4-21-2018

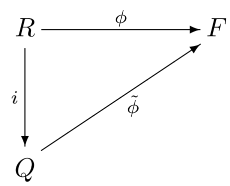
# The Quotient Field of an Integral Domain

The rationals $\mathbb{Q}$ are constructed from the integers $\mathbb{Z}$ by "forming fractions". This amounts to making all the nonzero elements of $\mathbb{Z}$ invertible. In fact, you can perform this construction for an arbitrary integral domain.

**Theorem.** Let $R$ be an integral domain.

(a) There is a field $Q$, the **quotient field** of $R$, and an injective ring map $i : R \to Q$.

(b) If $F$ is a field and $\phi : R \to F$ is an injective ring map, there is a unique ring map $\tilde{\phi} : Q \to F$ such that the following diagram commutes:




Heuristically, this means that $Q$ is the "minimal" way of inverting the nonzero elements of $R$.

**Proof.** The first step is to form the fractions. Let

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

(Think of $(a, b)$ as corresponding to the fraction $\dfrac{a}{b}$. The elements of $Q$ aren't actually fractions, but equivalence classes of fractions. Think of the situation in the rationals $\mathbb{Q}$: $\dfrac{1}{2}$ and $\dfrac{2}{4}$ are really the same element of $\mathbb{Q}$.)

Two rational fractions $\dfrac{a}{b}$ and $\dfrac{c}{d}$ are equal if and only if $ad = bc$. I'll use this idea to put an equivalence relation on $S$.

If $(a, b), (c, d) \in S$, write $(a, b) \sim (c, d)$ if and only if $ad = bc$. I claim this is an equivalence relation.

(a) Since $ab = ab$, I have $(a, b) = (a, b)$.

(b) If $(a, b) \sim (c, d)$, then $ad = bc$. So $bc = ad$, and hence $(c, d) \sim (a, b)$.

(c) Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. I want to show that $af = be$. The first equation yields $adf = bcf$, while the second equation yields $bcf = bde$. Therefore, $adf = bde$. Now $(c, d) \in S$ implies $d \neq 0$, and since $R$ is a domain, I may cancel $d$ to obtain $af = be$. Hence, $(a, b) = (e, f)$, which completes the proof of transitivity.

Let $Q$ be the set of equivalence classes. Let $[a, b] \in Q$ denote the equivalence class of $(a, b) \in S$. I want to show that $Q$ is a field with the appropriate properties.

First, I'll define the operations. For $[a, b], [c, d] \in Q$, define

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

Note that in each case $b, d \neq 0$ so $bd \neq 0$, and the expressions on the right at least make sense.

I now have some routine but extremely tedious verifications to perform. Since these operations are defined on equivalence classes, I must check that they're well-defined — i.e. that they're independent of the choices of representatives for the equivalence classes.

Once I have well-defined operations, I have to check all the axioms for a field. This entails checking all the ring axioms, commutativity, and the existence of inverses for nonzero elements. For example, I'll show that $[0, 1]$ functions as an additive identity, while $[1, 1]$ is the multiplicative identity.

It is probably a little much to expect you to wade through all of the ugly computations. Nevertheless, I'll show all the work below. I suggest that you at least verify that one of the two operations is well-defined, and that you work through the proof for at least one of the ring axioms.

First, I'll prove that addition and multiplication are well-defined. Suppose that $[a, b] = [a', b']$, so $ab' = a'b$, and $[c, d] = [c', d']$ so $cd' = c'd$.

1. Addition is well-defined.

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [a', b'] + [c', d'] = [a'd' + b'c', b'd'].$$

Now

$$(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd,$$

Hence, $[ad + bc, bd] = [a'd' + b'c', b'd']$.

2. Multiplication is well-defined.

$$[a, b][c, d] = [ac, bd] \quad \text{and} \quad [a', b'][c', d'] = [a'c', b'd'].$$

Now

$$(ac)(b'd') = ab'cd' = a'bc'd = (a'c')(bd).$$

Hence, $[ac, bd] = [a'c', b'd']$.

Next, I'll verify that $Q$ is a field. I have to verify the ring axioms, that multiplication is commutative, and that nonzero elements have inverses.

3. Addition is associative.

$$([a, b] + [c, d]) + [e, f] = [ad + bc, bd] + [e, f] = [adf + bcf + bde, bdf],$$

$$[a, b] + ([c, d] + [e, f]) = [a, b] + [cf + de, df] = [adf + bcf + bde, bdf].$$

4. Addition is commutative.

$$[a, b] + [c, d] = [ad + bc, bd] \quad \text{and} \quad [c, d] + [a, b] = [bc + ad, bd].$$

5. $[0, 1]$ is the additive identity.

$$[a, b] + [0, 1] = [a \cdot 1 + b \cdot 0, b] = [a, b].$$

6. $-[a, b] = [-a, b]$.

$$[a, b] + [-a, b] = [ab - ab, b^2] = [0, b^2].$$

However, $[0, b^2] = [0, 1]$, since $0 \cdot 1 = b^2 \cdot 0$.

7. Multiplication is associative.

$$([a, b][c, d])\,[e, f] = [ace, bdf] = [a, b]\,([c, d][e, f])\,.$$

8. Multiplication is commutative.

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

9. $[1, 1]$ is the multiplicative identity.

$$[a, b][1, 1] = [a, b].$$

10. Multiplication distributes over addition.

By commutativity of multiplication, it suffices to check this on one side.

$$[a,b]\left([c,d]+[e,f]\right)=[a,b][cf+de,df]=[acf+ade,bdf],$$

$$[a,b][c,d]+[a,b][e,f]=[ac,bd]+[ae,bf]=[abcf+abde,b^2df].$$

However,

$$(acf+ade)b^2df=ab^2cdf^2+ab^2d^2ef \quad \text{and} \quad (abcf+abde)bdf=ab^2cdf^2+ab^2d^2ef.$$

Therefore, $[acf+ade,bdf]=[abcf+abde,b^2df]$.

11. Nonzero elements have multiplicative inverses.

Suppose $[a,b]\neq[0,1]$, so $a\neq 0$. Then using $ab\cdot 1=1\cdot ab$, I have

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

Hence, $[b,a]=[a,b]^{-1}$.

This completes the verification that $Q$ is a field. Next, I'll construct the imbedding of $R$ into $Q$.

Define $i:R\to Q$ by $i(r)=[r,1]$. I'll check that $i$ is a ring map. First, $i(1)=[1,1]$.
Next,

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

Next, I'll show that $i$ is injective. Suppose $i(x)=[0,1]$ (since $[0,1]$ is the zero element of $Q$). Then $[x,1]=[0,1]$, or $x=0$. Therefore, $\ker i=\{0\}$, so $i$ is injective.

Finally, I'll complete the proof by verifying the universal property. Suppose that $F$ is a field and $\phi:R\to F$ is an injective ring map. Define $\tilde{\phi}:Q\to F$ by

$$\tilde{\phi}\left([a,b]\right)=\phi(a)\phi(b)^{-1}.$$

Observe that since $b\neq 0$, $\phi(b)\neq 0$ (injectivity), so $\phi(b)$ is invertible in the field $F$.
I have to check that the map is well-defined. Suppose that $[a,b]=[a',b']$, so $ab'=a'b$. Then

$$\phi(a)\phi(b')=\phi(a')\phi(b),$$
$$\phi(a)\phi(b)^{-1}=\phi(a')\phi(b')^{-1},$$
$$\tilde{\phi}\left([a,b]\right)=\tilde{\phi}\left([a',b']\right).$$

Next, I'll check that $\tilde{\phi}$ is a ring map. First,

$$\tilde{\phi}\left([1,1]\right)=\phi(1)\phi(1)^{-1}=1\cdot 1=1.$$

Next,

$$\tilde{\phi}\left([a,b]+[c,d]\right)=\tilde{\phi}\left([ad+bc,bd]\right)=\phi(ad+bc)\phi(bd)^{-1}=\phi(ad)\phi(bd)^{-1}+\phi(bc)\phi(bd)^{-1}=$$

$$\phi(a)\phi(d)\phi(b)^{-1}\phi(d)^{-1}+\phi(b)\phi(c)\phi(b)^{-1}\phi(d)^{-1}=\phi(a)\phi(b)^{-1}+\phi(c)\phi(d)^{-1}=\tilde{\phi}\left([a,b]\right)+\tilde{\phi}\left([c,d]\right).$$

Finally,

$$\tilde{\phi}\left([a,b][c,d]\right)=\tilde{\phi}\left([ac,bd]\right)=\phi(ac)\phi(bd)^{-1}=\phi(a)\phi(b)^{-1}\phi(c)\phi(d)^{-1}=\tilde{\phi}\left([a,b]\right)\tilde{\phi}\left([c,d]\right).$$

I need to check that $\tilde{\phi}$ makes the diagram commute. If $a \in R$,

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

Finally, I'll show that $\tilde{\phi}$ is the only map which could satisfy these conditions. If $\psi$ was another injective ring map filling in the diagram, then for $a \in R$,

$$\psi \cdot i(a) = \phi(a).$$

Hence, $\psi([a, 1]) = \phi(a)$.

Now let $b \in R$, $b \neq 0$. Since $\psi$ is a ring map,

$$1 = \psi([1, 1]) = \psi([b, 1][1, b]) = \psi([b, 1])\,\psi([1, b]) = \phi(b)\psi([1, b]).$$

$\phi$ is injective, so $\phi(b) \neq 0$, and it's invertible in $F$. Therefore, $\psi([1, b]) = \phi(b)^{-1}$.

Now put the results of the last two paragraphs together, again using the fact that $\psi$ is a ring map:

$$\psi([a, b]) = \psi([a, 1][1, b]) = \psi([a, 1])\,\psi([1, b]) = \phi(a)\phi(b)^{-1} = \tilde{\phi}([a, b]).$$

Thus, $\tilde{\phi}$ is the unique map filling in the diagram, and the proof is (finally!) complete. □

The standard argument for objects defined by universal properties shows that the quotient field of an integral domain is unique up to ring isomorphism. That is, if $R$ is a domain and $Q$ and $Q'$ are fields satisfying the universal property for the quotient field of $R$, then $Q \approx Q'$.

---

If $R$ is a field, then it is its own quotient field. To prove this, use uniqueness of the quotient field, and the fact that the identity map $\text{id} : R \to R$ satisfies the universal property.

In most cases, it is easy to see what the quotient field "looks like". For example, let $R$ be the domain $\mathbb{Q}[x]$ of polynomials with rational coefficients. The quotient field is $\mathbb{Q}(x)$, the field of **rational functions** with rational coefficients. It consists of all quotients $\dfrac{p(x)}{q(x)}$, where $p, q \in \mathbb{Q}[x]$ and $q \neq 0$, under the usual operations.

This may seem like a lot of work to produce something that is "obvious". But the reason this may seem "obvious" to you is that you've had lots of experience working with the the rational numbers $\mathbb{Q}$, the quotient field of the integers $\mathbb{Z}$.