Algebra 27-03-201

Let R be a ring $A \subset R$
A is called an ideal if:
- A is group w.r.t. $+$
- $\forall a \in A, \forall r \in R: ra \in A$ $(rA \subset A)$

Example $R = \mathbb{Z}$ $A = \{6k \mid k \in \mathbb{Z}\}$.

A finite integral domain is a field

Example $\{a+bi \mid a, b \in \mathbb{Z}_3, i^2 = 2\}$

$0 = (a+bi)(c+di)$
$= (ac+2bd) + (ad+bc)i$
$\Rightarrow ac+2bd = 0$ and $ad+bc = 0$
$0 = (a+2bi)(a+bi)(c+di)(c+2di)$
$= (a^2+b^2)(c^2+d^2) \Rightarrow$
$a^2+b^2 = 0$ or $c^2+d^2 = 0$

always $a^2+b^2 \neq 0$
$\neq 0$ $\neq 0$
$\Downarrow$
$a = 0$ $b = 0$

a	b	a^2+b^2
0	0	0
1	0	1
1	1	2
2	0	1
2	1	2
2	2	2

R is an integral domain and therefore a field

Remark ideals are used in the construction of finite fields

Example $R = \mathbb{Z}[x] = \{a_0 + a_1 x + \dots + a_4 x^4 \mid a_i \in \mathbb{Z}\}$.

$A = \{a(x) \in \mathbb{Z}[x] \mid a_0 = 0\} = \langle x \rangle$
$= \{x \cdot r(x) \mid r(x) \in \mathbb{Z}[x]\}$.

A ideal in R

$x^2+y^2=z^2$
$3^2+4^2=5^2$
$x^3+y^3=z^3$
Fermat $x^n+y^n=z^n$

R/A factoring

$R/A = \{ r+A \mid r \in R \}$.

$r+A = \{ r+a \mid a \in A \}$.

Example $R=\mathbb{Z}$, $A=\langle 3 \rangle$

$\mathbb{Z}/\langle 3 \rangle = \{ k+\langle 3 \rangle \mid k \in \mathbb{Z} \}$.

$= \{ \langle 3 \rangle, 1+\langle 3 \rangle, 2+\langle 3 \rangle \}$

Addition on R/A: $(r+A)+(s+A)$
$=(r+s)+A$

$A+A$
$= \{ a_1+a_2 \mid a_1, a_2 \in A \}$
$= A$

$r+A = r'+A$
$s+A = s'+A$
$(r+A)+(s+A) = (r'+A)+(s'+A)$

$(r+s)+A$ $(r'+s')+A$

$(r+s)-(r'+s') = \underbrace{(r-r')}_{\in A} + \underbrace{(s-s')}_{\in A} \in A$

when $t+A = u+A$
$\Leftrightarrow (t-u) \in A$

$(r+A)(s+A) = rs+A$

R/A is a ring.

0 element: A $(r+A)+A = r+A$
1 element: $1+A$ $(1+A)(r+A) =$

(if $1 \in R$) $r + A$.

$\mathbb{Z}/\langle 3 \rangle = \{\langle 3\rangle, 1+\langle 3\rangle, 2+\langle 3\rangle\}$.

$= \mathbb{Z}_3$ with $+, \cdot$

Example $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$. $i^2 = -1$

$A = \langle 2-i\rangle = \{(a+bi)(2-i) \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]/\langle 2-i\rangle \cong \mathbb{Z}_5$ (check example in the book)

Theorem Let R be a ring with $1 \in R$, A ideal in R

(i) R/A is a field $\Leftrightarrow$ A is maximal ideal

(ii) R/A is int. dom. $\Leftrightarrow$ A is prime ideal

Def. A is called prime ideal if $a, b \in R$ and $a \cdot b \in A \Rightarrow$ $a \in A$ or $b \in A$

Example $R = \mathbb{Z}$ $A = \langle 5\rangle$

$a, b \in \mathbb{Z}$, $a \cdot b \in \langle 5\rangle \Rightarrow 5 \mid a \cdot b$

$\Rightarrow 5 \mid a$ or $5 \mid b$

Def. $A \subset R$ ideal is called maximal if $A \subseteq B \subseteq R$ (B ideal)

then $A = B$ or $B = R$

Example $\langle 7\rangle$ in $\mathbb{Z}$ is maximal

$\langle 7\rangle \subsetneq B \subseteq \mathbb{Z}$

$b \in B$, $b \notin \langle 7\rangle$ $\gcd(b, 7) = 1$

$\Rightarrow x, y \in \mathbb{Z}$ s.t. $\underbrace{bx}_{\in B} + \underbrace{7y}_{\in \langle 7\rangle \subset B} = 1$

$\in B$

$1 \in B \Rightarrow B = R$

Conjecture: maximal = prime

However: $\langle x \rangle$ in $\mathbb{Z}[x]$ is prime

but $\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}$

$\Rightarrow \langle x \rangle$ is not maximal

maximal $\Rightarrow$ prime

Example $\mathbb{R}[x]/_{(x^2+1)} \approx \mathbb{C}$

($\langle x^2+1 \rangle$ ↑ max ideal)

$f(x), g(x) \in \mathbb{F}[x]$ $\mathbb{F}$ any field

$g(x) \neq 0$ zero polynomial

$\Rightarrow f(x) = q(x) \cdot g(x) + r(x)$ $\deg r(x) < \deg g(x)$

$(17 = 3 \cdot 5 + 2)$

$f(x) = 3x^4 + x^3 + 2x^2 + 1$ $g(x) = x^2 + 4x + 2$

divide $f(x)$ by $g(x)$.

$$x^2+4x+2 \,/\, 3x^4 + x^3 + 2x^2 + 1 \,\backslash\, 3x^2 - 11x$$
$$3x^4 + 12x^3 + 6x^2$$
$$-11x^3 - 4x^2 + 1$$

Remark: $q(x), r(x)$ are unique

Property If $f(a) = 0$ $a \in \mathbb{F}$

then $f(x) = (x-a) q(x)$

proof $f(x) = (x-a) \cdot q(x) + r(x)$

$\deg r(x) < 1$