Contents

LN 19

Prime Ideal

- Definition: Prime Ideal An ideal $I \subseteq R$, R is a ring is called prime if whenever $a, b \in I$ then $a \in I$ or $b \in I \, \forall a, b \in R$.

- Proposition For a commutative ring R, $I \subseteq R$ is a prime ideal iff $\dfrac{R}{I}$ is an integral domain (no-zero divisors)

  - Proof

    - $\Rightarrow$

    Suppose that $(a+I)(b+I) = 0$ ie $ab \in I$ but I is prime So $a \in I$ or $b \in I$ which means $a + I = 0$ or $b + I = 0$.

    - $\Leftarrow$ if $ab \in I$ then $(a+I)(b+I) = 0$ in $\dfrac{R}{I}$

    TODO_{sc1}

- Example $\mathbb{Z}$ as a ring - it has ideals $n\mathbb{Z}$ for $n \in \mathbb{Z}$ which ones are prime?

  $p\mathbb{Z}$ for p a prime are the prime ideals.

  What is $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$? By the "Proposition", this is an integral domain. This is a field!

- Fact Any finite itegral domain is a field.

  - Proof (By "Pigeon Hole Principle") Suppose that R is a finite integral domain and $a \in R, a \neq 0$. We need to find b such that $ab = 1$.

    - Define: $F : R \to R, r \mapsto ar$.

- Claim: F is a $1-1$.
  Suppose $ar = as$ for some $r, s \in R$ then $a(r-s) = 0$
  But R is an integral domain. So either $a = 0$ or \$r - s = \$.
  But $a \neq 0$ so $r = s$
  R is finite so F is onto!

So for some $B \in R, ab = 1$.

So R is a field!

Maximal Ideal

- Definition: Maximal ideal We call an ideal $I \subseteq R$ maximal if $I \neq R$ but if $I \subseteq J \subseteq R$, J is an ideal, then $I = J$ or $J = R$

- Proposition: For a commutative ring with 1, I is maximal iff $\frac{R}{I}$ is a field.

  - Proof

    - $\Leftarrow$ The only ideals in a field F are F and $\{0\}$. Because non-zero elements have multi-inverse TODO If a TODO
    - $\Rightarrow$ Suppose that $a + I \neq 0$ ie $a \notin I$ (I is maximal). Genereate the smallest ideal containing a and I.
      $\langle a, I \rangle = \{ra + rb : r \in R, b \in I\} \subset I$.
      So $R = \langle a, I \rangle$ so $1 = ra + rb$ for some $r \in R, b \in I$
      This means $(r + I)(a + I) = 1 + I$ in $\frac{R}{I}$
      Si $a + I$ has multiplicative inverse and $\frac{R}{I}$ is a field.

- Carollary: If R is a commutative ring with 1 then any maximal ideal is prime

  - Proof If I is maximal then $\frac{R}{I}$ is a field hense an integral domain So I is prime.

- Example $\frac{\mathbb{Z}}{p\mathbb{Z}}$ is both a field and an integral domain for p a prime so $p\mathbb{Z}$ is both prime and maximal in $\mathbb{Z}$.

PID: principlae ideal domain

Notice in $\mathbb{Z}$, every idael is 1-generated - of the form $\langle n \rangle$ where $n \in \mathbb{Z}$. $n =$ the smallest ideal TODO n, ie $n\mathbb{Z}$.

- Definition: PID

A integral domain M where all dieals are 1-generated is called a principle ideal domain. (PID).

TODO

- Example TODO
- Division algorithm If $f, g \in F[x]$ then there are unique $q, r \in F[x]$ such that $g = fq + r$ with $degree(r) < degree(f)$.
  - Long division algorithm $f = a_n x^n + ... + a_0$ $b = b_n x^m + ... + b_0$ TODO_{sc3}
  - Ideals in $F[x]$ Suppose $I \subseteq F[x], I \neq \{0\}$
    What does I look like?
    $I = \langle f \rangle$ the ideal generated by f.
    where f has the least degree among elements of I.
    * Why? Suppose $g \in I$. Use the division algorithm to divide g by f, ie $g = fq + r$ with $degree(r) < degree(f)$
      But notice $g \in I, fq \in I$ so r must be in I. So $r = 0$
      Which means, $g = fq$. So $g \in \langle f \rangle$