Session: 15

Course Material: Construction of finite field

Let R be a commutative ring and $p(x) \in R[x]$. We define $I = \{ p(x) f(x) | \; f(x) \in R[x] \}$. It is easy to check that I is an ideal of $R[x]$ and the ideal I is called **ideal generated by** $p(x)$**,** denoted by $I = \langle p(x) \rangle$.

Example 1:

1. If R is a commutative ring with unity u, then the ideal of R[x] generated by u is $I = \langle u \rangle = \{ u \, f(x) | \; f(x) \in R[x] \} = \{ f(x) | \; f(x) \in R[x] \} = R[x]$.

2. If R is a commutative ring and $p(x) = x$, then the ideal of R[x] generated by $p(x)$ is $I = \langle x \rangle = \{ x \, f(x) | \; f(x) \in R[x] \}$.

Theorem 1 (Gallian, et.al, 2010) Let *F* be a field and $p(x) \in F[x]$. $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over *F*.

Proof: ($\Rightarrow$) Suppose $\langle p(x) \rangle$ is a maximal ideal in $F[x]$, then $p(x)$ is neither the zero polynomial nor a unit in $F[x]$, because if $p(x)$ is zero polynomial, then $\langle p(x) \rangle$ = {0} is not maximal ideal in $F[x]$ and if $p(x)$ is a unit, then the unity $u \in \langle p(x) \rangle$, imply $\langle p(x) \rangle$ = $F[x]$ that is not maximal ideal in $F[x]$.

Let $p(x) = f(x) g(x)$, then $\langle p(x) \rangle = \langle f(x) g(x) \rangle \subseteq \langle f(x) \rangle \subseteq F[x]$. Thus $\langle p(x) \rangle = \langle f(x) \rangle$ or $\langle f(x) \rangle = F[x]$. In the first case, $\deg p(x) = \deg f(x)$, then $\deg g(x) = 0$ and in the second case, $\deg f(x) = 0$. Thus, $f(x)$ is a unit or $g(x)$ is a unit in $F[x]$. We conclude that $p(x)$ is irreducible over *F*.

($\Leftarrow$) Suppose that $p(x)$ is irreducible over *F*. Let I be any ideal of $F[x]$ such that $\langle p(x) \rangle \subseteq I \subseteq F[x]$. Because $F[x]$ is principle ideal domain (PID), then $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$, then $\langle p(x) \rangle \subseteq I = \langle g(x) \rangle$, then $p(x) \in \langle g(x) \rangle$. Therefore there exists $f(x) \in F[x]$

such that $p(x) = g(x)f(x)$. Because $p(x)$ is irreducible over *F*, then $g(x)$ is a unit or $f(x)$ is a unit in $F[x]$. For the first case, $g(x)$ is a unit , $I = \langle g(x) \rangle = F[x]$ and for the second case, $f(x)$ is a unit, $\langle p(x) \rangle = \langle g(x) \rangle = I$. We conclude that if $\langle p(x) \rangle \subseteq I \subseteq F[x]$, then $\langle p(x) \rangle = I$ or $I = F[x]$, thus $\langle p(x) \rangle$ is a maximal ideal in $F[x]$. □

Theorem 2 (Gallian, et.al, 2010) If *F* be a field and $p(x)$ is an irreducible polynomial over *F*, then $F[x] / \langle p(x) \rangle$ is a field.

Proof: clear.

A Finite field of p elements where p is prime is $\mathbb{Z}_p$.

Construction of finite field of p^n elements where p is prime, n > 1:

1. Take finite field $\mathbb{Z}_p$.
2. Find an irreducible polynomial $p(x)$ in $\mathbb{Z}_p[x]$ with $\deg p(x) = n$.
3. Construct finite field $\mathbb{Z}_p[x] / \langle p(x) \rangle = \left\{ f(x) + \langle p(x) \rangle \,\middle|\, f(x) \in \mathbb{Z}_p[x] \right\}$.

   The finite field $\mathbb{Z}_p[x] / \langle p(x) \rangle$ has p^n elements.

Example 2:

1. Construct a field with eight elements.

Answer: $8 = 2^3$, p = 2, n = 3.

1. Take finite field $\mathbb{Z}_2 = \{[0],[1]\}$.
2. Find an irreducible polynomial $p(x)$ in $\mathbb{Z}_2[x]$ with $\deg p(x) = 3$. We take $p(x) = x^3 + x + [1]$, and we know that $p(x)$ has no root in $\mathbb{Z}_2$. Thus, $p(x)$ is irreducible in $\mathbb{Z}_2[x]$.
3. Construct a field $\mathbb{Z}_2[x] / \langle x^3 + x + [1] \rangle = \left\{ f(x) + \langle x^3 + x + [1] \rangle \,\middle|\, f(x) \in \mathbb{Z}_2[x] \right\}$.

   Then $\mathbb{Z}_2[x] / \langle x^3 + x + [1] \rangle = \left\{ (a_2x^2 + a_1x + a_0) + \langle x^3 + x + [1] \rangle \,\middle|\, a_0, a_1, a_2 \in \mathbb{Z}_2 \right\}$

$$\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \{ [0] + \langle x^3 + x + [1] \rangle, [1] + \langle x^3 + x + [1] \rangle, x + \langle x^3 + x + [1] \rangle, x + [1] + \langle x^3 + x + [1] \rangle,$$

$$x^2 + \langle x^3 + x + [1] \rangle, x^2 + [1] + \langle x^3 + x + [1] \rangle, x^2 + x + \langle x^3 + x + [1] \rangle, x^2 + x + [1] + \langle x^3 + x + [1] \rangle \}$$

To simplify the notation, we write $a_2 x^2 + a_1 x + a_0$ to simply $a_2 x^2 + a_1 x + a_0 + \langle x^3 + x + 1 \rangle$.

So we have $\mathbb{Z}_2[x] \big/ \langle x^3 + x + [1] \rangle = \{ [0], [1], x, x + [1], \; x^2, x^2 + [1], x^2 + x, x^2 + x + [1] \}$

2. Construct a field with nine elements.

Answer: $9 = 3^2$, p = 3, n = 2.

1. Take finite field $\mathbb{Z}_3 = \{ [0], [1], [2] \}$.

2. Find an irreducible polynomial $p(x)$ in $\mathbb{Z}_3[x]$ with $\deg p(x) = 2$. We take $p(x) = x^2 + [1]$, and we know that $p(x)$ has no root in $\mathbb{Z}_3$. Thus, $p(x)$ is irreducible in $\mathbb{Z}_3[x]$.

3. Construct a field $\mathbb{Z}_3[x] \big/ \langle x^2 + [1] \rangle = \{ f(x) + \langle x^2 + [1] \rangle \mid f(x) \in \mathbb{Z}_3[x] \}$.

Then $\mathbb{Z}_3[x] \big/ \langle x^2 + [1] \rangle = \{ (a_1 x + a_0) + \langle x^2 + [1] \rangle \mid a_0, a_1 \in \mathbb{Z}_3 \}$

$$\mathbb{Z}_3[x] \big/ \langle x^2 + [1] \rangle = \{ [0], [1], [2], x, x + [1], x + [2], [2]x, [2]x + [1], [2]x + [2] \}$$

Exercises 1:

1. Fill completely the addition and multiplication tables of example 2 (part 1).
2. Construct a field of 4 elements.
3. Construct a field of 16 elements.
4. Construct a field of 25 elements.
5. Construct a field of 27 elements.