Abstract Algebra

Module 4

Section 27 : Prime and Maximal Ideals

June 14, 2021

Ring vs Factor Ring

- Ring may have **stronger** as well as **weaker** algebraic structure compared to its Factor Ring.
  - $\mathbb{Z}/p\mathbb{Z}$ is a Field. But, $\mathbb{Z}$ is not a Field.
  - $\mathbb{Z}/6\mathbb{Z}$ is not an Integral Domain. But, $\mathbb{Z}$ is an Integral Domain.
- Every ring R has two ideals,
  - Improper Ideal R
  - Trivial Ideal $\{0\}$

Definition (Ideal)

A subgroup of a ring R is an ideal if $rN \subset N$ & $Nr \subset N$, $\forall r \in R$.

Definition (Unit)

Unit is an element which has multiplicative inverse.

Ideal with Unit

Theorem (Ideal with Unit)

Let N be an ideal of ring R. Let u be a unit in N. Then $N = R$.

Proof.

$$N \underset{ideal}{\leq} R \implies \forall r \in R,\ rN \subset N$$

$$\text{Unit, } u \in N \implies \exists u^{-1} \in R,\ u^{-1}u = 1 \in N$$

$$r \in R,\ 1 \in N \implies r1 = r \in N$$

□

Corollary

A field contains no proper, nontrivial ideals.

Maximal Ideal, Prime Ideal

Definition (Maximal Ideal)

A proper ideal which is not contained in any other proper ideal.

$p\mathbb{Z} \subset \mathbb{Z}$

Let p be a prime. Then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ (Why ?)

Definition (Prime Ideal)

A proper ideal N is prime ideal if $ab \in N \implies a \in N$ or $b \in N$.

$\{0, 2\} \subset \mathbb{Z}_4$

$\{0, 2\}$ is a prime ideal of $\mathbb{Z}_4$
$0 = 0 \cdot x = x \cdot 0 = 2 \cdot 2$
$2 = 1 \cdot 2 = 2 \cdot 1$
Remember that $1 = 1 \cdot 1 = 3 \cdot 3$
Thus, prime ideal of $\mathbb{Z}_4$ containing 1 should also contain 3.

Maximal Ideal characterisation of Field

Theorem

Let R be a commutative Ring with unity.
M is a maximal ideal of R $\iff$ factor ring R/M is a field

Sufficient Part : Context

- Commutative Ring with unity R
- Maximal ideal M
  - Ideal $\implies \forall r \in R, rM \subset M, \ Mr \subset M$
  - Maximal $\implies M \subsetneq R$
- M is an ideal of $R \implies R/M$ is commutative ring with unity.
- M is maximal $\implies R/M$ is non-zero ie, $R/M \neq \{0 + M\}$
- $R/M \neq \{0+M\} \implies \exists(a+M) \in R/M, \ (a+M) \neq (0+M)$
  That is, $a \notin M$ and $a + M$ is not the additive identity of R/M
- $(a+M) \in R/M$ has multiplicative inverse $\implies R/M$ is a field

Proof : Characterisation of Field

Sufficient Part

- Suppose $a + M$ doesn't have multiplicative inverse in R/M
- $(R/M)(a + M) = \{(r + M)(a + M) : (r + M) \in R/M\}$
  - $x \in (R/M)(a + M) \implies x = (r + M)(a + M), \; r + M \in R/M$
- Claim : $(1 + M) \notin (R/M)(a + M)$
  - Suppose $(1 + M) \in (R/M)(a + M)$
  - $\exists (b + M) \in R/M$ such that $(b + M)(a + M) = (1 + M)$
  - $ba = ab = 1$ is a contradiction.
- $(R/M)(a + M)$ is non-trivial, proper ideal of R/M
  - $(a + M) = (1 + M)(a + M) \in (R/M)(a + M) \implies$ non-trivial
  - $(1 + M) \notin (R/M)(a + M) \implies$ proper
- Canonical Homomorphism, $\gamma : R \to R/M, \; \gamma(a) = a + M$
  - $\ker(\gamma) = M \implies M \subset \gamma^{-1}[(R/M)(a + M)]$
  - $\gamma^{-1}[(R/M)(a + M)]$ is a proper, ideal of R containing M

contradicts M is maximal ideal in R

Proof : Characterisation of Field

Necessary Part

- M is ideal of R
- Suppose R/M is a field.
- Suppose M is not Maximal ideal of R
  $\exists$ proper, ideal N containing M, ie, $N \subset M \subset R$
- Canonical Homomorphism, $\gamma : R \to R/M, \ \gamma(a) = a + M$
- $\gamma[N]$ is a proper, non-trivial ideal of R/M
  - $\gamma[M] = \{0 + M\} \subset \gamma[N] \implies$ non-trivial
  - $N \neq R \implies \exists b \in R$ such that
    $b \notin N, \ \gamma(b) = (b + M) \notin \gamma[N] \implies$ proper

  is a contradiction since R/M is a field.
  A field contains no proper, non-trivial ideal.

Ideal characterisation of Field

Corollary

A commutative ring with unity is a field if and only if it has no proper, non-trivial ideals.

Sufficient Part

- Commutative ring unit unity, R
- Suppose R is a field.
- R has no proper, non-trivial ideal.

Necessary Part

- Commutative ring unit unity, R
- Suppose R has no proper, non-trivial ideal.
- Maximal ideal $\{0\}$
- $R/\{0\} \simeq R$ is a field

Prime Ideal characterisation of Integral Domain

Theorem

- *Commutative Ring R with unity*
- *Proper ideal of R, $N \neq R$*
- *N is prime ideal $\iff$ factor ring R/N is integral domain*

Proof.

$$(a+N)(b+N) = ab + N = 0 + N \iff ab \in N$$

- R/N Prime Ideal, $ab \in N \implies a \in N$ OR $b \in N$

$$a \in N \text{ OR } b \in N \iff a + N = N \text{ OR } b + N = N$$

- Integral Domain (No zero Divisors),
  $(a+N)(b+N) = 0 + N \implies (a+N) = N$ OR $(b+N) = N$

Corollary

Corollary

Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof.

Suppose M is an ideal of a commutative ring R with unity

- M is maximal ideal of R
- $\implies R/M$ is a field
- $\implies R/M$ is an integral domain
- $\implies M$ is a prime ideal

□

Prime Field

Results

1. For ring R with unity 1, the function $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$ is a ring homomorphism.
2. For ring R with characteristic $n > 1$, R contains a subring isomorphic to $\mathbb{Z}_n$
3. For ring R with characteristic 0, R contains a subring isomorphic to $\mathbb{Z}$
4. For field F with prime characteristic p, F contains a subfield isomorphic to $\mathbb{Z}_p$
5. For field F with characteristic 0, F contains a subfield isomorphic to $\mathbb{Q}$

Definition (Prime Field)

The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are prime fields. (Why ? Semester 2)

Proof : Ring Homomorphism given by $\phi : \mathbb{Z} \to R$

Proof.

Let 1 be the unity of the Ring R with Unity

$$
\begin{aligned}
\phi(n+m) &= (n+m)\cdot 1 = \underbrace{(1+1+\cdots+1)}_{n+m \text{ summands}} \\
&= \underbrace{(1+1+\cdots+1)}_{n \text{ summands}} + \underbrace{(1+1+\cdots+1)}_{m \text{ summands}} \\
&= (n\cdot 1) + (m\cdot 1) = \phi(n) + \phi(m)
\end{aligned}
$$

$$
\begin{aligned}
\phi(n)\phi(m) &= (n\cdot 1)(m\cdot 1) \\
&= \underbrace{(1+1+\cdots+1)}_{n \text{ summands}} \underbrace{(1+1+\cdots+1)}_{m \text{ summands}} \\
&= \underbrace{(1+1+\cdots+1)}_{nm \text{ summands}} \\
&= (nm)\cdot 1 = \phi(nm)
\end{aligned}
$$

Proof: $\mathbb{Z}_n$ subring of Ring of Characteristic $n > 1$

- Suppose R is
  - a commutative ring with unity 1 and
  - characteristic n, $(n > 1)$
- $\phi : \mathbb{Z} \to R,\ \phi(m) = m \cdot 1$ is a (ring) Homomorphism
  - $\phi(1) = 1.1 = (1)$
  - $\phi(2) = 2 \cdot 1 = (1 + 1)$

    $\vdots$
  - $\phi(n-1) = (n-1) \cdot 1 = \underbrace{(1 + 1 + \cdots + 1)}_{n-1 \text{ summands}}$
  - $\phi(n) = n \cdot 1 = \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ summands}} = 0 = \phi(0)$
- Kernel $\ker(\phi) = \{\cdots, -2n, -n, 0, n, 2n, \cdots\} = n\mathbb{Z}$
- For any $n > 1$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
  - $\phi : R' \to R$ is ring homomorphism $\iff$ $\ker(\phi)$ is an ideal of R
- $\mathbb{Z}_n \underset{\text{congruence}}{\simeq} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(\phi) \underset{\text{canonical}}{\simeq} \phi[\mathbb{Z}] \leq R$

Proof: $\mathbb{Z}$ subring of Ring of Characteristic 0

- R is a commutative ring with unity 1 and characteristic 0
- $\phi : \mathbb{Z} \to R,\ \phi(n) = n \cdot 1$ is a ring homomorphism
- Claim : $\ker(\phi) = \{0\}$
  Suppose kernel is nontrivial, there exists $m \in \ker(\phi),\ m \neq 0$
  Then $m \in \ker(\phi) \implies \phi(m) = 0 \implies$ characteristic $\neq 0$
- $\mathbb{Z} \underset{\text{trivial}}{\simeq} \mathbb{Z}/\{0\} = \mathbb{Z}/\ker(\phi) \underset{\text{canonical}}{\simeq} \phi[\mathbb{Z}] \leq R$

Proof: $\mathbb{Z}_p$ subfield of Field of Prime Characteristic p

- Field F with characteristic n, $(n > 1)$
- $\phi : \mathbb{Z} \to F$ is a homomorphism.
- $\mathbb{Z}_n$ is a subring of F, $\mathbb{Z}_n \underset{\text{ring}}{\leq} F$
- Claim : n is a prime.
  - If n is not a prime, then $n = ab, a > 1, b > 1$
  - $\implies \mathbb{Z}_n$ has zero divisors a, b
  - $\implies F$ has zero divisors $\phi(a), \phi(b)$
- $\langle \mathbb{Z}_p, +_p, \times_p \rangle$ is a field
- $\mathbb{Z}_p$ is a subfield of F, $\mathbb{Z}_p \underset{\text{field}}{\leq} F$

Proof: $\mathbb{Q}$ subfield of Field of Characteristic 0

- Field F with characteristic 0
- $\mathbb{Z} \underset{\text{ring}}{\leq} F$
- $\mathbb{Z}$ is an integral domain
- $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$ (refer : Fraleigh §21)
  The smallest field containing the integral domain
- $\mathbb{Q} \underset{\text{field}}{\leq} F$

Field of characteristic 1 ?

Field of characteristics 1 does not exists.
Characterstic 1 $\implies$ $1 = 0$ is contradictory as $F = \{0\}$
Thus smallest/trivial field is $Z_2 = \{0, 1\}$

Principal ideal

Definition (ideal generated by an element)

Let R be a commutative ring with unity and $a \in R$. The ideal generated by a is the set of all elements of the form ra where $r \in R$.

$$\langle a \rangle = \{ra : r \in R\}$$

It is the smallest ideal containing a.

Definition (Principal ideal)

An ideal with a generator

Ideals of $\mathbb{Z}$

Every ideal of $\mathbb{Z}$ is a principal ideal.
An ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} = \langle n \rangle$

Ideal $\langle x \rangle$ of $F[x]$

$\langle x \rangle$ in $F[x]$ is the set of all polynomials with zero constant term.

Polynomials over field F, $F[x]$

Theorem

Every ideal in $F[x]$ is a principal ideal.

Proof.

- N be an ideal of $F[x]$, $N = \{0\} \implies N = \langle 0 \rangle$
- Suppose $N \neq \{0\}$. There exists a polynomial of minimum degree $g(x) \in N$, $g(x) \neq 0$
- Case 1 : degree of $g(x) = 0$
  - $g(x)$ is a constant. $g(x) \in F$. And has multiplicative inverse.
  - ideal N contains unit $g(x) \implies N = F[x] = \langle 1 \rangle$
- Case 2 : degree of $g(x) \geq 1$
  - $f(x) \in N \implies f(x) = q(x)g(x) + r(x)$ where degree of $r(x)$ is strictly less than the degree of $g(x)$
  - $r(x) \neq 0$ is a contradiction since degree of $g(x)$ is not minimum in $F[x]$ as $r(x) = f(x) - q(x)g(x) \in F[x]$
  - $f(x) \in N \implies f(x) = q(x)g(x) \implies F[x] = \langle g(x) \rangle$

Ideal generated by Irreducible Polynomials

$$\langle p(x) \rangle = \{0\} \iff p(x) = 0 \in F[x]$$

Theorem

Non-trivial ideal $\langle p(x) \rangle$ *is maximal* $\iff$ $p(x)$ *is irreducible over* F

Proof : Sufficient Part

- Suppose $\langle p(x) \rangle$ is maximal ideal in $F[x]$
- Claim : $p(x) \notin F$
  - $p(x) \in F \implies p(x)$ is a unit $\implies \langle p(x) \rangle = F[x]$
    $\implies p(x)$ is not a proper ideal
    $\implies \langle p(x) \rangle$ is not a maximal ideal
- Suppose $p(x)$ is reducible, $p(x) = f(x)g(x)$
  - Every maximal ideal is also prime ideal
    $f(x)g(x) \in \langle p(x) \rangle \implies f(x) \in \langle p(x) \rangle$ OR $g(x) \in \langle p(x) \rangle$
  - $\mathit{degree}(f(x)) < \mathit{degree}(p(x)) \implies f(x) \notin \langle p(x) \rangle$
- By contradiction, $p(x)$ is irreducible.

ideal generated by irreducible polynomial

Proof : Necessary Part

- Suppose $p(x)$ is irreducible over F
- Suppose $\langle p(x) \rangle$ is not maximal
  - There exists proper ideal N properly containing $\langle p(x) \rangle$
    That is, $\exists$ ideal N such that $\langle p(x) \rangle \subsetneq N \subsetneq F[x]$
- Every ideal in $F[x]$ is principal
  - $N = \langle g(x) \rangle$ for some $g(x) \in F[x]$
  - $p(x) \in N \implies p(x) = q(x)g(x)$
  - $p(x)$ irreducible $\implies q(x)$ is of degree 0 $\implies N = \langle p(x) \rangle$
    since $degree(g(x)) = 0 \implies g(x)$ is unit $\implies \langle g(x) \rangle = F[x]$
- By contradiction, there is no proper ideal N containing $\langle p(x) \rangle$
  - $p(x)$ is irreducible $\implies degree(p(x)) \geq 1$
    $\implies \langle p(x) \rangle \neq \langle 1 \rangle = F[x]$ That is, $\langle p(x) \rangle$ is a proper ideal
    $\implies \langle p(x) \rangle$ is a maximal ideal

Unique Factorisation in $F[x]$

Theorem

- *$p(x)$ an irreducible polynomial in $F[x]$.*
- $p(x)|r(x)s(x),\ \ r(x), s(x) \in F[x] \implies p(x)|r(x)$ *OR* $p(x)|s(x)$

Proof.

- $p(x)|r(x)s(x) \implies r(x)s(x) \in \langle p(x) \rangle$
- $\langle p(x) \rangle$ is a prime field
- $r(x) \in \langle p(x) \rangle$ OR $s(x) \in \langle p(x) \rangle$
- WLOG $r(x) \in \langle p(x) \implies p(x)|r(x)$

$\square$

Theorem (Unique Factorisation)

Every polynomial $p(x) \in F[x]$ has unique factorisation except for order and unit.

Thank You