Irreducible Polynomial

Let *D* be an integral domain.

A polynomial  from  that is neither the zero polynomial nor a unit in , such that whenever  is expressed as a product , with  and  from , then  or  is a unit in .

Reducible Polynomial

Let *D* be an integral domain.

A nonzero, nonunit polynomial from  that is not irreducible.

Reducibility Test for Degrees 2 and 3

Let *F* be a field. If  and  or 3, then  is reducible over *F* if and only if  has a zero in *F*.

Content of a polynomial

Polynomial coefficients are integer.

The greatest common divisor of the polynomial coefficients.

Primitive Polynomial

A polynomial in  with content 1.

Gauss’s Lemma

The product of two primitive polynomials is primitive.

Over *Q* Implies Over *Z*

Let . If  is reducible over *Q*, then it is reducible over *Z*.

Mod *p* Irreducibility Test

Let *p* be a prime and suppose that  with . Let  be the polynomial in  obtained from  by reducing all of its coefficients . If  is irreducible over  and , then  is irreducible over *Q*.

Eisenstein’s Criterion

Let . If there is a prime *p* such that *p* divides every coefficient of  except for  and  does not divide , then  is irreducible over *Q*.

Irreducibility of *p-*th Cyclotomic Polynomial

For any prime *p*, the *p*-th cyclotomic polynomial

 

is irreducible over *Q*.

 Is Irreducible if and Only if  is Maximal

Let *F* be a field and  . Then  is a maximal ideal in  if and only if  is irreducible over *F*.

 Is a Field

Let *F* be a field and  an irreducible polynomial over *F*. Then  is a field.

 Implies  or 

Let *F* be a field and let . If  is irreducible over *F* and , then or .

Unique Factorization in 

Every polynomial in  that is not the zero polynomial or a unit in  can be written in the form , where the ’s are irreducible polynomials of degree 0, and the ’s are irreducible polynomials of positive degree. Furthermore, if , where the ’s are irreducible polynomials of degree 0, and the ’s are irreducible polynomials of positive degree, then , and, after renumbering the *c*’s and *q(x)*’s, we have  for  and  for .