4.7 Field of Quotients of an Integral Domain

Motivation

$\mathbb{Z}$ is an integral domain but is not a field, since it does not contain multiplicative inverses for most elements.

On the other hand, if we "close it up" under multiplicative inverses — i.e., add in all the multiplicative inverses & their products with elements of $\mathbb{Z}$ — we obtain the field $\mathbb{Q}$ of rational numbers:

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \right\}.$$

Note, however, that this is not a listing of $\mathbb{Q}$ <u>without</u> duplication, since, for example,

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$$

So in "creating" $\mathbb{Q}$ from $\mathbb{Z}$ we don't merely create the set of all pairs of integers, but rather form an equivalence relation on pairs of integers:

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

and then letting $\frac{a}{b}$ denote the <u>equivalence class</u> of a pair with respect to the relation.

In the same way, we will show that given any integral domain D, we can form a "larger" field F in an analogous manner. Namely, we first define an appropriate equivalence relation on $D \times D$, and then define F to be the set of equivalence classes under this relation.

Construction

Let D be an integral domain, and let

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

Thus S is the set of all "legal fractions", but as with fractions of integers, many of these should define the same "rational number." So, we define a relation $\sim$ on S by declaring

$$(a,b) \sim (c,d) \iff ad = bc.$$

We claim that $\sim$ is an equivalence relation on S.

Exercise: Check that $\sim$ is reflexive & symmetric.

To show transitivity, suppose that we had

$$(a,b) \sim (c,d) \quad \& \quad (c,d) \sim (e,f).$$

Then $ad = bc$ and $cf = de$. Therefore

$$adf = bcf = bde.$$

& (e,f)

However, since (a,b) & (c,d) belong to S, we have $b \neq 0$, $d \neq 0$, $f \neq 0$. Therefore we can cancel these elements to get

$$af = be \qquad \text{so} \qquad (a,b) \sim (e,f).$$

This proves transitivity, so $\sim$ is an equivalence relation on S. The equivalence class of (a,b) would usually be denoted by $[(a,b)]$, but it is more suggestive if we write

$$[a/b] = [(a,b)] = \{(c,d) \in S : (a,b) \sim (c,d)\}$$

Note that the slash in $[a/b]$ has no meaning — it is just a placeholder, & we could just as well write $[a, b]$, as Herstein does. The symbols $[a/b]$ simply denote the equivalence class of (a,b) in S under the relation $\sim$.

Now we let F denote the set of equivalence classes:

$$F = \{[a/b] : (a,b) \in S\}$$

$$= \{[a/b] : a, b \in D, b \neq 0\}.$$

We will define addition & multiplication of elements of

F, and show that F is a field under these operations. Note that F is not a quotient ring — the elements of F are not cosets of an ideal. Therefore we cannot hope to simply appeal to results we have done before, we must prove all the field properties from scratch.

We define the operations of addition & multiplication exactly analogous to how they are defined on $\mathbb{Q}$.

Addition: Given $[a/b], [c/d] \in F$, we define

$$[a/b] + [c/d] = [ad+bc/bd].$$

Multiplication:

$$[a/b][c/d] = [ac/bd].$$

However, since there are many elements of S that may determine the same equivalence class $[a/b]$, our first task is to show these operations are well-defined. Although we rarely think about it, this is actually an issue even for ordinary rational numbers. For example, even though we know that $3/6 = 4/8$ and $2/5 = 4/10$, how do we know that

$$\frac{3}{6}\cdot\frac{2}{5} = \frac{6}{30} \quad \text{is the same as} \quad \frac{4}{8}\cdot\frac{4}{10} = \frac{16}{80}\ ?$$

Although we usually accept this without proof, we really

must verify that this is true.

Addition

Suppose that $[a/b] = [a'/b']$ & $[c/d] = [c'/d']$.

We must show that

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

is the same as

$$[a'/b'] + [c'/d'] = [a'd'+b'c'/b'd'].$$

To do this, we have to show that

$$(ad+bc, bd) \sim (a'd'+b'c', b'd')$$

or, in other words, we must show that

$$(ad+bc)(b'd') = (a'd'+b'c')(bd).$$

We just multiply out & verify these are equal:

$$(ad+bc)(b'd') = adb'd' + bcb'd'$$

$$= (ab')(dd') + (bb')(cd')$$

$$= (ba')(dd') + (bb')(c'd) \qquad \text{since } ab' = a'b \text{ \& } cd' = c'd$$

$$= (a'd' + b'c')(bd).$$

Therefore addition is well-defined.

Exercise: Show that multiplication is likewise well-defined.

Now we have to verify all of the properties needed to show that F is a field.

Exercise: Show that $[0/b] = [0/c]$ for all $b, c \neq 0$ in D.

This is the additive identity for F, i.e., 0 is F is $[0/b]$ for any (or all) $b \neq 0$ in D. To see this, note that

$$[0/b] + [c/d] = [0d + bc/bd] = [bc/bd].$$

But this is simply $[c/d]$, because

$$(bc)d = c(bd)$$

which implies

$$(bc, bd) \sim (c, d)$$

and hence $[bc/bd] = [c/d]$.

Exercise: Show that additive inverses are given by

$$-[a/b] = [-a/b].$$

Exercise: Show $+$ is commutative (easy) and associative (long).

Thus F is an abelian group under $+$. Now we have to check the multiplicative properties.

If there is a multiplicative identity $1 \in D$, then $[1/1]$ would clearly be a multiplicative identity for F. However, our definition of integral domain does not require the existence of a 1. Still, F will have a multiplicative identity.

Exercise: Show that $[a/a] = [b/b]$ for all $a, b \in D$ with $a, b \neq 0$.

This is the multiplicative identity in F, i.e., $1 = [a/a]$ for any & all $a \neq 0$ in D. To see this, take any $[c/d] \in F$. Then

$$1\,[c/d] = [a/a][c/d] = [ac/ad] = [c/d] \quad \text{(why?)}$$

Exercise: Show that multiplication is commutative & associative in F.

Multiplicative inverses: If there was a $1 \in D$, then we would be led to think about $[1/a]$ as a potential multiplicative inverse for $[a/1]$. But here doesn't have to be a $1 \in D$, and further the generic form of an element of F is $[a/b]$, not $[a/1]$. On the other hand, if $a, b \neq 0$ then

$$[a/b][b/a] = [ab/ab] = 1.$$

So every element $[a/b]$ of F that satisfies $a, b \neq 0$ has a multiplicative inverse.

Exercise: Show these are all the nonzero elements of F, i.e.,

$$[a/b] \neq 0 \iff a, b \neq 0.$$

The only thing left is the distributive law: Exercise!

Thus, we have shown that F is a field.

The field of quotients is often denoted by $Q(D)$, i.e., $F = Q(D)$.

Definition

F is called the field of quotients (or the fraction field) of D. We usually denote the elements of F by a/b

instead of $[a/b]$ or $[a,c]$, i.e.,

$$a/b = \{(c,d) \in S : ad = bc\}$$

Exercise

Suppose D is an integral domain with 1, & F is the field of quotients. Show that

$$\varphi : D \longrightarrow F$$
$$\varphi(a) = a/1$$

is an injective homomorphism.

Thus, if we "identify" the element $a \in D$ with the element $a/1 \in F$, then we can think of D as being a subring of F, just as we think of $\mathbb{Z}$ as being a subring of $\mathbb{Q}$. More precisely, D is isomorphic to a subring of F & is not actually a subset of F, but we usually abuse notation & write

$$D \subseteq F$$

meaning that $a \in D$ is identified with $a/1 \in F$.

What if D does not contain a 1? It's not as obvious, but still D is isomorphic to a subring of F.

Lemma

Let D be an integral domain & let F be its field of quotients. Choose any $a \neq 0$ in D, & define

$$\varphi: D \longrightarrow F$$
$$\varphi(d) = [da/a]$$

Then φ is an injective homomorphism.

Proof: Exercise. Note that φ will not be surjective (onto), but $\varphi: D \to \text{range}(\varphi)$ will be an isomorphism.

Exercise: Show that if $D = \mathbb{Z}$, then its field of quotients is isomorphic to $\mathbb{Q}$.

Exercise: Suppose D is an integral domain & F is its field of quotients. Show that if K is a field & $D \subseteq K$, then $F \subseteq K$. (More precise, show $\exists$ injective homomorphism $\psi: F \to K$.)

Thus, the field of quotients is the "smallest" field that contains D: any other field that contains D has an isomorphic image of F inside it.

Remark

If F is a field, then $D = F[x]$ is an integral domain. Its field of quotients, denoted

$$F(x) = Q(F[x]) = \left\{ f(x)/g(x) : f, g \in F[x],\ g \neq 0 \right\},$$

is called the field of rational functions over F.

Note that $f(x)/g(x)$ is really shorthand for an equivalence class - what does $f(x)/g(x)$ mean, exactly?