Modern Algebra Lecture Notes: Rings and fields set 5 (Revision 4)

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 17, 2010

Theorem 19: the Mod p irreducibility test

Statement

Let p be a prime and $f(x) \in \mathbb{Z}[x]$ is such that $\theta_p(f(x))$ has the same degree and is irreducible in $\mathbb{Z}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Notes

(1) There is a good fast method for factoring a polynomial over any $\mathbb{Z}_p$: Berlekamp's algorithm.

(2) This can be used as an irreducibility test of general utility: try factoring for a number of primes until there is only one factor.

(3) Berlekamp can be used to factor over $\mathbb{Z}$ either by choosing a very large prime, or by "lifting" a factorization mod p to higher powers of p, until the integer coefficients "appear".

Examples

(1) In $\mathbb{Z}[x]$ let $f(x) = \left(x^2+1\right)\left(x^3+x+3\right)^2$. Then this same factorization works modulo p for every prime $p > 3$ but over $\mathbb{Z}_3$, $f(x) = x^2(x^2+1)^3$.

(2) x^4+2 is irreducible over $\mathbb{Z}$ and $\mathbb{Z}_5$, but over $\mathbb{Z}_7$ we have $f(x) = (x^2+x+4)(x^2+6x+4)$ and over $\mathbb{Z}_3$, $f(x) = (x+1)(x+2)(x^2+1)$, where each of the factors is irreducible.

(3) $2+x^3+2x^7+x^{10}$ is reducible but changing x^3 to $2x^3$ makes it irreducible.

Statement of Theorem 19:

Let p be a prime and $f(x) \in \mathbb{Z}[x]$ is such that $\theta_p(f(x))$ has the same degree and is irreducible in $\mathbb{Z}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Proof

Assume, to get a contradiction, $f(x) = g(x).h(x)$ over $\mathbb{Z}$ where each of $g(x)$ and $h(x)$ has degree less than that of $f(x)$ and greater than 0.

Then $\theta_p(f(x)) = \theta_p(g(x)).\theta_p(h(x))$. Then $\deg \theta_p(g(x)) = \deg g(x)$ and $\deg \theta_p(g(x)) = \deg g(x)$, giving a non-trivial factorization of $\theta_p(f(x))$, which is impossible.

Therefore $f(x)$ is irreducible.$\square$

Theorem 20: Eisenstein's irreducibility test

Statement

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ have positive degree and suppose some prime $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Proof

To get a contradiction let $f(x) = g(x).h(x)$ with $g(x) = b_0 + \cdots + b_mx^m$ and $h(x) = c_0 + \cdots + c_lx^l$. Then $a_0 = b_0c_0$ and $a_n = b_mc_l$.

Since $p \mid a_0$ we have $p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$ p divides one of these and not the other. Suppose $p \mid b_0$ and $p \nmid c_0$.

Since $p \nmid a_n$ we have $p \nmid b_m$ so we may assume $p \mid b_0,\ b_1,\ b_2, \ldots, b_{t-1}$ but $p \nmid b_t$. But $a_t = b_tc_0 + b_{t-1}c_1 + \cdots + b_0c_t$ and we are given $p \mid a_t$.

Therefore $p \mid b_tc_0$ so $p \mid b_t$, which is false. Therefore $f(x)$ is irreducible. $\square$

Example

$12 + 4x + 21x^2 - 6x^3 + 3x^4 + x^7$ is irreducible over $\mathbb{Z}$ since we can take $p = 3$.

Theorem 21: $f(x)$ irreducible implies $F[x]/\langle f(x)\rangle$ is a field

Proof

Let A be the ideal $\langle f(x)\rangle$ and B and ideal with $A \subset B \subset F[x]$.

Since $F[x]$ is a principal ideal domain we must have $B = \langle g(x)\rangle$ for some polynomial $g(x) \in F[x]$. But $f(x) \in B$ so there is a polynomial $h(x)$ such that $f(x) = h(x)g(x)$.

But we are given $f(x)$ is irreducible, and we may assume non-zero. Hence one of $h(x)$ or $g(x)$ must be a non-zero constant polynomial (a unit of $F[x]$). If both are constant, $B = F[x]$

If both are constant, $B = F[x]$. If only one is constant, $B = A$. Therefore A is a maximal ideal.

Hence $F[x]/A = F[x]/\langle f(x)\rangle$, by Theorem 5 (set 1), is a field. $\square$

Example: Find the inverse of $[x+2]$ in $\mathbb{Q}[x]/\langle x^2+1\rangle$: let $a, b \in \mathbb{Q}$ be such that $[x+2][ax+b] = [1]$. Then $LHS = [ax^2 + x(2a+b) + 2b]$ or $[a(x^2+1) - a + x(2a+b) + 2b]$ which is $[x(2a+b) + 2b - a]$ so we want $2a+b = 0,\ 2b-a = 1$ or $a = -1/5,\ b = 2/5$, giving the inverse $[(-x+2)/5]$.

Theorem 22: irreducible polynomials over a field are like prime numbers

Statement

Let F be a field and let $f(x)$ in $F[x]$ be irreducible. Then if $f(x) \mid g(x).h(x)$ in $F[x]$ we must have $f(x) \mid g(x)$ or $f(x) \mid h(x)$.

Proof

Since $f(x)$ is irreducible, $F[x]/\langle f(x)\rangle$ is a field, hence an integral domain.

Since $f(x) \mid g(x).h(x)$ we have $g(x).h(x) \in \langle f(x)\rangle$. Thus $[g(x)][h(x)] = [g(x).h(x)] = [0]$ in $F[x]/\langle f(x)\rangle$.

Hence $[g(x)] = [0]$ or $[h(x)] = [0]$. But this means $g(x) \in \langle f(x)\rangle$ or $h(x) \in \langle f(x)\rangle$.

In other words $f(x) \mid g(x)$ or $f(x) \mid h(x)$.$\square$

Theorem 23: Unique factorization holds in $\mathbb{Z}[x]$

Statement

If $f(x) \in \mathbb{Z}[x]$ has positive degree then it can be factored, up to order, uniquely into the product of an integer and a set of polynomials of positive degree, irreducible over $\mathbb{Z}$.

Proof

The integer in the statement is the content of $f(x)$ so first take it out as a factor, $c(f(x)).f_1(x)$ where $f_1(x)$ is primitive and has the same degree as $f(x)$.

Let $n = \deg f_1(x)$. If $n = 1$ the polynomial is irreducible and we are done. So assume the result is true for every primitive polynomial of degree up to some given natural number $n > 1$.

If $f_1(x)$ is irreducible we are also done. So assume $f_1(x)$ has degree n and $f_1(x) = g(x).h(x)$ is a non-trivial factorization. Of course $g(x)$, $h(x)$ must be primitive, by Gauss' Lemma. Since their degrees are less than n they will have a factorization into irreducible polynomials by the inductive assumption.

Combining these factorizations gives a factorization of $f_1(x)$ into irreducibles and hence of $f(x)$.

Theorem 23: Uniqueness of the factors

The leading integer is unique because it is the content of $f(x)$, so we can assume $f(x)$ is primitive.

Suppose it factors into irreducibles as $f(x) = g_1(x).g_2(x)\cdots g_n(x)$ and $f(x) = h_1(x)\cdots h_m(x)$.

Then each $h_j(x) \mid f(x)$ which implies, using Theorem 22 many times, for some i, $h_j(x) \mid g_i(x)$.

But this means $h_j(x).k(x) = g_i(x)$ for some $k(x) \in \mathbb{Z}[x]$ and $g_i(x)$ is irreducible. Thus $k(x) = \pm 1$, a unit in $\mathbb{Z}$.

So for each j there is an i with $h_j(x) = \pm g_i(x)$. Similarly for each i there is a corresponding j. **If each of the $g_i(x)$'s and $h_j(x)$ are distinct respectively**, renumber to make the $i's$ and $j's$ identical so $m = n$ and

$$f(x) = g_1(x)\cdots g_n(x) = \pm h_1(x)\cdots h_n(x),\ g_i(x) = \pm h_i(x),\ 1 \leq i \leq m.$$

Uniqueness of the factors continued

If some factors have multiplicity we can write

$$f(x) = g_1(x)^{\alpha_1} \cdots g_m(x)^{\alpha_m} = \pm g_1(x)^{\beta_1} \cdots g_m(x)^{\beta_m}$$

for some $\alpha_i,\ \beta_i \in \mathbb{N}$, and where the $g_i(x)$ are now all distinct.

But if $\alpha_1 \neq \beta_1$, say $\alpha_1 > \beta_1$, we can cancel all the β_1 copies of $g_1(x)$ from the right hand side leaving $g_1(x) \mid g_2(x)^{\beta_2} \cdots g_m(x)^{\beta_m}$, so $g_1(x) \mid g_j(x)$ for some $j > 1$, which is impossible, since the $g_i(x)$ are all irreducible.

Hence $\alpha_1 = \beta_1$ and we can cancel all of the powers of $g_1(x)$ from each side. Then attend to $g_2(x)$ in the same manner leading to $\alpha_2 = \beta_2$ and so on, getting eventually $\alpha_i = \beta_i$ for all i, $1 \leq i \leq m$. Hence the factorization is unique up to ± 1.$\square$