P.1 4/11 Tuesday Week 11 April 11, 2017

Example: $R = \mathbb{Z}_3 \times \mathbb{Z}_4 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{3}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}), (\bar{1},\bar{3}), (\bar{2},\bar{0}), (\bar{2},\bar{1}), (\bar{2},\bar{2}), (\bar{2},\bar{3})\}$

$I = \{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{2},\bar{0})\}$ is an ideal of R.

calculating R/I

$R = \mathbb{Z}_n, \mathbb{Z},$

$\mathbb{Z}_n \times \mathbb{Z}_m$

*Try these!!

(a) calculate the elements of R/I

$(\bar{0},\bar{0}) + I = \{(\bar{0},\bar{0}), (\bar{1},0), (\bar{2},\bar{0})\} = (\bar{2},\bar{0}) + I$

$(\bar{0},\bar{1}) + I = \{(\bar{0},\bar{1}), (\bar{1},\bar{1}), (\bar{2},\bar{1})\}$

$(\bar{0},\bar{2}) + I = \{(\bar{0},\bar{2}), (\bar{1},\bar{2}), (\bar{2},\bar{2})\}$

$(\bar{0},\bar{3}) + I = \{(\bar{0},\bar{3}), (\bar{1},\bar{3}), (\bar{2},\bar{3})\}$

$R/I = \{(\bar{0},\bar{0}) + I, (\bar{0},\bar{1}) + I, (\bar{0},\bar{2}) + I, (\bar{0},\bar{3}) + I\}$

(b) multiply $(\bar{1},\bar{3}) + I$ and $(\bar{2},\bar{2}) + I$

put your answer in the form of one of your answers from part (a)

$$\boxed{(\bar{1},\bar{3}) + I}\boxed{(\bar{2},\bar{2}) + I} = (\bar{1},\bar{3})(\bar{2},\bar{2}) + I$$

$$= (\bar{2},\bar{6}) + I = (\bar{2},\bar{2}) + I = \boxed{(\bar{0},\bar{2}) + I}$$

Last time: Big Theorem Thursday

Let R be a commutative ring with $1 \neq 0$. Let M be an ideal of R with $M \neq R$, Then M is maximal iff R/M is a field.

Corollary The maximal ideal of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ where n is prime

Proof: Let I be an ideal of $\mathbb{Z}$. Then $I = n\mathbb{Z}$ where $n \geq 0$. If $n = 0$, then $I = \{0\}$

we have $\{0\} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$

so $\{0\}$ is not maximal

If $n=1$, then $I=\mathbb{Z}$

$\mathbb{Z}$ isn't maximal because it's the whole ring

suppose now $n \geq 2$

Then $I = n\mathbb{Z}$ which is maximal iff $\mathbb{Z}/n\mathbb{Z}$ is a field.

iff $\mathbb{Z}_n$ is a field (because $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$)

iff n is prime $\boxtimes$

Summary of the Ideals of $\mathbb{Z}$

Ideals of $\mathbb{Z}$	Prime Ideals of $\mathbb{Z}$	maximal ideals of $\mathbb{Z}$
$\{0\}$ ← Trivial Ideal	$\{0\}$	$2\mathbb{Z}$
$\mathbb{Z}$ ← whole Ring	$2\mathbb{Z}$	$3\mathbb{Z}$
$2\mathbb{Z}$	$3\mathbb{Z}$	$5\mathbb{Z}$
$3\mathbb{Z}$	$5\mathbb{Z}$	$7\mathbb{Z}$
$4\mathbb{Z}$	$7\mathbb{Z}$	$11\mathbb{Z}$
$6\mathbb{Z}$	$11\mathbb{Z}$	$13\mathbb{Z}$
$7\mathbb{Z}$	$13\mathbb{Z}$	$\vdots$
$8\mathbb{Z}$	$\vdots$	
$9\mathbb{Z}$		
$\vdots$		
$n\mathbb{Z}$, $n \geq 2$	$p\mathbb{Z}$ where p is prime	$p\mathbb{Z}$ where p is prime

Irreducibility Tests for Polynomials

Def: Let F be a field. Let $f(x) \in F[x]$ we say that f is reducible over F if there exists non-constant polynomials $g(x), h(x) \in F[x]$ where $f(x) = g(x)h(x)$.

If this is not the case, then we say that f is irreducible over F.

Example Is $f(x) = x^2 + 2x + 1$ reducible over $\mathbb{Q}$?

answer: Yes!

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

non-constant polys from $\mathbb{Q}[x]$

Note

$$\underbrace{x^2 + 5 = \overset{\text{constant poly}}{\left(\tfrac{1}{2}\right)}(2x^2 + 10)}_{\text{Doesn't count as reducible!}}$$

Example: Is $w(x) = x^2 + 1$ reducible of $\mathbb{R}$?

answer: No, if w factored non-trivially over $\mathbb{R}$ then $x^2 + 1 = (ax + b)(cx + d)$

where $a \neq 0$ and $c \neq 0$, $a, b, c, d \in \mathbb{R}$

plug in $x = -\frac{b}{a}$ then $(-\frac{b}{a})^2 + 1 = \underbrace{(a(-\frac{b}{a}) + b)}_{0}(c(-\frac{b}{a}) + d) = 0$

so, $(-\frac{b}{a})^2 = -1$

That can't happen since $a, b \in \mathbb{R}$ and so $(-\frac{b}{a}) \in \mathbb{R}$

so $x^2 + 1$ is irreducible over $\mathbb{R}$.

Example $x^2 + 1$ is reducible over $\mathbb{C}$

since $x^2 + 1 = (x + i)(x - i)$

Theorem: Let F be a field let $f(x) \in F[x]$ with $\deg(f) = 2$ or $\deg(f) = 3$. Then f is reducible over F iff there exists $\alpha \in F$ where $f(\alpha) = 0$

Example: $F = \mathbb{C}$ $f(x) = x^2 + 1$

$\deg(f) = 2$ so theorem applies

$f(i) = i^2 + 1 = -1 + 1 = 0$

since f has a root in $\mathbb{C}$,

F is reducible over $\mathbb{C}$.

Example: $F = \mathbb{R}$ $f(x) = x^2+1$

$\deg(f) = 2$ so theorem applies

$x^2+1=0$ has no roots in $\mathbb{R}$ so $f(x)$ is irreducible over $\mathbb{R}$.

Example: Is $f(x) = x^2 + \bar{1}$ irreducible over $\mathbb{Z}_3$?

$$F = \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

$\deg(f) = 2$ so theorem applies

$$\left.\begin{aligned} f(\bar{0}) &= \bar{0}^2 + \bar{1} = \bar{1} \neq 0 \\ f(\bar{1}) &= \bar{1}^2 + \bar{1} = \bar{2} \neq 0 \\ f(\bar{2}) &= \bar{2}^2 + \bar{1} = \bar{5} = \bar{2} \neq 0 \end{aligned}\right\}$$

f has no roots in $\mathbb{Z}_3$ so it is irreducible oven $\mathbb{Z}_3$

Example: Is $f(x) = x^4 + 2x^2 + 1$ irreducible over $\mathbb{R}$?

$$x^4 + 2x^2 + 1 = (x^2+1)(x^2+1)$$

NO, f is reducible

But the roots of f are $\pm i$ which are Not in $\mathbb{R}$.

Theorem doesn't apply here $\deg(f) = 4$

* Do not use the theorem if $\deg(f) > 3$

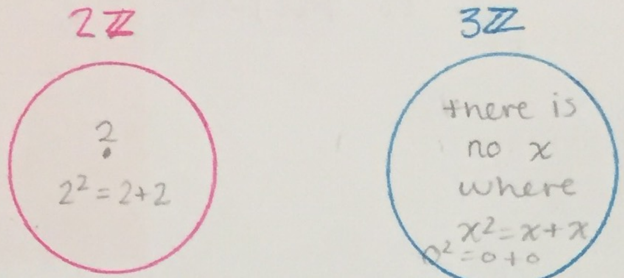
HW #4 (3) Show that $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic as rings

Idea:

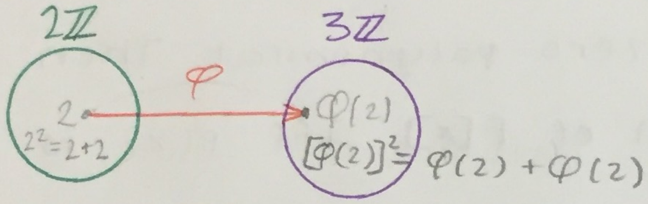
$x^2 = 2x$

$x(x-2) = 0$

$x = 0, 2$



Proof: Suppose $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ is a homomorphism



consider $\varphi(2)$

Note that $[\varphi(2)]^2 = \varphi(2^2) = \varphi(4) = \varphi(2+2) = \varphi(2) + \varphi(2)$

so, $[\varphi(2)]^2 - 2\varphi(2) = 0$

$\varphi(x+y) = \varphi(x) + \varphi(y)$

$\varphi(xy) = \varphi(x)\varphi(y)$

If $ab = 0$ then $a = 0$ or $b = 0$

Thus, $\varphi(2)[\varphi(2) - 2] = 0$

ok since we are in $3\mathbb{Z}$ and $3\mathbb{Z}$ satisfies

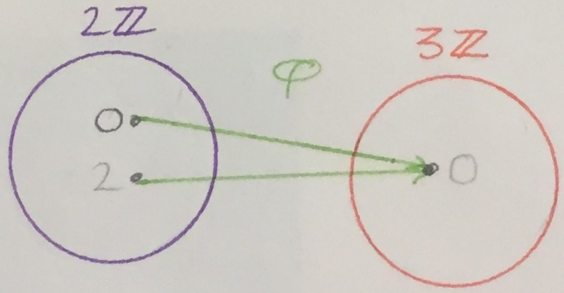
Hence, $\varphi(2) = 0$ or $\varphi(2) - 2 = 0$

we can't have $\varphi(2) - 2 = 0$ because $\varphi(2) = 2$ and $2 \notin 3\mathbb{Z}$

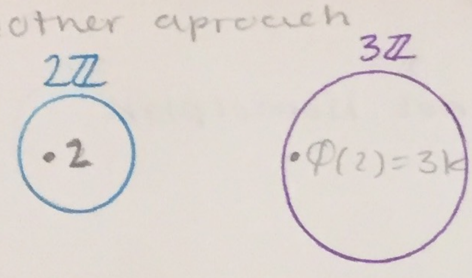
so, $\varphi(2) = 0$

But $\varphi(0) = 0$ also.

so φ is not 1-1 so there is no isomorphism



another aproach



$6k = \phi(2) + \phi(2) = \phi(4)$
$= \phi(2)\phi(2) = 9k^2$
$6k = 9k^2 \longrightarrow 3k[3k-2] = 0$
$k = 0$ or $\underbrace{k = \frac{2}{3}}_{\text{can't happen}}$

so $\phi(2) = 0$

$F[x] / \langle P(x) \rangle$
↑
Field if $\langle P(x) \rangle$ is a maximal ideal

Add to Theorem
Let $P(x) \in F[x]$ where $P(x) \neq 0$ and not a constant poly

Theorem: Let F be a field and $P(x) \in F[x]$ where $P(x)$ is not the zero polynomial. Then $\langle P(x) \rangle$ is a maximal ideal of $F[x]$ iff $P(x)$ is irreducible over F.

proof:

$(\Rightarrow)$ Suppose $\langle P(x) \rangle \neq \{0\}$ is a maximal ideal we know $\langle P(x) \rangle \neq F[x]$ so, $P(x)$ is not a unit, ie $P(x)$ is not a constant polynomial.

Suppose $\boxed{P(x) = f(x)g(x)}$ where $f(x), g(x) \in F[x]$ we will show that either $f(x)$ or $g(x)$ is a unit/(constant poly) so $P(x)$ is irreducible.

so $*$ $\deg(f) \leq \deg(P)$ and $\deg(g) \leq \deg(P)$

↑ (thm. from before) since F is an inte. domain and $P = fg$ we know $\deg(P) = \deg(f) + \deg(g)$

$\mathbb{Z}_4$ ← not an int. domain

$(\bar{2}x^2 + \bar{1})(\bar{2}x + \bar{3})$
$= \bar{4}x^3 + \bar{6}x^2 + \bar{2}x + \bar{3}$
$= \bar{2}x^2 + \bar{2}x + \bar{3}$

since $\langle P(x)\rangle$ is maximal, we know $\langle P(x)\rangle$ is a prime ideal [HW problem]

we know $f(x)g(x) = P(x) \in \langle P(x)\rangle$

since $\langle P(x)\rangle$ is a prime ideal either $f(x) \in \langle P(x)\rangle$ or $g(x) \in \langle P(x)\rangle$ so, either $f(x) = P(x)h_1(x)$ or $g(x) = P(x)h_2(x)$ where $h_1(x), h_2(x) \in F[x]$.

so either $\boxed{\deg(f) \geq \deg(P)}$ or $\boxed{\deg(g) \geq \deg(P)}$

combining this with * we have either

$\deg(f) = \deg(P)$ and $\deg(g) = 0$

or $\deg(f) = 0$ and $\deg(g) = \deg(P)$

So either $g(x)$ is a unit/constant or $f(x)$ is a unit/constant.

so, $P(x)$ is irreducible.

($\Leftarrow$) Suppose $P(x)$ is irreducible over F

Let's show that $\langle P(x)\rangle$ is maximal.

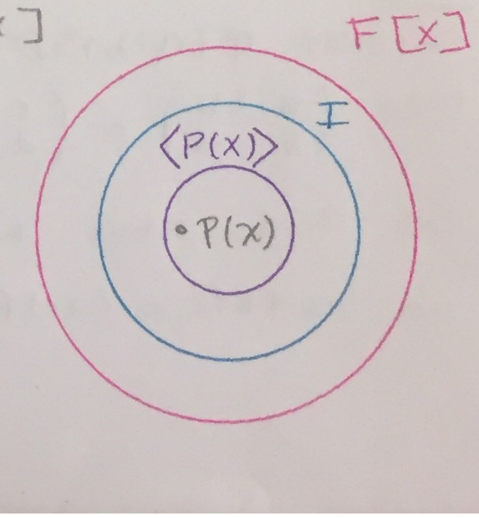
since $P(x)$ is not constant $\langle P(x)\rangle \neq F[x]$

Suppose I is an ideal of $F[x]$

where $\langle P(x)\rangle \subseteq I \subseteq F[x]$

since $F[x]$ is a PID we know

$I = \langle g(x)\rangle$ where $g(x) \in F[x]$



since $p(x) \in \langle p(x) \rangle$ and $\langle p(x) \rangle \subseteq I$

we know $p(x) \in I = \langle g(x) \rangle$

So, $p(x) = g(x)h(x)$ where $h(x) \in F[x]$

Since $p(x)$ is irreducible, either $g(x)$ or $h(x)$ is a constant polynomial.

If $g(x)$ is a constant polynomial, then $I = \langle g(x) \rangle = F[x]$

Now suppose $h(x) = c$, where $c \in F$, then $p(x) = \overset{\text{constant}}{c}\, g(x)$

In this case $I = \langle p(x) \rangle$

why? we know $\langle p(x) \rangle \subseteq I$

Let $z(x) \in I$. Then $z(x) = g(x)w(x)$ where $w(x) \in F[x]$

Then $z(x) = c^{-1} p(x) w(x) = p(x) \cdot [c^{-1} w(x)] \in \langle p(x) \rangle$

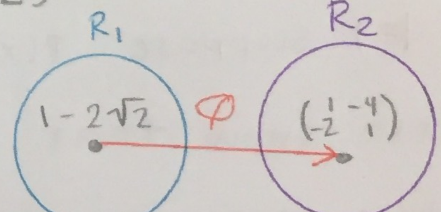
so $I \subseteq \langle p(x) \rangle$

So either $I = F[x]$ or $I = \langle p(x) \rangle$

So $\langle p(x) \rangle$ is maximal.

$R_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ $\quad R_2 = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$

$\varphi : R_1 \to R_2 \quad \varphi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$



1-1

Suppose $\varphi(a + b\sqrt{2}) = \varphi(c + d\sqrt{2})$

then $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = \begin{pmatrix} c & 2d \\ d & c \end{pmatrix}$

So $a = c$ and $b = d$

So $a + b\sqrt{2} = c + d\sqrt{2}$

onto

Let $M \in R_2$

Then $M_2 = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ where $a, b \in \mathbb{Z}$

and $a + b\sqrt{2} \in R_1$

and $\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = M$