Integral Domains and Fraction Field

Def: A zero divisor in a ring R is a nonzero element $a \in R$, for which there exists a nonzero $b \in R$ with either $ab = 0$ or $ba = 0$.

Ex: If $R = \mathbb{Z}_6$, then $2 \in R$ is a zero divisor because $2 \cdot 3 = 0$.

5 is not a zero divisor because if $5x = 0$ then $0 = 5 \cdot 0 = 5(5x) = (5^2) \cdot x = 1 \cdot x = x$.

Ex: If $R = M_2(\mathbb{C})$, then $A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ is a zero divisor because $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ satisfies $BA = 0_R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Def: A commutative ring with no zero divisors is called an <u>integral domain</u>.

Ex: $\mathbb{Z}_n$ is an integral domain if and only if $n = p$

Ex: A field is always an integral domain.

Ex: Let R be a commutative ring. Then $R[x]$ is an integral domain if and only if R is.

Ex: $\mathbb{Z}$ is an integral domain.

Integral domains always live inside fields!

- $\mathbb{Z} \subseteq \mathbb{Q}$
- $\mathbb{Z} \subseteq \mathbb{R}$
- $\mathbb{C}[x] \subseteq \mathbb{C}(x)$

There is a smallest such field, called a field of fractions.

<u>Def</u>: If $R \subseteq F$ and every element of F can be written as ab^{-1} for some $a, b \in R$, then F is called a field of fractions of R.

<u>Ex</u>: $\mathbb{R}$ is <u>NOT</u> a field of fractions of $\mathbb{Z}$. However $\mathbb{Q}$ is!

<u>Ex</u>: Consider $R = \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$. Its field of fractions is $F = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$.

<u>Ex</u>: Consider the ring $R = \mathbb{R}[[x]] = \{\sum_{k=0}^{\infty} a_k x^k \mid a_k \in \mathbb{R}\}$ of formal power series with real coefficients.
A field of fractions is the ring of Laurent series
$L = \mathbb{R}((x)) = \{\sum_{k=-n}^{\infty} a_k x^k \mid a_k \in \mathbb{R}\}$.

Do we always have such a field?

Given an integral domain R, we can build a bigger ring where division is allowed, called its field of fractions.

Start with a set $X = \{(a,b) \in R \times R \mid b \neq 0\}$

with an equivalence relation $\sim$ defined by

$$(a,b) \sim (c,d) \iff ad = bc$$

Let
$$[a,b] = \{(c,d) \in X \mid (a,b) \sim (c,d)\}$$
be the equivalence class of (a,b)

Def: The <u>field of formal fractions</u> $F(R)$ of an integral domain R is the set of equivalence classes

$$F(R) = X/\sim = \{[a,b] \mid a,b \in R, \ b \neq 0\}$$

with binary ops

$$[a_1,b_1] + [a_2,b_2] = [a_1b_2 + a_2b_1, \ b_1b_2]$$
$$[a_1,b_1] \cdot [a_2,b_2] = [a_1a_2, b_1b_2]$$

Theorem: $F(R)$ is a field

Ex: $R = \mathbb{Z}$,

$\mathbb{Q}$

$$[1,2]\cdot[3,7] = [3,14] \qquad \frac{1}{2}\cdot\frac{3}{7} = \frac{3}{14}$$

$$[1,2]+[3,7] = [1\cdot 7+2\cdot 3, 2\cdot 7] = [13,14] \qquad \frac{1}{2}+\frac{3}{7} = \frac{13}{14}$$

Idea: $F(R) \cong \mathbb{Q}$

Proof: $[a,b] \longmapsto \frac{a}{b}$ is a surjective hom. and since $F(R)$ is a field, it is an isom.

Ex: $R = \mathbb{C}[x]$, $F(R) \cong \mathbb{C}(x) = \{ f(x) \mid f(x) \text{ is rational function}\}$

Theorem: If R is an integral domain and $\varphi: R \to K$ is an injective ring homomorphism from R to a field K, then φ extends to a homomorphism $\tilde{\varphi}: F(R) \to K$ satisfying

$$\tilde{\varphi}([r,s]) = \varphi(r)\varphi(s)^{-1} \quad \forall\, r,s \in R, \ s \neq 0.$$

Cor: If K is a field of fractions of R, then $K \cong F(R)$.

Ex: If K is a field, $F(K) \cong K$.

Ex: The Gaussian integers are $R = \{a+ib \mid a,b \in \mathbb{Z}\}$ and $F(R) \cong \{a+ib \mid a,b \in \mathbb{Q}\}$.

Quotient Rings

Def: Let I be an ideal of a ring R. Then the quotient ring of R by I is

$$R/I = \{r+I \mid r \in R\}$$

with binary operations

$$(a+I)+(b+I) = (a+b)+I$$

and

$$(a+I)\cdot(b+I) = ab+I$$

The function $f: R \to R/I$, $f(a) = a+I$ is a ring homomorphism, called the quotient map.