21-237: Math Studies Algebra I November 4, 2022

Lecture 25 : Maximal ideals and principal ideal domains

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Proper ideals are contained in maximal ideals

An ideal I in R is **proper** $\iff I \neq R \iff 1 \notin I$.

Theorem: If I is proper, there is $J \supseteq I$ such that J is maximal.

Proof: Consider the poset $\mathbb{P} = \{I : I \text{ proper ideal of R}\}$ ordered by inclusion.

J is a maximal ideal of $R \iff J$ is a maximal element of $\mathbb{P}$.

We wish to apply Zorn's Lemma, but must first verify that its hypothesis holds for $\mathbb{P}$, namely that every chain of $\mathbb{P}$ has an upper bound. Note $I \in \mathbb{P}$, so $\mathbb{P} \neq \emptyset$.

Let $C \subseteq P$ be a chain. C is a set of proper ideals linearly ordered by inclusion, i.e. for $I_0, I_1 \in C$, either $I_0 \subseteq I_1$ or $I_1 \subseteq I_0$.

If $C = \emptyset$, C is bounded by I. Otherwise, let $K = \bigcup C = \{r \in R : \exists J \in C, r \in J\}$. For all $J \in C$, $J \subseteq K$. Observe C contains a non-empty set, so $K \neq \emptyset$.

Claim 1: K is an ideal. *Proof*: $0 \in K$. If $a, b \in K$, choose $J, J' \in C$ such that $a \in J$, $b \in J'$. WLOG, suppose $J \subseteq J'$. Then, $a, b \in J'$, so $a + b \in J' \subseteq K$. For $r \in R$, $ra \in J' \subseteq K$. □

Claim 2: K is proper. *Proof*: $1 \notin J$ for all $J \in C$, so $1 \notin K$, so $K \neq R$. □

By Zorn's Lemma, there is $J \supseteq I$ such that J is maximal. □

2 Closure

For rings R, S, $R \times S$ is the obvious construction (coordinate-wise operations on the cartesian product). Note: $(1, 0) \times (0, 1) = (0, 0)$ so $R \times S$ is not typically ID.

On the other hand, if R is an ID, then $R[x]$ is an ID.

3 More definitions

An ideal I is **principal** if $I = (a) = R_a$ for some $a \in R$.

An R-module M is **cyclic** if $M = R_m$ for some $m \in M$.

Note: If $(G, +)$ is any abelian group, we can define ng for $n \in \mathbb{Z}$, $g \in G$ in the natural way (g^n under multiplicative notation).

(1) This makes G into a $\mathbb{Z}$-module

(2) This is the only scalar multiplication defined on $\mathbb{Z} \times G$ that makes G a $\mathbb{Z}$-module.

(3) Every $\mathbb{Z}$-module arises in this way from some abelian group.

A **principal ideal domain** (PID) is a ring R such that

(1) R is an ID.

(2) All ideals are principal.

Examples: $\mathbb{Z}$ is a PID. For any field K, $K[x]$ is a PID.

Let R be a ring. Let I, J be ideals.

Let $I + J = \{a + b : a \in I, b \in J\}$. $I + j$ is an ideal. In fact, $I + J$ is the least ideal containing $I \cup J$.

$I \cap J$ is also an ideal. In fact, $I \cap J$ is the largest ideal contained in I, J.

Let $IJ = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{N}, a_i \in I, b_i \in J\}$. IJ is an ideal. In fact, it is the least ideal containing $\{ab : a \in I, b \in J\}$.

Note that $IJ \subseteq I \cap J$ since I and J are ideals.

Examples: For $I = 4\mathbb{Z}$, $J = 6\mathbb{Z}$, $I \cap J = 12\mathbb{Z}$, $I + J = 2\mathbb{Z}$ and $IJ = 24\mathbb{Z}$.

Let $a_1, \ldots, a_k \in R$. Define $(a_1, \ldots, a_k)$ to be the least ideal containing $a_1, \ldots, a_k$. It is given by $\{\sum_{i=1}^{k} r_i a_i : r_i \in R\}$.

Example: $\mathbb{Z}[x]$ is an ID, not PID. To see this, consider $(2, x) = \{p \in \mathbb{Z} : \text{constant term of } p \text{ is even}\}$. It cannot be generated by any single element.