Lecture 3

January 23, 2008
6:03 PM

$$\mathbb{R}[x]/\langle x^2+1\rangle \text{ "=" } \mathbb{C} = \left(\begin{matrix}\mathbb{R} \text{ "+" } i,\ i \text{ is a} \\ \text{root of } x^2+1=0\end{matrix}\right)$$

1. What does it mean?
2. Properties of ideals & quotients
3. The meaning of "="

<u>Reminder</u>: $A \subset R$ (R is a ring) is an "ideal" if

1. $A-A = \{x-y : x,y \in A\} \subset A$ } subgroup of $+$ } subring of R
2. $A \cdot A = \{x \cdot y : x,y \in A\} \subset A$
3. $R \cdot A = \{r \cdot x : x \in A, r \in R\} \subset A$ and $A \cdot R \subset A$

<u>Ex</u>: If $a \in R$ (R commutative)

$\langle a \rangle :=$ the smallest ideal in R containing a
$= \{ra : r \in R\} = R \cdot a$

$\langle a_1, \dots, a_n \rangle =$ smallest ideal containing $a_1, \dots, a_n$
$= \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r_1, \dots r_n \in R\}$
$= Ra_1 + \dots + Ra_n$

$r_1 \sim r_2 \bmod A$ if $r_1 - r_2 \in A$

$R/A = \{[r] : r \in R\}$

$[r]$: equiv. class of r

This is a ring.

$n\mathbb{Z} \subset \mathbb{Z}$, $n\mathbb{Z} = \langle n \rangle$ $\qquad \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle = \mathbb{Z}/n$

Today, R is always commutative.

<u>Def</u>: An ideal $A \subset R$ is "prime" if $\forall a,b \in R$, if $ab \in A$ means either $a \in A$ or $b \in A$.

<u>Ex</u>: $A = 104\mathbb{Z} \subset \mathbb{Z}$, not prime.

Ex: $A = 104\mathbb{Z} \subset \mathbb{Z}$, not prime.

$8 \notin A$, $13 \notin A$ $\quad 8 \cdot 13 \in A$

Ex2: $A = 8\mathbb{Z} \subset 2\mathbb{Z} = R$

$4 \notin A$, $4 \notin A$, $4 \cdot 4 = 16 \in A$

Claim: $n\mathbb{Z}$ is prime iff n is prime.

Proof: Assume $n = p$ is prime. $ab \in A$ iff $p | ab$
$\iff p | a$ or $p | b \iff a \in A$ or $b \in A$

Ex: Consider $A = \langle x \rangle \subset \mathbb{Z}[x]$

$\{$polynomials with constant term $= 0\}$ $= \{7x^2 - 3x + \underline{0}\}$

Claim: prime ideal

If $f \in \mathbb{Z}[x]$, $c(f) =$ "the constant term of f"

then $c(f \cdot g) = c(f) \cdot c(g)$

$(7x + \underline{8})(2x - \underline{9})$

So, if $c(f \cdot g) = 0 \Rightarrow c(f) = 0$ or $c(g) = 0$

So, if $f \cdot g \in A$, $\Rightarrow f \in A$ or $g \in A$.

Def: An ideal A which is an ideal in R is called a maximal ideal if:

1. $A \neq R$
2. If B is an ideal and $A \subset B \subset R$, then either $B = A$ or $B = R$

Claim: A is not maximal

$B = \langle x, 2 \rangle$
$= \{f : c(f) \in 2\mathbb{Z}\}$

$A \subsetneq B \subsetneq R$

Ex2: $\mathbb{R}[x]/\langle x^2+1\rangle$ "=" $\mathbb{C}$

Claim: $A=\langle x^2+1\rangle \subset \mathbb{R}[x]$ is maximal.

Proof: Assume $B \supsetneq A$ is an ideal.

Choose $f_1 \in B$ s.t. $f_1 \notin A$

$f_1 = 2x^8 - \pi x^7 + \dots$

$\sim ax+b \mod A$

$(ax+b) - f_1 \in A$ for some a & b

So $ax+b-f_1 = g$, $g \in A$

So $\underset{f_2}{\underset{\parallel}{ax+b}} = \underbrace{\underset{B}{\underset{\cap}{f_1}} + \underset{A \subset B}{\underset{\cap}{g}}}_{\in B}$ so $f_2 \neq 0$. (if $f_2=0$, $f_1 \in A$)

So $(ax-b)f_2 \in B$

$(ax-b)(ax+b) = a^2x^2 - b^2 \in B$

$a^2x^2 - b^2 - (a^2\underset{A\subset B}{\underset{\cap}{(x^2+1)}}) \in B$

$\cancel{a^2x^2} - b^2 - \cancel{a^2x^2} - a^2 = -b^2 - a^2 \in B$

$= -(a^2+b^2) \neq 0$

$\Rightarrow \frac{1}{-b^2-a^2} \cdot (-b^2-a^2) \in B$

$\Rightarrow 1 \in B \Rightarrow R \cdot 1 \subset B \Rightarrow R \subset B = R = B.$

Claim: prime $\not\Rightarrow$ maximal

$\langle x \rangle \subset \mathbb{Z}[x]$

maximal $\Rightarrow$ prime follows from Thm 1, 2 (in a ring with unity)

Thm 1: $A \subset R$ prime $\Leftrightarrow$ R/A is a domain

Thm 2: $A \subset R$ maximal $\Leftrightarrow$ R/A is a field. (in a ring with unity)

Ex for 1: $\langle x \rangle$ is prime in $\mathbb{Z}[x]$

$\mathbb{Z}[x]/\langle x \rangle = \mathbb{Z}$

Ex for 2: $\mathbb{R}[x]/\langle x^2+1\rangle$ "=" $\mathbb{C}$ is a field.

Proof of 1: ($\Rightarrow$) Assume A is prime, show R/A is a domain. Assume $[r_1][r_2]=[0]$.

$\Rightarrow [r_1 r_2]=[0]$

$\Rightarrow r_1 r_2 - 0 \in A$

$\xRightarrow{A \text{ is prime}} r_1 \in A$ or $r_2 \in A$ $\Rightarrow [r_1]=0$ or $[r_2]=0$

Hence R/A is a domain.

($\Leftarrow$)

Assume R/A is a domain and assume also $ab \in A$.

$\Rightarrow [ab]=0 \Rightarrow [a][b]=0$

$\xRightarrow[\text{domain}]{R/A \text{ is a}} [a]=0$ or $[b]=0$

$\Rightarrow a \in A$ or $b \in A$

Proof of 2.: Assume $A \subset R$ is maximal.

($\Rightarrow$)

We need to show that every $[b] \in R/A$ is invertible.

Since $[b] \neq 0$, $b \notin A$. Let $B = A + Rb$

Then $B \supset A$, yet $b \in B$ so $B \supsetneq A$.

So $B = R$, so $1 \in B$.

Thus for some $a \in A$ and $r \in R$, $1 = a + rb$

So in R/A, $[1] = [r \cdot b] = [r][b]$. So $[b]$ is invertible.

($\Leftarrow$)

Assume R/A is a field. Let B be an ideal st $B \supsetneq A$ so $\exists b$ s.t. $b \in B$, but $b \notin A \Rightarrow [b] \neq 0$

So $\exists r \in R$ s.t. $[r][b]=[1]$

So $rb - 1 = a$ for some $a \in A$.

$\Rightarrow 1 = rb - a \in RB - A \subset B - B \subset B \Rightarrow 1 \in B \Rightarrow B = R$

So A is maximal.

Isomorphism:

1 2 3 4 5 6 7 8 9

win: must have 3 cards out of X, $\Sigma = 15$

$\left.\begin{array}{l} A: 6, 7, 8, 9 \\ B: 5, 2, 1, \ldots \end{array}\right\}$ draw

Claim: This is Tic-Tac-Toe

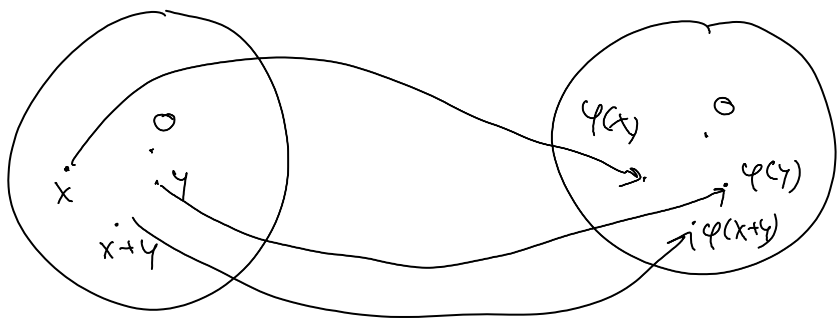
6	7	2
1	5	9
8	3	4

Σ — or | or / or \ = 15

$\cancel{6}$	$\cancel{7}$	2
1	5	$\cancel{9}$
$\cancel{8}$	3	4

Def: A function $\varphi: R \to S$ is called a homomorphism if:
1. $\varphi(0) = 0$
2. $\varphi(x+y) = \varphi(x) + \varphi(y)$
3. $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

Def: An isomorphism is a homomorphism that is 1-1 and onto (i.e. it is a bijection).



Ex: $\underbrace{\mathbb{R}[x]/\langle x^2+1\rangle}_{R"}$ is iso. to $\underbrace{\mathbb{C}}_{S"}$

Need to construct $\varphi: R \to S$

define $\varphi: R \to S$ by $\qquad R = \{[ax+b] : a, b \in \mathbb{R}\}$

$$\varphi([ax+b]) := ai + b$$

Clearly φ is 1-1 and onto.

Checked last time: 1. $\varphi(0) = \varphi([0]) = \varphi([0x+0]) = 0i+0 = 0$

3. $\varphi([ax+b][cx+d]) = \varphi([(ad+bc)x + (bd-ac)])$

$= (ad+bc)i + (bd-ac)$ $\quad =$

Yet $\varphi([ax+b]) \cdot \varphi([cx+d]) = (ai+b)(ci+d)$

$= (bd - ac) + (ad + bc)i$

<u>Ex2</u>: $R = \mathbb{C}$, $S = M_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a,b,c,d \in \mathbb{R} \right\}$

$\varphi(a+ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ 1-1, not onto

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ not in range ✓

Thus it is not an isomorphism.

1. $\varphi(0) = \varphi(0 + i0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ✓

2. Trivial ✓

3. $\varphi(a+ib)\varphi(c+id) = \varphi((a+ib)(c+id))$
$= \varphi(ac - bd + (ad+bc)i)$
$= \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix}$

$\varphi(a+ib)\varphi(c+id) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}$
$= \begin{pmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{pmatrix}$ = ✓

<u>Ex3</u>: $\varphi: \mathbb{Z} \to \mathbb{Z}/2$ $\{0,1\}$ Clearly not 1-1, onto ✓

$\varphi(n) = \text{parity of } n = n \bmod 2 = \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$

1. $\varphi(0) = 0$ ✓
2. $\varphi(n+m) = \varphi(n) + \varphi(m)$

parity of $n+m$ = parity of n + parity of m ✓

3. ✓

<u>Ex4</u>: $\mathbb{Z}/4 \xrightarrow{\cdot 5} \mathbb{Z}/10$ not onto, not 1-1

$0\ 1\ 2\ 3 \longrightarrow 0\ 5\ 0\ 5$

1. $\varphi(0) = 0$

2. $\varphi(x+y) = \varphi(x) + \varphi(y)$ | True because

$\underbrace{5(x+y)}_{+\bmod 4} = \underbrace{5x + 5y}_{+\bmod 10} \to$ not trivial | $10 \mid 5\cdot 4$

3. $\varphi(x\cdot y) \stackrel{?}{=} \varphi(x)\cdot\varphi(y)$

$5\cdot x\cdot 5\cdot y = 5\cdot xy$

$25xy = 5xy$ mod 10

$= 5xy = 5xy$ ✓

Ex 5: $\mathbb{Z}/4 \xrightarrow{\cdot 3} \mathbb{Z}/10$

$0\ 1\ 2\ 3 \longrightarrow 0\ 3\ 6\ 9$

$2+3=1 \longrightarrow \underbrace{6+9}_{=5} \neq 3$

Properties for $\varphi: R \to S$ (φ = homomorphism)

$\text{subring } A \subset R$, $\quad B \subset S$ ideal

$n \in \mathbb{Z}$

1. $\varphi(n\cdot r) = n\cdot\varphi(r)$

$\varphi(r^n) = \varphi(r)^n$

Proof of 1: induction ✓

2. $\varphi(A) = \{\varphi(a) : a \in A\}$ is a subring of S

Proof of 2: If $\varphi(a) \in \varphi(A)$

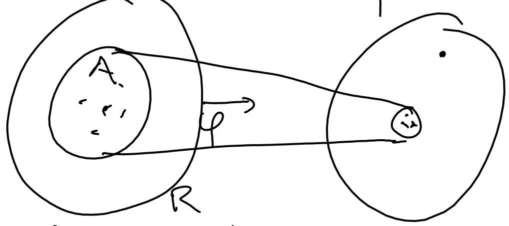
$\varphi(b) \in \varphi(A)$

Then $\varphi(a) + \varphi(b) = \varphi(a+b) \in \varphi(A)$

Same for multip.

$\varphi(R) = \operatorname{im}\varphi$ is a subring of S

3. Assume A is an ideal. is $\varphi(A)$ an ideal?



Not in general, yes if φ is onto

Proof of 3: Let $s \in S$. Let $\varphi(a) \in \varphi(A)$.

By onto-ness, $\exists\, r \in R$ s.t. $\varphi(r) = s$

By onto-ness, $\exists\, r \in R$ s.t. $\varphi(r) = s$

$$s \cdot \varphi(a) = \varphi(r)\,\varphi(a) = \varphi(\underbrace{r \cdot a}_{A}) \in \varphi(A)$$

$\boxtimes$

4. $\varphi^{-1}(B) := \{ r \in R : \varphi(r) \in B \}$ is always an ideal.