Math103b, lecture 5

Golsefidy

In the previous lecture we gave a formal definition of fractions of elements of an integral domain; suppose D is an integral domain, $a \in D$ and $b \in D \setminus \{0\}$, we let

$$[(a,b)] := \{(c,d) \in D \times (D \setminus \{0\}) | ad = bc\}.$$

We proved that $\{[(a,b)] | (a,b) \in D \times (D \setminus \{0\})\}$ is a partition of $D \times (D \setminus \{0\})$; and we set

$$\frac{a}{b} := [(a,b)] \text{ and } Q(D) := \left\{ \frac{a}{b} | \ a \in D, b \in D \setminus \{0\} \right\}.$$

Based on some tedious computation one can show:

Lemma 1 *Let* $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ *and* $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$. *Then these are well-defined operations; and* $(Q(D), +, \cdot)$ *is a ring.*

Parts of proof. Here I only emphasize on what it means to say these are well-defined operations and mention only some steps of proof.

The main point is that these operations are defined based on a choice of representatives for the fractions $\frac{a}{b}$ and $\frac{c}{d}$; meaning we have to show the following implications:

$$\left.\begin{array}{l} \frac{a}{b} = \frac{a'}{b'} \\ \frac{c}{d} = \frac{c'}{d'} \end{array}\right\} \overset{?}{\Rightarrow} \left\{\begin{array}{c} \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \\ \frac{ac}{bd} = \frac{a'c'}{b'd'} \end{array}\right.$$

I show the addition is well-defined; multiplication is similar.

$$\left.\begin{array}{l} \frac{a}{b} = \frac{a'}{b'} \\ \frac{c}{d} = \frac{c'}{d'} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} ab' = a'b \\ cd' = c'd \end{array}\right\} \overset{?}{\Rightarrow} b'd'(ad + bc) = bd(a'd' + b'c')$$

Let's continue our backward argument:

$$b'd'(ad + bc) = bd(a'd' + b'c') \Leftarrow$$
$$(ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb') \Leftarrow$$
$$ab' = a'b \text{ and } cd' = c'd.$$

Based on similar type of computation one can show that multiplication is well-defined and the distributive and associative properties hold; and so Q(D) is a ring. ■

Next we show that Q(D) is a field.

Lemma 2 *For any* $a \in D \setminus \{0\}$, $\frac{a}{a} = \frac{1}{1}$ *and* $\frac{0}{a} = \frac{0}{1}$; $\frac{1}{1}$ *is the identity of* $Q(D)$ *and* $\frac{0}{1}$ *is the zero of* $Q(D)$. *And* $Q(D)$ *is a field.*

Proof. $a \cdot 1 = 1 \cdot a$ implies that $\frac{a}{a} = \frac{1}{1}$; $a \cdot 0 = 0 = 0 \cdot 1$ implies that $\frac{0}{a} = \frac{0}{1}$. We have $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b}$ which implies that $\frac{0}{1}$ is the zero of $Q(D)$. We have $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$ which implies that $\frac{1}{1}$ is the identity of $Q(D)$.

Since D is an integral domain, $0 \neq 1$; and so $\frac{1}{1} \neq \frac{0}{1}$.

Since D is commutative, we can check that $Q(D)$ is commutative.

For $\frac{a}{b} \neq 0$, we have $a \neq 0$; and so $\frac{b}{a} \in Q(D)$; and $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$, which implies any non-zero element of $Q(D)$ is a unit. So overall we have that $Q(D)$ is a field. ■

$Q(D)$ is called the field of fractions of D. We notice that similar to $\mathbb{Q}$ that contains a copy of $\mathbb{Z}$, $Q(D)$ contains a copy of D:

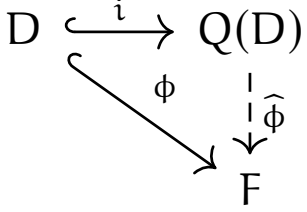
Lemma 3 *Suppose* D *is an integral domain and* $Q(D)$ *is its field of fractions. Then* $i : D \to Q(D), i(a) := \frac{a}{1}$ *is an injective ring homomorphism.*

Proof. $i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a+b}{1} = i(a+b)$ and similarly

$i(a)i(b) = \frac{a}{1}\frac{b}{1} = \frac{ab}{1} = i(ab)$; and so i is a ring homomorphism.

To show i is injective, we will show $\ker i = \{0\}$; suppose $a \in \ker i$; and so $\frac{a}{1} = \frac{0}{1}$, which implies $a = 0$. ■

Theorem 4 (Universal Property of Field of Fractions) *Suppose* D *is an integral domain and* $Q(D)$ *is its field of fractions. Suppose* F *is a field and* $\theta : D \longrightarrow F$ *is an injective ring homomorphism. Then there is a unique injective ring homomorphism* $\widehat{\theta} : Q(D) \longrightarrow F$ *such that* $\widehat{\theta}(i(a)) = \theta(a)$ *for any* $a \in D$. *Alternatively we can say the following is a commuting diagram:*



Proof. We start with the uniqueness part. We assume there is a $\widehat{\phi}$ which satisfies the desired properties; and we will find what it should be. For $b \in D \setminus \{0\}$, $\frac{1}{b}$ is the inverse of $\frac{b}{1}$; and so $\widehat{\theta}(\frac{1}{b}) = \widehat{\theta}(\frac{b}{1})^{-1} = \theta(b)^{-1}$. Hence we have

$$\widehat{\theta}(\frac{a}{b}) = \widehat{\theta}(\frac{a}{1}\frac{1}{b}) = \widehat{\theta}(\frac{a}{1})\widehat{\theta}(\frac{1}{b}) = \theta(a)\theta(b)^{-1}.$$

And so such a $\widehat{\theta}$ is uniquely determined by θ.

Now we show the existence part. From the uniqueness part we know that we have to consider $\widehat{\theta}(\frac{a}{b}) := \theta(a)\theta(b)^{-1}$ and show

that it does have the desired properties. Let's start by checking that $\widehat{\theta}$ is a ring homomorphism:

$$\begin{aligned}\widehat{\theta}(\frac{a}{b}+\frac{c}{d}) =&\widehat{\theta}(\frac{ad+bc}{bd}) = \theta(ad+bc)\theta(bd)^{-1}\\ =&(\theta(a)\theta(d)+\theta(b)\theta(c))\theta(b)^{-1}\theta(d)^{-1}\\ =&\theta(a)\theta(b)^{-1}+\theta(c)\theta(d)^{-1}\\ =&\widehat{\theta}(\frac{a}{b})+\widehat{\theta}(\frac{c}{d});\end{aligned}$$

and

$$\begin{aligned}\widehat{\theta}(\frac{a}{b}\frac{c}{d}) =&\widehat{\theta}(\frac{ac}{bd}) = \theta(ac)\theta(bd)^{-1}\\ =&\theta(a)\theta(c)\theta(b)^{-1}\theta(d)^{-1}\\ =&(\theta(a)\theta(b)^{-1})(\theta(c)\theta(d)^{-1})\\ =&\widehat{\theta}(\frac{a}{b})\widehat{\theta}(\frac{c}{d}).\end{aligned}$$

To show $\widehat{\theta}$ is injective, again we show its kernel is zero: suppose $\frac{a}{b} \in \ker\widehat{\theta}$; then $\widehat{\theta}(\frac{a}{b}) = \theta(a)\theta(b)^{-1} = 0$; and so $\theta(a) = 0$, which implies $a = 0$ as θ is injective. This implies that $\frac{a}{b} = \frac{0}{b} = \frac{0}{1}$.

We also notice that $\theta(1)\theta(1) = \theta(1)$; and so either $\theta(1) = 0$ or $\theta(1) = 1$ (by the cancellation law for integral domains). Since θ is injective and $0 \neq 1$, we deduce that $\theta(1) = 1$. Hence $\widehat{\theta}(i(a)) = \widehat{\theta}(\frac{a}{1}) = \theta(a)\theta(1)^{-1} = \theta(a)$; and claim follows. ■

In this course, for us is very important to know the statement of the above result and know how to use it. As you saw its proof consists of many easy steps with no new ideas.

Let's discuss two examples and see how the Universal Property of Field of Fractions can be used.

Example. Suppose $\mathbb{Z}[i] := \{a + bi | \, a, b \in \mathbb{Z}\}$ and $\mathbb{Q}[i] := \{a + bi | \, a, b \in \mathbb{Q}\}$. One can use the subring criterion and show that $\mathbb{Z}[i]$ and $\mathbb{Q}[i]$ are subrings of $\mathbb{C}$. $\mathbb{Z}[i]$ is called the ring of Gaussian integers. Prove that $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$.

General method. To show a given ring F is isomorphic to the field of fractions $Q(D)$ of a given integral domain D one can use the following steps:

Step 1. Show that F is a field.

Step 2. Find an injective ring homomorphism $\theta : D \to F$.

Step 3. Using Universal Property of Field of Fractions get that $\widehat{\theta} : Q(D) \to F, \widehat{\theta}(\frac{a}{b}) := \theta(a)\theta(b)^{-1}$ is an injective ring homomorphism.

Step 4. Prove that $\widehat{\theta}$ given in the previous step is surjective.

Proof of example. **Step 1.** To show $\mathbb{Q}[i]$ is a field, it is enough to show that any non-zero element is a unit (notice that $\mathbb{Q}[i]$ is

a non-zero subring of $\mathbb{C}$, and so it is an integral domain). For $a + bi \in \mathbb{Q}[i] \setminus \{0\}$, either $a \neq 0$ or $b \neq 0$; and so $a - bi \neq 0$. Hence we have

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Since $\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \in \mathbb{Q}$, we have that $\frac{1}{a+bi} \in \mathbb{Q}[i]$ which implies that $\mathbb{Q}[i]$ is a field.

Step 2. Clearly $\theta : \mathbb{Z}[i] \to \mathbb{Q}[i], \theta(a + bi) := a + bi$ is an injective ring homomorphism.

Step 3. As it is explained in the general case, by Universal Property of Field of Fractions

$$\widehat{\theta} : Q(\mathbb{Z}[i]) \to \mathbb{Q}[i], \widehat{\theta}(\frac{z}{z'}) := \theta(z)\theta(z')^{-1} = zz'^{-1}$$

is an injective ring homomorphism.

Step 4. Next we show that $\widehat{\theta}$ is surjective. Notice that any element of $\mathbb{Q}[i]$ can be written as $\frac{a+bi}{c}$ for some $a, b, c \in \mathbb{Z}$ (after taking the common denominator of the real and the imaginary parts). On the other hand, $\widehat{\theta}(\frac{a+bi}{c}) = (a + bi)c^{-1}$, which implies that $\widehat{\theta}$ is surjective. Therefore $\widehat{\theta}$ is a bijective ring homomorphism, which implies that $Q(\mathbb{Z}[i]) \simeq \mathbb{Q}[i]$. ■

Example. Suppose F is a field. Then $Q(F) \simeq F$.

Proof. Let $\theta : F \to F, \theta(a) := a$; clearly θ is an injective ring homomorphism. So by Universal Property of Field of Fractions $\widehat{\theta} : Q(F) \to F, \widehat{\theta}(\frac{a}{b}) := \theta(a)\theta(b)^{-1} = ab^{-1}$ is an injective ring homomorphism. We notice that for any $a \in F$, $\widehat{\theta}(\frac{a}{1}) = a \cdot 1^{-1} = a$; and so $\widehat{\theta}$ is surjective as well; and claim follows. ■