Welcome to MTH 562.

– sorry, NO CLASS this Friday Jan 20, 2012 (all hail the USA).

Text: Artin, "Algebra"

Evaluation:

25%	Homework	
25%	Exam 1	No Final Exam.
25%	Exam 2	
25%	Exam 3	

Broad Outline.

Then
MTH 561 (Artin Ch. 1–10).
Main Idea: Groups (non-commutative).
Main Example: Matrix Groups.
Applications: Geometry (Lie Theory, Physics)

Now
MTH 562 (Artin Ch. 11–16).
Main Idea: Rings (commutative).
Main Examples: $\mathbb{Z}$ (integers) & Polynomials.
Applications: Number Theory & Algebraic Geometry (Physics?)

Def: A ring is a set R with two binary operations $(a,b) \mapsto a+b$, $(a,b) \mapsto a \times b$.
Satisfying:

+ • $(R, +, 0)$ is an abelian group.
  - $a+b = b+a \quad \forall\, a,b \in R$
  - $a+(b+c) = (a+b)+c \quad \forall\, a,b,c \in R$
  - $\exists\, 0 \in R,\ a+0 = a \quad \forall\, a \in R$.
  - $\forall a \in R\ \exists\, b \in R,\ a+b = 0$
    (Notation: say $b =$ "$-a$")

× • $a \times (b \times c) = (a \times b) \times c \quad \forall\, a,b,c \in R$

• Distributive Laws
  - $a \times (b+c) = a \times b + a \times c$
    $(a+b) \times c = a \times c + b \times c$
    $\forall\, a,b,c \in R$.

☆ Warning: Artin also says

• $a \times b = b \times a \quad \forall a,b$ (commutative)
• $\exists\, 1 \in R,\ 1 \times a = a \quad \forall\, a \in R$

(i.e. $(R, \times, 1)$ is a commutative semigroup)

Let $R^\times \subseteq R$ be group of units.

$$R^\times = \{ a \in R : \exists\, b \in R,\ ab = ba = 1 \}$$

Everyone agrees: $R^\times \subsetneq R - \{0\}$.

is possible.

Def. A field is a comm. ring R with 1 such that $R^\times = R - \{0\}$.

Examples.

(1) $\mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$

(2) $\mathbb{Z}/n\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$

where $\bar{a} = a + n\mathbb{Z} = \{ \ldots, a-n, a, a+n, a+2n, \ldots \}$

and $\bar{a}\,\bar{b} = \overline{ab}$

$\bar{a} + \bar{b} = \overline{a+b}$

"Modular Arithmetic".

(3) $C[0,1] = \{ f : [0,1] \to \mathbb{R},\ f \text{ continuous} \}$

Given $f, g \in C[0,1]$ define $f+g$, fg by

$$(f+g)(x) := f(x) + g(x) \qquad \forall\, x \in [0,1].$$
$$(fg)(x) := f(x)\,g(x)$$

NB: $C[0,1]$ is also an $\mathbb{R}$-vector space with scalar mult by $r \in \mathbb{R}$:

$$(rf)(x) := r\,f(x).$$

Ring + $\mathbb{R}$-v.s. = $\mathbb{R}$-"algebra".

(4) If R is a ring, define the ring of polynomials

$$R[x] := \{ a_0 + a_1 x + a_2 x^2 + \cdots \;;\; a_0, a_1, \ldots \in R,$$
$$a_i = 0 \text{ for all but finitely many } i \}.$$
("$a_i = 0$ a.e." — almost everywhere)

Let $f(x) = \sum_k a_k x^k$, $g(x) = \sum_k b_k x^k$. Then

$$(f+g)(x) := f(x) + g(x)$$
$$= (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2$$
$$= \sum_k (a_k + b_k) x^k.$$

$$(fg)(x) := f(x)g(x) = (a_0 + a_1 x + \cdots)(b_0 + b_1 x + \cdots)$$
$$= a_0 b_0 + (a_0 b_1 + a_1 b_0) x$$
$$+ (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \cdots$$
$$= \sum_k \left(\sum_{i+j=k} a_i b_j \right) x^k$$

finite?

Define: Given $f = \sum a_k x^k \in R[x]$

$\deg(f) = \max\{n : a_n \neq 0\}$

i.e. $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

Q: $\deg(fg) = \deg(f) + \deg(g)$? (HW).

(5) $R[[x]]$

$:= \{a_0 + a_1 x + a_2 x^2 + \cdots \; ; \; a_0, a_1, \cdots \in R\}$

The ring of formal power series.

$+, \times$ same as $R[x]$.

Some structure theory:

Q: What is a subring?

Q: What is a ring homomorphism?

Some Business:

- HW 1 due Wed Feb 1.
- Exams
  1. Fri Feb 17
  2. Wed Mar 28
  3. Fri Apr 27

Today: Structure Theory

Group	Ring
Subgroup	Subring
Normal Subgroup	?

Recall: Given subgroup $H \leq G$,

$H \trianglelefteq G$ (normal) $\equiv$ $H = \ker \varphi$ for some group hom $\varphi: G \to G'$

$g \in G, h \in H \Rightarrow ghg^{-1} \in H$

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

$\ker \varphi = \{a \in G : \varphi(a) = 1_{G'}\}$.

Proof: Given $g \in G$, $a \in \ker \varphi$,

$\varphi(gag^{-1}) = \varphi(g)\underbrace{\varphi(a)}_{1}\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$

$\Rightarrow gag^{-1} \in \ker \varphi \Rightarrow \ker \varphi \leq G$.

Conversely, let $H \trianglelefteq G$ and construct the quotient group

$$G/H := \{ gH : g \in G \}$$

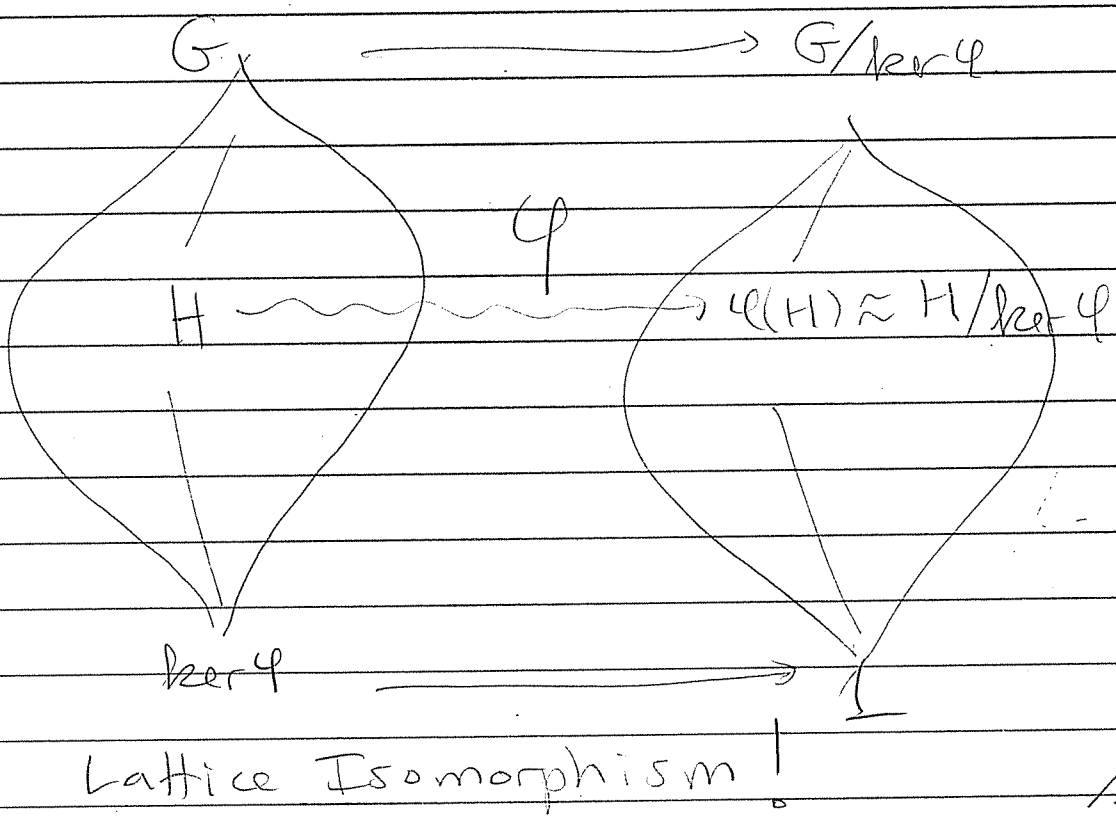
with $(aH)(bH) = (ab)H$. Then $H = \ker \pi$ for

$$\begin{aligned} G &\xrightarrow{\pi} G/H \\ g &\longmapsto gH. \end{aligned}$$

$\blacksquare$

$\rightsquigarrow$ Isomorphism Theorems.

Given hom $\varphi : G \to G'$.



Lattice Isomorphism!

$\blacksquare$

Now: Do same for rings.

DEF: Given ring R say $S \subseteq R$ is subring if:
- $a, b \in S \Rightarrow a+b \in S$ & $a-b \in S$ (i.e. $0 \in S$)
- $a, b \in S \Rightarrow ab \in S$.
- ($1 \in S$) ?? DO WE WANT THIS?

↑ if it exists

Q: Correct def. of ring hom? $\varphi: R \to S$

① $\varphi(a+b) = \varphi(a) + \varphi(b)$
② $\varphi(ab) = \varphi(a)\varphi(b)$.

Think... ① $\Rightarrow \varphi(0_R) = 0_S$
① $\Rightarrow \varphi(-a) = -\varphi(a)$

HW

Also want $\varphi(1_R) = 1_S$
$\varphi(a^{-1}) = \varphi(a)^{-1}$ if a^{-1} exists

But ② is not enough ☹ (Why?)

DEF: Say $\varphi: R \to S$ is ring homomorphism if
① $\varphi(a+b) = \varphi(a) + \varphi(b)$
② $\varphi(ab) = \varphi(a)\varphi(b)$
③ $\varphi(1_R) = 1_S$
$\forall a, b \in R$

↑ ↑ if they exist

Idea: kernels are important.

$\ker\varphi := \{ a \in R : \varphi(a) = 0_S \}$

- $\ker\varphi \subseteq R$ is (weak) subring.

Proof: Let $a, b \in \ker\varphi$ i.e. $\varphi(a) = \varphi(b) = 0$.
Then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$
& $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$
↖ HW3 MTH 561

$\Rightarrow a+b, ab \in \ker\varphi$.
(Possibly $1_R \notin \ker\varphi$)

- But more is true.
SPECIAL PROPERTY of KERNELS.

Given $a \in R$, $b \in \ker\varphi$ we have
$ab \in \ker\varphi$ & $ba \in \ker\varphi$.

Proof: HW 3 MTH561.
$\varphi(ab) = \varphi(a)\varphi(b) = \varphi(a) \cdot 0 = 0$
$\varphi(ba) = \varphi(b)\varphi(a) = 0 \cdot \varphi(a) = 0$

So What ?

DEF: Let $S \subseteq R$ be (weak) subring.
We say S is a (two-sided) ideal if

$r \in R,\ a \in S \implies ra \in S \ \&\ ar \in S$

(S closed under multiplication by R).

Remark: NO interesting ideal contains 1
since $1 \in S \implies S = R$.

Notion "subring" is troublesome. After today we'll never use it.

Better DEF: Say $I \subseteq R$ is an ideal if

(1) $a, b \in I \implies a+b \in I$
(2) $a \in I,\ r \in R \implies ar \ \&\ ra \in I$.

Fundamental Theorem: Given $I \subseteq R$,

I is ideal $\equiv$ $I = \ker \varphi$ for some ring hom $\varphi : R \to R'$.

Proof: Given ideal $I \trianglelefteq R$ need a hom $\varphi : R \to ?$ with $\ker \varphi = I$.

Note: $I \trianglelefteq R$ as "+" groups so we have group

$$R/I := \{ r + I : r \in R \}$$

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

Get $R \xrightarrow{\pi} R/I$ hom of "+" groups
$r \longmapsto r + I$

with $\ker \pi = I$.

Q: What more do we need? hom.
A: Need mult on R/I with $\pi(rs) = \pi(r)\pi(s)$.

DEF: $(r+I)\cdot(s+I) := (rs) + I$.

HW 1.4: This is well-defined since I is an ideal.

$\Rightarrow$ R/I is a ring ("quotient ring").

with ring hom $R \xrightarrow{\pi} R/I$
$r \longmapsto r + I$.

$I = \ker \varphi$. ▨

Business

- HW 1 Wed Feb 1
- Exams: Fri Feb 17
  Wed Mar 28
  Fri Apr 27
- Office Hours: Mon ~~12:20 – 1:10~~
  Wed ~~12:20 – 1:10~~
  Thurs 2:30 – 3:20

Groups
Subgroups
Normal Subgroups
} → Rings → Ideals

DEF: Say $I \subseteq R$ is an ideal if

(1) $u, v \in I \Rightarrow u+v \in I$
(2) $a \in R, u \in I \Rightarrow au \in I$ & $ua \in I$.
($RI \subseteq I$ & $IR \subseteq I$).

NB: Given $u, v \in I$ we have $-v \in I$
since $-1 \in R \Rightarrow (-1)v = -v \in I$. (HW 3.7)
Then $u - v = u + (-v) \in I$.

Given ideal $I \subseteq R$ we may construct the quotient ring

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

$(a+I) + (b+I) := (a+b) + I$ } HW Check well-defined.
$(a+I) \cdot (a+I) := (ab) + I$ }

Remark: Do we have

$$(ab) + I = (a+I)(b+I)$$
$$= \{(a+u)(b+v) : u, v \in I\} \quad ?$$

NO. We have

$(a+I)(b+I) \subseteq (ab) + I$.

~~not usually~~ a coset. Oh well ...

Fundamental Theorem: Given ring R and subset $I \subseteq R$ we have

I is ideal $\iff$ $\exists$ ring hom $\varphi : R \to R'$ with $I = \ker \varphi$.

Proof: Let $R' = R/I$, $\varphi : R \to R/I$

$a \longmapsto a + I$ ∎

Ideals of R have a "lattice" structure.

Given ideals $I, J \subseteq R$,

(1) $I \cap J$ is an ideal.

Proof:

- For $x, y \in I \cap J$ we have $x, y \in I$
$\Rightarrow x+y \in I$, $x, y \in J \Rightarrow x+y \in J$.
Hence $x+y \in I \cap J$.
- Given $a \in R$, $x \in I \cap J$ we have.
$x \in I \Rightarrow ax, xa \in I$, $x \in J \Rightarrow ax, xa \in J$.
Hence $ax, xa \in I \cap J$ ∎

(2) $I \cup J$ is not an ideal, so.... define.

$$I \vee J := \bigcap_{\text{ideals } S \supseteq I \cup J} S \supseteq I \cup J.$$

"smallest ideal containing $I \cup J$"

Proposition: $I \vee J = I + J$

$:= \{u+v : u \in I, v \in J\}$.

Proof: "$\subseteq$"

Note $I+J$ is an ideal.

- given $u_1+v_1, u_2+v_2 \in I+J$, we have
$(u_1+v_1)+(u_2+v_2) = (u_1+u_2)+(v_1+v_2) \in I+J$ ✓
($u_1+u_2 \in I$, $v_1+v_2 \in J$)

- given $a \in R$, $u+v \in I+J$ we have
$a(u+v) = (au)+(av) \in I+J$.
$(u+v)a = (ua)+(va) \in I+J$. ///

Hence $I+J$ is an ideal $\supseteq I \cup J$ (Why?)

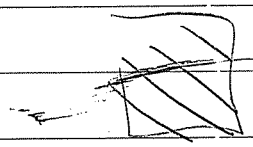
$\Rightarrow I \vee J = (I+J) \cap \bigcap_{\text{other } S \supseteq I \cup J} S \subseteq I+J$ ///

Next show $I+J \subseteq I \vee J$.

Given $u \in I$, $v \in J$ note that
$u \in I \subseteq I \cup J \subseteq I \vee J$.
$v \in J \subseteq I \cup J \subseteq I \vee J$.

Then since $I \vee J$ is an ideal,
$u, v \in I \vee J \Rightarrow u+v \in I \vee J$.

Since $u+v \in I \vee J \quad \forall u \in I, v \in J$,
we conclude
$I+J \subseteq I \vee J$.



"zero ideal" "unit ideal"

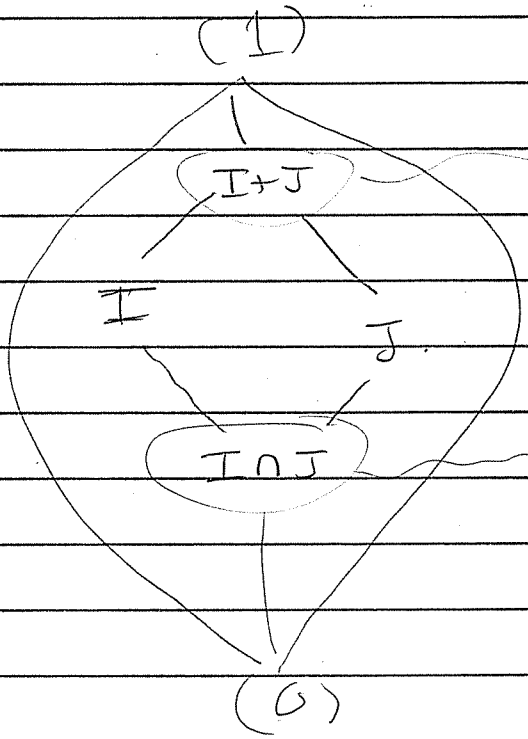
DEF: Let $(0) = \{0\} \subseteq R$, $(1) = R$,

$\mathcal{L}(R) := \{ I : I \subseteq R \text{ is ideal} \}$. Then

$(\mathcal{L}(R), \cap, +, (0), (1))$

is a lattice (the lattice of ideals)

Pic:



plays role of gcd = greatest common divisor

plays role of lcm = least common multiple.

Think:

- $A \subseteq B$ means "B divides A"
- (1) "divides everything"
- "everything divides" (0).

Office Hours Try Again:

Mon 1:25 – 2:15

Wed 1:25 – 2:15

Thurs 2:30 – 3:20

Typo(!) on HW 1 Problem 8(b)

$f(i) = f(-i) \in \mathbb{C} \quad \forall\, f(x) \in \mathbb{R}[x]$ FALSE

$\overline{f(i)} = f(-i) \in \mathbb{C} \quad \forall\, f(x) \in \mathbb{R}[x]$ TRUE

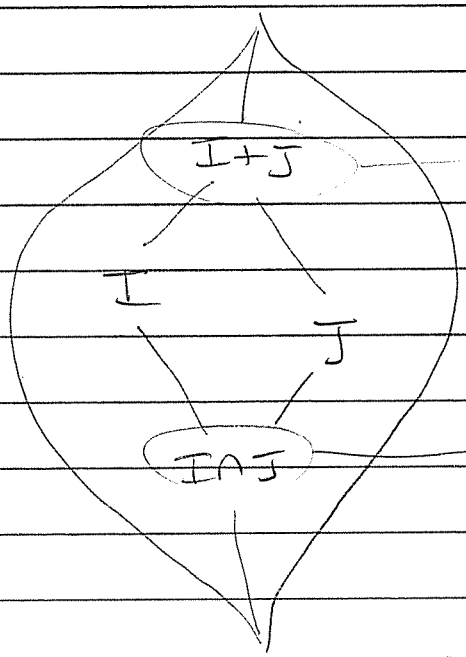
$(f(i) = 0 \iff f(-i) = 0)$

See fix on webpage ///

Recall the "Lattice" of Ideals $\mathcal{L}(R)$:

(see Wiki)

$(1) = R$ unit ideal



$(0) = \{0\}$ zero ideal.

1st Isomorphism Theorem:

Given ring homomorphism $\varphi : R \to S$ we have a canonical ring isomorphism

$$R/\ker\varphi \cong \operatorname{im}\varphi$$
$$a + \ker\varphi \longmapsto \varphi(a)$$

Proof: ① Well-Defined? Suppose $a+\ker\varphi = b+\ker\varphi$

$\Rightarrow \exists\, x, y \in \ker\varphi,\ a+x = b+y$

$\Rightarrow \varphi(a) = \varphi(a)+0 = \varphi(a)+\varphi(x) = \varphi(a+x)$

$= \varphi(b+y) = \varphi(b)+\varphi(y) = \varphi(b)+0 = \varphi(b)$ ✓

② Injective? sp. $\varphi(a) = \varphi(b)$.

$\Rightarrow \varphi(a-b) = \varphi(a) - \varphi(b) = 0$

$\Rightarrow a-b \in \ker\varphi$,

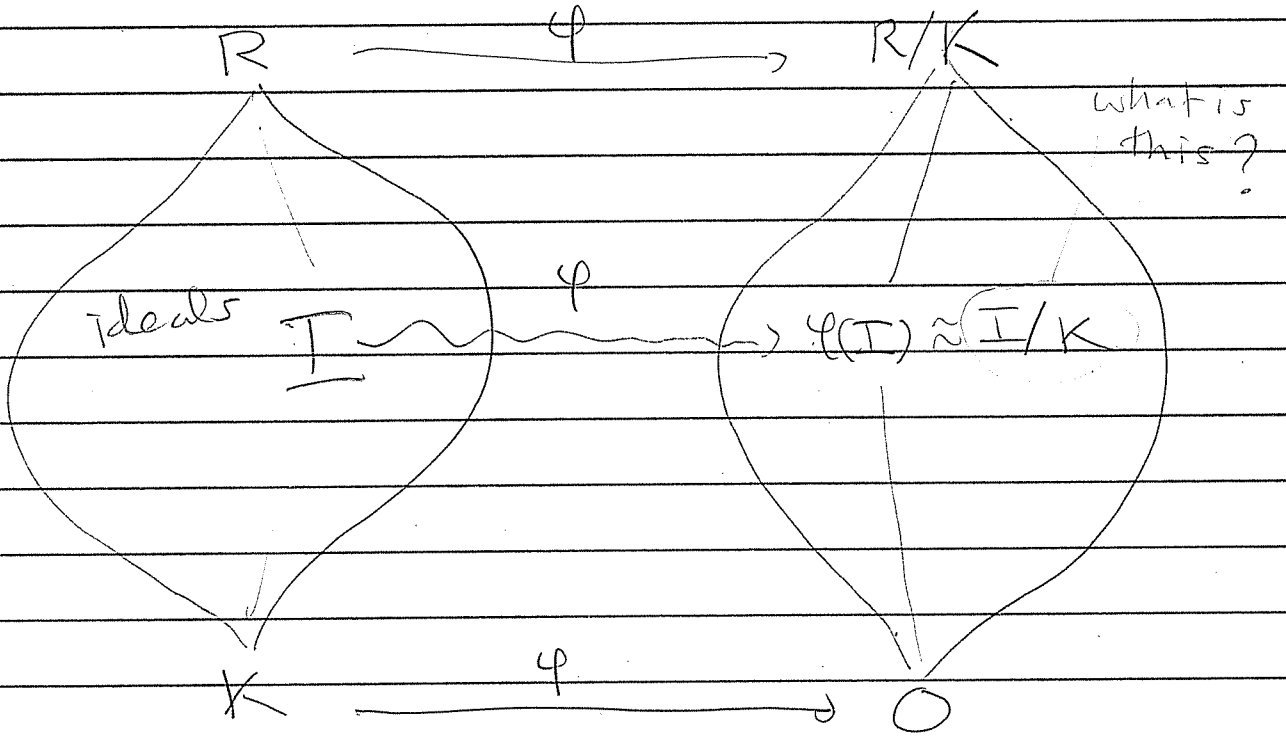
$\Rightarrow a+\ker\varphi = b+\ker\varphi$ ✓ (Recall Exam 2).

③ Surjective? Built-in.

④ Homomorphism? Built-in.

"The" Isomorphism Theorem:

Given surjective ring hom $\varphi: R \to R/K$ with $K = \ker\varphi$, there is a lattice isomorphism



Details i omitted :)

Take-away: Every category (groups, rings, etc.) has similar isomorphism theorems.

The Prototype : $\mathbb{Z}$

$\exists$ function $N: \mathbb{Z}\setminus\{0\} \longrightarrow \mathbb{N}$ such that
$\forall a, b \neq 0$ in $\mathbb{Z}$ $\exists$ $q, r \in \mathbb{Z}$,

① $a = qb + r$

② Either $r = 0$ OR $N(r) < N(b)$

Q: What is N ? ("norm function")

A: $N(a) = |a| = \begin{cases} a & \text{if } a > 0 \\ -a & \text{if } a < 0 \end{cases}$

Absolute Value

Theorem:

① Given $a \in \mathbb{Z}$ the set

$(a) := a\mathbb{Z} := \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$

is an ideal of $\mathbb{Z}$.

(the "principal ideal" generated by a)

② If $I \subseteq \mathbb{Z}$ is an ideal then

$I = (a)$ for some $a \in \mathbb{Z}$.

(every ideal of $\mathbb{Z}$ is principal).

Proof: (1) Exercise.

(2) Consider ideal $I \subseteq \mathbb{Z}$.
If $I = \{0\}$ then $I = (0)$, done ✓

So sp. $I \neq \{0\}$. Choose $a \in I$ with $N(a) = |a|$ minimal. Know $(a) \subseteq I$.

Claim: $I = (a)$.

Consider (any) other $d \in I$. Then $\exists$.

$$d = qa + r \quad \text{with} \quad 0 \leq r < |a|.$$

But $r = d - qa \in I \Rightarrow r = 0$
$\Rightarrow d = qa \in (a)$
Hence $I \subseteq (a)$. ∎

Remark: Every ideal of $\mathbb{Z}$ is principal. We say

$\mathbb{Z}$ is a PRINCIPAL IDEAL DOMAIN.

What did we use?
- Concept of "norm" - Euclid's Algorithm
- well-ordering

OK: HW 1 due Friday

OH: Mon 1:25 - 2:15

Wed 1:25 - 2:15

Thurs 2:30 - 3:20.

Recall

- Every ideal $I \subseteq \mathbb{Z}$ is principal.

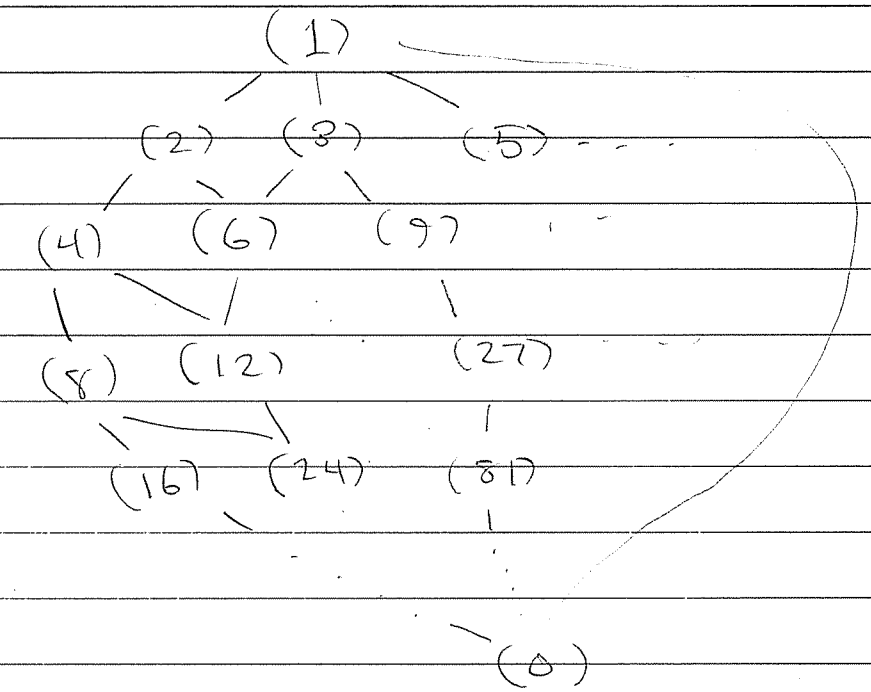
  I.e. $I = (a) = a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$

  for some $a \in \mathbb{Z}$.

Say $\mathbb{Z}$ is a PID ("Principal Ideal Domain")

- We have $(a) \subseteq (b) \iff b \mid a$.

$\Rightarrow$ lattice of ideals $\mathcal{L}(\mathbb{Z})$



$\cong$ $\mathbb{Z}$ ordered by divisibility

Given ideals $I, J \subseteq \mathbb{Z}$ with
$I = (a)$ & $J = (b)$, note

$$\left.\begin{aligned} I + J &= (d) \\ I \cap J &= (m) \end{aligned}\right\} \text{ for some } d, m \in \mathbb{Z}.$$

General: $I+J$ is smallest ideal with
$I+J \supseteq I$ & $I+J \supseteq J$.

Translation: d is largest integer with
$d \mid a$ & $d \mid b$
($d = \gcd(a,b)$ = greatest common divisor)

General: $I \cap J$ is biggest ideal with
$I \cap J \subseteq I$ & $I \cap J \subseteq J$.

Translation: m is smallest integer
with $a \mid m$ & $b \mid m$
($m = \operatorname{lcm}(a,b)$ = least common multiple).

Lattice Isomorphism Theorem for $\mathbb{Z}$.

Given ideal $(n) \subseteq \mathbb{Z}$ we get a familiar
quotient ring $\curvearrowright$

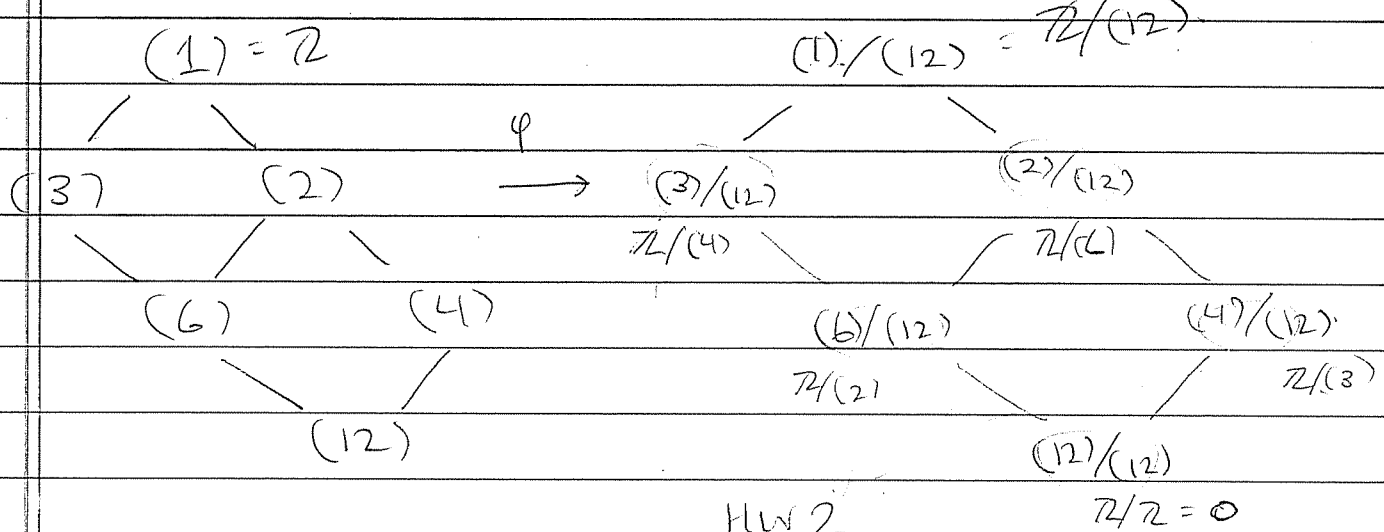
$$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z} = \{ a + n\mathbb{Z} : a \in \mathbb{Z} \}$$
$$= \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$$

where $\bar{a} = a + n\mathbb{Z} = \{ \ldots, a-n, a, a+n, a+2n, \ldots \}$

Canonical map $\varphi : \mathbb{Z} \to \mathbb{Z}/(n)$ $(\ker \varphi = (n))$
$a \longmapsto \bar{a}$

gives a <u>lattice isomorphism</u>.

Eg for $n = 12$



HW 2.

Corollary:

$\mathcal{L}(\mathbb{Z}/(n))$ = lattice of divisors of n.

Next Topic: Primality.

Q: What is the correct def. of "prime"?

TWO OPTIONS:

(1) Say p is "prime" if
$p|ab \Rightarrow a = \pm 1$ OR $b = \pm 1$.

(2) Say p is "prime" if
$p|ab \Rightarrow p|a$ OR $p|b$.

OOPS! In a general ring concepts (1) & (2) are distinct (neither implies the other).

DEF: Given $p \in R$,

(1) Say p is irreducible if
$p|ab \Rightarrow a$ OR b is a unit.
(unit = invertible).

(2) Say p is prime if
$p|ab \Rightarrow p|a$ OR $p|b$.

TRY to prove prime $\Rightarrow$ irreducible.

Proof: given $a \in R$ prime, suppose $a = bc$. Want to show b OR c is a unit.

since $a = 1bc \Rightarrow a \mid bc$
and a prime $\Rightarrow a \mid b$ OR $a \mid c$

WLOG say $a \mid b$. $\Rightarrow at = b$.

$\Rightarrow a = bc = atc$
$\Rightarrow a(1 - tc) = 0$

Now what?

We would like to say:
$a \neq 0$ hence $1 - tc = 0 \Rightarrow 1 = tc$
$\Rightarrow c$ is a unit.

$\Rightarrow a$ is irreducible ▨

Def: Say R is an integral domain if $ab = 0$
$\Rightarrow a = 0$ OR $b = 0$
(R has no "zero divisors").
and R is commutative with 1