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)**.**
$h \in \mathbb{Z}[x]$ irridicible $\Rightarrow$ 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

$$h \in \mathbb{Z}[x]$$
$$h = a_0 + a_1x + \cdots + a_nx^n$$

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 $\square$