MATH 369:
SECTION: 4.3 EXISTENCE ROOTS
11/03/2025

LOVE NEPALI

Class Summary

We started the class with the definition of polynomial congruences. Throughout the lesson, we focused mainly on understanding how congruence classes work in $F[x]/(p(x))$, when this structure forms a field, and how to find multiplicative inverses using Euclid's algorithm. We also explored examples like $\mathbb{Z}_2[x]/(x^2+x+1)$ and $\mathbb{R}[x]/(x^2+1)$ to see how these ideas connect to finite fields and complex numbers. The class ended with Kronecker's Theorem, showing that every polynomial has a root in some extension of a field.

Polynomial Congruences. Let F be a field and $p(x) \in F[x]$. We can consider the set of congruence classes in $F[x]$ modulo $p(x)$, written as

$$[a(x)] \text{ where } a(x) \equiv b(x) \pmod{p(x)} \text{ if } p(x) \text{ divides } (a(x)-b(x)).$$

Then $[a(x)]$ is the set of all polynomials congruent with $a(x)$ mod $p(x)$.

We define the addition and multiplication of congruence classes as follows:

$$[a(x)]+[b(x)] = [a(x)+b(x)], \quad [a(x)][b(x)] = [a(x)b(x)].$$

Theorem 1. This definition is well-defined; it doesn't matter which representatives we pick.

Proof. If $a(x) \equiv a'(x)$ and $b(x) \equiv b'(x)$ mod $p(x)$, then $a(x)+b(x) \equiv a'(x)+b'(x)$ and $a(x)b(x) \equiv a'(x)b'(x)$ mod $p(x)$. □

Unique Representatives.

Theorem 2. Every congruence class $[a(x)]$ has a unique representative $a(x)$ such that $\deg(a(x)) < \deg(p(x))$.

Proof. By the division algorithm, for any $b(x)$ we can write $b(x) = q(x)p(x)+a(x)$ with $\deg(a(x)) < \deg(p(x))$. Then $b(x) \equiv a(x)$ mod $p(x)$. □

Multiplicative Inverses. A class $[a(x)]$ has an inverse if there exists $[b(x)]$ such that $[a(x)][b(x)] = [1]$. By Euclid's algorithm, this happens if and only if $\gcd(a(x), p(x)) = 1$.

Theorem 3. $[a(x)]$ has a multiplicative inverse mod $p(x)$ if and only if $\gcd(a(x), p(x)) = 1$.

If $p(x)$ is irreducible, then all nonzero classes have inverses, so $F[x]/(p(x))$ is a field.

Example. Let $F = \mathbb{Z}_2$ and $p(x) = x^2+x+1$. Checking roots:

$$p(0) = 1, \quad p(1) = 1^2+1+1 = 3 \equiv 1 \pmod{2}.$$

No roots $\Rightarrow p(x)$ is irreducible. Thus $\mathbb{Z}_2[x]/(x^2+x+1)$ is a field.

Date: Nov 9, 2025.

Elements of the Field. The field has 4 elements:

$$\{[0], [1], [x], [x+1]\}.$$

Using $x^2 \equiv x + 1 \pmod{x^2 + x + 1}$.

Addition Table.

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

Multiplication Table.

$\cdot$	$[1]$	$[x]$	$[x+1]$	$[0]$
$[1]$	$[1]$	$[x]$	$[x+1]$	$[0]$
$[x]$	$[x]$	$[x+1]$	$[1]$	$[0]$
$[x+1]$	$[x+1]$	$[1]$	$[x]$	$[0]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$

Field with 4 Elements. This shows $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field with 4 elements. Recall $\mathbb{Z}_4$ is not a field, but this structure is.

Field Extensions. If F is a field and $p(x)$ is irreducible in $F[x]$, then

$$E = F[x]/(p(x))$$

is a field extension of F.

Theorem 4. If $p(x)$ is irreducible, then $E = F[x]/(p(x))$ is a field extension of F, and F is contained in E.

Example: Real Field Extension. Consider $\mathbb{R}[x]/(x^2 + 1)$. Every element can be written as $[a + bx]$, $a, b \in \mathbb{R}$.

$$[a + bx] + [c + dx] = [a + c + (b + d)x],$$
$$[a + bx][c + dx] = [ac + (ad + bc)x + bd(x^2)].$$

Since $x^2 \equiv -1$, we get:

$$[a + bx][c + dx] = [ac - bd + (ad + bc)x].$$

Define $\phi([a + bx]) = a + bi$. This map $\phi : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}$ is an isomorphism, as it preserves addition and multiplication.

Kronecker's Theorem.

Theorem 5 (Kronecker's Theorem)**.** If F is any field and $p(x) \in F[x]$ is any polynomial, then there exists a field extension E of F in which $p(x)$ has a root.

Idea. Let $q(x)$ be an irreducible factor of $p(x)$ in $F[x]$. Then $E = F[x]/(q(x))$ is a field, and in E, the class $[x]$ acts as a root of $q(x)$. □