Lecture 10: Factorization of Polynomials over a Field

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

The Evaluation Homomorphism

Theorem

Let F be a subfield of a field E, let $\alpha \in E$ and $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. The function

$$\begin{array}{cccc} \phi_\alpha : & F[x] & \longrightarrow & E \\ & f(x) & \longrightarrow & f(\alpha) \end{array}$$

is a homomorphism. The homomorphism ϕ_α is called the **evaluation homomorphism** *for fields.*

From definition of ϕ_α, we have

$$\begin{aligned} \phi_\alpha(x) &= \phi_\alpha(1_F x) = 1_F \alpha = \alpha, \\ \phi_\alpha(a) &= a, \text{for all } a \in F. \end{aligned}$$

For the simplicity, we consider $1_F =: 1$ and $0_F =: 0$.

The Evaluation Homomorphism

Examples:

1. Let $\phi_0 : \mathbb{Q}[x] \longrightarrow \mathbb{R}$, then

$$\phi_0 \left(a_0 + a_1 x + \cdots + a_n x^n \right) = a_0 + a_1 0 + \cdots + a_n 0 = a_0 .$$

2. Let $\phi_i : \mathbb{Q}[x] \longrightarrow \mathbb{C}$, then

$$\phi_i \left(x^2 + 1 \right) = i^2 + 1 = 0.$$

Thus $x^2 + 1 \in Ker\phi_i$.

Definition

Let F be a subfield of a field E and $\phi_\alpha : F[x] \longrightarrow E$ be the evaluation homomorphism. For $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, if

$$f(\alpha) = 0,$$

then α is a **zero** of $f(x)$.

Remark: Our aim is to find the zeros of polynomials. It is same that to find all $\alpha \in E$ such that $\phi_\alpha(f(x)) = 0$ and find all zeros of $f(x)$.

The Division Algorithm

Theorem (The Division Algoritm)

Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

and

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$$

be two polynomials in $F[x]$ *with* $a_n \neq 0, b_m \neq 0$ *and* $m > 0$. *Then* $\exists! q(x), r(x) \in F[x]$ *such that*

$$f(x) = g(x) q(x) + r(x),$$

where either $r(x) = 0$ *or* $\deg r(x) < \deg g(x)$.

Note that If $n = m = 0$, then $q(x) = f(x) g(x)^{-1}$ and $r(x) = 0$.

Remark: The Division Algorithm also holds for a commutative ring with unity when the leading coefficient of $g(x)$ is a unit.

Definition

Let $f(x)$ and $g(x)$ be two nonzero polynomials in $F[x]$. A polynomial $d(x) \in F[x]$ is called the **greatest common divisor** of $f(x)$ and $g(x)$, denoted $d(x) = \gcd(f(x), g(x))$, if

1. $d(x)$ is monic poynomial,
2. $d(x) \mid f(x)$ and $d(x) \mid g(x)$,
3. If $k(x) \mid f(x)$ and $k(x) \mid g(x)$, then $k(x) \mid d(x)$.

Moreover, there exists polynomials $s(x), t(x)$ such that $d(x) = f(x)s(x) + g(x)t(x)$.

Factor Theorem

Definition

Let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. If $\exists\ q(x) \in F[x]$ such that $f(x) = g(x)\,q(x)$, then we say that $g(x)$ **divides** $f(x)$ in $F[x]$ or $g(x)$ is a **factor** of $f(x)$.

Theorem (Remainder Theorem)

For $a \in F, \exists\ q(x) \in F[x]$ such that

$$f(x) = (x-a)\,q(x) + f(a).$$

Factor Theorem

From the remainder theorem, we have the following theorem.

Theorem (Factor Theorem)

$$a \in F \text{ is a zero of } f(x) \in F[x] \Leftrightarrow x - a \text{ is a factor of } f(x) \text{ in } F[x].$$

Factor Theorem

Let $f(x) \in F[x]$ be anonzero polynomial with degree n. From the factor theorem, we have

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_k)\, q_k(x),$$

where $q_k(x)$ has no zero. Since $\deg f(x) = n$, we have $k \leq n$.

Corollary

A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

A relation between cyclic groups and finite fields

Theorem

Let G be a finite group and let $(F^*, .)$ be a multiplicative group of a field F.

$$(G, .) < (F^*, .) \Rightarrow G \text{ is cyclic.}$$