TESTS FOR IRREDUCIBILITY OF POLYNOMIAL OVER THE RATIONAL FIELD

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Mathematics

by

Pedro A. Tirado

August 1968

GRADUATE COUNCIL APPROVAL

DEPARTMENTAL APPROVAL

ACKNOWLEDGEMENT

I would like to express my sincere thanks to Mr. Lester Laird, without whose perseverance and encouragement this paper would not have been possible; and to my wife, Ana, whose patience and understanding have made the task easier.

CHAPTER I

INTRODUCTION

The roots of a polynomial over a given field are the most valuable pieces of information about polynomials. If the polynomial does not have roots over a given field, it is called irreducible over the given field.

Irreducibility is a large topic in mathematics whereby mathematicians have developed many tests for irreducibility.

I. The Problem

The purpose of this paper is to present: (1.) the definition and construction of the polynomial ring; (2.) some properties of the polynomial ring; (3.) tests for irreducibility of polynomial over the rational field.

Limitations. Since polynomials is a very broad area, this paper will deal with only a few aspects of these areas.

Importance of the Problem. The problem of factorization of polynomials over the rational field appears very often in algebra. If the test for irreducibility and the theorems concerning roots of such polynomials are known, then the problem can be solved.

Brief History

In elementary algebra, expressions coming under the more technical definition of polynomial are studied largely in connection with the equations formed by setting them equal to zero.

The theory of equations was developed first by Lagrange, D'alambert, Gauss, Ivory and Cauchy in the 17th century.

The fundamental theorem of algebra (all equations have a real or imaginary root) was proved by Cauchy. On the nature of these roots, Budan and Fourier did a great amount of work. After the equation of fourth degree was solved, mathematicians became interested in solving equations of the fifth degree. Niel Abell (1802-1820) proved the impossibility of this solution. Then, in 1879 Kronecker gave a demonstration of this problem which is classical and appears in the modern books of algebra.

The remarkable theory of equation due to Galois has become one of the most important branches of algebra.

Concerning the irreducibility of polynomials over rationals, it was Kronecker (1882) who gave a general solution to the problem.

In 1830 Eisenstein proved a criterion for irreducibility which was generalized by Dummas in 1906. Recently,

many irreducibility tests have been developed for particular polynomials, such as Bernoulli, Legendre, etc.

CHAPTER II

CONSTRUCTION OF THE POLYNOMIAL RING

This chapter contains some definitions and theorems necessary for the development of the polynomial ring.

Section 2.A.

Definition 2.1. A non-empty set R is said to be an associative ring if in R there are defined two binary operations denoted by + and · respectively such that for all a, b, c, in R:

(1) a + b is in R

(2) a + b = b + a

(3) (a + b) + c = a + (b + c)

(4) There exists 0 in R such that a + 0 = a for every a in R

(5) There exists -a in R such that a + (-a) = 0

(6) a·(b + c) = a·b + a·c and (b + c)·a = b·a + c·a

(Remark: The product a·b will be written as ab to simplify the notation.)

Definition 2.2. A ring R is said to be commutative if and only if the multiplication of R is such that ab = ba for every a, b, in R.

Definition 2.3. A ring R is said to be a ring with unity if and only if there exists an element 1 in R such that a 1 = 1 a = a for every a in R.

Definition 2.4. An element $a \neq 0$ in a commutative ring R is said to be a zero-divisor if there exists an element b in R, $b \neq 0$, such that $ab = 0$.

Definition 2.5. A commutative ring R with unity is said to be an integral domain if and only if R is free of zero-divisors.

Definition 2.6. A commutative ring R with unity is called a field if and only if for every $a \neq 0$ in R there exists a^{-1} in R such that $aa^{-1} = 1$.

Definition 2.7. A subset S of a ring R is said to be a subring of R if and only if, under the operation of addition and multiplication defined in R, S itself forms a ring.

Definition 2.8. If a, b are in an integral domain R, then a divided b written $a|b$, if there exists c in R such that $b = ac$.

Definition 2.9. If a,b are in an integral domain R such that $a|b$ and $b|a$, then a and b are called associates.

Definition 2.10. If a, in an integral domain R, is an associate of 1, then a is called a unit.

Theorem 2.a.

An element u in an integral domain R is called a unit if and only if u^{-1} is in R.

Proof: If u is unit, then by 2.10 there exists v in R such that $uv = vu = 1$; therefore $v = u^{-1}$. If u^{-1} is in R, then $uu^{-1} = 1$ and u 1. Since 1 divides every element in R, then 1 divides u and thus u and 1 are associates.

Definition 2.11. A mapping ϕ from the ring R into the ring R' is said to be a homomorphism if and only if

(1) $\phi (a + b) = \phi (a) + \phi (b)$

and

(2) $\phi (ab) = \phi (a)\, \phi (b)$.

Definition 2.12. A homomorphism ϕ of R into R' is said to be an isomorphism if ϕ is a one-to-one mapping.

Theorem 2.b.

A field is an integral domain.

Proof: Let F be a field. Let $a \neq 0$ and b in F such that $ab = 0$.

Since F is a field, $b = 1b = a^{-1} ab = a^{-1}0 = 0$.

If $ba = 0$ with $a \neq 0$ the commutativity of F also implies $b = 0$. Therefore, F is free of zero-divisors, and by 2.5, F is an integral domain.

Section 2.B.

Construction of the Polynomial Ring. Let R and R' be two integral domains such that $R \subseteq R'$, and let X be a variable in R'.

By adding, subtracting and multiplying X with the elements a_i of R and with itself, all the expressions of the form $a_0X^0 + a_1X^1 + \ldots + a_nX^n$ can be constructed. The set R[X] is the set of all those expressions that have been constructed over R. The elements f(X), g(X). . . . ., h(X) in R[X] are called polynomials.

In $f(X) = a_0X^0 + a_1X^1 + \ldots + a_nX^n$ the elements $a_0, a_1, \ldots, a_n$ are in R, and are called coefficients. For any positive integer n X^n represents the product $X.X \ldots \underbrace{\quad}_{n} \ldots X$.

In the following $a_0X^0 + a_1X^1 + \ldots + a_nX^n$ will be written $\sum_{i=0}^{n} a_iX^i$ with the understanding that if $n > 0$, then $a_n \neq 0$.

Example 2.1. The following is a list of all the polynomials of the form $a_0X^0 + a_1X^1 + a_2X^2 + a_3X^3$ over I/(2).

$0X^0$

$1X^0$

$1X^1 + 0X^0$

$1X^2 + 0X^1 + 0X^0$

$1X^3 + 0X^2 + 0X^1 + 0X^0$

$1X^1 + 1X^0 + 0X^0$

$1X^2 + 0X^1 + 1X^0 + 0X^0$

$1X^3 + 0X^2 + 1X^0 + 0X^0$

$1X^2 + 1X^1 + 0X^0$

$1X^2 + 1X^1 + 1X^0 + 0X^0$

$1X^3 + 0X^2 + 1X^1 + 0X^0$

$1X^3 + 1X^2 + 0X^1 + 0X^0$

$1X^3 + 1X^1 + 1X^0 + 0X^0$

$1X^3 + 1X^2 + 1X^1 + 0X^0$

$1X^3 + 1X^2 + 1X^1 + 1X^0$

Definition 2.13.

If $P(X) = \sum_{i=0}^{n} a_i X^i$ and $q(X) = \sum_{j=0}^{m} b_j X^j$

are in $R[X]$, where R is an integral domain, then $P(X) = q(X)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.

i. e., two polynomials are equal if and only if their corresponding coefficients are equal.

Definition 2.14. If as before $P(X)$ and $q(X)$ are in $R[X]$, then $P(X) + q(X) = \sum_{k=0}^{MAX(m,n)} (a_k + b_k)X^k$.

Theorem 2.c.

$R[X]$, where R is an integral domain, contains a subring isomorphic to R.

Proof: Consider the mapping T from $R'[X]$ into R, where $R'[X]$ is the subring of $R[X]$ which contains all the polynomials of the form aX^0 for every a in R.

Let T be defined such that:

$T(aX^0) = a$ for every a in R.

It is easy to see that T is a one-to-one mapping.

Since:

(1) $T(a_1X^0 + a_2X^0) = T((a_1 + a_2)X^0) = a_1 + a_2$

$= T(a_1X^0) + T(a_2X^0)$

(2) $T(a_1X^0a_2X^0) = T((a_1a_2))X^0) = a_1a_2$

$= T(a_1X^0)\ T(a_2X^0)$, then T is an isomorphism from $R'[X]$ to R.

This theorem identifies $R'[X]$ with R, and thus it is possible to write a in place of aX^0, 0 in place of $S(X) = 0X^0$, 1 in place of $1X^0$, X in place of $1X^1$, X^j in place of $1X^j$ and -aX in place of (-a)X to help simplify the notation.

Definition 2.15. If as in 2.13 P(X) and q(X) are in R[X] then $P(X)q(X) = \sum_{s=0}^{m+n} C_sX^s$ where

$$C_s = \sum_{j+k=s} a_jb_k = a_sb_0 + a_{s-1}b_1 + \ldots + a_0b_s.$$

An illustration of this definition is the example:

$P(X) = 1 + X + 2X^2 \qquad q(X) = 2 + 3X + X^3$

then

$a_0 = 1,\ a_1 = 1,\ a_2 = 2,\ a_3 = a_4 = \ldots = 0$

$b_0 = 2,\ b_1 = 3,\ b_2 = 0,\ b_3 = 1,\ b_4 = b_5 = \ldots = 0$

$C_0 = a_0b_0 = 2$

$C_1 = a_1b_0 + a_0b_1 = 2 + 3 = 5$

$C_2 = a_2b_0 + a_1b_1 + a_0b_2 = 4 + 3 = 7$

$$C_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = 0 + 6 + 0 + 1 = 7$$

$$C_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 0 + 0 + 0 + 1 + 0 + 0 = 1$$

$$C_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = 0 + 0 + 0 + 2 + 0 + 0 = 2$$

Therefore,

$$(1 + X + 2X^2)(2 + 3X + X^3) = 2 + 5X + 7X^2 + 7X^3 + X^4 + 2X^5.$$

This definition is the same as the reader has always known.

Theorem 2.d.

If the operations of addition and multiplication are defined in $R[X]$ by 2.14 and 2.15, respectively, and R is an integral domain, then $R[X]$ is an integral domain.

Proof:

(1) Closure of addition follows from 2.14.

(2) The commutativity of addition in R implies the commutativity of $R[X]$, i.e.,

if $P(X) = \sum_{i=0}^{n} a_iX^i$ and $q(X) = \sum_{j=0}^{m} b_jX^j$

are in $R[X]$ then $P(X) + q(X) = \sum_{k=0}^{MAX(n,m)} (a_k + b_k)X^k =$

$$= \sum_{k=0}^{MAX(n,\,m)} (b_k + a_k)X^k = \sum_{j=0}^{m} a_jX^j + \sum_{i=0}^{n} a_iX^i = q(X) + P(X).$$

(3) In a similar manner, associativity of addition in R implies associativity of R[X].

For any $P(X) = \sum_{i=0}^{n} a_i X^i$, $q(X) = \sum_{j=0}^{m} b_j X^j$

and $h(X) = \sum_{P=0}^{s} c_p X^p$ in R[X].

Consider:

$$(P(X) + q(X)) + h(X) = \left(\sum_{i=0}^{n} a_i X^k + \sum_{j=0}^{m} b_j X^j\right) + \sum_{P=0}^{s} c_p X^p =$$

$$= \sum_{k=0}^{MAX(n,m)} (a_k + b_k)X^k + \sum_{P=0}^{s} c_p X^p =$$

$$= \sum_{t=0}^{MAX(n,m,s)} ((a_t + b_t) + c_t)X^t =$$

$$= \sum_{t=0}^{MAX(n,m,s)} (a_t + (b_t + c_t))X^t =$$

$$= \sum_{i=0}^{n} a_i X^i + \sum_{v=0}^{MAX(m,s)} (b_v + c_v)X^v =$$

$$= \sum_{i=0}^{n} a_i X^i + \left(\sum_{j=0}^{m} b_j X^j + \sum_{P=0}^{s} c_p X^p\right) = P(X) + (g(X)+h(X)).$$

$$= \sum_{i=0}^{n} a_i X^i + \sum_{v=0}^{MAX(m,s)} (b_v + c_v)X^v =$$

$$= \sum_{i=0}^{n} a_i X^i + \left(\sum_{j=0}^{m} b_j X^j + \sum_{P=0}^{s} c_p X^p \right) =$$

$$= P(X) + (q(X) + h(X)).$$

(4) The identity element of $R[X]$ is $S(X) = 0$, since for every $P(X) = \sum_{i=0}^{n} a_i X^i$ in $R[X]$ $P(X) + S(X) =$

$$= \sum_{i=0}^{n} (a_i + 0)X^i = \sum_{i=0}^{n} a_i X^i = P(X)$$

(5) For any $P(X) = \sum_{i=0}^{n} a_i X^i$ in $R[X]$ the inverse of $P(X)$ is $\sum_{i=0}^{n} (-a_i)X^i$ since $\sum_{i=0}^{n} a_i X^i +$

$$+ \sum_{i=0}^{n} (-a_i)X^i = \sum_{i=0}^{n} (a_i + (-a_1))\, X^i = \sum_{i=0}^{n} 0X^i = S(X) = 0$$

(6) Closure of multiplication follows from 2.15.

(7) Since for every $P(X) = \sum_{i=0}^{n} a_i X^i$ and

$q(X) = \sum_{j=0}^{m} b_j X^j$ in $R[X]$,

$$P(X)q(X) = \sum_{s=0}^{t+k} \sum_{t+k=s} a_t b_k X^s =$$

$$= \sum_{s=0}^{n+m} \sum_{t+k=s} b_k a_t X^s = q(X)P(X), \text{ then multiplication}$$

in $R[X]$ is commutative.

(8) If as before $P(X)$, $q(X)$ and $h(X)$ are in $R[X]$, then

$$(P(X)q(X))h(X) = \left(\sum_{s=0}^{m+n} \sum_{t+k=s} a_t b_k X^s \right) \sum_{P=0}^{s} c_p X^p =$$

$$= \sum_{v=0}^{m+n+s} \sum_{t+k+w=s} (a_t b_k) c_w X^s =$$

$$= \sum_{v=0}^{m+n+s} \sum_{t+k+w=s} a_t (b_k c_w) X^s =$$

$$= \sum_{i=0}^{n} a_i X^i \sum_{q=0}^{m+s} \sum_{u+v=q} b_u c_v X^q =$$

$$= \sum_{i=0}^{n} a_i X^i \left(\sum_{j=0}^{m} b_j X^j \sum_{P=0}^{s} c_p X^p \right) =$$

$= P(X)(q(X)h(X))$. Thus, multiplication in $R[X]$ is associative.

(9) Consider: $P(X)(q(X) + h(X))$ where $P(X)$, $q(X)$, $h(X)$ are defined in $R[X]$ as before, then

$$\sum_{i=0}^{n} a_i X^i \left(\sum_{j=0}^{m} b_j X^j + \sum_{P=0}^{s} c_p X^p \right) =$$

$$= \sum_{i=0}^{n} a_i X^i \left(\sum_{t=0}^{MAX(m,s)} (b_t + c_t) X^t \right) =$$

$$= \sum_{R=0}^{n + MAX(m,n)} \sum_{u+1=R} a_u (b_1 + c_1) X^R =$$

$$= \sum_{R=0}^{n + MAX(m,n)} \sum_{u+1=R} (a_u b_1 + a_u c_1) X^R =$$

$$= \sum_{R=0}^{n+m} \sum_{u+1=R} a_u b_1 X^R + \sum_{R=0}^{n+s} \sum_{U=1=R} a_u c_p X^R =$$

$$= \sum_{i=0}^{n} a_i X^i \sum_{j=0}^{m} b_j X^j + \sum_{i=0}^{n} a_i X^i \sum_{P=0}^{s} c_p X^p =$$

$= P(X)g(X) + P(X)h(X)$. In a similar manner, $(P(X) + g(X))\,h(X) = P(X)h(X) + g(X)h(X)$. Therefore, the distributive laws hold in $R[X]$.

(10) Consider: $w(X) = 1$ where 1 is the unity in R. Let $P(X) = \sum_{i=0}^{n} a_i X^i$ be any other polynomial in $R[X]$ by 2.15. $P(X)1 = P(X)$, then 1 is the unity of $R[X]$.

(11) Suppose that $P(X) = \sum_{i=0}^{n} a_i X^i \neq S(X)$ and

$q(X) = \sum_{j=0}^{m} b_j X^j \neq S(X)$ are in $R[X]$ such that

$P(X)q(X) = S(X)$ then by 2.15.

$$P(X)q(X) = \sum_{s=0}^{n+m} C_s X^s$$

Since $P(X)q(X) = S(X)$ this implies that

$$C_s = \sum_{j+k=s} a_j b_k = 0 \text{ for all } s.$$

Thus for $s = m + n$, $C_{m+n} = a_n b_m$, and $a_n b_m = 0$.

Since R is an integral domain, then $a_n = 0$ or $b_m = 0$ which is contrary to the assumption that for $n > 0$, $a_n \neq 0$. Therefore, $R[X]$ is free of zero-divisors.

Therefore, $R[X]$ is an integral domain.

CHAPTER III

This chapter contains some important properties of the polynomial ring $R[X]$ over an integral domain R, and of the polynomial ring $F[X]$ over a field F.

Section 3.A.

Definition 3.1. The polynomial $P(X) = \sum_{i=0}^{n} a_i X^i$, $P(X) \neq 0$, is said to have degree n, written as deg $P(X) = n$, if and only if $n > 0$ is the largest integer such that the leading coefficient $a_n \neq 0$. The degree of the zero polynomial is undefined.

Definition 3.2. A polynomial $f(X)$ is called a constant if deg $f(X) = 0$.

Lemma 3.a.

If $P(X) \neq 0$, $P(X) = \sum_{i=0}^{n} a_i X^i$ and $q(X) \neq 0$, $q(X) = \sum_{j=0}^{m} b_j X^j$ are in $R[X]$, where R is an integral domain, then deg $(P(X)q(X))$ = deg $P(X)$ + deg $q(X)$.

Proof: Since $a_n \neq 0$ and $b_m \neq 0$, then deg $P(X) = n$ and deg $q(X) = m$.

By 2.15:

$$C_{m+n} = a_n b_m \neq 0$$

Consider:

C_i, $i > m + n$

$$C_i = a_j b_{i-j}.$$

Since $i = j + (i - j) > m + n$, then $j > m$ or $i - j > n$. This implies $a_j = 0$ or $a_{i-j} = 0$. Therefore, $C_i = 0$.

Since the highest non-zero coefficient of $P(X)q(X)$ is C_{m+n}, then by 3.1 deg $(P(X)q(X)) = m + n =$ deg $P(X)$ + deg $q(X)$.

Theorem 3.b. (Corollary of 3.a.)

If $P(X)$ and $q(X)$ are two non-zero polynomials in $R[X]$, where R is an integral domain, then either $P(X) + q(X) = 0$, or deg $(P(X) + q(X)) \leq$ MAX(deg $P(X)$, deg $q(X)$).

The proof of this theorem is evident from 2.14.

Definition 3.3. A polynomial $q(X)$ in $R[X]$, where R is an integral domain, is said to divide the polynomial $P(X)$ in $R[X]$, written $q(X) \mid P(X)$. If in $R[X]$ there exists a polynomial $h(X)$ such that $P(X) = q(X)h(X)$.

Lemma 3.c. (The division algorithm)

If $f(X)$ and $q(X) \neq 0$ are in $F[X]$ where F is a field, then there exists unique polynomials $g(X)$ and $r(X)$ in $F[X]$ such that $f(X) = g(X)q(X) + r(X)$ where $r(X) = 0$ or deg $r(X) <$ deg $q(X)$.

Proof:

If deg $f(X) <$ deg $q(X)$ then there exists $g(X) = 0$ and $r(X) = f(X)$ in $F[X]$ such that $f(X) = 0q(X) + f(X)$. If $f(X) = 0$, then there exists $g(X) = 0$ and $r(X) = 0$ in

$F[X]$ such that $f(X) = 0q(X) + 0$. Suppose that $f(X) =$

$= \sum_{i=0}^{n} a_i X^i$ and $q(X) = \sum_{j=0}^{m} b_j X^j$ where $a_m \neq 0$,

$b_n \neq 0$, and $n \geq m$.

If $n = 1$ (using induction on n), $f(X) = aX + b$ and $q(X) = cX + d$, then there exists $g(X) = ac^{-1}$ and $r(X) = b - ac^{-1}d$ in $R[X]$ such that $f(X) = ac^{-1}(cX + d) + b - ac^{-1}d$ and the theorem is true.

Assume that the theorem is true for $k \leq n-1$ where k is a positive integer.

Consider:

$$f_1(X) = f(X) - (\frac{a_n}{b_m} X^{n-m})q(X).$$

Now, deg $f_1(X) \leq n-1$, and thus by the inductive assumption there exists $g_1(X)$ and $r(X)$ such that $f_1(X) = g_1(X)q(X) + r(X)$ where $r(X) = 0$, or deg $r(X) <$ deg $q(X)$.

Thus, $f(X) = (\frac{a_n}{b_m} X^{n-m})q(X) = g_1(X)q(X) + r(X)$ and

$f(X) = (\frac{a_n}{b_m} X^{n-m} + g_1(X))q(X) + r(X)$. If $g(X) =$

$= \frac{a_n}{b_m} X^{n-m} + g_1(X)$ then $f(X) = g(X)q(X) + r(X)$ where

$r(X) = 0$ or deg $r(X) <$ deg $g(X)$.

Suppose: $f(X) = g_1(X)q(X) + r_1(X) = g_2(X)q(X) + r_2(X)$, then $(g_1(X) - g_2(X))q(X) = r_2(X) - r_1(X)$.

If $r_2(X) \neq r_1(X)$, then $r_2(X) - r_1(X) \neq 0$, $g_1(X) - g_2(X) \neq 0$ and $q(X) \neq 0$.

By 3.b: $\deg (g_1(X) - g_2(X)) + \deg q(X) = \deg (r_2(X) - r_1(X)) \leq \text{MAX} (\deg r_2(X), \deg r_1(X)) < \deg q(X)$ which is impossible, then $r_1(X) = r_2(X)$. Since $q(X) \neq 0$, then $g_1(X) - g_2(X) = 0$, and $q_1(X) = q_2(X)$. This proves the uniqueness of the theorem.

Theorem 3.d.

The polynomial $P(X)$ in $F[X]$ is a unit if and only if $P(X)$ is a non-zero element of F, where F is a field.

Proof: By Theorem 2.a, every element $a \neq 0$ in F is a unit. By Theorem 2.d, part 10, 1 is the unity in $F[X]$. If $P(X)$ is a unit, then by 2.10, there exists $h(X)$ in $F[X]$ such that $P(X)h(X) = 1$ and by 3.a, $\deg (P(X)h(X)) = \deg P(X) + \deg h(X) = \deg (1) = 0$, which is possible only if $\deg P(X) = \deg h(X) = 0$. Therefore, $P(X) = C \neq 0$ in $F[X]$.

If $P(X) = C \neq 0$ in $F[X]$, then by 2.a, $P(X)$ is a unit.

Theorem 3.e.

The polynomials $P(X)$ and $q(X)$ in $F[X]$ are associates if and only if $P(X) = Cq(X)$ where $C \neq 0$ is in the field F.

Proof: If $P(X)$ and $q(X)$ are associates, then by 2.9, $q(X) \mid P(X)$ and $P(X) \mid q(X)$, by 3.3, $P(X) = h_1(X)q(X)$ and $q(X) = h_2(X)P(X)$

$P(X)q(X) = h_1(X)h_2(X)P(X)q(X)$ and $h_1(X)h_2(X) = 1$. Thus, $h_1(X) = C$, $h_2(X) = C^{-1}$.

Therefore, $P(X) = Cq(X)$, $q(X) = C^{-1}P(X)$. If $P(X) = Cq(X)$, then $q(X) \mid P(X)$, since $q(X) = C^{-1}P(X)$, then $P(X) \mid q(X)$, and $P(X)$ and $q(X)$ are associates.

Obviously, each polynomial $P(X) = \sum_{i=0}^{n} a_i X^i$ in $F[X]$ with $a_n \neq 0$ is associated with the unique monic polynomial $a_n^{-1}P(X)$. Where monic means a polynomial $f(X)$ in $F[X]$ with leading coefficient 1.

Definition 3.4. The monic polynomial $d(X)$ in $F[X]$ is the g. c. d. of $P(X)$ and $q(X)$ in $F[X]$ if and only if $d(X)$ has the following properties:

(1) $d(X) \mid P(X)$ and $d(X) \mid q(X)$.

(2) If $h(X) \mid P(X)$ and $h(X) \mid q(X)$, then $h(X) \mid d(X)$.

Theorem 3.f.

Every pair of polynomials $P(X)$ and $q(X)$ in $F[X]$, where F is a field, has a unique g. c. d. $d(X)$ in $F[X]$ and which can be written in the form $d(X) = a(X)P(X) + b(X)q(X)$ for $a(X)$, $b(X)$ in $F[X]$.

Proof: Let k be the set of all polynomials in $F[X]$ of the form $a(X)P(X) + b(X)q(X)$. k is not empty

because $P(X) = 1P(X) + 0q(X)$ is in k. Let $d(X)$ be a polynomial of least degree in k. $d(X)$ can be monic since the monic associated with each polynomial in k is in k.

Since $d(X)$ is in k, then $d(X) = a(X)P(X) + b(X)q(X)$.

By 3.c, $P(X) = s(X)d(X) + r(X)$ where $r(X) = 0$ or $\deg r(X) < \deg d(X)$. If $r(X) = 0$ $d(X) \mid P(X)$. If $r(X) \neq 0$, $r(X) = P(X) - s(X)d(X) = P(X) - s(X)((a(X)P(X) + b(X)q(X)) =$ $= P(X) - s(X)a(X)P(X) - s(X)b(X)q(X) = ((1 - s(X)a(X))P(X) +$ $+ (-s(X)b(X))q(X) = \bar{a}(X)P(X) + \bar{b}(X)q(X)$ where $\bar{a}(X)$ and $\bar{b}(X)$ are in $F[X]$. Thus, $r(X)$ is in k. $\deg r(X) < \deg d(X)$ is a contradiction. Therefore, $d(X) \mid P(X)$.

In a similar manner $d(X) \mid q(X)$.

Suppose there exists $d_1(X)$ in $F[X]$ such that $d_1(X) \mid P(X)$ and $d_1(X) \mid q(X)$. By 3.3

$$P(X) = d_1(X)h_1(X)$$

$$q(X) = d_1(X)h_2(X) \text{ and}$$

$$d(X) = d_1(X)h_1(X)a(X) + d_1(X)h_2(X)b(X)$$

$$d(X) = d_1(X)(h_1(X)a(X) + h_2(X)b(X))$$

$$d(X) = d_1(X)h_3(X)$$

Therefore, $d_1(X) \mid d(X)$, which completes part (2) of 3.4, and $d(X)$ is the g. c. d. of $P(X)$, $q(X)$.

Suppose there exists $d_2(X)$ in $F[X]$ such that $d_2(X)$ satisfies 3.4. Then $d(X) \mid d_2(X)$ and $d_2(X) \mid d(X)$. Therefore, $d_2(X)$ is an associate of $d(X)$. By 3.e, $d(X) =$ $= Cd_2(X)$. Since $d(X)$ and $d_2(X)$ are monic, then $C = 1$ and $d(X)$ is unique.

Definition 3.5. Two polynomials P(X) and q(X) in F[X] not both zero are called relatively prime if their g. c. d. is 1 in the field F.

Obviously, $1 = a(X)P(X) + b(X)q(X)$ for some a(X), b(X) in F[X].

Theorem 3.g. (Euclidean Algorithm)

This is an alternate method of proving the existence of the g. c. d. This method is also useful in expressing g. c. d. of two polynomials as a linear combination of these polynomials.

Proof: Let P(X) and q(X) be two non-zero polynomials in F[X], where F is a field. By 3.c,

(1.) $P(X) = g(X)q(X) + r_1(X)$

$r_1(X) = 0$ or $\deg r_1(X) < \deg q(X)$

(2.) $q(X) = q_1(X)r_1(X) + r_2(X)$

$r_2(X) = 0$ or $\deg r_2(X) < \deg r_1(X)$

(3.) $r_1(X) = q_2(X)r_2(X) + r_3(X)$

$r_3(X) = 0$ or $\deg r_3(X) < \deg r_2(X)$

. . . . . .

(k.) $r_{k-3}(X) = q_{k-1}(X)r_{k-1}(X) + r_k(X)$

$r_k(X) = 0$ or $\deg r_k(X) < \deg r_{k-1}(X)$

(k+1.) $r_{k-2}(X) = q_k(X)r_k(X) + r_{k+1}(X)$

$r_{k+1}(X) = 0$ or $\deg r_{k+1}(X) < \deg r_k(X)$,

Suppose $r_{k+1}(X) = 0$. By (k+1), $r_k(X) \mid r_{k-1}(X)$ and then by (k) $r_k(X) \mid r_{k-2}(X)$.

Using equations ((k-1), (k-2), . . . (3), (2), (1)), it follows $r_k(X) \mid r_1(X)$, $r_k(X) \mid r(X)$, which implies $R_k(X) \mid P(X)$ and $r_k(X) \mid q(X)$.

If the polynomial h(X) is in $F[X]$ such that $h(X) \mid P(X)$ and $h(X) \mid q(X)$, then by (1.) $h(X) \mid r(X)$, and by (2.) $h(X) \mid r_1(X)$ in the same manner as before but using equations ((3), (4), . . . , (k-1), (k), (k + 1)) in the order shown, it concludes that $h(X) \mid r_k(X)$.

Therefore, by 3.4, the monic $c^{-1}r_k(X)$, associated with $r_k(X)$ is the g. c. d. of P(X) and q(X).

Using induction on $r_k(X)$, let prove the second part of 3.g. For k = 1, $r_1(X) = P(X) - g_1(X)q(X)$; thus, $r_1(X)$ can be written as a linear combination of P(X) and q(X), which is the desired form in 3.f. Suppose it can be done in this manner for all $r_n(X)$ where $n \leq k-1$.

Consider: $r_{k-2}(X) = r_{k-1}(X)q_k(X) + r_k(X)$ by the above assumption, $r_{k-2}(X) = h_1(X)P(X) + h_2(X)q(X)$ and $r_{k-1}(X) = h_3(X)P(X) + h_4(X)q(X)$. Thus, $h_1(X)P(X) +$ $+ h_2(X)g(X) = h_3(X)P(X) + h_4(X)q(X))q_k(X) + r_k(X)$ and $P(X)(h_1(X) - h_3(X)q_k(X)) + q(X)(h_2(X) - h_4(X)q_k(X)) = r_k(X)$.

Therefore, by induction $r_k(X)$ can be written as a linear combination of P(X) and q(X), for k = 1, 2, . . .

Since deg $r_1(X) >$ deg $r_2(X) > > \ldots$ by 3.1, there exists $r_{k+1}(X)$ in $F[X]$ such that deg $r_{k+1} = 0$. By 3.2, $r_{k+1}(X) = C \neq 0$ in F, then obviously 1 is the g. c. d. of P(X) and q(X), and by 3.5, $1 = a(X)P(X) + b(X)q(X)$, which completes the proof of the theorem.

Example 3.1.

Using 3.g, and given $P(X) = 2X^3 - 4X^2 + X - 2$ and $q(X) = X^3 - X^2 - X - 2$, in $F[X]$ where F is a field, the procedure to find the g. c. d. of P(X) and q(X) is the following:

(1) $2X^3 - 4X^2 + X - 2 = 2(X^3 - X^2 - X - 2) - 2X^2 + 3X + 2$

$X^3 - X^2 - X - 2 = (-1/2X - 1/4)(-2X^2 + 3X + 2) +$

$+3/4X - 3/2$

$-2X^2 + 3X + 2 = -8/3X(3/4X - 3/2) - X + 2$

$3/4X - 3/2 = -3/4(-X + 2) + 0.$

Since the monic associated with $-X + 2$ is $X-2$, then $X-2$ is the g. c. d. of P(X) and q(X).

(2) The procedure to write $X - 2$ as a linear combination of P(X) and q(X) is the following:

$P(X) - 2q(X) = -2X^2 + 3X + 2$

$q(X) - (-1/2X - 1/4)(P(X) - 2q(X)) = 3/4X - 3/2$

$q(X) - (-1/2XP(X) + Xq(X) - 1/4P(X) + 1/2q(X)) =$

$= q(X) + 1/2XP(X) - Xq(X) + 1/4P(X) - 1/2q(X) = 3/4X - 3/2.$

$P(X) - 2q(X) + 8/3X(q(X) + 1/2XP(X) - Xq(X) + 1/4P(X) -$

$- 1/2q(X)) = -1(X - 2)$

$-P(X) + 2q(X) - 8/3q(X) - 4/3X^2P(X) + 8/3X^2q(X) - 2/3XP(X) +$

$+ 4/3Xq(X) = X - 2$

$q(X)(-2/3 + 4/3 + 8/3X^2) + P(X)(-4/3X^2 - 2/3X - 1) = X - 2.$

Definition 3.6. A nonconstant polynomial $P(X)$ in $F[X]$ where F is a field, is called irreducible or prime in $F[X]$ if its only divisors in $F[X]$ are its associates and the units.

Definition 3.7. A nonconstant polynomial $P(X)$ in $F[X]$, where F is a field, is called reducible if there exists at least $q(X)$ and $g(X)$ in $F[X]$, where $q(X)$ and $g(X)$ are not units or associates of $P(X)$, such that $d(X) = q(X)g(X)$. The polynomial $aX + b$ is irreducible in any field F.

Theorem 3.h.

If $P(X)$ is a prime polynomial in $F[X]$, where F is a field, and $q(X)$ is any other polynomial in $F[X]$, then either $P(X)$ and $q(X)$ are relatively prime, or else their g. c. d. is the monic associate of $P(X)$.

Proof: Suppose $d(X)$ is the g. c. d. of $P(X)$ and $q(X)$, then $d(X) \mid P(X)$; this implies either $d(X)$ is a monic associated with $P(X)$ or $d(X)$ is a unit in $F[X]$, i.e., $d(X)$ is a non-zero constant, which implies that $P(X)$ and $q(X)$ are relatively primes.

Theorem 3.i.

If P(X) is a prime polynomial in $F[X]$, where F is a field, such that $P(X) \mid g(X)h(X)$ for $g(X)h(X)$ in $F[X]$, then either $P(X) \mid h(X)$ or $P(X) \mid g(X)$.

Proof: Suppose d(X) is the g. c. d. of P(X) and g(X).

If d(X) is an associate of P(X), then $d(X) \mid g(X)$.

If d(X) is not an associate of P(X), then by 3.h, P(X) and g(X) are relatively prime consequently.

$1 = a(X)P(X) + b(X)g(X)$.

$h(X) = a(X)P(X)h(X) + b(X)g(X)h(X)$. Since $P(X) \mid g(X)g(X)$, then $h(X) = a(X)P(X)h(X) + b(X)P(X)h_1(X)$ and $h(X) = P(X)(a(X)h(X) + b(X)h_1(X))$, thus $P(X) \mid h(X)$.

Theorem 3.j. (Corollary of 3.i.)

Let P(X) be a prime polynomial in $F[X]$, where F is a field, such that $P(X) \mid g_1(X)g_2(X) \ldots g_s(X)$ where the product $g_1(X)g_2(X) \ldots g_s(X)$ is in $F[X]$, then $P(X) \mid g_i(X)$ for some $i = 1, 2, \ldots, s$.

Proof: If $s = 2$ (using induction on s), the theorem is true by 3.i. Suppose the theorem is true for $n \leq s-1$.

If $g_1(X)g_2(X) \ldots g_s(X)$ is arranged in the following manner, $g_1(X)g_2(X) \ldots g_s(X) = g_j(X)g_s(X)$ where $j = 1, 2, \ldots, n$, then by 3.i, $P(X) \mid g_j(X)$ or $P(X) \mid g_s(X)$ and

by the induction assumption $P(X) \mid g_t(X)$ where t is one of the integers 1, 2, . . ., n, thus either $P(X) \mid g_t(X)$ or $P(X) \mid g_s(X)$. Therefore $P(X) \mid g_m(X)$ where m is one of the integers 1, 2, . . ., s, which completes the proof of the theorem.

Theorem 3.k. (Corollary of 3.i.)

If P(X) and g(X) are relatively prime polynomials in $F[X]$ such that $P(X) \mid g(X)h(X)$ in $F[X]$, then $P(X) \mid h(X)$.

Proof: Since P(X) and g(X) are relatively prime, by 3.5,

$h_1(X)P(X) + h_2(X)g(X) = 1$. Thus,

$h_1(X)P(X)h(X) + h_2(X)g(X)h(X) = h(X)$

$h_1(X)P(X)h(X) + h_2(X)P(X)h_3(X) = h(X)$

$P(X)(h_1(X)h(X) + h_2(X)h_3(X)) = h(X)$

$P(X)h_4(X) = h(X)$, then $P(X) \mid h(X)$.

Theorem 3.l.

Every non-zero polynomial P(X) in $F[X]$ can be written uniquely (except for the order of the factors) in the form:

$P(X) = cP_1(X)P_2(X) \ldots P_r(X)$ where $c \neq 0$ is in the field F and $P_j(X)$ $(j = 1, 2, \ldots r)$ is a monic irreducible polynomial in $F[X]$.

Proof: If deg P(X) = 0, $P(X) = c \neq 0$ in F. Suppose deg P(X) = n > 0. If n = 1, $P(X) = aX + b = a(X + a^{-1}b)$.

Assume the theorem true for all polynomials of degree less than n. If P(X) is prime, $P(X) = cP_1(X)$ where $P_1(X)$ is the monic associated with P(X). If P(X) is reducible then by 3.7, $P(X) = g(X)h(X)$ where deg $g(X) > n$ and deg $h(X) > n$.

By induction:

$g(X) = c_1 g_1(X)g_2(X) \ldots g_s(X)$

$h(X) = c_2 h_1(X)h_2(X) \ldots h_t(X)$ and

$P(X) = (c_1c_2)g_1(X)g_2(X) \ldots g_s(X)h_1(X)h_2(X)$

$h_3(X) \ldots h_t(X)$, which is the desired form.

Assume uniqueness of factorization for polynomials of degree less than n. If deg P(X) = 0, there is nothing to prove. If deg P(X) = 1, consider $P(X) = a(X + a^{-1}b) =$ $= c(X + c^{-1}d)$. By 2.13, a = c and b = d. Therefore, the theorem is true for n = 1.

Now suppose:

$P(X) = cP_1(X)P_1(X) \ldots P_r(X) = dg_1(X) \ldots g_s(X)$.

Since $P_i(X)$ and $g_j(X)$ are monic, c = d.

By 3.3,

$P_1(X) \mid g_i(X)$ where i = 1, 2, . . . , s, and by 3.j,

$P_1(X) \mid g_i(X)$ for some i.

Suppose $P_1(X) \mid g_j(X)$. Since $P_1(X)$ and $g_j(X)$ are monic irreducible polynomials, then $P_1(X) = g_j(X)$. Therefore,

$P_2(X) \ldots P_r(X) = g_1(X) \ldots g_{j-1}(X)g_{j+1}(X) \ldots g_s(X)$,

which is of degree less than n. By the induction assumption, r = s and $P_i(X)$ are the $g_k(X)$ in some order. This completes the proof of the theorem.

By collecting repeating factors $P(X) = cP_1(X)^{a_1}P_2(X)^{a_2} \ldots P_s(X)^{a_s}$ where $P_1(X)$, $P_2(X) \ldots P_s(X)$ are the distinct irreducible factors of P(X) and $a_1, a_2, \ldots, a_s$ are positive integers.

Definition 3.8. The mapping Q from R[X] into R[S] where S is a fixed element in the ring R, and such that for every P(X) in R[X], Q(P(X)) = P(S), is called a polynomial function.

Theorem 3.m.

The mapping Q defined in 3.8, is a homomorphism from R[X] into R[S].

Proof: Since for every $P(X) = \sum_{i=0}^{n} a_i X^i$ and

$$q(X) = \sum_{j=0}^{m} b_j X^j \text{ in } R[X]$$

(1) $$Q(P(X) + q(X)) = Q\left(\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} b_j X^j\right) =$$

$$= Q\left(\sum_{t=0}^{MAX(n,m)} (a_t + b_t)X^t\right) = \sum_{t=0}^{MAX(n,m)} (a_t + b_t)S^t =$$

$$= \sum_{i=0}^{n} a_i S^i + \sum_{j=0}^{m} b_j S^j = P(S) + q(S) = Q(P(X)) + Q(q(X)).$$

$$(2)\quad Q(P(X)q(X)) = Q\Big(\sum_{q=0}^{n+m} \sum_{k+t=q} a_k b_t X^q\Big) =$$

$$= \sum_{q=0}^{m+n} \sum_{k+t=q} a_k b_t S^q = P(S)q(S) = Q(P(X))Q(q(X)).$$

Then Q is a homomorphism.

Given any element P(S) in R[S] there exists a polynomial P(X) in R[X] such that Q(P(X)) = P(S). Therefore, Q is an onto mapping from R[X] to R[S].

Since for an element P(S) in P[S] may exist more than one element in R[X] such that P(S) is the image of those elements, then Q is not one-to-one.

Section 3.B. Roots of Polynomials

Definition 3.9. An element a in a field F is called a root of the polynomial P(X) in F[X] if P(a) = 0.

Definition 3.10. The a in the field F is a root of P(X) in F[X] of multiplicity m if $(X - a)^m \mid P(X)$, whereas $(X - a)^{m+1} \nmid P(X)$.

Theorem 3.n. (Remainder Theorem)

If P(X) is in F[X] and a is in the field F, then P(a) is the remainder on dividing P(X) by X - a.

Proof: By 3.c, P(X) = q(X)(x - a) + r(X) where r(X) = 0 or deg r(X) < deg (x - a) = 1. Thus, r(X) = 0 or

deg r(X) = 0. In either case r(X) = r, a constant in F.

$$P(X) = q(X)(X-a) + r$$

$$P(a) = q(a)0 + r$$

$$P(a) = r.$$

Theorem 3.o. (Factor Theorem)

The element a in the field F is a root of the polynomial P(X) in F[X] if $X - a \mid P(X)$.

Proof: If $x - a \mid P(X)$, then $P(X) = (X - a)q(X) + r(X)$, where r(X) = r = 0, by 3.n, $r = P(a) = 0$.

Theorem 3.p.

Let $P(X) = \sum_{i=0}^{n} a_i X^i$ be in F[X] with $a_n \neq 0$.

If $r_1, r_2, \ldots, r_n$ are distinct elements of the field F such that $r_1, r_2, \ldots, r_n$ are roots of P(X), then $P(X) = a_n(X - r_1)(X - r_2) \ldots (X - r_n)$.

Proof: By induction on the degree of P(X), if n = 1, $P(X) = aX + b$. If r_1 is a root of P(X), by 3.o, $P(r_1) = ar_1 + b = 0$, $b = -ar_1$, $P(X) = aX - ar_1 = a(X-r_1)$, then the theorem is true.

Assume that the theorem is true for n = k.

Consider the polynomial g(X) in F[X] of degree k + 1 with leading coefficient a_n. Let $r_1, r_2, \ldots, r_{k+1}$ be distinct roots of g(X). If r_1 is a root of g(X), by 3.n, $g(X) = q(X)(X - r_1)$, where deg q(X) = k. The leading

coefficient of $q(X)$ is a_n. Since a_n is the coefficient of X^{k+1} in $g(X)$.

Suppose $r_i (i \neq 1)$ is any of the other roots of $P(X)$. By 3.o,

$P(r_i) = g(r_i)(r_i - r_1) = 0.$

Since $r_i - r_1 \neq 0$, then $g(r_i) = 0$. Thus, by 3.n, $r_2, r_3, \ldots r_{k+1}$ are roots of $q(X)$. Therefore,

$q(X) = a_n(X - r_2)(X - r_3) \ldots (X - r_{k+1})$ and

$P(X) = a_m(X - r_1)(X - r_2) \ldots (X - r_{k+1})$

By induction, the theorem is true.

Theorem 3.q. (Corollary of 3.p.)

A polynomial $P(X)$ in $F[X]$ of degree $n \geq 1$ has at most n distinct roots in the field F.

If $r_1, r_2, \ldots r_n$ are distinct roots of $P(X)$ then by 3.p, $P(X) = a_n(X - r_1)(X - r_2) \ldots (X - r_n)$.

Suppose r is another root of $P(X)$ by 3.o, $P(r) = a_n(r - r_1)(r - r_2) \ldots (r - r_n) = 0$. Since $a_n \neq 0$, then $(r - r_i) = 0$ for some i.

Therefore, $P(X)$ cannot have more than n distinct roots.

Theorem 3.r. (Corollary of 3.q.)

Let $P(X) = \sum_{i=0}^{n} a_i X^i$ and $q(X) = \sum_{j=0}^{m} b_j X^j$ with $a_n \neq 0$ and $b_m \neq 0$ being two polynomials in $F[X]$

where $n \geq m$. If $P(a_i) = q(a_i)$ for at least $n + 1$ distinct elements in F, then $P(X) = q(X)$.

Proof: Consider $h(X) = P(X) - q(X)$

If $h(X) \neq 0$, then deg $h(X) \leq n$

$h(a_i) = P(a_i) - q(a_i) = 0$ for $n + 1$ distinct elements in f. This contradicts 3.q. Therefore, $h(X) = P(X) - q(X) = 0$

$P(X) = q(X)$.

Newton's Interpolation Formula

By 3.r, there exists one, and only one, polynomial of degree $\leq n$, which, at $n + 1$ points a_i assumes given values $P(a_i)$. This polynomial is given by means of Newton's Interpolation Formula.

$$(1) \quad f(X) = D_0 + D_1(X - a_0) + D_0(X - a_0)(X-a_1) + \ldots$$
$$\ldots + D_n(X-a_0)(X - a_1) \ldots (X - a_{n-1}).$$

The coefficients $D_0, \ldots D_n$ can be computed as follows:

First, substitute $X = a_0$ in (1) which gives $f(a_0) = D_0$. Subtracting this from (1) and dividing by $X - a_0$:

$$(2) \quad \frac{f(X) - f(a_0)}{X - a_0} = D_1 + D_2(X - a_1) + \ldots + D_n(X-a_1) \ldots$$
$$\ldots (X - a_{n-1}). \quad \text{Where}$$
$$f(a_0, X) = \frac{f(X) - f(a_0)}{X - a_0} .$$

Substituting $X = a_1$ in (2), $f(a_0,a_1) = D_1$.

Subtracting this from (2) and dividing by $X - a_1$,

$$(3)\quad \frac{f(a_0,X) - f(a_0,a_1)}{X - a_1} = D_2 + D_3(X - a_2) + \ldots$$

$$\ldots + D_n(X - a_1) \ldots (X - a_{n-1}).$$

Where

$$f(a_0,a_1,X) = \frac{f(a_0,X) - f(a_0, a_1)}{X - a_1}.$$

If $X = a_2$,

$f(a_0,a_1,a_2) = D_2$.

Now by complete induction, it is defined that:

$$f(a_0, \ldots a_k,X) = \frac{f(a_0, \ldots a_{k-1}, X)-f(a_0,\ldots,a_{k-1},a_k)}{X - a_k}$$

As before,

$$f(a_0, \ldots, a_{k-1}, X) = D_k + D_{k+1}(X - a_k) + \ldots$$

$$\ldots + D_n(X - a_k) \ldots (X - a_{n-1}) \text{ and}$$

$f(a_0, \ldots a_k) = D_k$.

CHAPTER IV

The purpose of this chapter is to present some tests for irreducibility of polynomials over the rational field R.

In some cases, it is not difficult to see that some polynomials are irreducible. For example, consider the polynomial $X^2 + 1$ over the real field. $X^2 + 1$ is irreducible over the reals but is reducible over the complexes, for there, $X^2 + 1 = (X + i)(X - i)$ where $i^2 = -1$.

Consider the polynomial $X^2 - 2$ over the rationals. Suppose $X^2 - 2 = (X + a)(X + b)$. If $X = -b$ then, $(-b)^2 + 2 = (-b + a)0 = 0$ and $(-b)^2 = 2$, which is impossible. Therefore, $X^2 - 2$ is irreducible over the rationals but not over the reals, for there, $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.

In a similar manner it is possible to prove that the polynomials X, $X + 1$, $X^2 + 1$, $X^3 + 1$, $X^2 + X + 1$, $X^3 + X + 1$, $X^3 + X^2 + X + 1$ are irreducible over $I/(2)$.

In the great majority of the cases, it is not as simple as in the examples presented before to say that a polynomial is irreducible or is not. To simplify this work, mathematicians have developed tests for irreducibility.

This chapter is concerned with some tests for irreducibility of polynomials over the rational field.

Let $g(X)$ be a non-zero polynomial in $R[X]$. Since $g(X) = (1/a)f(X)$ where a is the g. c. d. of the denominators of the coefficients of $g(X)$, then $g(X)$ and $f(X)$ will have the same roots in the field of the rational numbers R. Therefore, without loss of generality it is possible to work with polynomials with integral coefficients.

Theorem 4.a.

Let $P(X) = \sum_{i=0}^{n} a_i X^i$ with $a_n \neq 0$ being a polynomial in $R[X]$, where R represents the rationals. If r/s, $(r, s) = 1$, is a root of $P(X)$, then $r \mid a_0$ and $s \mid a_n$.

By 3.9, $a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \ldots + a_0 = 0$,

eliminating denominators

$$a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_0 s^n = 0.$$

It follows that:

$$r(a_n r^{n-1} + a_{n-1} r^{n-2} + \ldots + a_1 s^{n-1}) = -a_0 s^n$$

All the terms in

$$r(a_n r^{n-1} + a_{n-1} r^{n-2} + \ldots + a_1 s^{n-1}) = a_0 s^n$$

are integers; therefore,

$r \mid a_0 s^n$ and since $(r,s) = 1$, then $r \mid a_0$. In a similar manner, $s(a_{n-1} r^{n-1} + \ldots + a_0 s^{n-1}) = -a_n r^n$

$s \mid a_n r^n$ and $s \mid a_n$.

This theorem is very useful for polynomials of degree ≤ 3. For polynomials of higher degree, it may be

very difficult to determine whether or not the polynomial is prime.

Example 4.1. As an illustration of Theorem 4.a, let $P(X) = 10X^5-15X^4-10X^3+20X^2-5$. If $r/s(r,s) = 1$ is a rational root, then $r|5$ and $r|10$. $r = \pm 1, 5$ and $s = 1, 2, 5, 10$. The possible roots are: 1, 1/2, 1/5, 1/10, -1, -1/2, -1/5, -1/10.

Since $P(1) = 0$, then by 3.o, $P(X) = (X-1)(10X^4-5X^3-15X^2+5X+5)$. In a similar manner, it is found that 1 is also a root of $10X^4-5X^3-15X^2+5X+5$; by 3.10, $P(X) = (X-1)^2(10X^3+5X^2-10X-5)$. Since -1/2 is a root of $10X^3+5X^2-10X-5$, then $P(X) = 10(X-1)^2(X+1/2)(X^2+5)$.

Kronecker's Method

Let $P(X)$ be a polynomial of degree n in $R[X]$. If $P(X)$ is reducible, it will have a factor of degree $\leq \frac{n}{2}$. Let s be the greatest integer $\leq \frac{n}{2}$. Now it is necessary to investigate whether $P(X)$ has a factor $g(X)$ of degree s. Form the function values $P(b_0)$, $P(b_1)$, ..., $P(b_s)$ for s+1 arbitrary integral arguments b_0, b_1. . . . b_s. If $g(X)|P(X)$, then $g(b_0)$ $P(b_0)$; $g(b_1)$, etc. But $P(b_i)$ has a finite number of factors; hence, there are only a finite number of possibilities for each $g(b_i)$, . . , $g(b_s)$. For each possibility, there corresponds one and only one polynomial $g(X)$, which can be found by the aid of Newton's

interpolation formula. Hence, there will be a finite number of polynomials g(X) which are possible factors of P(X).

By 3.3, it can be determined whether or not any of these actually are factors.

Example 4.2. As an illustration of Kronecker's Method, let $P(X) = X^3 + 1$.

$n = 3$ implies $s \leq 1$

$b_0 = 0$ $\quad P(0) = 1$

$b_1 = 1$ $\quad P(1) = 2$

$g(0) \mid P(0)$ implies $g(0) = 1$

$g(1) \mid P(1)$ implies $g(1) = 1$ or $g(1) = 2$.

The possible combinations are:

(1) 1, 1 (2) 1, 2 (3) 2, 1

Checking (1) by Newton's interpolation formula, it is found $g(0) = 1$, $g(1) = 1$.

$g(X) = D_0 + D_1X$ for $X = 0$

$g(0) = D_0 = 1$

$$P(1,X) = \frac{g(X) - g(0)}{X} = D_1 = \frac{1-1}{1} = 0$$

Therefore, $g(X) = 1$, which is a factor.

(2) $g(0) = 0$, $g(1) = 2$

$g(X) = D_0 + D_1X$ for $X = 0$

$g(0) = D_0 = 1$

$$P(1,X) = \frac{g(X) - g(0)}{X} = D_1 = \frac{2-1}{1} = 1$$

Therefore, $g(X) = 1 + X$.

Since $P(X) = (X + 1)(X^2 - X + 1)$, then $g(X)$ is a factor.

(3) $g(0) = 2 \qquad g(1) = 1$

$g(X) = D_0 + D_1X \quad$ for $X = 0$

$g(0) = D_0 = 2$

$$P(1,X) = \frac{g(X) - g(0)}{X} = D_1 = \frac{1-2}{1} = -1$$

$g(X) = 2 - X$.

Since $g(X) \nmid P(X)$, $2-X$ is not a factor.

It is evident that these calculations will usually be prohibitive in length. Frequently, the interest about polynomials is whether a particular polynomial is reducible or irreducible. A simple test or criterion that would give this information would be very useful. No such criterion which will apply to all classes of polynomials has been found, but some tests have been found which give information for particular polynomials. The next sections of this chapter will present some of these criteria.

Lemma 4.b.

Let the polynomials $P(X) = \sum_{i=0}^{n} a_iX^i$, $q(X) = \sum_{j=0}^{m} b_jX^j$ and $h(X) = \sum_{p=0}^{s} c_pX^p$ be in $I[X]$, where I represents the

integers, such that $P(X) = q(X)h(X)$. If P is a positive integer which is a divisor of every coefficient of $P(X)$, then P is a divisor of every coefficient of $q(X)$ or a divisor of every coefficient of $h(X)$.

Proof: Assume that $q(X)$ has at least one coefficient which is not divisible by P and also that $h(X)$ has at least one coefficient which is not divisible by P. Let b_s be the first coefficient of $q(X)$ such that $P \nmid b_s$ and let c_k be the first coefficient of $h(X)$ such that $P \nmid c_k$.

By the statement of the theorem $P(X) = q(X)h(X)$ and by 2.15,

$$(1)\quad a_{s+k} = b_s c_k + (b_{s+1}c_{k+1} + b_{s+2}c_{k-2} + \cdots + b_{s+k}c_0) + (b_{s-1}c_{k+1} + b_{s-2}c_{k+2} + \cdots + b_0 c_{s+k})$$

Now, by the choice of c_k, $P \mid c_{k-1}, c_{k-2}, \ldots, c_0$ consequently, $P \mid b_{s+1}c_{k-1} + \cdots b_{s+k}c_0$ in a similar manner, $P \mid b_{s-1}c_{k+1} + b_{s-2}c_{k+2} + \cdots + b_0 c_{s+k}$

Since $P \mid a_{s+k}$, then $P \mid b_s c_k$ which contradicts the assumption since $P \nmid b_s$ and $P \nmid c_k$.

Lemma 4.c. If $P(X)$ is a polynomial in $I[X]$ and $q(X)$, $h(X)$ are in $R[X]$ such that $P(X) = q(X)h(X)$, where I represents the integers and R the rationals, then there

exists $q_1(X)$ and $h_1(X)$ in $I[X]$ having the same degrees as $q(X)$ and $h(X)$, respectively, such that $P(X) = q_1(X)h_1(X)$.

Proof: If k and e are the l. c. m. of the denominators of the coefficients of $g(X)$ and $h(X)$ respectively, then $q(X) = kq_1(X)$ and $h(X) = eh_1(X)$, where $q_1(X)$ and $h_1(X)$ are in $I[X]$. Therefore,

(1) $keP(X) = q_1(X)h_1(X)$. If P is a prime such that $P \mid ke$, then by 4.b, P must divide all coefficients of $q_1(X)$ or of $h_1(X)$.

Therefore, P can be divided from both sides of (1). This can be done for all the prime factors of ke and finally get:

$$P(X) = q_1(X)h_1(X).$$

It is almost trivial that

$$\deg q(X) = \deg q_1(X) \text{ and } \deg h(X) = \deg h_1(X),$$

which completes the proof of the theorem.

Lemma 4.d. The mapping B of $I[X]$ into $I/(n)[X]$, I represents the integers, defined such that for all $P(X) = \sum_{i=0}^{n} a_i X^i$ in $I[X]$ $B(P(X)) = P'(X)$ where

$$P'(X) = \sum_{i=0}^{n} [a_i] X^i \quad \text{and} \quad [a_i] = a_i'$$

represents the class a_i for every i is an homomorphism of $I[X]$ onto $I/(n)[X]$ for each positive integer n.

Proof: Since for all $P(X) = \sum_{i=0}^{n} a_i X^i$ and

$q(X) = \sum_{j=0}^{m} b_j X^j$ in $I[X]$

(1) $B(P(X)) + q(X)) = B\left(\sum_{t=0}^{MAX(m,n)} (a_t + b_t)X^t\right) =$

$= \sum_{t=0}^{MAX(m,n)} B(a_t + b_t)'X^t = \sum_{t=0}^{MAX(m,n)} (a_t' + b_t')X^t =$

$= \sum_{i=0}^{n} a_i'X^i + \sum_{j=0}^{m} b_j X^j = P'(X) + q'(X) =$

$= B(P(X)) + B(q(X))$

(2) $B(P(X)q(X)) = B \sum_{s=0}^{m+n} \sum_{j+k=s} a_j b_k X^s =$

$= \sum_{s=0}^{m+n} \left(\sum_{j+k=s} a_j b_k \right)' X^s =$

$= \sum_{i=0}^{n} a_i'X^i \sum_{j=0}^{m} b_j'X^j = P'(X)q'(X) =$

$= B(P(X))B(P(X))$.

(3) For every polynomial $P'(X)$ in $I[X]$ such that $B(P(X)) = P'(X)$, thus B is an homomorphism of $I[X]$ onto $I/(n)[X]$.

Lemma 4.e. Let P(X) be a polynomial in $I[X]$ such that deg B(P(X)) = deg P(X), where I represents the integers and B is the mapping defined in 4.c. If B(P(X)) is irreducible in $I/(n)[X]$ then P(X) is irreducible in $I[X]$.

Proof: Let P(X), g(X), h(X) be polynomials in $I[X]$ such that P(X) = g(X)h(X). By 4.d,

B(P(X)) = B(g(X))B(h(X))

Since deg B(P(X)) = deg P(X), then

deg B(g(X)) = deg g(X) and deg B(h(X)) = deg h(X).

Therefore, B(P(X)) is reducible in $I/(n)[X]$. In a similar manner if B(P(X)) is reducible and deg B(P(X))=deg P(X), then P(X) is reducible. This implies that if B(P(X)) is irreducible and deg B(P(X)) = deg P(X), then P(X) is irreducible.

The Lemma 4.e states deg B(P(X)) = deg P(X) because if deg B(P(X)) $<$ deg P(X), then P(X) can be reducible and B(P(X)) can be irreducible. Such is the case when P(X) = $= 4X^2 - 11X - 3 = (4X + 1)(X - 3)$ and n = 2.

B((4X + 1)(X - 3)) = X + 1, which is reducible.

The polynomial $X^3 + X^2 + X + 1$ is irreducible over I/(3) but $w(X^3+X^2+X+1) = X^3+X^2-2X-2 = (X^2 - 1)(X + 1)$. Therefore, if w(P(X)) is reducible in $I/(n)[X]$ for some n, then no conclusions are drawn.

The Lemma 4.e, is useful in proving the criteria known as the Eisenstein's Criteria for irreducibility. Consider the polynomial $P(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$ in $I[X]$ where I represents the integers, and also consider the prime P. If B(P(X)) is reducible, it must be divisible by an irreducible polynomial over I/(P) of degree not exceeding $S \leq n/2$. If no one of the prime polynomials of degree S divides w(P(X)), then by 4.e, P(X) is irreducible. If w(P(X)) is reducible over I/(P), then no conclusions are drawn, and then it is possible to choose either a different prime or P^2. When P^2 is chosen, the situation is handled by Eisenstein's Criteria for irreducibility.

Theorem 4.f. (Eisenstein's Criteria)

If $P(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$ is a polynomial in $I[X]$ and let P be a prime such that $P \mid a_i$ $i = 0, 1, \ldots n-1$, $P \nmid a_n$ and $P^2 \nmid a_0$, then P(X) is irreducible, over integers I.

Proof: Suppose P(X) is reducible in $I/(P^2)$. By 3.7

$$a_0 + a_1X + \ldots + a_nX^n = (b_0 + b_1X + \ldots + b_mX^m)(c_0 + \ldots c_kX^k).$$

By 2.15:

$$a_0 = b_0c_0$$

Since $P \mid b_0c_0$, then P divides c_0 or P divides b_0 or P divides both c_0 and b_0.

Assume $P \mid c_0$ and $P \mid b_0$.

$b_0 = Pk_1$

$c_0 = Pk_2$

$b_0c_0 = P^2k_1k_2$, then

$P^2 \mid b_0c_0$, which contradicts the statement of the theorem. Therefore,

$P \mid c_0$ or $P \mid b_0$.

Suppose $P \nmid c_0$, then $P \mid b_0$.

$a_n = b_m c_k$

$P \nmid a_n$

$P \nmid b_m c_k$

$P \nmid c_k$

Choosing s as the smallest positive integer such that $P \mid c_s$, $0 < s \leq k$ By 2.15,

$a_s = b_0c_s + b_1c_{s-1} + \cdots + b_sc_0$. By the choice of s, $P \nmid b_0c_s$, and P divides all other terms of a_s. Then $P \nmid a_s$.

Since a_n is the only coefficient of P(X) such that $P \nmid a_n$, then $s = k = n$. Therefore, one of the factors will have degree n which makes P(X) irreducible over $I/(P^2)$.

Obviously, for any positive integer n, there exists polynomials of degree n over I that are prime over I.

Given $n = 4$ and $P = 5$, it is very easy to construct the polynomial $10 + 15X + 5X^2 + 25X^3 + 3X^4$, which is irreducible over I.

Theorem 4.8.

Let D be an integral domain. The mapping A from $D[X]$ into itself defined such that $A(a) = a$ for every polynomial constant in $D[X]$. For all $P(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$, in $D[X]$.

$A(P(X)) = P(X + 1)$ is an homomorphism.

Proof:

(1) For the constant polynomial the proof is trivial.

Now consider $P(X) = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$, and $q(X) = \sum_{j=0}^{m} b_j X^j$, $b_m \neq 0$, in $D[X]$.

$$(2)\quad A(P(X) + q(X)) = A \sum_{t=0}^{MAX(m,n)} (a_t + b_t)X^t =$$

$$= \sum_{t=0}^{MAX(m,n)} (a_t + b_t)(X + 1)^t =$$

$$= \sum_{i=0}^{n} a_i (X + 1)^i + \sum_{j=0}^{m} b_j (X + 1)^j =$$

$$= P(X + 1) + q(X + 1) = A(P(X)) + A(q(X))$$

$$(3)\quad A(P(X)q(X)) = A \sum_{s=0}^{m+n} \sum_{j+k=s} a_j b_k X^s \quad =$$

$$= \sum_{s=0}^{m+n} \sum_{j+k=s} a_j b_k (X+1)^s =$$

$$= \sum_{i=0}^{n} a_i (X+1)^i \sum_{j=0}^{m} b_j (X+1)^j = P(X+1)\, q(X+1) =$$

$$= A(P(X))A(q(X)).$$

Obviously deg A(P(X)) = deg P(X), and by Lemma 4.e, if A(P(X)) is irreducible, so will be P(X).

An application of the Theorems 4.f and 4.g are the polynomials called cyclotomic.

Definition 4.1. A complex number w is said to be a primite n^{th} root of unity if and only if $w^n = 1$, but $w^m \neq 1$ for any positive integer m n.

If $w = e^{2\pi/n} = \text{Cos } 2\pi/n + \text{Sin } 2\pi/n$, then w is a primitive, n^{th} roots of 1.

Definition 4.2. The polynomial $Qn(X) = \prod(X - w)$ where this product is taken over all the primitive n root of unity is called cyclotomic polynomial.

For example:

$Q_1(X) = X - 1$

$Q_2(X) = X + 1$

$Q_3(X) = (X - (1/2 + i\sqrt{3}/3)(X-(-1/2-i\sqrt{3}/2) =$

$= X^2 + X + 1$

Theorem 4.h.

$Q_n(X)$ is a monic polynomial with integer coefficients.

Proof: Consider the polynomial X^n-1 over the complex number such that $X^n-1 = \prod(X - a)$, where this product is taken over all a satisfying $a^n = 1$. By previous theorems in group theory this primitive root exists.

It is possible to write X^n-1 as follows:

$X^n-1 = \prod_{d|n} Q_d(X)$.

If $n = 1$ (using induction on n) $Q_1(X) = X - 1$, which is a monic polynomial with integral coefficients, then theorem is true for $n = 1$.

Assume the theorem is true for $k \leq n$ where k is an integer. Since $d|n$, then $d \leq n$ and by the induction assumption $Q_d(X)$ is a monic polynomial with integral coefficient. If $Q_d(X)$ is known for all positive $d < n$, then $Q_d(X) \mid \prod Q_d(X)$, and $\prod Q_d(X) = Q_n(X)g(X)$ where $g(X)$ is monic polynomial with integral coefficients, which implies that $X^n-1 = Q_n(X)g(X)$. Therefore, $Q_n(X) = X^n-1/g(X)$. By actual division, $Q_n(X)$ is a monic polynomial with integral coefficient.

Example 4.1. Consider the cyclotomic polynomial $P(X) = X^4 + X^3 + X^2 + 1$ in this polynomial does not exist such a prime which satisfies Eisenstein's Criteria.

In $A(P(X)) = (X + 1)^4 + (X + 1)^3+(X+1)^2+(X+1)+1 =$
$= X^4 + 5X^3 + 10X^2 + 10X + 5$. 5 divides all coefficients except 1 and $5^2 \nmid 5$.

By 4.g, P(X) is irreducible.

In general, given the cyclotomic polynomial

$$P(X) = 1 + X + \ldots + X^{P-1}$$

$$(X - 1)P(X) = X^{P}-1.$$

$$A((X-1)P(X)) = A(X-1)A(P(X)) = A(X^{P} - 1) =$$

$$= XA(P(X)) = (X + 1)^{P} - 1 = X^{P} + PX^{P-1} + \binom{P}{1} X^{P-2} + \ldots$$

$$\ldots + \binom{P}{P-1}X$$

$$A(P(X)) = X^{P-1} + \binom{P}{1}X^{P-2} + \ldots + \binom{P}{P-1}$$

Since $\binom{P}{V} = \dfrac{P(P-1)\ (P-2)\ \ldots\ (P-(v-1))\ (P-v)!}{v!(P-v)!} =$

$= \dfrac{P(P-1)(P-2)\ \ldots\ P-v+1}{v!}$, then P divides all the coefficients except the coefficient of X^{P-1}.

The constant term $\binom{P}{P-1} = \dfrac{P(P-1)!}{(P-1)!(P-P+1)!} = P$

is not divisible by P^2. Therefore, P(X + 1) is irreducible, and so is P(X).

There are many irreducible polynomials such as $X^2 + 1$ to which the criterion will not apply. This means that all the polynomials that satisfy the criteria are irreducible, but it does not mean that the polynomials that do not satisfy the criteria are reducible.

CHAPTER V

SUMMARY

This thesis contains definitions and theorems concerning the development of the polynomial ring in Section 2A of Chapter II. In Section 2B of the same chapter, the development of the polynomial ring was presented. Theorem 2.d in the same section shows that the polynomial ring $R[X]$ is an integral domain.

Chapter III presents in Section 3A, some properties of the polynomial ring, such as the division algorithm, the existence of the greatest common divisor in the polynomial ring, the Euclidean Algorithm, the factorization of a polynomial, and Theorem 3.m, which shows the existence of a homomorphism from $R[X]$ into $R[S]$.

Section 3B contains the remainder theorem, the factor theorem and some other theorems concerning roots and factorizations of polynomials. The Newton's interpolation formula is also in this section. In the fourth chapter, some general tests for irreducibility were presented, such as Theorem 4.a, the Kronecker method and the Eisenstein criteria. In order to present an application of the Eisenstein's criteria, the cyclotomic polynomial was defined. It was proved that the cyclotomic polynomial is a monic polynomial.

BIBLIOGRAPHY

BIBLIOGRAPHY

BOOKS

1. Beamont, Ross A., and Ball, Richard W. Introduction to Modern Algebra and Matrix Theory. New York: Holt, Rinehart, Wiston, 1954.

2. Birkhoff, Garrett, and Saunders, MacLane. A Survey of Modern Algebra. New York: The MacMillan Company, 1941.

3. Lewis, Donald J. Introduction to Algebra. New York: Harper and Row Publishers, 1965.

4. McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.

5. Hersteinn, I. N. Topics in Algebra. New York, Toronto, London: The MacMillan Company, 1964.

6. van der Wearden, B. L. Modern Algebra. Vol. 1. (Published by authority Attorney General of the U. S.) New York: Frederick Ungar Publishing Company, 1949. Translated by Fred Blum.