MA542 Lecture

Timothy Kohl

Boston University

February 10, 2025

Eisenstein's Criterion

Another important irreducibility test is this one due to Eisenstein in 1850.

Theorem

Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ and if there is a prime p such that $p \nmid a_n$ but $p \mid a_{n-1}, \ldots, p \mid a_0$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof.

Recall that $f(x)$ irreducible over $\mathbb{Q}$ implies $f(x)$ is irreducible over $\mathbb{Z}$. So say $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbb{Z}[x]$ where $1 \leq deg(g(x)) < n$ and $1 \leq deg(h(x)) < n$.

$$g(x) = b_r x^r + \cdots + b_0$$
$$h(x) = c_s x^s + \cdots + c_0$$

Since $p \mid a_0$ but $p^2 \nmid a_0$ then $p|b_0 c_0$ which means $p \mid b_0$ or $p \mid c_0$ *but not both.*
So say $p \mid b_0$ and $p \nmid c_0$. Since $p \nmid a_n = b_r c_s$ then $p \nmid b_r$ so there is a least integer t such that $p \nmid b_t$.
We have $a_t = b_t c_0 + \cdots + b_0 c_t$ and by assumption $p \mid a_t$ and by choice of t, $p \mid b_{t-1}, \ldots, b_0$ ergo $p \mid b_t c_0$ but this is impossible since $p \nmid b_t$ and $p \nmid c_0$. $\square$

With this theorem, we can manufacture examples of irreducible polynomials (of any degree) at will.

For example: $x^5 - 9x^4 + 3x^2 - 12$ satisfies the conditions with $p = 3$ since $p \nmid 1$, $p \mid -9$, $p \mid 3$, $p \mid 12$, but $p^2 \nmid 12$.

What's also useful about Eisenstein's criterion is that it is easy to make the examples have as large a degree as desired, since the irreducibility is deduced in terms of the coefficients.

High degree examples aren't as easy to construct/verify with the Mod p irreducibility test we discussed earlier.

An important class of examples where the Eisenstein criteria is used are the cyclotomic polynomials

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

which are ubiquitous throughout number theory etc.

The term 'cyclotomic' relates to the act of splitting a circle into (in this case p equal sized arcs), each of which corresponds to a sector of the circle of angle $\frac{2\pi}{p}$.

The reason for this connection is due to the roots of the polynomial $x^p - 1$

A root of $x^p - 1$ is a number whose p^{th} power is 1, and one may show that the p (distinct!) roots are ζ_p^i where $\zeta_p = e^{i\frac{2\pi}{p}}$ is primitive p^{th} root of unity.

There is nice visual for this we can give which shows where the term cyclotomic.

(N.B. The polynomial $x^p - 1$ is actually *not* irreducible since $x = 1$ is a root, and therefore $x^p - 1$ is divisible by $x - 1$, but if we factor out this root, then the result is $\Phi_p(x)$ which is irreducible as well shall demonstrate.)

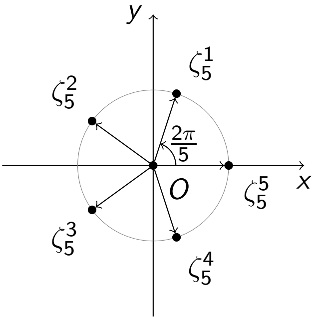
Recall from calculus 2 that $e^{it} = cos(t) + isin(t)$ and so $e^{i\frac{2\pi}{p}} = cos(\frac{2\pi}{p}) + isin(\frac{2\pi}{p})$ and so $\left(e^{i\frac{2\pi}{p}}\right)^k = e^{ik\frac{2\pi}{p}} = cos(k\frac{2\pi}{p}) + isin(k\frac{2\pi}{p})$.

As such $(\zeta_p^k)^p = \left(e^{ik\frac{2\pi}{p}}\right)^p = e^{ik2\pi} = cos(k2\pi) + isin(k2\pi) = 1$ for each k from 0 to $p-1$.

And one can check that each ζ_p^k is distinct as k varies from 0 to $p-1$. Note also, $\zeta_p^p = \zeta_p^0 = 1$.

These points all lie on the unit circle $x^2 + y^2 = 1$ and equidistributed at angles $k\frac{2\pi}{p}$.

So for $p = 5$ we have 5 roots of unity distributed around the circle at multiples of $2\pi/5$ (72 degrees).



and we see that these arcs subdivide the circle evenly.

Again, note $\zeta_5^5 = \zeta_5^0 = 1$ of course.

In order to prove the irreducibility of $\Phi_p(x)$ we actually need a small but important observation about Binomial coefficients.

If p is a prime then $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and for $k = 0$ and $k = p$ we have $\binom{p}{0} = 1$ and $\binom{p}{p} = 1$.

For $0 < k < p$ we observe that, since p is prime, p does **not** divide $k!$, nor does it divide $(p-k)!$, but that obviously p divides $p!$.

As such p divides $\binom{p}{k}$ for any $0 < k < p$.

We also need to recall the basic binomial theorem, namely:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

where, in a moment, our 'n' will be a prime p.

We still wish to show the following.

Proposition

For each prime p, Φ_p is irreducible.

Proof.

Let

$$\begin{aligned} f(x) &= \Phi_p(x+1) \\ &= \frac{(x+1)^p - 1}{(x+1)-1} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1} \end{aligned}$$

and so every coefficient of $f(x)$ (except that of x^{p-1}) is divisible by p, but $p^2 \nmid \binom{p}{p-1}$ and therefore by Eisenstein's criterion, $f(x)$ is irreducible. But $f(x)$ irreducible certainly implies that $\Phi_p(x)$ is irreducible since if $\Phi_p(x) = g(x)h(x)$ then $f(x) = g(x+1)h(x+1)$. $\square$

For $p = 3$ for example, we get that ζ_3 is one of the roots of $\Phi_3(x) = x^2 + x + 1$.

By the quadratic formula the two (complex) roots are

$$\frac{-1 \pm \sqrt{-3}}{2}$$

and one can show that $\zeta_3 = \dfrac{-1 + \sqrt{-3}}{2}$ since $sin(\frac{2\pi}{3}) > 0$.

And as with i giving rise to $\mathbb{Q}(i)$ one can also contemplate the field obtained by 'adjoining' ζ_3 to $\mathbb{Q}$.

In $\mathbb{Q}(\zeta_3) = \{a + b\zeta_3 \mid a, b \in \mathbb{Q}\}$ one adds elements by the rule $(a + b\zeta_3) + (c + d\zeta_3) = (a + c) + (b + d)\zeta_3$ but the multiplication requires a bit of analysis:

$$(a + b\zeta_3)(c + d\zeta_3) = (ac + bd\zeta_3^2) + (ad + bc)\zeta_3$$

so it's not clear that this operation is closed.

But we can observe that ζ_3 is a root of $x^2 + x + 1$ which means $\zeta_3^2 + \zeta_3 + 1 = 0$ so that $\zeta_3^2 = -\zeta_3 - 1$ which means

$$(ac + bd\zeta_3^2) + (ad + bc)\zeta_3 = (ad - bd) + (ad + bc - bd)\zeta_3$$

and also the other properties hold for a ring, and one can prove (exercise) that this is a field too.

Uniqueness of Factorization in $F[x]$

We've discussed irreducibility, now let's discuss the nature of factorization in $F[x]$.

We've already seen that in $F[x]$ one has a division algorithm whose statement (and as we'll see, implications) parallels the same statement in $\mathbb{Z}$.

Indeed in $\mathbb{Z}$ we have theorems about how integers factor into products of prime numbers which are 'indivisible' and we shall develop a similar sort of arithmetic in the ring $F[x]$.

In the natural numbers, one of the principle properties of prime numbers is not just that they have no factors except 1 and themselves, but that if $p \mid rs$ then $p \mid r$ and/or $p \mid s$.

In $F[x]$ the irreducible polynomials play a similar role.

Theorem

Let $p(x) \in F[x]$ be irreducible. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$ then either $p(x)$ divides $r(x)$ and/or $p(x)$ divides $s(x)$.

Proof.

Later... □

Corollary

If $p(x) \in F[x]$ is irreducible and divides a product $r_1(x)r_2(x)\cdots r_n(x)$ for $r_i(x) \in F[x]$ then $p(x)$ divides at least one $r_i(x)$.

Proof.

The statement is (trivially) true if $n = 1$. And for an arbitrary $r_1(x)r_2(x)\cdots r_n(x)$ if $p(x)$ divides

$$r_1(x)r_2(x)\cdots r_n(x) = r_1(x)\big(r_2(x)\cdots r_n(x)\big)$$

then by the theorem it either divides $r_1(x)$ or it divides $r_2(x)\cdots r_n(x)$ and if it divides $r_2(x)\cdots r_n(x)$ then it's dividing a product of $n-1$ polynomials so we may inductively assume the result is true,i.e. that $p(x)$ divides one of the $r_2(x),\ldots,r_n(x)$. $\square$

Theorem

If F is a field then every non-constant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducibles where the irreducibles are unique except for order and for unit, (i.e. non-zero constant) factors in F. That is if $f(x) = p_1 p_2 \cdots p_r = q_1 q_2 \ldots q_s$ for p_i and q_j irreducibles, then $r = s$ (the same number of irreducibles) and we may assume that $q_i = u_i p_i$ for u_i units of F (i.e. a non-zero number).

We won't give the proof here as this result is a special case of a more general statement about divisibility in integral domains. We will prove this more general result later.

For a perspective on this, you can look at the same situation for $\mathbb{Z}$.

For example $6 = 2 \cdot 3$ but also $6 = (-2)(-3) = (-1)2 \cdot (-1)3$ and similarly $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$ but also $48 = (-2) \cdot 2 \cdot (-2) \cdot (-2) \cdot (-3)$.

By the way since $U(\mathbb{Z})$ the only 'unit multiples' of an irreducible are '$\pm$(irreducible)' and in fact, in $\mathbb{Z}$ the only irreducibles are $\pm p$ for p a prime.