Homomorphism: $\varphi: R \to R'$.

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1) = 1.$$

Example: $\varphi: \mathbb{Z} \to \mathbb{F}_p$

Prop: There is exactly one homomorphism $\mathbb{Z} \to R$.

$\varphi: R \to R'$.

$\ker\varphi = \{ s \in R \mid \varphi(s) = 0 \}$.

Property of $\ker(\varphi)$:

1. closed under addition
2. If $s \in \ker(\varphi)$. then $rs \in \ker(\varphi)$ for all $r \in R$.

Ex: evaluation map

$$\mathbb{R}[x] \to \mathbb{R}$$
$$p(x) \mapsto p(a).$$

Prop (substitution principle)

$\varphi : R \to R'$ ring homomorphism.

$\forall \alpha \in R'$, there is a unique homomorphism

$\Phi : R[x] \to R'$, such that

$$\Phi(x) = \alpha.$$

More generally. $\forall \alpha_1, \alpha_2, \cdots \alpha_n$.

$\exists! \Phi : R[x_1, \ldots x_n] \to R'$. such that

$$\Phi(x_i) = \alpha_i.$$

Ex: $R \xrightarrow{\varphi} R' \hookrightarrow R'[x]$. (change of coefficients)

$$x \mapsto x.$$

$$f(x) = \sum a_i x^i \mapsto \sum \varphi(a_i) x^i$$

Defn: (Ideal) $I \subset R$.

① closed under addition

② If $s \in I$, $r \in R$, then $rs \in I$.

If $s_1, s_2, \ldots s_n \in I$, then

$\sum r_i s_i \in I$, $\forall r_1 \cdots r_n \in R$.

Defn: (Ideal generated by $s_1 \ldots s_n$)

$$I = \{ \sum r_i s_i \mid r_i \in R \} = (s_1, \ldots s_n)$$

principal ideal: $(a) = Ra = \{ ra \mid r \in R \}$.

(0) zero

(1) unit ideal $= R$.

proper neither (1) or (0)

Prop:

ⓐ Field F has exactly two ideals (0) and (1)

ⓑ any ring has only two ideals is a field.

Ideals in $\mathbb{Z}$,

Any subgroup in $\mathbb{Z}^+$ is an ideal.

$$n \cdot x = x + \cdots + x.$$

Classification of subgroups in $\mathbb{Z}^+$, (n).

all ideals are principal. ($I \subset \mathbb{Z}$, Find $x \in I$, $x \neq 0$. with minimal $|x|$)

Ideals in $F[x]$. F is a field.

any ideal in $F[x]$ is principal.

Find $0 \neq f(x) \in I$, such that.

$f(x)$ has minimal deg

G.C.D (Greatest common divisor) $f, g \in F[x]$.

$$(f, g) = (d(x))$$

a). $(d) = (f, g)$.

b) d divides f, d divides g.

c). If $e = e(x)$ divides f and g then $e(x)$ divides $d(x)$

d) $\exists\, p, q$, s.t. $d(x) = f \cdot p + g \cdot q$

use Euclidean algorithm to find $d(x)$.

$f(x) = x^2 - 2x - 3 = (x-3)(x+1)$

$g(x) = (x-3)(x^2+x+1)$

$= x^3 - 2x^2 - 2x - 3$.

$g(x) = x(x^2-2x-3) + (x-3)$

$(f, g) = (f, r) = (0, x-3) = (x-3)$

Quotient ring. R/I.

$R/I = R^+/I^+ = \{a + I \mid a \in I\}$

Defn and Thm: There is a unique ring structure on R/I, s.t. $R \to R/I$ is a ring homomorphism.

Defn: $(a+I)(b+I) = ab+I$.

check well-defined.

$$\begin{aligned} a+I &= a'+I \\ b+I &= b'+I \end{aligned} \quad \text{then} \quad \begin{aligned} a &= a'+u \\ b &= b'+v \end{aligned} \quad u,v \in I.$$

$$ab = a'b' + \underbrace{ub' + va' + uv}_{\in I}.$$

First isomorphism Thm:

If $f: R \to R'$ surjective ring homo

then $R/I \xrightarrow{\sim} R'$. $I = \ker f$.

Mapping property. If $f: R \to R'$ ring homo with $\ker f = K$. $\pi: R \to R/I$.

a) If $I \subset K$, then $\exists!\ \bar{R} = R/I \to R'$.

s.t. $\bar{f}\pi = f$.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & R' \\ R/I \arrow[ur, dotted, "\bar{f}"'] & \end{tikzcd}$$

b) If $K = I$, $\bar{f}$ is isomorphism and f surjective.

Thm (Correspondence Thm)

$\varphi : R \to R'$ is surjective ring homomorphism. $K = \ker\varphi$

$\{$ ideals in R containing $K \}$

$\longleftrightarrow \{$ ideals in $R' \}$

- If $I \supset K$, then $\varphi(I)$ is an ideal in R'
- If $\bar{I}$ is an ideal in R', then

$\varphi^{-1}(\bar{I})$ is an ideal in R.

step 1. $\varphi(I)$ is an ideal in R'.

$\varphi^{-1}(\bar{I})$ is an ideal in R

$\varphi(\varphi^{-1}(\bar{I})) = \bar{I}$. $\quad \varphi^{-1}(\varphi(I)) = I$