1.5 Lecture 5: The Field of Fractions of an Integral Domain

Suppose that R is an integral domain. One example of an integral domain is $\mathbb{Z}$, and another is $\mathbb{Q}[X]$, the ring of polynomials in one variable with rational coefficients.

(**Exercise** Show that the product of two non-zero polynomials in $\mathbb{Q}[X]$ is not the zero polynomial.)

Recall that a *field* is a commutative ring in which every non-zero element has an inverse for multiplication, such as $\mathbb{Q}$ or $\mathbb{R}$. Every field is an integral domain. The integral domains $\mathbb{Z}$ is a subring of the field $\mathbb{Q}$.

In the integral domain R (think of $\mathbb{Z}$ or $\mathbb{Q}[X]$), let a be a non-zero element (like 6 in $\mathbb{Z}$ or X^2+1 in $\mathbb{Q}[X]$). Then a is not a zero-divisor in R. If a is not a unit, we can consider whether it is possible to somehow extend the ring R to a bigger ring in which a has an inverse for multiplication. If we could do this simultaneously for all non-zero elements, what would the "extended" ring look like?

As an example, 3 has no inverse for multiplication in $\mathbb{Z}$. But $\mathbb{Z}$ can be extended to $\mathbb{Q}$, where 3 (and every non-zero integer) does have an inverse. We will show that the construction of $\mathbb{Q}$ from $\mathbb{Z}$ is an example of something that can be applied to integral domains in general.

Whn we first encounter fractions, it is probably in the context of splitting something into parts, so that every fraction has a numerical value that fits in to the order on the rational numbers. Then we get the addition and multiplication of fractions as a consequence, maybe making use of the numerial values, or maybe decimal representations, of rational numbers.

But if we started with just an integral domain and no order relation or numerical values or concept of "division into parts", could we have constructed the rational numbers just from the addition and multiplication on $\mathbb{Z}$? It's a good idea to think about the following construction for $\mathbb{Q}[X]$, to avoid getting distracted by the extra numerical information and order relation in $\mathbb{Z}$.

Construction of the Field of Fractions Let R be an integral domain. We write $R^\times$ for the set of non-zero elements of R. Then $R \times R^\times$ is the set of ordered pairs (a, b) where $a \in R$ and $b \in R$, $b \neq 0$. We define a relation $\sim$ on $R \times R^\times$ by

$$(a, b) \sim (a', b') \iff ab' = a'b.$$

Note: If our ring is $\mathbb{Z}$, this relation says exactly that $\frac{a}{b}$ and $\frac{a'}{b'}$ represent the same element of $\mathbb{Q}$, like $\frac{8}{6}$ and $\frac{40}{30}$ for example ($8 \times 30 = 40 \times 6$).

Now $\sim$ is an equivalence relation on $R \times R^\times$.

- $\sim$ is reflexive: $(a, b) \sim (a, b)$ is saying only that $ab = ab$. This is satisfied by all pairs (a, b).
- $\sim$ is symmetric: Suppose $(a, b) \sim (a', b')$. Then $ab' = a'b$, so $a'b = ab'$ and $(a', b') \sim (a, b)$.
- $\sim$ is transitive. Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ for elements a, c, e of R and elements b, d, f of $R^\times$. We need to show that $(a, b) \sim (e, f)$ which means $af = eb$. Since $(c, d) \sim (e, f)$ we know that $cf = ed$. Multiplying this equation by b and using both the commutativity and associativity of multiplication, it follows that $bcf = ebd$. Since $bc = ad$ (as $(a, b) \sim (c, d)$), it follows that $bcf = adf = afd = ebd$. Since $d \neq 0$ and we are in an integral domain, we can cancel d from $afd = ebd$ to conclude $af = eb$ which means exactly that $(a, b) \sim (e, f)$.

Note This argument uses everything we have - that our ring is commutative without zero divisors, and that the second entry of the pairs in $R \times R^\times$ is not zero. In a (commutative) ring with zero-divisors, is $\sim$ a transitive relation?

We write $F(R)$ now for the set of equivalence classes in $R \times R^\times$ under $\sim$. We denote the equivalence class of the pair (a, b) by $[a, b]$, which is saying that

$$[a, b] := \{(a', b') : a' \in R, b' \in R, b' \neq 0 \text{ and } ab' = a'b\}.$$

We define addition on $F(R)$ by

$$[a, b] + [c, d] = [ad + cb, bd].$$

We define multiplication on $F(R)$ by

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

The assertion is that $F(R)$ is a commutative ring with these operations, that it contains R as a subring, and that it contains a multiplicative inverse for each of its elements (i.e. it is a *field*). There are a number of items to be checked.

1. The addition and multiplication are well-defined on elements of $F(R)$, which are equivalence classes.

2. The addition satisfies the necessary axioms of commutativity, associativity and the existence of a zero element and additive inverse of each element.

3. The multiplication satisfies the necessary axioms of associativity, commutativity and the existence of an identity element.

4. Every non-zero element of $F(R)$ has an inverse for multiplication.

5. R is (identifiable with) a subset of $F(R)$ that contains the multiplicative identity element, and where its addtion and multiplication coincide with those of $F(R)$. (This is what it means for R to be a *subring* of $F(R)$).

Some of these are more routine than others.

1. Showing that addition is well-defined means showing that if $[a, b] = [a', b']$ and $[c, d] = [c', d']$ for elements a, b, c, d of R, then $[ad+cb, bd] = [a'd'+c'b', b'd']$. This means showing that if $ab' = a'b$ and $cd' = c'd$, then it must follow that $(ad + bc)b'd' = (a'd' + b'c')bd$. To see this:

   $$(ad + cb)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + c'b')bd.$$

   So addition is well-defined.

   To see that multiplication is well-defined, suppose that $[a, b] = [a', b']$ (so $ab' = a'b$) and $[c, d] = [c'd']$ (so $cd' = c'd$). We need to show that $[a, b] \times [c, d] = [a', b'] \times [c', d']$, that is $[ac, bd] = [a'c', b'd']$. This means $acb'd' = a'c'bd$, which is immediate from $ab' = a'b$ and $cd' = c'd$.

2. That addition is commutative and associative is routine to check. The zero element is $[0, 1]$ (which is equal to $[0, b]$ for any nonzero b), and the negative of $[a, b]$ is $[-a, b]$.

3. That multiplication is associative and commutative follows from the fact that the multiplication in R has these properties. The element $[1_R, 1_R]$ is the identity element for multiplication (this is the same as $[b, b]$ for any nonzero $b \in R$).

4. A non-zero element of $F(R)$ has the form $[a, b]$, where a and b are non-zero elements in R. The multiplicative inverse of $[a, b]$ in $F(R)$ is $[b, a]$. The product $[a, b] \times [b, a]$ is $[ab, ab]$, which is equal to $[1, 1]$ when $ab \neq 0$.

5. For any element a of R, we can consider a to be equal to the element $[a, 1]$ of $F(R)$. We note that $[a, 1] + [b, 1] = [a + b, 1]$ and $[a, 1] \times [b, 1] = [ab, 1]$. So the elements $[a, 1]$ of $F(R)$ add and multiply exactly as the elements of R do. Also the elements $[a, 1]$ and $[b, 1]$ are equal in $F(R)$ only if $a = b$ in R. So R is contained in $F(R)$ via the identification $a \leftrightarrow [a, 1]$ for $a \in R$, which respects the addition and multiplication in R and $F(R)$.

Definition 9. *The field* $F(R)$ *is called the* field of fractions *of* R.

Example 10. *The field of fractions of* $\mathbb{Z}$ *is* $\mathbb{Q}$.

Example 11. *The field of fractions of* $\mathbb{Q}[X]$ *is the set of all expressions of the form* $\frac{f(X)}{g(X)}$, *where* $f(X)$ *and* $g(X)$ *are polynomials in* $\mathbb{Q}[X]$ *and* $g(X) \neq 0$, *with the usual addition and multiplication of fractions involving polynomials. This is denoted by* $\mathbb{Q}(X)$ *and called the* function field *in one variable over* $\mathbb{Q}$, *or the* field of rational functions *in one variable over* $\mathbb{Q}$.

Remarks

1. We can think of the element $[a, b]$ of $F(R)$ as meaning the "fraction" $\frac{a}{b}$. What we have proved is that we can define a structure that extends the integral domain R and is a field, in exactly the way that $\mathbb{Q}$ extends $\mathbb{Z}$.

2. $F(R)$ is the smallest field that contains R as a subring, and every field that contains R as a subring must also contain (a copy of) $F(R)$.