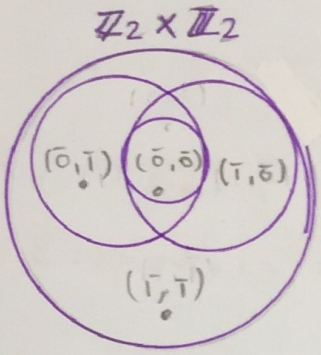
P. 1 5/9
HW 7

Tuesday Week 15 May 9, 2017

(3) Find all the maximal and prime ideals of $\mathbb{Z}_2 \times \mathbb{Z}_2$



Ideals (trivial)
$\{(\bar{0},\bar{0})\}$
$\mathbb{Z}_2 \times \mathbb{Z}_2$

other possible ideals
$\{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}$ ✓
$\{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$ ✓
$\{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{0},\bar{1})\}$ ✗
↳ not closed under +

$(\bar{1},\bar{1})$ is a unit so, if $(\bar{1},\bar{1})$ is an ideal then the ideal is the whole ring $\mathbb{Z}_2 \times \mathbb{Z}_2$

If R and S are rings and
I ideal of R
J ideal of S
I x J ideal of R x S

maximal	not maximal
$\{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}$	$\{(\bar{0},\bar{0})\}$
$\{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$	$\mathbb{Z}_2 \times \mathbb{Z}_2$

HW 7 #6
R is comm. w/ $1 \neq 0$

Prime	not prime
$\{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}$	$\mathbb{Z}_2 \times \mathbb{Z}_2$
$\{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}$	$I = \{(\bar{0},\bar{0})\}$ ← $(\bar{0},\bar{1})(\bar{1},\bar{0}) = (\bar{0},\bar{0})$

not in I, not in I, in I

P is a prime ideal in R if:
- P is an ideal
- $P \neq R$
- For every $a,b \in R$ if $ab \in P$ then $a \in P$ or $b \in P$

* Ideals of $\mathbb{Z}_2 = \{\bar{0},\bar{1}\}$ are $\{\bar{0}\}$ and $\mathbb{Z}_2$

HW 7

(5) Let R be a commutative ring w/ $1 \neq 0$

Then $\{0\}$ is a prime ideal iff R is an int. dom.

proof:

($\Leftarrow$) Suppose R is an int. domain

$\{0\}$ is always an ideal let's show its prime.

$\{0\} \neq R$ since R has at least two elements: 0 and 1

Suppose $a, b \in R$ and $ab \in \{0\}$

so $ab = 0$. Since R is an int. dom.

either $a = 0$ or $b = 0$.

so $a \in \{0\}$ or $b \in \{0\}$. So $\{0\}$ is prime.

$R \cong R/\{0\}$

R: int. dom.

So, $\{0\}$ is prime

($\Rightarrow$) Suppose $\{0\}$ is prime

Suppose $ab = 0$ where $a, b \in R$

Then $ab \in \{0\}$

since $\{0\}$ is prime, $a \in \{0\}$ or $b \in \{0\}$

so either $a = 0$ or $b = 0$

So, R is an integral domain. ☒

How to make a finite field of size p^n where p is prime

1. Find an irreducible poly $f(x) \in \mathbb{Z}_p[x]$ of degree n
2. let $E = \mathbb{Z}_p[x] / \langle f(x) \rangle$

HW #8

① construct a field of size 8.

$8 = 2^3$ ($n=3$, $p=2$)

* Goal find an irreducible poly $f(x)$ in $\mathbb{Z}_2[x]$ of degree 3

Possibilities

- $x \cdot x^3 + \bar{1}$
- $x \cdot x^3 = x \cdot x \cdot x$
- $x \cdot x^3 + x^2 + x + \bar{1}$ $\uparrow (x+\bar{1})(x^2+\bar{1})$
- $x \cdot x^3 + x = x(x^2+1)$
- $x^3 + x + 1$
- $\boxed{x^3 + x^2 + \bar{1}}$
- $x \cdot x^3 + x^2 + x$ $\uparrow x(x^2+x+\bar{1})$
- $x \cdot x^3 + x^2$ $\uparrow = x^2(x+\bar{1})$

$x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$ where $\bar{a}, \bar{b}, \bar{c} = \bar{0}, \bar{1}$

$x^3 + \bar{1} \leftarrow \bar{0}^3 + \bar{1} = \bar{1}$

$\bar{1}^3 + \bar{1} = \bar{2} = \bar{0}$

$x^3 + \bar{1}$ has a root in $\mathbb{Z}_2$ so its reducible in $\mathbb{Z}_2$

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

$f(\bar{0}) = \bar{0} + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$

$f(\bar{1}) = \bar{1}^3 + \bar{1}^2 + \bar{1} = \bar{3} = \bar{1} \neq \bar{0}$

So f has no roots in $\mathbb{Z}_2$

since $\deg(f) = 3$, f is irreducible in $\mathbb{Z}_2$

so $I = \langle x^3 + x^2 + \bar{1} \rangle$ is maximal. Thus,

$E = \mathbb{Z}_2[x] / I$ is a field.

F = Field

An ideal $\langle f(x) \rangle \neq \{0\}$ is maximal in $F[x]$ iff $f(x)$ is irreducible over F

$$E = \{(a+bx+cx^2)+I \mid a,b,c \in \mathbb{Z}_2\}$$

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

side note:

deg 1 irr	deg 2 irr	deg 3 irr
$x+\bar{1}$	$x^2+x+\bar{1}$	$x^3+x+\bar{1}$
x		$x^3+x^2+\bar{1}$

Don't worry about HW 3 only HW 3 #6 *

HW #7

(2) ideals in $\mathbb{Z}_8 = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7}\}$

$\langle \bar{x} \rangle = \langle -\bar{x} \rangle$

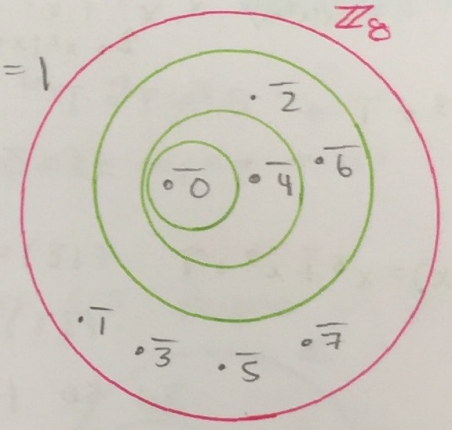
$\langle \bar{x} \rangle = \mathbb{Z}_n$ iff $\gcd(n,x)=1$

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

$\langle \bar{1} \rangle = \mathbb{Z}_n = \langle \bar{3} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle$

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

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



ideals of $\mathbb{Z}_8$

maximal	prime
$\{\bar{0},\bar{2},\bar{4},\bar{6}\}$	$\{\bar{0},\bar{2},\bar{4},\bar{6}\}$

possible prime

no $\{0\} \leftarrow \bar{2}\cdot\bar{4} \in \{0\}$ and $\mathbb{Z}_8$ is not an int. dom.
($\bar{2}$, $\bar{4}$ not in $\{0\}$)

no $\{\bar{0},\bar{4}\}$ $\bar{2}\cdot\bar{2} = \bar{4} \in \{\bar{0},\bar{4}\}$
($\bar{2}$, $\bar{2}$ not in $\{\bar{0},\bar{4}\}$)

Thursday Week 15 May 11, 2017

Final:

- Subring or not
- Ring or not
- units in a ring
- mult./add. identities
- int. domain or not
- HW 3 #6
- homomorphic or not
- iso. or not?
- $R \cong S$ or not

* $\langle x \rangle = \{rx \mid r \in R\}$
- ideal or not
- finding all ideals of a ring
- calculating R/I and doing calculations in R/I
- maximal or prime?
- make finite fields
- is all poly irr.
- Proofs about all objects in class
- kernal

- $S \not\subseteq R$ means $S \subseteq R$ is not true
- $S \subsetneq R$ means $S \subseteq R$ but $S \neq R$

HW 7 #4

Is $6\mathbb{Z}$ maximal in $\mathbb{Z}$? Is it prime?

$6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$

$3\mathbb{Z} = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$

since $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$, $6\mathbb{Z}$ is not maximal

or $6\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$

Facts about $\mathbb{Z}$

- ideals of $\mathbb{Z}$

$\{0\}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \ldots$ ie $n\mathbb{Z}$, $n \geq 0$

- max. ideals of $\mathbb{Z}$

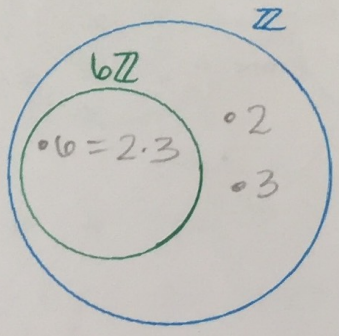
$p\mathbb{Z}$, p is prime

- Prime ideals of $\mathbb{Z}$

$\{0\}$, $p\mathbb{Z}$, prime

prime

Is $6\mathbb{Z}$ prime in $\mathbb{Z}$



$2, 3 \notin 6\mathbb{Z}$ but

$2 \cdot 3 = 6 \in 6\mathbb{Z}$

so $6\mathbb{Z}$ is not prime in $\mathbb{Z}$

Review:

I is prime in R

① I is an ideal of R

② $I \neq R$

③ For every $a, b \in R$

If $ab \in I$, then $a \in I$ or $b \in I$

Contrapositive

If $a \notin I$ and $b \notin I$, then $ab \notin I$

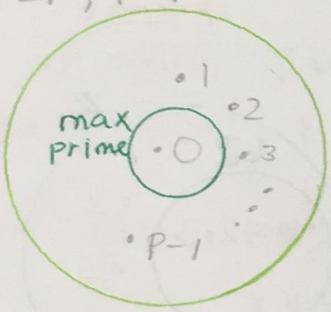
HW 7 #7

Give an example of a prime ideal that's not maximal.

EX 1: $\{0\}$ is prime in $\mathbb{Z}$, but not maximal since $\{0\} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$

EX 2: There's no ex. #2 ∴

Field
↓
$\mathbb{Z}_p$, p prime

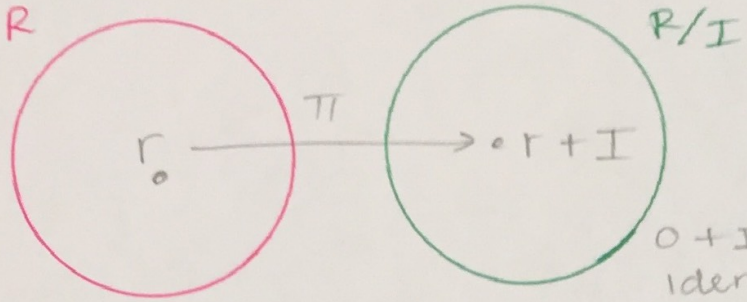


HW 6 #6

R is a ring, I is an ideal of R

$\pi : R \to R/I$

$\pi(r) = r + I$, π is an onto ring homo.



$0 + I$ is the additive identity in R/I

Proof: Let $x, y \in R$, then

$\pi(x+y) = (x+y) + I = (x+I) + (y+I) = \pi(x) + \pi(y)$

$\pi(xy) = xy + I = (x+I)(y+I) = \pi(x)\pi(y)$

onto: yes

consider a coset $r + I \in R/I$ where $r \in R$

Then $\pi(r) = r + I$

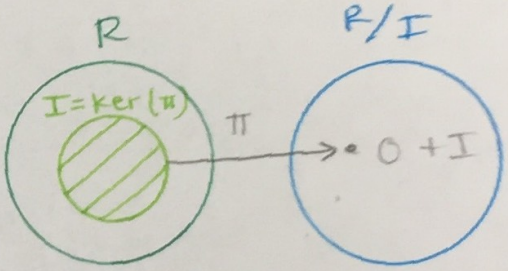
$\ker(\pi) = I$

pf: (1) suppose $i \in I$

Then $\pi(i) = i + I = 0 + I$

↑ since $i - 0 \in I$

so $i \in \ker(\pi)$, so $I \subseteq \ker(\pi)$



(2) suppose $x \in \ker(\pi)$

Then $\pi(x) = 0 + I$

so, $x + I = 0 + I$

Thus, $x = x - 0 \in I$

so $\ker(\pi) \subseteq I$ ☒

when is π 1-1?

π is 1-1 iff $\ker(\pi) = \{0\}$

iff $I = \{0\}$

HW 5

④ (a) let I be an ideal of $\mathbb{Z}_n$

I is a subgroup of $\mathbb{Z}_n$ under $+$

4550 $\mathbb{Z}_n$ is a cyclic group under $+$

so I is a cyclic subgroup of $\mathbb{Z}_n$ under $+$

So, $I = \underbrace{\langle \bar{a} \rangle}_{\text{cyclic subgroup generated by } \bar{a}}$ for some $\bar{a} \in \mathbb{Z}_n$

Thus, $I = \langle \bar{a} \rangle = \{\bar{0}, \bar{a}, \bar{a}+\bar{a}, \bar{a}+\bar{a}+\bar{a}, \ldots, \underbrace{\bar{a}+\bar{a}\cdots+\bar{a}}_{n \text{ times}}\}$

$= \{\bar{0}, \bar{a}, 2\bar{a}, 3\bar{a}, \ldots, \overline{(n-1)a}\}$

$= \{\bar{a} \cdot \bar{r} \mid \bar{r} \in \mathbb{Z}_n\}$