P.1 1/31 Tuesday Week 2 Jan. 31. 2017

Theorem: Let $R_1, R_2, \ldots R_n$ be rings

- Construct $R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \ldots, r_n) \mid r_1 \in R_1, r_2 \in R_2, \ldots r_n \in R_n\}$

define addition and multiplication as

$(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)$ and

$(r_1, r_2, \ldots, r_n) \cdot (s_1, s_2, \ldots, s_n) = (r_1 s_1, r_2 s_2, \ldots, r_n s_n)$

Then $R_1 \times R_2 \times \cdots \times R_n$ is a ring.

Example:

$$\mathbb{Z}_2 \times \mathbb{Z}_4 = \left\{ \begin{array}{l} (\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{3}) \\ (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}), (\bar{1},\bar{3}) \end{array} \right\}$$

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

$$(\bar{1},\bar{2}) \cdot (\bar{1},\bar{3}) = (\bar{1}\cdot\bar{1}, \bar{2}\cdot\bar{3}) = (\bar{1},\bar{6}) = (\bar{1},\bar{2})$$

- $(\bar{0},\bar{0}) + (\bar{a},\bar{b}) = (\bar{a},\bar{b}) = (\bar{a},\bar{b}) + \underline{(\bar{0},\bar{0})}$ ← additive identity

$(\bar{1},\bar{1})(\bar{a},\bar{b}) = (\bar{a},\bar{b}) = (\bar{a},\bar{b})\underline{(\bar{1},\bar{1})}$ ← mult identity

Def: Let R be a ring. Let $S \subseteq R$.

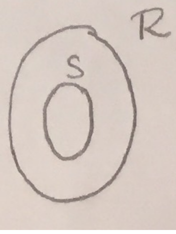
We say that S is a **subring** of R if S is a ring under the same operations as R.

Def: Let F be a field. Let $E \subseteq F$ Then E is a **subfield** of F if E is a field under the same operations as F.

Subring Criteria

- Let R be a ring and $S \subseteq R$, then S is a subring of R iff the following holds:

1. $0 \in S$
2. $a - b \in S \quad \forall\, a, b \in S$
3. $ab \in S \quad \forall\, a, b \in S$



Example:

Show that $12\mathbb{Z} = \{12n \mid n \in \mathbb{Z}\} = \{\dots, -36, -24, -12, 0, 12, 24, 36, \dots$

are a subring of $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

Proof:

① $0 = 12(0) \in 12\mathbb{Z}$

② Let $a, b \in 12\mathbb{Z}$, then $a = 12x$ and $b = 12y$

where $x, y \in \mathbb{Z}$

so $a - b = 12x - 12y = 12(x - y) \in 12\mathbb{Z}$

③ Let $\alpha, \beta \in 12\mathbb{Z}$, then $\alpha = 12\theta$ and $\beta = 12\omega$

where $\theta, \omega \in \mathbb{Z}$

so $\alpha\beta = (12\theta)(12\omega) = 12(12\theta\omega) \in 12\mathbb{Z}$

Q.E.D.

Example:

Consider the ring $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$

Let $L = \left\{ \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \middle| x, y, z \in \mathbb{R} \right\}$

Lets show that L is a subring of $M_2(\mathbb{R})$

Proof: ① $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in L$, (set $x = y = z = 0$)

② and ③ Let $A = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$, $B = \begin{pmatrix} d & 0 \\ e & f \end{pmatrix}$ be elements of L

$A - B = \begin{pmatrix} a-d & 0 \\ b-e & c-f \end{pmatrix} \in L$ and

$AB = \begin{pmatrix} ad & 0 \\ be & cf \end{pmatrix} \in L$ ▨

Integral Domains

Ex: In $\mathbb{Z}_6$, $\underset{\text{not } \bar{0}}{\bar{2}} \cdot \underset{\text{not } \bar{0}}{\bar{3}} = \bar{6} = \underset{\text{is } \bar{0}}{\bar{0}}$

Def: Let R be a ring. Let $x \in R$ with $x \neq 0$. We say that x is a **zero divisor** if $\exists\, y \in R$ with $y \neq 0$ and $xy = 0$
(y would be a zero divisor too)

Example: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

zero divisors	why?
$\bar{2}$, $\bar{3}$	$\bar{2} \cdot \bar{3} = 0$
$\bar{4}$	$\bar{4} \cdot \bar{4} = 0$

not zero divisors	why?
$\bar{0}$	because its $\bar{0}$
$\bar{1}$	$\bar{1} \cdot \bar{1} = \bar{1} \neq \bar{0}$ $\quad$ $\bar{1} \cdot \bar{4} = \bar{4} \neq 0$ $\bar{1} \cdot \bar{2} = \bar{2} \neq 0$ $\quad$ $1 \cdot \bar{5} = \bar{5} \neq 0$ $\bar{1} \cdot \bar{3} = \bar{3} \neq 0$
$\bar{5}$	$\bar{5} \cdot \bar{1} = \bar{5} \neq 0$ $\quad$ $\bar{5} \cdot \bar{4} = \overline{20} = \bar{2} \neq 0$ $\bar{5} \cdot \bar{2} = \overline{10} = \bar{4} \neq 0$ $\quad$ $5 \cdot 5 = \overline{25} = \bar{1} \neq \bar{0}$ $\bar{5} \cdot \bar{3} = \overline{15} = \bar{3} \neq 0$

Ex: what are the zero divisors of $\mathbb{Z}$?

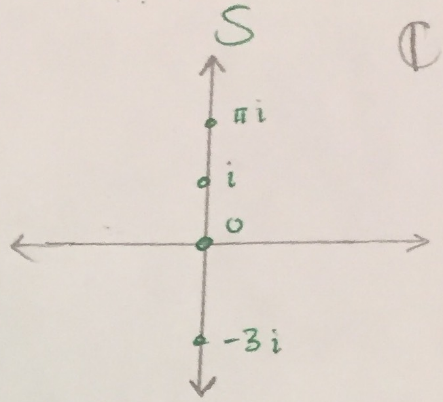
there are none!

can't have a $\binom{\text{non}}{\text{zero}} \cdot \binom{\text{non}}{\text{zero}} = \text{zero}$

HW 2/2

HW #1

#1 (c)



Let $S = \{ix \mid x \in \mathbb{R}\}$

Is S a ring? $\boxed{\text{No}}$

-not closed under multiplication

$i \cdot i = -1$

In S   in S   not in S

Def Let R be a ring, $x \in R$, $x \neq 0$,
x is a **zero divisor** iff $\exists y \in R$, $y \neq 0$
where $xy = 0$
not 0 Not 0

Number Theory (4460)

Thm: Let $a, b, c \in \mathbb{Z}$, $c \neq 0$
If $c \mid ab$ and $\gcd(c, a) = 1$ then $c \mid b$
divides

Ex: In $\mathbb{Z}_6$
zero divisors: $\bar{2}, \bar{3}, \bar{4}$
not zero divisors: $\bar{1}, \bar{5}$

Theorem: Let $\bar{x} \in \mathbb{Z}_n$ where $\bar{x} \neq \bar{0}$
Then $\bar{x}$ is a zero divisor iff $\gcd(x, n) > 1$

Proof:
($\Rightarrow$) Suppose $\bar{x}$ is a zero divisor.
Then $\exists \bar{y} \in \mathbb{Z}_n$ with $\bar{y} \neq \bar{0}$ and $\bar{x} \cdot \bar{y} = \bar{0}$
so $xy \equiv 0 \pmod{n}$, Thus $n \mid xy$
Suppose $\gcd(x, n) = 1$, Then, $n \mid y$ by number theory theorem. But this means $\bar{y} = \bar{0}$ $\left(n \mid y \Rightarrow y = nk \Rightarrow \bar{y} = \bar{n}\bar{k} = \bar{0}\bar{k} = \bar{0},\ k \in \mathbb{Z} \right)$
which isn't true. So $\gcd(x, n) > 1$

($\Leftarrow$) Now suppose the $\gcd(x, n) > 1$
Let $d = \gcd(x, n)$
Note: $0 < \frac{n}{d} < n$, since $d > 1$
$\frac{n}{d} \in \mathbb{Z}$ since $d \mid n$ by def. of gcd.
since $0 < \frac{n}{d} < n$, we know $\overline{\frac{n}{d}} \neq \bar{0}$
in $\mathbb{Z}_n$ $\bar{0} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

Ergo $\bar{x} \cdot \left(\overline{\frac{n}{d}}\right) = \overline{\frac{xn}{d}} = \left(\overline{\frac{x}{d}}\right) \cdot \bar{n} = \left(\overline{\frac{x}{d}}\right) \cdot \bar{0} = \bar{0}$
$d \mid x$ since $d = \gcd(x, n)$
so $\frac{x}{d} \in \mathbb{Z}$

So $\bar{x}$ is a zero divisor. $\square$

Ex: Find the zero divisors of $\mathbb{Z}_{12}$

$\bar{x}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$
$\gcd(x,12)$	1	2	3	4	1	6	1	4	3	2	1

zero divisors: $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$

Ex: Find the zero divisors of $\mathbb{Z}_7$

$\bar{x}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\gcd(x,7)$	1	1	1	1	1	1

No zero divisors

Fact: If p is a prime then $\mathbb{Z}_p$ has no zero divisors

proof: Let $\bar{x} \in \mathbb{Z}_p$ with $\bar{x} \neq \bar{0}$

Then $x \not\equiv 0 \pmod{p}$. That is, p does not divide x.

since p is a prime, $\gcd(x,p) = 1$ or p

If $\gcd(x,p) = p$, then $p \mid x$. This isn't the case

so $\gcd(x,p) = 1$

so $\bar{x}$ is not a zero divisor!

2nd proof: (by contradiction)

Suppose $\mathbb{Z}_p$ had a zero divisor

Then $\exists\ \bar{x}, \bar{y} \in \mathbb{Z}_p$ with $\bar{x} \neq \bar{0}$ and $\bar{y} \neq \bar{0}$ and $\bar{x} \cdot \bar{y} = \bar{0}$

Then $xy \equiv 0 \pmod{p}$ so $p \mid xy$ so either $\underbrace{p \mid x \text{ or } p \mid y}$

$x \equiv 0 \pmod{p}$ or $y \equiv 0 \pmod{p}$

then $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$

contradiction!!!

Number Theory

Let $x, y, p \in \mathbb{Z}$

If p is prime and $p \mid xy$ then $p \mid x$ or $p \mid y$

Def: Let R be a ring
we say that R is an **integral domain** if

(1) R is commutative with identity $1 \neq 0$

(2) R has NO zero divisors

* commutative means: $ab = ba$ $\forall a, b \in R$

* another way to write (2): If $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$

Examples of Integral Domains

$\mathbb{Z}_p$, p is a prime

$\mathbb{Z}$

$\mathbb{Q}$

$\mathbb{R}$

$\mathbb{C}$

* $\mathbb{Z}_6$ is not an integral domain since $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$

* $M_2(\mathbb{R})$ not an integral domain
- not commutitive
- has zero divisors

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

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

Proof: ($\Leftarrow$) we've done this direction

($\Rightarrow$) (contrapositive)

Suppose n is not prime
Then $n = ab$ with $1 < a, b < n$
Then n doesn't divide a or b,
so $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$
but $\bar{a} \cdot \bar{b} = \bar{n} = \bar{0}$
so $\bar{a}$ and $\bar{b}$ are zero divisors
so $\mathbb{Z}_n$ is not an integral domain $\boxtimes$

* $\bar{x} = \bar{0}$ iff $x \equiv 0 \pmod{n}$ iff $n \mid x$