* If $\phi : R \to S$ is a surjective homomorphism and $\ker\phi = \{0\}$, then $\phi$ is an isomorphism:

Pf: Need to show injectivity, so take $\phi(r_1)$ & $\phi(r_2)$

Suppose $\phi(r_1) = \phi(r_2)$ [Want to show $r_1 = r_2$ in $R$].

Note $\underline{\phi(r_1) - \phi(r_2)} = 0$, So.... $\phi(r_1 - r_2) = 0$

$r_1 - r_2 = 0 \Rightarrow r_1 = r_2$, hence $\phi$ is injective.

Conclude $\phi$ is an iso$^{m/}$. ∎

* $\ker\phi \subset R$ is an ideal of $R$, Let $r_1, r_2 \in \ker\phi < R$

Check $r_1 - r_2 \in \ker\phi$. Form $\phi(r_1 - r_2)$ & see if that is $0$ in $S$. $\phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0 - 0 = 0$

Hence $r_1 - r_2 \in \ker\phi$

Now take $r \in \ker\phi$ and $x \in R$.

Consider $\phi(rx) = \phi(r)\phi(x) = 0 \cdot \phi(x) = 0$

So $rx \in \ker\phi$ and hence $\ker\phi < R$ is an ideal ∎

5. Show that mapping $x \xrightarrow{\phi} 5x$ from $\mathbb{Z}_5$ to $\mathbb{Z}_{10}$

is/is not homo$^{my}$

$\phi(\underline{2+4}) = \phi(\underline{6}) = \phi(1) = 5$,

$\phi(2) + \phi(4) = 0 + 0$

So.... $\phi(2+4) \neq \phi(2) + \phi(4)$ so, no!

9. Given field $\mathcal{F}$, let $F_\alpha \subset \mathcal{F}$ be a subfield, then

$\bigcap_{\alpha \in \Lambda} F_\alpha$ is a subfield of $\mathcal{F}$.

Subfield Test: Check $a-b$ & $ab^{-1}$ ($\underline{b \neq 0}$) in intersection for arbitrary $a, b$

Note since $a$ & $b$ are in intersection, they are in every $F_\alpha$. Because every $F_\alpha$ is a subfield, $a-b$ and $ab^{-1}$ belong to <u>every</u> $F_\alpha$. But this is enough to conclude

$a-b,\ ab^{-1} \in \bigcap_{\alpha \in \Lambda} F_\alpha$. ∎

Prop. $\forall\, n,m \in \cancel{\mathbb{Z}}\ \mathbb{N}$ w/ $m \neq n$, $n\mathbb{Z} \not\cong m\mathbb{Z}$

<u>Proof:</u> Suppose FSOC that $n\mathbb{Z} \cong m\mathbb{Z}$ for $m \neq n$.
Then $\exists\ \phi : n\mathbb{Z} \to m\mathbb{Z}$ s.t. $\phi$ is bijective & op. preserving.

So $\phi(n) = m$ since $\phi$ is surjective.
since generators map to generators.

In general $\phi(nx) = mx$.

Let $x = n$,

$$\phi(nn) = mn$$

But $\phi(nn) = \phi(n)\phi(n)$ by prop of homomorphism.

So $\phi(n) \cdot \phi(n) = mm = mn$.

Cancellation gives $m = n$ $\Rightarrow\Leftarrow$ since $m \neq n$.

Therefore, $n\mathbb{Z} \not\cong m\mathbb{Z}$. $\square$

* Let $\phi : R \to S$ be a ring homo$^{m/y}$
Show $\phi$ takes idempotents to idempotents
Idempotent : $a^2 = a$ for $a \in R$

Want to show $\phi(a)\cdot\phi(a) = \phi(a)$ in $S$.

$$\phi(a^2) = \phi(a)\cdot\phi(a) = [\phi(a)]^2$$

$$\downarrow$$

$$\phi(a)$$

* Show in a PID $R$, if $\phi : R \to S$ is homo$^{m/y}$

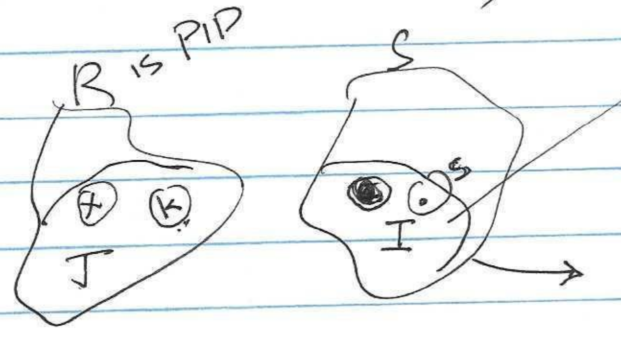
Want to show $S$ is PID.

Take ideal $I \subset S$ by Th$^m$ 15.1(4) $\phi^{-1}(I) = J$, an ideal in $R$.

By assumption $J = \langle k \rangle$. So pick $s \in I$

Must show $s \in I$ is <u>some</u> multiple of single generator.

$s = \phi(x)$ for some $x \in J$, but $x = k\bar{x}$




, generator of $I$ is $\phi(k)$

$\phi(x) = s$

$x = k\bar{x}$

★ Let $R$ be a commutative ring with prime characteristic $p$. Show the "Frobenius map" $x \overset{\phi}{\mapsto} x^p$ is a ring homomorphism (endomorphism).

Show $\phi(x+y) = \phi(x) + \phi(y)$

, $\phi(xy) = \phi(x)\phi(y)$

(i) $\phi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$

$= x^0 y^p + \cdots (p) + + \cdots x^p y^0$

$\phi(x) + \phi(y) = x^p + y^p = x^p + y^p$

$\phi(xy) = (xy)^p = x^p y^p \overset{?}{=} \phi(x)\phi(y) = x^p y^p$

same

$\binom{p}{1} = \frac{p!}{(p-1)!\,1!} = p$

$\binom{p}{2} = \frac{p!}{(p-2)!\,2!} = \frac{p(p-1)}{2}$