§1 Lecture 12-02

Theorem 1.1 (Finding a field from an integral domain)
Let D be an integral domain. $\exists$ a field $\mathbb{F}_D$ and an injective homomorphism $\phi : D \to \mathbb{F}_D$ such that every $f \in F_D$ is equal to $\phi(d_1) \cdot \phi(d_2)^{-1}$ for some $d_1, d_2 \in D$.

$\mathbb{F}_D$ is called the field of fractions equal associated to D.

Example 1.2
$\mathbb{Q}[x]$ is not a field, but $\mathbb{Q}(x) = \{p/q : p, q \in \mathbb{Q}[x],\ q \neq 0\}$ is a field.

Example 1.3
If D is a field, then $D = \mathbb{F}_D$.

§1.1 Construction of $\mathbb{F}_D$

We represent a/b as (a, b).

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

Define $\sim$ on S such that $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 b_2 = a_2 b_1$. i.e.

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \quad \text{if and only if} \quad a_1 b_2 = a_2 b_1$$

Proof that $\sim$ is an equiv relation.

1. Reflexive

   $a_1 b_1 = a_1 b_1$

   $(a_1, b_1) \sim (a_1, b_1)$

2. Symmetric

   If $(a_1, b_1) \sim (a_2, b_2)$, then $(a_2, b_2) \sim (a_1, b_1)$

3. Transitive

   If $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, then $(a_1, b_1) \sim (a_3, b_3)$.

$\square$

Claim: $+, \cdot$ are well-defined on $S/\sim$. Proof as an exercise.

Notation:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 b_2}{a_2 b_2}$$

$$(a_1, b_1) + (a_2, b_2) = (a_1 b_2 + a_2 b_1, b_1 b_2)$$
$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

Claim: $(S/\sim, \cdot, +, 0/1, 1/1) \equiv \mathbb{F}_D$ is a field.

with inverses

$$(\frac{a}{b})^{-1} = \frac{b}{a} \quad \text{if} \quad a \neq 0$$
$$-(\frac{a}{b}) = (-\frac{a}{b})$$

Proof. Check associativity, distributivity, commutativity. (Exercise)

$$\frac{0}{1} + \frac{a}{b} = \frac{0b + a1}{b1} = \frac{a}{b} \checkmark$$

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

$$\frac{a}{b} \neq 0 \quad (a \neq 0)$$
$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} \sim \frac{1}{1}$$
$$\Rightarrow \frac{b}{a} = (\frac{a}{b})^{-1}$$

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

□

§1.2 Factorization

Let R be a commutative ring with unity.

Definition 1.4 (Definition of divides, unit, and associate)**.** a divides b if $\exists c \in R$ such that $a \cdot c = b$.

A unit u is an element with an inverse.

a and b are associates if $a = b \cdot u$ for a unit u.

Example 1.5

$$4 = 2 \cdot 2 = (-2) \cdot (-2)$$
$$2 = \underbrace{(-1)}_{\text{unit}} \cdot (-2)$$

Note 1.6. Being associates is an equivalence relation.

$$a = b \cdot u$$
$$\Rightarrow b = a \cdot u^{-1}$$

Example 1.7
In $\mathbb{Z}$, associates are $\pm n$

Definition 1.8 (Irreducible. Prime)**.**

Suppose D is an integral domain.

$p \in D$ non-zero, non-unit is irreducible if $p = ab \Rightarrow a$ is a unit or b is a unit.

p is prime if $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$.

§1.3 Summary

Key take away: Really just trying to do what the rationals did to the integers, but to a general integral domain. This is useful because fields are very easy to work with, while integral domains are not very easy to work with.

What's special about the prime numbers? You can uniquely factor everything into a product of prime numbers. Everything you do with $\mathbb{Z}$ crucially lies on this fact. The question is whether or not you could do this with all general rings. The answer is not always, but many times you can.