2/28 HW

x is an idempotent element if $x^2 = x$

Let R be an integral domain. Show that R has exactly two independent elements.

proof: If R is an integral domain then it has an identity $1 \neq 0$ element.

And $0^2 = 0$ and $1^2 = 1$

so 0 and 1 are idempotents.

- why are these the only 2 elements?

Suppose $x \in R$ and $x^2 = x$

so $x^2 - x = 0$

thus $x(x-1) = 0$

since R is an integral domain either

$x = 0$ or $x - 1 = 0$

so $x = 0$ or $x = 1$ ▨

- Let R be a ring with additive identity 0 and multiplicative identity 1, if $1 = 0$ then $R = \{0\}$

Proof:

Let $x \in R$, then

$x = 1 \cdot x = 0 \cdot x = 0$

So, $P = \{0\}$ ▨

$\mathbb{Z}_6$ ← not an integral domain

$\overline{0}^2 = \overline{0}$ $\overline{5}^2 = \overline{25} = \overline{1}$

$\overline{1}^2 = \overline{1}$

$\overline{2}^2 = \overline{4}$

$\overline{3}^2 = \overline{9} = \overline{3}$

$\overline{4}^2 = \overline{16} = \overline{4}$

idempotents

$\overline{0}, \overline{1}, \overline{3}, \overline{4}$

HW 1 #3

Let R and S be commutative rings with identity elements 1_R and 1_S

Then $(x,y) \in R \times S$ is a unit iff x is a unit of R and y is a unit of S.

proof:

($\Leftrightarrow$) Let $(x,y) \in R \times S$

$(x,y) \in R \times S$ is a unit iff $\exists\ (r,s) \in R \times S$

where $(x,y)(r,s) = \underbrace{(1_R, 1_S)}_{\text{mult. identity of } R \times S}$

iff $(xr, ys) = (1_R, 1_S)$ for some $r \in R$ and $s \in S$

iff $xr = 1_R$ and $ys = 1_S$ for some $r \in R$ and $s \in S$

iff x is a unit in R and y is a unit in S

Tuesday Week 6 Feb. 28, 2017

Theorem:

- Let R be a commutative ring with identity $1 \neq 0$

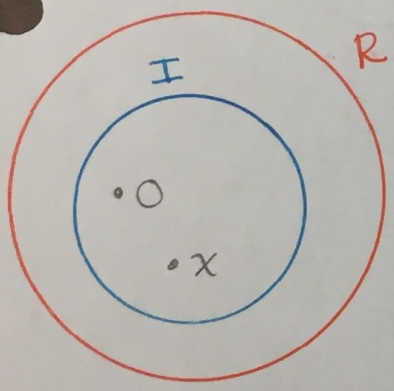
  R is a field iff the only ideals of R is $\{0\}$ and R.

Proof: ($\Leftarrow$) suppose that R has only two ideals: $\{0\}$ and R.

To show R is a field we need to show that every non-zero element has a multiplicative inverse.

Let $x \in R$ with $x \neq 0$

consider the ideal $I = \langle x \rangle = Rx = \{rx \mid r \in R\}$

- 

  Since $x \neq 0$, I is an ideal with at least two elements 0 and x.

  so, $I \neq \{0\}$. Thus, $I = R$

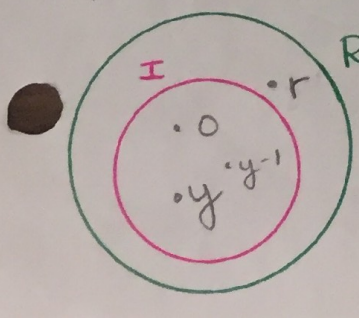
  so, $1 \in I$

  Thus, $1 = rx$ for some $r \in R$

  so x has a multiplicative inverse

  Therefore, R is a field.

($\Rightarrow$) Let R be a field. Suppose I is an ideal of R and $I \neq \{0\}$. we must show $I = R$

- 

  Since $I \neq \{0\}$ $\exists\, y \in I$ with $y \neq 0$

  note: $y^{-1} \in I$

  since $y^{-1} = \underbrace{y^{-1}y^{-1}}_{\text{in } R}\underbrace{y}_{\text{in } I}$

since R is a field y^{-1} exists in R

and $\underbrace{y^{-1}}_{\text{in } R}\underbrace{y}_{\text{in } I} = 1 \in I$ since I is an ideal

Let $r \in R$, then $r = \underbrace{r}_{\text{in } R} \cdot \underbrace{1}_{\text{in } I} \in I$

since I is an ideal

so, $R = I$ ▨

Example: In the homework you show that every ideal of $\mathbb{Z}_n$ is principal. More specifically if I is an ideal of $\mathbb{Z}_n$ then $\exists\ \bar{k} \in \mathbb{Z}_n$ where

$$I = \langle \bar{k} \rangle = \{\bar{x} \cdot \bar{k} \mid \bar{x} \in \mathbb{Z}_n\}$$

$$= \{\bar{0} \cdot \bar{k}, \bar{1} \cdot \bar{k}, \bar{2} \cdot \bar{k}, \ldots, (\overline{n-1}) \cdot \bar{k}\}$$

$$= \{\bar{0}, \bar{k}, \bar{k}+\bar{k}, \bar{k}+\bar{k}+\bar{k}, \ldots, \underbrace{\bar{k}+\bar{k}+\cdots+\bar{k}}_{n-1 \text{ times}}\}$$

This is the subgroup generated by k

For $\mathbb{Z}_n$, the ideals are just the cyclic group. (which are all the subgroups since $\mathbb{Z}_n$ is cyclic.)

Find all the ideals of $\mathbb{Z}_{12}$

(Recall from 4550, $\langle -\bar{k} \rangle = \langle \bar{k} \rangle$)

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{11} \rangle = \langle \bar{1} \rangle = \mathbb{Z}_{12}$

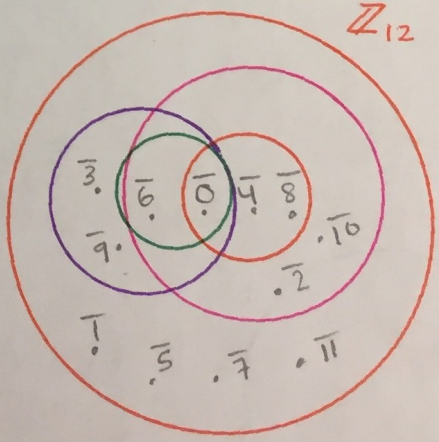
$\langle \bar{10} \rangle = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$

$\langle \bar{9} \rangle = \langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\langle \bar{8} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$

$\langle \bar{7} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_{12}$

$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}\}$



3/2 HW

HW #1, #3

(3) (b) Find units of $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{0})(\bar{1},\bar{1})(\bar{1},\bar{2})\}$

(additive identity: $(\bar{0},\bar{0})$; mult. identity: $(\bar{1},\bar{1})$)

from theorem last time

units of $\mathbb{Z}_2 : \bar{1}$

units of $\mathbb{Z}_3 : \bar{1},\bar{2}$

units of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are $(\bar{1},\bar{1}),(\bar{1},\bar{2})$

$(\bar{1},\bar{2}) \cdot (\bar{1}\cdot\bar{2}) = (\bar{1},\bar{4}) = (\bar{1},\bar{1})$

$(\bar{1},\bar{2})^{-1} = (\bar{1},\bar{2})$ ← It's its own inverse.

Is this an integral domain?

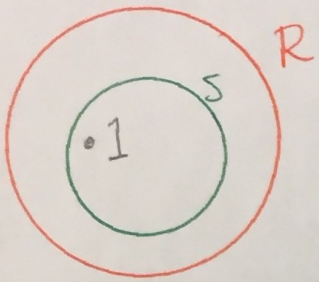
$(\bar{0},\bar{1}) \cdot (\bar{1},\bar{0}) = (\bar{0},\bar{0})$

not $(\bar{0},\bar{0})$

- NO! not an integral domain

HW #2

④ (a) Let R be an integral domain and S be a subring of R with $1 \in S$. Prove S is an integral domain.



Proof: Since $S \subseteq R$ and R is commutative we have that S is commutative. Since $1 \in S$, we know that S is a commutative ring with 1. S has no zero divisors because if say $x, y \in S$ with $x \neq 0$, $y \neq 0$ and $xy = 0$, then R would have zero divisors which it does not. So, S has no zero divisors and is an integral domain. ▨

To show something is NOT an integral domain:

- not commutative
- no mult. identity
- has zero divisors

HW #2

① (e) is $\mathbb{Z}_{106}$ an integral domain?

$$\overline{2} \cdot \overline{53} = \overline{106} = \overline{0}$$

$\overline{2}$, $\overline{53}$: not zero; $\overline{0}$: zero

No since $\mathbb{Z}_{106}$ has zero divisors

Theorem: $\mathbb{Z}_n$ is an integral domain iff n is prime.

Theorem: $\mathbb{Z}_n$ is a field iff n is prime

② (a) $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$

If $n=1$, $n\mathbb{Z} = \mathbb{Z}$ ✓ is an integral domain.

If $n \geq 2$, $1 \in n\mathbb{Z}$ so it is not an integral domain.

HW 1

⑥ Let R be a ring and $a \in R$

Let $I_a = \{x \in R \mid ax = 0\}$

Prove that I_a is a subring of R.

Ex: $R = \mathbb{Z}_6$

$a = 2$

$I_2 = \{\bar{x} \in \mathbb{Z}_6 \mid \bar{2} \cdot \bar{x} = \bar{0}\}$

$I_2 = \{\bar{0}, \bar{3}\}$

$x = \bar{0} \to \bar{2} \cdot \bar{0} = \bar{0}$

$x = \bar{1} \to \bar{2} \cdot \bar{1} = \bar{2}$

$x = \bar{2} \to \bar{2} \cdot \bar{2} = \bar{4}$

$x = \bar{3} \to \bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

$x = \bar{4} \to \bar{2} \cdot \bar{4} = \bar{8} = \bar{2}$

$x = \bar{5} \to \bar{2} \cdot \bar{5} = \bar{10} = \bar{4}$

Proof:

(1) Note that $a \cdot 0 = 0$, so $0 \in I_a$

(2)/(3) Let $y, z \in I_a$

Then $ay = 0$ and $az = 0$

so $a(y - z) = ay - az = 0 - 0 = 0$

so $y - z \in I_a$

and $a(yz) = (ay) \cdot z = 0 \cdot z = 0$

so $yz \in I_a$ ☑

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

(1) $a = b = 0$ then $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$

(2)/(3) Let $C, D \in R$ then $C = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ & $D = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

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

$C - D = \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in R$ and $CD = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in R$

☑

If we know

- $0 \in R$
- $x, y \in R$ then $x - y \in R$

- Let $z \in R$
  then $0 - z \in R$
- Let $a, b \in R$
  then $a - (-b) \in R$
  $a + b$

- Is $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ commutative?

Let $C, D \in R$, then $C = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $D = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$, $a, b, c, d \in \mathbb{R}$ and

$$CD = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} cd & 0 \\ 0 & db \end{pmatrix} = DC$$

Yes, it is commutative

- Does R have an identity?

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$ yes

- Does R have zero divisors?

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\in$ in R; $\in$ in R; ↑ additive identity

so R is not an integral domain

whats the difference between Field and integral dom.

Field

commutative ring R with $1 \neq 0$, every non-zero $x \in R$ has a mult. inverse (i.e. is a unit)

Integral domain

commutative Ring R with $1 \neq 0$, every non-zero x is NOT a zero divisor

Field $\rightarrow$ integral domain

finite integral domain $\rightarrow$ field

integral domain $\not\rightarrow$ Field.

Ex: $\mathbb{Z}$ is an integral domain that is not a field. for ex, $3 \in \mathbb{Z}$ but 3 has no mult. inverse since $\frac{1}{3} \notin \mathbb{Z}$

units of $\mathbb{Z}$ are $\{1, -1\}$

units

- units of $R \times S$
- unit of $\mathbb{Z}_n$ $(\mathbb{Z}_n^\times)$
- Hw $\mathbb{Q}(\sqrt{2})$ $\leftarrow$ field
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ is a unit iff $\underbrace{ad-bc \neq 0}_{\text{determinant}}$
- units of $\mathbb{Z}$ are $\{1, -1\}$
- units of $R[x]$ are units of R (R is an integ. dom)

$\mathbb{Z}_4$ is not an int. domain $\nearrow$ $\mathbb{Z}_4[x]$

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

$\bar{1} + \bar{2}x$ is a unit