Last updated: Dec 6, 2024

Abstract Algebra Notes Week 14 Wed, Dec 4 2024

MATH CLUB @ UML !

Math enthusiasts interested in becoming part of the leadership board should email:

@ Lee, Cori (Math office manager)

@ Frank, Emmett B. (Math major)

Today

Quiz

Lecture maximal ideal

Group quiz part I

Lecture prime ideal

Group quiz part II

Next week

Quiz

Brief lecture

Review

Recall

Lemma 6.3 (about cosets) (Written on the board during quiz)

$s+I = t+I$ iff $t \in s+I$ iff $t-s \in I$

Ideal test Recall

A subset I is an ideal of R if:

* I is an additive subgroup of R
* If $a \in I$ and $r \in R$ then both $\underbrace{ar \text{ and } ra \text{ are in } I}$.

"the absorbing property of I"

Ex 12 (Ch 14 Gallian) <u>Motivating Example</u>

Let $\mathbb{R}[x]$ denote the ring of polynomials w/ real coefficients.

Let $I = \langle x^2+1 \rangle$

$= \{ f(x)(x^2+1) : f(x) \in \mathbb{R}[x] \}$,

the principal ideal generated by x^2+1.

The quotient $\mathbb{R}[x]/I = \{ g(x) + I : g(x) \in \mathbb{R}[x] \}$ by def

<u>Note 1:</u>

If $g(x) \in \mathbb{R}[x]$, then we can write

$$g(x) = q(x)(x^2+1) + r(x)$$

where $r(x)$ is the remainder when dividing $g(x)$ by x^2+1.

So $r(x)=0$ or the degree of $r(x)$ is less than 2.

So $r(x) = ax+b$ for some $a, b \in \mathbb{R}$.

So we can write each coset $g(x) + I$ as

$$g(x) + \langle x^2+1 \rangle = \underbrace{q(x)(x^2+1) + r(x)} + \langle x^2+1 \rangle$$

$$= r(x) + \langle x^2+1 \rangle$$

the ideal $\langle x^2+1 \rangle$ absorbs the term $q(x)(x^2+1)$

So $\mathbb{R}[x]/I = \{ (ax+b) + I : a, b \in \mathbb{R} \}$

<u>Note 2:</u> $x^2 - (-1) = x^2+1 \in I$, so $x^2 + I = -1 + \langle x^2+1 \rangle$

Compare this with how $i^2 = -1$ in $\mathbb{C}$

Prop $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$, a field

Proof Consider the evaluation homomorphism

$\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}$ defined by

$\varphi(p(x)) = p(i)$

Then $x^2+1 \in \ker \varphi$ since $i^2+1=0$.

In fact, $\ker \varphi = \langle x^2+1 \rangle$.

The map φ is surjective since

for any $a+bi$ where $a, b \in \mathbb{R}$,

we have $\varphi(a+bx) = a+bi$.

By the 1st Isomorphism Thm,

$$\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}.$$

Recall from Sec 16.3

Fact: ("If an ideal contains unity, it is not proper")

Let R be a ring with unity 1.
If I is an ideal of R and $1 \in I$, then $I = R$.

$\boxed{\text{Lemma 1}}$ (to be used to prove Thm 16.35 and Prop 16.38)

Let R be a commutative ring with unity 1,

and I a proper ideal of R.

Then R/I is a commutative ring with unity $1+I$.

Sec 16.4

Part I: maximal ideals

We will characterize certain ideals and quotient rings of commutative rings

<u>Def</u> Let M be an ideal of a ring R. Then M is a <u>maximal ideal</u> of R if:

* M is a proper ideal (meaning $M \neq R$)
* For any ideal I of R containing M, either $I = M$ or $I = R$

(meaning, M is not a proper subset of any ideal of R except R itself)

<u>Thm</u> (Thm 16.35) Assume R is a commutative ring with unity. Let M be an ideal of R. Then M is a maximal ideal of R iff R/M is a field.

<u>Proof</u> (Proof of "$\Rightarrow$" forward direction) See book

(Proof of "$\Leftarrow$" backward direction) Suppose R/M is a field. So the zero element $0_R + M = M$ and the unity elt $1_R + M$ are two distinct elts. This means that $M \neq R$, so M is a proper subset of R.

Next, we show the maximal property of M:

Let I be an ideal of R containing M. If $I = M$, then we are done.

So suppose $M \subsetneq I$. (Note to self: Goal is to show $I = R$)

Since $M \subsetneq I$, there is an elt $a \in I$ but $a \notin M$.

So $a+M$ is a nonzero elt in R/M.

Since R/M is a field, there exists an elt $b+M$ in R/M

such that

$$(a+M)(b+M) = ab+M = 1+M.$$

So $1 \in ab+M$, that is, $1 = ab+m$ for some $m \in M$.

Since $a \in I$ and $b \in R$, $ab \in I$ (by "absorbing" property of ideals)

Since $m \in M \subset I$, $m \in I$

So $ab+m \in I$ (since an ideal is a subring and so is closed under addition).

Therefore $r1 = r \in I$ for all $r \in R$. Hence $I = R$ $\square$

Ex: If R is a field, then $R/\{0\}$ is a field,

so the zero ideal is a maximal ideal.

Recall Sec 16.2

Thm 16.16 Every finite integral domain is a field.

Example 16.17 For every prime p, $\mathbb{Z}_p$ is a field.

<u>Example</u> (Ex 16.36) If p is prime, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a fied, so $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Example: $2\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

<u>Example</u> If n is not prime, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is not a field (it's not an integral domain), so

$n\mathbb{Z}$ is not a maximal ideal

Example: $6\mathbb{Z} \subset 3\mathbb{Z}$

$\{\ldots,-6, 0, 6, 12, \ldots\}$ $\quad$ $\{\ldots,-6,-3,0,3,6,9,12,\ldots\}$

<u>Recall week 11 notes</u>

The set $J = \{ f(x) \in \mathbb{Z}[x] : f(0) \text{ is an even integer} \}$ is an ideal of $\mathbb{Z}[x]$. We see $\langle x \rangle \subsetneq J$ for example $x+2 \in J$ but not in $\langle x \rangle$.

So $\langle x \rangle$ is not a maximal ideal of $\mathbb{Z}[x]$.

—— end part I ——

Sec 16.4 | Part II: Prime ideals

Def Let R be a commutative ring, and let P be an ideal of R.

Then P is a <u>prime ideal</u> of R if:

* P is a proper ideal (meaning $P \neq R$)
* whenever $ab \in P$ (for $a, b \in R$), either $a \in P$ or $b \in P$

Example $P = \{0, 2, 4, 6, 8, 10\}$ is a prime ideal in $\mathbb{Z}_{12}$.

Pf Suppose $ab \in P$. Then ab is even.

Then either a is even or b is even.

Example $P = \langle x \rangle = \{ f(x)\, x : f(x) \in \mathbb{Z}[x] \}$

is a prime ideal in $\mathbb{Z}[x]$

(note: earlier we said $\langle x \rangle$ is not maximal in $\mathbb{Z}[x]$)

Pf Observe that $\langle x \rangle = \{ g(x) \in \mathbb{Z}[x] : \underbrace{g(0) = 0}_{\text{constant term of } g(x) \text{ is } 0} \}$.

Let $a(x), b(x) \in \mathbb{Z}[x]$.

Suppose $a(x) b(x) \in P$, then $a(0)\, b(0) = 0$.

Since $a(x), b(x) \in \mathbb{Z}[x]$, we know

the constant terms of $a(x)$ and $b(x)$,

$$a(0) \text{ and } b(0)$$

are integers.

Since $\mathbb{Z}$ is an integral domain,

$$\text{either } a(0) = 0 \text{ or } b(0) = 0.$$

So either $a(x) \in P$ or $b(x) \in P$. $\square$

Prop (Prop 16.38) Let R be a commutative ring with unity 1, and P an ideal of R.

Then P is a prime ideal iff R/P is an integral domain.

Proof (First, prove "$\Longrightarrow$" forward direction)

Suppose P is a prime ideal. Then P is proper.

So R/P is a commutative ring with unity $1+P$ by Lemma 1. So we only need to show R/P has no zero divisors.

Suppose

$$(a+P)(b+P) = ab+P = 0+P = P.$$

Then $ab \in P$. Since P is prime, either $a \in P$ or $b \in P$.

So either $a+P = 0+P$ or $b+P = 0+P$

(that is, either $a+P$ or $b+P$ is the zero elt in R/P)

So R/P has no zero divisors.

(Next, prove "$\Longleftarrow$" backward direction)

Assume R/P is an integral domain.

Suppose $a, b \in R$ and $ab \in P$.

Then

$$(a+P)(b+P) = ab+P = P,$$

the zero elt of R/P.

Since R/P is an integral domain, it has no zero divisor, so either $a+P = P$ or $b+P = P$, i.e. either $a \in P$ or $b \in P$.

So P is prime $\square$

Ex If R is an integral domain then $R/\{0\}$ is an integral domain.
So $\{0\}$ is a prime ideal of R.

Ex Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

The quotient ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ is an integral domain iff n is prime

(in fact, $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime).

So the prime ideals of $\mathbb{Z}$ are

$p\mathbb{Z}$ for p prime

and the zero ideal $\{0\}$.

Note: This justifies the use of the word "prime" in the def of prime ideals.

SFI: Student feedback on instruction

www.uml.edu/sfi (deadline: Dec 20)

(sfi documents will be available to instructors starting Dec 31)