Visual Algebra

Lecture 8.8: Prime and primary ideals

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Prime ideals

Euclid's lemma (300 B.C.)

If a prime p divides ab, then it must divide a or b.

Definition

Let R be a commutative ring. An ideal $P \subsetneq R$ is prime if $ab \in P$ implies $a \in P$ or $b \in P$.

Examples

1. The ideal (n) of $\mathbb{Z}$ is a prime ideal iff n is a prime number (possibly $n = 0$).
2. In $\mathbb{Z}[x]$, the ideals $(2, x)$ and (x) are prime.
3. The ideal $(2, x^2 + 5)$ is not prime in $\mathbb{Z}[x]$ because

$$x^2 - 1 = (x+1)(x-1) \in (2, x^2 + 5), \qquad \text{but } x \pm 1 \notin (2, x^2 + 5).$$

Proposition (exercise)

R is an integral domain if and only if $0 := \{0\}$ is a prime ideal. □

Prime ideals

Proposition

An ideal $P \subsetneq R$ is prime iff R/P is an integral domain.

Proof

Consider the canonical quotient

$$\pi \colon R \longrightarrow R/P, \qquad \pi(r) = \overline{r} := r + P.$$

Note that the zero element is $\overline{0} = P = p + P$, for any $p \in P$, and

$$\overline{a}\,\overline{b} = \overline{ab}, \qquad \text{because } (a+P)(b+P) = ab + P.$$

Using the definitions, and our "boring but useful coset lemma",

$$\begin{aligned} P \text{ is prime} \quad &\Longleftrightarrow \quad ab \in P \;\Rightarrow\; a \in P \text{ or } b \in P \\ &\Longleftrightarrow \quad \overline{ab} = 0 \;\Rightarrow\; \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0} \\ &\Longleftrightarrow \quad R/P \text{ is an integral domain.} \end{aligned}$$

□

Corollary

In a commutative ring, every maximal ideal is prime. □

Primary ideals

Definition

Let R be a commutative ring. An ideal $P \subsetneq R$ is primary if $ab \in P$ implies $a \in P$ or $b^n \in P$ for some $n \in \mathbb{N}$.

In the integers:

- The prime ideals are of the form $(p) = p\mathbb{Z}$, for some prime p.
- The primary ideals are of the form $(p^n) = p^n\mathbb{Z}$, for some prime p.
- Every ideal can be written uniquely as an intersection of primary ideals. For example,

  $$200\mathbb{Z} = 8\mathbb{Z} \cap 25\mathbb{Z}.$$

  This is its primary decomposition.

Remark

An ideal P of R is:

- prime iff the only zero divisor of R/P is zero,
- primary iff every zero divisor of R/P is nilpotent.