Lecture 11: Gauss's lemma

Monday, August 21, 2017 8:24 AM

In the last lecture we proved the 1^{st} version of Gauss's lemma.

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

Based on the 1^{st} version, we prove the 2^{nd} version of Gauss's lemma (which is an extension of the 1^{st} version).

Gauss's lemma For any $f, g \in \mathbb{Z}[x] \setminus \{0\}$,

$$c(fg) = c(f)\, c(g).$$

Pf. $f = c(f)\, f_1$ and $g = c(g)\, g_1$, where f_1, g_1 are primitive polynomials. So by the previous lemma $f_1 g_1$ is primitive; this means $c(f_1 g_1) = 1$.

So $fg = c(f)\, c(g)\, f_1 g_1 \Rightarrow$

$$c(fg) = c(f)\, c(g)\, c(f_1 g_1)$$
$$= c(f)\, c(g). \qquad \blacksquare$$

Lecture 11: Reducibility over Z and Q

Monday, August 21, 2017 8:34 AM

Theorem. Suppose $f(x) \in \mathbb{Z}[x]$ has degree ≥ 1 and it is primitive. Then, if $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

In fact we prove the following slightly stronger tatement: if $f(x) = g(x) \cdot h(x)$ for $g, h \in \mathbb{Q}[x]$ of degree ≥ 1, then $\exists\, a_1, a_2 \in \mathbb{Q}$ s.t.

① $a_1 \cdot a_2 = 1$ and

② $a_1 g(x) \in \mathbb{Z}[x]$, $a_2 h(x) \in \mathbb{Z}[x]$.

In particular, $f(x) = g_2(x)\, h_2(x)$, $g_2(x), h_2(x) \in \mathbb{Z}[x]$ and $\deg g_2 = \deg g$, $\deg h_2 = \deg h$.

(g_1 and h_1 are auxiliary polynomials in the proof.)

Pf. Suppose to the contrary that $f(x) = g(x)\, h(x)$ for some $g, h \in \mathbb{Q}[x]$. Then $\exists\, r, s \in \mathbb{Z}^+$ s.t.

$g_1(x) = r\, g(x) \in \mathbb{Z}[x]$ and $h_1(x) = s\, h(x) \in \mathbb{Z}[x]$

(simply multiply by a common denominator of the coeff.)

Lecture 11: Irreducibility over Z and Q

Monday, August 21, 2017 12:58 PM

So $rs\, f(x) = g_1(x)\, h_1(x)$. Hence

$$rs\, c(f) = c(g_1)\, c(h_1)$$

Since f is primitive, $c(f) = 1$. So $rs = c(g_1)\, c(h_1)$.

Let g_2, h_2 be the primitive polynomials such that

$$g_1(x) = c(g_1)\, g_2(x) \quad \text{and} \quad h_1(x) = c(h_1)\, h_2(x).$$

Then $rs\, f(x) = c(g_1)\, c(h_1)\, g_2(x)\, h_2(x)$,

which implies $f(x) = g_2(x)\, h_2(x)$ as $rs = c(g_1)\, c(h_1)$.

Notice that $g_2(x) = \dfrac{r}{c(g_1)}\, g(x)$ and $h_2(x) = \dfrac{s}{c(h_1)}\, h(x)$. So

$\deg g_2 = \deg g$ and $\deg h_2 = \deg h$.

(let $a_1 = r/c(g_1)$ and $a_2 = s/c(h_1)$.) ∎

Theorem. Let p be a prime, $n \in \mathbb{Z}^{\geq 1}$, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

If $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.

Pf. If not, then $f(x) = g(x)\, h(x)$ for $g, h \in \mathbb{Q}[x]$ with $\deg \geq 1$.

Lecture 11: Irreducibility over Z_p and Q

Tuesday, August 22, 2017 10:37 PM

By the previous theorem $\exists\, g_2, h_2 \in \mathbb{Z}[x]$ s.t.

(1) $f(x) = g_2(x)\, h_2(x)$ (2) $\deg g_2, \deg h_2 \geq 1$.

Since $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is a ring homomorphism,

$c_p(f) = c_p(g_2)\, c_p(h_2)$.

As the leading coefficient of f is 1, the product of the leading coefficients of $g(x)$ and $h(x)$ is 1. Hence the leading coefficients of $g(x)$ and $h(x)$ are ± 1. Therefore $\deg c_p(g) = \deg g \geq 1$ and $\deg c_p(h) = \deg h \geq 1$.

So $c_p(f) = c_p(g)\, c_p(h)$ implies that f is reducible in $\mathbb{Z}_p[x]$, which is a contradiction. ■

Another important irreducibility criterion is Eisenstein Criterion.

Theorem (Eisenstein Criterion) Let p be a prime. Suppose

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

$p \nmid a_n$, $p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_0$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Lecture 11: Eisenstein Criterion

Wednesday, August 23, 2017 12:24 AM

Ex. Is $f(x)=x^4-2x^3+4x^2-6x+10$ irreducible in $\mathbb{Q}[x]$?

Answer. Yes; notice that $2\nmid 1$, $2\mid -2$, $2\mid 4$, $2\mid -6$, $2\mid 10$, and $4\nmid 10$. So by Eisenstein Criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Later we prove that in $F[x]$ any non-constant poly. can be written as a product of irreducible poly. in a unique way. A corollary of this fact is

Lemma. Let F be a field, $n\in\mathbb{Z}^+$. If $x^n=u(x)\,v(x)$ for $u(x), v(x)\in F[x]$, then for some $c\in F\setminus\{0\}$ and $k\in\mathbb{Z}^{\geq 0}$, $u(x)=c\,x^k$ and $v(x)=c^{-1}x^{n-k}$.

We will prove the above lemma later. Next using the above lemma, we will prove the Eisenstein Criterion. For an alternative and more basic approach look at your book.

Proof of the Eisenstein Criterion base on the above lemma.

Suppose to the contrary that $\exists\, g, h\in\mathbb{Q}[x]$ s.t.

Lecture 11: Eisenstein Criterion

Wednesday, August 23, 2017 12:49 AM

① $f(x) = g(x)h(x)$ ② $\deg g, \deg h \geq 1$.

So by a theorem that we proved earlier, $\exists g_2, h_2 \in \mathbb{Z}[x]$

s.t. $\deg g_2, \deg h_2 \geq 1$ and $f(x) = g_2(x)\, h_2(x)$.

Hence $c_p(f) = c_p(g_2)\, c_p(h_2)$.

Since $p \mid a_{n-1}, \dots, p \mid a_0$, $c_p(f) = c_p(a_n)\, x^n$.

Since $p \nmid a_n$ and $\mathbb{Z}_p$ is a field,

$$x^n = \underbrace{\left(c_p(a_n)^{-1}\, c_p(g_2)\right)}_{u(x)}\ \underbrace{c_p(h_2)}_{v(x)}, \quad u(x), v(x) \in \mathbb{Z}_p[x].$$

So by the previous lemma, $\exists\, c \in \mathbb{Z}_p \setminus \{0\}$, $k \in \mathbb{Z}^{\geq 0}$,

$$u(x) = c\, x^k \quad \text{and} \quad v(x) = c^{-1}\, x^{n-k}.$$

Thus $c_p(g_2) = c_p(a_n) \cdot c \cdot x^k$ and $c_p(h_2) = c^{-1} x^{n-k}$.

Notice that $\deg c_p(g_2) \leq \deg g_2$, $\deg c_p(h_2) \leq \deg h_2$,

and $\deg c_p(g_2) + \deg c_p(h_2) = n = \deg g_2 + \deg h_2$.

So $\deg c_p(g_2) = \deg g_2 \geq 1$ and $\deg c_p(h_2) = \deg h_2 \geq 1$.

Therefore the constant terms of g_2 and h_2 are divisible

Lecture 11: Eisenstein Criterion

Wednesday, August 23, 2017 11:43 PM

by p as the constant terms of $c_p(g_2)$ and $c_p(h_2)$ are zero.

Hence the constant term of $g_2(x)\, h_2(x)$ is divisible by p^2. (Notice that the constant term of g_2 is $g_2(0)$ and the constant term of h_2 is $h_2(0)$. So

$p \mid g_2(0)$ and $p \mid h_2(0)$, which implies $p^2 \mid g_2(0)\, h_2(0)$.)

This contradicts the assumption that p^2 does <u>not</u> divide the constant term of $f(x) = g_2(x)\, h_2(x)$. ∎

<u>Remark</u>. One way to prove the mentioned lemma without using "unique factorization" is proving it by induction on <u>n</u> and observing

$$
\begin{aligned}
x \mid u(x)\, v(x) &\iff 0 \text{ is a zero of } u(x)\, v(x) \\
&\iff u(0)\, v(0) = 0 \\
&\iff \text{either } u(0) = 0 \text{ or } v(0) = 0 \\
&\iff x \mid u(x) \text{ or } x \mid v(x).
\end{aligned}
$$

We will get back to this later.