MTH302: INTEGERS, POLYNOMIALS AND MATRICES
LECTURE 5, September 1, 2020

VARADHARAJ R. SRINIVASAN

*K*eywords: Prime Ideals.

1. Prime Ideals

Prime Ideals: Let R be a commutative ring. An ideal I of R is called a *prime* ideal if the following conditions hold:

Pr-1. $I \neq R$.
Pr-2. If for $x, y \in R$, $xy \in I$ then $x \in I$ or $y \in I$.

Remark 1.1. Let R be a commutative ring. Then R is an integral domain if and only if (0) is a prime ideal.

Examples.

- Let F be a field. Then (0) is the only prime as well as the maximal ideal of F.
- The ideals of $\mathbb{Z}$ of the form $p\mathbb{Z}$, where p is a prime number, are prime as well as the maximal ideals of $\mathbb{Z}$. The ideal (0) is a prime ideal but not a maximal ideal.

Let R be a ring,

$$N := \{a \in R \mid a^n = 0 \text{ for some positive integer } n\} \text{ and } \qquad N' := \bigcap_{P,\ P \text{ is a prime ideal}} P.$$

If $a \in N$ and P is any prime ideal of R then since $a^n = 0$ for some positive integer n, we have $a^n = 0 \in P$. It follows that $a \in P$ and thus $N \subseteq N'$.

Theorem 1.2. *If R is a commutative ring with 1 then $N = N'$.*

Proof. We only need to show $N' \subseteq N$. Suppose on the contrary that there is an element $a \in N'$ such that $a \notin N$. Let $S = \{1, a, a^2, \cdots\}$ and observe that $0 \notin S$. Consider

$$\mathscr{C} = \{I \mid I \text{ is an ideal of } R \text{ and } I \cap S = \emptyset\}$$

Since $(0) \cap S = \emptyset$, we see that $\mathscr{C} \neq \emptyset$. Clearly, $\mathscr{C}$ is a poset with the partial order $\subseteq$. Let Y be chain and $B = \cup_{I \in Y} I$. Then as done in the last lecture, it can be show that B is an ideal of R. If $S \cap B \neq \emptyset$ then $S \cap I \neq \emptyset$ for some $I \in Y$, which is absurd. So $S \cap B = \emptyset$ and thus $B \in \mathscr{C}$. It is obvious that B is an upper bound for Y. Therefore, by Zorn's Lemma, $\mathscr{C}$ has a maximal element, which we denote it by P.

We claim that P is a prime ideal. Let $x \notin P$ and $y \notin P$. Then it is easy to see that $J_1 := P + Rx = \{k + r \cdot x \mid k \in P \text{ and } r \in R\}$ and $J_2 = P + Ry = \{l + r \cdot y \mid l \in P \text{ and } r \in R\}$ are ideals of R such that $P \subsetneq J_i$ for $i = 1, 2$. Then $J_i \cap S \neq \emptyset$ (why?). Let $a^n \in J_1$ and $a^m \in J_2$ for nonnegative integers n, m. Then $a^n = k + r \cdot x$ and $a^m = l + s \cdot y$ for $k, l \in P$ and $r, s \in R$. Now

$$a^{n+m} = a^n \cdot a^m = k \cdot l + k \cdot s \cdot y + r \cdot x \cdot l + r \cdot s \cdot x \cdot y.$$

Since $k, l \in P$, if $x \cdot y \in P$ then $a^{n+m} \in P$, which contradicts the fact that $S \cap P = \emptyset$. Thus $x \cdot y \notin P$ and this proves our claim.

Now, we have obtained that a prime ideal P such that $S \cap P = \emptyset$. In particular, $a \notin P$. This contradicts the fact that $a \in N'$. Thus we have proved that $a \in N$. □

2. Generators of subrings and ideals

Let X be a subset of a ring R.

Subring generated by X. The subring generated by X is the smallest subring of R containing X. Equivalently, it is the intersection of all subrings of R that contains X. Elements of the subring generated by X are of the form

$$x_{11} \cdot x_{12} \cdots x_{1n_1} + x_{21} \cdot x_{22} \cdots x_{2n_2} + \cdots + x_{l1} \cdot x_{l2} \cdots x_{ln_l},$$

where $x_{ij} \in X$ and x_{ij} <u>need not</u> be distinct.

Left ideal generated by X. The left ideal generated by X is the smallest left ideal of R containing X. Equivalently, it is the intersection of all left ideals of R that contains X. Elements of the left ideal generated by X are of the form

$$\sum_{\substack{i=1 \\ x_i \in X}}^{l} n_i x_i \ + \sum_{\substack{j=1 \\ r_j \in R,\ y_j \in X}}^{m} r_j \cdot y_j, \quad l, m, n, n_i \text{ are positive integers and } \ x_i, y_j \text{ and } r_j \ \text{ need not be distinct.}$$

Remark 2.1. The left ideal generated by $X = \{x\}$ is the set $\{nx + r \cdot x \mid n \in \mathbb{N}, r \in R\}$ and is called the *principal left ideal* generated by x. The left ideal (respectively, subring) generated by the empty set is the (0) ideal (respectively, subring). A similar definition holds for the right ideal generated by the set X.

Two-sided ideal generated by X. The two-sided ideal generated by X is the smallest two sided ideal of R containing X. Equivalently, it is the intersection of all two-sided ideals of R that contains X. Elements of the two-sided ideal generated by X are of the form.

$$\sum_{\substack{i=1 \\ x_i \in X, n \in N}}^{m_i} n_i x_i + \sum_{\substack{j=1 \\ r_j \in R, x_j \in X}}^{m_j} r_j \cdot x_j + \sum_{\substack{k=1 \\ s_k \in R, y_k \in X}}^{m_k} y_k \cdot s_k + \sum_{\substack{l=1 \\ a_l, b_l \in R, z_l \in X}}^{m_l} a_l \cdot z_l \cdot b_l.$$

Remark 2.2. The two-sided ideal generated by $X = \{x\}$ is the set $\{nx + r \cdot x + x \cdot s + a \cdot x \cdot b \mid n \in \mathbb{N} \text{ and} r, s, a, b \in R\}$ and is called the *principal two-sided ideal* generated by x.

Principal ideal ring. A commutative ring is called a *principal ideal ring* if every ideal is generated by a single element.

Principal ideal domain. A principal ideal ring R is called a *principal ideal domain* if R is an integral domain.

Finitely generated ideal. An (left/right/two-sided) ideal I is said to be *finitely generated* if there is a finite subset X of I such that the (left/right/two-sided) ideal generated by the set X equal I.