Lecture 20: The content of a polynomial

Monday, May 21, 2018 10:27 AM

The goal of today's lecture is to prove the following:

Theorem. Suppose $f(x) \in \mathbb{Z}[x]$ is a primitive polynomial. If for some prime p, $c_p(f) \in \mathbb{Z}_p[x]$ is irreducible, and $\deg f = \deg c_p(f)$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Recall. For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \setminus \{0\}$, the content $\alpha(f)$ of f is $\gcd(a_0, a_1, \ldots, a_n)$.

- $\forall f \in \mathbb{Z}[x] \setminus \{0\}$, $\exists \overline{f}$: primitive, $f(x) = \alpha(f)\,\overline{f}(x)$.
- $c_p(f) = 0 \iff p \mid \alpha(f)$
- $\alpha(cf) = c\,\alpha(f) \quad \forall c \in \mathbb{Z}^+$.

Lemma. Suppose $f, g \in \mathbb{Z}[x]$ are primitive. Then fg is primitive.

pf. If not, $\exists$ p : prime s.t. $p \mid \alpha(fg)$. Hence $c_p(fg) = 0$. and so $c_p(f)\,c_p(g) = 0$. (*) Since p is prime, $\mathbb{Z}_p$ is an integral domain; and so $\mathbb{Z}_p[x]$ is an integral domain. Thus (*) implies either $c_p(f) = 0$ or $c_p(g)$. Therefore either $p \mid \alpha(f)$ or $p \mid \alpha(g)$ which contradicts the primitivity of f

and g. ∎

Gauss's lemma For $f, g \in \mathbb{Z}[x] \setminus \{0\}$, $\alpha(fg) = \alpha(f)\,\alpha(g)$.

Pf. $f(x) = \alpha(f)\,\bar{f}(x)$ where $\bar{f}$ is primitive. $\Rightarrow$

$g(x) = \alpha(g)\,\bar{g}(x)$ where $\bar{g}$ is primitive.

$f(x)\,g(x) = \alpha(f)\,\alpha(g)\,\bar{f}(x)\,\bar{g}(x)$. $\Rightarrow$

$\alpha(fg) = \alpha(\alpha(f)\alpha(g)\,\bar{f}\,\bar{g}) = \alpha(f)\,\alpha(g)\,\alpha(\bar{f}\,\bar{g})$. $\Rightarrow$

- $\bar{f}$, $\bar{g}$ primitive $\Rightarrow \bar{f}\bar{g}$ primitive $\Rightarrow \alpha(\bar{f}\bar{g}) = 1$

$$\alpha(fg) = \alpha(f)\,\alpha(g).$$ ∎

Going from $\mathbb{Q}$ to $\mathbb{Z}$.

Theorem. Suppose $f(x) \in \mathbb{Z}[x]$ is primitive and $f(x) = g_1(x)\,g_2(x)$ for some $g_1, g_2 \in \mathbb{Q}[x]$. Then $\exists\, a_1, a_2 \in \mathbb{Q}^\times$ s.t.

(1) $a_1 a_2 = 1$ (2) $\bar{g}_1(x) := a_1 g_1(x)$ and $\bar{g}_2(x) := a_2 g_2(x)$ are in $\mathbb{Z}[x]$ and primitive.

In particular, $f(x) = \bar{g}_1(x)\,\bar{g}_2(x)$ and $\deg \bar{g}_1 = \deg g_1$, $\deg \bar{g}_2 = \deg g_2$.

Monday, May 21, 2018 10:52 AM

Pf. Since $g_1, g_2 \in \mathbb{Q}[x]$, $\exists\ n_1, n_2 \in \mathbb{Z}^+$ s.t.

$\tilde{g}_1(x) = n_1 g_1(x)$ and $\tilde{g}_2(x) = n_2 g_2(x)$ are in $\mathbb{Z}[x]$.

(Take the common denominator of all the coefficients.)

So $n_1 n_2 f(x) = \tilde{g}_1(x)\,\tilde{g}_2(x)$. Therefore by Gauss's lemma,

$$n_1 n_2\, c(f) = c(\tilde{g}_1)\, c(\tilde{g}_2).$$

Since f is primitive, $n_1 n_2 = c(\tilde{g}_1)\, c(\tilde{g}_2)$. (I)

On the other hand, there are primitive polynomials $\bar{g}_1$ and $\bar{g}_2$ such that $\tilde{g}_1(x) = c(\tilde{g}_1)\,\bar{g}_1(x)$ and $\tilde{g}_2(x) = c(g_2)\,\bar{g}_2(x)$.

Hence $n_1 n_2 f(x) = \tilde{g}_1(x)\,\tilde{g}_2(x) = c(\tilde{g}_1)\,\bar{g}_1(x)\, c(\tilde{g}_2)\,\bar{g}_2(x)$

$$= c(\tilde{g}_1)\, c(\tilde{g}_2)\, \bar{g}_1(x)\,\bar{g}_2(x) \quad \text{(II)}$$

By (I) and (II), $n_1 n_2 f(x) = n_1 n_2\, \bar{g}_1(x)\,\bar{g}_2(x)$; and so

$$f(x) = \bar{g}_1(x)\,\bar{g}_2(x).$$

We also notice that $\bar{g}_i(x) = \dfrac{n_i}{c(\tilde{g}_i)}\, g_i(x)$; and so

$a_i := \dfrac{n_i}{c(\tilde{g}_i)}$ satisfies our claim. ∎

Lecture 20: Decompositions over Q and Z

Monday, May 21, 2018 11:06 AM

By induction on n, we can extend Gauss's lemma to product of m factors and consequently extend the previous result.

Gauss's lemma. For $f_1, \dots, f_m \in \mathbb{Z}[x]$, $\alpha(f_1 \cdot \dots \cdot f_m) = \alpha(f_1) \cdot \dots \cdot \alpha(f_m)$.

Pf. We proceed by induction on m; we have already prove the case of $m=2$; Induction step.

$$\alpha(f_1 \cdot f_2 \cdot \dots \cdot f_{m+1})$$

$$= \alpha(f_1 \cdot f_2 \cdot \dots \cdot f_{m-1} \cdot (f_m f_{m+1}))$$

$$\overset{\text{By the induction hypothesis}}{=} \alpha(f_1) \cdot \alpha(f_2) \cdot \dots \cdot \alpha(f_{m-1}) \cdot \alpha(f_m f_{m+1})$$

$$= \alpha(f_1) \cdot \alpha(f_2) \cdot \dots \cdot \alpha(f_{m-1}) \cdot \alpha(f_m) \cdot \alpha(f_{m+1}) \cdot \blacksquare$$

(The 2 factors case)

Theorem. Suppose $f(x) \in \mathbb{Z}[x]$ is primitive, and $f(x) = \prod_{i=1}^{n} g_i(x)$ for some $g_i(x) \in \mathbb{Q}[x]$. Then $\exists\, a_1, \dots, a_m \in \mathbb{Q}^\times$ s.t.

(1) $a_1 \cdot a_2 \cdot \dots \cdot a_m = 1$, (2) $\overline{g}_i(x) := a_i g_i(x)$ is in $\mathbb{Z}[x]$ and primitive for any i.

In particular, $f(x) = \prod_{i=1}^{m} \overline{g}_i(x)$ and $\deg g_i = \deg \overline{g}_i$.

Pf: Argument is identical to the case of $m=2$. $\exists\, n_i \in \mathbb{Z}^+$ s.t. $\tilde{g}_i(x) = n_i g_i(x)$. Then $\left(\prod_{i=1}^{m} n_i\right) f(x) = \prod_{i=1}^{m} \tilde{g}_i(x)$. Hence by

Lecture 20: Decompositions over Q and Z

Monday, May 21, 2018 11:24 AM

Gauss's lemma, $\left(\prod_{i=1}^{m} n_i\right) c(f) = \prod_{i=1}^{m} c(\tilde{g}_i)$. Hence

$$\prod_{i=1}^{m} n_i = \prod_{i=1}^{m} c(\tilde{g}_i). \quad \text{(I)}$$

On the other hand, $\exists\, \overline{g}_i(x) \in \mathbb{Z}[x]$ primitive s.t.

$$\tilde{g}_i(x) = c(\tilde{g}_i)\, \overline{g}_i(x); \text{ and so}$$

$$\left(\prod_{i=1}^{m} n_i\right) f(x) = \prod_{i=1}^{m} \tilde{g}_i(x) = \left(\prod_{i=1}^{m} c(\tilde{g}_i)\right) \cdot \prod_{i=1}^{m} \overline{g}_i(x). \quad \text{(II)}$$

Therefore by (I) and (II)

$$f(x) = \prod_{i=1}^{m} \overline{g}_i(x);$$

and we notice that

$$\overline{g}_i(x) = \frac{1}{c(\tilde{g}_i)}\, \tilde{g}_i(x) = \frac{n_i}{c(\tilde{g}_i)}\, g_i(x).$$

Hence $a_i := \dfrac{n_i}{c(\tilde{g}_i)}$ satisfies our claims. ∎

<u>Cor.</u> Suppose $f(x) \in \mathbb{Z}[x]$ is primitive and $\deg f \geq 1$. Then $f(x)$ is irreducible in $\mathbb{Z}[x] \iff f(x)$ is irreducible in $\mathbb{Q}[x]$.

<u>Pf.</u> ($\Longrightarrow$) If not, $f(x) = g_1(x)\, g_2(x)$ for some $g_1, g_2 \in \mathbb{Q}[x]$ and $\deg g_i \geq 1$. Then $\exists\, \overline{g}_i(x) \in \mathbb{Z}[x]$ s.t. $\deg \overline{g}_i = \deg g_i \geq 1$

and $f(x) = \overline{g}_1(x)\,\overline{g}_2(x)$, which implies f is not irreducible in $\mathbb{Z}[x]$.

($\Leftarrow$) Suppose f is not irreducible in $\mathbb{Z}[x]$. Since $\deg f \geq 1$, $f \neq 0$ and a unit. So $f(x) = g_1(x)\,g_2(x)$ for some $g_1, g_2 \in \mathbb{Z}[x] \setminus \{0\}$. As f is irred. in $\mathbb{Q}[x]$, either $\deg g_1 = 0$ or $\deg g_2 = 0$. W.L.O.G. let's assume $g_1(x) = c \in \mathbb{Z} \setminus \{0\}$. Then $c \mid \alpha(f) = 1$; and so $g_1(x) \in \{\pm 1\}$ which is a contradiction. ■

Pf of the mentioned irreducibility criterion.

Suppose to the contrary that $f(x)$ is not irreducible in $\mathbb{Q}[x]$. Since $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$, $\deg c_p(f) \geq 1$. Since $\deg f \geq \deg c_p(f)$, we have $\deg f \geq 1$. So not being irreducible implies $\exists\, g_1, g_2 \in \mathbb{Q}[x]$ s.t. $\deg g_i \geq 1$ and $f(x) = g_1(x)\,g_2(x)$. Hence $\exists\, \overline{g}_1, \overline{g}_2 \in \mathbb{Z}[x]$ primitive s.t. $\deg \overline{g}_i = \deg g_i \geq 1$ and $f(x) = \overline{g}_1(x)\,\overline{g}_2(x)$. (To be continued!)