Section IV.21. The Field of Quotients of an Integral Domain

Note. This section is a homage to the rational numbers! Just as we can start with the integers $\mathbb{Z}$ and then "build" the rationals by taking all quotients of integers (while avoiding division by 0), we start with an integral domain and build a field which contains all "quotients" of elements of the integral domain. This is our first encounter with the idea of starting with an algebraic structure and then *extending* it to a larger, more complete structure. In this case we are extending an integral domain to a field that contains all inverses of elements of the integral domain (and possibly [*probably*] more).

Note. We start with integral domain D and extend it to a field of quotients F following the text's steps:

Step 1. Define the elements of F.

Step 2. Define $+$ and $\cdot$ on F.

Step 3. Verify the field axioms for $+$ and $\cdot$ on F.

Step 4. Show that F can be viewed as containing D as an integral subdomain.

Note. For part of Step 1, we define the set $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. The analogy with $\mathbb{Q}$ is that we think of $p/q \in \mathbb{Q}$ as $(p, q) \in \mathbb{Z} \times \mathbb{Z}$. Notice that for $p_1/q_1, p_2/q_2 \in \mathbb{Q}$ if we have $p_1/q_1 = p_2/q_2$ then $p_1q_2 = p_2q_1$. This is the motivation for the next definition (and notice that equality of the "quotients" is dealt with in terms of multiplication).

Definition 21.1. Two elements $(a, b), (c, d) \in S$ are *equivalent*, denoted $(a, b) \sim (c, d)$, if and only if $ad = bc$.

Lemma 21.2. The relation $\sim$ between elements of S is an equivalence relation.

Note. To complete Step 1, we define F as the set of equivalence classes of S under $\sim$. We denote the equivalence class containing (a, b) as $[(a, b)]$.

Note. For Step 2, we define $+$ and $\cdot$ on F, again by mimicing the behavior of $\mathbb{Q}$, as given in the following lemma.

Lemma 21.3. For $[(a, b)], [(c, d)] \in F$, the equations

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

$$\text{and } [(a, b)] \cdot [(c, d)] = [(ac, bd)]$$

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

Note. The real claim of Lemma 21.3 is that $+$ and $\cdot$ can be defined using *any* element of an equivalence class. That is, the sum and product of two elements of F can be computed using *any* representatives of the equivalence classes involved in the sum and product.

Lemma. (Step 3) F as defined above is a field. That is,

1. $+$ in F is commutative.
2. $+$ in F is associative.
3. $[(0,1)]$ is the additive identity in F.
4. $[(-a,b)]$ is the additive inverse for $[(a,b)]$ in F.
5. $\cdot$ is associative in F.
6. $\cdot$ is commutative in F.
7. The distribution laws hold in F:

   $$[(a,b)] \cdot ([(c,d)] + [(r,s)]) = [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(r,s)]$$

   (right distribution will follow from commutivity of $\cdot$).
8. $[(1,1)]$ is the multiplicative identity in F.
9. If $[(a,b)] \in F$, $[(a,b)] \neq [(0,1)]$, then $[(b,a)] \in F$ is the multiplicative inverse of $[(a,b)]$.

Note. "Lemma" establishes that F is a field (Step 3). We now only need to establish that D is an integral subdomain of F. This is the next lemma.

Lemma 21.4. (Step 4) The map $i : D \to F$ given by $i(a) = [(a,1)]$ is an isomorphism of D with a subring of F

Theorem 21.5. Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Strictly speaking, every element of F is a quotient of two elements of $i[D]$ where i is as defined in Lemma 21.4.) Such a field is a *field of quotients of* D.

Proof. The lemmas of this section establish that the field exists. Let $[(a,b)] \in F$. Then

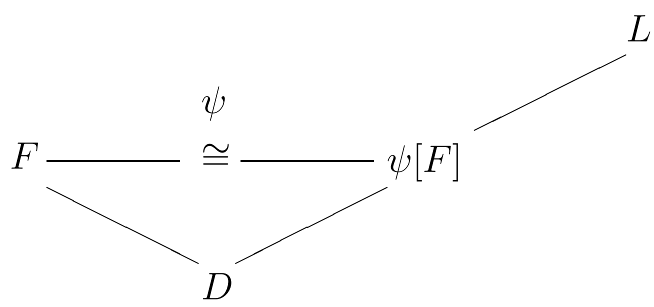
$$[(a,b)] = [(a,1)] \cdot [(1,b)] = i(a) \cdot (i(b))^{-1} = i(a)/i(b).$$

Here, "/" means multiplication by the multiplicative inverse. Notice that the multiplicative inverse of $[(b,1)]$ is $[(1,b)]$, so the inverse of $i(b)$ is $(i(b))^{-1}$ since i is an isomorphism from D to $i[D]$. ∎

Note. The next result shows that the field F created above containing integral domain D is minimal and that the field of quotients of D is unique.

Theorem 21.6. Let F be a field of quotients of D and let L be any field containing D. Then there exists a map $\psi : F \to L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$. (Technically, $\psi([a,1]) = a$, or $\psi \circ i : D \to L$ where $(\psi \circ i)(a) = \psi(i(a)) = \psi([a,1]) = a$ where $i : D \to F$ is as defined in Lemma 21.4.)

Note. The minimality concept in Theorem 21.6 can be illustrated with a diagram:



The idea is that any field L containing D also contains F—well, strictly speaking, L contains the isomorphic image of F, $\psi[F]$. So there is no "smaller" field than F which contains D. The fact that ψ is an isomorphism yields the uniqueness ("up to isomorphism").

Corollary 21.8. Every field L containing an integral domain D contains a field of quotients of D.

Corollary 21.9. Any two fields of quotients of an integral domain are isomorphic.

Revised: 11/22/2014