We have now seen a variety of different kinds of rings: commutative and noncommutative rings, rings with or without identity.

We can form new rings from old rings via the Cartesian product.

Recall that for two nonempty sets $R$ and $S$, the Cartesian product is the set of ordered pairs:

$$R \times S = \{(r, s) : r \in R, s \in S\}.$$

**Example.** Let $T$ be the Cartesian product of the commutative rings with identity, $R = \mathbb{Z}_2$ and $S = \mathbb{Z}_3$.

Then

$$T = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

We define an addition on $T$ through the components, or component-wise:

<table>
<thead>
<tr>
<th></th>
<th>(0,0)</th>
<th>(0,1)</th>
<th>(0,2)</th>
<th>(1,0)</th>
<th>(1,1)</th>
<th>(1,2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(1,0)</td>
<td>(1,1)</td>
<td>(1,2)</td>
</tr>
<tr>
<td>(0,1)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(0,0)</td>
<td>(1,1)</td>
<td>(1,2)</td>
<td>(1,0)</td>
</tr>
<tr>
<td>(0,2)</td>
<td>(0,2)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(1,2)</td>
<td>(1,0)</td>
<td>(1,1)</td>
</tr>
<tr>
<td>(1,0)</td>
<td>(1,0)</td>
<td>(1,1)</td>
<td>(1,2)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
</tr>
<tr>
<td>(1,1)</td>
<td>(1,1)</td>
<td>(1,2)</td>
<td>(1,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(0,0)</td>
</tr>
<tr>
<td>(1,2)</td>
<td>(1,2)</td>
<td>(1,0)</td>
<td>(1,1)</td>
<td>(0,2)</td>
<td>(0,0)</td>
<td>(0,1)</td>
</tr>
</tbody>
</table>

We define a multiplication on $T$ also component-wise.

<table>
<thead>
<tr>
<th></th>
<th>(0,0)</th>
<th>(0,1)</th>
<th>(0,2)</th>
<th>(1,0)</th>
<th>(1,1)</th>
<th>(1,2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
</tr>
<tr>
<td>(0,1)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
</tr>
<tr>
<td>(0,2)</td>
<td>(0,0)</td>
<td>(0,2)</td>
<td>(0,1)</td>
<td>(0,0)</td>
<td>(0,2)</td>
<td>(0,1)</td>
</tr>
<tr>
<td>(1,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(0,0)</td>
<td>(1,0)</td>
<td>(1,0)</td>
<td>(1,0)</td>
</tr>
<tr>
<td>(1,1)</td>
<td>(0,0)</td>
<td>(0,1)</td>
<td>(0,2)</td>
<td>(1,0)</td>
<td>(1,1)</td>
<td>(1,2)</td>
</tr>
<tr>
<td>(1,2)</td>
<td>(0,0)</td>
<td>(0,2)</td>
<td>(0,1)</td>
<td>(1,0)</td>
<td>(1,2)</td>
<td>(1,1)</td>
</tr>
</tbody>
</table>

With an exhaustive effort using these tables, we can show that $T$ is a commutative ring with identity.

What is the multiplicative identity of $T$? It is $(1,1)$.

**Theorem 3.1.** Let $R$ and $S$ be rings. The Cartesian product $R \times S$ is a ring with addition and multiplication on $R \times S$ defined by

$$(r, s) + (r', s') = (r + r', s + s'), \quad (r, s)(r', s') = (rr', ss').$$
If both $R$ and $S$ are commutative, then so is $R \times S$. If both $R$ and $S$ have an identity, then so does $R \times S$.

Idea of Proof. Using the eight axioms of rings for $R$ and $S$ we check that $T = R \times S$ satisfies all of the eight axioms of a ring.

If $R$ and $S$ are commutative, then $(r, s)(r', s') = (rr', ss') = (r'r, s's) = (r', s')(r, s)$, showing that $T$ is a commutative ring.

If $R$ and $S$ have identities $1_R$ and $1_S$ respectively, then $(1_R, 1_S)$ is the identity for $T$. □

As in Linear Algebra, where we look for subspaces of a vector space, we can look for subrings of a ring.

Definition. A nonempty subset $S$ of a ring $R$ is called a subring of $R$ if the set $S$ is a ring under the addition and multiplication of $R$.

Examples. (a) The nonempty subset $E = 2\mathbb{Z}$ of even integers is a subring of $\mathbb{Z}$.

(b) The subset $O$ of odd integers is not a subring of $\mathbb{Z}$ because the sum of two odd integers is not odd.

(c) The set of diagonal matrices

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{R} \right\}$$

is a subring of $M(\mathbb{R})$.

(d) The ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and the ring $\mathbb{Q}$ is a subring of $\mathbb{R}$.

Because $\mathbb{Q}$ is a field and $\mathbb{R}$ is a field, we say that $\mathbb{Q}$ is a subfield of $\mathbb{R}$.

Similarly, $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Theorem 3.2. Suppose $R$ is a ring. A subset $S$ of $R$ is a subring of $R$ if

(i) $S$ is closed under addition (if $a, b \in S$, then $a + b \in S$),

(ii) $S$ is closed under multiplication (if $a, b \in S$, then $ab \in S$),

(iii) $0_R \in S$, and

(iv) for each $a \in S$, the equation $a + x = 0_R$ has a solution $x$ in $S$.

Idea of Proof. One simply verifies that all of the eight axioms hold for $S$ given the four conditions above.

Examples. (a) The subset $\{0, 4\}$ of $\mathbb{Z}_8$ is closed under addition, closed under multiplication, contains $0_R$, and for $a = 0$ or $a = 4$, the equation $a + x = 0_R$ has a solution, namely $x = 0$ and $x = 4$ respectively in $\mathbb{Z}_8$. Thus $S$ is a subring of $\mathbb{Z}_8$.

(b) The set

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}.$$

is a subset of $\mathbb{R}$, but is it a subring?

We check each condition in Theorem 3.2.
Condition (i). For $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, we have
\[ a_1 + b_1 \sqrt{5} + a_2 + b_2 \sqrt{5} = (a_1 + a_2) + (b_1 + b_2) \sqrt{5} \in \mathbb{Q}(\sqrt{5}) \]
because $a_1 + a_2 \in \mathbb{Q}$ and $b_1 + b_2 \in \mathbb{Q}$.

Condition (ii). For $a_1, a_2, b_1, b_2 \in \mathbb{Q}$, we have
\[(a_1 + b_1 \sqrt{5})(a_2 + b_2 \sqrt{5}) = a_1a_2 + 5b_1b_2 + (a_1b_2 + a_2b_1) \sqrt{5} \in \mathbb{Q}(\sqrt{5}) \]
because $a_1a_2 + 5b_1b_2 \in \mathbb{Q}$ and $a_1b_2 + a_2b_1 \in \mathbb{Q}$.

Condition (iii). The zero element $0_{\mathbb{R}} = 0 + 0 \sqrt{5}$ of $\mathbb{R}$ belongs to $\mathbb{Q}(\sqrt{5})$.

Condition (iv). For $a + b \sqrt{5} \in \mathbb{Q}(\sqrt{5})$, a solution of $a + b \sqrt{5} + x = 0$ is the element $x = -a - b \sqrt{5}$ which is in $\mathbb{Q}(\sqrt{5})$ because $-a, -b \in \mathbb{Q}$.

Having satisfied the four conditions of Theorem 3.2, the set $\mathbb{Q}(\sqrt{5})$ is a subring of $\mathbb{R}$.

Is $\mathbb{Q}(\sqrt{5})$ a field, and hence a subfield of $\mathbb{R}$?

The ring $\mathbb{Q}(\sqrt{5})$ is commutative because it is a subring of the commutative ring $\mathbb{R}$.

Does the ring $\mathbb{Q}(\sqrt{5})$ have an identity?

Yes, it does, and it is the identity of $\mathbb{R}$, namely $1_{\mathbb{R}} = 1$, which is not $0_{\mathbb{R}}$.

Now it remains to show that $\mathbb{Q}(\sqrt{5})$ satisfies Axiom 12: for each nonzero $a + b \sqrt{5} \in \mathbb{Q}(\sqrt{5})$, the equation $(a + b \sqrt{5})x = 1$ has a solution in $\mathbb{Q}(\sqrt{5})$.

Since the numbers we are working with live in $\mathbb{R}$, we can solve $(a + b \sqrt{5})x = 1$ by dividing both sides by $a + b \sqrt{5}$ to get
\[ x = \frac{1}{a + b \sqrt{5}}. \]

We need to show that this $x$ is actually in $\mathbb{Q}(\sqrt{5})$.

Here we have
\[ x = \frac{1}{a + b \sqrt{5}} \frac{a - b \sqrt{5}}{a - b \sqrt{5}} = \frac{a - b \sqrt{5}}{a^2 - 5b^2}. \]

This only makes sense if $a^2 - 5b^2 \neq 0$, which does not follow from $a + b \sqrt{5} \neq 0$, but from $\sqrt{5}$ not being rational.

Thus
\[ x = \left( \frac{a}{a^2 - 5b^2} \right) - \left( \frac{b}{a^2 - 5b^2} \right) \sqrt{5} \in \mathbb{Q}(\sqrt{5}) \]
and so $\mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{R}$.

(c) The set $\mathbb{Z}[\sqrt{5}] = \{a + b \sqrt{5} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{5})$ because it is closed under addition, closed under multiplication,
\[(a_1 + b_1 \sqrt{5})(a_2 + b_2 \sqrt{5}) = (a_1a_2 + 5b_1b_2) + (a_1b_2 + a_2b_1) \sqrt{5} \in \mathbb{Z}[\sqrt{5}],\]
contains the zero element of $\mathbb{Q}(\sqrt{5})$, and the equation $(a + b \sqrt{5}) + x = 0$ has a solution $x = -a - b \sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$. 