Section 18 Rings and Fields

In early childhood you get used to having two algebraic operations, addition and multiplication. A ring is an algebraic object which emulates this.

**Definition** A ring is a set \( R \) with two binary operations, addition and multiplication, satisfying:

1. \( \langle R, + \rangle \) is an abelian group, with add. identity \( 0 \in R \).
2. \((ab)c = a(bc)\)
3. Distributive laws \( \{a(b+c) = ab + ac, (a+b)c = ac + bc\} \)

**Examples:** \( R, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}^n \)

**Ex** \( M_n(R) = m \times n \) matrices \((AB)C = A(BC), A(B+C) = AB + AC\), etc.

**Ex** \( F = \{f : R \rightarrow R\} \)

\((f + g)(x) = f(x) + g(x)\) \( (fg)(x) = f(x)g(x)\).

**Ex** \( \mathbb{Z}_n \)

For instance, consider \( \mathbb{Z}_3 \):

\[
\begin{array}{c|ccc}
+ & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}
\]

\(2(1+2) = 2 \cdot 1 + 2 \cdot 2\)

Actual proof that \( R_2 \) and \( R_3 \) hold for \( \mathbb{Z}_n \) is going to wait until later. Just accept for now that \( \mathbb{Z}_n \) is a ring.

**Theorem:** If \( R \) is a ring, then:

1. \( 0a = 0 = a0 \) \( \forall a \in R \)
2. \( a(-b) = (-a)b = -(ab) \)
3. \( (-a)(-b) = ab \)

\( (a-c)(b) = a(b) - c(b) = ab - cb \)

\( (-a)(-b) = -(a(-b)) = 0(-b) = 0 \)
Theorem

If $R_1, R_2, ..., R_n$ are rings, then so is

$\prod_{i=1}^n R_i = R_1 \times R_2 \times \cdots \times R_n$ under operations:

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1+b_1, a_2+b_2, ..., a_n+b_n)$$

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$$

More examples of rings:

$\mathbb{Z} \times \mathbb{Z}_3, \ \mathbb{Q} \times M_2(\mathbb{R})$

Most, though not all rings will have a multiplicative identity, usually called 1, having property $1 \cdot a = a \cdot 1 = a$. Back to such a ring is a ring with identity.

**Example**

$F$ has mult. identity $f : (R \rightarrow R), f(x) = 1$.

**Example**

$M_n(R)$ has mult. identity $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$

**Example**

$\mathbb{Z}/10$ has no mult. identity.

Multiplicative inverses:

Some elements of a ring with identity will have multiplicative inverses. Such elements are called units of the ring.

**Example**

In $\mathbb{Z}/10$: $1 \cdot 1 = 1, \quad 3 \cdot 7 = 1, \quad 9 \cdot 9 = 1$.

Units of $\mathbb{Z}/10$ are 1, 3, 7, 9.

Elements 0, 2, 4, 5, 6, 8, 9 are not units.

Exercise

Show units of a ring form a multiplicative group.

Units of $\mathbb{Z}/10$: 3, 1, 3, 7, 3

Thus group of units $\cong \mathbb{Z}_4$. 

<table>
<thead>
<tr>
<th>1</th>
<th>3</th>
<th>4</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
Now we add more structure to a ring:

**Def** A division ring is a ring for which every nonzero element is a unit.

**Ex** \( \mathbb{Q}(n, \mathbb{R}), \mathbb{R}, \mathbb{C}, \mathbb{Z}_2 \)

**Def** A field is a commutative division ring.

**Ex** \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2 \) ... we will see other examples.

*Definitions*

If \( R \) and \( S \) are rings, \( \varphi: R \rightarrow S \) is a **homomorphism** if \( \varphi(a+b) = \varphi(a) + \varphi(b) \) and \( \varphi(ab) = \varphi(a)\varphi(b) \), \( \forall a, b \in R \).

If \( \varphi \) is 1-1 and onto homomorphism it is an **isomorphism**.

\[ \text{Ker}(\varphi) = \{ a \in R \mid \varphi(a) = 0 \} \]

A subset \( S \subseteq R \) is a subring of \( R \) if \( S \) is also a ring under \( R \)'s operations. We write \( S \subseteq R \).

**Ex** \( \mathbb{Z} \subseteq \mathbb{R}, \mathbb{Q} \subseteq \mathbb{R}, \mathbb{R} \subseteq \mathbb{C}, \mathbb{Z} \subseteq \mathbb{C} \)

**How to show subset \( S \subseteq R \) is a subring**

1. Show \( S \) is an additive subgroup of \( R \\)
   1. closed under addition.
   2. \( 0 \in S \)
   3. If \( a \in S \) then \( -a \in S \).
2. Show \( S \) is closed under multiplication.

*Do This for* \( \text{Sec 15 #12} \)