LECTURE 4

Author
Tom Jeong

January 15, 2025

Contents

1 Polynomials in Fields

$p(x) \in K(x)$

$$p = f \cdot g, f, g \in K(x)$$
$$\partial f, \partial g > 0$$
$$\partial f, \partial g < \partial p$$

case 1 $\partial p = 2$

$p = f \cdot g$

$\partial f = \partial g = 1$

p is irreduciable $\leftrightarrow$ p doesn't have units in K (quadrati formula)

case 2:$\partial p = 3$

$\partial f = 1,$

$\partial g = 2$

p is irrudicible $\leftrightarrow$ p doens't have a root in K

case 3:$\partial p = 4$

$\partial f = 2, \partial g = 2$ or $\partial f = 1, \partial g = 3$

$$\mathbb{Q}[x]$$
$$p \in \mathbb{Z}[x]?$$

Lemma 1.1 (Gauss' Lemma)**.**
$h \in \mathbb{Z}[x]$ irridlucible $\Rightarrow$ h is irreducible in $\mathbb{Q}[x]$
($\Leftarrow$): is this true? (no)

$$h = f \cdot g$$
$$h = 2x + 2 = 2(x + 1) \text{ where } \partial f, \partial g < \partial h$$

this constant is not a unit.

Proof.
Suppose $h = f \cdot g$ where $f, g \in \mathbb{Q}[x]$. Clear denominators in f, g.
There is the smallest positive integer k such that $k \cdot h = \bar{f} \cdot \bar{g}$ where $\bar{f}, \bar{g} \in \mathbb{Z}[x]$
There is a prime p dividing k. Let's look at $kh = \bar{f}\bar{g}$ in $\mathbb{Z}_p(x)$
in $\mathbb{Z}_p, 0 = \bar{f}_p \cdot \bar{g}_p$ Z: integral domain, so either one must be 0,

$\bar{f}_p = 0$ or $\bar{g_p} = 0 \rightarrow$ either all coefficients of $\bar{f}$ or all coefficients of $\bar{g}$ iare divisible by $p \rightarrow$ k can be reduced. contradiction.

□

2 Eisenstein's Criterion

$$h \in \mathbb{Z}[x]$$
$$h = a_0 + a_1 x + \cdots + a_n x^n$$

suppose that there exists a prime p such that:

1. $p | a_0, \ldots, a_{n-1}$
2. $p \not| a_n$
3. $p^2 \not| a_0$

$\rightarrow f$ is irreducible in $\mathbb{Q}[x]$

Proof.
suffice to show that h is irridubcible in $\mathbb{Z}[x]$ (Gauss lemma)
Suppose $h = f \cdot g,$ where $f, g \in \mathbb{Z}[x]$ and $\partial f, \partial g < \partial h$
Let's look at $h = fg \mod p$
$h_p = f_p g_p$
$a_n x^n = f_p g_p$
$a_n \not\equiv 0 \mod p$
look $a_0, p \mid a_o, p^2 \nmid a_0$
$\rightarrow p$ divides constant termg, f or g but not both

WLOG,
$p \mid$ constant term of g and $p \nmid$ constant term of $g \rightarrow g_p$ is a polynomial with a constant term

$$a_n x^n = f_p \cdot g_p$$

$\mathbb{Z}_p(x)$ UFD but we have two different factorizations.. contradiction
$rightarrown \mathbb{Z}[x]$can only factor $h = fg, \partial f = 0$ but then divide h by f ☐

2.1 Applicatinos of Eisenstein's criterion

ex.

$$x^4 - 2$$

is irriducible, $p = 2$

$$2x^5 - 4x^3 + 8x^3 + 14x^2 + 7 = h(x)$$

$h(x)$ irreducible $\Leftrightarrow h(\frac{1}{x})x^u, u = \partial h$
$2 - 4x + 8x^2 + 15x^3 + 7x^5$ is irreducible by eisenstein p = 2.

$$h = 1 + x + x^2 + \cdots + x^{p-1}$$

p - prime

Proposition 2.1. h(x) is irreducible in $\mathbb{Q}[x]$

$h(x) = \dfrac{x^p - 1}{x - 1}$

Proof.

consider $h(x+1) = \dfrac{(x+1)^p - 1}{x} = \sum_{k=1}^{p}(\binom{p}{k}x^{p-1})$

$(x+1)^p = \dfrac{x^p + px^{p-1} + \binom{p}{2}p^{x-2} + \dots px + 1 - 1}{x}$

here $p \mid \binom{p}{k}$ $0 < k < p$ □

Several notations of field extentsions

$L/K K \subsetneq L,$ where K, L fields

$L : K, M : L : K$ where $L/K, M/L$

$[L : K] =$ degree of field extesion (dimension L as K vector space)$L/K, L : K$

Theorem 2.2 (Tower Theorem)**.** Let $K \subseteq L \subseteq M$ be fields. Then $[M : K] = [M : L] \cdot [L : K]$

Proof. Let $a_1, \dots, a_s$ be a basis of L as a K-vector space, so $[L : K] = s$. Let $b_1, \dots, b_t$ be a basis of M as an L-vector space, so $[M : L] = t$. For any $l \in L$, we can write $l = \sum_{i=1}^{s} f_i a_i$ where $f_i \in K$. Claim: The set $a_i b_j : 1 \leq i \leq s, 1 \leq j \leq t$ forms a basis of M as a K-vector space. To prove this claim, we need to show:

Linear Independence: Any linear combination $\sum_{i,j} k_{ij}(a_i b_j) = 0$ with $k_{ij} \in K$ implies all $k_{ij} = 0$ Spanning: Any element of M can be written as a linear combination of the $a_i b_j$ with coefficients in K

1. To show $a_i b_j$ are linearly independent: Suppose $\sum_{i=1}^{s} \sum_{j=1}^{t} k_{ij}(a_i b_j) = 0$ where $k_{ij} \in K$. For each fixed j, let $c_j = \sum_{i=1}^{s} k_{ij} a_i \in L$ Then our equation becomes $\sum_{j=1}^{t} c_j b_j = 0$ Since b_j is a basis of M over L, we must have $c_j = 0$ for all j For each j: $0 = c_j = \sum_{i=1}^{s} k_{ij} a_i$ Since a_i is a basis of L over K, we must have $k_{ij} = 0$ for all i, j

2. To show $a_i b_j$ span M as a K-vector space: Let $m \in M$. Since b_j is a basis of M over L, we can write: $m = \sum_{j=1}^{t} l_j b_j$ where $l_j \in L$ For each l_j, since a_i is a basis of L over K, we can write: $l_j = \sum_{i=1}^{s} k_{ij} a_i$ where $k_{ij} \in K$ Substituting: $m = \sum_{j=1}^{t}(\sum_{i=1}^{s} k_{ij} a_i) b_j = \sum_{i=1}^{s} \sum_{j=1}^{t} k_{ij}(a_i b_j)$ Therefore, m is in the span of $a_i b_j$

□