1st isomorphism theorem.

$f: R \to R'$ surjective. ring hom.

$R/I \to R'$ isomorphism. $I = \ker f$

Other version:

$f: R \to R'$. Image of f, $\mathrm{Im} f$ is a subring of R'

$R/I \to \mathrm{Im} f$ is ring isomorphism.

Thm (correspondence Thm)

$\varphi: R \to R'$ surjective ring hom.

$K = \ker \varphi$.

$\{\text{Ideals in } R \text{ containing } K\} \xleftrightarrow{1:1} \{\text{Ideals in } R'\}$.

$I \longmapsto \varphi(I)$

$\varphi^{-1}(\tilde{I}) \longleftarrow \tilde{I}$

a) If $\boxed{I \supset K}$, then $\varphi(I) = \{\varphi(s) \mid s \in I\}$ is an ideal in R'.

b) • If $\tilde{I}$ is an ideal in R', then

$$\varphi^{-1}(\tilde{I}) = \{ s \in R \mid \varphi(s) \in \tilde{I} \}.$$

is an ideal in R

Pf: Step 1 verify a), b).

Step 2. $\varphi(\varphi^{-1}(\tilde{I})) = \tilde{I}$.

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

Step 1: a) I an ideal in R,

$\varphi(I)$ addition subgroup of R'.

If $r' \in R'$, $s \in I$. $\underbrace{r' \cdot \varphi(s)}$

since φ surjective, $r' = \varphi(r)$ for some $r \in R$.

$r'\varphi(s) = \varphi(r) \cdot \varphi(s) = \varphi(\underset{\substack{\uparrow \\ I}}{r \cdot s}) \in \varphi(I)$ because $r \in R$, $s \in I$.

b) check it.

Step 2: $\varphi^{-1}(\varphi(I)) = I$.

"$I \subset \varphi^{-1}(\varphi(I))$".

$s \in I$, then $\underline{\varphi(s)} \in \underline{\varphi(I)}$. So $s \in \varphi^{-1}(\varphi(I))$

($\varphi(s) \in A$, then $s \in \varphi^{-1}(A)$)

"$\varphi^{-1}(\varphi(I)) \subset I$".

$s \in \varphi^{-1}(\varphi(I)) \Rightarrow \underline{\varphi(s) \in \varphi(I)}$.

$\Rightarrow \varphi(s) = \varphi(r)$ for some $r \in I$,

$\Rightarrow \varphi(s-r) = 0$, $s - r \in \ker\varphi \subset I$.

So $s = \underbrace{(s-r)}_{\in I} + \underbrace{r}_{\in I} \in I$.

Classify ideals in some rings.

Division with remainder + correspondence Thm.

$\mathbb{Z}$, $R[x]$.

Ex: $\mathbb{Z}$, What are the ideals.

Claim: all the ideals in $\mathbb{Z}$ are principal.

i.e. $I = (a)$ $a \in \mathbb{Z}$. $a \cdot \mathbb{Z}$

$= \{am \mid m \in \mathbb{Z}\}$.

Pf: I ideal of $\mathbb{Z}$.

Look for $a \in \mathbb{Z}$, s.t. a has the minimal absolute value.

$I = \{0\}$

Define $a = \min \left\{ |n| \,\middle|\, \begin{array}{l} n \in I \\ n \neq 0 \end{array} \right\}$.

① $a \in I$, because $a = \pm n$ for some $n \in I$

② If $b \in I$, $b = a \cdot m + r$, $m, r \in \mathbb{Z}$.

$|r| < a$.

$\Rightarrow r = \underset{\substack{\Uparrow \\ I}}{b} - \underset{\substack{\Uparrow \\ I}}{am} \in I$. $|r| < a$. $r = 0$.

$b = am$. $I = (a)$.

(Rmk: R has two ideals $\{0\}$, R)

Ex: $\mathbb{Z}/n\mathbb{Z}$, $f: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

$\underline{\{\text{ideals of } \mathbb{Z}/n\mathbb{Z}\}} \longleftrightarrow \underline{\{\text{ideals of } \mathbb{Z} \text{ containing } \ker f = n\mathbb{Z}\}}$.

$(a) \supset (n)$, $\Leftrightarrow$ $n \in (a)$.

$n = ab$. a is a divisor of n.

$n = 6$, $\underline{\mathbb{Z}/6\mathbb{Z}}$

n has divisors $1, 2, 3, 6$.
$-1, -2, -3, -6$

$(2) = (-2)$, $(3) = (-3)$, $(6) = (-6)$, $(1) = (-1)$

ideals in $\mathbb{Z}/6\mathbb{Z}$ are $\underline{(1)/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}}$

$\underline{(2)/(6)}$, $\underline{(3)/(6)}$, $\underline{(6)/(6) = \{0\}}$.

Useful facts:

$I = (a)$, $J = (b)$.

$I \subset J$ iff b divides a.

$a = b \cdot s$ for some $s \in R$.

Ex: $\mathbb{C}[t]$.

Every ideal in $\mathbb{C}[t]$ is principal.

(PWR).

pf: I ideal in $\mathbb{C}[t]$,

$I \neq (0)$

then look at $\{ \deg p(x) \mid p(x) \in I, \ p(x) \neq 0 \}$.

has a minimal $= a$.

assume $\deg f(x) = a$.

Claim: $I = (f(x))$

$g(x) \in I$, $g(x) = f(x) \cdot q(x) + r(x)$

$\deg r(x) < \deg f(x)$.

$$r(x) = \underset{\substack{\cap \\ I}}{g(x)} - \underset{\substack{\cap \\ I}}{f(x) \cdot q(x)} \in I.$$

$r(x) = 0, \quad g(x) = f(x) \cdot q(x)$

$\Rightarrow \quad I = (f(x)).$

Ex: $\quad \mathbb{C}[t] / (t^2 - 1)$

ideals are from ideals of

$\mathbb{C}[t]$ containing $(t^2 - 1)$.

$(f(x)) \supset (t^2 - 1)$

$f(x)$ divides $t^2 - 1$.

$f(x) = 1, \quad t-1, \quad t+1, \quad t^2 - 1$

$\mathbb{C}[t] / (t^2 - 1)$ has four ideals

Ex: How to find kernel.

$$\varphi : \mathbb{C}[x, y] \to \mathbb{C}[t].$$
$$x \mapsto t.$$
$$y \mapsto t^2.$$
$$a \in \mathbb{C} \mapsto a$$

any $f(x,y)$ is mapped to $f(t,t^2)$

$\ker\varphi$? $g(x,y) \in \ker\varphi$

$g(t,t^2) = 0.$

① $y-x^2 \in \ker\varphi.$ $(y-x^2) \subset \ker\varphi.$

② Claim $(y-x^2) = \ker\varphi.$

DWR: $g(x,y) \in \mathbb{C}[x][y]$

$$\underbrace{g(x,y)}_{\ker\varphi} = \underbrace{(y-x^2)\cdot q(x,y)}_{\in\ker\varphi} + r(x,y)$$

deg of $r(x,y)$ in y < deg of $(y-x^2)$ in y. $=1$

deg of y in $r(x,y) < 1.$

$r(x,y) = r(x).$

$r(x,y) \in \ker\varphi.$ $r(t,t^2)=0$

$r(t)=0.$

$r=0.$ so $g(x,y) = (y-x^2)\, q(x,y)$

Correspondence theorem:

$$\varphi : \mathbb{C}[x, y] \to \underline{\mathbb{C}[t]}$$

$$\ker \varphi = (y - x^2) \qquad \tilde{I} = (f(t)).$$

$$\varphi^{-1}(\tilde{I}) = (f(x), y - x^2)$$

From correspondence

$$I \longrightarrow \varphi(I) = (f(t))$$

If we find I, such that

$\varphi(I) = (f(t)) = \tilde{I}$, and $I \supset \ker\varphi$.

then $I = \varphi^{-1}(\tilde{I})$

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

Cor:

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

$K = \ker \varphi$.

$$\left\{ \begin{matrix} I \supset K \\ I \text{ ideal in } R. \end{matrix} \right\} \xleftrightarrow{1:1} \{ \tilde{I} \text{ ideal in } R' \}.$$

$$R/I \xrightarrow{\cong} R'/\tilde{I}.$$

Pf: $f: R \xrightarrow{\varphi} R' \longrightarrow R'/\tilde{I}$.

$$\ker f = \varphi^{-1}(\tilde{I})$$
$$= I.$$

so $R/I \cong R'/\tilde{I}$.

adding relations.

~~Adjoining elements~~. (Quotient step by step)

$$R/(a,b) \cong \left. R/(a) \middle/ (\bar{b}) \right.$$

$\bar{b} = b + (a)$ in $R/(a)$

$\varphi : R \longrightarrow R/(a)$

$\varphi^{-1}(\bar{b}) = (a, b)$

(same argument in the example

$\mathbb{C}[x, y] \to \mathbb{C}[t]$

$x \longmapsto t$

$y \longmapsto t^2$).

$R/(a, b) \cong R/(a) \big/ (\bar{b})$

Ex: $\mathbb{Z}[i]$ ring of Gauss integers. $i^2 = -1$.

$\mathbb{Z}[i] = \{ a + bi \mid a \cdot b \in \mathbb{Z} \}$.

$a + bi + c \cdot i^3 + d \, i^4$

$= a + bi + c \cdot (-1) \cdot i + d \cdot (-1)^2$

$= \underline{a + d} + \underline{(b - c)} i$.

$\mathbb{Z}[i]$ is a ring. (subring of $\mathbb{C}$)

$\mathbb{Z}[i] / (i-2)$??

Observation. $\mathbb{Z}[i] \cong \mathbb{Z}[x] / (x^2+1)$.

why? $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$.

$x \mapsto i$.

$\ker \varphi = (x^2+1)$ (Proved by DWR)

if $g(x) \in \ker \varphi$.

$\underline{g(x) = (x^2+1) q(x) + r(x)}$

$\deg r(x) \leq 1$. $r(x) \in \mathbb{Z}[x]$.

$r(i) = 0$, but $i \notin \mathbb{Z}$.

$r(x) = 0$, $g(x) = (x^2+1) q(x)$

$$\mathbb{Z}[i] / (i-2) \cong \frac{\mathbb{Z}[x] / (x^2+1)}{(x-2)}$$

$$\cong \mathbb{Z}[x] / (x^2+1,\ x-2)$$

$$\cong \mathbb{Z}[x]/(x-2) \Big/ (x^2+1)$$

$$\mathbb{Z}[x]/(x-2) \cong \mathbb{Z}.$$

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}.$$
$$x \longmapsto 2.$$

$$\cong \mathbb{Z}/(2^2+1) \cong \mathbb{Z}/5\mathbb{Z}.$$