Notes 2/24/22

$n\mathbb{Z} = \{ nt \mid t \in \mathbb{Z} \} = (n)\mathbb{Z}$

$= \{ 0, n, 2n, \ldots \}$
$-n, -2n, \ldots$

Jenna
Stephanie
Kimberly

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/-n\mathbb{Z}$

$|\mathbb{Z}/n\mathbb{Z}| = \#$ of elements $= n$

$\mathbb{Z}/I = \{$ left cosets $\}$ I an ideal

$= \{ a+I \mid a \in \mathbb{Z} \}$

$a+I = \{ a+d \mid d \in I \}$ ← left coset

$I = 5\mathbb{Z} = \{ 0, 5, 10, \ldots$
$-5, -10, \ldots \}$

$99+I = \{ 99, 104, 109, \ldots \}$
$94, \ldots$

Fact $\mathbb{Z}$ cosets are either equal or disjoint

Let $a+I$, $b+I$ be $\mathbb{Z}$ cosets

Suppose they have an element in common.

$c \in a+I$ $\}$ $c = a+w$ for some $w \in I$
$c \in b+I$ $\}$ $c = b+v$ ——— $v \in I$

Claim: Then $a+I = b+I$

$a+w = b+v$
$a = b+v-w$

Part 1 $a+I \subseteq b+I$

Part 2 $b+I \subseteq a+I$

Part 1 Let $x \in a+I$.

WTS $x \in b+I$

So $x = a+\alpha$ for some $\alpha \in I$

$x = b+(r-w+\alpha)$

$r-w+\alpha \in I$

$\therefore x = b+\gamma$ for some $\gamma = r-w+\alpha$, $\gamma \in I$

$\therefore x \in b+I$

$99+I = 4+I$

$$5 \overline{)\,99\,} \quad 19 \text{ R } 4$$
$$95$$

$99 = 19 \cdot 5 + 4$

$99 \in 99+I$

$99 = 99+0$

$99 \in 4+I$

$99 = 4+19 \cdot 5$

$$\mathbb{Z}/5\mathbb{Z} = \{0+I, 1+I, 2+I, 3+I, 4+I\}$$

$5\mathbb{Z} = I$

$|\mathbb{Z}/n\mathbb{Z}| = n$

$|\mathbb{Z}/m\mathbb{Z}| = m$

If $\exists$ a bijection between $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$

then they have the same # of elements $\therefore n = m$ or $n = -m$

---

① Ring homomorphism

R, S $\quad f: R \to S$

is a ring homomorphism if

$f(r+s) = f(r) + f(s)$

$f(r \cdot s) = f(r) \cdot f(s)$

$f(1_R) = 1_S$

$R = \mathbb{Z}/n\mathbb{Z}$ $\quad 0_R = 0 + n\mathbb{Z}$ $\quad n\mathbb{Z} = I$

$1_R = 1 + n\mathbb{Z}$

$(a + I) + (b + I) = (a + b) + I$

$(a + I)(b + I) = (ab) + I$

I is an ideal in R is commutative w.r.t

(1) Closed under +

(2) Closed under mult. by elements from R

(1) If $a, b \in I$ then $(a+b) \in I$

(2) If $a \in I$ and $r \in R$ then $ar \in I$ and $ra \in I$

Claim: Multiplication of cosets is well-defined.

What does this mean?

Means: If $a+I = a'+I$ and $b+I = b'+I$

then we wts

$$ab+I = a'b'+I$$

$b \in b+I$

$b+b' \in I$

$b = b+R$ for some $R \in I$

$0 \in I$

$\therefore ab+0 = ab \in ab+I.$

$a+I \leftarrow a = a+0 \in a+I$ since $0 \in I$

$\therefore a \in a'+I$

Hence $a = a'+\alpha$ for some $\alpha \in I$

Similarly $b = b'+\beta$ ——— $\beta \in I$

$$ab = (a'+\alpha)(b'+\beta)$$
$$= a'(b'+\beta) + \alpha(b'+\beta)$$
$$= a'b' + (a'\beta + \alpha b' + \alpha\beta)\gamma$$

$a'\beta \in I$ since $\beta \in I$

$\alpha b' \in I$ since $\alpha \in I$

$\alpha\beta \in I$ since $\alpha \in I$

$$= a'b' + \gamma \quad \text{for some } \gamma \in I$$
$$\in a'b' + I$$

11.06 $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$(1+I) \longrightarrow 1+I$$
$$(1+I)+(1+I) \longrightarrow (1+I)+(1+I)$$
$$2+I \longrightarrow 2+I$$

11.10

$M_2(\mathbb{R}) = \{ 2\times 2 \text{ matrices with entries in } \mathbb{R} \}$

11.08 $f: R \to S$ is a ring homomorphism

(1) f is a homomorphism

(2) f is 1-1

(3) f is onto

R is an integral domain $\iff S$ is

$\Rightarrow$ Assume R is an integral domain

WTS S is an integral domain.

What is an integral domain?

Commutative Ring with Identity

and no zero divisors, i.e.

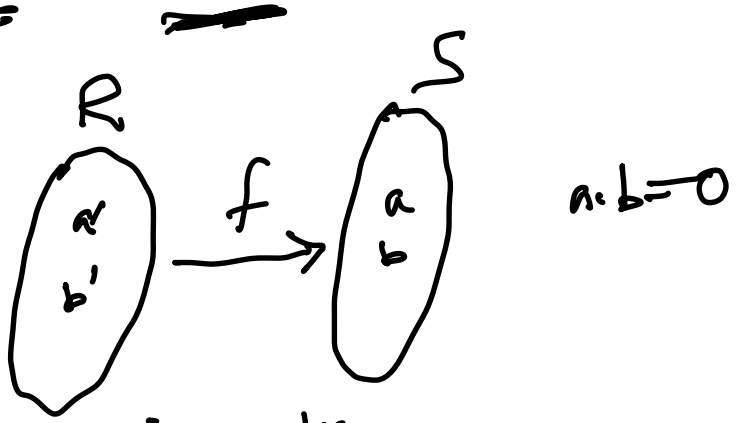
if $a \cdot b = 0$ then $a = 0$ or $b = 0$

WTS S has no zero divisor

Let $a, b \in S$, and suppose

$a \cdot b = 0$

WTS $a = 0$ or $b = 0$



Suppose $a \neq 0$ and $b \neq 0$

wts $a \cdot b \neq 0$ i.e. show $ab \neq 0$

Since f is onto $\exists\, a' \in R$ with

$$f(a') = a$$

and $\exists\, b' \in R$ with

$$f(b') = b$$

So $f(a'b') = f(a') \cdot f(b')$ since f is a homomorphism

$= a \cdot b$

$= 0$

$f(0) = 0$

$\therefore\ a'b' = 0$ since f is 1-1

Lemma If f is a ring homomorphism

$f: R \to S$

then $f(0) = 0$

$0 + 0 = 0$

$f(0+0) = f(0)$

$f(0) + f(0) = f(0)$

$[f(0) + f(0)] - f(0) = f(0) - f(0)$

$f(0) = 0$

$f(a'b') = f(2)$

$\therefore a'b' = 0$ since f is 1-1.

But $a', b' \in R$, and R has no zero divisors. $\therefore a' = 0$ or $b' = 0$

$a = f(a') = f(0) = 0$

or

$b = f(b') = f(0) = 0$

F is a field – commutative ring with identity

– every non-zero element in F has a multiplicative inverse

$\mathbb{Q} = \{$ rationals $\}$ field

$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1 \quad a \neq 0$

$\mathbb{Z}_p \quad p =$ prime.

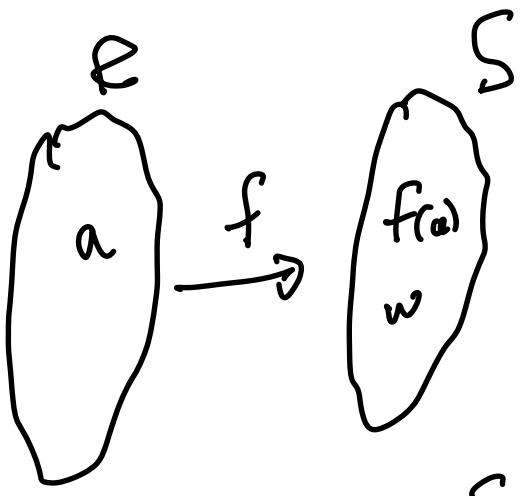
Suppose $f: R \to S$ an isomorphism

suppose R is a field. Will S is a field

$\Leftarrow$ Conversely suppose S is a f.d. WTS R is a field

Let $a \in R$, $a \neq 0$

WTS a has an inverse under $\cdot$.



Consider $f(a) \in S$

Since f is 1-1, $a \neq 0 \Rightarrow f(a) \neq 0$

$f(a) \in S$

$\therefore$ $f(a)$ has an inverse in S

Say $w = f(a)^{-1}$ $\quad f(a) \cdot w = 1_S$

Since f is onto, $\exists\, b \in R$ with

$f(b) = w$

$a \longrightarrow f(a)$

$b \longrightarrow w$

$f(a) \cdot w = 1_S$

Since f is a homomorphism

$f(1_R) = 1_S$

$f(ab) = f(a)f(b) = f(a) \cdot w = 1_S$

$f(ab) = f(1_R)$

f is 1-1.

$\therefore \quad ab = 1_R$

So a is a unit in R,

if a has an inverse in R.