3. Check all the field axioms to show that F is a field under these operations.
4. Show that F can be viewed as containing D as an integral subdomain.

Steps 1, 2, and 4 are very interesting, and Step 3 is largely a mechanical chore. We proceed with the construction.

Step 1 Let D be a given integral domain, and form the Cartesian product

$$D \times D = \{(a, b) \mid a, b \in D\}$$

We are going to think of an ordered pair (a, b) as representing a *formal quotient* a/b, that is, if $D = \mathbb{Z}$, the pair (2, 3) will eventually represent the number $\frac{2}{3}$ for us. The pair (2, 0) represents no element of $\mathbb{Q}$ and suggests that we cut the set $D \times D$ down a bit. Let S be the subset of $D \times D$ given by

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

Now S is still not going to be our field as is indicated by the fact that, with $D = \mathbb{Z}$, *different* pairs of integers such as (2, 3) and (4, 6) can represent the *same* rational number. We next define when two elements of S will eventually represent the same element of F, or, as we shall say, when two elements of S are *equivalent*.

26.2 Definition Two elements (a, b) and (c, d) in S are **equivalent,** denoted by $(a, b) \sim (c, d)$, if and only if $ad = bc$. ■

Observe that this definition is reasonable, since the criterion for $(a, b) \sim (c, d)$ is an equation $ad = bc$ involving elements in D and concerning the known multiplication in D. Note also that for $D = \mathbb{Z}$, the criterion gives us our usual definition of *equality* of $\frac{a}{b}$ with $\frac{c}{d}$, for example, $\frac{2}{3} = \frac{4}{6}$ since (2)(6) = (3)(4). The rational number that we usually denote by $\frac{2}{3}$ can be thought of as the collection of *all* quotients of integers that reduce to, or are equivalent to, $\frac{2}{3}$.

26.3 Lemma The relation $\sim$ between elements of the set S as just described is an equivalence relation.

Proof We must check the three properties of an equivalence relation.

Reflexive $(a, b) \sim (a, b)$ since $ab = ba$, for multiplication in D is commutative.

Symmetric If $(a, b) \sim (c, d)$, then $ad = bc$. Since multiplication in D is commutative, we deduce that $cb = da$, and consequently $(c, d) \sim (a, b)$.

Transitive If $(a, b) \sim (c, d)$ and $(c, d) \sim (r, s)$, then $ad = bc$ and $cs = dr$. Using these relations and the fact that multiplication in D is commutative, we have

$$asd = sad = sbc = bcs = bdr = brd.$$

Now $d \neq 0$, and D is an integral domain, so cancellation is valid; this is a crucial step in the argument. Hence from $asd = brd$ we obtain $as = br$, so that $(a, b) \sim (r, s)$. ◆

We now know, in view of Theorem 0.22, that $\sim$ gives a partition of S into equivalence classes. To avoid long bars over extended expressions, we shall let $[(a, b)]$, rather than $\overline{(a, b)}$, be the equivalence class of (a, b) in S under the relation $\sim$. We now finish Step 1 by defining F to be the set of all equivalence classes $[(a, b)]$ for $(a, b) \in S$.

Step 2 The next lemma serves to define addition and multiplication in F. Observe that if $D = \mathbb{Z}$ and $[(a, b)]$ is viewed as $(a/b) \in \mathbb{Q}$, these definitions applied to $\mathbb{Q}$ give the usual operations.

26.4 Lemma For $[(a,b)]$ and $[(c,d)]$ in F, the equations

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

and

$$[(a,b)][(c,d)] = [(ac, bd)]$$

give well-defined operations of addition and multiplication on F.

Proof Observe first that if $[(a,b)]$ and $[(c,d)]$ are in F, then (a,b) and (c,d) are in S, so $b \neq 0$ and $d \neq 0$. Because D is an integral domain, $bd \neq 0$, so both $(ad+bc, bd)$ and (ac, bd) are in S. (Note the crucial use here of the fact that D has no divisors of 0.) This shows that the right-hand sides of the defining equations are at least in F.

It remains for us to show that these operations of addition and multiplication are well defined. That is, they were defined by means of representatives in S of elements of F, so we must show that if different representatives in S are chosen, the same element of F will result. To this end, suppose that $(a_1, b_1) \in [(a,b)]$ and $(c_1, d_1) \in [(c,d)]$. We must show that

$$(a_1d_1 + b_1c_1, b_1d_1) \in [(ad+bc, bd)]$$

and

$$(a_1c_1, b_1d_1) \in [(ac, bd)].$$

Now $(a_1, b_1) \in [(a,b)]$ means that $(a_1, b_1) \sim (a,b)$; that is,

$$a_1b = b_1a.$$

Similarly, $(c_1, d_1) \in [(c,d)]$ implies that

$$c_1d = d_1c.$$

To get a "common denominator" (common second member) for the four pairs (a,b), (a_1, b_1), (c,d), and (c_1, d_1), we multiply the first equation by d_1d and the second equation by b_1b. Adding the resulting equations, we obtain the following equation in D:

$$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b.$$

Using various axioms for an integral domain, we see that

$$(a_1d_1 + b_1c_1)bd = b_1d_1(ad+bc),$$

so

$$(a_1d_1 + b_1c_1, b_1d_1) \sim (ad+bc, bd),$$

giving $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad+bc, bd)]$. This takes care of addition in F. For multiplication in F, on multiplying the equations $a_1b = b_1a$ and $c_1d = d_1c$, we obtain

$$a_1bc_1d = b_1ad_1c,$$

so, using axioms of D, we get

$$a_1c_1bd = b_1d_1ac,$$

which implies that

$$(a_1c_1, b_1d_1) \sim (ac, bd).$$

Thus $(a_1c_1, b_1d_1) \in [(ac, bd)]$, which completes the proof. ◆

It is important to *understand* the meaning of the last lemma and the necessity for proving it. This completes our Step 2.

Step 3 Step 3 is routine, but it is good for us to work through a few of these details. The reason for this is that we cannot work through them unless we *understand* what we have done. Thus working through them will contribute to our understanding of this construction. We list the things that must be proved and prove a couple of them. The rest are left to the exercises.

1. Addition in F is commutative.

Proof Now $[(a, b)] + [(c, d)]$ is by definition $[(ad + bc, bd)]$. Also $[(c, d)] + [(a, b)]$ is by definition $[(cb + da, db)]$. We need to show that $(ad + bc, bd) \sim (cb + da, db)$. This is true, since $ad + bc = cb + da$ and $bd = db$, by the axioms of D. ◆

2. Addition is associative.
3. $[(0, 1)]$ is an identity element for addition in F.
4. $[(-a, b)]$ is an additive inverse for $[(a, b)]$ in F.
5. Multiplication in F is associative.
6. Multiplication in F is commutative.
7. The distributive laws hold in F.
8. $[(1, 1)]$ is a multiplicative identity element in F.
9. If $[(a, b)] \in F$ is not the additive identity element, then $a \neq 0$ in D and $[(b, a)]$ is a multiplicative inverse for $[(a, b)]$.

Proof Let $[(a, b)] \in F$. If $a = 0$, then

$$a1 = b0 = 0,$$

so

$$(a, b) \sim (0, 1),$$

that is, $[(a, b)] = [(0, 1)]$. But $[(0, 1)]$ is the additive identity by Part 3. Thus if $[(a, b)]$ is not the additive identity in F, we have $a \neq 0$, so it makes sense to talk about $[(b, a)]$ in F. Now $[(a, b)][(b, a)] = [(ab, ba)]$. But in D we have $ab = ba$, so $(ab)1 = (ba)1$, and

$$(ab, ba) \sim (1, 1).$$

Thus

$$[(a, b)][(b, a)] = [(1, 1)],$$

and $[(1, 1)]$ is the multiplicative identity by Part 8. ◆

This completes Step 3.

Step 4 It remains for us to show that F can be regarded as containing D. To do this, we show that there is an isomorphism i of D with a subdomain of F. Then if we rename the image of D under i using the names of the elements of D, we will be done. The next lemma gives us this isomorphism. We use the letter i for this isomorphism to suggest *injection*; we will inject D into F.

26.5 Lemma The map $i : D \to F$ given by $i(a) = [(a, 1)]$ is an isomorphism of D with a subring D' of F.

Proof For a and b in D, we have

$$i(a + b) = [(a + b, 1)].$$

Also,

$$i(a) + i(b) = [(a, 1)] + [(b, 1)] = [(a1 + 1b, 1)] = [(a + b, 1)]$$