1.3 Lecture 3: Units in Rings

As we have already mentioned, the axioms of a ring are not very restrictive concerning how the operation of multiplication should behave - all we ask is that it should be associative and have an identity. The existence of an identity element means that we can consider whether something like *division* is possible in the ring; we can try to identify pairs of elements that are related to each other in the way that a rational number is related to its reciprocal or in the way that a non-singular matrix is related to its inverse.

Definition 3. *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.*

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 2×2 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 $\bar{1}$ and $\bar{5}$; each of these is its own inverse.
   Question What is special about 1 and 5 in relation to 6, among the elements of $\mathbb{Z}/6\mathbb{Z}$?
5. What are the units in $M_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries?

NOTATION: We will denote the set of units in a ring R by $\mathcal{U}(R)$.

REMARKS

1. If R is a ring having two or more elements then it follows from Theorem 2 that the zero element of R and the multiplicative identity in R cannot be the same element (Exercise: write out the details!).
2. If R has two or more elements then 0_R cannot be a unit in R, again by Theorem 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. (This is called the zero ring and as an example of a ring it is not very instructive).
4. 1_R is always a unit in R since it is its own inverse.

The next theorem is about a special property of the subset of a ring consisting of the units. For any (non-zero) ring R, $\mathcal{U}(R)$ is a subset of R that includes the (multiplicative) identity element but not the zero element. Is $\mathcal{U}(R)$ just a set, or does it have algebraic structure of its own? The full ring R has addition and multiplication defined on it. If we take two units of R we can add them in R; will the result be a unit? If we take two units of R and multiply them (in R), will the result be a unit? If the answer to this second question is yes, then the set of units of R is itself an algebraic structure with respect to the multiplication of R, and we can study its properties.

Algebraists are always on the lookout for substructures of the objects that they are studying, which are themselves algebraic structures with respect to the operation(s) of the larger object. The general thinking behind this practice is that small structures should be easier to understand than bigger ones, and that we have some chance of understanding (at least partially) a large complicated algebraic structure if we can identify smaller parts of it that are themselves algebraic structures.

Theorem 4. *Let* R *be a ring with identity element* 1_R*. Then* $U(R)$ *is a group under the multiplication of* R*.*

Note: $U(R)$ is called the *unit group* of R.

Proof of Theorem ??: 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

$$\begin{aligned}(rs)(s^{-1}r^{-1}) &= r(ss^{-1})r^{-1} \\ &= r1_R r^{-1} \\ &= rr^{-1} \\ &= 1_R.\end{aligned}$$

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

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

3. $U(R)$ contains an inverse for each of its elements.
   To see this, suppose $r \in U(R)$, 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 $U(R)$.

This proves the theorem. □

EXAMPLES

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

2. The unit group of the matrix ring $M_n(\mathbb{R})$ is the *general linear group* $GL(n, \mathbb{R})$ 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.

Question: In general, can anything be said about the behaviour of $U(R)$ with respect to addition in R?

Suppose that R is a ring with identity. Then we know that the unit group of R cannot include the zero element of R, but any non-zero element of R could potentially be a unit. A particularly nice thing to happen is for *every* non-zero element of R to be a unit. Rings in which this occurs are worthy of special study.

Definition 5. *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), but not $\mathbb{Z}/6\mathbb{Z}$.

A ring with identity in which every non-zero element is a unit is called a *division ring*. Commutative division rings are fields. Non-commutative division rings are not a bit more exotic, but we will meet one a bit later.