$\mathbb{Z} \times \mathbb{Z}$ is a ring with these operations

$$(a,b)+(x,y)=(a+x,b+y)$$
$$(a,b)(x,y)=(ax,by)$$

distributive rule:

$$(a,b)\left[(x,y)+(w,z)\right]$$
$$=(a,b)(x+w,y+z)$$
$$=(ax+aw,by+bz)$$
$$=(ax,by)+(aw,bz)$$
$$=(a,b)(x,y)+(a,b)(w,z)$$

associative

$$(a,b)\left[(x,y)(w,z)\right]$$
$$=(a,b)(xw,yz)$$
$$=(a(xw),b(yz))$$
$$=((ax)w,(by)z)=(ax,by)(w,z)$$
$$=\left[(a,b)(x,y)\right](w,z)$$

Ex: Let $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be given by $\varphi(a,b)=a$

φ is a ring hom.

Let $x=(a_1,b_1)$ and $y=(a_2,b_2)$ be in $\mathbb{Z}\times\mathbb{Z}$.
Then,

$$\varphi(x+y)=\varphi(a_1+a_2,b_1+b_2)=a_1+a_2=\varphi(a_1,b_1)+\varphi(a_2,b_2)=\varphi(x)+\varphi(y)$$

and

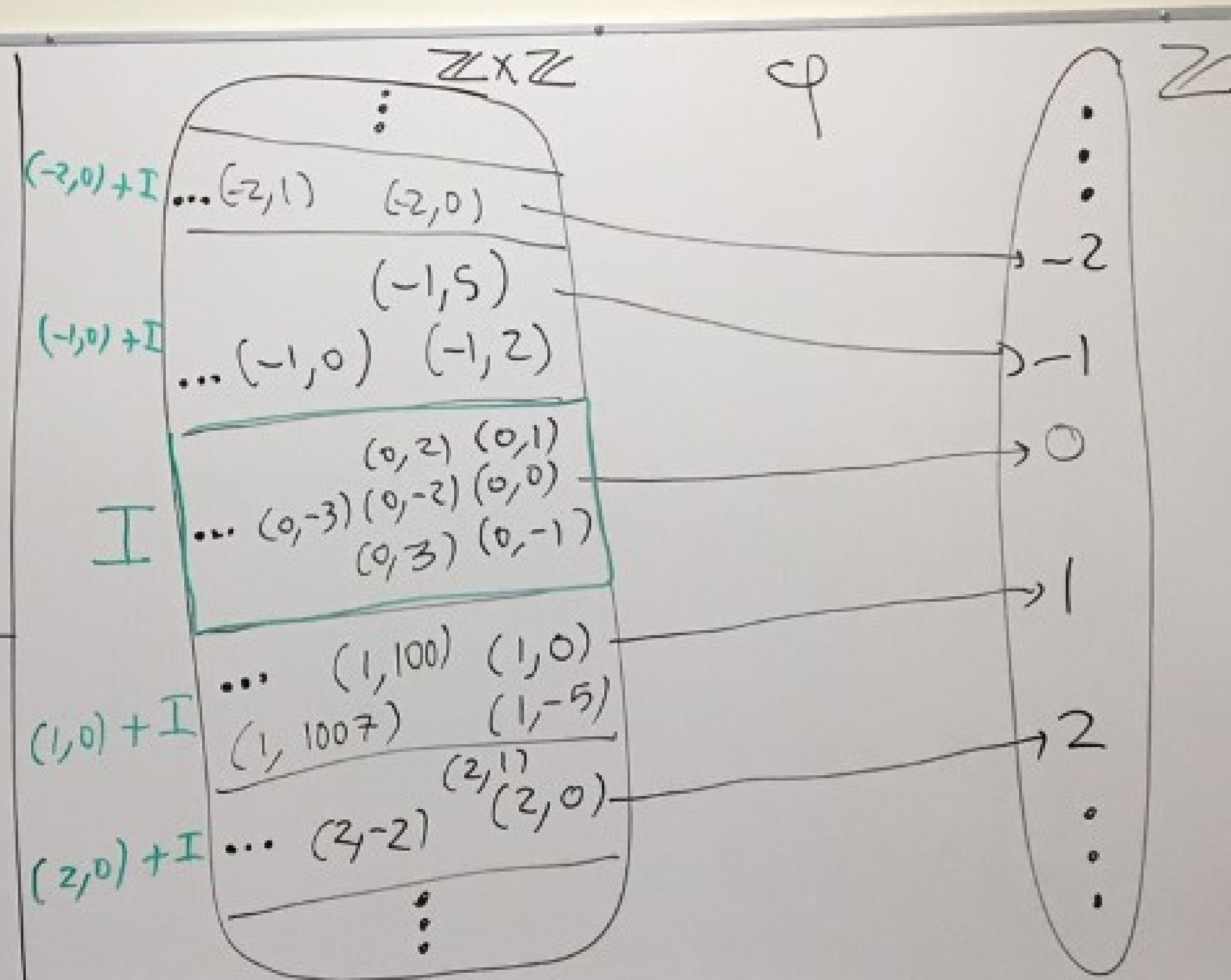
$$\varphi(xy)=\varphi(a_1a_2,b_1b_2)=a_1a_2=\varphi(a_1,b_1)\varphi(a_2,b_2)=\varphi(x)\varphi(y)$$

$+\varphi(y)$

Kernel of φ

$$\ker(\varphi) = \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid \varphi(a,b) = 0\}$$
$$= \{(a,b) \in \mathbb{Z}\times\mathbb{Z} \mid a = 0\}$$
$$= \{(0,b) \mid b \in \mathbb{Z}\}$$

So, $I = \ker(\varphi) = \{(0,b) \mid b \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}\times\mathbb{Z}$.



1st iso. thm

$$\mathbb{Z}\times\mathbb{Z}/I \cong \operatorname{im}(\varphi) = \mathbb{Z}$$

$\boxed{7.4}$ – Properties of ideals

Def: Let R be a commutative ring. We say that an ideal I of R is principal if there exists $a \in R$ where

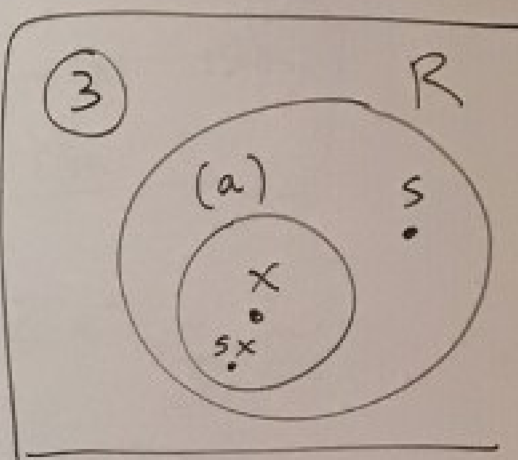
$$\underbrace{I = \{ra \mid r \in R\}}_{\text{notated by } Ra \text{ or } (a)}$$

ideal generated by a

Prop: If R is a commutative ring and $a \in R$ then

$$(a) = \{ra \mid r \in R\}$$

is an ideal of R.



proof:

① Since R is a ring, $\exists\, 0 \in R$. Thus, $0 = 0 \cdot a \in (a)$.

② Let $x, y \in (a)$. Then $x = r_1 a$ and $y = r_2 a$ where $r_1, r_2 \in R$. Then $x - y = r_1 a - r_2 a = \underbrace{(r_1 - r_2)}_{\text{in } R} a \in (a)$

③ Let $x \in (a)$ and $s \in R$. Then $x = ra$ for some $r \in R$. Then, $sx = s(ra) = \underbrace{(sr)}_{\text{in } R} a \in (a)$ and

$xs = (ra)s \overset{\text{R is commutative}}{=} (rs)a \in (a)$.

By ①, ②, ③ (a) is an ideal of R.

Ex: All the ideals of $\mathbb{Z}$ are principal.

Any ideal of $\mathbb{Z}$ is of the form

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = (n)$$

where $n \geq 0$.

Prop: Let R be a ring with identity $1 \neq 0$.

① Let I be an ideal of R. Then $I = R$ iff I contains a unit of R.

② Suppose further that R is commutative. Then, R is a field iff the only ideals of R are $\{0\}$ and R.

P

①

$(\Longrightarrow)$

S

$(\Longleftarrow)$

uni-

be

in F

Sinc

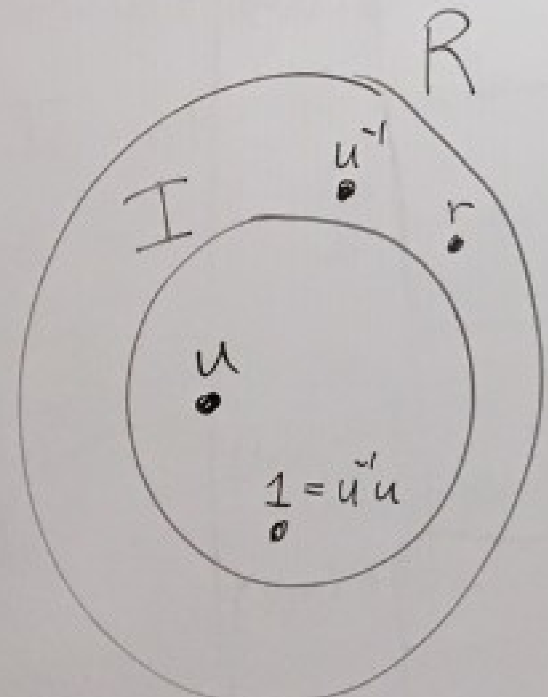
Proof:

① Let I be an ideal of R.

($\Longrightarrow$) If $I = R$, then $1 \in I$.
So, I contains a unit.

($\Longleftarrow$) Suppose I contains a unit of R. Let $u \in I$ be a unit. So, u^{-1} exists in R with $u^{-1}u = uu^{-1} = 1$.
Since I is an ideal

$$1 = \underbrace{u^{-1}}_{\text{in } R}\ \underbrace{u}_{\text{in } I} \in I.$$



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

So, $R \subseteq I$.
Thus, $R = I$.

Side note:

1-step method of proof

$$r = \underbrace{(r \cdot u^{-1})}_{\text{in } R}\ \underbrace{u}_{\text{in } I} \in I$$

(2) Suppose R is a commutative ring with $1 \neq 0$.

($\Longrightarrow$) Suppose R is a field.
Let I be an ideal of R.
Either $I = \{0\}$ or $I \neq \{0\}$.
Suppose $I \neq \{0\}$. Then there exists $x \in I$ with $x \neq 0$.
Since R is a field and $x \neq 0$ we have that x is a unit.
So by part 1, $I = R$.
Thus, either $I = \{0\}$ or $I = R$.

($\Longleftarrow$) Suppose the only ideals of R are $\{0\}$ and R.
We want to show that R is a field.
Let $x \in R$ with $x \neq 0$.
We need to show that x is a unit.
Consider the ideal

$$I = (x) = \{xr \mid r \in R\}$$

By assumption either $I = \{0\}$ or $I = R$.

unit.

} or $I=R$.

We know $x = x \cdot 1 \in I$

[Here we are using that $1 \neq 0$ is in R]

And $x \neq 0$.

So, $I \neq \{0\}$.

since $x \in I$ and $x \neq 0$

Thus, $I = R$.

So, $1 \in I$.

Thus, $1 = xr$ for some $r \in R$.

So, x is a unit.

Thus every non-zero element of R is a unit. So, R is a field. $\blacksquare$