1 The Quotient Field

Theorem 1.1

If D is an integral domain (a ring with no zero divisors; it's a ring with multiplicative cancellation), then there exists a field $\mathbb{F}$ that contains D as a subring.

Here are some examples:

1. Consider $\mathbb{Z} \subseteq \mathbb{Q}$. $\mathbb{Z}$ is an integral domain while $\mathbb{Q}$ is a field. We know that the integers look like:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

We can define the rationals like so:

$$\mathbb{Q} := \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\} \right\}$$

Definition 1.1

If D is an integral domain, we can define:

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

We can define an equivalence relation on S by $(a, b) \sim (c, d)$ if and only if $ad = bc$. Then, we can write $F = \frac{S}{\sim}$ and:

$$\frac{a}{b} = [(a, b)] = \{(c, d) \in S \mid (a, b) \sim (c, d)\}$$

Here, we use the operation:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

We call F the field of fractions or the field of quotients of D.

Remarks:

- In $\mathbb{Q}$, we know that $\frac{2}{4} = \frac{1}{2}$. So, we can say that $(2, 4)$ is "equal" to $(1, 2)$.
- The idea is that $\frac{a}{b} = cd \iff ad = bc$.

1.1 Equivalence Relation

We say that $(a, b) \sim (c, d)$ if and only if $ad = bc$.

- Reflexive: $(a, b) \sim (a, b)$ because $ab = ba$ as D is commutative.
- Symmetric: $(a, b) \sim (c, d) \implies ad = bc \implies cb = da \implies (c, d) \sim (a, b)$.
- Transitive: $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f) \implies ad = bc$ and $cf = de$. Then, $adf = bcf \implies adf = bde \implies daf = dbe \implies af = be$ since D is an integral domain. This tells us that $(a, b) \sim (e, f)$ as expected.

Thus, this equivalence relation is well-defined as a set.

1.1.1 Addition Well-Defined

Note that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Remember that, depending on the representation (a, b) of $\frac{a}{b}$, we might get the same values. For example, $\frac{1}{2} = \frac{2}{4}$. So, suppose $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Then:

$$\begin{aligned}
(ad + bc)(b'd') &= adb'd' + bcb'd' \\
&= (ab')dd' + (cd')bb' && \text{Ring is commutative} \\
&= (a'b)dd' + (c'd)(bb') && \text{By the equivalence relation} \\
&= (a'd' + c'b')(bd)
\end{aligned}$$

Thus, $\frac{ad+bc}{bd} = \frac{a'd'+c'b'}{b'd'}$. Finally, if $\frac{a}{b}, \frac{c}{d} \in F$, then $b, d \neq 0$. This implies that $bd \neq 0$ since D is an integral domain. This tells us that $\frac{ad+bc}{bd} \in F$.

1.1.2 Addition Commutative

Here, we have:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b}$$

1.1.3 Addition Associative

This is similar to above.

1.1.4 Additive Identity

The identity is $\frac{0}{1} = \frac{0}{a} \in F$ for all $a \neq 0$. This is because:

$$\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}$$

1.1.5 Additive Inverse

For an element $\frac{a}{b}$, its inverse is $\frac{-a}{b}$. This is because:

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b^2} = \frac{ab - ab}{b^2} = \frac{0}{b^2} = \frac{0}{1}$$

1.1.6 Multiplication Well-Defined

Let $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Then:

$$acb'd' = (ab')(cd') = (ba')(dc') = (a'c')(bd) \implies \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Also, $\frac{a}{b}, \frac{c}{d} \in F$ so $b, d \neq 0$ and thus $bd \neq 0$ since D is an integral domain. Thus, $\frac{ac}{bd} \in F$.

1.1.7 Multiplication Associative

$$\left(\frac{a}{b}\frac{c}{d}\right) = \frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)$$

1.1.8 Multiplication Commutative

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}$$

1.1.9 Multiplication Unity

The unity is $\frac{1}{1} \in F$. This is because:

$$\frac{1}{1}\frac{a}{b} = \frac{1a}{1b} = \frac{a}{b}$$

1.1.10 Multiplicative Inverses

If $\frac{a}{b} \neq \frac{0}{1}$, then $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. Note that:

$$\frac{a}{b} \neq \frac{0}{1} \implies a1 \neq b0$$

In other words, $a \neq 0$ and thus $\frac{b}{a} \in F$. Thus:

$$\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$$

1.1.11 Multiplication Distributive

This is left as an exercise.

1.2 Subring

How is D a subring of F? In $\mathbb{Q}$, we write $\frac{2}{1}$ as 2. Well:

$$a \in D \mapsto \frac{a}{1} \in F$$

In other words, we have a homomorphism.

1.3 Examples of Fields of Fractions

Here are some examples.

1. $\mathbb{Z} \mapsto \mathbb{Q}$.
2. $\mathbb{R}[x] \mapsto \mathbb{R}(x) = \left\{\frac{f(x)}{g(x)} \mid f, g \in \mathbb{R}[x], g \neq 0\right\}$.
3. $\mathbb{F}_p[x] \mapsto \mathbb{F}_p(x) = \left\{\frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}_p[x], g \neq 0\right\}$. Note that $\mathbb{F}_p(x)$ has infinite size and has characteristic p. Additionally, $x + 1 \in \mathbb{F}_p[x]$ has no multiplicative inverse.

2 Ring Homomorphism

Ring homomorphism is very similar in nature to group homomorphisms. Here, a ring homomorphism preserves the ring operations.

Definition 2.1: Ring Homomorphism

A **ring homomorphism** φ from a ring R to a ring S is a mapping from R to S that preserves the ring operation. That is, for all $a, b \in R$:

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \varphi(ab) = \varphi(a)\varphi(b)$$

Remark: As is the case for groups, the operations on the left of the equal signs are those of R, while the operations on the right side are those of S.

Along with ring homomorphisms, there is also ring isomorphisms.

Definition 2.2: Ring Isomorphism

A **ring isomorphism** is a ring homomorphism that is both one-to-one and onto (i.e. bijective).

2.1 Properties of Ring Homomorphisms

Theorem 2.1

Let φ be a ring homomorphism from a ring R to a ring S, and let A be a subring of R and let B be an ideal of S.

1. For any $r \in R$ and any positive integer n, $\varphi(nr) = n\varphi(r)$ and $\varphi(r^n) = (\varphi(r))^n$.
2. $\varphi(A) = \{\varphi(a) \mid a \in A\}$ is a subring of S.
3. If A is an ideal and φ is onto S, then $\varphi(A)$ is an ideal.
4. $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$ is an ideal of R.
5. If R is commutative, then $\varphi(R)$ is commutative.
6. If R has a unity 1, $S \neq \{0\}$, and φ is onto, then $\varphi(1)$ is the unity of S.
7. φ is an isomorphism if and only if φ is onto and $\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\} = \{0\}$.
8. If φ is an isomorphism from R onto S, then φ^{-1} is an isomorphism from S onto R.

2.2 Examples of Ring Homomorphism

Here are some examples of ring homomorphisms.

2.2.1 Example 1: Integers and Modulo

Consider the mapping:

$$k \mapsto k \pmod{n}$$

This is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$, and is called the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.

2.2.2 Example 2: Complex Numbers

Consider the mapping:

$$a + bi \mapsto a - bi$$

This is a ring homomorphism from the complex numbers onto the complex numbers.

2.2.3 Example 3: Functions

Consider the ring of all polynomials with real coefficients $\mathbb{R}[x]$. Consider the mapping:

$$f(x) \mapsto f(1)$$

This is a ring homomorphism from $\mathbb{R}[x]$ onto $\mathbb{R}$.