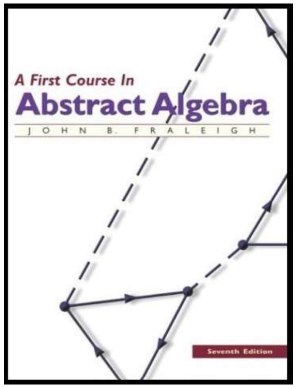
Introduction to Modern Algebra

Part IV. Rings and Fields

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



Lemma 21.2.

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

Proof. First, $(a, b) \sim (a, b)$ since $ab = ba$ since multiplicative in D is commutative. So $\sim$ is reflexive.

Second, if $(a, b) \sim (c, d)$ then $ad = bc$. By commutativity of multiplication, $cb = da$ and so $(c, d) \sim (a, d)$ and $\sim$ is symmetric.

Thirdly, suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (r, s)$. Then $ad = bc$ and $cs = dr$. Therefore

$$\begin{aligned} asd &= sad \text{ by commutativity} \\ &= sbc \text{ since } ad = bc \\ &= bcs \text{ by commutativity} \\ &= bdr \text{ since } cs = dr \\ &= brd \text{ by commutativity.} \end{aligned}$$

Lemma 21.2 (continued).

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

Proof (continued). So $(a, b) \sim (c, d)$ and $(c, d) \sim (r, s)$ implies $asd = brd$. Since $d \neq 0$ and D is an integral domain (no divisors of 0), then by Theorem 19.5 the laws of cancellation hold and so $as = br$. That is $(a, b) \sim (r, s)$ and $\sim$ is transitive.

Therefore $\sim$ is an equivalence relation, as claimed. □

Lemma 21.3.

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.

Proof. First, notice for $[(a, b)], [(c, d)] \in F$, we have $(a, b), (c, d) \in S$ with $b \neq 0$ and $d \neq 0$. So $bd \neq 0$ since 0 is an integral domain and $(ad + bc, bd), (ac, bd) \in S$ and so the right hand sides of the two equations are in fact elements of F.

Now to show the independence of the choice of representatives from the equivalence classes. Let $(a_1, b_1) \in [(a, b))]$ and $(c_1, d_1) \in [(c, d)]$. Then $(a_1, b_1) \sim (a, b)$ and $(c_1, d_1) \sim (c, d)$. So $a_1 b = b_1 a$ and $c_1 d = d_1 c$. So $a_1 b (d_1 d) + c_1 d (b_1 b) = b_1 a (d_1 d) + d_1 c (b_1 b)$ and so $(a_1 d_1 + b_1 c_1) bd = b_1 d_1 (ad + bc)$ and then $(a_1 d_1 + b_1 c_1, b_1 d_1) \sim (ad + bc, bd)$.

Lemma 21.3 (continued).

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.

Proof (continued). That is $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad+bc, bd)]$. So addition in F is well defined. As above, $a_1b = b_1a$ and $c_1d = d_1c$ imply $a_1b(c_1d) = b_1a(d_1c)$ or $a_1c_1bd = b_1d_1ac$. That is $(a_1c_1, b_1d_1) \sim (ac, bd)$, and $(a_1c_1, b_1d_1) \sim [(ac, bd)]$. So multiplication is F is well defined, as claimed. □

Lemma 21.A.

Lemma 21.A. 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 commutativity 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 $[(a,b)]$.

Lemma 21.A (continued 1).

Lemma 21.A.

1. $+$ in F is commutative.
2. $+$ in F is associative.

Proof.
1. Let $[(a,b)] \in F$. Then $[(a,b)] + [(c,d)] = [(ad+bc, bd)] = [(cb+da, db)]$ since $ad + bc = cb + da$ and $bd = db$ in integral domain D.

2. Let $[(a,b)], [(c,d)], [(r,s)] \in F$. Then $([(a,b)] + [(c,d)]) + [(r,s)] = [(ad+bc, bd)] + [(r,s)] = [(ad+bc)s + (bd)r, (bd)s] = [a(ds) + b(cs+dr), b(ds)] = [(a,b)] + [(cs+dr, ds)] = [(a,b)] + ([(c,d)] + [(r,s)])$ and $+$ is associative.

Lemma 21.A (continued 2).

Lemma 21.A.

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.

Proof.
3. Let $[(a,b)] \in F$, then $[(a,b)] + [(0,1)] = [(a(1) + b(0), b(1))] = [(a,b)]$. Since $+$ is commutative, $[(0,1)] + [(a,b)] = [(a,b)]$ and $[(0,1)]$ is the additive identity.

4. For $[(a,b)] \in F$, $b \neq 0$ and so $[(-a,b)] \in F$. Now $[(a,b)] + [(-a,b)] = [a(b) + b(-a), b] = [0,b]$. Now $[0,1] \sim [0,b]$ since $0 \cdot b = 1 \cdot 0$. So $[(a,b)] + [(-a,b)] = [(0,1)]$ and since $+$ is commutative, $[(-a,b)] + [(a,b)] = [(0,1)]$ and $[(-a,b)]$ is the $+$ inverse of $[(a,b)]$.

Lemma 21.A (continued 3).

Lemma 21.A.

5. $\cdot$ is associative in F.
6. $\cdot$ is commutative in F.

Proof (continued).
5. Let $[(a,b)], [(c,d)], [(r,s)] \in F$. Then $[(a,b)] \cdot ([(c,d)] \cdot [(r,s)]) = [(a,b)] \cdot [(cr,ds)] = [(acr,bds)] = [(ac,bd)] \cdot [(r,s)] = ([(a,b)] \cdot [(c,d)]) \cdot [(r,s)]$ and $\cdot$ is associative.

6. Let $[(a,b)], [(c,d)] \in F$. Then $[(a,b)] \cdot [(c,d)] = [(ac,bd)] = [(ca,db)]$, since $\cdot$ is commutative in D, $= [(c,d)] \cdot [(a,b)]$. So $\cdot$ is commutative in F.

Lemma 21.A (continued 5).

Lemma 21.A.

9. If $[(a,b)] \in F$, $[(a,b)] \neq [(0,1)]$, then $[(b,a)] \in F$ is the multiplicative inverse of $[(a,b)]$.

Proof (continued).
9. Since $[(a,b)] \neq [(0,1)]$, then $a \neq 0$ and so $[(b,a)] \in F$. Now $[(a,b)] \cdot [(b,a)] = [(ab,ba)]$. Since $(ab,ba) = (ab,ab) \sim (1,1)$, then $[(a,b)] \cdot [(b,a)] = [(1,1)]$. Since $\cdot$ is commutative by (6), $[(b,a)] \cdot [(a,b)] = [(1,1)]$ and $[(b,a)]$ is the multiplicative inverse of $[(a,b)]$. □

Lemma 21.4.

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

Proof. First,

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

Also,

$$i(ab) = [(ab,1)] = [(a,1)] \cdot [(b,1)] = i(a) \cdot i(b).$$

Now to show i is one-to-one. Suppose $i(a) = i(b)$ then $[(a,1)] = [(b,1)]$ and so $(a,1) \sim (b,1)$, or $a1 = 1b$, or $a = b$. So i is one-to-one and i preserves sums and products. Next i is onto its range which is a subset of F. Therefore i is a ring isomorphism between D and a subring of F. In fact, since D is an integral domain, so is $i[D]$. □

Theorem 21.6.

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 $a \in D$.

Proof. By definition, any element of F is a quotient of elements in $i[D]$. If $f \in F$ satisfies $f = i(a) \cdot (i(b))^{-1}$, then we denote this as $f = a/_F b$ (here, 'a' and 'b' are treated as elements of F^* although they are not, but their images $i(a)$ and $i(b)$ are in F). Define $\psi : F \to L$ as $\psi(a) = a$ for $a \in D$ $\psi(f) = \psi(a)/_L\psi(b)$ for $f = a/_F b \in F \backslash i[D]$. We now need to verify that ψ is well-defined (notice that f may be the quotient of many pairs of elements of $i[D]$, so we need to make sure that the definition of ψ is independent of this representation of f as a quotient). First, if $f = a/_F b$ then $b \neq 0$ and since ψ is the identity function on D and $0 \in D$, then $\psi(f) = \psi(a)/_l\psi(b)$ is defined because $\psi(b) \neq 0$ (since $b \neq 0$).

Theorem 21.6 (continued 1).

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 $a \in D$.

Proof (continued). Now if $f = a/_F b = c/_F d$, then $ad = bc$ (as a product of elements of D) and so $\psi(ad) = \psi(bc)$. But since ψ is the identity on D, $\psi(ad) = \psi(a)\psi(d)$ and $\psi(bc) = \psi(b)\psi(c)$. So $\psi(a)\psi(d) = \psi(b)\psi(c)$ and $\psi(a)/_L\psi(b) = \psi(c)/_L\psi(d)$. Therefore $\psi(f)$ is well-defined.

Now to show that ψ is an isomorphism. First, let $x, y \in F$, so $x = a/_F b$ and $y = c/_F d$ for some $a, b, c, d \in D$, $b \neq 0$, $d \neq 0$. Then $\psi(xy) = \psi((a/_F b) \cdot (c/_F d)) = \psi((ac)/_F(bd)) = \psi(ac)/_L\psi(bd)$, by definiton of ψ on F, $= (ac)/_L(bd)$, since ψ is identity on D, $= (ac)/_L(bd)$, since ψ is identity on D, $= (a/_L b)(c/_L d)$, since D is integral domain, $= \psi(a/_F b)\psi(c/_F d) = \psi(x)\psi(y)$.

Theorem 21.6 (continued 2).

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 $a \in D$.

Proof (continued). Next $\psi(x + y) = \psi(a/_F b + c/_F d) = \psi((ad + bc)/_F(bd)) = \psi(ad + bc)/_L\psi(bd)$, be definition of ψ on F, $= (ad + bc)/_L(bd)$, since ψ is the identity on D, $= a/_L b + c/_L d = \psi(a/_F b) + \psi(c/_F d) = \psi(x) + \psi(y)$.

Finally, to show ψ is one-to-one, suppose $\psi(a/_F b) = \psi(c/_F d)$. Then $\psi(a)/_L\psi(b) = \psi(c)/_L\psi(d)$ and $\psi(a)\psi(d) = \psi(b)\psi(c)$ or (since ψ is the identity on D) $ad = bc$. Therefore, $a/_F b = c/_F d$ and so ψ is one-to-one. Therefore ψ is an isomorphism, as desired. □

Corollary 21.8.

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

Proof. From the proof of Theorem 21.6, we know that F is a field and ψ is a ring (and field) isomorphism, so $\psi[F]$ is a field. As seen in the proof, $\varphi[F]$ is a field of quotients of elements of D subfield of D. □

Corollary 21.9.

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

Proof. Suppose L is a field of quotients of D. Then every element $x \in L$ is of the form $x = a/_L b$ for some $a, b \in D$. So $L \subseteq \psi[F]$ using the notation of Theorem 21.6, and similarly $\psi[F] \subseteq L$. So $\psi[F] = L$ and the two fields of quotients F and L are isomorphic. □