Lecture 27

Prime and maximal ideals

(27.0) Let R be a commutative ring. Recall that an abelian subgroup $\mathfrak{a} \subset R$ is an ideal in R if

$$\forall\, a \in \mathfrak{a},\ r \in R \ ; \quad ra \in \mathfrak{a}$$

(27.1) Definition. A proper ideal $\mathfrak{p} \subsetneq R$ is a <u>prime ideal</u> if for every $a, b \in R$ we have

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

A proper ideal $\mathfrak{m} \subsetneq R$ is a <u>maximal ideal</u> if

$$\left.\begin{array}{l} \mathfrak{m} \subsetneq \mathfrak{a} \\ \mathfrak{a} \subset R \text{ an ideal} \end{array}\right. \implies \mathfrak{a} = R$$

(27.2) Prop. Maximal ideals exist.

Proof. Let $\mathcal{I}$ = set of all proper ideals of R. The set $\mathcal{I}$ is non-empty as $(0) \in \mathcal{I}$. It is partially ordered by inclusion.

Consider a chain (= a totally ordered subset of $\mathcal{I}$)

$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ Define $\mathfrak{a} := \bigcup_{j \geq 1} \mathfrak{a}_j$

Claim: $\mathfrak{a} \in \mathcal{I}$.

Pf. of the claim: $a, b \in \mathfrak{a} \Rightarrow \exists\, \ell$ s.t. $a, b \in \mathfrak{a}_\ell$

$\Rightarrow a + b \in \mathfrak{a}_\ell \Rightarrow a + b \in \mathfrak{a}$

Thus we can show that $\mathfrak{a}$ is a subgroup. Similarly if

$a \in \mathfrak{a}$, $r \in R$, $\exists\, \ell$ s.t. $a \in \mathfrak{a}_\ell \Rightarrow r.a \in \mathfrak{a}_\ell \Rightarrow r.a \in \mathfrak{a}$

Hence $\mathfrak{a} \subset R$ is an ideal. If $\mathfrak{a} = R$ then $1 \in \mathfrak{a}$, meaning $\exists\, \ell \geq 1$ s.t. $1 \in \mathfrak{a}_\ell$ which contradicts the fact that $\mathfrak{a}_\ell \subsetneq R$.

In conclusion $\mathfrak{a} \in \mathcal{I}$ and $\mathfrak{a}_j \subset \mathfrak{a}$ $\forall j \geq 1$. In other words, every chain in $\mathcal{I}$ has a supremum. By Zorn's lemma, there are maximal elements in $\mathcal{I}$ $\square$

Cor. Let $\mathfrak{a} \subsetneq R$ be a proper ideal. Then there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.

[use the proposition for $R/\mathfrak{a}$].

(27.3) Prop. (i) A proper ideal $\mathfrak{p} \subsetneq R$ is prime iff

$R/\mathfrak{p}$ is an integral domain.

(ii) A proper ideal $\mathfrak{m} \subsetneq R$ is maximal iff $R/\mathfrak{m}$ is a field

Proof (i) $\mathfrak{p}$ is prime $\Leftrightarrow$ $a\cdot b \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

$\Leftrightarrow$ $\pi(a)\pi(b) = 0$ in $R/\mathfrak{p}$ $\Rightarrow$ $\pi(a) = 0$ or $\pi(b) = 0$

(here $\pi : R \longrightarrow R/\mathfrak{p}$)

$\Leftrightarrow$ $R/\mathfrak{p}$ is an integral domain.

(ii) Easy Lemma. A comm ring A is a field iff

(0) and A are the only ideals in A.

(proof left as an exercise).

Now $R/\mathfrak{m}$ is a field $\Leftrightarrow$ (0) and $R/\mathfrak{m}$ are the only

ideals of $R/\mathfrak{m}$

Since $\{\text{Ideals in } R/\mathfrak{a}\} \longleftrightarrow \{\text{Ideals in } R \text{ containing } \mathfrak{a}\}$

(see §25.6 page 6)

$R/\mathfrak{m}$ is a field $\Leftrightarrow$ the only ideals of R containing $\mathfrak{m}$

are $\mathfrak{m}$ and R $\Leftrightarrow$ $\mathfrak{m} \subsetneq R$ is a max'l ideal $\square$

Cor. Every maximal ideal is prime.

(27.4) Example. $R = \mathbb{Z}$. $\{(0), (p)\}_{\substack{p \in \mathbb{Z}_{\geq 2} \\ \text{prime}}}$ are all the prime ideals. (0) is prime but not maximal. (p) is maximal for every $p \geq 2$ prime.

(27.5) Prop. Let $f : A \longrightarrow B$ be a ring hom between two comm. rings A & B. Let $q \subsetneq B$ be a prime ideal. Then $p = f^{-1}(q) \subsetneq A$ is a prime ideal.

Note – The statement would be false for maximal ideals. eg. $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$, $q = (0)$ is a max'l ideal but $f^{-1}((0)) = (0)$ is not max'l.

Proof:– $ab \in p \Rightarrow f(a) \cdot f(b) \in q$

$\Rightarrow f(a) \in q$ or $f(b) \in q \Rightarrow a \in p$ or $b \in p$

(as q is prime)

Hence $p \subsetneq A$ is prime. $\square$

(27.6) Definition — A commutative ring R is called <u>local</u> if it has only one max'l ideal.

Examples. (i) every field is local.

(ii) $R = \mathbb{C}[x]/(x^3)$ is local [true for <u>any field K</u>, not just $\mathbb{C}$].

(iii) $R = K[[x]]$ power series in one variable is <u>local</u>.

$$f \in R \ : \quad f = a_0 + a_1 x + a_2 x^2 + \dots = \sum_{\ell=0}^{\infty} a_\ell x^\ell$$

Addition (componentwise) $$\left(\sum_{k=0}^{\infty} a_k x^k\right) + \left(\sum_{\ell=0}^{\infty} b_\ell x^\ell\right) = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

Mult. $$\left(\sum_{k=0}^{\infty} a_k x^k\right)\left(\sum_{\ell=0}^{\infty} b_\ell x^\ell\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

Prop. R is local iff ($\mathfrak{m} =$) the set of all non-units in R is an ideal.

Proof — Assume R is local with unique max'l ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is proper, every element of $\mathfrak{m}$ is a non-unit.

Conversely if $a \in R$ is not a unit, $(a) \subsetneq R$.

By Cor (27.2) on page 2 above, $(a) \subset$ some max'l ideal $= \mathfrak{m}$. Hence $\mathfrak{m}$ = set of all non-units is an ideal.

($\Leftarrow$) If $\mathfrak{m}$ = the set of all non-units is an ideal, then $\mathfrak{m}$ is maximal (clear since every ideal properly containing $\mathfrak{m}$ will have a unit in it, implying it is R).

Furthermore if $\mathfrak{a} \subsetneq R$ is an ideal, then every $a \in \mathfrak{a}$ is a non-unit $\Rightarrow \mathfrak{a} \subset \mathfrak{m}$. Thus $\mathfrak{m}$ is the unique max'l ideal. $\square$

Example (ii) $\quad R = K[x]/(x^3) \ni a_0 + a_1 x + a_2 x^2 =: f(x)$

Claim $\quad f(x)$ is a unit $\Leftrightarrow a_0 \in K \setminus \{0\}$.

Pf. $\quad (a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2) = 1$

$$\Leftrightarrow \quad \begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \end{aligned} \qquad \text{i.e.} \qquad \begin{aligned} b_0 &= a_0^{-1} \quad (\text{so } a_0 \neq 0) \\ b_1 &= -a_1 a_0^{-2} \\ b_2 &= a_0^{-1}(-a_0^{-1} a_2 + a_0^{-2} a_1^2) \end{aligned}$$

Thus $\quad$ Set of non-units $= (x)$ is an ideal

$\Rightarrow$ R is local w/ unique max'l ideal $= (x)$.

(27.7) Definition. Recall $a \in R$ is called a unit if it has a multiplicative inverse.

$x \in R$ is called <u>nilpotent</u> if $\exists\, n \geq 1$, such that $x^n = 0$.

Let $\mathcal{N}$ = set of all nilpotent elements of R.

Lemma. $\mathcal{N}$ is an ideal of R. (called nil radical)

Proof. $a, b \in \mathcal{N} \Rightarrow \exists\, k, l \geq 1$ s.t. $a^k = 0 = b^l$

$$\Rightarrow (a+b)^{k+l} = \sum_{j=0}^{k+l} \binom{k+l}{j} a^j b^{k+l-j} = 0$$

$\Rightarrow a + b \in \mathcal{N}$.

Similarly, $r \in R$, $a \in \mathcal{N}$ $(\Rightarrow \exists\, k \geq 1$ s.t. $a^k = 0)$ $\Rightarrow (r \cdot a)^k = 0$

$\Rightarrow r \cdot a \in \mathcal{N}$. Hence $\mathcal{N}$ is an ideal. $\square$