7

FIELDS, RINGS, AND HOMOMORPHISMS:
ILLUSTRATIONS FROM THE
FIBONACCI SEQUENCE

7.1 Fields

It becomes necessary to explain the technical term ‘field’ in order to be able to use it with precision. A field is a structure consisting of a set whose elements are related by two binary operations (i.e. rules of combination) as opposed to a group whose elements are related by one only. The elements are closed under both operations, usually addition and multiplication, and each operation has the commutative and associative properties. In symbols:

\[
\begin{align*}
  a+b &= b+a \\
  ab &= ba \\
  (a+b)+c &= a+(b+c) \\
  (ab)c &= a(bc).
\end{align*}
\]

Also the two operations are connected by the distributive property for multiplication over addition:

\[
a(b+c) = ab + ac.
\]

There are two distinct identity elements, one for each operation, 0 for addition, 1 for multiplication:

\[
a+0 = 0 \text{ and } a \times 1 = 1.
\]

Each element has an inverse element \(a'\) (the negative of \(a\)) for addition, and each non-zero element has an inverse \(a^{-1}\) (the reciprocal of \(a\)) for multiplication:

\[
a + a' = 0 \text{ and } aa^{-1} = 1.
\]

The system has no zero divisors (see section 1.15).

If \(ab = 0\), then \(a = 0\), or \(b = 0\).

The last two properties mentioned (existence of a reciprocal and no zero divisors) are the distinguishing marks of a field when comparing it with other less well-behaved systems. The integers, for instance, do not possess reciprocals: the inverse of 3 according to the definition is 1/3 but then 1/3 is not an integer. The residues to a composite modulus do not all possess reciprocals and there are zero divisors among them.
The most familiar example of a field is the set of rational numbers \( p/q \) where \( p \) and \( q \) are integers and \( q \neq 0 \).

Other examples of fields are the set of real numbers, the set of numbers \( a+b\sqrt{2} \) when \( a \) and \( b \) are rational numbers (\( a \) and \( b \) not both zero), and the set of residues to a prime modulus. Let us consider the residues modulo 5. All the usual rules for integers hold and in addition each non-zero element has a multiplicative inverse. The elements 2 and 3 are mutually inverse and the elements 1 and 4 are self-inverse. The usual symbol for this field is \( Z_5 \).

Another way of summing up the properties of a field is to say that the elements form a commutative group for addition and that the non-zero elements form another commutative group for multiplication, the two operations being linked together by the distributive property.

## 7.2 Rings

Now that we have defined a field it is profitable to contrast and compare it with a ring, which is another structure possessing two rules of combination. A ring resembles a field in that its elements form a commutative group for addition and it has the distributive property, but it may fail to qualify as a field for some or all of four reasons, all to do with multiplication:

1. Some of its elements may not possess a multiplicative inverse. This is the only reason for the integers not being classed as a field.

2. It may have zero divisors (see section 1.15). The set of residue classes to a composite modulus fails to qualify for this reason as well as for having elements with no multiplicative inverse.

3. The ring may not have a unity element. The even integers are an example.

4. It need not be commutative for multiplication. Matrices give us examples of non-commutative rings.

A field may be regarded as a particular example of a ring since it has all the properties required of a ring and some extra ones besides.

Let us now examine in some detail the ring \( Z_{10} \) of residue classes modulo 10. We already know that its elements form a commutative group for addition. Both \( \{0, 5\} \) and \( \{0, 2, 4, 6, 8\} \) are normal subgroups and it is instructive to set out both addition and multiplication tables of \( Z_{10} \) in an order based on \( \{0, 5\} \). It will be seen that this subgroup and its cosets are also components of the multiplication table 7.2.