MATH 415

Modern Algebra I

Lecture 35:
Ideals in polynomial rings.

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 $p(0) = p(1) = 1 \neq 0$.

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.

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

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.