Rings and fields

Zero divisors, multiplicative inverses and units

Next, some algebra that doesn’t work...

\( \mathbb{Z}_8 \) again (focus on multiplication):

\[
\begin{array}{c|cccccccc}
\cdot & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
2 & 0 & 2 & 4 & 6 & 0 & 2 & 4 & 6 \\
3 & 0 & 3 & 6 & 1 & 4 & 7 & 2 & 5 \\
4 & 0 & 4 & 0 & 4 & 0 & 4 & 0 & 4 \\
5 & 0 & 5 & 2 & 7 & 4 & 1 & 6 & 3 \\
6 & 0 & 6 & 4 & 2 & 0 & 6 & 4 & 2 \\
7 & 0 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
\end{array}
\]

Notice that \( 2 \cdot 2 = 4 \) and also that \( 2 \cdot 6 = 4 \). So

\[ 2 \cdot 2 = 2 \cdot 6 \]

Now, in regular integer algebra, if \( 2x = 2y \), we can cancel the 2’s and conclude that \( x = y \). Is that the case here?

The zero factor property

Another property that we expect on the integers (or reals) is the **zero factor** property:

If \( xy = 0 \), then \( x = 0 \) or \( y = 0 \).

This is the property that we’re using whenever we solve equations by factoring - when you solve

\[ x^2 + 3x + 2 = 0 \]

by factoring as

\[ (x + 1)(x + 2) = 0 \]

and concluding \( x = -1 \) or \( x = -2 \), you’re making use of that property.

Now, go look at \( \mathbb{Z}_8 \). Give a pair of numbers whose product is 0, yet both the numbers themselves are nonzero.
**Zero divisor**

Let $R$ be a ring. Suppose that $a$ and $b$ are nonzero elements in $R$ such that either $ab = 0$ or $ba = 0$. The $a$ and $b$ are called zero divisors for the ring.

Recall that we don’t require multiplication to be commutative in rings (that’s why the either/or above).

Example:

- What elements in $\mathbb{Z}_8$ are zero divisors?

- Notice anything about the elements that are not zero divisors?

Example:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

- What elements in $\mathbb{Z}_5$ are zero divisors?

- Any surprises there?
Example:
Does $\mathbb{R}$ (all reals) or its subsets $\mathbb{Z}$ or $\mathbb{Q}$ have any elements which are zero divisors?

Example:
Using trial and error, come up with a couple elements of $M_{2,2}$ which are not themselves the zero matrix, but whose product is the zero matrix. Does it matter in what order you multiply the matrices?

Example:
And, this thing again (the ring $R = \{a, b, c\}$ with operations $+$ and $\ast$ as below):

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

<table>
<thead>
<tr>
<th>$\ast$</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
</tbody>
</table>

What elements (if any) are zero divisors?
Multiplicative inverses

Let $R$ be a ring with unity (unity element denoted 1). Let $x$ and $y$ be members of $R$. If $yx = xy = 1$, then $y$ is called the **multiplicative inverse** of $x$. We denote $y$ by the symbol $x^{-1}$.

**Example:**
Which elements in $\mathbb{Z}_8$ have multiplicative inverses? Give the inverse of each element that has one.

Example:
Which elements in $\mathbb{Z}_5$ have multiplicative inverses? Give the inverse of each element that has one.

Example:
Verify that the matrices $A$ and $B$ are inverses of each other. Be sure to show both orders of the multiplication - matrix multiplication is not in general commutative.

$$A = \begin{bmatrix} 1 & -1 \\ 3 & 5 \end{bmatrix} \quad B = \begin{bmatrix} 0.625 & 0.125 \\ -0.375 & 0.125 \end{bmatrix}$$
Units

An element $x$ in a ring $R$ with unity is called a **unit** if it has a multiplicative inverse.

So, 1, 3, 5, and 7 are units in $\mathbb{Z}_8$. 1, 2, 3, and 4 are units in $\mathbb{Z}_5$.

**Conjecture:**
Make a conjecture about elements in a ring $\mathbb{Z}_m$ that relates units and zero divisors.

**Prove it:**

**Corollary:**
As a corollary to that conjecture, what can you say about $\mathbb{Z}_m$ when $m$ is prime?
Example:
Which elements in $R$ are units?

\[
\begin{array}{ccc}
+ & a & b & c \\
a & c & a & b \\
b & a & b & c \\
c & b & c & a \\
\end{array}
\quad
\begin{array}{ccc}
* & a & b & c \\
a & c & b & a \\
b & b & b & b \\
c & a & b & c \\
\end{array}
\]

Some facts about zero divisors and units in rings

- A ring has at most one unity.
- If an element has a multiplicative inverse, then that inverse is unique.
- In $\mathbb{R}$ and $\mathbb{Q}$, every nonzero element is a unit. There are no zero divisors.
- No element can be both a unit and a zero divisor.
- You can have elements in a ring which are neither, however - every element in $\mathbb{Z}$ other than 1 and $-1$ is neither a unit nor a zero divisor.
- In a ring with no zero divisors, the zero factor property works (if $xy = 0$, then either $x = 0$ or $y = 0$).