§5  THE FIELD OF QUOTIENTS

3. Which of \( \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \) and \( \mathbb{Z}_6 \) are fields, and why?
4. Show that any finite integral domain is a field.
5. Show that every subring of a field is an integral domain.
6. Show that a subset of a finite field is a subfield if and only if it is closed under addition and multiplication and contains more than one element.
7. Show that any morphism \( \alpha : F \to F' \) of fields is a morphism of quotients, in the sense that \( b \neq 0 \) and \( a \) in \( F \) give \( \alpha(a/b) = (aa)/(ab) \) in \( F' \).
8. Assume that \( \mathbb{Q} \subset \mathbb{R} \) are fields:
   (a) Prove for \( d = 7 \) or \( 11 \) that the set \( \mathbb{Q}(\sqrt{d}) \) of all real numbers \( a + b\sqrt{d} \) for \( a, b \in \mathbb{Q} \) is a field.
   (b) Show that the function \( a + b\sqrt{7} \mapsto a + b\sqrt{11} \) is not an isomorphism \( \mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}(\sqrt{11}) \).
   *(c) Prove that there is no isomorphism \( \mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}(\sqrt{11}) \) of fields.

5. The Field of Quotients

The integral domain \( \mathbb{Z} \) is not itself a field, but it is contained in the familiar field \( \mathbb{Q} \) of all rational numbers. Now each rational number \( x = m/n \), for \( m, n \in \mathbb{Z} \) and \( n \neq 0 \), may be described as the solution \( x \) in \( \mathbb{Q} \) of the equation \( nx = m \) with coefficients \( m \) and \( n \) in \( \mathbb{Z} \). This suggests that the field \( \mathbb{Q} \) might be formally constructed from \( \mathbb{Z} \) as the set of all solutions \( m/n \) to such equations. The field \( \mathbb{Q} \) so constructed will turn out to be the "smallest" field containing \( \mathbb{Z} \).

This construction of a field of quotients applies not just to the domain \( \mathbb{Z} \) of integers, but to any integral domain \( D \); it will embed that domain \( D \) in a field \( \mathbb{Q}(D) \), the field of quotients of \( D \), which may be described as follows.

**Theorem 12.** For each integral domain \( D \) there is a field \( \mathbb{Q}(D) \) and a monomorphism \( j : D \to \mathbb{Q}(D) \) of rings such that every element \( x \in \mathbb{Q}(D) \) is a quotient \( (ja)/(jb) \), where \( a \) and \( b \neq 0 \) are elements of \( D \). Moreover, any monomorphism \( \alpha : D \to F \) on \( D \) to a field can be written as a composite \( \alpha = \alpha' \circ j \) for a unique morphism \( \alpha' : \mathbb{Q}(D) \to F \) of fields.

**Proof:** Since the elements of the field \( \mathbb{Q}(D) \) are to be quotients \( a/b \) of elements \( a \) and \( b \neq 0 \) of \( D \), we start with all such pairs \( (a, b) \), introduce for them an equality like the equality of quotients \( a/b \), and define for them operations of addition and multiplication by the formulas (20) and (21) used for sums and products of actual quotients.

In detail, let \( D^* \) be the set of all non-zero elements of \( D \). In the product set \( D \times D^* \) define a relation of congruence by

\[
(a, b) \equiv (a', b') \iff ab' = a'b. \tag{24}
\]