

2/25/14

Exam 1 Thursday

Today Review

Next week: NO CLASS

(But I will assign HW 3)

Review for Exam 1

① Properties of general rings

② Properties of  $\mathbb{Z}$  &  $K[x]$

① Definitions of

ring / homomorphism / subring / ideal.

We say  $(R, +, \cdot, 0, 1)$  is a ring if

- $(R, +, 0)$  is abelian group
- $(R, \cdot, 1)$  is commutative semigroup
- For all  $a, b, c \in R$  we have

$$a(b+c) = ab+ac$$

- $0 \neq 1$

Given rings  $R, S$  we say  $\varphi: R \rightarrow S$   
is a ring homomorphism if

}

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$ .

If  $\varphi: R \rightarrow S$  is a ring hom then

$$\text{im } \varphi := \{ \varphi(r) : r \in R \} \subseteq S$$

is a subring and

$$\text{ker } \varphi := \{ r \in R : \varphi(r) = 0_S \} \subseteq R$$

is not a subring. What is it?

Def: We say  $I \subseteq R$  is an ideal if

- $I$  is a subgroup of  $(R, +, 0)$
- For all  $a \in I$ ,  $b \in R$  we have  
 $ab \in I$ .

★ Theorem: Given subset  $I \subseteq R$  we have

$I$  is an ideal  $\iff \exists$  ring  $R'$  and hom  
 $\varphi: R \rightarrow R'$  with  $I = \text{ker } \varphi$ .

Proof  $\Leftarrow$  Easy

$\Rightarrow$ . We must construct the ring  $R'$  and the map  $\varphi$ . Given an ideal  $I \subseteq R$  we define a relation on  $R$  by.

$$a \sim b \iff a - b \in I.$$

Prove that this is an equivalence

- $a \sim a$
- $a \sim b \Rightarrow b \sim a$
- $a \sim b \ \& \ b \sim c \Rightarrow a \sim c$

with equivalence classes given by cosets

$$\begin{aligned} [a] &= \{ b \in R : a \sim b \} \\ &= \{ b \in R : a - b \in I \} \\ &= \{ b \in R : a - b = x \in I \} \\ &= \{ a + x : x \in I \} \\ &= a + I. \end{aligned}$$

Prove that we have

$$a + I = b + I \iff a \sim b.$$

Consider the set of cosets

$$R/I := \{ a+I \mid a \in R \}.$$

Define addition and multiplication by

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

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

Show that these are well-defined and make  $R/I$  into a ring. Show that the map

$$\begin{aligned} \varphi: R &\longrightarrow R/I \\ a &\longmapsto a+I. \end{aligned}$$

is a ring homomorphism with  $\ker \varphi = I$ .

★ First Isomorphism Theorem:  
Given a ring homomorphism

$$\varphi: R \longrightarrow S$$

↓

the function

$$\begin{aligned}\bar{\varphi} : R/\ker \varphi &\rightarrow \text{im } \varphi \\ a + \ker \varphi &\longmapsto \varphi(a)\end{aligned}$$

is a ring isomorphism.

Proof: It's a surjective ring map (easy).  
To see that it's well defined and  
injective note that

$$\begin{aligned}a + \ker \varphi = b + \ker \varphi &\iff a - b \in \ker \varphi \\ &\iff \varphi(a - b) = 0 \\ &\iff \varphi(a) - \varphi(b) = 0 \\ &\iff \varphi(a) = \varphi(b)\end{aligned}$$

$\implies$  well-defined  $\checkmark$

$\Leftarrow$  injective  $\checkmark$

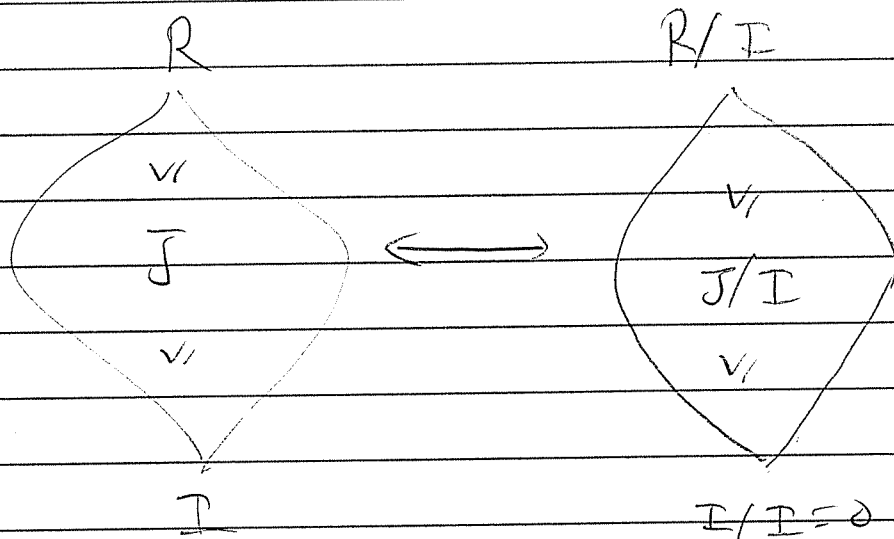
### ★ Correspondence Theorem

Given ideals  $I \subseteq J \subseteq R$  note that

$$J/I := \{ a + I : a \in J \}$$

is an ideal of  $R/I$ .

then the map  $J \mapsto J/I$  defines an isomorphism of lattices



Proof omitted. ///

Applications:

- classify subgroups of  $\mathbb{Z}/n\mathbb{Z}$ .
- prove that

$I \leq R$  maximal  $\iff R/I$  field.

Recall the Diamond Isomorphism from HW 2:

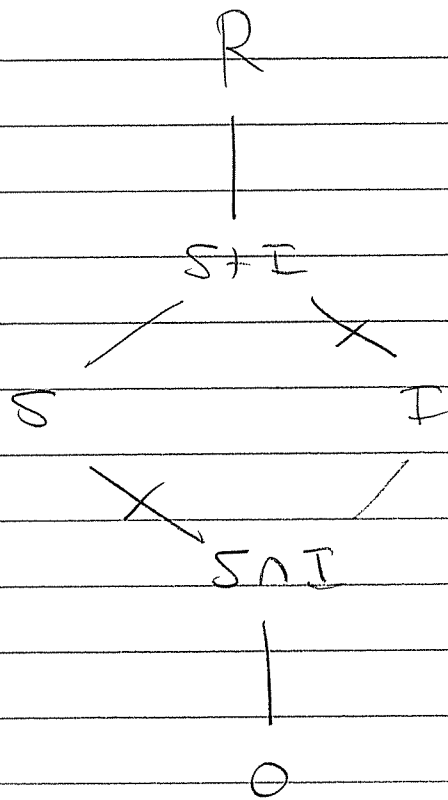


IF  $S \subseteq R$  is a subring and  $I \subseteq R$  is an ideal, then

- $S+I \subseteq R$  is a subring
- $I \subseteq S+I$  is an ideal
- $S \cap I \subseteq S$  is an ideal
- We have an isomorphism

$$\frac{S}{S \cap I} \cong \frac{S+I}{I}$$

Picture :



See the Diamond ?

## (2) Properties of $\mathbb{Z}$ and $K[x]$

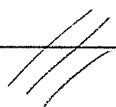
We say ring  $R$  is a domain if

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

We say domain  $R$  is Euclidean if we have  $\delta: R - \{0\} \rightarrow \mathbb{N}$  such that for all  $a, b \in R$  with  $b \neq 0$ , there exist  $q, r \in R$  such that

- $a = qb + r$
- $r = 0$  or  $\delta(r) < \delta(b)$ .

★ Theorem: Euclidean  $\implies$  PID.

Proof: Let  $I \leq R$  be an ideal. If  $I = (0)$  we're done so suppose  $I \neq (0)$  and choose  $0 \neq a \in I$  with  $\delta(a)$  minimal. Show that  $I = (a)$ . 

Corollary:  $\mathbb{Z}$  and  $K[x]$  are PIDs.



This follows from the fact that  $\mathbb{Z}$  is Euclidean with  $\delta(n) = |n|$  and  $K[x]$  is Euclidean with  $\delta(f) = \deg(f)$ . ///

[ Given a ring  $R$  and  $f(x), g(x) \in R[x]$ , recall that if  $g(x)$  is monic then  $\exists q, r \in R[x]$  such that

- $f(x) = q(x)g(x) + r(x)$
- $r = 0$  or  $\deg(r) < \deg(g)$ .

If  $R = K$  a field then every nonzero  $g \in K[x]$  is monic, hence  $K[x]$  is Euclidean. ]

Since  $\mathbb{Z}$  is a PID, every ideal looks like  $(n)$  for  $n \in \mathbb{Z}$ .

Recall that

$$(a) + (b) = (d)$$

$$(a) \cap (b) = (m)$$

where  $d = \gcd(a, b)$  &  $m = \text{lcm}(a, b)$ .

Thus given ideals  $I, J \in R$  we think

$$I + J \approx \gcd(I, J)$$

$$I \cap J \approx \text{lcm}(I, J).$$

If  $I + J = (1)$  (i.e. if  $I, J$  are "coprime")  
then we have

$$I \cap J = IJ \quad \text{and}$$

$$\frac{R}{IJ} \approx \frac{R}{I} \times \frac{R}{J}.$$

When  $R = \mathbb{Z}$  and  $a, b \in \mathbb{Z}$  are coprime  
this says that

$$\mathbb{Z}/(ab) \approx \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

"Chinese Remainder Theorem"

This gives an isomorphism of groups of units:

$$(\mathbb{Z}/(ab))^{\times} \approx (\mathbb{Z}/(a))^{\times} \times (\mathbb{Z}/(b))^{\times}$$

and this implies that



$$\varphi(ab) = \varphi(a) \varphi(b)$$

$\varphi$  = Euler's totient function.

We use this to compute

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

$$\begin{aligned} \text{E.g. } \varphi(100) &= 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ &= 40. \end{aligned}$$

Then applying Lagrange's Theorem to  $(\mathbb{Z}/(n))^{\times}$  gives Euler's Theorem

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

for all  $a, n$  with  $\gcd(a, n) = 1$ .

Application: Compute the last two digits of  $73^{402}$ .

↓

$$73^{402} = 73^{10 \cdot 40 + 2}$$
$$= (73^{40})^{10} 73^2$$

$$\equiv (1)^{10} \cdot 73^2 \pmod{100}$$

$$\equiv 73^2 \pmod{100}$$

$$\equiv 5329 \pmod{100}$$

$$\equiv 29 \pmod{100}$$

MAGIC .

$$\begin{array}{r} \phantom{0} 73 \\ \times 73 \\ \hline 219 \\ 5110 \\ \hline 5329 \end{array}$$