§1 Lecture 11-22

Non constant $f \in \mathbb{F}[x]$ is irreducible over F if f cannot be expressed as $f = gh$ where $\deg(g), deg(h) \geq 1$

Theorem 1.1 (Fundamental Theorem of Algebra)
Every $f \in \mathbb{C}[x]$ can be expressed as $f = l(x - r_1)(x - r_2)(\cdots)(x - r_n)$ where l is the leading coefficient of f and n is the degree of f.

Corollary 1.2
Only degree 1 polynomials can be irreducible in $\mathbb{C}$.

Example 1.3
Let $f \in \mathbb{R}[x]$ with $\deg(f)$ is odd and $\deg(f) > 1$.

Theorem 1.4
An ideal $\langle p \rangle \subset \mathbb{F}[x]$ is maximal $\Leftrightarrow p$ is irreducible over $\mathbb{F}$.

Recall 1.5. Ideal $p = gh$. $\langle p \rangle \subsetneq \langle g \rangle \subseteq \mathbb{F}[x]$

Theorem 1.6
$\mathbb{F}[x]/\langle p \rangle$ is a field $\Leftrightarrow \langle p \rangle$ is a maximal ideal $\Leftrightarrow p$ is irreducible.

So $\mathbb{F}[x]/\langle p \rangle$ is a field $\Leftrightarrow p$ is irreducible.

Example 1.7
$\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$ motivating amazing case.

Lemma 1.8
A degree 2 or 3 polynomial $p \in \mathbb{F}[x]$ is irreducible $\Leftrightarrow p$ has no zero.

Proof. If $p = gh$ with $\deg(g), \deg(h) \geq 1$, then one of these, say g, has $\deg(g) = 1$. Therefore $p = (x - r)g$ for $r \in \mathbb{F} \Leftrightarrow p(r) = 0$. □

Example 1.9

$x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ because it has no roots. $p(0) = 1$ and $p(1) = 1$.

$x^3 + x + 1$ is reducible in $\mathbb{Z}_3[x]$ because it has a root. $p(0) = 1$. $p(1) = 0$. $p(2) = 2$

$x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$ has no roots.

Therefore

$$\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle \text{ is a field}$$
$$\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle \text{ is a field}$$
$$\mathbb{Z}_3[x]/\langle x^3 + x + 1\rangle \text{ is not a field}$$
$$(x + 2 + \langle x^3 + x + 1\rangle)((x^2 + ax + b) + \langle x^3 + x + 1\rangle) = 0 + \langle x^3 + x + 1\rangle$$

Lemma 1.10

Each element of $\mathbb{Z}_n[x]/\langle p\rangle$ (where n is prime) is of the form $a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_0 + \langle p\rangle$. Assume p is monic and that p is irreducible of degree d.

Note that each element can be written in the form $f = \langle p\rangle$ to hvae $\deg(f) < d = \deg(p)$.

Idea:

$$p = x^d + q$$
$$(x^d + \langle p\rangle) + (q + \langle p\rangle) = (x^d + q + \langle p\rangle) = 0 + \langle p\rangle.$$

So we can replace any occurence of x^d by $-q$ and have the same element.

§1.1 Eisention's Criterion

Let p be prime.

Let $f = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$

Suppose

1. p divides each a_i except a_n
2. p^2 does not divide a_0

Then f is irreducible over $\mathbb{Q}$.

Example 1.11

$2x^3 + 25x + 5$ is irreducible use $p = 5$.

$2x^5 + 6x^4 + 5x^3 + 9x^2 + 0x^1 + 30$