Lecture 6: The Field of Quotients of an Integral Domain

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Ring Embeddings

Definition

A ring R is said to be **embedded** in a ring S if there exists a monomorphism of R into S.

From this definition, any ring R can be embedded in a ring S if there exist a subring of S which is isomorphic to R, i.e., $R \simeq f(R) < S$.

Theorem

Any ring R can be embedded in a ring S with identity such that R is an ideal of S.

The Field of Quotients of an Integral Domain

Motivated by the construction of $\mathbb{Q}$ from $\mathbb{Z}$, here we show that any integral domain D can be embedded in a field F. In particular, every element of F can be written as a quotient of elements of D. The field F will be called as a **field of quotients (field of fractions)** of an integral domain D.

Theorem

Any integral domain D can be embedded in a field F.

Proof: The proof strategy can be given in the following 4 steps:

1. Determine the elements of F by using elements of D.
2. Define the binary operations $+$ and $.$ on F.
3. Check the field axioms for $(F, +, .)$
4. Show that D can be embedded in F.

(1) Let D be an integral domain.

- Then
$$D \times D = \{(a, b) \mid a, b \in D\}.$$
- Consider the subset
$$S = D \times D^{*} = \{(a, b) \mid a, b \in D, b \neq 0\}.$$
- For $(a, b), (c, d) \in S$,
$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$
- The equivalence class $a/b := \overline{(a, b)} = \{(c, d) \mid (c, d) \sim (a, b)\}$.
$$F = \{a/b \mid (a, b) \in S\}.$$

(2) For $a/b, c/d \in F$,

$$\begin{aligned} a/b + c/d \; &: = (ad + bc)/bd \\ a/b.c/d \; &: = ac/bd \end{aligned}$$

are well-defined.

(3) Now we show that $(F, +, .)$ is a field by the axioms of D.

F_1) $(F, +)$ is a commutative group.

- $+$ is commutative and associative in F.
- $0/b \in F$ is the additive identity element.
- The inverse of $a/b \in F$ is $(-a)/b \in F$.

F_2) $(F^*, .)$ is a commutative group.

- . is commutative and associative in F.
- $b/b \in F$ is the multiplicative identity element.
- The inverse of $0/b \neq a/b \in F$ is $b/a \in F$. That is, $(a/b).(b/a) = ab/ba = b/b$.

F_3) . is distributive over $+$ in F.

The Field of Quotients of an Integral Domain

(4) Finally we show that D can be embedded in a field F.
The function $f : D \to F$ given by $f(a) = a/1_D$ for $a \in D$ is one-to-one homomorphism. That is,

$$(i)\, f(a+b) = (a+b)/1_D = a/1_D + b/1_D = f(a) + f(b)$$

$$(ii)\, f(ab) = (ab)/1_D = (a/1_D)(b/1_D) = f(n)\, f(m),$$

and $f(a) = f(b) \Rightarrow a/1_D = b/1_D$, so $(a, 1_D) \sim (b, 1_D)$ implies $a1_D = b1_D$, thus $a = b$.
It is clear that $f(D)$ is a subring of F. Thus, $f : D \to f(D) < F$ is an isomorphism; that is, $D \simeq f(D)$.

Remarks:

- The field $(F, +, .)$ is called **the field of quotients of** D if there exists a subring D' of F such that $D \simeq D' < F$. Also every element of F can be expressed as a quotients of two elements of D, since

$$a/b = (a/1_D)(1_D/b) = (a/1_D)(b/1_D)^{-1}.$$

($\mathbb{Q}$ is a field of quotients of $\mathbb{Z}$.)

- Every field containing an integral domain D contains a field of quotients of D.
- The field of quotients of D is the smallest field containing D. That is, no field K such that $D \subset K \subset F$.
  ($\mathbb{Q}$ is a field of quotients of $\mathbb{Z}$, $\mathbb{R}$ is not a field of quotients of $\mathbb{Z}$.)

- Any field of quotients of a **field** F is isomorphic to F.
  ($\mathbb{R}$ is a field of quotients of $\mathbb{R}$.)
- Any two fields of quotients of D are isomorphic. Isomorphic integral domains have isomorphic field of quotients.

Example: Find the field of quotients of $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.
The field of quotients of $\mathbb{Z}[i]$ is

$$\{c + id \mid c, d \in \mathbb{Q}\}.$$

Example: Find the field of quotients of $\mathbb{Z}_5$.

$$S = \mathbb{Z}_5 \times \mathbb{Z}_5^* = \left\{ \left(\bar{0}, \bar{1}\right), \left(\bar{0}, \bar{2}\right), \left(\bar{0}, \bar{3}\right), \left(\bar{0}, \bar{4}\right), \left(\bar{1}, \bar{1}\right), \ldots, \left(\bar{4}, \bar{4}\right) \right\}.$$

$$\begin{aligned} \bar{0}/\bar{1} &= \left\{ \left(\bar{c}, \bar{d}\right) \mid \left(\bar{c}, \bar{d}\right) \sim \left(\bar{0}, \bar{1}\right) \right\} \\ &= \left\{ \left(\bar{c}, \bar{d}\right) \mid \bar{c}\bar{1} = \bar{d}\bar{0} \right\} \\ &= \left\{ \left(\bar{0}, \bar{1}\right), \left(\bar{0}, \bar{2}\right), \left(\bar{0}, \bar{3}\right), \left(\bar{0}, \bar{4}\right) \right\} \end{aligned}$$

$$\begin{aligned} \bar{1}/\bar{1} &= \left\{ \left(\bar{1}, \bar{1}\right), \left(\bar{2}, \bar{2}\right), \left(\bar{3}, \bar{3}\right), \left(\bar{4}, \bar{4}\right) \right\} \\ \bar{1}/\bar{2} &= \left\{ \left(\bar{1}, \bar{2}\right), \left(\bar{2}, \bar{4}\right), \left(\bar{3}, \bar{1}\right), \left(\bar{4}, \bar{3}\right) \right\} = \bar{3}/\bar{1} \\ \bar{1}/\bar{3} &= \left\{ \left(\bar{1}, \bar{3}\right), \left(\bar{2}, \bar{1}\right), \left(\bar{3}, \bar{4}\right), \left(\bar{4}, \bar{2}\right) \right\} = \bar{2}/\bar{1} \\ \bar{1}/\bar{4} &= \left\{ \left(\bar{1}, \bar{4}\right), \left(\bar{2}, \bar{3}\right), \left(\bar{3}, \bar{2}\right), \left(\bar{4}, \bar{1}\right) \right\} = \bar{4}/\bar{1} \end{aligned}$$

Hence $F = \left\{ \bar{0}/\bar{1}, \bar{1}/\bar{1}, \bar{2}/\bar{1}, \bar{3}/\bar{1}, \bar{4}/\bar{1} \right\}$. It is obvious that $\begin{aligned} f : \mathbb{Z}_5 &\longrightarrow F \\ \bar{a} &\longrightarrow \bar{a}/\bar{1} \end{aligned}$ is an isomorphism.