MATH 415

Modern Algebra I

Lecture 23:
Prime and maximal ideals.
Ideals in polynomial rings.

Prime ideals

Definition. A (two-sided) ideal I in a ring R is called **prime** if for any elements $x, y \in R$ we have

$$xy \in I \implies x \in I \text{ or } y \in I.$$

Example. In the ring $\mathbb{Z}$, every nontrivial proper ideal is of the form $n\mathbb{Z}$, where $n > 1$. This ideal is prime if and only if n is a prime number.

The entire ring R is always a prime ideal of itself. The trivial ideal $\{0\}$ is prime if and only if the ring R has no divisors of zero.

Theorem The ideal I is prime in the ring R if and only if the factor ring R/I has no divisors of zero.

Proof ("if"). Suppose $xy \in I$ while $x, y \in R \setminus I$. Then $x + I \neq 0 + I$ and $y + I \neq 0 + I$ while $(x + I)(y + I) = xy + I = I$ so that $x + I$ and $y + I$ are divisors of zero in R/I.

Maximal ideals

Definition. A (two-sided) ideal I in a ring R is called **maximal** if $I \neq R$ and for any ideal J satisfying $I \subset J \subset R$, we have $J = I$ or $J = R$.

Example. In the ring $\mathbb{Z}$, every nontrivial proper ideal is of the form $n\mathbb{Z}$, where $n > 1$. This ideal is contained in an ideal $m\mathbb{Z}$ if and only if m divides n. It follows that the ideal $n\mathbb{Z}$ is maximal if and only if it is prime.

Theorem A proper ideal I in the ring R is maximal if and only if the factor ring R/I has no (two-sided) ideals other than the trivial ideal and itself.

Definition. A non-trivial ring R is called **simple** if it has no ideals other than the trivial ideal and itself.

A ring is simple if and only if the trivial ideal $\{0\}$ is maximal.

Theorem A proper ideal I in the ring R is maximal if and only if the factor ring R/I is simple.

Proof. Consider a map $\phi : R \to R/I$ given by $\phi(x) = x + I$ for all $x \in R$. This map is a homomorphism of rings.

Suppose R/I has a nontrivial proper ideal J'. Then $J = \phi^{-1}(J')$ is an ideal in R such that $I \subset J \subset R$. Since the map ϕ is onto, it follows that $J \neq I$ and $J \neq R$. In particular, the ideal I is not maximal.

Conversely, assume that there is an ideal J in R such that $I \subset J \subset R$ while $J \neq I$ and $J \neq R$. Then $J' = \phi(J)$ is an ideal in $\phi(R) = R/I$. The ideal J' is nontrivial since J is not contained in the kernel $\mathrm{Ker}(\phi) = I$. Since $I \subset J$, it follows that $\phi(J) = J'$ is disjoint from $\phi(R \setminus J)$. In particular, J' is a proper ideal in R/I.

Theorem Suppose R is a commutative ring with unity. Then R is simple if and only if it is a field.

Proof. Assume R is a field and let I be a nontrivial ideal in R. Take any nonzero element $a \in I$. Since R is a field, this element admits a multiplicative inverse a^{-1}. Then for any $x \in R$ we have $x = 1x = (aa^{-1})x = a(a^{-1}x) \in I$. That is, $I = R$.

Now assume R is not a field. Then there is a nonzero element $a \in R$ that does not admit a multiplicative inverse. Hence $aR = \{ax \mid x \in R\}$, which is an ideal in R, does not contain the unity 1. In particular, aR is a proper ideal. It is nontrivial since $a = a \cdot 1 \in aR$.

Corollary 1 Suppose R is a commutative ring with unity. Then a proper ideal $I \subset R$ is maximal if and only if the factor ring R/I is a field.

Corollary 2 Suppose R is a commutative ring with unity. Then any maximal ideal in R is prime.

Remark. If the ring R is not commutative then the corollaries (and the preceding theorem) may fail. For example, in the ring $\mathcal{M}_{n,n}(\mathbb{R})$ of $n \times n$ matrices with real entries ($n \geq 2$), the trivial ideal is maximal but not prime. Note that this ring does have one-sided proper nontrivial ideals.

Ideals in the ring of polynomials

Theorem Let $\mathbb{F}$ be a field. Then any ideal in the ring $\mathbb{F}[x]$ is of the form

$$p(x)\mathbb{F}[x] = \{p(x)q(x) \mid q(x) \in \mathbb{F}[x]\}$$

for some polynomial $p(x) \in \mathbb{F}[x]$.

Theorem Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$ be a polynomial of positive degree. Then the following conditions are equivalent:

- $p(x)$ is irreducible over $\mathbb{F}$,
- the ideal $p(x)\mathbb{F}[x]$ is prime,
- the ideal $p(x)\mathbb{F}[x]$ is maximal,
- the factor ring $\mathbb{F}[x]/p(x)\mathbb{F}[x]$ is a field.

Examples. • $\mathbb{F} = \mathbb{R}$, $p(x) = x^2 + 1$.

The polynomial $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}$. Hence the factor ring $\mathbb{R}[x]/I$, where $I = (x^2 + 1)\mathbb{R}[x]$, is a field. Any element of $\mathbb{R}[x]/I$ is a coset $q(x) + I$. It consists of all polynomials in $\mathbb{R}[x]$ leaving a particular remainder when divided by $p(x)$. Therefore it is uniquely represented as $a + bx + I$ for some $a, b \in \mathbb{R}$. We obtain that

$$(a + bx + I) + (a' + b'x + I) = (a + a') + (b + b')x + I,$$

$$\begin{aligned}(a + bx + I)(a' + b'x + I) &= aa' + (ab' + ba')x + bb'x^2 + I \\ &= (aa' - bb') + (ab' + ba')x + bb'(x^2 + 1) + I \\ &= (aa' - bb') + (ab' + ba')x + I.\end{aligned}$$

It follows that a map $\phi : \mathbb{C} \to \mathbb{R}[x]/I$ given for all $a, b \in \mathbb{R}$ by $\phi(a + bi) = a + bx + I$ is an isomorphism of rings. Thus $\mathbb{R}[x]/I$ is a model of complex numbers. Note that the imaginary unit i corresponds to $x + I$, the coset of the monomial x.

Problem. Let $\mathbb{F}_4$ be a field with 4 elements and $\mathbb{F}_2$ be its subfield with 2 elements. Find a polynomial $p \in \mathbb{F}_2[x]$ that has no zeros in $\mathbb{F}_2$, but has a zero in $\mathbb{F}_4$.

Let $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$. Then $\mathbb{F}_2 = \{0, 1\}$. Since $\{1, \alpha, \beta\}$ is a multiplicative group (of order 3), it follows from Lagrange's Theorem that $x^3 = 1$ for all $x \in \{1, \alpha, \beta\}$. In other words, 1, α and β are zeros of the polynomial $q(x) = x^3 - 1$.

We have $x^3 - 1 = (x - 1)(x^2 + x + 1)$, which holds over any field. It follows that α and β are also zeros of the polynomial $p(x) = x^2 + x + 1$. Note that $p(0) = p(1) = 1 \neq 0$.

- $\mathbb{F} = \mathbb{Z}_2$, $p(x) = x^2 + x + 1$.

We have $p(0) = p(1) = 1 \neq 0$ so that p has no zeros in $\mathbb{Z}_2$. Since $\deg(p) \leq 3$, it follows that the polynomial $p(x)$ is irreducible over $\mathbb{Z}_2$. Therefore $\mathbb{Z}_2[x]/(x^2 + x + 1)\mathbb{Z}_2[x]$ is a field. This factor ring consists of 4 elements: 0, 1, α and $\alpha + 1$, where $\alpha = x + p(x)\mathbb{Z}_2[x]$. Observe that α and $\alpha + 1$ are zeros of the polynomial p.

- $\mathbb{F} = \mathbb{Z}_2$, $p(x) = x^3 + x + 1$.

There are two polynomials of degree 3 irreducible over $\mathbb{Z}_2$: $p(x) = x^3 + x + 1$ and $q(x) = p(x - 1) = x^3 + x^2 + 1$. In particular, the factor ring $\mathbb{Z}_2[x]/(x^3 + x + 1)\mathbb{Z}_2[x]$ is a field. It consists of 8 elements: 0, 1, β, $\beta + 1$, β^2, $\beta^2 + 1$, $\beta^2 + \beta$ and $\beta^2 + \beta + 1$, where $\beta = x + p(x)\mathbb{Z}_2[x]$. Observe that β, β^2 and $\beta^2 + \beta$ are zeros of the polynomial p while $\beta + 1$, $\beta^2 + 1$ and $\beta^2 + \beta + 1$ are zeros of the polynomial q.