$r0 = 0$
$rI \subseteq I$

Ideal: $5\mathbb{Z} \subseteq \mathbb{Z}$

$3(5\mathbb{Z}) = 15\mathbb{Z} \subseteq 5\mathbb{Z}$
$rI \subseteq I$

Sections 7.3, 7.4 Homomorphisms, Quotients, Ideals

Recall An *ideal* $I \subseteq R$ is a subring for which $rI \subseteq I$ and $Ir \subseteq I$

Left ideal $I \subseteq R$ " " " " $rI \subseteq I$.
Right ideal $I \subseteq R$ " " " " $Ir \subseteq I$.

Given an ideal $I \subseteq R$, $R/I = \{r + I \mid r \in R\}$ is a ring with operations $(r+I) + (s+I) = (r+s)+I$, $(r+I)(s+I) = rs + I$.
Addition identity is I.

Theorem 7 (First Isomorphism Theorem for Rings)

Suppose $\varphi : R \longrightarrow S$ is a ring homomorphism. Then:
- $\ker\varphi$ is an ideal in R, and $R/\ker\varphi \cong \varphi(R) \subseteq S$.
- $\varphi = \theta \circ \pi$ in following diagram, and θ is an isomorphism.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \varphi(R) \subseteq S \\ R/\ker\varphi \arrow[ur, "\theta"', "\sim"] & \end{tikzcd}$$

$$r \longmapsto \varphi(r), \qquad r \longmapsto r + \ker\varphi \longmapsto \varphi(r)$$

Also, if $I \subseteq R$ is any ideal, then it is the kernel of the homomorphism $\pi : R \longrightarrow R/I$, $\pi(r) = r + I$.

Example $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}$ $\quad \varphi(f) = f(0)$ (eval. homo.)

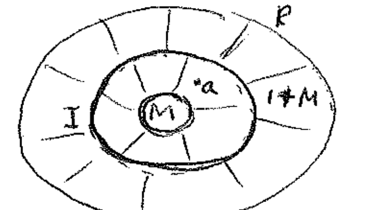
$\ker\varphi = \{0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid a_i \in \mathbb{R}, n \geq 1\}$

$\mathbb{R}[x]/\ker\varphi \cong \mathbb{R}$.

In this example, the kernel takes up "almost all" of $\mathbb{R}[x]$. In fact there is no larger proper ideal $I \subseteq \mathbb{R}[x]$ with $\ker\varphi \subset I \subseteq \mathbb{R}[x]$

Definition An ideal $M \subseteq R$ is *maximal* if there is no ideal I with $M \subsetneq I \subsetneq R$.

Proposition 11 In a ring with 1, every ideal is contained in some maximal ideal.



Note M not maximal
$\Leftrightarrow \exists\ M \subset I \subset R$
$\Leftrightarrow \exists\ a \in I - M$
$\Leftrightarrow (a+I)(r+I) = ar + I \neq 1 + I \ \forall r$

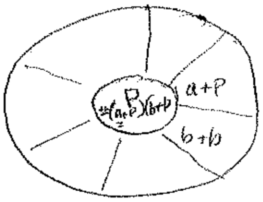
Proposition 12 Suppose R commutative. Then M maximal $\Leftrightarrow R/M$ is a field.

Definition An ideal P in a commutative ring R is **prime** if $\forall a, b \in R$, $ab \in P \Rightarrow a \in P$ or $b \in P$.

$p \in \mathbb{Z}^+$ is prime if ...... $ab = p \Rightarrow a = p$ or $b = p$

Ex $8\mathbb{Z}$ not prime in $\mathbb{Z}$. $6, 4 \notin 8\mathbb{Z}$, $6 \cdot 4 = 24 \in 8\mathbb{Z}$,
$5\mathbb{Z}$ is prime in $\mathbb{Z}$. If $ab \in 5\mathbb{Z}$ then one of a, b is a multiple of 5.

Proposition 13 Suppose R is commutative. Then
P is a prime ideal in $R \iff R/P$ is an integral domain.



R/P not ID $\iff$ P not prime

By previous two propositions every maximal ideal is prime.
M maximal $\iff R/M$ field $\Rightarrow R/M$ I.D. $\iff M$ Prime,
Not every prime ideal is maximal:

Example $P = \{a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{Z}\} \subseteq \mathbb{Z}[x]$
is prime because $\mathbb{Z}[x]/P \cong \mathbb{Z}$ is an integral domain.
Its not maximal, as follows:
$P \subset \{2a_0 + a_1x + a_2x^2 + \dots + a_nx^n\} \in \mathbb{Z}[x]$.

Definition If $a \in R$, the principal ideal generated by a is

$$(a) = \{\sum_{i=1}^{k} r_i a s_i \mid k \in \mathbb{Z}^+, r_i, s_i \in R\}$$

This is the smallest ideal containing a. If R is commutative

$$(a) = \{ra \mid r \in R\}$$

Example $5 \in \mathbb{Z}$ $\quad (5) = 5\mathbb{Z}$ $\quad x \in (5) \iff 5 \mid x$

$a \in R$ $\quad x \in (a) \iff a \mid x$

Principal ideals are key instruments in describing "arithmetic" in rings.
Ex $(x) = \{0 + a_1x + a_2x^2 + \dots + a_kx^k\} \subseteq \mathbb{R}[x]$ $\quad (x) = \ker\varphi$, $\varphi: \mathbb{R}[x] \to \mathbb{R}$, $\varphi(f) = f(0)$.

Ideals Generated by sets

Definition If $A \subseteq R$, then the ideal generated by A is

$$(A) = \bigcap_{\substack{A \subseteq I \subseteq R \\ I \text{ is ideal}}} I = \left\{ \sum_{i=1}^{k} r_i a_i s_i \;\middle|\; k \in \mathbb{Z}^+,\ a_i \in A,\ r_i, s_i \in R \right\}$$

$$= \text{(smallest ideal containing } A\text{)}$$

This is the smallest ideal containing A. If R is commutative, then

$$(A) = \bigcap_{A \subseteq I \subseteq R} I = \left\{ \sum_{i=1}^{k} r_i a_i \;\middle|\; k \in \mathbb{Z}^+,\ a_i \in A,\ r_i \in R \right\}.$$

r