IRREDUCIBILITY OF POLYNOMIALS

BY

Md. Mahatabuddin

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Science.

McGill University
Montreal

March 1964

Gratitude is owing to Professor H. Schwerdtfeger for his kind help and encouragement.

TABLE OF CONTENTS

CHAPTER I

Prerequisites

In many mathematical investigations such as determination of degree of a field extension, determination of the Galois group etc. the knowledge of ineducibility of a polynomial f(x), or if reducible the nature of the irreducible factors of f(x) are desired. We wish to give here a brief survey of the polynomial domain, factorisation in such a domain and the criteria by which non factorisability of a polynomial in such a domain can be determined. We shall try to make the contents self supporting and self explanatory as much as possible within the scope of our present work.

1. Definitions:

(a) Elements: Objects of investigation in mathematics are numbers, symbols, points, lines and various other things. These will be denoted by the general name "element".

(b) Sets: A collection of elements will be called a "set" A. The set A is formed by collecting together certain elements having a given property p. For example, if the elements are students and property p is the property of being "student of McGill University", then A will be the set of all students of McGill University. If an element "a" has the property "p" then a is said to be an element of the set "A": This is technically denoted as $a \in A$: and is read as "a belongs to A".

(c) Subset: If every element of a set A is an element of another set B then A will be called a subset of B. This in notation we shall write $A \subseteq B$.

(d) Composition: A composition in a set A is an operation by which every pair of elements a, b of the set A is composed to form an element of the same set A.

We call a composition either addition or multiplication or by such similar names. The addition or multiplication of a, b will be denoted as respectively by a+b and ab. The choice of these names are quite arbitrary and what is called addition may be called multiplication and vice versa.

In a set A there may be more than one composition.

(e) A composition, say addition, in A is called

(i) Associative, if a+(b+c) = (a+b)+c, $\forall a,b,c \in A$, $\forall$ = for every

(ii) Commutative, if a+b=b+a, $\forall a,b \in A$,

(f) Two compositions, say addition and multiplication, in A are called (left) distributive, if a(b+c) = ab+ac, (right) distributive, if (a+b)c = ac+bc.

(g) Semigroup: If in a set A a composition is defined and the composition thus defined is associative then A is called a semigroup (w.r.t. the composition).

Thus A is a semigroup w.r.t. addition if for every $a,b,c \in A$

(i) $a+b \in A$

(ii) $(a+b)+c = a+(b+c)$.

(h) Group: A set A is called group (w.r.t. addition) if for every $a,b,c \in A$

(i) $a+b \in A$,

(ii) $(a+b)+c = a+(b+c)$,

(iii) the equations $a+x = b$, $y+a = b$ are solvable in A.

If the composition is addition the group is called additive. Similarly one can define a multiplicative group.

The property (iii) in the definition of the group is equivalent to the property

(iii)* $\exists$ (there exists) in A an element, say 0, to be called zero or additive identity element such that $a+0=0+a=a$, $\forall a \in A$, and $\forall a \in A \exists$ in A an element, say, $-a$ and called the additive inverse of a, such that $a+(-a)=a-a=-a+a=0$.

We shall denote the multiplicative identity and the multiplicative inverse of a by 1 and a^{-1} respectively, whenever the composition is multiplation and these elements exist in A.

Theorem: In a group the equations $a+x=b$, $y+a=b$ are solvable uniquely.

Proof: Let z be a fixed solution of $y+a=0$ i.e. $z+a=0$.

Now $z+(a+x)=z+b$

or $(z+a)+x=z+b$

or $x=z+b \Rightarrow$ every solution is $z+b$.

(i) Commutative group: If the group composition is commutative then the group is called a commutative group or an abelian group.

Examples (i) The set of all integers form a semigroup w.r.t. both addition and multiplication.

(ii) The set of all integers form a commutative group w.r.t. ordinary addition but not w.r.t. multiplication.

(j) Ring: Let a set R is a group w.r.t. addition and semigroup w.r.t. multiplication such that the addition and the multiplication is connected by the distributive laws, then R is called a ring.

Thus a set R with two compositions, say addition and multiplication is a ring if for every $a,b,c \in R$

(i) $a+b,\ ab \in R$,

(ii) $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$,

(iii) $a+x=b$, $y+a=b$ solvable in R

(iv) $a(b+c)=ab+ac$, $(a+b)c=ac+bc$.

A ring may or may not be commutative w.r.t. either or both of the compositions.

In a ring R

$a+0=a=0+a$ for any $a \in R$.

Multiplying by $b \in R$, $b(a+0)=ba$

or $ba+b0=ba$

but $ba+0=ba$

As R is additively a group, the equation $ba+x=ba$ has only one solution and hence

$$b0=0$$

Similarly one can prove that $0b=0$

Thus the additive identity 0 of the ring R has the property $0b=b0=0, \forall\ b \in R$

On account of this peculiar property, the additive identity is called 'a zero elelment of R'.

In a ring R, only the additive identity has this porperty for, if 0_1 in any other element having this property, then

$$0=00_1=0_1$$

As $a0=0$ and $0a=0$, it follows that if one factor is zero then the product is zero.

But the converse is not necessarily true in a ring. It may happen that $ab=0$ but $a \neq 0$, $b \neq 0$. In such a case a is

called a left divisor of zero relative to b and b is called a right divisor of zero relative to a. If R is commutative then the left divisors are also right divisiors. But in general it is not so.

Example. All square matrices of order n over a ring R form a ring $M_n(R)$. But this ring is not multiplicatively commutative and it has divisors of zero.

For take n=2, $A=\begin{pmatrix}2&4\\-1&-2\end{pmatrix}$, $B=\begin{pmatrix}0&2\\0&-1\end{pmatrix}$. Then $A\neq((0))$, $B\neq((0))$ but $AB=\begin{pmatrix}0&0\\0&0\end{pmatrix}=((0))$ and $BA=\begin{pmatrix}-2&-4\\1&2\end{pmatrix}\neq((0))$

If R has no divisors of zero i.e. $ab=0\Rightarrow a=0$ or $b=0$ or both $=0$ then R is called a ring without divisors of zero.

Theorem: A ring R is without divisors of zero iff the cancellation law: if $c\neq0$ and $ac=bc$ or $ca=bc$ or $ca=cb$ then $a=b$, holds.

For if R has no divisors of zero then $ac=bc\Rightarrow(a-b)c=0$ by the distributive law, but $c\neq0$ and there exists no divisor of zero $\Rightarrow a-b=0\Rightarrow a=b$. Conversely if the cancellation law holds and $ac=0$ with $c\neq0\Rightarrow ac=0=oc$ hence cancelling c, we get $a=0$ i.e. there exists no divisor of zero.

In a ring, the commutative law of addition is a consequence of the other laws in most cases. Indeed one can prove the theorem:

In a ring R addition is commutative if there exists in R at least one element which is not a left divisor (or a right divisor) of zero.

Proof:- In R, calculate the product $(a+b)(c+d)$ in two ways

$$(a+b)(c+d)=(a+b)c+(a+b)d=(ac+bc)+(ad+bd)$$

Again $(a+b)(c+d)=a(c+d)+b(c+d)=(ac+ad)+(bc+bd)$

$\therefore$ $ac+(bc+ad)+bd=ac+(ad+bc)+bd$ by associative law.

$\therefore$ cancelling, $bc+ad=ad+bc$

Putting $c=d$, $bc+ac=ac+bc$

or $[(b+a)-(a+b)]c=0$

choosing c not a right divisor of zero we get

$$(b+a)-(a+b)=0$$

i.e. $b+a=a+b$

(k) Integral domain: A (multiplicatively) commutative ring without divisors of zero is called an integral domain.

As the elelments of a ring R do not necessarily form a group w.r.t. multiplication, R may or may not contain the multiplicative identity 1 i.e. an element 1 such that

$a1=1a=a, \forall a \in R$.

For brevity we shall sometimes refer an integral domain by simply "a domain".

(l) Units of a ring: Let a ring R contains 1, then the elements $a \in R$ for which a^{-1}, with the property $aa^{-1}=a^{-1}a=1, \in R$ are called units of R.

It is easy to prove that the units of R form a multiplicative subgroup of R.

(m) Skew field: A ring is called a skew field if its non zero elements form a multiplicative group.

Some properties of the skew field F are evident.

(1) There exists always an identity element 1 in F such that

$a1=1a=a, \forall a \in F$.

(2) To each element $a \neq 0 \in F \exists$ an inverse a^{-1} such that

$$aa^{-1}=a^{-1}a=1$$

(3) A skew field has no divisors of zero

For if $ab=0$ and $a \neq 0$ then $0=a^{-1}0=a^{-1}(ab)=(a^{-1}a)b=b$

(4) If $a \neq 0$, $ax=b$, $ya=b$ are uniquely solvable.

(n) Field: A skew field in which multiplication is commutative is called a field.

Thus a set F with two compositions, addition and multiplication is a field if for every $a,b,c \in F$

(i) $a+b$, $ab \in F$,

(ii) $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$,

(iii) $a+b=b+a$, $ab=ba$,

(iv) $a+x=b$, $ax=b$, $a \neq 0$ in the 2nd case, are solvable,

(v) $a(b+c)=ab+ac$.

Examples: The set of all rational numbers, the set of all real numbers, the set of all complex numbers are examples of fields.

Obviously in a field every nonzero element is an unit. If $A \subseteq B$ and A and B are both fields such that the compositions of A are the compositions of B then A is called a subfield of B. Similarly one defines subgroups, subrings etc.

(o) Order of an element: Let a be an element of a group G (say additive) then $a+a=2a \in G$, $2a+a=3a \in G$ and so $na \in G$, for any positive integer n. on the other hand $-a \in G$ and $-a-a=-2a \in G$ and so $-na \in G$, for any positive integer n. Thus, if $a \in G$ then $na \in G$ for all integral values of n, positive or negative, with the convention $0.a=0$ (additive identity of the group).

Two distincts cases may occur. All elements

$\ldots,-ha,\ldots,-ka,\ldots,-2a,-a,\ 0a=0,a,2a,\ldots,ka,\ldots,ha\ldots$

may or may not be distinct.

1) If all multiples ha are distinct, the element a is said to be of order zero.

2) If all multiples are not distinct, let $ha=ka$, $h>k$ for some integers h,k.

$\therefore (h-k)a=0$

Let n be the smallest positive integer for which $na=0$. Then $na=0,a,2a,\ldots,(n-1)a$ are all distinct. For $ha=ka$, $0\leq k<h<n \Rightarrow (h-k)a=0$ where $h-k<n$ which contradicts the assumption that n is the smallest such integer. Now if m is any integer then m can be expressed as

$m=qn+p,\ 0\leq p<n$

$ma=(qn+p)a=q(na)+pa=0+pa=pa$

Thus all multiples are expressed by, $0a=0,a,2a,\ldots,(n-1)a$. Here n is called the order of the element a.

(p) Quotient field: Let R be an integral domain with elements a,b,c,... For every pair of elements (a,b) with $b\neq 0$ construct the fractions $\frac{a}{b}$. Define $\frac{a}{b}=\frac{c}{d}$ iff $ad=bc$. Then obviously i) $\frac{a}{b}=\frac{a}{b}$; (ii) $\frac{a}{b}=\frac{c}{d} \Rightarrow \frac{c}{d}=\frac{a}{b}$ and (iii) $\frac{a}{b}=\frac{c}{d}$ and $\frac{c}{d}=\frac{g}{h} \Rightarrow \frac{a}{b}=\frac{g}{h}$

So if we consider the class of all equal fractions then these classes have no common element unless they are identical. Denote the class in which $\frac{a}{b}$ occurs by $\frac{a}{b}$.

Define addition and multiplication of the classes by the rules $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$ and $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$ respectively.

Then under these definitions of addition and multiplication

the classes form a field. Denote this field by Q(R). Q(R) is called the quotient field of R.

(q) Characteristic of a ring (or of a field):

The characteristic of a ring R (or of a field F) is defined to be the integer which is the least common multiple of the additive orders of all elements of R (or of F). In case there exists no such finite integer then the characteristic of the ring (or field) is said to be zero. Thus if p is characteristic of R, $pa=0$, $\forall a \in R$.

Theorem: The non zero characteristic of a ring without divisors of zero must be a prime integer p.

Proof: If possible let the characteristic $p \neq 0$ be not prime. Then $p = rs$ where, say, r is a prime integer.

$$\text{Now } (ra)(sb) = (a+\ldots+a)(b+\ldots+b)$$
$$= ab+ab+\ldots+ab, \text{ by the distributive law}$$
$$= (rs)(ab)=p(ab)$$

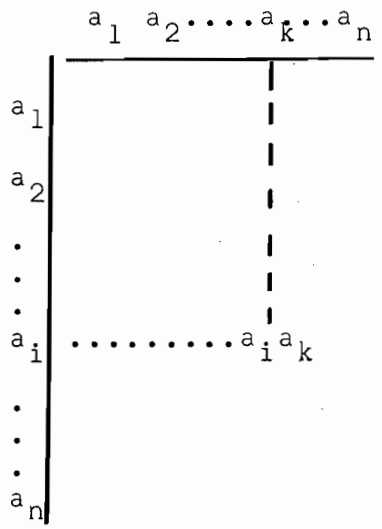
As p is the characteristic $p(ab)=0 \Rightarrow (ra)(sb)=0$. As there exists no divisors of zero, one factor, say $ra=0$.

$$\text{But } 0=(ra)b=(a+\ldots+a)b=ab+ab+\ldots+ab$$
$$=a(b+\ldots+b)=a(rb)$$

Taking $a \neq 0$ one gets $rb = 0$. Thus r is the common multiple of the orders of a and b and as a,b are arbitrary, r is the characteristic. Contradicting p is the characteristic.

Theorem: A finite integral domain is a field.

Proof: Let $a_1, a_2, \ldots, a_n$ be the elements of the integral domain. Construct the multiplication table.



Then in the row of products with any given element say a_i, all elements must occur.

For if not let any element say a_p is repeated twice i.e. $a_i a_r = a_p = a_i a_s$ where $a_r \neq a_s$

$$\therefore a_i(a_s - a_r) = 0$$

But $a_i \neq 0$, $a_s - a_r \neq 0 \Rightarrow$ the integral domain has divisions of zero, Contradiction.

Then the equation $a_i x = a_j$ is solvable. For a_j occurs somewhere in the row and x is then the colum head. Similarly $y a_i = a_j$ is solvable. Hence the theorem.

Theorem: The characteristic of a finite ring R is an integer $\neq 0$.

Proof: For if $a \in R$, $na = a+a+..+a \in R$

As R is finite there exists some least positive integer p such that $pa=0$. Then the least common multiple of all such p's will be characteristic.

Theorem: In an integral domain R of characteristic p,

$(a \pm b)^p = a^p \pm b^p$; $(a \pm b)^{p^f} = a^{p^f} \pm b^{p^f}$

Proof: As the multiplication is commutative, and distributive law holds in R, the ordinary binomial theorem for the positive integral index holds in R.

$$\therefore (a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{p}b^p$$

but $\binom{p}{i} = \frac{p!}{i!\,(p-i)!} = \frac{p(p-1)\ldots(p-i+1)}{i!} = p.k,$

since p is prime, k is a positive integer if $i < p$.

So all the middle terms are p multiple of an element of R, so they are zero. Hence the result.

Similar is the case with the other forms.

Let F be a proper subfield of F^1 i.e. $F \subset F^1$ and both are fields w.r.t. the same compositions. The field F^1 is called an extension of the field F. The process by which F^1 may be obtained from F is called the process of extension.

The smallest subfield of a field is called a <u>prime field</u>.

Theorem: The prime field of a field is unique.

Proof: For, if F_1 and F_2 are two prime fields of a field F, then $F_3 = F_1 \cap F_2$ = the set of common elements of F_1 and F_2, is a field. F_3 is non empty, since $0, 1 \in F_3$. Moreover $F_3 \subseteq F_1$. $F_3 \subset F_1$ $\Rightarrow F_1$ is not prime. Hence $F_3 = F_1$. Similarly $F_3 = F_2$.

$$\therefore F_3 = F_1 = F_2$$

Let F be a subfield of F^1 then the identity 1 is common to both F and F^1. Now for any integer p and any $a \in F$

$$pa = a+a+\ldots+a, \text{ p terms}$$
$$= 1.a + a.1 + \ldots + 1.a$$
$$= (1+1+\ldots+1)a$$
$$= (p1)a$$

So if pl = 0 then (pl)a = 0a=0, i.e. pa=0 $\forall a \in F$, i.e. characteristic of F is the additive order of 1. As 1 is common to both F and F^1, they have the same characteristic.

If the characteristic of F is $p \neq 0$, then the prime field of F will generally be represented by F_p or by R_p Evidently the characteristic of F_p is p.

Example: If R is the domain of common integers and p is a prime integer then $R_p = \{(rp+q: r=0,\pm1,\pm2,\ldots): q=0,1,2,\ldots p-1\}$ i.e. the residue class of integers mod p form an integral domain. R_p has only a finite number of elements. Hence, by a previous theorem, R_p is a field. The characteristic of this field is p and this field has no subfield. So R_p is a prime field.

But if p is not a prime integer then R_p is a ring of characteristic p, having divisors of zero. For, if p=rs then $(r) \neq (0)$, $(s) \neq (0)$ but (r)(s) = (rs)=(p)=(0).

(r) Homomorphism and isomorphism.

Let A of elements a,b,c,... and A^1 of elements $a^1, b^1, c^1, \ldots$ be two sets. Let each have one composition, say, multiplication. Now let there exists between A and A^1 a unique correspondence.

$$h: \quad A \longrightarrow A^1$$

such that every element of A corresponds with certain element of A^1 and that if by h, $a \longrightarrow a^1$, $b \longrightarrow b^1$

then $ab \longrightarrow a^1b^1$

Put $a^1=h(a)$, $b^1=h(b)$, $(ab)^1 = h(ab)$

Then $h(ab) = (ab)^1 = a^1b^1 = h(a)h(b)$.

A correspondence h: $A \longrightarrow A^1$ having this property viz.

$$h(ab) = h(a)h(b)$$

is called a homomorphism of A into A^1. If every element of A^1 has correspondence with certain element of A then the homomorphism H is called onto.

Let h is onto, then through the correspondence h: $a \longrightarrow a^1$ is unique, the inverse corespondence h^{-1}: $a^1 \longrightarrow a$ may not be unique. In other words, though one element a corresponds to one element a^1 by h, yet one element a^1 may correspond to many element a by h^{-1}.

If h^{-1} is also unique i.e. if h is $1 \longleftrightarrow 1$, then h is called an isomorphism between A and A^1. In notation $A \simeq A^1$.

As the isomorphism is biunique

$$A \simeq A' \text{ implies } A' \simeq A.$$

For, $h^{-1}[h(ab)] = h^{-1}[h(a)h(b)]$, by the condition of homomorphism h

$$\therefore ab = h^{-1}(a^1b^1)$$

$$\text{i.e. } h^{-1}(a^1)h^{-1}(b^1) = h^{-1}(a^1b^1)$$

Thus h^{-1} is also a homomorphism.

If A and A^1 has two compositions, say addition and multiplication, then the correspondence

$$h: A \longrightarrow A^1$$

is a homomorphism if $a \longrightarrow a^1$, $b \longrightarrow b^1$ implies

$$ab \longrightarrow a^1b^1, \quad a+b \longrightarrow a^1 + b^1$$

In other words a homomorphism $h: A \longrightarrow A^1$ is such that

$$h(ab) = h(a)h(b); \quad h(a+b) = h(a)+h(b)$$

As before h is isomorphism if h is biunique i.e. when h is $1 \leftrightarrow 1$.

(s) Classes of residues:

We have already given an example R_p of classes of residues mod p where R is the domain of common integers and p is a prime integer.

Now let R be an arbitrary integral domain with identity 1. Then it can be verified that all elements rq, $r \in R$ and q a fixed element of R, form an integral domain (0), which is a subdomain of R.

If q is not an unit then this domain does not contain 1.

Moreover if $x \in R, y \in (0)$ then $xy=yx=rqx=xrq=r_1 q \in (0)$.

$$\therefore R.(0) \subseteq (0)$$

A subdomain of R which satisfies this property is called an ideal in R.

Now let us establish a relation α, called congruence relation, between the elements of R such that $a \alpha b$ iff $a-b \in (0)$ i.e. iff $a-b=rq$ for some $r \in R$.

Then

(i) $a \alpha a$, for $a-a=0=0q \in (0)$

(ii) $a \alpha b \Rightarrow b \alpha a$, for if $a-b=rq$ then $b-a=(-r)q$

(iii) $a \alpha b$, $b \alpha c \Rightarrow a \alpha c$, for $a-b=r_1 q, b-c=r_2 q \Rightarrow a-c=a-b+b-c$

$$=(r_1+r_2)q = r_3 q$$

Thus under the relation α the elements of R is divided into distinct disjoint subsets of R such that if a,b belong to the same subset of R then $a-b=rq$ for some $r \in R$. In this case a is called congruent to b mod q and denoted as $a \equiv b$, mod q. Denote the subset in which a belongs by (a).

The subsets thus obtained may be considered as new algebraic elements. They form a set R_q, called the classes of residues mod q.

Now if $a \alpha b$, $c \alpha d$ then $a-b=r_1 q$, $c-d=r_4 q$

$\therefore$ $a-b+c-d = (a+c)-(b+d)=(r_1+r_4)q$

$ac-bd=(r_1 d+r_4 b+r_1 r_4 q)q$

i.e. $\{a+c\} \alpha \{b+d\}$ and $ac \alpha bd$.

Because of this property of α one can define addition and multiplication between the elements of R_γ as follows,

$(a)+(b) = (a+b)$, $(a)(b) = (ab)$.

Then under this definition of addition and multiplication R_γ is a commutative ring.

For further properties of R_γ we shall give a theorem in the next article.

2. Factorisation in an Integral domain

Let R be an integral domain. In R an element c is said to be divisible by a if there exists another element b such that

$c=ab$

Both a and b are called divisors or factors of c. In notation we shall write this as $a \mid c$ (or $b \mid c$). Let R contain units. Then if e is any unit and a an arbitrary element then

$a=ee^{-1}a=ek$, where $k=e^{-1}a$.

Thus every unit is a divisor of every element. If c=ab and a or b or both are units then we say c has only trivial factors.

Let e is an unit and a arbitrary element of R then

ae is called an "associate" of a. Thus if U is the group of units of R, then the set of all associates of a is

$$(a)=aU=\{ae: e\in U\}$$

For, if b is any associate then $b=ae, e\in U$.

An element which is not an unit and is not divisible by any element other than by its associates and units is called a prime element.

If $(a) = (p_1)^{r_1}.(p_2)^{r_2}.....(p_n)^{r_n}$, where p_i are prime elements and $r_1, r_2, \ldots, r_n$ are positive integers, n being finite, then a is called factorisable and this representation is called a factorisation of (a).

As $(a) = aU$ and $(p_i) = p_i U$

$$(a)=aU= p_1^{r_1}U^{r_1}p_2^{r_2}U^{r_2}\ldots p_n^{r_n}U^{r_n}$$

$$= Up_1^{r_1}p_2^{r_2}\ldots p_n^{r_n}$$

$$\text{i.e. } a = ep_1^{r_1}p_2^{r_2}\ldots p_n^{r_n}, \quad \text{where } e\in U.$$

Thus if this representation exists for a, with finite n, then a is called factorisable. If every element $a \neq 0$ of an integral domain R is factorisable then R is said to be a factorisable domain.

Theorem: A factorisable domain must contain prime elements.

Proof: For, otherwise a will have infinite factors.

Theorem: A factorisable domain must contain the identity 1.

Proof: For take a prime $p\in R$. Then since p is factorisable $p = ep' \Rightarrow$ R has units $\Rightarrow$ R has the identity 1.

If every nonzero element $a\in R$ has the unique representation $(a)=(p_1)^{r_1}.(p_2)^{r_2}....(p_n)^{r_n}$ in R/U, where R/U is the set

of all classes of associated elements of R, then R is called a <u>domain of unique factorisation.</u>

Thus in R, two factorisations of the element a

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} = q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s},$$

are such that there exists a one to one correspondence between the prime elements p_i and q_j, such that the corresponding primes being associated.

Examples: 1. The set of all integers form a domain of unique factorisation.

2. The set of all even integers form an integral domain. This domain does not contain the multiplicative identity 1. This is not a factorisable domain. For example 6 has no factor in this domain.

3. An example of a domain of nonunique factorisation is $c(\sqrt{-6}) = \{a+b\sqrt{-6} : a,b \text{ being integers}\}$.

In $c(\sqrt{-6})$, $6 = 2 \cdot 3 = -(\sqrt{-6})^2$

But $\sqrt{-6}$ is not associated to 2 or 3 as ± 1 are the only units of this integral domain.

Theorem: The necessary and sufficient condition that an integral domain R with identity 1 is factorisable is that there should exist a norm N(a) for each $a \neq 0$ such that

$N(a) = \text{integer} \geq 0$;

$N(ab) \geq N(a)$, where the equality holds only when b is a unit.

Proof: Let R be factorisable, then for $a \in R$

$a = e_1 p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$, p_i being primes, r_i positive integers, e_1 unit.

There might be more than one factorisation.

Take $N(a) = \min (r_1 + r_2 + \ldots + r_n)$.

As r_i are integers ≥ 0, $N(a) \geq 0$.

If $N(a)=0$, all r_i are zero $\Rightarrow$ a is a unit.

Next let $b = e_2 q_1^{s_1} q_2^{s_2} \ldots q_m^{s_m}$, where q_i are primes.

Then $ab = e_1 e_2 p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n} q_1^{s_1} q_2^{s_2} \ldots q_m^{s_m}$

$N(ab) = \min (r_1 + r_2 + \cdots + r_n + s_1 + s_2 + \cdots + s_m)$

$\geq \min (r_1 + r_2 + \cdots + r_n)$, as $s_1 + s_2 + \cdots + s_m \geq 0$.

Hence the equality holds only when $s_1 + s_2 + \cdots + s_m = 0$.

Hence $N(ab) \geq N(a)$ where the equality holds only when b is a unit.

Thus the condition is necessary.

The condition is also sufficient. For let there exist a norm function N(a) satisfying the conditions and let R be nonfactorisable. Let $a \neq 0$ be a non factorisable element. Then a is neither a unit nor a prime, for these are factorisable.

So a must be divisible by another element a_1, not associated to it.

$$\therefore \quad a = a_1 b_1$$

Here at least one factor, say b_1, is non factorisable. Otherwise a becomes factorisable

Now $N(a) = N(a_1 b_1) > N(b_1)$ as a_1 is not a unit.

As the norms are positive integers,

$$N(a) \geq N(b_1) + 1$$

As b_1 is again nonfactorisable, the argument can be repeated and if b_2 be a nonfactorisable factor of b_1

$$N(b_1) \geqslant N(b_2)+1$$

$$\therefore\ N(a) \geqslant N(b_2)+2$$

Repeating this n times

$$N(a) \geqslant N(b_n)+n,$$

where n is any integer.

As n can be as large as we like. N(a) does not exist. This contradicts our assumption. Hence D is factorisable.

Theorem: The necessary and sufficient condition that a factorisable domain R is a domain of unique factorisation is that a product ab is divisible by a prime element p, if and only if one factor is divisible by p.

Proof: The condition is necessary.

For let the factorisation be unique and

$$a = e_1 p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

$$b = e_2 q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}$$

Then $c = ab = e_1 e_2 p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}$.

If the prime p divides one of the factors a and b then p is associated to one of the primes p_i (or q_j). As p_i (or q_j) occurs in the factorisation of c, c is also divisible by p. On the other hand if c is divisible by p, then p is associated to one of p_i or q_j.

Hence either a or b is divisible by p. Thus the condition holds in R.

The condition is also sufficient.

For let the condition holds in R. If possible let there exist two factorisations of an element a.

$$a = e_1 p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$
$$= e_2 q_1^{l_1} q_2^{l_2} \cdots q_s^{l_s}$$

Then the prime p_i divides a and hence by the given condition at least one of the primes q_i, say q_j, is divisible by p_i. As both p_i and q_j are primes they are associated. As this is true for every pair p_i and q_j, the two factorisatiosn are same. Hence the factorisation is unique in R.

In a factorisable domain R, a common factor d of two elements a and b which is such that every common factor of a and b is a factor of d is called the heighest common factor (abbreviated: h.c.f.) of a and b. This we shall denote by (a,b).

Evidently h.c.f. d=(a,b) is determined except for a unit .

If (a,b)=e = an unit, then a is called relatively prime to b.

Similarly one can define the least common multiple (abbreviated: l.c.m.) of two elements a,b as the element m which is such that both a,b are factors of m and every common multiple of a,b is a multiple of m. In notation m= [a,b].

Theorem: If the factorisation in R is unique then both h.c.f. and l.c.m. exist for every pair of elements a,b; $a \neq 0, b \neq 0$.

Proof: For, let

$$a = e_1 p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$
$$b = e_2 p_1^{s_1} p_2^{s_2} \cdots p_m^{s_m},$$

here some of the indices may be zero.

Let $t_i = \min\{r_i, s_i\}$ and $k_i = \max\{r_i, s_i\}$

Then $(a,b) = e_3 p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$

$$[a,b] = c_4 p_1^{k_1 k_2} p_2 \cdots p_m^{k_m} .$$

A factorisable domain R in which (a,b) exists and (a,b) = ca+db for some suitable c,d$\in$R, is called a Prüfer domain.

Theorem: A prüfer domain R is a domain of unique factorisation.

Proof: Let p be a prime and ab be divisible by p in R.

$$\therefore ab = kp \ , \ k \in R$$

If p is relatively prime to b

$$e = (b,p) = c_1 b + c_2 p, \quad e \text{ unit} .$$

$$\therefore ae = c_1 ab + c_2 ap$$

$$= c_1 kp + c_2 ap$$

$$= (c_1 k + c_2 a)p$$

As e is a unit and p is a prime, thisimplies that a is divisible by p. Thus if ab is divisible by p and b is not divisible by p then a is divisible by p. Hence R is a domain of unique factorisation.

Theorem: If p is a prime element, then R_p, the classes of residues mod p , is an integral domain when R is a domain of unique factorisation and is a field when R is a Prüfer domain.

Proof: Let R be a domain of unique factorisation. Then ab is divisible by p iff either a or b is divisible by p.

$$\therefore ab \equiv 0, \text{ mod } p, \text{ iff } a \equiv 0, \text{ mod } p \text{ or } b \equiv 0, \text{ mod } p.$$

i.e. R_p has no divisor of zero.

R_p satisfies all the other properties of an integral domain.

$$\therefore R_p \text{ is an integral domain.}$$

Now let R be a Prüfer domain. Then R is a domain of

unique factorisation and consequently R_p is an integral domain.

But in R_p, $(a) = x(d)$ is solvable if $(d) \neq (0)$.

For, as $(d) \neq (0)$, p is not a divisor of d.

As p is prime $1 = (d, p) = cd + c^1 p$

$$\therefore a = acd + ac^1 p$$

$$\therefore (a) = (acd), \text{ since } (ac^1 p) = (0)$$

$$= (ac)(d)$$

$$\therefore x = (ac) = (a)(c)$$

i.e. the solution of $(a) = x(d)$ exists if $(d) \neq (0)$

$$\therefore R_p \text{ is a field}$$

An integral domain E is called a generalised Euclidean domain if a norm function $N(a)$, $\forall a \neq 0 \in E$, can be defined such that

1) $N(a) = \text{integer} \geq 0$,

2) $N(ab) \geq N(a)$, for $a \neq 0$, $b \neq 0$,

3) E is the direct product PXQ where P,Q are multiplicative semigroups having common identity 1 such that

(i) if $p \in E$ and $N(p)$ is least then $p \in P$, and

(ii) $\forall\ p \in P$ and $\forall\ q \in Q$ $N(q) \geq N(p)$ where the equality holds only when q is a unit. i.e. $E = \{ pq : p \in P, q \in Q \}$, P,Q satisfying these two properties,

4) There exists for every pair of elements a,b, E with $a \neq 0$ a representation $pb = qa + r$ in which $p \in P$ and either $r = 0$ or $N(r) < N(a)$.

If P is the group of units then E is called simply an Euclidean domain.

Theorem: In E $N(a) \geq N(1) = N(e)$ where e is a unit of E.

For $N(a) = N(a.1) \geq N(1)$.... by definition (2)

Also $N(1) = N(ee^{-1}) \geq N(e)$... by definition (2)

But $N(e) = N(e.1) \geq N(1)$

$\therefore N(e) = N(1)$

$\therefore N(1)$ is least and all units has the least norm and belongs to P, and if $p \notin P$ then $N(p) = N(1)$.

Theorem: $N(ab) > N(a)$ if $b \notin P$.

Proof: Put $c = ab$

As $a \neq 0$, $b \neq 0$; $\therefore c \neq 0$.

$\therefore$ we have $pa = qc + r$, for suitable p,q,r; $r = 0$ or $N(r) < N(c)$ by definition (4),

(i) If $r \neq 0$, $r = pa - qc = pa - qab = a(p - qb)$

$\therefore$ by definition (2), $N(r) \geq N(a)$

$\therefore N(c) > N(r) \geq N(a)$

i.e. $N(ab) > N(a)$

If r=0.

(ii) then $pa = qc = qab$

$\therefore p = qb$, since cancellation law holds in an integral domain

$\therefore N(p) \geq N(b)$... by definition (2)

As N(p) is least, $N(p) = N(b)$

$\therefore b \notin P$.

$\therefore$ If $b \notin P$ then r cannot be $= 0 \Rightarrow$, by (i), $N(ab) > N(a)$.

We could consider the relation $pc = qa + r$ but this gives us no information except that $r = 0$ and $q = pb$.

Theorem: In the generalised Euclidean domain the h.c.f. (a_1,a_2) is expressible linearly in terms of a_1 and a_2.

Proof: For this purpose suppose $N(a_2) \leq N(a_1)$ and apply definition (4) repeatedly. Then

$$p_1a_1 = q_1a_2 + a_3; \quad a_3 = 0 \text{ or } N(a_3) < N(a_2)$$

$$p_2a_2 = q_2a_3 + a_4; \quad a_4 = 0 \text{ or } N(a_4) < N(a_3)$$

etc.

As $N(a_i)$ is a decreasing sequence of positive integers, it must terminate and hence after s steps, say, the above procedure ends. The last steps are

$$p_{s-2}a_{s-2} = q_{s-2}a_{s-1} + a_s$$

$$p_{s-1}a_{s-1} = q_{s-1}a_s + a_{s+1}$$

$$p_sa_s = q_sa_{s+1}$$

Then $a_{s+1} = p_{s-1}a_{s-1} - q_{s-1}a_s$

$$= p_{s-1}a_{s-1} - q_{s-1}(p_{s-2}a_{s-2} - q_{s-2}a_{s-1})$$

$$= (p_{s-1} + q_{s-1}q_{s-2})\, a_{s-1} - q_{s-1}p_{s-2}a_{s-2}$$

Eleminating successively a_s, a_{s-1}, ..., a_3 in this way, one gets finally

$$a_{s+1} = c_1a_1 + c_2a_2,$$

when $c_1, c_2 \in E$.

This process is known as Euclidean algorithmus.

It follows from $a_{s+1} = c_1a_1 + c_2a_2$, that every common divisor of a_1 and a_2 and therefore the h.c.f. (a_1,a_2) is a divisor of a_{s+1}.

Conversely, from the relation $p_s a_s = q_s a_{s+1}$ it follows that a_{s+1} is a divisor of $p_s a_s$. Multiply the (s-1) th relation by p_s, (s-2) th relation by $p_s p_{s-1}$ etc. Then

$$p_s p_{s-1} a_{s-1} = p_s q_{s-1} a_s + p_s a_{s+1}$$
$$p_s p_{s-1} p_{s-2} a_{s-2} = p_s p_{s-1} q_{s-1} a_{s-1} + p_s p_{s-1} a_s.$$
$$\cdots \qquad \cdots$$

As a_{s+1} is a divisor of $p_s a_s$ and hence of $p_s p_{s-1}$ and hence of $p_s p_{s-1} p_{s-2} a_{s-2}$ etc... and of $p_s p_{s-1} \cdots p_2 a_2$ and of $p_s p_{s-1} \cdots p_2 p_1 a_1$. Putting $p_i^1 = p_s p_{s-1} \cdots p_i$ one gets that a_{s+1} is a divisor of $p_1^1 a_1$ and of $p_2^1 a_2$, where $p_1^1, p_2^1 \in p$.

Now if a is any element of E then as E = PxQ, and P,Q both commutative, being subsets of E, a can be expressed as $a = pa^1$ where $p \in P, a^1 \in Q$ and either a^1 ia a unit, in which case $a \in P$ or a^1 has no factor belonging to P except 1.

Express a_{s+1}, a_1, a_2 as the product

$a_1 = \pi_1 a_1'$, $a_2 = \pi_2 a_2'$, $a_{s+1} = pa$, where π_1, π_2, $p \in P$ and a_1' , a_2' , $a \in Q$ and have no factors in P except 1.

$\therefore p_1' a_1 = p_1' \pi_1 a_1'$

$p_2' a_2 = p_2' \pi_2 a_2'$, where $p_1'\pi_1, p_2'\pi_2 \in P$, as P is a semigroup.

As $a_{s+1} = pa$ divides $p_1' a_1 = p_1' \pi_1 a_1'$, $p_2' a_2 = p_2' \pi_2 a_2'$ hence by the above property a divides a_1', a_2'.

$\therefore$ a is a divisor of (a_1', a_2')

i.e. $(a_1', a_2') = \lambda' a$.

on the other hand $a_{s+1} = c_1 a_1 + c_2 a_2$

i.e. $pa = c_1 \pi_1 a_1' + c_2 \pi_2 a_2'$.

Hence every common divisor of a_1, a_2 and hence h.c.f. (a_1', a_2') is a divisor of a.

$\therefore a = \lambda(a_1', a_2')$

$\therefore a = \lambda\lambda' a$

As E is an integral domain

$\lambda\lambda' = 1$

i.e. λ, λ' are units.

$\therefore$ a may be taken as $a = (a_1', a_2')$

Now for any $p \in P$, $p = p_1 . a \Rightarrow N(p) = N(p_1 a) \geq N(a) \Rightarrow$ [illegible] $a \in P$,

since N(P) is least and if N (p) is least then $p \in P$.

So from the relation

$$pa = c_1 \pi_1 a_1' + c_2 \pi_2 a_2'$$

we get that, a common divisor of π_1, π_2 and hence the h.c.f. (π_1, π_2) is a divisor of p.

$\therefore p = \pi(\pi_1, \pi_2), \pi \in p$

But as $a_1 = \pi_1 a_1', a_2 = \pi_2 a_2'$

$$(a_1, a_2) = (\pi_1, \pi_2)(a_1', a_2')$$

$\therefore a_{s+1} = pa = \pi(\pi_1, \pi_2)(a_1', a_2') = \pi(a_1, a_2)$

Thus $a_{s+1} = c_1 a_1 + c_2 a_2 = \pi(a_1, a_2)$ i.e. h.c.f. of a_1, a_2 is expressed linearly interms of a_1, a_2.

We sum up the properties of the generalised Euclidean domain as

i) $N(ab) \geq N(a)$, the equality holds only when $b \in P$.

ii) $\pi(a_1, a_2) = c_1 a_1 + c_2 a_2, \pi \in P$.

If E is an Euclidean domain then P = U = group of units. Hence from above

(i^1) $N(ab) \geq N(a)$, the equality holds only when b is a unit

(ii^1) $(a_1, a_2) = c_1 a_1 + c_2 a_2$.

(i^1) implies that E is a factorisable domain, and

(ii^1) implies that E is a Prüfer domain.

Hence we get the theorem: The Euclidean domain is a domain of unique factorisation.

If E is the generalised Euclidean domain then $P \supset U$. For the elements of Q, $N(ab) > N(a)$ unless b is a unit.

Hence the elements of Q are factorisable. So if the elements of P are factorisable then the elements of E are also factorisable.

Now for any two element $a_1, a_2 \in Q$ if (a_1, a_2) = unit then a_1 is prime to a_2. In this case

$$\pi e = c_1 a_1 + c_2 a_2, \pi \in P, e \text{ unit}.$$

If b is any element of Q

$$e\pi b = c_1 a_1 b + c_2 a_2 b .$$

If $a_2 b$ is divisible by a_1, $a_2 b = k a_1$, $k \in Q$

$$\therefore e\pi b = c_1 a_1 b + c_2 a_2 b = c_1 a_1 b + c_2 k a_1$$

$$= a_1 (c_1 b + c_2 k)$$

As $a_1 \in Q$, a_1 divides b.

Thus if $a_1 \in Q$ and is prime to a_2 but divides $a_2 b$ then a_1 divides b.

$\therefore$ The semigroup Q is uniquely factorisable. Hence we get the theorem: If P is uniquely factorisable, the generalised Euclidean domain is uniquely factorisable.

CHAPTER II

1. POLYNOMIAL DOMAIN

Let R be a ring in which addition is commutative; a,b,c,..., with or without suffix are its elements. Let x be an indeterminate. We take powers of x and multiply it with the elements of R, assuming that this multiplication is commutative i.e. $ax^n = x^n a$. In particular we shall consider x^0 and shall assume $ax^0 = a$ for every $a \in R$.

Then the expressions of the form

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n,$$

n finite integer ≥ 0 are called polynomials over the ring R.

In the expression for p(x) the heighest index n of x, for which $a_n \neq 0$ is called the degree of the polynomial. a_i is called the coefficient of x^i and in particular a_0, the coefficient of x^0 and a_n the coefficient of x^n, n being the degree of that polynomial, are respectively called the constant term and the leading coefficient of the polynomial.

Generally the terms for which, coefficients are zero are not written in the expression for p(x). However one can write these terms whenever feels necessary.

We define the addition and multiplication of two polynomials

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$q(x) = b_0 + b_1 x + \ldots + b_m x^m$$

$$= b_0 + b_1 x + \ldots + b_m x^m + b_{m+1} x^{m+1} + \ldots + b_n x^n,$$

assuming $n > m$ and $b_{m+1} = b_{m+2} = \ldots = b_n = 0$, respectively by

$$p(x)+q(x)=(a_0+b_0)+(a_1+b_1)x+\ldots+(a_m+b_m)x^m+\ldots+(a_n+b_n)x^n$$

and $$p(x)\cdot q(x)=c_0+c_1x+\ldots+c_mx^m+\ldots+c_nx^n+\ldots+c_{m+n}x^{m+n},$$

where $c_\nu = \sum_{i+j=\nu} a_i b_j, \qquad \nu=0,1,\ldots,m+n$

From this rule of addition and multiplication it can easily be proved that all polynomials form a ring in which addition is commutative. We denote this ring by $R[x]$. The additive identity of $R[x]$ is the zero polynomial $0(x) = 0 + 0x + 0x^2 + \ldots + 0x^n$, 0 being the additive identy of R. As from the above conventions $0 = 0x^0$, one can assume $0=0(x)=0x^0=0+0x+\ldots+0x^n$.

Sometimes x is called variable and the elements of R are called constants.

In $R[x]$, the definitions of addition and multiplication imply

(i) $a(bx^k) = (ab)x^k$

(ii) $(a+b)x^k = ax^k+bx^k$.

(iii) $(ax^k)(bx^j) = abx^{k+j}$

In the product of polynomials we have

$$c_{m+n} = a_n b_m$$

$\therefore$ If R has no divisor of zero $c_{m+n} = a_n b_m \neq 0$ when $a_n \neq 0, b_m \neq 0$.

As $p(x)q(x) = c_0+c_1x+\ldots+c_{m+n}x^{m+n}$,

$p(x)q(x) \neq 0(x) \Rightarrow R[x]$ has no divisor of zero and degree of $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$.

Conversely if $R[x]$ has no divisor of zero R can not have any divisor of zero, since by the assumption $a_0x^0 = a_0$ one gets

$R \subset R[x]$.

Moreover if R is multiplicatively commutative, then

$$c_\nu = \sum_{i+j=\nu} a_i b_j = \sum_{i+j=\nu} b_j a_i \Rightarrow p(x)q(x) = q(x)p(x),$$

i.e. $R[x]$ is commutative.

Thus if R is an integral domain then $R[x]$ is also an integral domain.

Let R contain the multiplicative identity 1 then $\forall$ $a \in R$ $ax = (a1)x = a(1x)$, so in this case one can assume $1x = x$ and that $x \notin R[x]$.

Theorem: If R is an integral domain then the units of R are the only units of $R[x]$.

Proof: Let $p(x)$ is a unit of $R[x]$, $\Rightarrow$ $p(x)$ has an inverse, say $q(x)$, in $R[x]$ such that $p(x)q(x) = 1$.

So degree $(p(x)q(x))$ = deg 1 = 0

But degree $(p(x)\ q(x))$ = degree $p(x)$ + degree $q(x)$.

$\therefore$ 0 = degree $p(x)$ + degree $q(x)$

But if $f(x) \neq 0(x)$ degree $f(x) \geq 0$.

$\therefore$ degree $p(x)$ = 0 = degree $q(x)$

$\therefore$ $p(x) = p$, $q(x) = q$ such that $p, q \in R$ and $pq = 1$ i.e. they are units of R.

2. Factorisation in a polynomial domain.

For the consideration of factorisation in a polynomial domain $R[x]$ we shall suppose R is an integral domain with unique factorisation. As R is an integral domain $R[x]$ is also an integral domain.

In $R[x]$ if $f(x) \neq 0(x)$ we define norm $f(x) = N(f(x))=$ degree $f(x)$.

Then

(i) $N(f(x)) \geq 0$

(ii) $N(p(x).q(x)) = N(p(x)) + N(q(x)) \geq N(p(x)), N(q(x))$.

In $R[x]$, a division algorithem is possible..

For, let $a(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$

$b(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$, $n \geq m$,

be two polynomials of $R[x]$. As R is a domain of unique factorisation h.c.f. $k = (a_0, b_0)$ exists. Then $a_0 = kl_0$, $b_0 = km_0$. It is seen that

$m_0 a(x) - l_0 x^{n-m} b(x) = c_1(x)$ where $N[c_1(x)] \leq n-1$

If $m \leq n-1$ we can apply the same process to $c_1(x)$ and $b(x)$ and get

$m_1 c_1(x) - l_1 x^{n-m-1} b(x) = c_2(x)$, $N[C_2(x)] \leq n-2$

By repeating this process till $N[c_i(x)] < m$ and combining all these steps we get

$p.a(x) = q(x)b(x) + r(x)$

where $N(p)=0$ and $N[r(x)] < N[b(x)]$ ...(1)

Thus, given any two polynomials $a(x), b(x)$ of $R[x]$ one can find p, $q(x)$, $r(x)$ satisfying (1).

Let d be the h.c.f. of the coefficients $a_0, a_1, \ldots, a_n$ then

$a_i = da'_i$ for $i = 0, 1, \ldots, n$

so $a(x) = d(a'_0 x^n + a'_1 x^{n-1} + \ldots + a'_n) = d\, a'(x)$, where the h.c.f. $(a'_0, a'_1, \ldots a'_n) = 1$.

d is called the content of $a(x)$ and in abbreviation: cont $a(x)$.

The polynomial whose content ia 1 is called a primitive polynomial. Thus $a^1(x)$ is a primitive polynomial and may be called prim a(x).

$\therefore$ $a(x) = da^1(x) = \text{cont } a(x) \text{ prim } a(x)$.

Theorem: Primitive polynomials of $R[x]$ form a multiplicative semigroup.

Proof: Let $a(x) = a_0+a_1x +\ldots+ a_n x^n$

$b(x) = b_0+b_1x +\ldots+b_m x^m$,

be two primitive polynomials. Then $a(x)b(x) = c(x)= \sum c_\nu x^\nu$ where $c_\nu = \sum_{i+j=\nu} a_i b_j$, $\nu = 0, 1, \ldots m+n$; must be primitive. If not, the coefficient c_ν must be divisible by a prime p, for all ν.

Suppose that a_r is the first coefficient of a(x) and b_s, be the first coefficient of b(x) those are not divisible by p. i.e. $a_i \equiv 0$, $i < r$ and $b_j \equiv 0$, $j < s$ mod p

$\not\equiv 0$, $i = r$ $\not\equiv 0$, $j = s$

Then as $c_\nu = \sum_{i+j=\nu} a_i b_j$

$i+j =$

$$c_{r+s} \equiv a_r b_s \bmod p$$

But $c_{r+s} \equiv 0 \bmod p$ i.e. $a_r b_s \equiv 0 \bmod p$ i.e. p divides the product $a_r b_s$. But as R is the domain of unique factorisation p divides either a_r or b_s, contrary to the assumption. Hence the theorem.

The result proves that $R[x]$ is a direct product of R and the semigroup of primitive polynomials.

So $R[x]$ satisfies all the properties of a generalised Euclidean domain, where, for $a(x) \neq 0(x)$, $N(a(x)) =$ degree a(x). Moreover as R is a domain of unique factorisation $R[x]$ is a domain of unique factorisation.

If R is a field then $R[x]$ is an Euclidean domain, so in this case also $R[x]$ is a domain of unique factorisation.

Theorem: $f(x)$ reducible $\Leftrightarrow$ $f(x+a)$ reducible in $R[x]$, where R is a ring with identity 1 and $a \in R$.

Proof: $f(x)$ reducible implies $f(x) = g(x)h(x)$.

Now in the definition of product we asumed nothing upon x except that $ax^n = x^n a$, $\forall\, a \in R$ and for every positive integer n. So the product remains valid if we replace x by $x+a$.

$\therefore\ f(x+a) = g(x+a) \cdot h(x+a)$

As $1 \in R$, $x \in R[x]$. Hence for any $a \in R$, $(x+a)^n$ agrees a binomial expansion in $R[x]$ and we get $g(x+a)$, $h(x+a)$ as polynomials in x i.e.

$$f(x+a) = g_1(x)h_1(x).$$

conversely if $f(x+a) = p(x)q(x)$ then putting $x = y-a$ we get

$$f(y) = p(y-a)q(y-a)$$

$$= p_1(y)q_1(y),$$ expanding by binomial theorrem and rearranging by the law of addition.

So replacing the indeterminate y by x

$$f(x) = p_1(x)\, q_1(x)$$

Hence the theorem

Let $F = Q(R)$ the quotient field of the integral domain R.

Theorem: Every polynomial $\phi(x)$ of $F[x]$ corresponds to unique primitive polynomial $p_1(x)$ such that $\phi(x) = \frac{a_1}{b_1} p_1(x)$, where $a_1, b_1 \in R$.

Proof: For $\phi(x) = \frac{p(x)}{b_1}$, where b_1 is the product of all the denominators of $\phi(x)$ and $p(x) \in R[x]$.

Also $\phi(x) = \frac{a_1}{b_1} p_1(x)$, where a_1 is the content of $p(x)$ and $p_1(x)$ the corresponding primitive polynomial.

Let $\phi(x)$ has another such representation i.e.

$$\phi(x) = \frac{a_2}{b_2} p_2(x)$$

$$\therefore \phi(x) = \frac{a_1}{b_1} p_1(x) = \frac{a_2}{b_2} p_2(x)$$

or $$a_1 b_2 p_1(x) = a_2 b_1 p_2(x), \ldots (\alpha)$$

As both $p_1(x)$ and $p_2(x)$ are primitive $a_1 b_2 = c a_2 b_1$ where c is a unit. Substituting this in (α)

$$p_1(x) = c\, p_2(x)$$

i.e. they differ only by a multiple of a unit.

Theorem: If a polynomial $\phi(x)$ of $R[x]$ is factorisable in $F[x]$ then $\phi(x)$ is also factorisable in $R[x]$.

Proof: Let $\phi(x) = d\, f(x)$, where $f(x)$ is primitive

$$= p(x)q(x), \text{ in } F[x]$$

$$= \frac{a}{b} p_1(x) \frac{c}{d} q_1(x), \text{ where } p_1(x), q_1(x) \text{ are primitives}$$

$$= \frac{ac}{bd} \psi(x), \text{ where } \psi(x) = p_1(x) q_1(x) \text{ is primitive.}$$

But $\phi(x)$ corresponde to two primitives $f(x)$ and $r(x)$

$\Rightarrow cf(x) = r(x) = p_1(x) q_1(x)$, where c is a unit

$\Rightarrow f(x)$ has factors in $R[x]$

$\Rightarrow \phi(x)$ has factors in $R[x]$, since $d \in R$

Let R be the domain of common integers and p is a prime integer, then R_p, the residue class of integers mod p, is a field. Hence both $R[x]$ and $R_p[x]$ are domains of unique factorisation.

A polynomial $f(x) = a_0+a_1x+\ldots+a_nx^n \in R[x]$ corresponds to a unique polynomial $\overline{f(x)} = \bar{a}_0+\bar{a}_1x+\ldots+\bar{a}_nx^n$, where $\bar{a}_i \equiv a_i \pmod p$

Theorem: $f(x)$ factorisable in $R[x]$ implies $\overline{f(x)}$ factorisable in $R_p[x]$.

Proof: Let $f(x)=g(x)h(x)$ in $R[x]$, where

$$g(x) = b_0 + b_1x+\ldots+b_rx^r$$

$$h(x) = c_0 + c_1x+\ldots+c_sx^s \quad , \; r+s = n = \text{degree } f(x)$$

$$\therefore a_i = b_ic_0+b_{i-1}c_1+\ldots+b_0c_i$$

$$\therefore \bar{a}_i = \overline{b_ic_0+b_{i-1}c_1+\ldots+b_0c_i}$$

$$= \bar{b}_i\bar{c}_0+\bar{b}_{i-1}\bar{c}_1+\ldots+\bar{b}_0\bar{c}_i \; .$$

$$\therefore \overline{f(x)} = \overline{g(x)}\,\overline{h(x)}$$

i.e. $\overline{f(x)}$ is factorisable in $R_p[x]$

The converse however is not necessarily true. $\overline{f(x)}$ may be factorisable in $R_p[x]$, though $f(x)$ is irreducible in $R[x]$. However, by the theorem, if $\overline{f(x)}$ is irreducible in $R_p[x]$ then $f(x)$ is necessarily irreducible in $R[x]$ and as $R_p[x]$ has only a finite number of irreducible polynomials of a given degree (see chapter IV) one can see whether $\overline{f(x)}$ is factorisable or not. If $\overline{f(x)}$ is not factorisable in $R_p[x]$ then one concludes $f(x)$ is not factorisable in $R[x]$.

It may be noted that if the leading coefficient of $f(x)$ is not divisible by p then none of the leading coefficients of $g(x)$ and $h(x)$ can be divisible by p. Hence $\overline{g(x)}$, $\overline{h(x)}$ has the same degree as $g(x)$, $h(x)$ respectively.

Zeros of Polynomial

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynimial of $R[x]$, R integral domain with 1. An element α of R, for which $f(\alpha)=0$, is called a zero of f(x).

Theorem: If α is a root of f(x), then $x-\alpha$ is a factor of f(x).

Proof: As division algorithem is possible in $R[x]$, we have, dividing f(x) by $x-\alpha$,

$$f(x) = q(x).(x-\alpha) + r, \text{ where } r \in R$$

Substituting $x = \alpha$, we get

$$0 = f(\alpha) = q(\alpha).0+r$$
$$= 0 + r$$
$$\therefore r = 0$$
$$\therefore f(x) = q(x)\ (x-\alpha).$$ Hence the thorem.

Theorem: If $\alpha_1, \alpha_2, \ldots, \alpha_k$ are different roots of f(x) then $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)$ is a factor fo f(x).

Proof: As α_1 is a root

$$f(x) = p_1(x)(x-\alpha_1)$$

Again as α_2 is a root of f(x)

$$0 = f(\alpha_2)=p_1(\alpha_2)(\alpha_2-\alpha_1)$$

As $\alpha_2 \neq \alpha_1$, $\alpha_2-\alpha_1 \neq 0$

and as R has no divisor of zero $p_1(\alpha_2)=0 \Rightarrow \alpha_2$ is a root of $p_1(x)$.

$$\therefore p_1(x) = p_2(x)(x-\alpha_2)$$
$$\therefore f(x)=p_1(x)(x-\alpha_1)=p_2(x)(x-\alpha_2)(x-\alpha_1)$$

Continuing this process k times, one gets

$$f(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)p_k(x)\ .$$

Hence the theorem.

Corollary: From the above it is obvious that in an integral domain a polynomial of degree $n \neq 0$ has at most n distincts roots.

If however, R is not an integral domain the number of roots of f(x) in R may be greater than the degree of f(x). For example, the polynomial x^3-x has six roots in the ring of residue class of integers mod 6.

Definition: If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, then, we define, the derivative of f(x) (abbreviated $f'(x)$) to be the polynomial

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1.$$

From this definition one can easily prove

i) $(f(x)+g(x))' = f'(x) + g'(x)$

ii) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

iii) $(f(g(x)))' = f'(g(x))g'(x)$.

Definition: if f(x) is divisible by $(x-\alpha)^k$ but not by $(x-\alpha)^{k+1}$ then α is called a root of multiplicity k, of f(x). If k=1 then α is called a simple root.

Now let α be a root of multiplicity k, of f(x),

$$\therefore f(x) = (x-\alpha)^k f_1(x), \text{ such that } f_1(\alpha) \neq 0$$

$$\therefore f'(x) = k(x-\alpha)^{k-1} f_1(x) + (x-\alpha)^k f_1'(x)$$

Differentiating successively one gets

$$f^{(k)}(x) = k! f_1(x) + (x-\alpha) f_2(x)$$

i.e. $f(\alpha)=0$, $f'(\alpha)=0$, $f''(\alpha)=0, \ldots, f^{(k-1)}(\alpha) = 0$ but $f^{(k)}(\alpha) = k! f_1(\alpha) \neq 0$, as $f_1(\alpha) \neq 0$.

Theorem: Let $f(x)=a_0 + a_1x + \ldots + a_nx^n \in R[x]$, where R is the domain of common integers. Then if a rational number p/q, (p prime to q),

is a root of f(x) then $p \mid a_0$, $q \mid a_n$ and $(p-mq) \mid f(m)$ for any integer m.

Proof: We have

$$f(p/q) = a_0 + a_1 p/q + \ldots + a_n (p/q)^n = 0$$

$$\therefore a_0 q^n + a_1 q^{n-1} p + a_2 q^{n-2} p^2 + \ldots + a_n p^n = 0$$

i.e. p is a root of

$$\phi(x) = a_0 q^n + a_1 q^{n-1} x + a_2 q^{n-2} x^2 + \ldots + a_n x^n$$

i.e. $\phi(x) = (x-p)g(x)$

Equating constant terms of both the sides and remembering $(p,q) = 1$ one gets $p \mid a_0$

Putting $x = p + q$ in $\phi(x)$, one gets $q \mid a_n$.

Again putting $x = mq$ one gets $(p-mq) \mid \phi(mq)$

But $\phi(mq) = q^n f(m)$

And as $(p,q) = 1$, $(p-mq) \mid f(m)$

Hence the theorem.

This theorem can conveniently be used to determine rational roots (hence linear factors), if any, of a polynomial over the domain of common integers R. For, as R is the domain ofunique factorisation a_0 and a_n has only a finite number of factors. One can choose p and q from these factors and see whether, for an arbitrary integer m, $(p-mq) \mid f(m)$ or not. If not, one concludes that p/q is not a root of f(x). On the other hand if $(p-mq) \mid f(m)$ then by actually substituting one finds the value of f(p/q). If it is zero then p/q is a root f(x), other wise not. As there are only finite number of p's and q's one tries only finite nos. to find rational roots if any.

The above theorem is also true in any domain of unique factorisation with the identity 1.

3. Extended domains and fields.

Definition: A polynomial $f(x)$ of $R[x]$ is called irreducible in $R[x]$ if there exist no $g(x)$, $h(x) \in R[x]$, such that

$f(x) = g(x)h(x)$ and degree $g(x) \geq 1$, degree $h(x) \geq 1$.

Obviously an irreducible polynomial has no root in R. But it might have a root in R_1 where $R \subset R_1$.

For example, x^2+1 has no root in $R[x]$, where R is the field of real numbers. But it has roots in $C[x]$, where C is the field of complex numbers and so x^2+1 is factorisable in $C[x]$.

Now let $f(x) = \sum_{i=0}^{n} a_i x^i$ be an irreducible polynomial of $F(x)$ where F is a field. Let α be an element (not belonging to $F(x)$) such that $f(\alpha)=0$....(1). One may take α an arbitrary symbol which satisfies all the postulates for the indeterminate x, in relation to F, together with (1).

Consider the set $F(\alpha)$ of all elements of the form

$p(\alpha) = b_0+b_1\alpha+ +\ldots+b_{n-1}\alpha^{n-1}$,

b_i , $i=0,1,\ldots n-1, \in F$

Then $F(\alpha)$ is a field, For if

$q(\alpha) = c_0+c_1\alpha+\ldots c_{n-1}\alpha^{n-1}$

then $p(\alpha) +q(\alpha) = (b_0+c_0)+(b_1+c_1)\alpha+\ldots+(b_{n-1}+c_{n-1})\alpha^{n-1}$

$= \alpha_0 +\alpha_1\alpha+\ldots+\alpha_{n-1}\alpha^{n-1}$, where $\alpha_i = b_i+c_i$, $i=0,\ldots,n-1$.

$= \alpha(\alpha)$ say.

For multiplication of $p(\alpha)$ and $q(\alpha)$ we see that $p(\alpha)$ corresponds to the polynomial $p(x) = b_0+b_1x+\ldots+b_{n-1}x^{n-1}$ and similarly we

get the corresponding polynomials $q(x)$ and $r(x) = p(x)q(x)$. Now if the degree of $r(x)$ is less than n then $r(x)$ corresponds to the element $r(\alpha)$ of $F(\alpha)$ which is evidently the product of $p(\alpha)$ and $q(\alpha)$.

If however the degree of $r(x)$ is $\geq n$, then in $F[x]$

$$r(x) = g(x)f(x) + h(x),$$

where degree $h(x) < n$.

$$\therefore r(\alpha) = g(\alpha)f(\alpha) + h(\alpha)$$
$$= g(\alpha).0 + h(\alpha)$$

Hence $r(\alpha)$ i.e. $p(\alpha)q(\alpha) \in F(\alpha)$.

Let the inverse of $p(\alpha)$ is

$$p^{-1}(\alpha) = u_0 + u_1\alpha + \ldots + u_{n-1}\alpha^{n-1},$$

Then $1 = p(\alpha)p^{-1}(\alpha) = a_0u_0 + (a_0u_1 + a_1u_0)\alpha + \cdots + a_nu_{n-1}\alpha^{2n-2}$.

$$\therefore a_0u_0 = 1 \text{ i.e. } u_0 = \frac{1}{a_0},$$

$$a_0u_1 + a_1u_0 = 0 \text{ i.e. } u_1 = -\frac{1}{a_0}a_1u_0 = -\frac{a_1}{a_0^2}.$$

etc.

Thus if $p(\alpha) \neq 0$, $p^{-1}(\alpha)$ can be determined as above.

The other properties of a field can easily be verified in $F(\alpha)$.

Hence $F(\alpha)$ is a field.

$F(\alpha)$ is an extension of F. The extension has been done with a root of an irreducible polynomial $f(x)$ of $F[x]$. α is called algebralic to F and the extension is called simple algebraic extension.

It may be noted that we have assumed α to be a root of an irreducible polynomial $f(x)$ over F. Consequently α does not belong to F. If however $\alpha \in F$, in which case $f(x)$ is reducible in $F[x]$ with $x - \alpha$ as a factor, one may consider α as a root of

$x - \alpha$ and find $F(\alpha)$. Obviously here $F(\alpha) = F$.

Theorem: Let α_1 and α_2 be two roots of an irreducible polynomial $f(x)$ of degree $n \geq 2$, over a field F. Then there is an isomorphism

$$\phi: F(\alpha_1) \longrightarrow F(\alpha_2), \text{ such that } \phi(\alpha_1) = \alpha_2 .$$

Proof: The elements of $F(\alpha_1)$ are $\sum_{i=0}^{n-1} a_i \alpha_1^i$ and those of $F(\alpha_2)$ are $\sum_{i=0}^{n-1} a_i \alpha_2^i$, $a_i \in F$.

Now establish the correspondence $\phi: F(\alpha_1) \longrightarrow F(\alpha_2)$, such that $\phi\left(\sum_{i=0}^{n-1} a_i \alpha_1^i\right) = \sum_{i=0}^{n-1} a_i \alpha_2^i$.

Then $\phi(\Sigma a_i \alpha_1^i + \Sigma b_i \alpha_1^i) = \phi(\Sigma (a_i + b_i)\alpha_1^i) = \Sigma (a_i + b_i)\alpha_2^i$

$= \Sigma a_i \alpha_2^i + \Sigma b_i \alpha_2^i = \phi(\Sigma a_i \alpha_1^i) + \phi(\Sigma b_i \alpha_1^i)$;

$\phi(\Sigma a_i \alpha_1^i \cdot \Sigma b_i \alpha_1^i) = \phi\left(\sum_{i=0}^{2n-2} c_i \alpha_1^i\right)$, $c_i = \sum_{j+k=i} a_j b_k$,

$= \sum_{i=0}^{2n-2} c_i \alpha_2^i = \Sigma a_i \alpha_2^i \cdot \Sigma b_i \alpha_2^i = \phi(\Sigma a_i \alpha_1^i) \cdot \phi(\Sigma b_i \alpha_1^i)$.

The relation $\phi\left(\sum_{i=0}^{2n-2} c_i \alpha_1^i\right) = \sum_{i=0}^{2n-2} c_i \alpha_2^i$ remains valid because α_1 and α_2 are the roots of the same polynomial.

Now it is obvious that the correspondence ϕ is $1 \leftrightarrow 1$ between the elements of $F(\alpha_1)$ and $F(\alpha_2)$.

So ϕ is an isomorphism.

Putting $a_1 = 1$, $a_0 = a_2 = \ldots = 0$, one gets $\phi(\alpha_1) = \alpha_2$.

The most important consequence of this theorem is that any algebraic relation between one root of an irreducible polynomial and the elements of F remains true if this root is replaced by any other root of the polynomial.

Theorem: Let F_1 and F_2 be two isomorphic fields and ϕ is an isomorphism $F_1 \to F_2$. If the polynomial $f_1(x) = \sum_{j=0}^{m} c_j x^j$, $c_j \in F_1$, is irreducible over F_1 then $f_2(x) = \sum_{j=0}^{m} \phi(c_j) x^j$ is irreducible over F_2. Further if α_i is a root of $f_i(x)$, $i=1,2$,

then $F_1(\alpha_1) \simeq F_2(\alpha_2)$ with an extension isomorphism ψ of ϕ such that $\psi(\alpha_1) = \alpha_2$.

[The isomorphism ψ is an extension of ϕ if for all $c \in F$, one has $\psi(c) = \phi(c)$.]

Proof: Between the elements of $F_1(x)$ and $F_2(x)$ establish the correspondence $\xi: \sum_{i=0}^{n} a_i x^i \longrightarrow \sum_{i=0}^{n} \phi(a_i) x^i$, $a_i \in F$.

Then $\xi(\Sigma a_i x^i) = \Sigma \phi(a_i) x^i$

Now $\xi(\Sigma a_i x^i + \Sigma b_i x^i) = \xi(\Sigma (a_i + b_i) x^i) = \Sigma \phi(a_i + b_i) x^i$

$= \Sigma (\phi(a_i) + \phi(b_i)) x^i = \Sigma \phi(a_i) x^i + \Sigma \phi(b_i) x^i$

$= \xi(\Sigma a_i x^i) + \xi(\Sigma b_i x^i)$

$\xi(\Sigma a_i x^i \cdot \Sigma b_i x^i) = \xi(\Sigma c_i x^i)$, $c_i = \sum_{j+k=i} a_j b_k$

$= \Sigma \phi(c_i) x^i = \Sigma \phi(a_i) x^i \Sigma \phi(b_i) x^i$

$= \xi(\Sigma a_i x^i) \cdot \xi(\Sigma b_i x^i)$, since ϕ is an isomorphism.

As the correspondence $\phi: a_i \longrightarrow \phi(a_i)$ is $1 \longleftrightarrow 1$, the correspondence ξ is $1 \longleftrightarrow 1$ and hence ξ is an isomorphism.

If $f_2(x) = \sum_{j=0}^{n} \phi(c_j) x^j = \Sigma \phi(a_i) x^i \cdot \Sigma \phi(b_k) x^k$,

then $\xi(\Sigma a_i x^i \Sigma b_k x^k) = \Sigma \phi(a_i) x^i \cdot \Sigma \phi(b_k) x^k = f_2(x)$

But $\xi(f_1(x)) = f_2(x)$ and ξ is $1 \longleftrightarrow 1$,

$\therefore f_1(x) = \Sigma a_i x^i \Sigma b_k x^k$, i.e. $f_1(x)$ is reducible.

Again if $\Psi: \Sigma a_i \cdot \alpha_1^i \longrightarrow \Sigma \phi(a_i) \alpha_2^i$, then since the degrees of $f_1(x)$ and $f_2(x)$ are equal and the correspondence between the coefficients of same powers of α's, in the correspondence ψ, is isomorphic, one can prove just as in the case of ξ above, that ψ is an isomorphism between $F_1(\alpha_1)$ and $F_2(\alpha_2)$.

Putting $a_1 = 1$, $a_0 = a_2 = \ldots = 0$, we get $\psi(\alpha_1) = \alpha_2$, since $\phi(1) = 1$ for any isomorphism ϕ. Putting $a_1 = a_2 = \ldots = a_n = 0$ we get

$$\psi(a_0) = \phi(a_0)$$

Theorem: h.c.f. is preserved in an extension $F'[x]$, where $F' \geq F$, both fields.

Proof: Let $f(x)$, $g(x)$ be two polynomials of $F[x]$ and

$$(f(x),\ g(x)) = h(x)$$

Then since $F[x]$ is an Euclidean domain there exist suitable $p(x), q(x) \in F[x]$ such that

$$h(x)=p(x)f(x)+q(x)g(x)$$

Now let $(f(x),g(x))=h_1(x)$ in $F'[x]$. So there exist $l(x), m(x) \in F'[x]$ such that $l(x)h_1(x)=f(x)$, $m(x)h_1(x)=g(x)$

$$\therefore h(x)=h_1(x)\{p(x)l(x) + q(x)\ m(x)\}$$

$$\therefore h_1(x) \mid h(x) .$$

But every common factor and hence the h.c.f. of $f(x)$, $g(x)$ in $F[x]$ is also a common factor of $f(x), g(x)$ in $F'[x]$

$$\therefore h(x) \mid h_1(x)$$

i.e. $h(x)$, $h_1(x)$ are associated.

$$\therefore h(x)=b\ h_1(x),$$ where b is a unit.

Theorem: Two polynomials $f(x)$, $g(x)$ of $F[x]$, F field, have a common factor of degree ≥ 1 iff they have at least one common root in a suitable extension.

Proof: If $h(x)$ is a common factor of degree ≥ 1 then the roots of $h(x)$ are also roots of both $f(x)$ and $g(x)$.

Conversely if $f(x)$, $g(x)$ has a common root α then in $F(\alpha)[x]$ $x-\alpha$ is a factor of both $f(x)$, $g(x)$, hence is a factor of h.c.f. $(f(x), g(x))$ in $F(\alpha)[x]$. But h.c.f. does not change in an extension. So $f(x), g(x)$ have a common factor of degree ≥ 1 in $F[x]$.

Corollary: f(x), g(x), have common root, f(x) irreducible $\Rightarrow$ f(x) $\mid$ g(x).

In the extension $F(\alpha)$ of the field F by the root α of an irreducible polynomial f(x) the elements of $F(\alpha)$ are of the form

$$b_o + b_1\alpha + \ldots\ldots + b_{n-1}\alpha^{n-1},$$

$b_o, b_1, \ldots\ldots, b_{n-1} \in F$.

Now let F be a subfield of a field F^1. Then F^1 is an extension of F. If there exists finite number of elements $\alpha_1, \alpha_2, \cdots, \alpha_m \in F^1$ such that every element of F^1 can be expressed as

$$a_1\alpha_1 + a_2\alpha_2 + \ldots\ldots\ldots + a_m\alpha_m,$$

$a_i \in F$, then F^1 is called a finite extension of F. If moreover all α_i, are independent over F i.e. $c_1\alpha_1 + c_2\alpha_2 + \ldots\ldots + c_m\alpha_m = 0$ implies all $c_i = 0$, then m is called the degree of the extension and one writes this as $m = [F^1 : F]$. If there exists an element $\beta \in F^1$ such that $F^1 = F(\beta)$ i.e. if every element $\gamma \in F^1$ can be expressed as $\gamma = d_o + d_1\beta + \ldots\ldots + d_{m-1}\beta^{m-1}$, where $d_i \in F$ and $m = [F^1 : F] > 1$, then β is called a primitive element of the extension.

In the above example $F(\alpha)$ is a finite extension of F, α is the primitive element and $[F(\alpha) : F] = n$.

Definition: If a field E is an extension of a field F such that a polynomial $\phi(x)$ of $F[x]$ is factorised into linear factors in $E[x]$ and if $\phi(x)$ cannot be so factorised in any intermediate field, then E is called the splitting field of $\phi(x)$. Thus the smallest field E in which $\phi(x)$ is factorisable into linear factors is called the splitting field of $\phi(x)$.

Theorem: Splitting field E exists for every polynomial $\phi(x)$ of $F[x]$.

Proof: As every polynomial $\phi(x)$ is reducible into prime factors in $F[x]$, it is enough to consider the proposition when $\phi(x)$ is irreducible.

As $\phi(x)$ is irreducible in $F[x]$, extend F algebraically to $F_1 = F(\alpha_1)$, where α_1 is a root of $\phi(x)$. F_1 may contain other roots of $\phi(x)$ besides α_1. Let the roots $\alpha_1, \ldots, \alpha_k \in F_1$.

Then in $F_1[x]$,

$$\phi(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)\phi_{11}(x)\,\phi_{12}(x)\ldots\phi_{1r}(x),$$

where $\phi_{1i}(x)$ are irreducible in $F_1[x]$ and degree $\phi_{1i}(x) <$ degree $\phi(x)$.

Now extend F_1 by a root of $\phi_{11}(x)$ to F_2 and proceed as above. In $F_2[x]$,

$$\phi(x) = (x-\alpha_1)\ldots(x-\alpha_k)(x-\alpha_{k+1})\ldots(x-\alpha_s)\,\phi_{21}(x)\ldots\phi_{2t}(x),$$

where $\phi_{2i}(x)$ are irreducible and degree $\phi_{2i}(x) <$ degree $\phi_{11}(x)$.

As the degrees of $\phi_{ki}(x)$ are decreasing, we arrive, at least in n steps (n being the degree of $\phi(x)$), in a field E such that in E $\phi_{ki}(x)$ are all linear and $\phi(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$.

E is the splitting field of $\phi(x)$.

Definition: An irreducible polynomial f(x) of $F[x]$ which has no multiple roof in an extension of F is called separable, otherwise it is called inseparable.

Let us investigate the inseparable polynomials of $F[x]$.

Let f(x) be an irreducible polynomial of $F[x]$ and α be a root of f(x) of multiplicity $K > 1$ in an extension of F. Then

$f(x)=(x-\alpha)^k . q(x)$, where $q(\alpha) \neq 0$, in that extension.

$\therefore$ Differentiating $f'(x) = (x-\alpha)^k q'(x) + k\,(x-\alpha)^{k-1} q(x)$

or $f'(x) = (x-\alpha)^{k-1}\{(x-\alpha) q'(x) + k q(x)\}$.

As $k > 1$, α is a root of $f'(x)$ of multiplicity $k-1$.

$\therefore$ The h.c.f. $(f(x), f'(x)) = (x-\alpha)^{k-1} \psi(x)$.

Conversely, if every root of $f(x)$ is simple, then [illegible]

$f'(x) = (x-\alpha)\, q'(x) + q(x)$.

$\therefore$ $f'(\alpha) = q(\alpha) \neq 0$, for every root α of $f(x)$.

$\therefore$ α is not a root of $f'(x)$ i.e. f, f' has no common root.

$\therefore$ $(f(x), f'(x))$ is an element of F, i.e. f, f' has no common factor of degree ≥ 1 in $F[x]$ (since h.c.f. does not change in an extension).

Thus the necessary and sufficient condition that $f(x)$ may have a multiple root is that the h.c.f. (f, f') is a polynomial of degree ≥ 1.

Now if $f(x)$ is irreducible, then it can have no common factor with a polynomial of lower degree $f'(x)$ unless $f'(x) = 0\ (x)$. Thus if $f(x) \equiv \sum_{i=0}^{n} a_i x^i$ is irreducible and still have multiple roots in an extension then,

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1} = 0\ (x)$$

$\therefore$ $i a_i = 0$, for each $i \neq 0$ ..... (I)

Two cases possible:

1) If the characteristic of $F = 0$ then from (I) $a_i = 0$ for all $i \neq 0$.

$\therefore$ $f(x) \equiv a_0$

i.e. In this case an irreducible polynomial of degree ≥ 1 can not have a multiple root.

2) Let the characteristic of F be $p \neq 0$ then (I) is true only when for $a_i \neq 0$, $i = kp$ i.e. if i is an integral multiple of p.

$\therefore$ one can write $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots + a_{np} x^{np}$, some of the coefficients a_{ip} may be zero.

Conversely if f(x) is of the above type then $f'(x) = 0$

Thus $f(x) = \phi(x^p)$, when $\phi(x) = a_0 + a_1 x + \ldots + a_n x^n$.

$\therefore$ If the characteristic of F is $p \neq 0$, an irreducible polynomial of $F[x]$ can have multiple root iff $f(x) = \phi(x^p)$.

Now let f(x) be an inseparable irreducible polynomial over the field F of characteristic $p \neq 0$.

Then $f(x) = g(x^p)$

But it may be such that g(x) is again $= h(x^p)$

$\therefore \ldots f(x) = h(x^{p^2})$

So suppose that $f(x) = \phi(x^{p^m})$ but $\neq \psi(x^{p^{m+1}})$ where $m \neq 0$ as f(x) is inseparable.

Hence $\phi(y)$ is irreducible in $F[y]$. For if

$$\phi(y) = \phi_1(y)\ \phi_2(y)$$

Then $f(x) = \phi_1(x^{p^m})\ \phi_2(x^{p^m})$, which contradicts the assumption that f(x) is irreducible.

Also $\phi'(y) \neq 0$. For if $\phi'(y) = 0$, $\phi(y) = \psi(y^p)$ as before and hence $f(x) = \psi(x^{p^{m+1}})$ which contradicts our hypothesis.

Thus $\phi(y)$ is separable and in a suitable extension

$$\phi(y) = (y-\beta_1)(y-\beta_2)\ldots(y-\beta_{n_0})$$

$$\therefore f(x) = (x^{p^m} - \beta_1)(x^{p^m} - \beta_2)\ldots(x^{p^m} - \beta_{n_0})$$

Now if α_i is a root of f(x) it must be a root of $x^{p^m} - \beta_i$ (say)

$$\therefore \alpha_i^{p^m} - \beta_i = 0$$

i.e. $\beta_i = \alpha_i^{p^m}$

$$\text{and } x^{p^m} - \beta_i = x^{p^m} - \alpha_i^{p^m} = (x - \alpha_i)^{p^m}$$

$$\therefore f(x) = [(x-\alpha_1)(x-\alpha_2).....(x-\alpha_{n_0})]^{p^m}$$

$$= [\xi(x)]^{p^m}, \text{ where } \xi(x) = (x-\alpha_1)(x-\alpha_2).....(x-\alpha_{n_0}).$$

If the degree of f(x) is n then $n = n_0 p^m$

Thus f(x) has only $n_0 = n/p^m$ distinct roots, each root having the same multiplicity p^m. The splitting field of f (x) is same as that of ξ (x).

Definitions: A field N is called normal over F if [N:F] is finite and each irreducible polynomial of F[x] that has one root in N is split up completely in N[x].

Let K be the smallest extension of F such that f(x) $\in$ K[x] splits up linearly in K[x] then K is called the algebraic closure of F or algebraically closed.

Regarding algebraically closed field we state here the following important theorem due to Steinitz: " For every field F the closed field K exists. K is unique (except for isomorphism) ".

It can be proved that the field of complex numbers is algebraically closed. So every polynomial is reduced to linear factors over the complex field.

Conclusion: It is clear from the above discussions that the reducibility of polynomials depends on the domain or field over which they are defined. An irreducible polynomial may not be irreducible in an extension. In fact any polynomial has its splitting field and every field has its algebraic closure such that over the closed field any polynomial is reduced to linear factors.

4. Polynomial domain in several indeterminates.

We have defined polynomials in a single indeterminate x over a ring or integral domain or field R and obtained $R[x]$. This process is usually expressed as 'R[x] is obtained from R by the adjunction of x'.

We can proceed further. We can extend $R[x]$ by a second indeterminate y and construct $R[x][y]$. If R is a ring in which addition is communtative, then R[x] and hence R[x][y] is also a ring. The elements of this ring are

$$p(x,y) = p_m(x)\, y^m + p_{m-1}(x)\, y^{m-1} + \ldots + p_0(x),$$

where $p_k(x) = \sum_j a_{jk} x^j$.

$$\therefore p(x,y) = \sum_k \left(\sum_j a_{jk} x^j\right) y^k.$$

We define addition and multiplication in $R[x][y]$ precisely as before considering $p_i(x)$ as coefficients. Then from this definition it follows that

$$p(x,y) = \sum_k \sum_j (a_{jx} x^j)\, y^k.$$

Again one can construct $R[y]$ first and then $R[y][x]$. Then the elements of $R[y][x]$ are

$$p(y,x) = q_n(y)\, x^n + q_{n-1}(y)\, x^{n-1} + \ldots + q_0(y),$$

where $q_j(y) = \sum_k a_{jk} y^k$.

$$\therefore p(y,x) = \sum_j \sum_k (a_{jk} y^k)\, x^j.$$

Let R contains the identity 1. Then we may consider $x, y \in R[x][y]$, so we can remove the parenthesis in the above sums.

Now $ax = xa$

$(ax)\, y = y(xa)$

Taking $a = 1$; $xy = yx$

$$\therefore\ x^j y^k = y^k x^j$$

$$\therefore\ \sum_k \sum_j a_{jk} x^j y^k = \sum_j \sum_k a_{jk} y^k x^j$$

$$\therefore\ R[x][y] = R[y][x].$$

If however R does not contain 1, still one may assume

$$(ax^j)\ y^k = (ay^k)\ x^j.$$

This assumption is permissible since it does not change definitions of addition and multiplication.

From this assumption (if required)

$$R[x][y] = R[y][x] .$$

This common ring is denoted by $R[x,y]$, which is therefore independent of the order of adjunction.

In a similar manner one can get the polynomial ring

$$R[x_1, x_2 \ldots\ldots, x_n] .$$

Its elements are

$$p\ (x_1, x_2 \ldots\ldots, x_n) = \sum a_{i_1, i_2 \ldots\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} .$$

By the degree of a term $a_{i_1 i_2 \ldots\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots\ldots x_n^{i_n}$ we mean the sum $\sum_{j=1}^{n} i_j$. The maximum of the degrees of the non vanishing terms is called the degree of the polynomial $p\ (x_1, \ldots, x_n)$.

A polynomial $p\ (x_1, x_2, \ldots\ldots, x_n)$ is said to be homogeneous and of degree m if

$$p(tx_1, tx_2 \ldots\ldots, tx_n) = t^m\ p\ (x_1, x_2, \ldots\ldots, x_n)$$

$$\therefore\ \sum a_{i_1 i_2 \ldots i_n} t^{i_1 + i_2 + \cdots + i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$
$$= t^m \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Thus the necessary and sufficient condition for homogenety is that $m = i_1 + i_2 + \ldots\ldots + i_n$, for all $i_1, i_2, \ldots, i_n$.

The homogeneous polynomials are also called "forms" of degree m.

Collecting homogeneous terms of different degrees together, one can write an arbitrary polynomial of degree m

$$p(x_1, x_2, \ldots\ldots, x_n) = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

as $p(x_1, x_2, \ldots, x_n) = U_o + U_1(x_1, \ldots, x_n) + \ldots + U_m(x_1 \ldots\ldots, x_n)$, where $U_i(x_1, x_2, \ldots\ldots x_n)$ is a homogeneous polynomial of degree i, i=0, 1, ..., m.

As $R[x,y] = R[x][y]$, a polynomial $p(x,y)$ is a polynomial in y over $R[x]$ and hence one can define the derivative $p'(x,y)$ over $R[x]$ just as in the case of a single indeterminate. To avoid confusion one writes this derivative $p'(x,y)$ as $\frac{\partial p}{\partial y}$. Similarly one can define $\frac{\partial p}{\partial x}$.

From this definition one can prove the Euler's theorem on homogeneous polynomials of degree m, viz;

$$m.p(x_1, \ldots, x_n) = x_1 \frac{\partial p}{\partial x_1} + x_2 \frac{\partial p}{\partial x_2} + \cdots + x_n \frac{\partial p}{\partial x_n}.$$

For factorisation in a polynomial domain of several variables we have the following extensions of the theorems of the previous articles.

(1) R ring without divisors of zero implies $R[x]$ is a ring without divisors of zero and hence by induction $R[x_1, \ldots\ldots, x_n]$ is a ring without divisors of zero if R is so.

(2) R integral domain implies $R[x]$ integral domain and hence by induction $R[x_1, \ldots\ldots, x_n]$ is also integral domain if R is so.

(3) R integral domain with unique factorisation implies $R[x]$ integral domain with unique factorisation and hence $R[x_1, \ldots, x_n]$ is also an integral domain with unique factorisation if R is so.

The concept of primitive polynomials can also be introduced here. Let F be a field. Then a polynomial f of $F[x_1,.....x_n]$ is called primitive w. r. t. $x_1, x_2,.....x_{n-1}$, if it is primitive w. r. t. the integral domain $F[x_1,.....,x_{n-1}]$ i.e. if it does not have a non constant factor that depends only on $x_1,....,x_{n-1}$.

Proceeding precisely as in the case of one indeterminate one can prove that if $f(x_1,....,x_n)$ considered as a polynomial over $F[x_1,x_2...,x_{n-1}]$ have factors with coefficients in the quotient field of $F[x_1...,x_{n-1}]$ then it has factors with coefficients in $F\ x_1,.....x_{n-1}$.

Theorem: If a homogeneous polynomial over a ring R without divisors of zero is factorisable then the factors are homogeneous.

Proof: Let $p = p\ (x_1,.....,x_n)$ be homogeneous and of degree m and

$$= q(x_1,.....x_n)\ r\ (x_1.....,x_m)$$

For brevity suppose $q = q(x_1,.....x_n)$ and $r = r\ (x_1,....,x_n)$.

Let $q\ (x_1,....,x_n) = u_0 + u_1 + \cdots + u_s$,

and $r\ (x_1,....,x_n) = v_0 + v_1 + \cdots + v_t$, where

$u_i = u_i\ (x_1, x_2, \cdots, x_n)$ and $v_i = v_i\ (x_1, x_2, \cdots x_n)$ are homogeneous polynomials of degree i. Then

$$p\ (x_1,....,x_n) = (u_0 + u_1 + \cdots + u_s)(v_0 + v_1 + \cdots + v_t)$$
$$= u_0 v_0 + (u_0 v_1 + u_1 v_0) + (u_0 v_2 + u_1 v_1 + u_2 v_0) + \cdots$$
$$+ (u_0 v_t + u_1 v_{t-1} + \cdots) + \cdots + u_s v_t,$$

where the sum within each parethesis is a homogeneous polynomial of degree equal to the sum of the subscripts of u and v of any term within that parenthesis and no two such sums have equal degree. So $p\ (x_1,...,x_n)$ must be equal to one of these sums and all other sums within respective

parethesis be zero, i.e. zero polynomial. Then equating these sums with zero and remembering that $R[x_1,....x_n]$ has no divisors of zero we get that both $q(x_1,....x_n)$ and $r(x_1,....,x_n)$ are homogeneous. Hence the theorem.

If however R has divisors of zero then the theorem is not necessarily true. For example,

$$(a_1x^2 + a_2y^2)\ (b_1y + b_2) = a_1b_1\ x^2y + a_2b_1y^3 + a_1b_2x^2 + a_2b_2y^2$$

can be made homogeneous by choosing a_1, a_2, b_2 none equal to zero but $a_1b_2 = 0$, $a_2b_2 = 0$.

If R is a domain of unique factorisation with characteristic zero then we can use Eulers theorem on homogeneous functions to prove the above theorem.

For m.p. $= x_1\frac{\partial p}{\partial x_1} + \cdots\cdots + x_n\frac{\partial p}{\partial x_n}$

But $\frac{\partial p}{\partial x_i} = r\frac{\partial q}{\partial x_i} + q\frac{\partial r}{\partial x_i}$, hence $mp = q\left(x_1\frac{\partial r}{\partial x_1} + \cdots + x_n\frac{\partial r}{\partial x_n}\right) + r\left(x_1\frac{\partial q}{\partial x_1} + \cdots + x_n\frac{\partial q}{\partial x_n}\right)$

$$= q(k\cdot r + \alpha) + r(t\cdot q + \beta)$$

where k and t are respectively the degrees of r and q and α and β are polynomials, both zero otherwise are such that every term of α is a multiple of some term of r.

Moreover α does not contain all those terms of r whose degrees are k. Similar is the case with β.

$\therefore$ $mp = kqr + tqr + q\alpha + r\beta$

$\therefore$ $(k + t - m)\ qr + q\alpha + r\beta = 0$

$\therefore$ From the properties of R it follows that r and q divides each other i.e. they are associates.

$\therefore$ $p = er^2$, were e is a unit of R.

$\therefore$ r must be homogeneous

$\therefore$ q is also homogeneous.

Symmetric polynomials

A polynomial of $F[x_1, \ldots\ldots x_n]$, F field, which is invariant under all permutations of the indeterminates x_i is called a symmetric polynomial of $x_1, x_2, \ldots\ldots, x_n$.

The following are called elementary symmetric polynomials

$$\sigma_1 = x_1 + x_2 + \ldots\ldots + x_n$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \ldots\ldots + x_{n-1} x_n$$

$$\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_n + \ldots\ldots + x_{n-2} x_{n-1} x_n.$$

$$\sigma_n = x_1 x_2 x_3 \ldots\ldots x_n$$

Obviously each polynomial $\phi(\sigma_1, \sigma_2, \cdots, \sigma_n)$, when σ_i are replaced by their representations in x_i is a symmetric polynomial in $x_1, \ldots\ldots x_n$.

The converse of this is also true, i.e. "every symmetric polynomial in $x_1, \ldots\ldots x_n$ can be expressed uniquely in terms of elementary symmetric polynomials $\sigma_1, \sigma_2, \cdots, \sigma_n$". This is the main theorem of symmetric polynomial. We however do not give the proof here.

Now let $f(x) = x^n + a_1 x^{n-1} + \ldots\ldots + a_n$ be a polynomial of $F[x]$, F field. Then in the splitting field of f (x).

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots\ldots (x - \alpha_n),$$

$\alpha_1, \alpha_2, \cdots \alpha_n$ being the roots of f(x).

Multiplying out

$$f(x) = x^n - (\alpha_1 + \alpha_2 + \cdots + \alpha_n) x^{n-1} + \ldots\ldots + (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n.$$

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_1$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = +a_2$$

$$\alpha_1\alpha_2 \cdots \alpha_n = (-1)^n a_n.$$

That is the elementary symmetric functions in the roots of a polynomial belong to the field defining the polynomial.

Hence by the main theorem of symmetric polynomial we prove that "any function which is symmetric in all the roots of a polynomial belongs to the field defining the polynomial".

CHAPTER III

Irreducibility critéria for polynomials

In the previous chapter we gave several theorems concerning reducibility of a given polynomial in a given domain R[x]. In this chapter we wish to discuss it in a more detail.

The determination of irreducibility of an arbitrary polynomial is however difficult and this is usually done by tricks and trials. There are various irreducibility criteria applicable to different polynomials depending upon their nature, of which the most simplest one is due to Eisenstein. Because of its simple and useful characteristic we wish to begin our study with this theorem.

Eisenstien's theorem: Let $f(x) = a_o + a_1 x + \ldots\ldots + a_n x^n \in R[x]$, where R is a domain of unique factorisation with 1. Then if there exists a prime p such that

$$a_i \equiv 0 \bmod p,\ i = 0, 1, \ldots, n-1$$

$$a_n \not\equiv 0 \bmod p,$$

$$a_o \not\equiv o \bmod p^2,$$

then f(x) is irreducible in R[x] and hence in F [x], where F is the quotient field of R.

Proof: If possible let f(x) = g (x) h (x), where $g(x) = \sum_{\nu=0}^{r} b_\nu x^\nu$, $h(x) = \sum_{\nu=0}^{s} c_\nu x^\nu$, such that $r > 0, s > 0, r+s = n$.

Comparing constant terms, $a_o = b_o c_o$, but a_0 is divisible by the prime p hence either b_o divisible by p or c_o divisible by p but not both. For in that case $a_o \equiv 0 \bmod p^2$. So suppose $c_o \not\equiv 0$, mod.p. Moreover all coefficients of g (x) can not be divisible by p. For in that case

all coefficients of f(x) and in particular a_n will be divisible by p, contradicting the hypothesis.

Let b_t be the first coefficient of g (x) not divisible by p, then $0 < i \leq r < n$.

Now $0 \equiv a_i = b_i c_o + b_{i-1} c_1 + \ldots + b_o c_i$

But $b_k \equiv 0$, mod p, $k < i$ (by assumption)

$\therefore b_i c_o \equiv 0$, mod p, and since $b_i \not\equiv 0$, mod.p,

$\therefore c_o \equiv 0$, mod p, i.e. c_o divisible by p, a contradiction.

$\therefore$ f(x) is irreducible in $R[x]$.

The other part is a consequence of a previous theorem.

It may be observed that the theorem is also true if $a_i \equiv 0$, mod p, i = 1,2,,....n. $a_o \not\equiv 0$, mod p, $a_n \not\equiv 0$, mod p^2.

There are cases where the theorem is not directly applicable but is so if f(x) is replaced by f(x + a) for some $a \in R$. In which case f(x+a) irreducible implies, by a previous theorem, f(x) is irreducible.

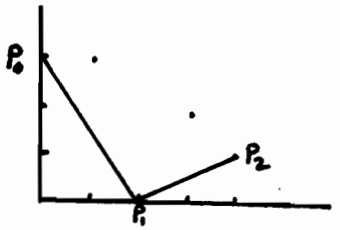
So is the case with $f(x) = x^2 + 1$, for $f(x+1) = x^2 + 2x + 2$ is irreducible over the field of rational numbers by the above criteria and hence $x^2 + 1$ is irreducible over this field.

An important generalisation of Eisenstien's theorem is due to G. Dumas. We shall give here the theorem (without proof) and deductions from it. In all our discussions in this connection, we shall suppose R a domain of unique factorisation with 1.

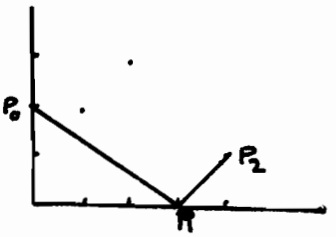
Let $f(x) = \sum_{i=0}^{n} a_i p^{k_i} x^i \in R[x]$, where p is a prime element of R and $(a_i, p) = 1$. Let the points (i, b_i) be plotted in the usual

way. From this set of points a subset $\{P_j\}_{j=0}^{r}$ is obtained by choosing P_o as the point (o, b_o), $P_r = (n, b_n)$ and P_j $(j = 1, \ldots r-1)$ as (k_j, b_{k_j}) where $(1 \leq k_j < n)$ and moreover k_j is the greatest integer such that no point (i, b_i) lies below the line through P_{j-1} and P_j for $j = 1, \ldots . r$. The figure composed of these line segments $p_{j-1}\, p_j$ is called the Newton polygon for f(x) corresponding to the given p.

As for example, if $f(x) = 72 + 72\,x + 27\,x^2 + 4\,x^3 + 6\,x^4$, the Newton polygons corresponding to p = 2 and p = 3 are as given below.



p = 2



p = 3

Follwing is the detail explainatinn for constructing Newton polygon.

Plott the points (i, b_i), occuring as indices of x and p respectively, in the terms $a_i\, p^{bi}\, x^i$ of f(x), on (s,t) plane as usual.

Let the set of these point be E. Let $P_o = (o, b_o)$. Take $P_1 = (i_j, b_{i_j}) \in E$ such that i_j is the maximum possible integer for which no point of E lies below the line segment $P_o P_1$. Then take $P_2 = (i_k, b_{i_k}) \in E$ such athat $i_k > i_j$ and i_k is the maximum possible integer for which no point of E lies below the line segment $P_1 P_2$. Continue this process until we get $P_k = (n, b_n)$. The polygon $P_1 P_2 \ldots P_{k-1} P_k$ is called the Newton polygon for f(x) relative to the prime p.

One may choose successive P_i's in the following way:

Let us start with P_o and take any point $P_1' \in E$ such that $P_1' = (i_j, b_{i_j})$, then if $\frac{b_{i_j} - b_o}{b_j} = \frac{B}{I}$, the equation of the line P_oP_1' is $It - Bs = F$ $(= Ib_o = Ib_{i_j} - Bi_j)$ and equation of any other line with the slope $\frac{B}{I}$ and passing through certain point (s^1, t^1) is $It-BS = It^1-Bs^1$.

Taking I positive, the distances of these two straight lines from the origin are $\frac{F}{\sqrt{I^2 + B^2}}$ and $\frac{I v^1 - B u^1}{\sqrt{I^2 + B^2}}$ respectively, with proper sign.

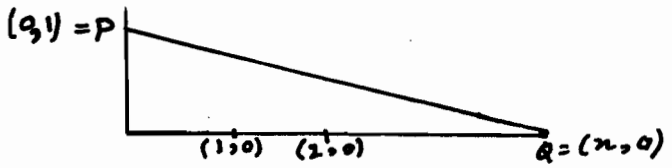
So if $It^1 - BS^1 \geq F$ the point (s^1, t^1) cannot lie below the line $P_o P_1'$. So P_1 may be obtained by starting from P_o and taking any point $(i_j, b_{ij}) \in E$ and determining $\frac{B}{I}$ and F and seeing whether $Ib_i - Bi \geq F$, for $i = 1,2,\ldots,n$ or not. If $Ib_i - Bi \geq F$ for all $i = 1,2,\ldots,n$ take the maximum i_j for which $Ib_i - Bi = F$ and call this point $(i_j, b_{i_j}) = P_1$. However, if $Ib_i - Bi \neq F$ for all $i = 1,\ldots,n$ take one of the points of E for which $Ib_i - Bi < F$. Consider this point as P_1' and find again $\frac{B}{I}$ and F and verify as above. In a finite number of steps we can find P_1. Repeat the same process to obtain P_2 etc.

Theorem of Dumas: Let the segments of the Newton polygon for f(x) corresponding to p be subdivided by lattice points occuring on them and let the resulting segments connecting adjacent points of division be called the elements of the polygon. If $f(x) = g(x)\, h(x)$, then the Newtonpolygon for g (x) corresponding to p can be formed by joining some of the elements of the polygon for f (x) without changing their

lengths or slopes. Moreover, the Newton polygon for h(x) corresponding to p can be formed in the same manner by precisely those elements not used in the polygon for g(x).

Though Dumas' theorem can not be applied to determine irreducibility of an arbitrary polynomial of R[x], however, in special cases it is helpful .

For example, Eisenstien's irreducibility criterion is a corollary of Dumas' theorem. For, here the Newton polygon is the line segment PQ, joining the points P = (0,1) and Q = (n,0), which containes no other lattice point on it. Consequently the Newton polygon of g(x) for the same p is PQ so that f(x) is irreducible.



Secondly it supplies us information about certain other polynomials. For example consider the polynomial $f(x) = 72 + 72x + 27x^2 + 4x^3 + 6x^4$. It's, Newton polygons for p = 2 and p = 3 are given in the page 58. So if it is factorisable the Newton's polygon for p = 2 gives that it will have two factors each of degree 2. Whereas, that for p = 3 gives that it will have two factors, one of degree 3 and the other of degree 1. Consequently the polynomial is not factorisable.

So, for an artibrary polynomial f(x) one may determine all the Newton's polygon for different p's occuring in it and thereby determine what the degree of possible factors maybe. If they do not agree for all p then f(x) must be irreducible.

Thirdly, Dumas' theorem provides us another generalisation of

Eisenstien's theorem.

Theorem: Let $f(x) = \sum_{i=0}^{n} a_i p^{bi} x^i \in R[x]$, p a prime, $(a_i, p) = 1$, $i = 0, 1, \ldots, n$. Then if $Ib_i - Bi > Ib_o$, $i = 1, \ldots, n-1$ and the relation $S = \dfrac{n(b_o - t)}{b_o - b_n}$ considered as an equation in (s,t) has no integral solution for $1 \leq s \leq n-1$ then f(x) will be irreducible, where $\dfrac{b_n - b_o}{n} = \dfrac{B}{I}$ i.e. $\dfrac{B}{I}$ is the reduced fraction $\dfrac{b_n - b_o}{n}$, B prime to I, I positive, and i, b_i be the indices of x and p respectively.

Proof: The proof of the theorem is quite easy. For, by the Dumas' theorem if the Newton polygon of f(x) corresponding to some p is such that it is the line segment joining the points $P_o = (0, b_o)$ and $P_1 = (n, b_n)$ and that the line segment $P_o P_1$ has no other lattice point on it then f(x) is irreducible.

By hypothesis f(x) satisfied all these conditions. For, firstly as the line through $(0, b_o)$ and (n, b_n) i.e. the equation

$$S = \frac{n(b_o - t)}{b_o - b_n}$$

has no integral solution in the range $1 \leq s \leq n-1$, there exists no lattice point within the line segment joining $(0, b_o)$ and (n, b_n) except these end points.

Moreover this is the Newton polygon for f(x). For slope of this line is $\dfrac{b_o - b_n}{n} = \dfrac{B}{I}$ and by hypothesis $Ib_i - Bi > Ib_o$, $i = 1, \ldots, n-1$.

So all points $(i, b_i) \in E$, except the points $(0, b_o)$, (n, b_n), lie above this line.

Hence the theorem.

Eisenstien's criteria is obtained by putting $b_o = 1$, $b_n = 0$. For, here the equation $s = \frac{n(b_o - t)}{b_0 - b_n} = n(1-t)$ i.e. $t = 1 - \frac{s}{n}$ has no integral solution for $1 \leq s \leq n-1$.

Moreover since $\frac{B}{I} = -\frac{1}{n}$; $Ib_i - Bi = nb_i + i > Ib_o = n$ always, if $b_i \geq 1$, $i = 1, 2, \ldots, n-1$.

$\therefore$ f (x) is irreducible.

Cor. The binomic polynomial $p_1^{b_1} p_2^{b_2} \ldots p_i^{b_i} x^n - p_{i+1}^{b_{i+1}} p_{i+2}^{b_{i+2}} \ldots p_k^{b_k}$, p_j different primes, is irreducible over R if for any $b_j \neq b_q$ the relation

$$s = \frac{n(b_j - t)}{b_j}, \quad i+1 \leq j \leq k$$

$$\text{or } s = \frac{n.t}{b_q}, \quad 1 \leq q \leq i,$$

considered as an equation in (s, t), has no integral solution in the range $1 \leq s \leq n-1$.

From the above corollary we obtain the following result:

Let $f(x) = p_1^{b_1} p_2^{b_2} \ldots\ldots p_i^{b_i} . x^n - p_{i+1}^{b_i} \ldots\ldots p_k^{b_k} = ax^n - b$ be factorisable and S be the degree of a factor. Then from the corollary

$$S = \frac{n(b_j - t)}{b_j}, \quad i+1 \leq j \leq K$$

$$= \frac{nt}{b_q}, \quad 1 \leq q \leq i \text{ ; for suitable t's}$$

So $\frac{n}{s} = \frac{b_j}{b_j - t} = \frac{bq}{t} = \frac{\ell}{m}$, say, where ℓ and m are relatively prime,

so $\ell t = mb_q \Rightarrow \ell \mid mb_q \Rightarrow \ell \mid b_q$, $1 \leq q \leq i$;

and $\ell (b_j - t) = mb_j \Rightarrow \ell \mid mb_j \Rightarrow \ell \mid b_j$, $i+1 \leq j \leq k$

So if f(x) is factorisable S exists and is less than n, so ℓ exists and is greater than 1.

That is h.c.f. $(b_1, b_2, \ldots\ldots, b_k, n) > 1$ is a necessary condition for the reducibility of f(x) as given above.

This result implies (1) $p \mid a$ but $p^2 \nmid a$, p prime, $\Rightarrow$ f(x) irreducible,

(2) $p \mid b$ but $p^2 \nmid b$, p prime, $\Rightarrow$ f(x) irreducible,

(3) n prime $\Rightarrow$ f (x) irreducible unless

$b_i = n.r$, $i = 1, \ldots, k$.

Dumas' theorem supplies us also some information about the maximum possible number of factors of a polynomial of $R[x]$.

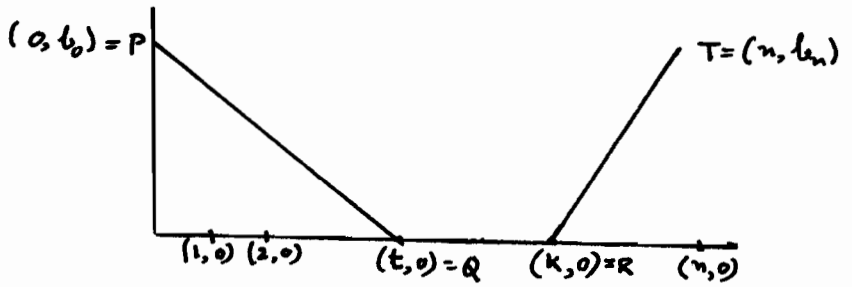
Theorem: Let $f(x) = a_o + a_1 x + \ldots\ldots + a_n x^n$ be a polynomial ~~with~~ $\in R[x]$ ~~integral coefficients~~ and let a_t and a_k be the 1st and last coefficients respectively of f(x) such that they are not divisible by a prime p then the maximum possible number of factors of f (x) over R is

$$\{ \min (t, b_o) + (k-t) + \min (n-k, b_n) \}$$

where $p^{b_o} \mid a_o$ but $p^{b_o+1} \nmid a_o$ and $p^{b_n} \mid a_n$ but $p^{b_n+1} \nmid a_n$.

In case the no. of factors is $\{ \min. (t, b_o) + \min (n-k, b_n) + U \}$, for some positive integer U, then there exist U factors whose leading coefficient and constant terms are not divisible by p.

Proof: The Newton polygon of f(x) corresponding to p is the following polygon PQRT.



The maximum no. of lattice points on PQRT is obviously

$$\min.\ (t,\ b_o) + k-t + \min.\ (n-k,\ b_n).$$

So maximum no. of factors of f(x) over R cannot be greater than this number. This is the proof of the 1st part.

If the number of factors of f(x) is

$$\min\ (t, b_o) + \min\ (n-k,\ b_n) + U,$$

where U positive, then surely the Newton polygon for U factors will be parts of QR. So their constant terms and leading coefficients cannot be divisible by p.

Cor. If t = k, in the theorem, then the maximum possible number of factors of f(x) over R is

$$\min,(t,b_o) + \min.\ (n-t,\ b_n).$$

This result can be stated formally as:

Let $f(x) = \sum_{i=0}^{n} a_i\ x^i$ be a polynomial with ~~integral~~ coefficients $\in R$.
Let a prime p divides every coefficient of f(x) except a_t and $p^{b_9} \mid a_9$, $p^{b_o+1} \nmid a_o$, $p^{b_n} \mid a_n$, $p^{b_n+1} \nmid a_n$ then maximum possible number of factors of f(x) over R is

$$\min.\ (t,b_o) + \min.\ (n-t,\ b_n).$$

The above theorem can be further generalised: -

Theorem: Let $f(x) = a_o + a_1x + \ldots + a_n\ x^n$, $a_i \in R$. . Let p_i be

an arbitrary prime element such that $p_i^{b_{oi}} \mid a_o$, $p_i^{b_{oi}+1} \nmid a_o$, $p_i^{b_{ni}} \mid a_n$, $p_i^{b_{ni}+1} \nmid a_n$ and a_{t_i} and a_{k_i} be the 1st and last coefficients. respectively of f(x) such that they are not divisible by p_i, then the maximum possible number of factors of f(x) over R is

$$\min.\left\{ \min.(t_i, b_{o_i}) + k_i - t_i + \min(n-k_i, b_{n_i}) \right\} .$$

In fact one needs only to calculate for those primes which divide at least one of a_o or a_n. For, for other primes the number within the 2nd bracket is n.

Cor. For the polynomial $p_1^{b_1} p_2^{b_2} \ldots\ldots p_i^{b_i} x^n - p_{i+1}^{b_{i+1}} \ldots\ldots p_k^{b_k}$ the maximum number of irreducible factors is

$$\min.\left\{ \min.(n, b_j) \right\}, \quad 1 \leq j \leq k.$$

So if some $b_j = 1$ then the above polynomial is irreducible.

An important class of irreducible polynomials over the field of rational numbers are the cyclotomic polynomials.

Consider the polynomial $f(x) = x^n - 1$ over the field of rational numbers. Then $f'(x) = nx^{n-1} \neq 0(x)$, i.e. $f'(x)$ has no root other than zero. Hence f(x) has no multiple root.

In the splitting field of f(x), $f(x) = (x-\alpha_1)(x-\alpha_2) \ldots\ldots (x-\alpha_n)$, where $\alpha_1, \alpha_2, \ldots \alpha_n$ are the n distinct nth roots of 1.

If α is a root of $x^n - 1 = 0$ such that it is not a root of any polynomial $x^m - 1$, $m < n$, then α is called a primitive root of $x^n - 1$. Then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are all distinct and each of them is a root of $x^n - 1$. Moreover $x^n - 1$ has only n roots, so they are all the roots of $x^n - 1$.

The number of primitive roots of $x^n - 1$ is denoted by $\phi(n)$, which is called Euler's ϕ function or indicator.

We shall find the value of $\phi(n)$.

If α is a primitive root then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ are all the roots of $x^n - 1$. Also if the order of α^h is n then α^h is also a primitive root. Let us find the order of α^h for arbitrary h.

Suppose $(h,n) = \rho$ then $n = \lambda_1 \rho$, $h = \lambda_2 \rho$, $(\lambda_1, \lambda_2) = 1$

$\therefore \quad \lambda_1 = \frac{n}{\rho} = \frac{n}{(n,h)}$

Now $(\alpha^h)^{\lambda_1} = \alpha^{\lambda_1 \lambda_2 \rho} = \alpha^{\lambda_2 n} = (\alpha^n)^{\lambda_2} = 1$

Also λ_1 is the least +ive integer satisfying this condition.

For, let $\theta < \lambda_1$ and $\alpha^{h\theta} = 1$

Then as $(\lambda_1, \lambda_2) = 1$

$\therefore \lambda_1 \theta_1 + \lambda_2 \theta_2 = 1$ for suitable θ_1 and θ_2.

$\therefore \quad \alpha^{\theta\rho} = \alpha^{\theta\rho(\lambda_1\theta_1 + \lambda_2\theta_2)} = \alpha^{\theta\rho\theta_1\lambda_1} \cdot \alpha^{\theta\rho\theta_2\lambda_2}$

$= \alpha^{n\theta\theta_1} \cdot \alpha^{h\theta\theta_2}$

$= 1$

which implies $\alpha^{\theta\rho} = 1$ where $\theta\rho < \lambda_1\rho = n$ since $\theta < \lambda_1$, contradicting that α is a primitive root.

$\therefore \quad \lambda_1 = \frac{n}{(n,h)}$ is the order of α^h.

So α^h is a primitive root iff $(n,h) = 1$

So number of primitive roots is equal to the number of positive integers less than n and prime to n, including the interger 1 as one of such integers.

Let $\rho = \phi(n)$ and $\alpha_1, \alpha_2, \cdots, \alpha_\rho$ be the primitive roots of $x^n - 1$

Then the polynomial $X_n(x) = (x-\alpha_1)(x-\alpha_2).....(x-\alpha_r)$ is called the cyclotomic polynomial of order n. Its roots are therefore the primitive roots of x^n-1 and its degree is $r = \phi(n)$.

Theorem: $X_n(x)$ is irreducible over R_o, the field of rational numbers.

Proof: Firstly we shall give some difinitions.

Let $f(x) = \prod_{i=1}^{m} (x-\beta_i)$

$g(x) = \prod_{j=1}^{n} (x-\gamma_j)$

Then we define $R(f,g) = \prod_{i=1}^{m} g(\beta_i) = (-1)^{mn} \prod_{j=1}^{n} f(\gamma_j) = (-1)^{mn} R(g,f)$

and $D(f) = (-1)^{\frac{m(m-1)}{2}} . R(f,f') = (-1)^{\frac{m(m-1)}{2}} f'(\beta_i)$.

R is called the resultant of the polynomials f(x) and g(x), while D is called the discriminant of the polynomial f(x).

For the product polynomial f(x). g(x)

$$D(f.g) = \pm R(f.g., f'g + f.g')$$

$$= \pm \prod_i f'(\beta_i) g(\beta_i) \prod_j f(\gamma_j) g'(\gamma_j)$$

$$= \pm \prod_i f'(\beta_i) \prod_j g'(\gamma_j) \prod_i g(\beta_i) \prod_j f(\gamma_j)$$

$$= \pm D(f) D(g) R(f,g)^2$$

Similarly $D(f.g.h.) = \pm D(f) D(g) D(h) R(f,g)^2 R(g.h)^2 R(h,f)^2$

So if $f(x) = x^n - 1$, then β_i are $1, \alpha, \ldots, \alpha^{n-1}$,

and $f'(x) = n x^{n-1}$.

$\therefore D(x^n-1) = \pm n.n. \alpha^{n-1} . n\alpha^{2(n-1)} ..... n\alpha^{(n-1)^2}$.

$$= \pm n^n \cdot \alpha^{(1+.....+n)(n-1)}$$

$$= \pm n^n \cdot \alpha^{\frac{(n+1)\ (n-1)n}{2}}$$

$$= \pm n^n .$$

Now we give the proof of the theorem, which is due to I. Schur.

Let X_n be reducible over R_0 and f(x) be an irreducible factor of X_n. Assume $\eta = \alpha^p$ where $(p,n) = 1$, α root of f(x), p prime and suchat that η is not a root of f(x).. η exists, otherwise all roots of X_n are roots of f(x) consequently $f(x) = X_n$ i.e. X_n is irreducible.

Assume g(x) be the irreducible polynomial with leading coefficient 1 and with root η. Then as g(x) is irreducible and g(x), X_n have common root η, $g(x) \mid X_n$. Also we may assume leading coefficient of f(x) be 1 and as f(x), g(x) are both irreducible (f(x), g(x)) = 1

$$\therefore f(x) \cdot g(x) \mid X_n$$

which implies $f(x) \cdot g(x) \mid x^n - 1$

$$\therefore x^n - 1 = f(x)\, g(x)\, h(x).$$

As the leading coefficient for f(x), g(x) and x^n-1 is 1, the leading coefficient of h (x) is also 1. As x^n- 1 has integral coefficients we have by Gauss* theorem all f(x), g(x), h(x) have integral coefficients.

$$\therefore D(x^n - 1) = \pm n^n = D(f.g.h.) = \pm D(f).\ D(g).\ D(h).$$

$R^2(f,g)\ R^2(g,h)\ R^2(h,f)$. As all the factors in the right hand side are integers, we may write n^n = an integer. R(f,g).

* Gauss theorem: If $f(x) = g(x)h(x) \in R_0[x]$, leading coefficients of f(x), g(x), h(x), be 1, then f(x) have integral coefficients implies both g(x), h(x) have integral coefficients.

Now if $g(x) = (x-\eta)(x-\eta_2)\ldots\ldots(x-\eta_t)$, then

$R(f,g) = \pm f(\eta)\, f(\eta_2)\ldots\ldots f(\eta_t)$

Again, $f(x^p) \equiv (f(x))^p$, mod p

$= (f(x))^p + p.f_1(x)$,

where $f_1(x)$ has integral coefficients.

$\therefore f(\eta) = f(\alpha^p) = 0 + p.f_1(\alpha)$, since $f(\alpha) = 0$,

$= p.\ f_1(\eta^p)$, since η is also a primitive root.

As η_i are roots of the same irreducible polynomial $g(x)$,

$\therefore f(\eta_i) = p.f_1(\eta_i^p)$, $i=1, 2\ldots t$, where $\eta_1 = \eta$.

$\therefore R(f,g) = \pm p^t f_1(\eta^p)\ f_1(\eta_2^p)\ f_1(\eta_3^p)\ldots f_1(\eta_t^p)$.

$\ldots\ p \mid R(f,g)$.

$\therefore p \mid n^n \Rightarrow p \mid n$, contradicts that $(p,n) = 1$.

Hence the theorem.

<u>Abel's theorem</u>: If p is prime $x^p - a$ is reducible iff $a = b^p$, $b \notin F$, F field, $a \notin F$.

Proof: If $a = b^p$, then $x^p - a = x^p - b^p = (x-b)(x^{p-1} + bx^{p-2} + \ldots + b^{p-1})$, when characteristic of $F \neq p$, and $= (x-b)^p$, when characteristic of F is p.

Conversely, let $x^p - a$ be reducible, then if θ is a root $x^p - a = 0$ then $\theta, \epsilon\theta, \ldots\ldots \epsilon^{p-1}\theta$ are all the roots of $x^p - a = 0$, where ϵ is a primitive root of $x^p - 1 = 0$.

$\therefore x^p - a = (x-\theta)(x-\epsilon\theta)\ldots\ldots(x-\epsilon^{p-1}\theta)$

$= \phi(x) \cdot \psi(x)$ say.

then $\phi(x) = (x - \theta\epsilon^{\nu_1})(x-\theta\epsilon^{\nu_2})\ldots\ldots(x-\theta\epsilon^{\nu_b})$

$\therefore$ The constant term of $\phi(x) = \theta^b \epsilon^{\nu_1+\nu_2+\cdots+\nu_b} = c$, say, $\in F$.

Then $c^p = \theta^{pp} \epsilon^{p(v_1+\cdots+v_p)} = a^s$, since $\theta^p = a$, $\epsilon^p = 1$.

Now (s,p) = 1, hence there exist integers n, v such that $ns+vp = 1$.

$$\therefore a^{ns+vp} = a^{ns} \cdot a^{vp}$$

$$= (a^s)^n \cdot (a^v)^p$$

$$= (c^p)^n \cdot (a^v)^p$$

$$= (c^n \cdot a^v)^p$$

$$= b^p, \text{ where } b = c^n \cdot a^v \in F.$$

Theorems of Capelli

Let f(x) = g(h(x)), where g(y), h(x) both are polynomials over a field F of characteristic zero and both have leading coefficients 1.

Also let in the splitting field of g(y)

$$g(y) = y^k + a_1 y^{k-1} + \cdots + a_k = (y-\beta_1)(y-\beta_2)\cdots(y-\beta_k),$$

i.e. $\beta_1, \beta_2, \cdots, \beta_k$ are all the roots of g(y).

Theorem 1: f(x) is reducible over F iff(i) either g(y) is reducible over F, or (ii) g(y) irreducible over F and $h(x)-\beta_i$ is reducible over $F(\beta_i)$, i=1,2.....,k.

Proof: Let f(x) be reducible then since

$$f(x) = g(h(x)) = (h(x)-\beta_1)(h(x)-\beta_2)\cdots(h(x)-\beta_k).$$

either g(y) is reducible or $h(x)-\beta_i$ is reducible over $F(\beta_i)$, i=1,....k.

Conversely let g(y) be reducible then obviously f(x) is reducible.

Otherwise let $h(x)-\beta_i$ is reducible over $F(\beta_i)$, then

over $F(\beta_1)$....$h(x)-\beta_1 = \phi_1(\beta_1, x)\cdot\phi_2(\beta_1, x)\cdots\phi_t(\beta_1, x)$,

over $F(\beta_2)$....$h(x)-\beta_2 = \phi_1(\beta_2, x)\cdot\phi_2(\beta_2, x)\cdots\phi_t(\beta_2, x)$,

Over $F(\beta_k)$....$h(x)-\beta_k = \phi_1(\beta_k, x)\cdot\phi_2(\beta_k, x),\ldots\phi_t(\beta_k, x)$, where

$\phi_i(\beta_j, x)$ are irreducible over $F(\beta_j)$.

$\therefore$ Multiplying $f(x) = \prod_{r=1}^{k} (h(x) - \beta_r) = \Phi_1(x)\,\Phi_2(x)\ldots\Phi_t(x)$,

where $\Phi_\lambda(x) = \phi_\lambda(\beta_1, x)\,\phi_\lambda(\beta_2, x)\ldots\phi_\lambda(\beta_k, x)$, $\lambda = 1, 2, \ldots, t$.

As the r.h.s. is symmetric in all β_i's hence $\Phi_\lambda(x)$ is a polynomial over F.

Thus $f(x) = \prod_{\lambda=1}^{t} \Phi_\lambda(x)$ i.e. $f(x)$ is reducible over F.

Lemma: $\Phi_\lambda(x)$ is irreducible over F.

If not let $\psi(x)$ be an irreducible factor of $f(x)$, then $\psi(x)$ is a factor of some $\Phi_i(x)$. For, as $\psi(x)$ is irreducible $(\Phi_i(x), \psi(x)) = 1$ or $\psi(x)$ and $F[x]$ is a domain of unique factorisation.

Suppose $\psi(x) \mid \phi_1(x)$.....(a)

But $\Phi_1(x) = \prod_{s=1}^{k} \phi_1(\beta_s, x)$, where $\phi_1(\beta_j, x)$ are irreducible over $F(\beta_j)$.

Hence by the same argument, as above, we have $\phi_1(\beta_j, x) \mid \psi(x)$, form some j, over $F(\beta_j)$

$\therefore \psi(x) = \phi_1(\beta_j, x) \cdot q(\beta_1, x)$, over $F(\beta_j)$.

But β_j is a root of an irreducible polynomial $g(y)$.

$\therefore \psi(x) = \phi_1(\beta_1, x)\, q(\beta_1, x)$

$\psi(x) = \phi_1(\beta_2, x)\, q(\beta_2, x)$

$\psi(x) = \phi_1(\beta_3, x)\, q(\beta_3, x)$

$\psi(x) = \phi_1(\beta_k, x)\, q(\beta_k, x)$

But, as $\phi_1(\beta_i, x)$ are irreducible, $(\phi_1(\beta_i, x), \phi_1(\beta_j, x)) = 1$

$\therefore \phi_1(\beta_1, x) \cdot \phi_1(\beta_2, x) \cdot \ldots \cdot \phi_1(\beta_k, x) = \Phi_1(x) \mid \psi(x)$.....(b)

$\therefore$ from (a) and (b) $\Phi_1(x) = \psi(x)$ an irreducible factor of $f(x)$.

Hence the lemma.

Theorem 2: Let $f(x) = g(h(x)) = \bar{g}(\bar{h}(x))$, where

$g(y) = y^k + \ldots = (y-\beta_1)(y-\beta_2)\ldots(y-\beta_k)$ in the splitting field of $g(y)$, and

$\bar{g}(y) = y^h + \ldots\ldots\ldots$, $h(x) = x^h + \ldots\ldots$, $\bar{h}(x) = x^k + \ldots$

so that degree $f(x) = m = kh$ and $(k,h) = 1$.

Then $f(x)$ is reducible over F iff $g(y)$ or/and $\bar{g}(y)$ are reducible over F.

Proof: If $g(y)$ or/and $\bar{g}(y)$ is reducible then obviously $f(x)$ is reducible.

Conversely let $f(x)$ be reducible and assume $g(y)$, $\bar{g}(y)$ are irreducible over F. Then by theorem 1, $h(x) - \beta_i$ be reducible over $F(\beta_i)$, so that $h(x) - \beta_i = \phi_1(\beta_i, x) \cdot \phi_2(\beta_i, x) \ldots\ldots \phi_t(\beta_i, x)$, and

$f(x) = \Phi_1(x) \cdot \Phi_2(x) \ldots\ldots \Phi_t(x)$.

Degree $\Phi_\lambda(x) = m_\lambda = kn_\lambda$ where n_λ = degree $\phi_\lambda(\beta_i, x)$ which is independent of i.

Also $m_\lambda = h\bar{n}_\lambda$ (considering the polynomial $\bar{g}(\bar{h}(x))$.

$\therefore k \mid m_\lambda, h \mid m_\lambda$ and $(k,h) = 1$

$\therefore kh \mid m_\lambda$ i.e. $m \mid m_\lambda \Rightarrow m = m_\lambda$

$\therefore$ degree $f(x)$ = degree $\Phi_\lambda(x)$, i.e. $t=1 \Rightarrow f(x)$ is not reducible, a contradiction.

Hence the theorem.

The most important application of the above theorems is the determination of reducibility of the binomial expression $x^n - a$.

Let $f(x) = x^n - a$, $a \in F$, F field of characteristic zero, $n \geq 2$.

Let $m = kh$, where $(k,h) = 1$

Then $f(x) = x^n - a = x^{kh} - a = (x^k)^h - a = (x^h)^k - a$.

$\therefore$ By the theorem 2,

$x^n - a$ is reducible over F iff either $y^k - a$ or $y^h - a$ or both are reducible over F.

Let $n = p_1^{k_1} p_2^{k_2} \ldots\ldots p_s^{k_s}$, where p_i are different prime integers. Then $x^n - a$ is reducible over F iffat least one of $x^{p_1^{k_1}} - a, \ldots\ldots$ $x^{p_s^{k_s}} - a$ is reducible over F.

Now $x^{p^u} - a$ is reducible over F, for odd p, iff $x^p - a$ reducible over F.

For, by theorem 1, $x^{p^u} - a = (x^{p^{u-1}})^p - a$ reducible over F iff either $g(y) = y^p - a$ reducible over F or $g(y)$ is irreducible over F and $h(x) - \beta = x^{p^{u-1}} - \beta$ is reducible over $F(\beta)$, where β is a root of $g(y)$ i.e. $\beta^p = a$.

But, by the same theorem, $h(x) - \beta = x^{p^{u-1}} - \beta$ is reducible over $F(\beta)$ implies $g_1(y) = y^p - \beta$ is reducible over $F(\beta)$ or $y^p - \beta$ is irreducible over $F(\beta)$ and $x^{p^{u-2}} - \beta'$ is reducible over $F(\beta, \beta') = F(\beta')$,

Where β' is a root of $g_1(y)$, i.e. $\beta'^p = \beta$.

Now in the first case, i.e. when $g_1(y) = y^p - \beta$ is reducible over $F(\beta)$ we have by Abel's theorem $\beta = (\gamma)^p$ where $\gamma \in F(\beta)$ i.e.

$$\gamma = a_0 + a_1\beta + \ldots + a_{p-1}\beta^{p-1},$$
$$= \varphi(\beta) \text{ say}$$
$$\therefore \beta = (\varphi(\beta))^p$$

As β is a root of an irreducible polynomial $g(y) = y^p - a$

$$\beta_2 = (\varphi(\beta_2))^p$$
$$\ldots\ldots\ldots$$
$$\beta_p = (\varphi(\beta_p))^p, \text{ where } \beta, \beta_2, \ldots \beta_p \text{ are all the roots of } g(y).$$

Hence multiplying $\beta \cdot \beta_2 \ldots \beta_p = (\varphi(\beta) \cdot \varphi(\beta_2) \ldots\ldots \varphi(\beta_p))^p$

The expression under the parenthesis in the right hand side is a symmetric function in all the roots of g(y) hence belongs to the ground field F.

$\therefore \quad \beta\beta_2 \cdots\cdots \beta_p = b^p$, where $b \in F$

But $x^p - a = (x-\beta)(x-\beta_2)\cdots\cdots(x-\beta_p)$

$$\Rightarrow \beta\beta_2 \cdots\cdots \beta_p = a$$

$\therefore \quad a = b^p$

That is $y^p - a$ is reducible (by Abel's theorem), which contradicts our previous hypothesis. Hence $x^{p^{n-1}} - \beta$ is reducible over $F(\beta)$ implies $g_1(y) = y^p - \beta$ is irreducible over $F(\beta)$ and $x^{p^{n-2}} - \beta'$ is reducible over $F(\beta')$, where $\beta'^p = \beta$

Arguing $n-2$ times in this way we prove that $x^p - \xi$ is reducible over $F(\xi)$, where $\xi^p = \eta$ and $\eta^{p^{n-3}} = a$.

So by theorem 1, either $x^p - \xi$ reducible over $F(\xi)$ or $x^p - \xi$ is irreducible over $F(\xi)$ and $x^p - \xi'$ is reducible over $F(\xi')$ where $\xi'^p = \xi$

The first case contradicts that $x^p - \eta$ was irreducible over $F(\eta)$ and the second case contradicts that $x^p - \xi$ was irreducible over $F(\xi)$.

Hence the result.

To consider the reducibility of $x^{2^n} - a$ over F we prove that $x^{2^n} - a$ is reducible over F iff(i) $a = b^2$, or (ii) when $n > 1$, $a = -4c^4$, $c \in F$.

Proof: The statement can easily be verified when $n = 1$ and $n = 2$.

Let us assume that the statement is true when $n = n-1$ and consider $x^{2^n} - a$.

Now if $a = b^2$ then $x^{2^n} - a = (x^{2^{n-1}})^2 - b^2 = (x^{2^{n-1}} + b)(x^{2^{n-1}} - b)$,

and if $a = -4b^4$ $x^{2^n} - a = (x^{2^{n-2}})^4 + 4b^4$

$$= (x^{2^{n-1}} + 2bx^{2^{n-2}} + 2b^2)(x^{2^{n-1}} - 2bx^{2^{n-2}} + 2b^2)$$

Conversely let $x^{2^n} - a = (x^{2^{n-1}})^2 - a$ be reducible over F. Hence, by theorem 1, either $y^2 - a$ is reducible over F. i.e. $a = b^2$, for some $b \in F$, or $y^2 - a$ is irreducible over F and $x^{2^{n-1}} - \sqrt{a}$ is reducible over $F(\sqrt{2})$. Hence by our induction assumption either (i) $\sqrt{a} = (c\sqrt{a} + b)^2$, $b, c, \in F$ i.e. $\sqrt{a} = c^2 a + b^2 + 2bc\sqrt{a}$.

$\therefore c^2 a + b^2 = 0$, $2bc = 1$ which implies $c = \frac{1}{2b}$, $c^2 = \frac{1}{4b^2}$

$\therefore a = -4b^4$.

or (ii) $\sqrt{a} = -4d^4$, $d \in F(\sqrt{2})$,

$= -4(c\sqrt{a} + b)^4$; $b, c, \in F$,

$= -4(c^2 a + b^2 + 2bc\sqrt{a})^2$

$= -4(C\sqrt{a} + B)^2$

$= -4(C^2 a + B^2 + 2BC\sqrt{a})$

$\therefore C^2 a + B^2 = 0$, $-8BC = 1$ i.e. $C = \frac{1}{2} \cdot \frac{-1}{2^2 B}$ OR $C^2 = \frac{1}{4} \cdot \frac{1}{2^4 B^2}$

$\therefore a = -4 \cdot 2^4 B^4 = -4h^4$, $h \in F$.

$\therefore$ The statement is true when $k = n$. Hence the statement is true in general.

Wenow give a method for determining all the factors of a binomial expression over the field of rational numbers. The method is, however, labourious and have very little practical utility

Let F by any field. $x^3 - c$ be an irreducible polynomial over F having θ as a root. Then in $F(\theta)$ any element $\alpha \neq 0$ is given by

$$\alpha = a_1 + a_2\theta + a_3\theta^2 , \quad (a_1, a_2, a_3) \neq (0,0,0) \in F.$$

Then $\alpha^{-1} = b_1 + b_2\theta + b_3\theta^2 \in F(\theta)$, $b_i \in F$.

$\therefore 1 = \alpha\alpha^{-1} = (a_1 + a_2\theta + a_3\theta^2)(b_1 + b_2\theta + b_3\theta^2)$.

Equating coefficients of powers of θ

$$1 = a_1b_1 + a_3b_2c + a_2b_3c$$
$$0 = a_2b_1 + a_1b_2 + a_3b_3c \qquad \ldots\ldots(a)$$
$$0 = a_3b_1 + a_2b_2 + a_1b_3$$

As α^{-1} exists, (a) is solvable for b_1, b_2, b_3 and

$$b_1 = \frac{\begin{vmatrix} 1 & a_3c & a_2c \\ 0 & a_1 & a_3c \\ 0 & a_2 & a_1 \end{vmatrix}}{D} \qquad b_2 = \frac{\begin{vmatrix} a_1 & 1 & a_2c \\ a_2 & 0 & a_3c \\ a_3 & 0 & a_1 \end{vmatrix}}{D} \qquad b_3 = \frac{\begin{vmatrix} a_1 & a_3c & 1 \\ a_2 & a_1 & 0 \\ a_3 & a_2 & 0 \end{vmatrix}}{D},$$

Where $D = \begin{vmatrix} a_1 & a_3c & a_2c \\ a_2 & a_1 & a_3c \\ a_3 & a_2 & a_1 \end{vmatrix}$.

So that $D \neq 0$.

As for any triplets of elemts. a_1, a_2, a_3 not all zero we can get α and α^{-1}; $D \neq 0$ for any such $a_1, a_2, a_3 \in F$.

If however $x^3 - c$ is reducible over F then there exists at least one set of three elements $(a_1, a_2, a_3) \neq (0,0,0)$ such that

$$0 = a_1 + a_2\theta + a_3\theta^2$$

So that (a) is not solvable for b's i.e. $D = 0$

Generalising the above result we get, the necessary and sufficient condition in order that $x^n - c$, $c \in F$, be irreducible over F is

$$D_1 = \begin{vmatrix} a_1 & a_nC & a_{n-1}C & \cdots & a_2C \\ a_2 & a_1 & a_n C & \cdots & a_3C \\ \cdots & \cdots & & & \cdots \\ \cdots & \cdots & & & \cdots \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_1 \end{vmatrix} \neq 0$$

for any set of n elements $a_1, a_2 \ldots\ldots\ldots, a_n \in F$ and not all zero.

So if C is any rational number we get a similar determinent over the field of rational numbers, the vanishing of which for a set of rational nos. $(a_1, a_2, \ldots\ldots, a_n) \neq (0,0,\ldots\ldots,0)$ is the necessary and sufficient condition for the factorisability of the polynomial $x^n - C$ over rational field.

Now if θ be any root of $x^n - C = 0$ then $\theta, \xi\theta, \xi^2\theta, \cdots, \xi^{n-1}\theta$ are all the roots of $x^n - C = 0$, where ξ is a primitive nth root of unity.

$$\therefore x^n - C = (x - \theta)(x - \xi\theta)\ldots\ldots\ldots(x - \xi^{n-1}\theta)$$

$$= \phi_1(x) \cdot \phi_2(x) \ldots\ldots\ldots \phi_K(x) \text{ say.}$$

then $\phi_j(x) = (x - \xi^{\nu_1}\theta)(x - \xi^{\nu_2}\theta)\ldots\ldots\ldots(x - \xi^{\nu_s}\theta)$, $1 \leq s \leq n-1$

The coefficient of x^r, $0 \leq r \leq s$ in $\phi_j(x)$ is, say,

$$a_r = (-1)^{s-r}\theta^{s-r} \cdot \alpha$$

where α = sum of products of combinations of $\xi^{\nu_1}, \xi^{\nu_2}, \ldots, \xi^{\nu_s}$ taken s-r at a time.

Then $|a_r| = |\theta^{s-r}| \cdot |\alpha|$

$$\leq |\theta^{s-r}| \cdot (|\xi^{\nu_i}| + |\xi^{\nu_j}| + \cdots\cdots + |\xi^{\nu_k}|)$$, the number of terms within the parenthesis being $\binom{s}{s-r}$.

$= |C|^{\frac{s-r}{n}} \cdot \binom{s}{s-r}$ $\quad [\because |\epsilon^{\nu}| = 1$

$= |C|^{\frac{s-r}{n}} \cdot \binom{s}{r}$ $\quad \lessdot |C|^{\frac{s-r}{n}} \binom{n}{n}$

$\leq |C|^{\frac{s-p}{n}} \cdot \binom{n}{\frac{n}{2}}$ or $|C|^{\frac{s-p}{n}} \binom{n}{\frac{n-1}{2}}$ acc. as n is even or odd.

(1).....So when $|C| \geq 1$, the coeff. of x^r, $0 \leq r \leq n-1$ in $\phi_j(x)$ is $\lessdot |C| \cdot \binom{n}{\frac{n}{2}}$ if n is even

and $\lessdot |C| \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd.

(2)....and when $|C| \leq 1$, the coeff. of x^r, $0 \leq r \leq n-1$, is $|C|^{\frac{1}{n}} \cdot \binom{n}{\frac{n}{2}}$,

if n is even and is $\lessdot |C|^{\frac{1}{n}} \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd.

Now let $C = \frac{p}{q}$, $(p,q) = 1$, both p,q positive, otherwise we write $x^n - C$ as $x^n + C$.

Then $x^n - C = \phi_1(x) \cdot \phi_2(x) \ldots\ldots \phi_k(x)$

$qx^n - p = \phi_{11}(x) \cdot \phi_{21}(x) \ldots\ldots \phi_{k1}(x)$

such that $\phi_{j1}(x)$ have integral coefficients.

So when $|C| \geq 1$, from (1), coeff. of x^r, $0 \leq r \leq n-1$, in $\phi_{j1}(x)$ is $\lessdot q \cdot |C| \cdot \binom{n}{\frac{n}{2}}$ if n is even and is $\lessdot q \cdot |C| \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd i.e. $\lessdot p \cdot \binom{n}{\frac{n}{2}}$ if n is even and $\lessdot p \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd.

and when $|C| \leq 1$, from (2), coeff of x^r, $0 \leq r \leq n-1$, in $\phi_{j1}(x)$ is $\lessdot q \cdot |C|^{\frac{1}{n}} \cdot \binom{n}{\frac{n}{2}}$ if n is even and $\lessdot q \cdot |C|^{\frac{1}{n}} \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd,

i.e. $\lessdot q \cdot \binom{n}{\frac{n}{2}}$, if n is even and $\lessdot q \cdot \binom{n}{\frac{n-1}{2}}$ if n is odd.

Thus the coefficients of $\phi_{j1}(x)$, which are integral, are numerically less than max $(p,q).\left(\frac{n}{\frac{n}{2}}\right)$, if n is even and numerically less than

max. $(p,q).\left(\frac{n}{\frac{n-1}{2}}\right)$, if n is odd.

But $(a_1, a_2, \ldots\ldots, a_n) \neq (0,0,\ldots,0)$ be the coefficients of $\phi_{j1}(x)$ iff

$$D_1 = \begin{vmatrix} a_1 & a_n c & a_{n-1} C & \ldots & a_2 c \\ a_2 & a_1 & a_n c & \ldots & a_3 c \\ \ldots\ldots & \ldots & \ldots & \ldots & \ldots \\ a_n & a_{n-1} & a_{n-2} & & a_1 \end{vmatrix} = 0$$

So we can choose any set of n integers from within $-\ell$ to ℓ (or from within - m to m), (where ℓ = max $(p,q).\left(\frac{n}{\frac{n}{2}}\right)$, if n even and

m= max$(p,q).\left(\frac{n}{\frac{n}{2}} - 1\right)$, if n odd) and put it in D_1.

If $D_1 = 0$ then they are the coefficients of some $\phi_{j1}(x)$ such that a_i is the coefficient of x^{i-1}. If $D_1 \neq 0$ then they are not the coefficients of any factor of $q\,x^n - p$.

We repeat this process with all possible choice of n integers taken from within $-\ell$ to ℓ (or from within - m to m). If there exists no such n integers for which $D_1 = 0$ then $q\,x^n - p$ is irreducible. Consequently $x^n - p/q$ i.e. $x^n - C$ irreducible.

However if $\phi_{j1}(x)$ is known then $\phi_j(x)$ will be known from the relation $q^{\frac{s}{n}}\,\phi_j(x) = \phi_{j1}(x)$, s being the degree of $\phi_{j1}(x)$.

Schoenemann polynomials: Let $f(x) = \phi(x)^n + p.h(x)$, where $\phi(x)$ is irreducible mod p, p a prime element, $n>1$ and r = degree $\phi(x) \geq 1$. and degree $h(x) < nr$, is a polynomial of $R[x]$, where R is a domain of unique factorisation.

Schoenemann theorem: $f(x)$ is reducible mod p^2 iff $h(x) \equiv 0(x)$ (mod p and $\phi(x)$), ie. iff all coefficients of $h(x)$ are divisible by p and $h(x)$ is divisible by $\phi(x)$, i.e. iff $h(x) = p.\phi(x)\, h_1(x)$.

Proof: The condition is necessary. For let $f(x)$ is reducible, mod p^2. Then

(1) ... ... $f(x) = \psi_1(x).\psi_2(x) + p^2 g(x)$, $\psi_1(x)$ and $\psi_2(x)$ being not constants.

(2) ... ... $\therefore \phi(x)^n + ph(x) = \psi_1(x).\psi_2(x) + p^2 g(x)$.

Now $\phi(x)$ is irreducible, mod p,

$\therefore \psi_1(x) \equiv \phi(x)^{n_1}$, mod p,

i.e. $\psi_1(x) = \phi(x)^{n_1} + pg_1(x)$,

and $\psi_2(x) \equiv \phi(x)^{n_2}$, mod p,

i. e. $\psi_2(x) = \phi(x)^{n_2} + p.g_2(x)$

Hence from (1), $f(x) \equiv \phi(x)^n + p(\phi(x)^{n_1} g_2(x) + \phi(x)^{n_2} g_1(x))$, mod p^2, and from (2), $h(x) \equiv \phi(x)^{n_1}.g_2(x) + \phi(x)^{n_2} g_1(x)$, mod p^2.

Now, $n_1 > 0$, $n_2 > 0$, for if $n_1 = 0$ then $n_2 = n$ and hence $h(x) \equiv \phi(x)^n g_1(x) + g_2(x)$, such that degree $h(x) \geq nr$, contradicts our assumption.

$\therefore h(x) \equiv \phi(x)(\phi(x)^{n_1-1} g_2(x) + \phi(x)^{n_2-1} g_1(x))$, mod p

$\equiv 0(x)$, (mod $\phi(x)$, p)

The condition is also sufficient.

For, $ph(x) = p^2 \phi(x)\, h_1(x)$,

implies $f(x) = \phi(x)^n + p^2 \phi(x)\, h_1(x)$

$\equiv \phi(x)^n \pmod{p^2}$

As $n > 1$, $f(x)$ is factorised, mod p^2.

Eisenstien's theorem is a corollary of Schoeneman's theorem. For, putting $\phi(x) = ax$, where $a \not\equiv 0 \pmod{p}$ and $f(x) = a^n x^n + ph(x)$, where $h(x) = b_1 x^{n-1} + b_2 x^{n-2} + \ldots\ldots + b_n$ (say), one gets $f(x)$ reducible mod p^2 iff $h(x) \equiv 0\ (x), (\text{mod } p, ax)$. Putting $b_n \not\equiv 0 \pmod{p}$, one get $f(x)$ irreducible mod p^2. Hence by a previous theorem $f(x)$ is also irreducible over R. But those are also the conditions of Eisenstien's theorem. Hence the statement.

We have given some inportant theorems concerning reducibility of some particular polynomials over some specific domains or fields. But none of them is applicable to an arbitrary polynomial.

We now give here a method, due to Kronecker, by which one can determine the irreducible factors of an arbitrary polynomial over a domain of unique factorisation R.

As any polynomial of $R[x]$ factorisable over the quotient field of R is also factorisable over R; so irreducibility of $f(x)$ over R implies also its irreducibility over the quotient field of R. We shall suppose R has only a finite number of units.

Firstly, in $R[x]$, $f(x) = g(x)\, h(x)$ implies $f(a) = g(a)\, h(a)$ for every $a \in R$. For if $f(x) = \sum C_i x^i$, $g(x) = \sum U_j x^j$, $h(x) = \sum V_k x^k$, then $C_i = \sum_{j+k=i} U_j V_k$.

$\therefore$ $g(a)\ h\ (a) = (\sum_j U_j a^j)(\sum_k V_k a^k) = \sum_i (\sum_{j+k=i} U_j V_k)\ a^{j+k} = \sum_i C_i a^i = f(a)$,

by the commulative and distributive property of R.

Now let the degree of $f(x) = 2n$ or $2n+1$. Then the degree of at least one factor say $g(x)$ is $\leq n$. Let $g(x) = U_o + U_1 x + \ldots + U_m x^n$ where $U_o, U_1, \ldots, U_n \in R$, which we wish to determine.

Take $n+1$ distinct elements $a_o, a_1, \ldots, a_n \in R$.

Then $f(a_i) = g(a_i)\ h(a_i)$, $i=0, 1, \ldots, n$.

If $f(a_j) = 0$, then $x - a_j$ is a factor of $f(x)$. Taking $x - a_j = g(x)$ we can try to find factors of $h(x)$ applying the method as we shall soon find for $f(x)$. So let $f(a_i) \neq 0$, $i = 0, 1, \ldots, n$.

Now $g(a_i)$ is a factor of $f(a_i)$. As the factorisation is unique in R, $f(a_i)$ has only a finite number of factors i.e. $f(a_i) = g_{i1}\ g_{i2} \ldots g_{ik}$, say, and $g(a_i)$ is one of these factors. So there exists only a finite number of possibilities.

Taking one possible value, $g(a_i) = g_{ij} = g_i$ (say) $i=0,1,\ldots n$; one gets

$$U_o + U_1 a_o + U_2 a_o^2 + \ldots\ldots + U_n a_o^n = g_o$$
$$U_o + U_1 a_1 + U_2 a_1^2 + \ldots\ldots + U_n a_1^n = g_1$$
$$U_o + U_1 a_n + U_2 a_n^2 + \ldots\ldots + U_n a_n^n = g_n$$

This system of equations for $U_o, U_1, \ldots, U_n$ is uniquely solvable, for, the rank of coefficient metrix is $n+1$.

Indeed the determinant

$$\Delta = \begin{vmatrix} 1 & a_o & a_o^2 & \ldots & a_o^n \\ 1 & a_1 & a_1^2 & \ldots & a_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_n & a_n^2 & \ldots & a_n^n \end{vmatrix} = \prod (a_i - a_k)$$
$$i > k,$$
$$1 \leq i \leq n$$
$$0 \leq k \leq n-1$$

does not vanish as $a_i \neq a_k$.

[The value of this determinant can be found by multiplying each column by a_o and subtracting it from the next and then calculating it by the recurrence formula so obtained.]

Thus $U_i = \frac{\Delta_i}{\Delta}$ where Δ_i is the determinant obtained from Δ by replacing i + 1 th column of Δ by $\begin{pmatrix} U_o \\ U_1 \\ \vdots \\ U_n \end{pmatrix}$, i=0,1,.....n.

Thus g(x) is uniquely determined.

By actual division find whether g(x) is a factor of f(x). If f(x) so found is not a factor try the next possibility $g(a_i) = = g_{ik}$. As there exists only a finite number of g_{ik}'s and finite number of units, the number of all such possibilities is finite. So we get a factor in a finite number of steps if f(x) is reducible. Otherwise f(x) is irreducible. One can now repeat this method to a factor of f(x) thus obtained and find all the irreducible factors of f(x).

The labour may be minimused by neglecting those sets of choice $g_o, g_1, \ldots, g_n$ for which either $U_i = \frac{\Delta_i}{\Delta}$ is not an element of R, at least for one i (i.e. if Δ_i is not divisible by Δ for some i) i=0,....,n; or C_o is not divisible by U_o or C_{2n} (or C_{2n+1}) is not divisible by U_n thus determined.

In an arbitrary integral domain the difficulty of the above theorem however lies in the fact that we have not been able to give a procedure to find all the factors of the elements a_i of R. If R is the domain of common integers this however is not difficult. As the prime factors of an integer a are all less than a, one can, in a finite number of trial and error method, find all the factors of a.

For this domain however, one can find possible factors of $\overline{f}(x)$ in $R_p[x]$ by transforming f(x) to residue class mod p, p prime integer and thus one can obtain the possible degrees of the factors of f(x) and the possible coefficients of these factors. Thus if $U_i \not\equiv d \mod p$, where d is the coefficient of x^i of any factor of degree m of $\overline{f}(x)$ then the combination $U_o, U_1, \ldots\ldots, U_n$ may be neglected.

CHAPTER IV

Irreducibility of polynomials over a finite integral domain or field.

As every finite integral domain is a field there is only one case to consider: the case of irreducibility of polynomials over a finite field.

It may be convenient to discuss briefly the nature of a finite field.

A field Γ which contains only a finite number of elements is called a finite (Galois) field.

As the prime field (i.e. the smallest sub field) of Γ is a finite field, the characteristic of Γ must be a prime integer p. In fact the prime field F_p of characteristic p are examples of Galois fields. Γ is a finite extension of F_p. Hence every element of Γ can be expressed as

$$\beta = b_1 \alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n, \quad b_i \in F_p, \alpha_i \in \Gamma.$$

As b_i can take only p values, β can have p^n values. Then Γ contains only p^n elements where $n = [\Gamma : F_p]$. As Γ is a field the non-zero elements of Γ form a multiplicative group A with p^n-1 elements. Hence an element β must have an (multiplicative) order γ which is a factor of p^n-1. Thus β is a root of $x^{p^n-1}-1 = 0$, $x^{p^n-1}-1$ being a polynomial of $F_p[x]$.

On the other hand $x^{p^n-1} - 1 = 0$ has only p^n-1 roots. Therefore the group A consists of the roots of $x^{p^n-1}-1 = 0$ only.

Thus the elements of Γ are roots of $x^{p^n} - x = 0$

Conversely it is possible to construct a Galois field with p^n elements, for every positive integer n and every prime p.

For, take F_p and considering $x^{p^n}-x$ as a polynomial over F_p construct its splitting field Γ. In Γ the roots of $x^{p^n}-x=0$ form a subfield. For

$$\alpha^{p^n}=\alpha,\ \beta^{p^n}=\beta \Rightarrow (\alpha\pm\beta)^{p^n}=\alpha^{p^n}\pm\beta^{p^n}=\alpha\pm\beta$$
$$(\alpha/\beta)^{p^n}=\alpha^{p^n}/\beta^{p^n}=\alpha/\beta$$
$$(\alpha\beta)^{p^n}=\alpha^{p^n}\cdot\beta^{p^n}=\alpha\cdot\beta$$

As the splitting field Γ is the smallest field containing these roots, Γ Contains only these roots. As Γ is uniquely determined (except for ismorphism) by p and n, it is usual to denote it by F_{p^n}

Theorem: F_{p^n} subfield of $F_{p^m} \iff n \mid m$.

Proof: Let $F_{p^n} \subset F_{p^m}$ then obviously $n \leq m$, $\therefore$ the elements of F_{p^n} are roots of $x^{p^n}-x = 0$.

Now if $\beta \in F_{p^n}$ then $\beta^{p^n}=\beta$, also $\beta \in F_{p^m}$ $\therefore \beta^{p^m}=\beta$.

So if $m = qn + r$ $(0 \leq r < n)$, then

$$\beta = \beta^{p^m} = \beta^{p^{(qn+r)}} = \beta^{p^{qn}\cdot p^r} = (\beta^{p^{qn}})^{p^r} = \beta^{p^r}$$

$\therefore$ For any $\beta \in F_{p^n}$ $\beta = \beta^{p^r}$

Take β a primitive root of $x^{p^n-1}-1 = 0$, then p^n is the smallest prime power such that $\beta^{p^r}=\beta$ $\therefore r = 0$.

Conversely if $m = qn$ then for any $\beta \in F_{p^n}$, $\beta^{p^n}=\beta$.

$$\therefore \beta^{p^{nq}}=\beta \Rightarrow \beta^{p^m}=\beta \Rightarrow \beta \in F_{p^m}.$$

$\therefore F_{p^n} \subset F_{p^m}$

Theorem: Every finite extension of a Galois field has a primitive element and is a normal extension.

For, a finite extension of F_{p^m} is a F_{p^n} which contains the primitive roots of $x^{p^n-1}-1=0$ considered as a polynomial over F_{p^m}. Hence

$$F_{p^n} = F_{p^m}(\alpha)$$

α being a primitive root.

As $x^{p^n-1}-1$ is split up in F_{p^n}, F_{p^n} is a normal extension.

Consider now the polynomial $f(x) = x^m-1$ over F_p. Since $f'(x) = mx^{m-1}$, if m is not divisible by the characteristic p of F_p then $f'(x) \neq 0$ i.e. $f'(x)$ has no root other than zero. Hence $f(x)$ is spearable i.e. $f(x)$ has no multiple root in any field extension. If m is divisible by p, put $f(x) = x^m-1 = x^{p^t m'}-1$, where h.c.f. $(m', p) = 1$, then $f(x) = (x^{m'}-1)^{p^t}$. So $f(x)$ has m' distincts roots, each being of multiplicity p^t and each root being a root of $x^{m'}-1 = 0$. So in this case also the roots of x^m-1 are obtainable from those of a similar equation. Hence in our future discussions we shall suppose that the degree m of $f(x)$ is not divisible by the characteristic p.

Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ are all the primitive roots of $x^m-1 = 0$ over F_p. We have already defined that the polynomial $X_m=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r)$ is called the cyclotomic polynomial of order m. It's degree is $r = \phi(m)$.

Evidently $X_m \mid x^m-1$.

Now we have $d \mid m \Rightarrow x^d-1 \mid x^m-1 \Rightarrow X_d \mid x^m-1$.

So $x^m-1 = X_1 . X_{d_1} X_{d_2} \ldots\ldots X_m \psi(x)$, where d_i are all the factors of m.

$\therefore$ deg. $(x^m-1) = m = \phi(1) + \phi(d_1) + \ldots\ldots + \phi(m) + \deg \psi(x)$

But $m = \sum_{d \mid m} \phi(d)$

$\therefore \deg \psi(x) = 0$

$\therefore x^m-1 = \prod_{d \mid m} X_d$

$\therefore x^{p^n}-x = x(x^{p^n-1}-1) = x \prod_{d \mid p^n-1} X_d$

So if $m \mid p^n-1$, X_m splits linearly in $F_{p^n}[x]$.

We shall now determine the irreducible polynomials of $F_{p^n}[x]$. Let g(x) be an irreducible polynomial of $F_{p^n}[x]$ of degree m. If α be a root of g(x) then $F_{p^n}(\alpha)$ is a finite extension of F_{p^n} and $F_{p^n}(\alpha) = F_{p^{nm}}$.

But $F_{p^{nm}}$ is a normal field. So it contains all the roots of $x^{p^{nm}-1}-1 = 0$. As g(x) is an arbitrary irreducible polynomial it follows that all irreducible polynomials of degree m over F_{p^n} are factors of $x^{p^{nm}-1}-1 = 0$.

But $x^{p^{nm}-1}-1 = \prod_{d \mid p^{nm}-1} X_d$

So as g(x) is irreducible it must be a factor of certain cyclotomic polynomials X_q, $q \mid p^{nm}-1$. Moreover as for every factor k of m there exists a subfield $F_{p^{nk}}$ of $F_{p^{nm}}$ (i.e. $F_{p^n} \subset F_{p^{nk}} \subset F_{p^{nm}}$), q should not be a factor of $p^{nk}-1$, $k < m$ and $k \mid m$.

For, in that case X_q is split up linearly in $F_{p^{nk}}$.

q is to be called the exponent of g (x).

As X_q is normal (since each root of X_q is a primitive root of $x^q-1=0$), all factors of X_q must be of the same degree m. Hence if $N^q_{mp^n}$ be the number of irreducible polynomials of degree m and exponent q over F_{p^n} then

$m.N^q_{mp^n} = \phi(q)$, where $\phi(q)$ is the Euler's function.

Thus if $q \mid p^{nm}-1$ but $\nmid p^{nk}-1$, $0 < k < m$, $k \mid m$ then X_q is reducible or irreducible over F_{p^n} according as $\phi(q) > m$ or $\phi(q) = m$. If $\phi(q) = m.t$ then X_q has t irreducible factors over F_{p^n} each of degree m. $F_{p^{nm}}$ may be obtained by extending F_{p^n} by a root of anyone of these factors.

Thus we get the theorem:

Any irreducible polynomial of degree m over F_{p^n} is a factor of X_q such that $q \mid p^{nm}-1$, but $\nmid p^{nk}-1$, $0 < k < m$, $k \mid m$.

We can use the relation $x^{p^{nm}} - x = x\prod_{d \mid p^{nm}-1} X_d$ and the above theorem to find out all the irreducible polynomials of degree m.

Example To find all the irreducible polynomials of degree 6 over R_2 (residue classes modulo 2). All the irreducible polynomials of degree 6 over R_2 are factors of

$$x^{2^6}-x = x\,(x^{63}-1)$$

$$= xX_1(x)\,X_3(x)\,X_7(x)\,X_9(x)\,X_{21}(x)\,X_{63}(x)$$

$$= x(x-1)\,(x^2+x+1)\,(x^6+x^5+\ldots..+1)\,(x^6+x^3+1)(x^{12}-\ldots+1)$$

$$(x^{36}-\ldots\ldots+1)$$

Of all the factors of degree ≥ 6 only $X_7(x)$ is factorised into factors of degree < 6. This is because 7 is a factor of 2^3-1 where $3 < 6$ and $3 \nmid 6$. Where as it can be verified that over R_2 $X_9(x)$ is irreducible, $X_{21}(x)$ is reduced to two factors each of degree 6 and $X_{63}(x)$ is reduced to six factors each of degree 6.

Number of irreducible factors of degree m over F_{p^n}

We have for every factor k of m, $x^{p^{nk}}-x$ is a factor of $x^{p^{nm}}-x$. Moreover all irreducible polynomials of degree k over F_{p^n} are factors of $x^{p^{nk}}-x$, considered as a polynomial over F_{p^n}. So for every factor k of m all irreducible polynomials of degree k over F_{p^n} are factors of $x^{p^{nm}}-x$. Again if $k \nmid m$ there exists no irreducible polynomial of degree k over F_{p^n} which is a factor of $x^{p^{nm}}-x$. For in that case $F_{p^{nk}}$ would be subfield of $F_{p^{nm}}$ and $x^{p^{nk}}-x$ would be a factor of $x^{p^{nm}}-x$ which implies that $k \mid m$ contradicting that $k \nmid m$.

So if $h_{p^n}(d)$ be the number of irreducible factors of degree d over F_{p^n} then $p^{nm} = \sum_{d \mid m} d.h_{p^n}(d)$

But if g(m) and f(d) are two arithmetical functions then

$$g(m) = \sum_{d \mid m} f(d) \iff f(m) = \sum_{d \mid m} \mu(d)\, g\left(\frac{m}{d}\right),$$ where $\mu(d)$ is the Mobius μ function i.e.

$$\mu(d) = \begin{cases} (-1)^r, & \text{if } \alpha_1, \alpha_2, \cdots, \alpha_r \text{ all } = 1 \\ 0, & \text{if at least one of } \alpha_i > 1 \\ 1, & \text{if } d = 1 \end{cases}$$

where $d = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r}$, p_i primes.

So by this formula $m \cdot h_{p^n}(m) = \sum_{d|m} \mu(d) \cdot p^{n \cdot \frac{m}{d}}$ where from $h_{p^n}(m)$ can be calculated.

Thus of the total number of $(p^n-1)(\underbrace{p^n.p^n....p^n}_{m \text{ factors}}) = p^{(m+1)n} - p^{mn}$ polynomials of degree m, over F_{p^n} only $h_{p^n}(m)$ polynomials are irreducible.

Reducibility of X_q over F_{p^n}

The degree of X_q is $\phi(q)$, hence, by the previous theorem, all irreducible polynomials of degree $\phi(q)$ over F_{p^n} are factors of

$$x^{p^{n \cdot \phi(q)}-1} - 1 = \prod_{d | p^{n \cdot \phi(q)}-1} X_d .$$

One can simplify the right hand side and verify whether X_q is reducible or not over F_{p^n}.

The above process is however labourious. On the other hand we observe that if $p \nmid q$, there always exists a least positive integer k such that $(p^n)^k \equiv 1 \pmod{q}$. If q is prime the relation is obvious, since the classes of residues mod q form a field. If q is not prime then also the elements p_j such that h.c.f. $(p_j, q) = 1$, form a multiplicative group in the ring of classes of residues mod q. So from the relation

$$k N_{k p^n}^{q} = \phi(q),$$

the number of irreducible factors of X_q over F_{p^n} is $\frac{\phi(q)}{k}$, where k is the least positive integer such that $(p^n)^k \equiv 1 \pmod{q}$. Each of the factors of X_q is of degree k.

If $k = 1$ then X_q splits up linearly over F_{p^n}.

Summary: There exists only a finite number of irreducible polynomials of degree m over F_{p^n}. They are factors of $x^{p^{nm}}-x$ and also factors of X_q such that $q \mid p^{nm}-1$, but $q \nmid p^{nk}-1$, $0 < k < m$, $k \mid m$. All other polynomials of degree m over F_{p^n} is reducible.

Bibliography

1. B.L. van der Waerden: Modern Algebra, New York, 1953.
2. G. Birkhoff and S. MacLane: A survey of Modern Algebra, The Macmillan Co., New York, 1953.
3. A. A. Albert: Modern Higher Algebra, The University of Chicago Press, Chicago, 1937.
4. N. Jacobson: Lectures in Abstract Algebra, V-1, D. Van Nostrand Co., Inc., New York, 1951.
5. L. E. Dickson: Linear Groups with an exposition of the Galois Field Theory, Dover Publications, Inc., New York.
6. N.H. McCoy: Rings and Ideals, The Mathematical Association of America.
7. N. Tschebotarö̈w: Grundzüge Der Galois'schen Theorie, Groningen, 1950.
8. G. Dumas: Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels - J. Math. Pures Appl. Vol2 - 1906, pp 191 -258.
9. J. H. Wahab: New case of irreducibility for Legendre polynomial, Duke Math. J. Vol. 19, 1952, pp 167-169.
10. J. H. Wahab: Irreducibility of Polynomials, Amer. Math. Monthly, Vol.68, 1961, pp 366-367.