Course 311: Abstract Algebra
Academic year 2007-08
Chapter 2: Rings and Polynomials

D. R. Wilkins

Contents

2 Rings and Polynomials

2.1 Rings, Integral Domains and Fields

Definition A *ring* consists of a set R on which are defined operations of *addition* and *multiplication* satisfying the following axioms:

- $x+y = y+x$ for all elements x and y of R (i.e., addition is *commutative*);
- $(x+y)+z = x+(y+z)$ for all elements x, y and z of R (i.e., addition is *associative*);
- there exists an an element 0 of R (known as the *zero element*) with the property that $x+0 = x$ for all elements x of R;
- given any element x of R, there exists an element $-x$ of R with the property that $x+(-x) = 0$;
- $x(yz) = (xy)z$ for all elements x, y and z of R (i.e., multiplication is *associative*);
- $x(y+z) = xy+xz$ and $(x+y)z = xz+yz$ for all elements x, y and z of R (the *Distributive Law*).

Lemma 2.1 *Let R be a ring. Then $x0 = 0$ and $0x = 0$ for all elements x of R.*

Proof The zero element 0 of R satisfies $0+0 = 0$. Using the Distributive Law, we deduce that $x0+x0 = x(0+0) = x0$ and $0x+0x = (0+0)x = 0x$. Thus if we add $-(x0)$ to both sides of the identity $x0+x0 = x0$ we see that $x0 = 0$. Similarly if we add $-(0x)$ to both sides of the identity $0x+0x = 0x$ we see that $0x = 0$. ∎

Lemma 2.2 *Let R be a ring. Then $(-x)y = -(xy)$ and $x(-y) = -(xy)$ for all elements x and y of R.*

Proof It follows from the Distributive Law that $xy+(-x)y = (x+(-x))y = 0y = 0$ and $xy+x(-y) = x(y+(-y)) = x0 = 0$. Therefore $(-x)y = -(xy)$ and $x(-y) = -(xy)$. ∎

A subset S of a ring R is said to be a *subring* of R if $0 \in S$, $a+b \in S$, $-a \in S$ and $ab \in S$ for all $a, b \in S$.

A ring R is said to be *commutative* if $xy = yx$ for all $x, y \in R$. Not every ring is commutative: an example of a non-commutative ring is provided by the ring of $n \times n$ matrices with real or complex coefficients when $n > 1$.

A ring R is said to be *unital* if it possesses a (necessarily unique) non-zero multiplicative identity element 1 satisfying $1x = x = x1$ for all $x \in R$.

Definition A unital commutative ring R is said to be an *integral domain* if the product of any two non-zero elements of R is itself non-zero.

Definition A *field* consists of a set K on which are defined operations of *addition* and *multiplication* satisfying the following axioms:

- $x+y = y+x$ for all elements x and y of K (i.e., addition is *commutative*);
- $(x+y)+z = x+(y+z)$ for all elements x, y and z of K (i.e., addition is *associative*);
- there exists an an element 0 of K known as the *zero element* with the property that $x + 0 = x$ for all elements x of K;
- given any element x of K, there exists an element $-x$ of K with the property that $x + (-x) = 0$;
- $xy = yx$ for all elements x and y of K (i.e., multiplication is *commutative*);
- $x(yz) = (xy)z$ for all elements x, y and z of K (i.e., multiplication is *associative*);
- there exists a non-zero element 1 of K with the property that $1x = x$ for all elements x of K;
- given any non-zero element x of K, there exists an element x^{-1} of K with the property that $xx^{-1} = 1$;
- $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all elements x, y and z of K (the *Distributive Law*).

An examination of the relevant definitions shows that a unital commutative ring R is a field if and only if, given any non-zero element x of R, there exists an element x^{-1} of R such that $xx^{-1} = 1$. Moreover a ring R is a field if and only if the set of non-zero elements of R is an Abelian group with respect to the operation of multiplication.

Lemma 2.3 *A field is an integral domain.*

Proof A field is a unital commutative ring. Let x and y be non-zero elements of a field K. Then there exist elements x^{-1} and y^{-1} of K such that $xx^{-1} = 1$ and $yy^{-1} = 1$. Then $xyy^{-1}x^{-1} = 1$. It follows that $xy \neq 0$, since $0(y^{-1}x^{-1}) = 0$ and $1 \neq 0$. ∎

The set $\mathbb{Z}$ of integers is an integral domain with respect to the usual operations of addition and multiplication. The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of rational, real and complex numbers are fields.

2.2 Ideals

Definition Let R be a ring. A subset I of R is said to be an *ideal* of R if $0 \in I$, $a + b \in I$, $-a \in I$, $ra \in I$ and $ar \in I$ for all $a, b \in I$ and $r \in R$. An ideal I of R is said to be a *proper ideal* of R if $I \neq R$.

Note that an ideal I of a unital ring R is proper if and only if $1 \notin I$. Indeed if $1 \in I$ then $r \in I$ for all $r \in R$, since $r = r1$.

Lemma 2.4 *A unital commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.*

Proof Suppose that R is a field. Let I be a non-zero ideal of R. Then there exists $x \in I$ satisfying $x \neq 0$. Moreover there exists $x^{-1} \in R$ satisfying $xx^{-1} = 1 = x^{-1}x$. Therefore $1 \in I$, and hence $I = R$. Thus the only ideals of R are $\{0\}$ and R.

Conversely, suppose that R is a unital commutative ring with the property that the only ideals of R are $\{0\}$ and R. Let x be a non-zero element of R, and let Rx denote the subset of R consisting of all elements of R that are of the form rx for some $r \in R$. It is easy to verify that Rx is an ideal of R. (In order to show that $yr \in Rx$ for all $y \in Rx$ and $r \in R$, one must use the fact that the ring R is commutative.) Moreover $Rx \neq \{0\}$, since $x \in Rx$. We deduce that $Rx = R$. Therefore $1 \in Rx$, and hence there exists some element x^{-1} of R satisfying $x^{-1}x = 1$. This shows that R is a field, as required. ∎

The intersection of any collection of ideals of a ring R is itself an ideal of R. For if a and b are elements of R that belong to all the ideals in the collection, then the same is true of 0, $a + b$, $-a$, ra and ar for all $r \in R$.

Let X be a subset of the ring R. The ideal of R *generated* by X is defined to be the intersection of all the ideals of R that contain the set X. Note that this ideal is well-defined and is the smallest ideal of R containing the set X (i.e., it is contained in every other ideal that contains the set X).

We denote by $(f_1, f_2, \ldots, f_k)$ the ideal of R generated by any finite subset $\{f_1, f_2, \ldots, f_k\}$ of R. We say that an ideal I of the ring R is *finitely generated* if there exists a finite subset of I which generates the ideal I.

Lemma 2.5 *Let R be a unital commutative ring, and let X be a subset of R. Then the ideal generated by X coincides with the set of all elements of R that can be expressed as a finite sum of the form $r_1x_1 + r_2x_2 + \cdots + r_kx_k$, where $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$.*

Proof Let I be the subset of R consisting of all these finite sums. If J is any ideal of R which contains the set X then J must contain each of these finite sums, and thus $I \subset J$. Let a and b be elements of I. It follows immediately from the definition of I that $0 \in I$, $a + b \in I$, $-a \in I$, and $ra \in I$ for all $r \in R$. Also $ar = ra$, since R is commutative, and thus $ar \in I$. Thus I is an ideal of R. Moreover $X \subset I$, since the ring R is unital and $x = 1x$ for all $x \in X$. Thus I is the smallest ideal of R containing the set X, as required. ∎

Each integer n generates an ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers. This ideal consists of those integers that are divisible by n.

Lemma 2.6 *Every ideal of the ring $\mathbb{Z}$ of integers is generated by some non-negative integer n.*

Proof The zero ideal is of the required form with $n = 0$. Let I be some non-zero ideal of $\mathbb{Z}$. Then I contains at least one strictly positive integer (since $-m \in I$ for all $m \in I$). Let n be the smallest strictly positive integer belonging to I. If $j \in I$ then we can write $j = qn + r$ for some integers q and r with $0 \leq r < n$. Now $r \in I$, since $r = j - qn$, $j \in I$ and $qn \in I$. But $0 \leq r < n$, and n is by definition the smallest strictly positive integer belonging to I. We conclude therefore that $r = 0$, and thus $j = qn$. This shows that $I = n\mathbb{Z}$, as required. ∎

2.3 Quotient Rings and Homomorphisms

Let R be a ring and let I be an ideal of R. If we regard R as an Abelian group with respect to the operation of addition, then the ideal I is a (normal) subgroup of R, and we can therefore form a corresponding quotient group R/I whose elements are the cosets of I in R. Thus an element of R/I is of the form $I + x$ for some $x \in R$, and $I + x = I + x'$ if and only if $x - x' \in I$. If

x, x', y and y' are elements of R satisfying $I + x = I + x'$ and $I + y = I + y'$ then

$$\begin{aligned}(x + y) - (x' + y') &= (x - x') + (y - y'),\\ xy - x'y' &= xy - xy' + xy' - x'y' = x(y - y') + (x - x')y'.\end{aligned}$$

But $x - x'$ and $y - y'$ belong to I, and also $x(y - y')$ and $(x - x')y'$ belong to I, since I is an ideal. It follows that $(x + y) - (x' + y')$ and $xy - x'y'$ both belong to I, and thus $I + x + y = I + x' + y'$ and $I + xy = I + x'y'$. Therefore the quotient group R/I admits well-defined operations of addition and multiplication, given by

$$(I + x) + (I + y) = I + x + y, \qquad (I + x)(I + y) = I + xy$$

for all $I + x \in R/I$ and $I + y \in R/I$. One can readily verify that R/I is a ring with respect to these operations. We refer to the ring R/I as the *quotient* of the ring R by the ideal I.

Example Let n be an integer satisfying $n > 1$. The quotient $\mathbb{Z}/n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers by the ideal $n\mathbb{Z}$ generated by n is the ring of congruence classes of integers modulo n. This ring has n elements, and is a field if and only if n is a prime number.

Definition A function $\varphi: R \to S$ from a ring R to a ring S is said to be a *homomorphism* (or *ring homomorphism*) if and only if $\varphi(x+y) = \varphi(x)+\varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in R$. If in addition the rings R and S are unital then a homomorphism $\varphi: R \to S$ is said to be *unital* if $\varphi(1) = 1$ (i.e., φ maps the identity element of R onto that of S).

Let R and S be rings, and let $\varphi: R \to S$ be a ring homomorphism. Then the kernel $\ker \varphi$ of the homomorphism φ is an ideal of R, where

$$\ker \varphi = \{x \in R : \varphi(x) = 0\}.$$

The image $\varphi(R)$ of the homomorphism is a subring of S; however it is not in general an ideal of S.

An ideal I of a ring R is the kernel of the quotient homomorphism that sends $x \in R$ to the coset $I + x$.

Definition An isomorphism $\varphi: R \to S$ between rings R and S is a homomorphism that is also a bijection between R and S. The inverse of an isomorphism is itself an isomorphism. Two rings are said to be *isomorphic* if there is an isomorphism between them.

The verification of the following result is a straightforward exercise.

Proposition 2.7 *Let $\varphi: R \to S$ be a homomorphism from a ring R to a ring S, and let I be an ideal of R satisfying $I \subset \ker \varphi$. Then there exists a unique homomorphism $\overline{\varphi}: R/I \to S$ such that $\overline{\varphi}(I + x) = \varphi(x)$ for all $x \in R$. Moreover $\overline{\varphi}: R/I \to S$ is injective if and only if $I = \ker \varphi$.* ∎

Corollary 2.8 *Let $\varphi: R \to S$ be ring homomorphism. Then $\varphi(R)$ is isomorphic to $R/\ker \varphi$.*

2.4 The Characteristic of a Ring

Let R be a ring, and let $r \in R$. We may define $n.r$ for all natural numbers n by recursion on n so that $1.r = r$ and $n.r = (n-1).r + r$ for all $n > 0$. We define also $0.r = 0$ and $(-n).r = -(n.r)$ for all natural numbers n. Then

$$(m+n).r = m.r + n.r, \qquad n.(r+s) = n.r + n.s,$$

$$(mn).r = m.(n.r), \qquad (m.r)(n.s) = (mn).(rs)$$

for all integers m an n and for all elements r and s of R.

In particular, suppose that R is a unital ring. Then the set of all integers n satisfying $n.1 = 0$ is an ideal of $\mathbb{Z}$. Therefore there exists a unique non-negative integer p such that $p\mathbb{Z} = \{n \in \mathbb{Z} : n.1 = 0\}$ (see Lemma 2.6). This integer p is referred to as the *characteristic* of the ring R, and is denoted by $\mathrm{char}R$.

Lemma 2.9 *Let R be an integral domain. Then either $\mathrm{char}R = 0$ or else $\mathrm{char}R$ is a prime number.*

Proof Let $p = \mathrm{char}R$. Clearly $p \neq 1$. Suppose that $p > 1$ and $p = jk$, where j and k are positive integers. Then $(j.1)(k.1) = (jk).1 = p.1 = 0$. But R is an integral domain. Therefore either $j.1 = 0$, or $k.1 = 0$. But if $j.1 = 0$ then p divides j and therefore $j = p$. Similarly if $k.1 = 0$ then $k = p$. It follows that p is a prime number, as required. ∎

2.5 Polynomial Rings

Let R be a unital commutative ring. The set of all polynomials

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

in an indeterminate x with coefficients $c_0, \ldots, c_n$ in the ring R themselves constitute a ring, which we shall denote by $R[x]$. If the coefficient c_n of

highest power of x is non-zero then the polynomial is said to be of degree n, and the coefficient c_n is referred to as the *leading coefficient* of the polynomial. The polynomial is said to be *monic* if the leading coefficient c_n is equal to the multiplicative identity element 1 of the ring R.

Two polynomials with coefficients in the ring R are equal if and only if they are of the same degree and corresponding coefficients are equal. Polynomials may be added, subtracted and multiplied in the usual fashion.

We now consider various properties of polynomials whose coefficients belong to a *field* K (such as the field of rational numbers, real numbers or complex numbers).

Lemma 2.10 *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial with coefficients in K. Then, given any polynomial $h \in K[x]$, there exist unique polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$.*

Proof If $\deg h < \deg f$ then we may take $q = 0$ and $r = h$. In general we prove the existence of q and r by induction on the degree $\deg h$ of h. Thus suppose that $\deg h \geq \deg f$ and that any polynomial of degree less than $\deg h$ can be expressed in the required form. Now there is some element c of K for which the polynomials $h(x)$ and $cf(x)$ have the same leading coefficient. Let $h_1(x) = h(x) - cx^m f(x)$, where $m = \deg h - \deg f$. Then either $h_1 = 0$ or $\deg h_1 < \deg h$. The inductive hypothesis then ensures the existence of polynomials q_1 and r such that $h_1 = fq_1 + r$ and either $r = 0$ or else $\deg r < \deg f$. But then $h = fq + r$, where $q(x) = cx^m + q_1(x)$. We now verify the uniqueness of q and r. Suppose that $fq + r = f\overline{q} + \overline{r}$, where $\overline{q}, \overline{r} \in K[x]$ and either $\overline{r} = 0$ or $\deg \overline{r} < \deg f$. Then $(q - \overline{q})f = r - \overline{r}$. But $\deg((q - \overline{q})f) \geq \deg f$ whenever $q \neq \overline{q}$, and $\deg(r - \overline{r}) < \deg f$ whenever $r \neq \overline{r}$. Therefore the equality $(q - \overline{q})f = r - \overline{r}$ cannot hold unless $q = \overline{q}$ and $r = \overline{r}$. This proves the uniqueness of q and r. ∎

Any polynomial f with coefficients in a field K generates an ideal (f) of the polynomial ring $K[x]$ consisting of all polynomials in $K[x]$ that are divisible by f.

Lemma 2.11 *Let K be a field, and let I be an ideal of the polynomial ring $K[x]$. Then there exists $f \in K[x]$ such that $I = (f)$, where (f) denotes the ideal of $K[x]$ generated by f.*

Proof If $I = \{0\}$ then we can take $f = 0$. Otherwise choose $f \in I$ such that $f \neq 0$ and the degree of f does not exceed the degree of any non-zero polynomial in I. Then, for each $h \in I$, there exist polynomials q and r in $K[x]$

such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$. (Lemma 2.10). But $r \in I$, since $r = h - fq$ and h and f both belong to I. The choice of f then ensures that $r = 0$ and $h = qf$. Thus $I = (f)$. ∎

Definition Polynomials $f_1, f_2, \ldots, f_k$ with coefficients in some field K. are said to be *coprime* if there is no non-constant polynomial that divides all of them.

Theorem 2.12 *Let $f_1, f_2, \ldots, f_k$ be coprime polynomials with coefficients in some field K. Then there exist polynomials $g_1, g_2, \ldots, g_k$ with coefficients in K such that*

$$f_1(x)g_1(x) + f_2(x)g_2(x) + \cdots + f_k(x)g_k(x) = 1.$$

Proof Let I be the ideal in $K[x]$ generated by $f_1, f_2, \ldots, f_k$. It follows from Lemma 2.11 that the ideal I is generated by some polynomial d. Then d divides all of $f_1, f_2, \ldots, f_k$ and is therefore a constant polynomial, since these polynomials are coprime. It follows that $I = K[x]$. But the ideal I of $K[x]$ generated by $f_1, f_2, \ldots, f_k$ coincides with the subset of $K[x]$ consisting of all polynomials that may be represented as finite sums of the form

$$f_1(x)g_1(x) + f_2(x)g_2(x) + \cdots + f_k(x)g_k(x)$$

for some polynomials $g_1, g_2, \ldots, g_k$. It follows that the constant polynomial with value 1 may be expressed as a sum of this form, as required. ∎

Definition A non-constant polynomial f with coefficients in a field K is said to be *irreducible* over K if it is not divisible by any non-constant polynomial of lower degree with coefficients in K.

Any polynomial with coefficients in a field K may be factored as a product of irreducible polynomials. This is easily proved by induction on the degree of the polynomial, for if a non-constant polynomial is not itself irreducible, then it can be factored as a product of polynomials of lower degree.

Lemma 2.13 *Let K be a field. Then the ring $K[x]$ of polynomials with coefficients in K contains infinitely many irreducible polynomials.*

Proof Let $f_1, f_2, \ldots, f_k \in K[x]$ be irreducible polynomials, and let

$$g = f_1 f_2 \cdots f_k + 1.$$

Then g is not divisible by $f_1, f_2, \ldots, f_k$, and therefore no irreducible factor of g is divisible by any of $f_1, f_2, \ldots, f_k$. It follows that $K[x]$ must contain irreducible polynomials distinct from $f_1, f_2, \ldots, f_k$. Thus the number of irreducible polynomials in $K[x]$ cannot be finite. ∎

The proof of Lemma 2.13 is a direct analogue of Euclid's proof of the existence of infinitely many prime numbers.

Proposition 2.14 *Let f, g and h be polynomials with coefficients in some field K. Suppose that f is irreducible over K and that f divides the product gh. Then either f divides g or else f divides h.*

Proof Suppose that f does not divide g. We must show that f divides h. Now the only polynomials that divide f are constant polynomials and multiples of f. No multiple of f divides g. Therefore the only polynomials that divide both f and g are constant polynomials. Thus f and g are coprime. It follows from Proposition 2.12 that there exist polynomials u and v with coefficients in K such that $1 = ug + vf$. Then $h = ugh + vfh$. But f divides $ugh + vfh$, since f divides gh. It follows that f divides h, as required. ∎

Proposition 2.15 *Let K be a field, and let (f) be the ideal of $K[x]$ generated by an irreducible polynomial f with coefficients in K. Then $K[x]/(f)$ is a field.*

Proof Let $I = (f)$. Then the quotient ring $K[x]/I$ is commutative and has a multiplicative identity element $I+1$. Let $g \in K[x]$. Suppose that $I+g \neq I$. Now the only factors of f are constant polynomials and constant multiples of f, since f is irreducible. But no constant multiple of f can divide g, since $g \notin I$. It follows that the only common factors of f and g are constant polynomials. Thus f and g are coprime. It follows from Proposition 2.12 that there exist polynomials $h, k \in K[x]$ such that $fh + gk = 1$. But then $(I+k)(I+g) = I+1$ in $K[x]/I$, since $fh \in I$. Thus $I+k$ is the multiplicative inverse of $I+g$ in $K[x]/I$. We deduce that every non-zero element of $K[x]/I$ is invertible, and thus $K[x]/I$ is a field, as required. ∎

2.6 Gauss's Lemma

We shall show that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ if and only if it cannot be expressed as a product of polynomials of lower degree with *integer* coefficients.

Definition A polynomial with integer coefficients is said to be *primitive* if there is no prime number that divides all the coefficients of the polynomial

Lemma 2.16 (Gauss's Lemma) *Let g and h be polynomials with integer coefficients. If g and h are both primitive then so is gh.*

Proof Let $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_rx^r$ and $h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$, and let $g(x)h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{r+s}x^{r+s}$. Let p be a prime number. Then the polynomials g and h must both have at least one coefficient that is not divisible by p. Let j and k be the smallest values of i for which p does not divide b_i and c_i respectively. Then $a_{j+k} - b_jc_k$ is divisible by p, since $a_{j+k} - b_jc_k = \sum_{i=0}^{j-1} b_ic_{j+k-i} + \sum_{i=0}^{k-1} b_{j+k-i}c_i$, where p divides b_i for all $i < j$ and p divides c_i for all $i < k$. But p does not divide b_jc_k since p does not divide either b_j or c_k. Therefore p does not divide the coefficient a_{j+k} of gh. This shows that the polynomial gh is primitive, as required. ∎

Proposition 2.17 *A polynomial with integer coefficients is irreducible over the field $\mathbb{Q}$ of rational numbers if and only if it cannot be factored as a product of polynomials of lower degree with integer coefficients.*

Proof Let f be a polynomial with integer coefficients. If f is irreducible over $\mathbb{Q}$ then f clearly cannot be factored as a product of polynomials of lower degree with integer coefficients. Conversely suppose that f cannot be factored in this way. Let $f(x) = g(x)h(x)$, where g and h are polynomials with rational coefficients. Then there exist positive integers r and s such that the polynomials $rg(x)$ and $sh(x)$ have integer coefficients. Let the positive integers u and v be the highest common factors of the coefficients of the polynomials $rg(x)$ and $sh(x)$ respectively. Then $rg(x) = ug_*(x)$ and $sh(x) = vh_*(x)$, where g_* and h_* are primitive polynomials with integer coefficients. Then $(rs)f(x) = (uv)g_*(x)h_*(x)$. We now show that $f(x) = mg_*(x)h_*(x)$ for some integer m. Let l be the smallest divisor of rs such that $lf(x) = mg_*(x)h_*(x)$ for some integer m. We show that $l = 1$. Suppose that it were the case that $l > 1$. Then there would exist a prime factor p of l. Now p could not divide m, since otherwise $(l/p)f(x) = (m/p)g_*(x)h_*(x)$, which contradicts the definition of l. Theorefore p would have to divide each coefficient of $g_*(x)h_*(x)$, which is impossible, since it follows from Gauss's Lemma (Lemma 2.16) that the product g_*h_* of the primitive polynomials g_* and h_* is itself a primitive polynomial. Therefore $l = 1$ and $f(x) = mg_*(x)h_*(x)$. Now f does not factor as a product of polynomials of lower degree with integer coefficients. Therefore either $\deg f = \deg g_* = \deg g$, or else $\deg f = \deg h_* = \deg h$, Thus f is irreducible over $\mathbb{Q}$, as required. ∎

2.7 Eisenstein's Irreducibility Criterion

Proposition 2.18 (Eisenstein's Irreducibility Criterion) *Let*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

be a polynomial of degree n with integer coefficients, and let p be a prime number. Suppose that

- *p does not divide a_n,*
- *p divides $a_0, a_1, \ldots, a_{n-1}$,*
- *p^2 does not divide a_0.*

Then the polynomial f is irreducible over the field $\mathbb{Q}$ of rational numbers.

Proof Suppose that $f(x) = g(x)h(x)$, where g and h are polynomials with integer coefficients. Let $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_rx^r$ and $h(x) = c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$. Then $a_0 = b_0c_0$. Now a_0 is divisible by p but is not divisible by p^2. Therefore exactly one of the coefficients b_0 and c_0 is divisible by p. Suppose that p divides b_0 but does not divide c_0. Now p does not divide all the coefficients of $g(x)$, since it does not divide all the coefficients of $f(x)$. Let j be the smallest value of i for which p does not divide b_i. Then p divides $a_j - b_jc_0$, since $a_j - b_jc_0 = \sum_{i=0}^{j-1} b_ic_{j-i}$ and b_i is divisible by p when $i < j$. But b_jc_0 is not divisible by p, since p is prime and neither b_j nor c_0 is divisible by p. Therefore a_j is not divisible by p, and hence $j = n$ and $\deg g \geq n = \deg f$. Thus $\deg g = \deg f$ and $\deg h = 0$. Thus the polynomial f does not factor as a product of polynomials of lower degree with integer coefficients, and therefore f is irreducible over $\mathbb{Q}$ (Proposition 2.17). ∎