Integral Domains

Def: Let R be a ring. A zero divisor is an element $r \in R$ which is not zero and there is some $0 \neq s \in R$ with $rs = 0$ or $sr = 0$.

Ex: $R = M_2(\mathbb{C})$ $\quad \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Ex: $R = \mathbb{Z}_6$ $\quad$ Then $2 \cdot 3 = 0$ so both 2 and 3 are zero divisors!

Def: A ring R with identity is called an integral domain if it has no zero divisors

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ integral domains (any field is an integral domain)

Ex: $\mathbb{Q}[x]$ is an integral domain

Ex: $\mathbb{Z}_{20}$ $\quad 4 \cdot 5 = 0$, so $\mathbb{Z}_{20}$ has zero divisors!

Ex: $\mathbb{Z}_7$ $\quad 7 \cdot 1 = 0$ but 7 isnt even in $\mathbb{Z}_7$. So no problem

it's an integral domain

Ex: $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime.

Def: The characteristic of a ring R is the gcd of the set $\{n \in \mathbb{Z} \mid nr = 0 \ \forall r \in R\}$.

$\text{char}(\mathbb{R}) = 0 \qquad \text{char}(\mathbb{Z}) = 0 \qquad \text{char}(\mathbb{Z}_n) = n$

<u>Note</u>: $3r = r + r + r \qquad r^3 = r \cdot r \cdot r$

<u>Field of Fractions</u>:

Big idea: if R is an integral domain, we can always find a field F with $R \subseteq F$.

<u>Def</u>: A <u>field of fractions</u> of an commutative integral domain R is a field F containing R where every $c \in F$ is of the form ab^{-1} for some $a, b \in R$.

<u>Note</u>: b^{-1} makes sense in F but not nec. in R.

<u>Ex</u>: $R = \mathbb{Z}$, $F = \mathbb{Q}$ $\qquad \frac{2}{7} = 2 \cdot 7^{-1}$

<u>Ex</u>: $\underbrace{R = \mathbb{Q}[x]}_{\text{ring of polynomials}}$, $\underbrace{F = \mathbb{Q}(x)}_{\text{ring of rational functions}}$

<u>Ex</u>: $R = \mathbb{Q}[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \;\middle|\; a_0, a_1, a_2, \ldots \in \mathbb{Q} \right\}$.

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j} \right) x^n$$

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_n x^n b_m x^m = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j} \right) x^n$$

R is an integral domain!

$$F = \mathbb{Q}((x)) = \left\{ \sum_{n=-l}^{\infty} a_n x^n \;\middle|\; l \in \mathbb{Z}, a_{-l}, a_{-l+1}, a_{-l+2}, \ldots \in \mathbb{Q} \right\}$$

field of formal Laurent series

Theorem: Every integral domain has a fraction field

The proof is constructive:

Start w/ an ~~integral~~ commutative integral domain R + build a field F.

$F_0 = \{(a,b) \mid a,b \in R \text{ and } b \neq 0\}$

Define a relation $\sim$ on F_0 by $(a,b) \sim (c,d)$ iff $ad = bc$

Check: $\sim$ is an equivalence relation!

$(a,b) \sim (a,b)$? $ab = ab$ Yes! Reflexive

if $(a,b) \sim (c,d)$ is $(c,d) \sim (a,b)$?

$ad = bc \Rightarrow cb = da$ Yes! Symmetric

if $(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$

is $(a,b) \sim (e,f)$?

$(ad = bc \ \& \ cf = de) \Rightarrow af = be$

$ad = bc$

$adf = bcf$

$adf = bde$

$d(af - be) = 0$

$\cancel{d = 0}$ $\quad \boxed{af = be}$

Transitive!

Define $F = \{[(a,b)] \mid (a,b) \in F_0\}$

Here $[(a,b)] = \{(c,d) \in F_0 \mid ad = bc\}$

Notation: we write $\frac{a}{b}$ to mean $[(a,b)]$

$[(2r,2s)] = [(r,s)]$ $\qquad \frac{2a}{2b} = \frac{a}{b}$

Rings can be weird. R commutative integral domain

$r, s \in R$ $\quad \frac{r}{s}$??

Equivalence relation: $\frac{rt}{st} = \frac{r}{s}$

Make F into a ring!

$$\left.\begin{aligned} \frac{r}{s} + \frac{r'}{s'} &:= \frac{rs' + r's}{ss'} \\ \frac{r}{s} \cdot \frac{r'}{s'} &:= \frac{rr'}{ss'} \end{aligned}\right\}$$

1) Well-defined
2) $(R, +)$ abelian group
3) $\cdot$ associative
4) distributive props.

Interesting part: are these well-defined?

If $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ and $\frac{r_1'}{s_1'} = \frac{r_2'}{s_2'}$, is $\boxed{\frac{r_1}{s_1} + \frac{r_1'}{s_1'} = \frac{r_2}{s_2} + \frac{r_2'}{s_2'}}$

$r_1 s_2 = r_2 s_1 \qquad r_1' s_2' = r_2' s_1'$

is $\frac{r_1}{s_1} \frac{r_1'}{s_1'} = \frac{r_2}{s_2} \frac{r_2'}{s_2'}$

$$\frac{r_1}{s_1} + \frac{r_1'}{s_1'} = \frac{r_1 s_1' + r_1' s_1}{s_1 s_1'} \qquad \frac{r_2}{s_2} + \frac{r_2'}{s_2'} = \frac{r_2 s_2' + r_2' s_2}{s_2 s_2'}$$

$=?$

$$(r_1 s_1' + r_1' s_1)(s_2 s_2') \overset{?}{=} (r_2 s_2' + r_2' s_2)(s_1 s_1')$$

$$r_1 s_1' s_2 s_2' + r_1' s_1 s_2 s_2' \overset{?}{=} r_2 s_2' s_1 s_1' + r_2' s_2 s_1 s_1'$$

$$r_2 s_1 s_1' s_2' + r_2' s_1' s_1 s_2$$

Multiplication is checked similarly.

What is the zero element of F?

$\frac{0}{1}$ is <u>the</u> zero element of F

<u>NOTE</u>: $\frac{0}{s} = \frac{0}{1}$ because $0 \cdot 1 = 0 \cdot s$

$0 = 0$

Why do we avoid zero divisors?

S'pose R is commutative w/ identity and $z \in R$ is a zero divisor

<u>Claim</u>: the binary operations are not well defined

<u>Proof</u>: Take $0 \neq w \in R$ w/ $zw = 0$

$\frac{z}{z} \cdot \frac{w}{w} = \frac{0}{0} \longleftarrow$ not in F.