Types of Rings

Fields = very nice rings, where

every nonzero element is invertible

and multiplication is commutative.

Matrices = not so nice rings, where

the multiplication is not

commutative and $\exists$ elements

that are nonzero, yet square

to zero!

What's in between these examples?

Principal Ideals

Let R be a ring.

$I \subseteq R$ an ideal is **principal** if $\exists$

$x \in R$, $I = \langle x \rangle$

where $\langle x \rangle$ = the smallest

ideal of R containing x.

Theorem: (commutative, unital case) If R is a commutative and unital ring, then if $I = \langle x \rangle$ for $x \in R$, then

$$I = \{xy \mid y \in R\}.$$

proof: Let $J = \{xy \mid y \in R\}$.

First, prove that J is an ideal containing x.

If so, then by definition,

$I \subseteq J$.

Note: If $\{I_\alpha\}_{\alpha \in S}$ is any collection of ideals, then

$\bigcap_{\alpha \in S} I_\alpha$ is also an ideal.

Then if $x \in R$,

$$\boxed{\langle x \rangle = \bigcap_{\substack{I \text{ ideal in } R \\ x \in I}} I}$$

J is an ideal

Let $z \in R$, $t \in J$.

Then $\exists\ y \in R$,

$$t = xy.$$

But then since R is commutative,

$$zt = tz = (xy)z = x\cdot(y\cdot z) \in J$$

Taking $z \in J$ gives the closure under multiplication for J.

Now let $t, q \in J$. Then

$\exists\ y, p \in R$,

$$t = xy$$

$$q = xp$$

Then

$$t - q = xy - xp = x(y-p) \in J$$

So J absorbs elements of R

and passes the subring test

provided $J \neq \emptyset$.

But since R is unital,

$$x = x \cdot 1_R \in J$$

$$\Rightarrow J \neq \emptyset.$$

Therefore, J is an ideal containing x, so by definition, $I \subseteq J$ since I is the smallest ideal containing x.

But since $x \in I$ and I is an ideal, $x \cdot y \in I$ $\forall\, y \in R \Rightarrow J \subseteq I$.

Therefore, we have equality:

$$I = J$$

$$\langle x \rangle = \{xy \mid y \in R\}$$

$\square$

Definition: (integral domain) A ring R is said to be an **integral domain** if R is commutative and unital, and

$$\boxed{x \cdot y = 0_R \Rightarrow x = 0_R \text{ or } y = 0_R}$$

$\forall\, x, y \in R$.

Example 1: ($K[x]$) If K is a field, then $K[x]$ is an integral domain but not a field!

If $p(x), q(x) \in K[x]$,

$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$$

("deg" = degree of)

Then if $p(x) \cdot q(x) = 0$ and $p(x) \neq 0$, $q(x) \neq 0$, then

$$\deg(p(x) \cdot q(x)) \geq \deg(p(x)) \neq -\infty$$

$$\deg(p(x) \cdot q(x)) \geq \deg(q(x)) \neq -\infty$$

Therefore, $p(x)\cdot q(x) \neq 0$.

So if the product of two polynomials is zero, one of the polynomials has to be zero. Since we already knew $k[x]$ was unital and commutative, $k[x]$ is an integral domain.

However, $p(x) \in k[x]$ is invertible if and only if $\deg(p(x)) = 0$, i.e., $p(x) \in k^{\times}$.

So $k[x]$ is not a field.

Definition: (Principal Ideal Domain)

A ring R is called a **principal ideal domain** if R is an integral domain and every ideal of R is principal.

Example 2: Take $R = \mathbb{Z}$. Then R is an integral domain ($m \cdot n = 0 \Rightarrow m = 0$ or $n = 0$) and we've shown that if $H \leq (\mathbb{Z}, +)$, then H is generated as a subgroup by some $n \in \mathbb{Z}$:

$H = \langle n \rangle$ as a subgroup.

Then if I is an ideal of $\mathbb{Z}$, we know that $(I, +) = \langle n \rangle$ for some $n \in \mathbb{Z}$ as a subgroup.

But then $I = \langle n \rangle$, and

moreover, $\forall\ m \in \mathbb{Z}$,

if $r \in I$, $\exists\ k \in \mathbb{Z}$,

$r = k \cdot n$. Then

$$m \cdot r = m \cdot (k \cdot n) = (m \cdot k) \cdot n \in \langle n \rangle$$

$\Rightarrow \langle n \rangle$ is an ideal.

Therefore, every ideal in $\mathbb{Z}$

is principal, so $\mathbb{Z}$ is

a principal ideal domain.

Definition: (prime, irreducible elements)

Let R be an integral domain. Then $x \in R$ is said to be irreducible if whenever one writes $x = y \cdot z$ for $y, z \in R$, then either $y = x \cdot u$ where u is a unit of R or $z = x \cdot u$.

We say x is prime if for any $y, z \in R$, if $\exists\ t \in R$ with

$y \cdot z = t \cdot x$, then

$\exists\ s \in R$ with either

$y = s \cdot x$ or $z = s \cdot x$.

Note: in R, these terms are identical.

Prime Ideals

Let R be a commutative ring.

Then an ideal I of R is said to be prime if whenever $x, y \in R$ and $x \cdot y \in I$, then $x \in I$ or $y \in I$.

Observation: ($\mathbb{Z}$) Prime ideals are all of the form $I = \langle p \rangle$ for some prime $p \in \mathbb{N}$ (or $I = \{0\}$)

Theorem: (R/I for I prime)

If R is commutative and unital, then I an ideal of R is prime if and only if R/I is an integral domain.

proof: $\Rightarrow$ Suppose R is prime and that $x, y \in I$,

$$\underbrace{(x+I)(y+I)} = I \quad (\text{zero in } R/I)$$

$$xy + I = I$$

$$\Rightarrow xy \in I$$

Since I is prime,

either x or y is in I.

Then if $x \in I$,

$x+I = I$, and if

$y \in I$,

$y+I = I$, so

R/I is an integral domain

$\Leftarrow$ if R/I is an integral domain,

$x, y \in R$, and $x \cdot y \in I$,

then

$$\underbrace{(x \cdot y)+I}_{(x+I)(y+I)} = I$$

$$(x+I)(y+I) = I$$

$\Rightarrow$ either $x + I = I$ $(x \in I)$

or $y + I = I$ $(y \in I)$

$\square$

Corollary: (maximal $\Rightarrow$ prime) Every maximal ideal in a commutative, unital ring is prime.

proof: If $I \subsetneq R$ is maximal, then R/I is a field, and so is an integral domain. By the previous theorem, I must be prime.

$\square$