Axioms (1) through (6) hold, but is this multiplication associative?

We investigate: for \(A, B, C \in M(\mathbb{R})\) we have

\[A(BC) = A(B^T CB) = (B^T CB)^T AB^T CB = B^T C^T BAB^T CB,\]

and

\[(AB)C = (A^T BA)C = C^T (A^T BA)C.\]

These are not the same, and so Axiom (7) fails, that is, the multiplication is not associative.

Example. For a commutative ring \(R\) with identity, is the set \(M(R)\) of all \(2 \times 2\) matrices with entries in \(R\), and equipped with addition and multiplication extended from \(R\) to the matrix level, a ring? a commutative ring? a ring with identity?

If \(R = \mathbb{Z}\), then the set \(M(\mathbb{Z})\) of all integer valued \(2 \times 2\) matrices is a noncommutative ring with identity \(I\) (the \(2 \times 2\) identity matrix).

If \(R = \mathbb{Z}_n\), then the set \(M(\mathbb{Z}_n)\) of all \(\mathbb{Z}_n\)-valued \(2 \times 2\) matrices is a noncommutative ring with identity \(I\).

Example. Is there a commutative ring \(R\) without identity for which the set \(M(R)\), of all \(2 \times 2\) a matrices with entries in \(R\), is a noncommutative ring without identity?

Yes, for the ring \(k\mathbb{Z}\) for each \(k \geq 2\) we have that \(M(R)\) is a noncommutative ring without identity.

Example. To see the abstract part of all of this in action, we consider the set \(R = \{a, b, c, d\}\) of four elements with addition and multiplication defined according to the following tables.

<table>
<thead>
<tr>
<th>+</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>b</td>
<td>a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>a</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
</tbody>
</table>
There are no numbers here to add and multiply, only the manipulation of four symbols according to the tables.

This is abstract algebra.

The set \( R \) with the operations of addition and multiplication is a ring, where it is easy to verify that addition and multiplication are both commutative (because the tables are symmetric).

However, it is messy to verify Axioms (7) and (8) (the associativity of multiplication and the distributivity of multiplication over addition) because one has to check every case. For instance,

\[
a(bc) = aa = a \quad \text{and} \quad (ab)c = ac = a,
\]

and

\[
a(b + c) = ad = a \quad \text{and} \quad ab + ac = a + a = a.
\]

Which element of \( R \) is the additive identity? It is \( a \).

Does \( R \) has a multiplicative identity? Yes, it is \( d \).

Thus \( R \) is a commutative ring with identity.

The ring \( \mathbb{Z}_n \) for \( n \) composite does not have the property that there exists two nonzero elements whose product is nonzero.

Definition. An integral domain is a commutative ring \( R \) with identity \( 1_R \neq 0_R \) such that

11. For \( a, b \in R \), if \( ab = 0_R \), then \( a = 0_R \) or \( b = 0_R \).

Examples. For \( p \) a positive prime integer, the ring \( \mathbb{Z}_p \) is an integral domain by Theorem 2.8.

The ring \( \mathbb{Z} \) is also an integral domain, from which we can form the ring \( \mathbb{Q} \) of fractions \( a/b \) for \( a, b \in \mathbb{Z} \) with \( b \neq 0 \), on which we define an equivalence relation

\[
\frac{a}{b} \equiv \frac{r}{s} \quad \text{when} \quad as = br,
\]

and on the equivalence classes we define addition + and multiplication \( \cdot \) by

\[
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.
\]

Do you see why we need \( \mathbb{Z} \) to be an integral domain to do this? In the multiplication so that for nonzero \( b \) and \( d \) we always have \( bd \neq 0 \).

Definition. A field is a commutative ring \( R \) with identity \( 1_R \neq 0_R \) that satisfies

12. For each \( a \neq 0_R \) in \( R \), the equation \( ax = 1_R \) has a solution \( x \in R \).

Examples For a positive prime \( p \), the integral domain \( \mathbb{Z}_p \) is a field by Theorem 2.8.

The integral domains \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are fields.