Residue homomorphisms and Irreducibility

Sunday, August 20, 2017 11:23 PM

In the previous lecture we extended the residue map $\mathbb{Z} \to \mathbb{Z}_n$ to the ring of polynomials: $c_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$; and we used the residue homomorphism to show certain polynomials in $\mathbb{Z}[x]$ do not have a zero in $\mathbb{Q}$.

<u>Proposition</u>. Let p be a prime, and

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

Suppose $c_p(f)$ does not have a zero in $\mathbb{Z}_p$. Then f does not have a zero in $\mathbb{Q}$.

We proved the above proposition in two steps:

<u>Step 1.</u> Having a zero in $\mathbb{Q}$ $\Rightarrow$ Having a zero in $\mathbb{Z}$.

<u>Step 2.</u> Use the residue homomorphism to get a zero in $\mathbb{Z}_p$.

Next we will prove an <u>irreducibility criterion</u>.

<u>Theorem</u>. Let p be a prime, and

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

Suppose $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$. Then f is irreducible in $\mathbb{Q}[x]$.

An irreducibility criterion based on residue maps

Wednesday, August 23, 2017 10:08 PM

Similar to the proof of the proposition, we prove the contrapositive of this theorem; and it is done in two steps:

<u>Step 1.</u> Reducibility over $\mathbb{Q}$ implies reducibility over $\mathbb{Z}$ (and slightly stronger version).

<u>Step 2.</u> Using the residue homomorphism to get reducibility over $\mathbb{Z}_p$.

Before we start the proof, let's point out a few examples:

<u>Ex.</u>: • $2x$ is irreducible in $\mathbb{Q}[x]$. In fact any polynomial of degree 1 is irreducible in $\mathbb{Q}[x]$; Otherwise $\exists\, f, g \in \mathbb{Q}[x]$, $\deg f, \deg g \geq 1$ and $2x = f(x)\, g(x)$. So $\deg(2x) = 1 = \deg f + \deg g \geq 2$ which is a contradiction.

• $2x$ is reducible in $\mathbb{Z}[x]$ as $2x = (2)(x)$ and $2, x \notin U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$.

Towards Gauss's lemma

Wednesday, August 23, 2017 10:23 PM

So the big difference is that $2 \in U(\mathbb{Q}[x]) = \mathbb{Q}\setminus\{0\}$, but it is not a unit in $\mathbb{Z}[x]$.

<u>Ex.</u> $2x^2+4$ is irreducible in $\mathbb{Q}[x]$ as it is of degree 2 and does not have a zero in $\mathbb{Q}$.

- $2x^2+4 = (2)(x^2+2)$ and $2, x^2+2 \notin U(\mathbb{Z}[x]) = \{\pm 1\}$ imply that $2x^2+4$ is reducible in $\mathbb{Z}[x]$.

So the first thing we have to check, when we'd like to find out if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, is to find $\gcd(a_n, \dots, a_0)$, and see if it is 1 or not.

<u>Definition</u>. For $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, let $\alpha(f) = \gcd_{i=1}^{n}(a_i)$.
$(f \neq 0)$

<u>Ex.</u> $\alpha(2x) = 2$ • $\alpha(2x^2+4) = 2$ • $\alpha(x^3+3x+6) = 1$.

Let's recall three related properties of g.c.d.

<u>Recall</u> ① Let $d = \gcd(a_0, \dots, a_n)$. Then $\gcd\left(\frac{a_0}{d}, \dots, \frac{a_n}{d}\right)$

② If $p \mid a_0, p \mid a_1, \dots, p \mid a_n$, then $p \mid \gcd(a_0, \dots, a_n)$

Towards Gauss's lemma

Wednesday, August 23, 2017 10:39 PM

③ For $c \in \mathbb{Z}^+$, $\gcd(ca_0, ca_1, \dots, ca_n) = c \gcd(a_0, \dots, a_n)$.

Let's see what each one of the above properties implies about the defined α function.

- For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x] \setminus \{0\}$, let $\alpha(f) = d$.

Then $f(x) = d \underbrace{\left(\frac{a_n}{d} x^n + \dots + \frac{a_0}{d}\right)}_{f_1(x) \in \mathbb{Z}[x]}$ and

$$\alpha(f_1) = \gcd\left(\frac{a_n}{d}, \dots, \frac{a_0}{d}\right) = 1.$$

<u>Def.</u> $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ is called <u>primitive</u> if $\alpha(f) = 1$.

So for $f(x) \in \mathbb{Z}[x] \setminus \{0\}$, we have $f(x) = \alpha(f)\, f_1(x)$ where $f_1(x)$ is primitive.

- $c_p(f) = 0 \Leftrightarrow p \mid a_0, \dots, p \mid a_n \Leftrightarrow p \mid \gcd(a_0, \dots, a_n) \Leftrightarrow p \mid \alpha(f)$.

So $\quad c_p(f) = 0 \iff p \mid \alpha(f)$.

(Here $f(x) = a_n x^n + \dots + a_1 x + a_0$ as before.)

- For $c \in \mathbb{Z}^+$, $\alpha(cf) = \gcd(ca_0, \dots, ca_n) = c \gcd(a_0, \dots, a_n)$.

So $\quad \alpha(cf) = c\, \alpha(f)$.

Now let's see how these can help.

Gauss's lemma

Monday, August 21, 2017 8:24 AM

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

Pf. Suppose to the contrary that $\alpha(fg) \neq 1$. Then there is a prime p which divides $\alpha(fg)$. So $p \mid \alpha(fg)$, which implies $c_p(fg)=0$. Since $c_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is a ring homomorphism, $c_p(f)\, c_p(g)=0$.

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p[x]$ is an integral domain. Hence $c_p(f)c_p(g)=0$ implies that either $c_p(f)=0$ or $c_p(g)=0$. Therefore either $p \mid \alpha(f)$ or $p \mid \alpha(g)$, which contradicts the assumption that f and g are primitive. ∎

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

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

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

Gauss's lemma

Monday, August 21, 2017 8:34 AM

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

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

<u>Theorem.</u> 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 statement: if $f(x) = g(x) \cdot h(x)$ for $g, h \in \mathbb{Q}[x]$ of degree ≥ 1, then $\exists g_2, h_2 \in \mathbb{Z}[x]$ s.t.

① $f(x) = g_2(x) h_2(x)$

② $\deg g_2 = \deg g$ and $\deg h_2 = \deg h$.

h_1 and g_1 will be some auxi. poly. in the proof.

<u>Pf.</u> 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.)

It is useful to think about $\left(\frac{3x}{2}\right)\left(\frac{2x+2}{3}\right)$

Irreducibility over Z implies irreducibility over Q

Monday, August 21, 2017 12:58 PM

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

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

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

Let g_2, h_2 be the primitive polynomials such that

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

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

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

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

$\underline{\text{Theorem.}}$ 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 $\mathbb{Q}[x]$.

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

Irreducibility over Z_p implies irreducibility over 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 $\mathbb{Q}[x]$.

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.

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

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.

Definition of an ideal

Wednesday, August 23, 2017 11:53 PM

Def. Let R be a ring. A subset I of R is called an ideal if

① $\forall x, y \in I$, $x - y \in I$ (additive subgp)

② $\forall r \in R$, $x \in I$, $rx, xr \in I$.

A historical note. In order to solve Fermat's last conjecture, which says the only integer solutions of $x^n + y^n = z^n$ are the trivial ones if $n \geq 3$, Kummer studied rings of the form $\mathbb{Z}[\zeta_n]$ where ζ_n is an n^{th} root of unity. In such rings an element does not necessarily of unique factorization into "prime" factors; but Kummer showed in appropriate sense ideals do have such a unique factorization; and he called them ideal numbers Later Dedekind, Hilbert, and Noether developed the theory of ideals for general rings.

(In one of the exercises you are working with $\mathbb{Z}[\omega]$, where ω is a 3^{rd} root of unity.)