

Lecture 19 (Primes, Maximal Ideals and Fields)

Definition 19.1 (Prime Ideals) Let R be a commutative ring. An ideal P of R is called prime if $P \neq R$, and for $a, b \in R$,

$$ab \in P \Rightarrow a \in P \text{ or } b \in P.$$

Remarks

1. Equivalently P is prime if and only if the quotient ring $R/P \neq O$ and has no zero-divisors.
2. The zero ideal of R is prime if and only if R has no zero-divisors.
3. In particular for a commutative ring with identity the zero ideal is a prime ideal if and only if R is an integral domain.

Lemma 19.2 (Primes Elements and Prime Ideals) Let R be a commutative ring. Then a non-zero element $p \in R$ is prime if and only if pR , the principal ideal it generates, is a prime ideal.

Proof The ideal $pR \neq R$ if and only if p is not a unit. For $a, b \in R$, $ab \in pR$ if and only if $p|ab$, and $p|a$ or $p|b$ if and only if $a \in pR$ or $b \in pR$. \square

Corollary If R is a principal ideal domain then the prime ideals of R are the zero ideal O and the ideals pR , $p \in R$ a prime element.

Definition 19.3 (Maximal Ideals) An ideal M of a commutative ring R is called maximal if $M \neq R$ and for an all ideals I of R , $M \subseteq I$ implies $I = M$ or $I = R$.

Proposition 19.4 (Field and Maximal Ideals) Let R be a commutative ring with an identity element. Then an ideal M is maximal if and only if R/M is a field.

Proof All quotients of a commutative ring with an identity element are commutative and have an identity element. From tutorials we know a field is a commutative ring with 1 with two ideals O and R , $O \neq R$. Equivalently a field is a commutative ring with an identity element in which the zero ideal is maximal. We also know the Third Isomorphism Theorem which tells that reducing modulo M sets up an order preserving 1–1 correspondence between the ideals of R containing M and the ideals of R/M . Hence the ideal M is a maximal in R if and only if the zero ideal of R/M is maximal in R/M , which is the case if and only if R/M is a field.

Corollary Maximal ideals are prime.

Proof An ideal $M \neq R$ in a commutative ring with identity is prime if and only if R/M is an integral domain, and fields are integral domains. \square

Theorem 19.5 Let R be a principal ideal domain and $\pi \in R$ an irreducible element. Then $R/\pi R$ is a field.

Proof Because principal ideal domains are integral domains they are commutative and have an identity element. Hence so do all their quotient rings. Irreducibles are not units. Consequently $\pi R \neq R$. So $R/\pi R$ is not the zero ring. It remains to show the non zero elements of $R/\pi R$ have (multiplicative) inverses. Equivalently given $a \notin \pi R$, i.e. $\pi \nmid a$, we show there are $x \in R$ with $ax \equiv 1 \pmod{\pi R}$.

Suppose $a \notin \pi R$, i.e. a is not a multiple of π . The ideal $aR + \pi R = dR$, where $d \in R$ is a g.c.d. of a and π . Now $d|\pi$ implies d is a unit or an associate of π , because π is irreducible. But $d|a$, and $\pi \nmid a$. So d is not an associate of π . So d is a unit. Hence $aR + \pi R = dR = R$. Now $1 \in R = aR + \pi R$ means that for some $x, y \in R$, $ax + \pi y = 1$. Reducing modulo π we find $ax \equiv 1 \pmod{\pi R}$. \square

Examples

1. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field for p a prime number.
2. Recall if $p \equiv 3 \pmod{4}$ is prime number, p is irreducible in $\mathbb{Z}[i]$. So $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a field. This field has p^2 elements.

For example taking $p = 3$,

$$\mathbb{Z}[i]/3\mathbb{Z}[i] = \{0, 1, 2, i, 1 + i, 1 + 2i, 2i, 1 + 2i, 2 + 2i \pmod{3}\}.$$

3. If F is a field and $m(x)$ is irreducible in $F[x]$, $F[x]/m(x)F[x]$ is a field.