1.3 Units in Rings

Definition 1.3.1 Let $R$ be a ring with identity element $1_R$ for multiplication. An element $r \in R$ is called a unit in $R$ if there exists $s \in R$ for which

$$r \times s = 1_R \text{ and } s \times r = 1_R.$$ 

In this case $r$ and $s$ are (multiplicative) inverses of each other.

Example 1.3.2

1. In $\mathbb{Q}$ every element except 0 is a unit; the inverse of a non-zero rational number is its reciprocal.

2. In $\mathbb{Z}$ the only units are 1 and $-1$; no other integer can be multiplied by an integer to give 1.

3. In $M_2(\mathbb{R})$, the units are the $2 \times 2$ matrices with non-zero determinant, and the identity element is \[
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}.
\]

4. In $\mathbb{Z}/6\mathbb{Z}$ the only units are 1 and 5; each of these is its own inverse.

We will denote the set of units in a ring $R$ with identity by $U(R)$.

Remarks

1. If $R$ has two or more elements then it follows from Lemma 1.2.2 that $0 \neq 1_R$.

2. If $R$ has two or more elements then $0_R$ cannot be a unit in $R$, again by Lemma 1.2.2.

3. It is possible for a ring to have only one element; for example the subset of $\mathbb{Z}$ containing only 0 is a ring.

4. $1_R$ is always a unit in $R$ since it is its own inverse.

Theorem 1.3.3 Let $R$ be a ring with identity element $1_R$. Then $U(R)$ is a group under the multiplication of $R$. ($U(R)$ is called the unit group of $R$).

Note: The statement that $U(R)$ is a group under multiplication means that:

- $U(R)$ is closed under multiplication - whenever elements $a$ and $b$ belong to $U(R)$, so does their product $ab$.

- $U(R)$ contains an identity element for multiplication.

- $U(R)$ contains a multiplicative inverse for each of its elements.

Proof: We need to show

1. $U(R)$ is closed under the multiplication of $R$; i.e. that $rs$ is a unit in $R$ whenever $r$ and $s$ are units in $R$. So assume that $r$ and $s$ belong to $U(R)$ and let $r^{-1}$ and $s^{-1}$ denote their respective inverses in $R$. Then

\[
(rs)(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1_Rr^{-1} = rr^{-1} = 1_R.
\]

Similarly $(s^{-1}r^{-1})(rs) = 1_R$ and so $s^{-1}r^{-1}$ is an inverse in $R$ for $rs$, and $rs \in U(R)$. 

4
2. \( \mathcal{U}(R) \) contains an identity element for multiplication. This is true since \( 1_R \in \mathcal{U}(R) \).

3. \( \mathcal{U}(R) \) contains an inverse for each of its elements.

   To see this, suppose \( r \in \mathcal{U}(R) \), and let \( r^{-1} \) be the inverse of \( r \) in \( R \). Then \( r^{-1}r = 1_R \) and \( rr^{-1} = 1_R \), so \( r \) is the inverse of \( r^{-1} \), and \( r^{-1} \) is in \( \mathcal{U}(R) \).

This proves the theorem. \( \square \)

Examples

1. \( \mathcal{U}(\mathbb{Z}) = \{-1, 1\} \) is a cyclic group of order 2.

2. The unit group of the matrix ring \( M_n(\mathbb{R}) \) is the general linear group \( \text{GL}(n, \mathbb{R}) \) of \( n \times n \) invertible matrices over \( \mathbb{R} \).

3. The unit group of \( \mathbb{Q} \) is denoted \( \mathbb{Q}^\times \) and consists of all non-zero rational numbers.

Definition 1.3.4 A ring with identity is called a field if it is commutative and every non-zero element is a unit (so we can divide by every non-zero element).

Examples of fields include \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \) and \( \mathbb{Z}/5\mathbb{Z} \) (check).

A ring with identity in which every non-zero element is a unit is called a division ring. Commutative division rings are fields. Examples of non-commutative division rings are not so easy to find, but we will see at least one later in the course.