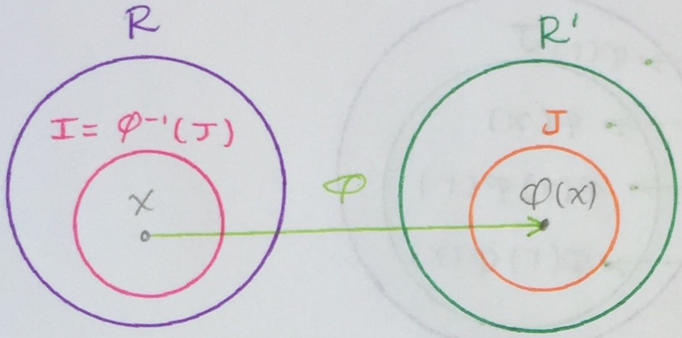
Tuesday, Week 12 April 18. 2017

Tuesday's Special

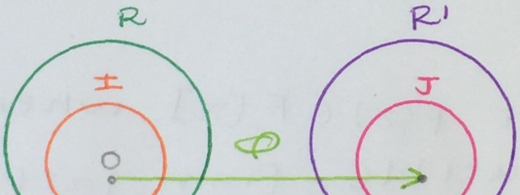
Let R and R' be rings with additive identities 0 and $0'$. Let $\varphi : R \to R'$ be a ring homomorphism. Let J be an ideal of R'.

Prove that $I = \varphi^{-1}(J) = \{x \in R \mid \varphi(x) \in J\}$ is an ideal of R.



Proof of Tuesday's Special

- Since φ is a homomorphism we know $\varphi(0) = 0'$ and since J is an ideal of R', we know $0' \in J$ so $\varphi(0) \in J$. Thus, $0 \in I$



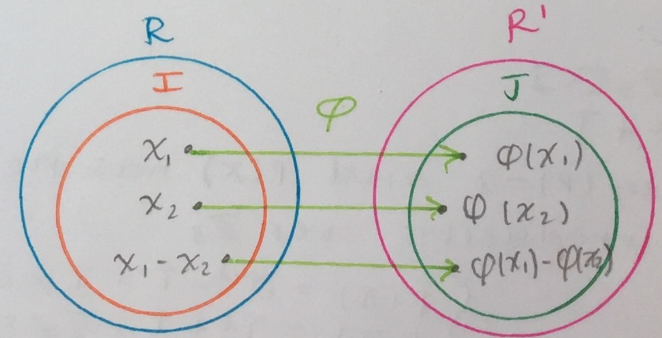
- Let $x_1, x_2 \in I$. so, $\varphi(x_1) \in J$ and $\varphi(x_2) \in J$. since J is an ideal $\varphi(x_1) - \varphi(x_2) \in J$.

since φ is a hom.

$\varphi(x_1 - x_2) = \varphi(x_1) - \varphi(x_2)$

so $\varphi(x_1 - x_2) \in J$

so $x_1 - x_2 \in I$

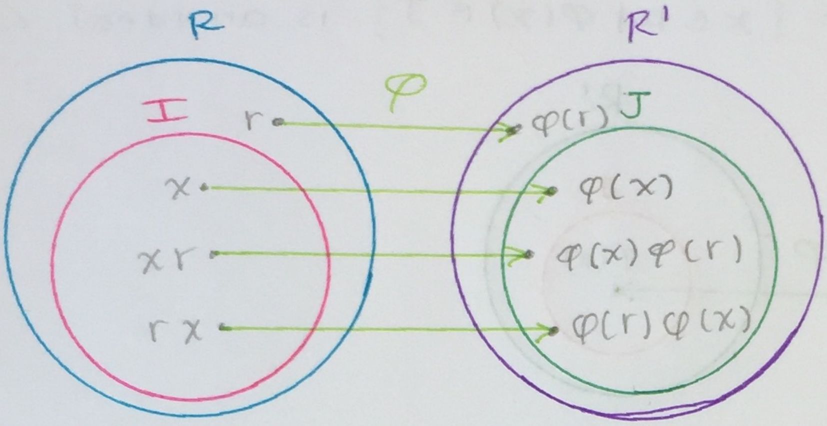


• let $x \in I$ and $r \in R$ we need to show $xr \in I$ and $rx \in I$.

Since $x \in I$, we know $\varphi(x) \in J$.

since J is an ideal, and $\varphi(x) \in J$ and $\varphi(r) \in R'$ we know that $\varphi(x)\varphi(r) \in J$

and $\varphi(r)\varphi(x) \in J$



since φ is a homomorphism

$\varphi(xr) = \varphi(x)\varphi(r)$ and $\varphi(rx) = \varphi(r)\varphi(x)$

so $\varphi(xr) \in J$ and $\varphi(rx) \in J$

thus $xr \in I$ and $rx \in I$ ▨

Continued from last time

Let F be a field and let $p(x) \in F[x]$ where $p(x)$ is non-constant and irreducible. From last time we know that $I = \langle p(x) \rangle$ is a maximal ideal of $F[x]$. Thus, $F[x]/I$ is a field.

Example:

$F[x] = \mathbb{Z}_3[x]$

$p(x) = x^2 + \bar{1}$

since $\deg(p) = 2$ and $p(x)$ has no roots in $\mathbb{Z}_3$, $p(x)$ is irreducible over $\mathbb{Z}_3$

$$\begin{cases} p(\bar{0}) = \bar{0}^2 - \bar{1} = \bar{1} \neq \bar{0} \\ p(\bar{1}) = \bar{1}^2 + \bar{1} = \bar{2} \neq \bar{0} \\ p(\bar{2}) = \bar{2}^2 + \bar{1} = \bar{5} \neq \bar{0} \end{cases}$$

so $I = \langle x^2 + \bar{1} \rangle$ is a maximal ideal of $\mathbb{Z}_3[x]$

Thus, $E = \mathbb{Z}_3[x]/I$ is a field.

$E = \{\bar{0}+I,\ \bar{1}+I,\ \bar{2}+I,\ x+I,\ (x+1)+I,\ (x+\bar{2})+I,\ 2x+I,$
$(\bar{2}x+\bar{1})+I,\ (\bar{2}x+\bar{2})+I,\ x^2+I,\ (x^2+\bar{1})+I,\ (x^2+x+\bar{1})+I, \dots\}$

Note that $\boxed{(x^2+\bar{1})+I = \bar{0}+I}$ since $x^2+\bar{1} \in I$

key equation

$\boxed{I = \{(x^2+\bar{1})f(x) \mid f(x) \in \mathbb{Z}_3[x]\}}$

$\boxed{a+I = b+I \text{ iff } a-b \in I}$

so, $x^2+I = -\bar{1}+I = \bar{2}+I$

$-\bar{1} = \bar{2}$ in $\mathbb{Z}_3$

we can use this equation to reduce polys of $\geq$ deg 2 in E

For Example:

$(x^4+x^3+\bar{2}x+\bar{1})+I = (x^4+I)+(x^3+I)+(\bar{2}x+I)+(\bar{1}+I)$

$= (x^2+I)(x^2+I)+(x^2+I)(x+I)+(\bar{2}x+I)+(\bar{1}+I)$

$= (\bar{2}+I)(\bar{2}+I)+(\bar{2}+I)(x+I)+(\bar{2}x+I)+(\bar{1}+I)$

$x^2+I=\bar{2}+I$

$= (\bar{4}+I)+(\bar{2}x+I)+(\bar{2}x+I)+(\bar{1}+I)$

$= (\bar{4}x+\bar{5})+I = (x+\bar{2})+I$

Theorem:

Let F be a field and $p(x) \in F[x]$ be a non-constant irreducible polynomial. Let $n = \deg(p(x))$.

Let $I = \langle p(x) \rangle$. Let $E = F[x]/\langle p(x) \rangle$

Then,

$$E = \{(a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}) + I \mid a_0, a_1, \dots, a_{n-1} \in F\}$$

moreover, if $(a_0 + a_1x + \dots a_{n-1}x^{n-1}) + I = (b_0 + b_1x + \dots + b_{n-1}x^{n-1}) + I$

then $a_0 = b_0,\ a_1 = b_1, \dots, a_{n-1} = b_{n-1}$

Example:

$$F[x] = \mathbb{Z}_3[x]$$

$P(x) = x^2 + \bar{1}$, $\quad I = \langle x^2 + \bar{1} \rangle$, $\quad n = 2$

$$E = \mathbb{Z}_3[x]/I = \{ \bar{0} + I,\ \bar{1} + I,\ \bar{2} + I,\ x + I,\ (x + \bar{1}) + I,$$
$$(x + \bar{2}) + I,\ 2x + I,\ (2x + \bar{1}) + I,\ (\bar{2}x + \bar{2}) + I \}$$

and $\quad x^2 + I = \bar{2} + I$

$$[(\bar{2}x + \bar{2}) + I][\bar{2}x + I] = (\bar{4}x^2 + \bar{4}x) + I \underset{\bar{4} = \bar{1}}{=} (x^2 + x) + I$$

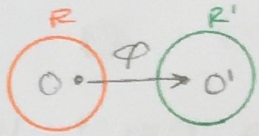
$$\underset{x^2 + I = \bar{2} + I}{=} (\bar{2} + x) + I$$

$$[(\bar{2}x + \bar{2}) + I] + [\bar{2}x + I] = (\bar{4}x + \bar{2}) + I = (x + \bar{2}) + I$$

P.1 4/20 Thursday Week 12 April 20, 2017

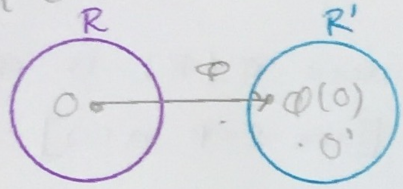
HW 4 #7

Let R and R' be rings. Let $\varphi: R \to R'$ be a ring homomorphism. Prove the following:



(a) $\varphi(0) = 0'$

Let 0 and 0' be the additive identities of R and R'



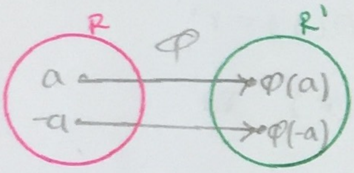
Then $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$

so, $-\varphi(0) + \varphi(0) = -\varphi(0) + \varphi(0) + \varphi(0)$

Then, $0' = 0' + \varphi(0)$. so $0' = \varphi(0)$

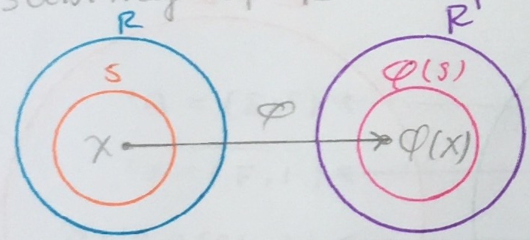
(b) $\varphi(-a) = -\varphi(a)$

Let $a \in R$. Then $\varphi(a) + \varphi(-a) = \varphi(a-a) = \varphi(0) = 0'$ ↑ Part (a)



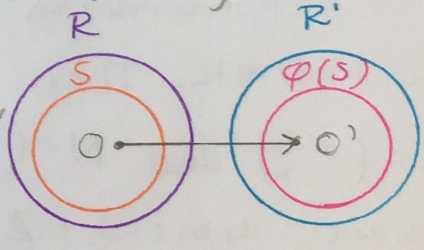
so $\varphi(-a) = -\varphi(a)$

(c) If S is a subring of R then $\varphi(S) = \{\varphi(x) \mid x \in S\}$ is a subring of R'



Let 0 and 0' be the additive identities of R and R'

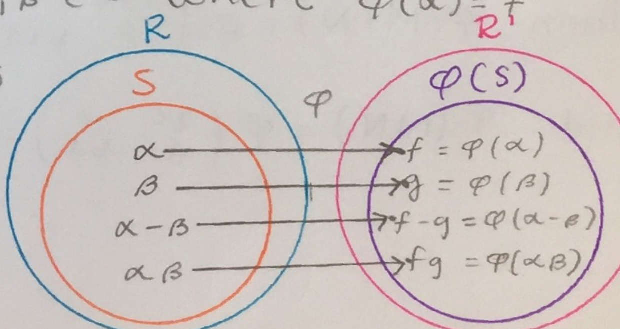
Recall $\varphi(S) = \{\varphi(x) \mid x \in S\}$



- since S is a subring of R we know $0 \in S$. By (a), $\underbrace{\varphi(0) = 0'}_{\text{in } \varphi(S) \text{ since } 0 \in S}$ so $0' \in \varphi(S)$

- Let $f, g \in \varphi(S)$ so there exists $\alpha, \beta \in S$ where $\varphi(\alpha) = f$ and $\varphi(\beta) = g$. we know that $\alpha - \beta \in S$ since S is a subring of R and $\varphi(\alpha - \beta) = \varphi(\alpha) - \varphi(\beta) = f - g$

  so $f - g \in \varphi(S)$

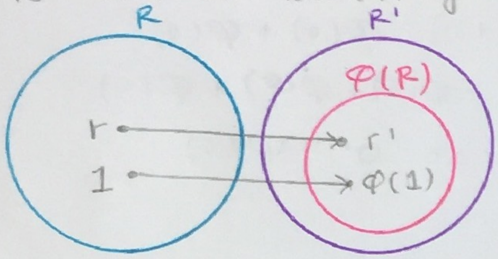


also $\alpha\beta \in S$ since S is a subring of R

and, $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta) = fg$

so $fg \in \varphi(S)$ ☒

(d) If R has a mult. identity denoted by 1, then $\varphi(1)$ is a mult. identity of $\varphi(R)$



From (c) we know $\varphi(R)$ is a subring of R' [Take $S=R$ in (c)]

Let $r' \in \varphi(1) = \varphi(1)\cdot r' = r'$

Then, $r'\cdot\varphi(1) = \varphi(r)\varphi(1) = \varphi(r\cdot 1) = \varphi(r) = r'$

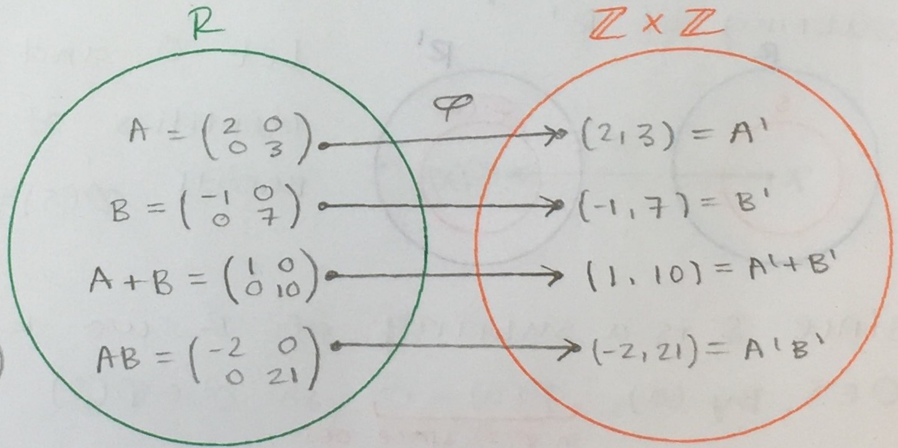
and $\varphi(1)\cdot r' = \varphi(1)\varphi(r') = \varphi(1\cdot r) = \varphi(r) = r'$

so, $\varphi(1)$ is a mult. identity for $\varphi(R)$. ☒

HW4 #6

(a) $R = \left\{\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} \mid a, b \in \mathbb{Z}\right\}$, R is a subring of $M_2(\mathbb{R})$

(b) $R \cong \mathbb{Z}\times\mathbb{Z}$



where $\varphi\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} = (a, b)$

φ is a homomorphism.

Let $M, N \in R$. Then

$M = \begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix}$ and $N = \begin{pmatrix} c & 0 \\ 0 & d\end{pmatrix}$

where $a, b, c, d \in \mathbb{Z}$

Then $\varphi(M+N) = \varphi\begin{pmatrix} a+c & 0 \\ 0 & b+d\end{pmatrix} = (a+c, b+d) = (a,b) + (c,d) = \varphi(M) + \varphi(N)$

and $\varphi(MN) = \varphi\begin{pmatrix} ac & 0 \\ 0 & bd\end{pmatrix} = (ac, bd) = (a,b)(c,d) = \varphi\begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix}\varphi\begin{pmatrix} c & 0 \\ 0 & d\end{pmatrix}$

$= \varphi(M)\varphi(N)$

P. 2 4/20

φ is 1-1

Suppose $\varphi\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \varphi\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{Z}$

Then $(a, b) = (c, d)$ so, $a = c$ and $b = d$

Thus, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

φ is onto

Let $(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z}$

where $\alpha, \beta \in \mathbb{Z}$ Then $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \in R$

and $\varphi\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = (\alpha, \beta)$