

§31 Field of Fractions of an Integral Domain

Let D be an integral domain, i.e., a commutative ring with identity which has no zero divisors, distinct from the null ring. Let a, b, c be elements of D such that

$$a \neq 0, \quad ab = ac. \quad (\text{i})$$

If a has a multiplicative inverse a^{-1} in D , we could multiply both sides of this equation by a^{-1} and obtain

$$b = c. \quad (\text{ii})$$

But we do not know whether a has an inverse in D and we cannot argue in this way. Nevertheless, it is true that (i) implies (ii) in an integral domain: from (i), we get

$$ab - ac = 0$$

$$a(b - c) = 0,$$

and, since $a \neq 0$ and D has no zero divisors,

$$b - c = 0$$

$$b = c.$$

Hence the cancellation law holds in an integral domain D just as if the nonzero elements in D had inverses in D , i.e., as if $D \setminus \{0\}$ were a group under multiplication.

It is the objective of this paragraph to show that any integral domain is in fact a subring of a ring F such that $F \setminus \{0\}$ is a commutative multiplicative group, i.e., a subring of a *field* F . We can then say that the nonzero elements in D do have inverses, perhaps not in D , but certainly in F .

First we show that finite integral domains are always fields.

31.1 Theorem: *If an integral domain has finitely many elements, then it is a field.*

Proof: (cf. Lemma 9.3) Let D be an integral domain with finitely many elements. We are to show that every nonzero element of D has a multiplicative inverse in D .

Let $a \in D$, $a \neq 0$. Since $|D|$ is finite, the elements

$$a, a^2, a^3, \dots, a^n, \dots$$

of D cannot be all distinct. So there are natural numbers $k, l \in \mathbb{N}$ such that $a^k = a^l$, with $k < l$, say. We obtain then

$$\begin{aligned} a^k - a^l &= 0 \\ a^k - a^k a^{l-k} &= 0 \\ a^k(1 - a^{l-k}) &= 0, \end{aligned}$$

where 1 is the identity of D . Since D has no zero divisors and $a \neq 0$, we conclude $a^k = a \cdot a \cdot \dots \cdot a \neq 0$, which yields

$$\begin{aligned} 1 - a^{l-k} &= 0 \\ a^{l-k} &= 1, \\ a \cdot a^{l-k-1} &= 1. \end{aligned}$$

Thus $a^{l-k-1} \in D$ is an inverse of a . So D is a field. \square

Starting from an integral domain D , we now construct, without any hypothesis on $|D|$, a field F which contains D as a subring. This construction is an immediate generalization of the construction of \mathbb{Q} from \mathbb{Z} , whose basic moments we recollect: every rational number is a fraction $\frac{a}{b}$ of integers a, b , with $b \neq 0$; different fractions can represent the same

rational number, in fact $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$ (where $a, b, c, d \in \mathbb{Z}$

and $b \neq 0 \neq d$); the addition of two rational numbers $\frac{a}{b}, \frac{c}{d}$ is carried out

by writing them with a common denominator and adding the numerators $(\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd})$; the multiplication is carried

out by multiplying the numerators and denominators separately $(\frac{a}{b} \cdot \frac{c}{d} =$

$\frac{ac}{bd})$; an integer a is considered to be equal to the rational number $\frac{a}{1}$.

All these carry over to the more general case of an arbitrary integral domain D in place of \mathbb{Z} , and give rise to a field F which is related to D in the same way as \mathbb{Q} is related to \mathbb{Z} . The elements of F will be like "fractions" of elements of D . We introduce them in the next two lemmas.

31.2 Lemma: Let D be an integral domain and put

$$S := \{(a,b): a,b \in D, b \neq 0\} = D \times (D \setminus \{0\}).$$

We define a relation \sim on S by declaring

$$(a,b) \sim (c,d) \text{ if and only if } ad = bc$$

for all $(a,b), (c,d) \in S$. Then \sim is an equivalence relation on S .

Proof: (i) For all $(a,b) \in S$, we have $(a,b) \sim (a,b)$ since $ab = ba$. So \sim is reflexive.

(ii) If $(a,b), (c,d) \in S$ and $(a,b) \sim (c,d)$, then

$$ad = bc$$

$$da = cb$$

$$cb = da$$

$$(c,d) \sim (a,b)$$

and \sim is symmetric.

(iii) If $(a,b), (c,d), (e,f) \in S$ and $(a,b) \sim (c,d), (c,d) \sim (e,f)$, then

$$ad = bc \text{ and } cf = de$$

$$adf = bcf \text{ and } bcf = bde$$

$$daf = dbe$$

$$d(af - be) = 0.$$

From $(c,d) \in S$, we know $d \neq 0$, and, since D has no zero divisors, we obtain $af - be = 0$. Thus $af = be$, so $(a,b) \sim (e,f)$ and \sim is transitive.

So \sim is an equivalence relation on S . □

31.3 Lemma: Let D be an integral domain, $S = D \times (D \setminus \{0\})$, and let \sim be the equivalence relation of Lemma 31.2. For $(a,b) \in S$, we designate the equivalence class of (a,b) by $[a:b]$. Thus $[a:b] = \{(c,d) \in S: (c,d) \sim (a,b)\}$.

Let $F = \{[a:b]: (a,b) \in S\}$ be the set of all equivalence classes of the elements in S . For all $[a:b], [c:d] \in F$, we put

$$[a:b] + [c:d] = [ad + bc : bd],$$

$$[a:b] \cdot [c:d] = [ac : bd].$$

Then $+$ and \cdot are well defined operations on F .

Proof: First we remark that, if $(a,b), (c,d) \in S$, then $b,d \neq 0$, and so $bd \neq 0$ since D has no zero divisors. Thus $(ad + bc, bd), (ac, bd) \in S$ and therefore $[ad + bc:bd], [ac:bd] \in F$.

We must show that $+$ and \cdot are well defined operations on F . This means we must show that the implication

$$[a:b] = [x:y], [c:d] = [z:u] \implies [ad + bc:bd] = [xu + yz:yu], [ac:bd] = [xz:yu]$$

is valid. This implication is equivalent to

$$(a,b) \sim (x,y), (c,d) \sim (z,u) \implies (ad + bc, bd) \sim (xu + yz, yu), (ac, bd) \sim (xz, yu)$$

which, in turn, is equivalent to

$$ay = bx, cu = dz \implies (ad + bc)yu = bd(xu + yz), ac \cdot yu = bd \cdot xz,$$

where $b, d, y, u \neq 0$. But certainly, when $ay = bx, cu = dz$, we have

$$(ad + bc)yu = adyu + bcyu = ay \cdot du + by \cdot cu = bx \cdot du + by \cdot cu = bx \cdot du + by \cdot dz \\ = bd \cdot xu + bd \cdot yz = bd(xu + yz) \text{ and } ac \cdot yu = ay \cdot cu = bx \cdot dz = bd \cdot xz. \quad \square$$

31.4 Theorem: *With the notation of Lemma 31.3, $(F, +, \cdot)$ is a field.*

Proof: (i) According to Lemma 31.3, $+$ is a binary operation on F .

(ii) $+$ is associative since for any $[a:b], [c:d], [e:f] \in F$, we have

$$\begin{aligned} ([a:b] + [c:d]) + [e:f] &= [ad + bc:bd] + [e:f] \\ &= [(ad + bc)f + (bd)e : (bd)f] \\ &= [a(df) + b(cf + de) : b(df)] \\ &= [a:b] + [cf + de:df] \\ &= [a:b] + ([c:d] + [e:f]). \end{aligned}$$

(iii) $[0:1]$ is a right additive identity since $[a:b] + [0:1] = [a1 + b0 : b1] = [a:b]$ for any $[a:b] \in F$. (Notice that $[0:1] = [0:d]$ for all $d \in D, d \neq 0$.)

(iv) Any $[a:b] \in F$ has a right additive inverse: $[-a:b]$ is the opposite of $[a:b]$, for $[a:b] + [-a:b] = [ab + b(-a) : b^2] = [0:b^2] = [0:1]$.

(v) $+$ is commutative since for any $[a:b], [c:d] \in F$, we have

$$[a:b] + [c:d] = [ad + bc:bd] = [cb + da:db] = [c:d] + [a:b].$$

We proved that $(F, +)$ is a commutative group. We now check the remaining ring axioms.

(1) According to Lemma 31.3, \cdot is a binary operation on F .

(2) \cdot is associative since for any $[a:b], [c:d], [e:f] \in F$, we have

$$\begin{aligned} ([a:b] \cdot [c:d]) \cdot [e:f] &= [ac:bd] \cdot [e:f] \\ &= [(ac)e : (bd)f] \\ &= [a(ce) : b(df)] \\ &= [a:b] \cdot [ce:df] \\ &= [a:b] \cdot ([c:d] \cdot [e:f]). \end{aligned}$$

(D) For all $[a:b], [c:d], [e:f] \in F$, we have

$$\begin{aligned} [a:b] \cdot ([c:d] + [e:f]) &= [a:b] \cdot [cf + de:df] \\ &= [a(cf + de) : b(df)] \\ &= [acf + ade : bdf] \\ &= [bacf + bade : bddf] && \text{(why?)} \\ &= [ac \cdot bf + bd \cdot ae : bd \cdot bf] \\ &= [ac:bd] + [ae:bf] \\ &= [a:b] \cdot [c:d] + [a:b] \cdot [e:f] \end{aligned}$$

and one of the distributivity laws hold in F . We must prove the other distributivity law. We can give an argument similar to the above, but we show presently that \cdot is commutative, and this will give the other distributivity law as a bonus.

We have *not* yet proved that $(F, +, \cdot)$ is a ring.

(3) \cdot is commutative since for any $[a:b], [c:d] \in F$, we have

$$[a:b] \cdot [c:d] = [ac:bd] = [ca:db] = [c:d] \cdot [a:b].$$

As we have already remarked above, this yields the distributivity law we have not checked:

$$\begin{aligned} ([c:d] + [e:f]) \cdot [a:b] &= [a:b] \cdot ([c:d] + [e:f]) \\ &= [a:b] \cdot [c:d] + [a:b] \cdot [e:f] \\ &= [c:d] \cdot [a:b] + [e:f] \cdot [a:b] \end{aligned}$$

for all $[a:b], [c:d], [e:f] \in F$.

We now proved that $(F, +, \cdot)$ is a commutative ring.

(4) $[1:1]$ is the multiplicative identity because

$$[a:b] \cdot [1:1] = [a1:b1] = [a:b]$$

for all $[a:b] \in F$. Since multiplication is commutative, there holds also $[1:1] \cdot [a:b] = [a:b]$ for any $[a:b] \in F$. (Notice that $[1:1] = [d:d]$ for all $d \in D$ with $d \neq 0$.)

Thus $(F, +, \cdot)$ is a commutative ring with identity. It remains to show that every nonzero element in F has a multiplicative inverse in F .

(5) For all $[a:b] \in F \setminus \{0\}$, we show that $[b:a]$ is a multiplicative inverse of $[a:b]$. First of all, since $[a:b] \neq [0:1]$ in F ,

(a,b) is not equivalent to $(0,1)$ in S

$$a1 \neq b0$$

$$a \neq 0$$

$$(b,a) \in S$$

and $[b:a]$ is an element of F . Secondly, $[a:b] \cdot [b:a] = [ab:ba] = [ab:ab] = [1:1]$ = multiplicative identity of F . Thus $[b:a]$ is a multiplicative inverse of $[a:b] \neq [0:1]$ in F .

This proves that $(F, +, \cdot)$ is a field. □

31.5 Theorem: Let D be an integral domain and let $(F, +, \cdot)$ be the field of Theorem 31.4. Then D is isomorphic to a subring of F .

Proof: Let $\varphi: D \rightarrow F$. We demonstrate that φ is a one-to-one ring homomorphism. For all $a, b \in D$,

$$a\varphi + b\varphi = [a:1] + [b:1] = [a1 + 1b:1 \cdot 1] = [a + b:1] = (a + b)\varphi$$

$$a\varphi \cdot b\varphi = [a:1] \cdot [b:1] = [ab:1 \cdot 1] = [ab:1] = (ab)\varphi,$$

thus φ is a homomorphism. Also

$$\begin{aligned} \text{Ker } \varphi &= \{a \in D: a\varphi = \text{zero element of } F\} \\ &= \{a \in D: [a:1] = [0:1]\} \\ &= \{a \in D: (a,1) \sim (0,1)\} \\ &= \{a \in D: a \cdot 1 = 1 \cdot 0\} \\ &= \{a \in D: a = 0\} \\ &= \{0\} \end{aligned}$$

and hence φ is one-to-one. By Theorem 30.18, D is isomorphic to the subring $\text{Im } \varphi = D\varphi = \{[a:1] \in F: a \in D\}$ of F . □

31.6 Definition: Let D be an integral domain. Then the field of Theorem 31.4 is called the *field of fractions* or the *field of quotients* of D .

From now on, we shall write $\frac{a}{b}$ for $[a:b]$. The elements of F will be called *fractions* (of elements from D). Furthermore, we identify the integral domain D with its image $D\varphi$ under the mapping in Theorem 31.5. Thus we write a instead of $\frac{a}{1}$ and regard D as a subring of F . Then the inverse of $b \in D \subseteq F$ is $\frac{1}{b} \in F$ and that of $\frac{a}{b}$ is $\frac{b}{a}$ (here $a, b \in D, a, b \neq 0$). With these notations, calculations are carried out in the usual way.

Starting from an integral domain D , we constructed the field F of fractions of D . Now this field F is also an integral domain, too, and we may repeat our construction and obtain the field of fractions of F , say F_1 . However, nothing is gained by this repetition, for F_1 is not essentially distinct from F .

31.7 Theorem: *Let K be a field and let K_1 be the field of fractions of K . Then K_1 is isomorphic to K .*

Proof: From Theorem 31.6, we know that $\varphi: K \rightarrow K_1$ is an isomorphism

$$a \rightarrow \frac{a}{1}$$

from K onto $K\varphi = \text{Im } \varphi$. We will show that $\text{Im } \varphi = K_1$.

Any element of K_1 can be written as $\frac{a}{b}$, where $a, b \in K$ and $b \neq 0$. Since K is a field and $b \neq 0$, there is an inverse $b^{-1} \in K$ of b in K . Thus $ab^{-1} \in K$ and

$$\frac{a}{b} = [a:b] = [ab^{-1}:1] = \frac{ab^{-1}}{1} = (ab^{-1})\varphi \in \text{Im } \varphi.$$

This proves $K_1 \subseteq \text{Im } \varphi$, so $\text{Im } \varphi = K_1$ and K_1 is isomorphic to K . □

Next we show that the field of fractions of an integral domain is the smallest field containing that integral domain.

31.8 Theorem: *Let D be an integral domain and F the field of fractions of D . If K is any field that contains D , then K contains a subring isomorphic to F .*

Proof: We construct an isomorphism from F onto a subring of K . The elements of F are fractions $\frac{a}{b}$, where $a, b \in D$ and $b \neq 0$. Regarded as an element of K , b has an inverse b^{-1} in K , so $ab^{-1} \in K$. Let $\psi: F \rightarrow K$.

$$\frac{a}{b} \rightarrow ab^{-1}$$

ψ is a well defined mapping, for if $\frac{a}{b} = \frac{c}{d}$ ($a, b, c, d \in D, b \neq 0 \neq d$), then $ad = bc$, so $ad \cdot b^{-1}d^{-1} = bc \cdot b^{-1}d^{-1}$, so $ab^{-1} = cd^{-1}$, so $(\frac{a}{b})\psi = (\frac{c}{d})\psi$. Now

$$\begin{aligned} (\frac{a}{b} + \frac{c}{d})\psi &= (\frac{ad+bc}{bd})\psi = (ad+bc)(bd)^{-1} \\ &= (ad+bc)d^{-1}b^{-1} = ab^{-1} + cd^{-1} = (\frac{a}{b})\psi + (\frac{c}{d})\psi \end{aligned}$$

$$\text{and } (\frac{a}{b} \cdot \frac{c}{d})\psi = (\frac{ac}{bd})\psi = (ac)(bd)^{-1} = ac \cdot d^{-1}b^{-1} = ab^{-1} \cdot cd^{-1} = (\frac{a}{b})\psi \cdot (\frac{c}{d})\psi$$

for any two fractions $\frac{a}{b}, \frac{c}{d}$ in F and ψ is a ring homomorphism. Here ψ is one-to-one because $\text{Ker } \psi = \{0\}$, for $\frac{a}{b} \in \text{Ker } \psi$ implies $(\frac{a}{b})\psi = 0$, so $ab^{-1} = 0$, so $a = abb^{-1} = 0b^{-1} = 0$, so $\frac{a}{b} = \frac{0}{b} = \frac{0}{1} = 0$. Hence F is isomorphic to the subring $\text{Im } \psi$ of K (Theorem 30.18). \square

Exercises

1. Let $D_1 = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, $D_2 = \{a + 2bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ and $E = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{R} : a, b, c \in \mathbb{Z}\}$. Show that D_1, D_2, E are integral domains and describe, as simply as you can, the elements in the field of fractions of these integral domains.

2. Let R be a commutative ring and let M be a nonempty multiplicatively closed subset of R . For ordered pairs in $R \times M$, we put

$$(r, m) \sim (r', m') \quad \text{if and only if} \quad \text{there is an } n \in M \text{ such that } n(rm' - r'm)$$

Show that \sim is an equivalence relation on $R \times M$. Denote the equivalence class of (r, m) by $\frac{r}{m}$ and define, on the set $M^{-1}R$ of all equivalence classes, addition and multiplication by

$$\frac{r}{m} + \frac{r'}{m'} = \frac{rm' + mr'}{mm'} \quad \text{and} \quad \frac{r}{m} \cdot \frac{r'}{m'} = \frac{rr'}{mm'}$$

Prove that $M^{-1}R$ is a commutative ring with identity under these operations.

3. Keep the notation of Ex. 2. Prove that, if A is an ideal of R , then $M^{-1}A = \{\frac{a}{m} \in M^{-1}R : a \in A, m \in M\}$ is an ideal of $M^{-1}R$. If A, B are ideals of R , then $M^{-1}(A + B) = M^{-1}A + M^{-1}B$ and $M^{-1}(A \cap B) = M^{-1}A \cap M^{-1}B$. Does every ideal of $M^{-1}R$ have the form $M^{-1}A$ for some ideal A of R ?

4. Let R be a commutative ring with identity and let P be a prime ideal of R (see §30, Ex. 11). Show that $M := R \setminus P$ is a multiplicatively closed subset of R . Prove that $M^{-1}R$, in the notation of Ex. 2, has a unique maximal ideal (see §30, Ex. 12).

5. Discuss the rings in Example 29.2(e),(g) under the light of Ex. 3 and 4.