Journal of Mathematical Research & Exposition
Vol 19, No. 2, 367-373, May 1999

# Some Structures of Irreducible Polynomials over a Unique Factorization Domain $R$ *

*Wang Rui*
(Dept. of Comp. Sci., Yunnan University, Kunming 650091)

**Abstract**: In this paper, we give the conception of implicit congruence and nonimplicit congruence in a unique factorization domain $R$ and establish some structures of irreducible polynomials over $R$. A classical result, Eisenstein's criterion, is generalized.

**Keywords**: unique factorization domain, prime element, nonimplicit congruence, irreducible polynomial

**Classification**: AMS(1991) 11J/CLC O156

**Document code**: A **Article ID**: 1000-341X(1999)02-0367-07

## 1. Introduction

Early in the middle of the 19th century, F. G. M. Eisenstein, a German mathematician, gave this famous criterion[1, 2]:

**Theorem** *Suppose that*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

*is a polynomial with coefficients in a unique factorization domain R. If there exists a prime element $p \in R$ such that*

$$1.^{\circ}\ p \nmid a_n;\quad 2.^{\circ}\ p \mid a_0, a_1, \cdots, a_{n-1};\quad 3.^{\circ}\ p^2 \nmid a_0,$$

*then $f(x)$ is irreducible over R or its quotient field.*

Recently, someone shows[3] that Eisenstein's irreducible condition is necessary and sufficient if the degree of f(x) is 2, only sufficient if that of f(x) is greater than 2. Therefore, it will be meaningful to improve and extend Eisenstein's theorem.

## 2 Main Results

* **Received date**: 1996-08-18; **Revised date**: 1999-02-28
**Biography**: Wang Rui(1960-), male, born in Tongxian country, Beijing city. M. Sc., currently an associate professor at Yunnan University.

Let $R$ be a unique factorization domain in this paper.

**Lemma 2.1** *Suppose that $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with coefficients in $R$, where $n$ is an integer $>2$. If there exist a prime element $p \in R$ and a coefficient $a_k$ $(m < k \leq n)$ such that*

$$1.^\circ\ p \nmid a_k; \quad 2.^\circ\ p \mid a_0, a_1, \cdots, a_m; \quad 3.^\circ\ p^2 \nmid a_0,$$

*where $0 < m < n$, and $2m \geq n$, then $f(x)$ can not be decomposed into the product of two polynomials over $R$ or its quotient field, whose degrees are equal to or less than $m$ (i.e. $\leq m$).*

In the above lemma, the case of $m = n-1$ is just Eisenstein's criterion.

We draw inspiration from Lemma 2.1 and give the following result:

**Theorem 2.2** *Suppose that $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with coefficients in $R$. If there exist a prime element $p \in R$ and a coefficient $a_k$ of $f(x)$ $(0 \leq k \leq n)$ such that*

$$1.^\circ\ p \nmid a_k; \quad 2.^\circ\ p \mid a_0, a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n; \quad 3.^\circ\ p^2 \nmid a_0, a_n,$$

*then $f(x)$ can be decomposed at most into the product of two polynomials over $R$, whose degrees are $k$ and $(n-k)$, respectively.*

The following cases are clear.

**Corollary 2.2.1** *If $k$ in Theorem 2.2 is equal to $0$ or $n$, then $f(x)$ is irreducible over $R$ or its quotient field.*

**Corollary 2.2.2** *If $k = n-1$ or $1$ in Theorem 2.2, then $f(x)$ can be decomposed at most into the product of two polynomials over $R$ or its quotient field, whose degrees are $1$ and $n-1$, respectively.*

**Corollary 2.2.3** If *$k = [n/2]$ in Theorem 2.2, then $f(x)$ can be decomposed at most into the product of two polynomials over $R$ or its quotient field, whose degrees are $[n/2]$ and $n-[n/2]$, respectively. Here $[x]$ is the largest integer less than or equal to $x$.*

**Remark 1** Reducible polynomials whose coefficients adapt to Theorem 2.2 are easily found:

**Example 1** Let $n$ be a positive integer, then the following polynomial

$$px^{3n} - (p^3 + e)x^n + p = (px^{2n} + p^2 x^n - e)(x^n - p)$$

is reducible over $R$, where $p$, $e$ are a prime element and a unit element of $R$, respectively.

**Remark 2** On the other hand, the unique possiblity of decomposition over $R$ or its quotient field is left in Theorem 2.2 but its Corollary 2.2.1. So the irreducibility of $f(x)$ over $R$ or its quotient field in Theorem 2.2 can not be determined.

**Remark 3** By the way, according to the proof in §3 of this paper, if $f(x)$ in Theorem 2.2 is reducible over $R$ or its quotient field, then both of its divisors are the irreducible polynomials that adapt to Eisenstein's condition (or Corollary 2. 2. 1).

Combining Lemma 2. 1 and Theorem 2. 2, we get easily the following result:

**Theorem 2. 3** *Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with coefficients in $R$. If $p, q \in R$ are two distinct prime elements, and $a_k, a_s$ $(0<k<n, \max\{k, n-k\}<s \leq n)$ are $f(x)$'s coefficients, such that*

$1^\circ$ $p \nmid a_k$, $q \mid a_s$;

$2^\circ$ $p \mid a_0, a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n$; $q \mid a_0, a_1, \cdots, a_{s-1}$;

$3^\circ$ $p^2 \nmid a_0, a_n$; $q^2 \nmid a_0$,

*then $f(x)$ is irreducible over $R$ or its quotient field.*

A proof of this theorem can be replaced by the following example:

**Example 2** Let $R = Z$, the polynomial

$$g(x) = 3x^{11} + 6x^9 - 5x^3 - 15$$

is irreducible over $Z$ or its quotient field $Q$, here $Z$ is the set of all integers

First, we have $3 \nmid a_3$; $3 \mid a_0, a_1, a_2, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}$; and $3^2 \nmid a_0, a_{11}$, from Theorem 2. 2 it follows that $g(x)$ can be divisible at most by the irreducible polynomials over $Z$ or $Q$, whose degree is 3 or 8 Second, we also have $5 \nmid a_9$; $5 \mid a_0, a_1, \cdots, a_8$; and $5^2 \nmid a_0$, from Lemma 2. 1 it follows that $g(x)$ can not be decomposed into the product of two polynomials over $Z$ or $Q$, whose degrees are 3 and 8, 4 and 7, or 5 and 6 Combining the first and the second the irreducibility of $g(x)$ over $Z$ or $Q$ holds

With the help of implicit or nonimplicit congruence, to be defined, another way to construct irreducible polynomials over $R$ or its quotient field will be obtained

**Definition 2. 4**[4, 5] *Let $R$ be a unique factorization domain. For $a, b, m \in R$ and $m \neq 0$ We call $a$ is implicit congruent to $b$ (mod $m$) if there exists a divisor of $b$ such that $a$ is congruent to this divisor (mod $m$). It is denoted by $a \equiv (b)$ (mod $m$). Conversely, we call $a$ is not implicit congruent to $b$ (mod $m$) if $a$ is not congruent to any divisor of $b$ (mod $m$), it is denoted by $a \not\equiv (b)$ (mod $m$).*

**Example 3** Let $R = Z$, then $7 \equiv (4)$ (mod 5) because $7 \equiv 2$ (mod 5) and $4 \equiv 0$ (mod 2); $15 \not\equiv (2)$ (mod 3) because $15 \not\equiv -2, -1, 1$, or 2 (mod 3).

We introduce some of the basic properties of implicit or nonimplicit congruence Let $m, n, p \in R$, $p \neq 0$, and $e$ be a unit element of $R$.

1) If $m \equiv n$ (mod $p$), then $m \equiv (n)$ (mod $p$), or $n \equiv (m)$ (mod $p$), but its inverse is not true

2) If $m \not\equiv (n)$ (mod $p$), then $m \not\equiv n$ (mod $p$), but its inverse is not true

3) If $m \equiv -e$, or $e$ (mod $p$), then, for any $n \in R$, $m \equiv (n)$ (mod $p$).

It is obvious that the implicit congruence and its inverse contain the usual congruence in $R$.

With the help of nonimplicit congruence, we improve Theorem 2. 2 into a criterion for irreducibility of polynomials over $R$.

**Theorem 2.5** *Suppose that* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ *is a polynomial with coefficients in* $R$, *where* $n$ *is an integer* $> 2$. *If there exists a prime element* $p \in R$ *and a term* $a_k\,(0 < k < n)$ *such that*

1.° $p \nmid a_k$, *and* $a_k \not\equiv (a_0 \cdots a_n) \pmod{p^2}$;
2.° $p \mid a_0, a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n$;
3.° $p^2 \nmid a_0,\ a_n$,

*then* $f(x)$ *is irreducible over* $R$ *or its quotient field.*

Especially, when $k = n-1$ in Theorem 2.5, we get:

**Theorem 2.6** *Suppose that* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ *is a polynomial with coefficients in* $R$ $(n > 2)$. *If there exists a prime element* $p \in R$ *such that*

1.° $p \nmid a_{n-1}$, and $a_{n-1} \not\equiv (a_0a_n) \pmod{p}$;
2.° $p \mid a_0, a_1, \cdots, a_{n-2}$;
3.° $p^2 \nmid a_0$,

*then* $f(x)$ *is irreducible over* $R$ *or its quotient field.*

**Remark 1** Comparing Theorems 2.5, 2.6 with Theorem 2.2, we find $a_k$ in Theorems 2.5, 2.6 is neither $a_0$ nor $a_n$. Because we have Eisenstein's theorem or Corollary 2.2.1 when $a_k$ is $a_0$ or $a_n$.

**Remark 2** Conditions 1°, 2°, 3° in Theorem 2.2 is the same as that in Theorem 2.5 except $a_k \not\equiv (a_0, a_n) \pmod{p^2}$.

**Remark 3** The condition $p \nmid a_n$ is given up, as for Theorem 2.6, relation $a_k \not\equiv (a_0 \cdots a_n) \pmod{p^2}$ changes into $a_k \not\equiv (a_0 \cdots a_n) \pmod{p}$.

Theorem 2.5, 2.6 are just the desired results

**Example 4** Suppose that

$$\varphi(x) = 5x^n - 6x^{n-1} - 5, \quad n > 2$$

Using Eisenstein's theorem, Theorem 2.2, or Theorem 2.3, we can not get $\varphi(x)$ has irreducible property over $Z$ or $Q$. But we have 1.° $5 \nmid 6 = a_{n-1}$, and $a_{n-1} = 6 \not\equiv (5 \times 5) \pmod{5^2}$; 2.° $5 \mid a_0, a_1, \cdots, a_{n-2}a_n$; and 3.° $5^2 \nmid a_0, a_n$. From Theorem 2.5 it follows that $\varphi(x)$ is irreducible, and furthermore, polynomials $5x^n + 6x^{n-2} - 5$, $5x^n + 6x^{n-3} - 5, \cdots$, or $5x^n + 6x - 5$, are irreducible over $Z$ or $Q$. Theorem 2.6 fails to $\varphi(x)$ because $6 \equiv (5 \times 5) \pmod{5}$.

## 3. Proof of Theorems

Theorem 2.2 is basic for Theorems 2.3, 2.5. First we prove Lemma 2.1, then give a proof of Theorem 2.2.

**Proof of Lemma 2.1** Suppose that $f(x)$ can be factorized into the product of two polynomials over $R$ or its quotient field, whose degrees are equal to or less than $m$. Let $f(x) = g(x)h(x)$, where $g(x) = b_sx^s + b_{s-1}x^{s-1} + \cdots + b_1x + b_0$, $h(x) = c_tx^t + c_{t-1}x^{t-1} + \cdots + c_1x +$

$c_0$; $t+s=n$; $1\le t\le s\le m<k$. Then we have:

$$
\begin{aligned}
&a_n = b_s c_t;\\
&a_{n-1} = b_s c_{t-1} + b_{s-1} c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_k = b_s c_{k-s} + b_{s-1} c_{k-s+1} + \cdots + b_{k-1} c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_s = b_s c_0 + b_{s-1} c_1 + \cdots + b_{s-t} c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_1 = b_1 c_0 + b_0 c_1;\\
&a_0 = b_0 c_0,
\end{aligned}
\qquad \text{(I)}
$$

By hypothesis $p \mid a_0$ and $p^2 \nmid a_0$ we have (1) $p \mid b_0, p \nmid c_0$, or (2) $p \mid c_0, p \nmid b_0$. Furthermore, from the condition $p \mid a_0, a_1, \cdots, a_m$ $(1\le t\le s\le m)$ and relation (I) it follows that

$$p \mid b_0, b_1, \cdots, b_s; \text{ or } p \mid c_0, c_1, \cdots, c_t;$$

Hence we get $p \mid a_k$ contrary to 1° in Lemma 2.1. The lemma holds

Improving the above proof, we obtain Theorem 2.2

**Proof of Theorem 2.2** Suppose that $f(x)$ can be decomposed into the product of two polynomials over $R$, whose degrees are neither $k$ nor $(n-k)$. Let $f(x) = g(x)h(x)$, where $g(x) = b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0$, $h(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0$, $b_i, c_j \in R$, $i = 0, 1, \cdots, s$; $j = 0, 1, \cdots, t$; $t+s=n$; $1\le t\le s<n$; $t\ne k$ or $(n-k)$. The following relations are obtained by comparing coefficients of the equation $f(x) = g(x)h(x)$ on its both sides:

$$
\begin{aligned}
&a_n = b_s c_t;\\
&a_{n-1} = b_s c_{t-1} + b_{s-1} c_t;\\
&\cdots\ \ \cdots\ \ \cdots\ \ \cdots\\
&a_s = b_s c_0 + b_{s-1} c_1 + \cdots + b_{s-t} c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_t = b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t;\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_1 = b_1 c_0 + b_0 c_1\\
&a_0 = b_0 c_0;
\end{aligned}
\qquad \text{(II)}
$$

It is clear that there are only three cases to be considered:

1) $1\le t\le s<k\le n$. From Lemma 2.1 it follows that Theorem 2.2 is true.

2) $1\le t<k<s<n$. By hypothesis $p \mid a_0, p^2 \nmid a_0$, $p \mid a_0, a_1, \cdots, a_{k-1}$ $(t<k)$, and relation (II), we have (1) $p \mid b_0, b_1, \cdots, b_{k-1}$; or (2) $p \mid c_0, c_1, \cdots, c_t$. $p \mid a_k$ follows from (2), contrary to hypothesis $p \nmid a_k$ (1° in Theorem 2.2).

Case (1) is to be discussed: On the other hand, by hypothesis $p \mid a_n$, $p^2 \nmid a_n$, $p \mid a_n, a_{n-1}, \cdots, a_s, \cdots, a_{k+1}$ $(k<s)$, and relation (II), we have (i) $p \mid b_s, b_{s-1}, \cdots, b_{s-1}, \cdots, b_{k+1-t}$ $(k+1-t\le k)$, or (ii) $p \mid c_t, c_{t-1}, \cdots, c_0$.

Combing (1) and (i), we get (iii) $p \mid b_0, b_1, \cdots, b_s$. Hence any of both (ii) and (iii) leads to $p \mid a_k$ contrary to 1° in Theorem 2.2.

3) $0 \leq k < t \leq s < n$. With the help of the symmetry of case 1) and case 3), our proof is the same as that of case 1).

The theorem follows from the above.

From Theorem 2.2 its corollaries follow. Theorem 2.3 is a direct result of both Theorem 2.2 and Lemma 2.1. Now we give a proof of Theorem 2.5.

**Proof of Theorem 2.5** First, the conditions 1°, 2°, 3° in Theorem 2.5 except $a_k \not\equiv (a_0 \cdots a_n) \pmod{p^2}$ $(0 < k < n)$ is the same as that in Theorem 2.2. From Theorem 2.2, it follows that $f(x)$ can be decomposed at most into the product of two irreducible polynomials over $R$ or its quotient field, whose degrees are $k$ and $(n-k)$, respectively. Let $f(x) = g(x)h(x)$, where $g(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$, $h(x) = c_{n-k}x^{n-k} + c_{n-k-1}x^{n-k-1} + \cdots + c_1 x + c_0$; $k \neq 0$ or $n$. The following equations are obtained by comparing coefficients of the equation $f(x) = g(x)h(x)$ on its both sides:

$$
\begin{aligned}
&a_n = b_k c_{n-k};\\
&a_{n-1} = b_k c_{n-k-1} + b_{k-1} c_{n-k};\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_{2k-n} c_{n-k};\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_{n-k} = b_{n-k} c_0 + b_{n-k-1} c_1 + \cdots + b_0 c_{n-k};\\
&\cdots\ \cdots\ \cdots\ \cdots\\
&a_1 = b_1 c_0 + b_0 c_1;\\
&a_0 = b_0 c_0
\end{aligned}
\qquad \text{(III)}
$$

In view of the symmetry of the conditions 1°, 2°, 3° in Theorem 2.5, there are only two cases to be considered:

1) $1 \leq n-k < k < n$. By hypothesis $p \mid a_n, a_{n-1}, \cdots, a_{k+1}, p^2 \nmid a_n$, and equation (III), we have (1) $p \mid b_k, b_{k-1}, \cdots, b_{2k-n+1}$, or (2) $p \mid c_{n-k}, \cdots, c_1$. On the other hand, by hypothesis $p \mid a_0, a_1, \cdots, a_{k-1}$, $p^2 \nmid a_0$, and equation (III) we have (i) $p \mid b_0, b_1, \cdots, b_{k-1}$, or (ii) $p \mid c_0, c_1, \cdots, c_{n-k}$.

Inequality $2 \leq 2k-n+1 \leq k$ follows from $1 \leq n-k < k < n$. The combination of (1) and (i) implies $p \mid b_0, b_1, \cdots, b_k$, thus $p \mid a_k$ contrary to 1° in Theorem 2.5. Similarly, the combination of (1) and (ii), or (2) and (ii) implies $p \mid a_k$, this is contrary to $p \nmid a_k$. The combination of (2) and (i) implies $a_k \equiv b_k c_0 \pmod{p^2}$, which contradicts the hypothesis $a_k \not\equiv (a_0 a_n) \pmod{p^2}$ of 1° in Theorem 2.5.

2) $1 \leq n-k = k$, i.e. $2k = n$. This implies $a_k = a_{n-k} = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$ in equation (III). From $p \mid a_n, a_{n-1}, \cdots, a_{k+1}$; $p^2 \nmid a_n$; and (III), we get (1) $p \mid b_k, b_{k-1}, \cdots, b_1$, or (2) $p \mid c_k, c_{k-1}, \cdots, c_1$. Inversely, from $p \mid a_0, a_1, \cdots, a_{k-1}$, $p^2 \nmid a_0$; and (III), we also get (i) $p \mid b_0, b_1, \cdots, b_{k-1}$, or (ii) $p \mid c_0, c_1, \cdots, c_{k-1}$. Combining (1) and (i), or (2) and (ii), we have $p \mid a_k$ contrary to $p \nmid a_k$ of 1° in Theorem 2.5. Combining (1) and (ii), or (2) and (i), we have $a_k \equiv b_0 c_k \pmod{p^2}$, or $a_k \equiv b_k c_0 \pmod{p^2}$. They contradict the hypothesis $a_k \equiv (a_0 a_n) \pmod{p^2}$ of 1° in Theorem 2.5.

From the above the theorem is proved.

Now we return to the proof of Theorem 2.6.

**Proof of Theorem 2.6** First, From Lemma 2.1, it is clear that if $f(x)$ is reducible over $R$ or its quotient field, then $f(x)$ can be decomposed at most into the product of irreducible polynomial whose degree are 1 and $(n-1)$, respectively. Let $f(x) = g(x)h(x)$, where $g(x) = b_1x + b_0$, $h(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$, $b_i, c_j \in R$, $i = 0, 1$; $j = 0, 1, \cdots, n-1$, then we have

$$\begin{aligned} a_n &= b_1c_{n-1}; \\ a_{n-1} &= b_1c_{n-2} + b_0c_{n-1}; \\ &\cdots\ \cdots\ \cdots\ \cdots \\ a_1 &= b_1c_0 + b_0c_1; \\ a_0 &= b_0c_0 \end{aligned} \tag{IV}$$

By $p \mid a_0, a_1, \cdots, a_{n-2}$; $p^2 \nmid a_0$; and (IV), we get (1) $p \mid b_0, b_1$, or (2) $p \mid c_0, c_1, \cdots, c_{n-2}$. It is clear that case (1) is contrary to $p \nmid a_{n-1}$ of 1° in Theorem 2.6. Furthermore, case (2) implies $a_{n-1} \equiv b_0c_{n-1} \pmod p$, which contradicts $a_{n-1} \not\equiv (a_0a_n) \pmod p$ of 1° in Theorem 2.6. Hence the theorem holds.

## References

[1] Department of Mathematics and Mechanics, Beijing University, Advanced Algebra, People Education Press, Beijing, 1978.

[2] Ke Shao. Sun Qi. *Lecture on Number Theory* (1), (2) [M]. Advanced Education Press, Beijing, 1986.

[3] Zheng Geyu. *Applications of Eiseustein's Cirterion (1)*、*(2)* [J]. Bulletin of Mathematics, Sinica, 1988, **2**, 1990, **2**

[4] Wang Rui. *A Criterion for irreducible polynomials over a unique facorization domain* [J]. Bulletin of Mathematics Sinica, 1995, **11**: 42-44.

[5] Wang Rui. *Congruence relations for its subsystems of residue with mod p* [J]. Acta. Math. Sinica, 1997, **40**(6): 947-950.

# 唯一分解整环 $R$ 上不可约多项式的若干结构

王　瑞

(云南大学计算机科学系, 昆明650091)

## 摘　要

本文在唯一分解整环 $R$ 上引入隐含同余和非隐含同余概念 从而获得 $R$ 上多项式不可约性的若干结构 一百多年来首次对著名的 Eisenstein 不可约定理作出重要推广.