2. Lecture 2 – Prime and maximal ideals, radicals

Theorem. *Let A be a ring. The following are equivalent:*

(1) *A is a field.*
(2) *A has exactly two ideals, $(0) \neq (1)$.*
(3) *Every homomorphism $\phi\colon A \to B$ with $B \neq 0$ is injective.*

Proof. (1) $\Rightarrow$ (2), since if $I \subset A$ is an ideal with $I \neq (0)$, there is an $a \neq 0$ in I. Since A is a field, there is an element $b \in A$ with $ab = 1$, hence $1 \in I$. Then for every $c \in A$, we have $c = c1 \in I$, so $I = A = (1)$.

(2) $\Rightarrow$ (3) If $B \neq 0$, then $1 \neq 0$ in B. Since $\phi(1) = 1$, we have $1 \notin \ker\phi$, and so $\ker\phi \neq (1)$. Hence $\ker\phi = (0)$, which means ϕ is injective.

(3) $\Rightarrow$ (1) Omitted □

2.1. Prime and maximal ideals.

Definition. Let A be a ring, and let $\mathfrak{a} \subseteq A$ be an ideal. We say $\mathfrak{a}$ is a

- **prime** ideal if, for any $a, b \in A \setminus \mathfrak{a}$ we have $ab \notin \mathfrak{a}$
- **maximal** ideal if $\mathfrak{a} \neq (1)$, and the only ideal containing $\mathfrak{a}$ is (1).

Example. In $\mathbb{Z}$, the prime ideals are (0) and (p) for primes p. These are prime since

$$a, b \notin (0) \Leftrightarrow a, b \neq 0 \Rightarrow ab \neq 0 \Leftrightarrow ab \notin (0)$$

and

$$a, b \notin (p) \Leftrightarrow p \text{ does not divide } a, b \Rightarrow p \text{ does not divide } ab \Leftrightarrow ab \notin (p)$$

The maximal ideals are the ideals (p), for all primes p.

Example. Let k be a field. The ideals of $k[x]$ are all principal. An ideal $(f) \subseteq k[x]$ is

- prime if f is irreducible or $f = 0$.
- maximal if f is irreducible.

Proposition. (1) *An ideal $\mathfrak{a} \subseteq A$ is prime if and only if $A/\mathfrak{a}$ is an integral domain.*
(2) *It is maximal if and only if $A/\mathfrak{a}$ is a field.*

Proof. (1) If $\mathfrak{a}$ is prime, then given $a, b \in A \setminus \mathfrak{a}$, we have $ab \notin \mathfrak{a}$. Then $(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} \neq 0 + \mathfrak{a} \in A/\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is not prime, there exist $a, b \in A \setminus \mathfrak{a}$ such that $ab \in \mathfrak{a}$, which gives that $(a + \mathfrak{a})(b + \mathfrak{a}) = 0$ in $A/\mathfrak{a}$, proving $A/\mathfrak{a}$ is not an integral domain.

(2) $A/\mathfrak{a}$ is a field $\Leftrightarrow$ $A/\mathfrak{a}$ has exactly two ideals $\Leftrightarrow$ There are exactly two ideals in A containing $\mathfrak{a}$ $\Leftrightarrow$ $\mathfrak{a}$ is maximal

□

Corollary. *Every maximal ideal is a prime ideal.*

Proof. $\mathfrak{a}$ maximal $\Leftrightarrow$ $A/\mathfrak{a}$ a field $\Rightarrow$ $A/\mathfrak{a}$ an integral domain $\Leftrightarrow$ $\mathfrak{a}$ a prime ideal. □

Example. Let k be a field, let $a_1, \ldots, a_n \in k$ and consider the homomorphism $\phi\colon k[x_1, \ldots, x_n] \to k$ given by $\phi(f) = f(a_1, \cdots, a_n)$, i.e. evaluate the polynomial f by substituting a_i for x_i. This ϕ is surjective, and the ideal $\ker\phi$ is maximal, since

$$k[x_1, \ldots, x_n]/\ker\phi \cong \operatorname{im}\phi = k,$$

which is a field.

2.2. **Existence of maximal ideals.**

Theorem. *Let A be a non-zero ring. There exists a maximal ideal $\mathfrak{m} \subseteq A$.*

Corollary. *If $\mathfrak{a} \subset A$ is an ideal and $\mathfrak{a} \neq (1)$, then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.*

Proof. $A/\mathfrak{a}$ has a maximal ideal, which under the correspondence between ideals of A and those of $A/\mathfrak{a}$ gives a maximal ideal containing $\mathfrak{a}$. □

Corollary. *Let f be a ring. Then f is a non-unit if and only if f is contained in a maximal ideal.*

Proof. f a non-unit $\Leftrightarrow (f) \neq (1) \Leftrightarrow (f) \subseteq \mathfrak{m}$ for a maximal $\mathfrak{m} \Leftrightarrow f \in \mathfrak{m}$ for a maximal $\mathfrak{m}$. □

The proof of the theorem uses **Zorn's lemma**.

Definition. A **partially ordered set** is a set S and a binary relation $\leq$ on the elements of S such that

(1) For all $x \in S$, $x \leq x$.
(2) For $x, y, z \in S$ such that $x \leq y$ and $y \leq z$, we have $x \leq z$.
(3) If $x \leq y$ and $y \leq x$, then $x = y$.

Remark. Given x, y in a partially ordered set S, they may be incomparable in the sense that neither $x \leq y$ nor $y \leq x$.

Definition. Let R be a subset of a partially ordered set $(S, \leq)$. An element $x \in S$ is an **upper bound** for R if for every $y \in R$ we have $y \leq x$.

Definition. An element $x \in S$ is **maximal** if there is no $y \in S$ with $x < y$ (meaning $x \leq y$ and $y \neq x$).

Definition. A subset $R \subseteq S$ of a partially ordered set is a **chain** if for every $x, y \in R$ we have either $x \leq y$ or $y \leq x$.

Example. The set of positive integers admits a partial ordering with $m \leq n$ if and only if $n \mid m$. So e.g. $2 \geq 4 \geq 12$, while 2 and 3 are incomparable. The subset $R = \{2^n \mid n \geq 0\}$ is a chain, since every pair of elements is comparable. This set has a unique maximal element 1.

Theorem (Zorn's lemma)**.** *Let S be a partially ordered set, and assume that every chain $R \subseteq S$ has an upper bound. Then S has a maximal element.*

Proof of existence of maximal ideals. Let S be the set of ideals $\mathfrak{a} \subseteq A$ such that $\mathfrak{a} \neq (1)$. We claim that every chain in S admits an upper bound. Let $\{\mathfrak{a}_i\}_{i \in R}$ be a chain of ideals in S. Define $\mathfrak{a} = \bigcup_{i \in R} \mathfrak{a}_i$. We then have

(1) $\mathfrak{a}$ is a subgroup of $(A, +)$: If $a, b \in \mathfrak{a}$, there are $i, j \in R$ such that $a \in \mathfrak{a}_i$ and $b \in \mathfrak{a}_j$. Now as R is totally ordered, we have either $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ or $\mathfrak{a}_j \subseteq \mathfrak{a}_i$. In either case, we will have that $a + b$ is contained in the bigger of the two ideals, so $\mathfrak{a}$ is closed under addition. It's easy to check that $\mathfrak{a}$ is closed under additive inverses and multiplication from A, so $\mathfrak{a}$ is an ideal.
(2) $\mathfrak{a} \neq (1)$, since if $1 \in \mathfrak{a}$, we must have $1 \in \mathfrak{a}_i$ for some $i \in R$, contradicting the assumption that $\mathfrak{a}_i \in S$.

Thus $\mathfrak{a}$ is an upper bound for the chain R. Since every chain of ideals has an upper bound, Zorn's lemma tells us that maximal ideals exist. □

2.3. **Local rings.**

Definition. A ring A is **local** if it has precisely one maximal ideal.

Example. Every field is a local ring with maximal ideal (0).

Example. Let p be a prime, and let $k \geq 1$. Then the ideals of $\mathbb{Z}/(p^k)$ correspond to ideals of $\mathbb{Z}$ which contain (p^k). These are given by (n), where n divides p^k, and so the ideals of $\mathbb{Z}/(p^k)$ are the images of

$$(p^k) \subset (p^{k-1}) \subset \cdots \subset (p) \subset \mathbb{Z}.$$

The unique maximal ideal is the image of (p), so $\mathbb{Z}/(p^k)$ is local.

Example. Let k be a field, and let $A = k[x]/(x^2)$. The ideals of A are in bijection with the ideals of $k[x]$ which contain (x^2). Such an ideal is of the form (f) with f dividing x^2, which means that up to some scalar multiple it is either 1, x or x^2. So in $k[x]$ there are three ideals containing (x^2), namely $(1), (x)$ and (x^2). In A, if we let $\overline{x}$ be the image of x under the quotient map, we have three ideals total

$$(0) = (\bar{x}^2) \subset (\bar{x}) \subset (1) = A.$$

The ideal $(\bar{x})$ is the unique maximal element of A, so A is local.

Proposition. *In a local ring A with maximal ideal $\mathfrak{m}$, the set of units is $A \setminus \mathfrak{m}$.*

Proof. $f \in A$ is a unit $\Leftrightarrow$ f is not contained in a maximal ideal $\Leftrightarrow$ $f \notin \mathfrak{m}$. □

2.4. **Radicals.**

Definition. An element a of a ring A is **nilpotent** if there exists an $n \geq 1$ such that $x^n = 0$. The set of nilpotent elements of A is called the **nilradical** of A, denoted $\mathfrak{N}$.

Proposition. *The nilradical of A is an ideal.*

Proof. It is easy to see that if $a \in \mathfrak{N}$, and $x \in A$, then $-a \in \mathfrak{N}$ and $xa \in \mathfrak{N}$. To see that $\mathfrak{N}$ is closed under addition, observe that if $a, b \in \mathfrak{N}$, we have $m, n \geq 0$ such that $a^m = b^n = 0$. Now compute

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}.$$

If $i \geq m$, then $a^i = 0$, while if $i < m$, then $m + n - i \geq n$ so $b^{m+n-i} = 0$. Hence all terms vanish and so $a + b \in \mathfrak{N}$. □

Theorem. *The nilradical $\mathfrak{N}$ of A is the intersection of all prime ideals of A.*

Half of the proof. Easy half: If $f \in A$ is nilpotent and $\mathfrak{p}$ is prime ideal, then $f^n = 0 \Rightarrow f^n \in \mathfrak{p} \Leftrightarrow f \in \mathfrak{p}$. This gives us $\mathfrak{N} \subseteq \cap\mathfrak{p}$.

Hard half: If $f \in A$ is contained in all prime ideals of A, then f is nilpotent. □

Example. In any integral domain, obviously f is nilpotent if and only if $f = 0$, so $\mathfrak{N} = (0)$.

In $\mathbb{Z}/(p^k)$, we have just one prime ideal (p), so $\mathfrak{N} = (p)$.

Definition. Let A be a ring. The **Jacobson radical** of A, denoted $\mathfrak{R}$, is the intersection of all the maximal ideals of A.

Example. In $\mathbb{Z}$, a field k, and $k[x_1, \ldots, x_n]$, we have $\mathfrak{R} = (0)$, while in a local ring A, we by definition have $\mathfrak{R} = \mathfrak{m}$, the unique local ideal.

Key concepts Lecture 2

- Prime ideal
- Maximal ideal
- Prime and maximal ideals in $\mathbb{Z}$ and $k[x]$
- Quotient rings of prime and maximal ideals are integral domains and fields, respectively
- Theorem of existence of maximal ideals, statement and corollaries
- Theorem of existence of maximal ideals, main idea of proof
- Local ring
- Nilradical
- Description of nilradical via prime ideals
- Jacobson radical