GROUP ANALYSIS AND THEIR APPLICATIONS ON

DIFFERENTIAL EQUATIONS

**A PROJECT REPORT**

***Submitted by***

**POORANI.A**

**CB.SC.I5MAT17020**

***in partial fulfillment of the requirements for the award of the***

***degree of***

**BACHELOR OF SCIENCE**

**IN**

**MATHEMATICS**



**AMRITA SCHOOL OF ENGINEERING**

**AMRITA VISHWA VIDYAPEETHAM**

**COIMBATORE 641112**

**APRIL 2020**

**AMRITA VISHWA VIDYAPEETHAM**

**AMRITA SCHOOL OF ENGINEERING, COIMBATORE, 641112**



**BONAFIDE CERTIFICATE**

This is to certify that the project report entitled **“Group Analysis and their Applications on Differential Equations”** submitted by **CB.SC.I5MAT17020 POORANI.A** in partial fulfillment of the requirements for the award of the **Degree of Bachelo**r **of Science** in **MATHEMATICS** is a bonafide record of the work carried out under my guidance and supervision at Amrita School of Engineering, Coimbatore.

Class Advisor Project Coordinator

Designation Designation

Chairperson

Department of Mathematics

Dr. J. Ravichandran

The project was evaluated by us on:

Internal Examiner External Examiner

**DEDICATION**

*To my beloved Parents, Guide and Friends****.***

**ACKNOWLEDGEMENTS**

*I would like to warmly acknowledge and express my deep sense of gratitude and indebtedness to my guide*

***Dr.PRAKASH. P****, Department of Mathematics, Amrita Vishwa Vidyapeetham, Coimbatore, for his keen guidance, constant encouragement and prudent suggestions during the course of my study and preparation of the final manuscript of this Project.*

*I would like to thank the faculty members of Department of Mathematics for allowing me to work for this Project.*

*My heartfelt thanks to all my friends for their invaluable co-operation and constant inspiration during my Project work.*

*I owe a special debt gratitude to my revered parents, my sister for their blessings and inspirations.*

*Coimbatore, POORANI.A*

*March 2020*

Contents

Chapter 0 INTRODUCTION 1

Chapter 1 GROUP THEORY 2

Chapter 2 RING THEORY AND INTEGRAL

DOMAIN 7

Chapter 3 FIELD THEORY AND EXTENSION 12

Chapter 4 REDUCIBLE AND IRREDUCIBLE

POLYNOMIAL 15

Chapter 5 SYMMETRY ANALYSIS OF

DIFFERENTIAL EQUATION 20

Bibliography 27

**0**

**INTRODUCTION**

**When we see it for the first time,it looks so abstract that it seems impossible something like this could have any real-world applications.**

**-Edward Frenkel,Love and Math**

In the latter part of the nineteenth century, Sophus Lie introduced the notion of

continuous groups, now known as Lie groups, in order to unify and extend various

specialized methods for solving ordinary differential equations (ODEs). Lie was inspired

by the lectures of Sylow given at Christiania (present-day Oslo) on Galois theory and

Abel’s related works. [In 1881 Sylow and Lie collaborated in a careful editing of Abel’s

complete works.] Lie showed that the order of an ODE could be reduced by one,

constructively, if it is invariant under a one-parameter Lie group of point transformations.

Lie’s work systematically related a miscellany of topics in ODEs including:

integrating factor, separable equation, homogeneous equation, reduction of order, the

methods of undetermined coefficients and variation of parameters for linear equations,

solution of the Euler equation, and the use of the Laplace transform. Lie (1881) also indicated

that for linear partial differential equations (PDEs), invariance under a Lie group

leads directly to superpositions of solutions in terms of transforms.

A symmetry of a system of differential equations is a transformation that maps any solution to another solution of the system. In Lie’s framework such transformations

are groups that depend on continuous parameters and consist of either point transformations (point symmetries), acting on the system’s space of independent and dependent variables, or, more generally, contact transformations (contact symmetries), acting on the space of independent and dependent variables as well as on all first derivatives of the dependent variables. Elementary examples of Lie groups include translations, rotations, and scalings. An autonomous system of first-order ODEs, i.e., a stationary flow, essentially defines a one-parameter Lie group of point transformations. Lie showed that for a given differential equation (linear or nonlinear), the admitted continuous group of point transformations, acting on the space of its independent and dependent variables, can be determined by an explicit computational algorithm (Lie’s algorithm).

1

**CHAPTER 1**

**GROUP THEORY**

**Introduction**

The term group was used by Galois around 1830 to describe sets of one-to-one functions on finite sets that could be grouped together to form a set closed under composition. As is the case with most fundamental concepts in mathematics, the modern definition of a group that

follows is the result of a long evolutionary process. Although this definition was given by both Heinrich Weber and Walther von Dyck in 1882, it did not gain universal acceptance until the 20th centuary.

**Binary Operation**

**Definition 1.1:**

Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

**Definition 1.2:**

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say that G is a group under this operation if the following three properties are hold :

1.**Associativity**:The operation is associative; that is, (ab)ca(bc), for a, b, c in G.

2.**Identity**:There is an element e (called the identity) in G such that ae = ea = a, for all a in G.

3.**Inverses**: For each element a in G, there is an element b in G (called an inverse of a) such that ab = ba = e.

**Abelian Group**

**Definition 1.3:**

If a group G has the property that ab = ba for every pair of elements a and b in G, we say the group is Abelian.

**Non-Abelian Group**

**Definition 1.4:**

A group is non-Abelian if there is some pair of elements a and b for which ab ba.

2

**Example1.1**: The set of integers Z={0, the set of rational numbers Q (for quotient), and the set of real numbers R are all groups under ordinary addition. In each case, the identity is 0 and the inverse of a is –a.

Note that a the set {0, 1, 2, 3} is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not.

**Properties of Group**

* **Uniqueness of the Identity**:

In a group G, there is only one identity element.

* **Cancellation**:

In a group G, the right and left cancellation laws hold; that is, ba =ca implies b = c, and ab = ac implies b = c.

* **Uniqueness of Inverse**:

For each element a in a group G, there is a unique element b in G such that ab = ba = e.

* **Socks and shoes property:**

(ab) -1=b-1a-1.

**Order of a Group**

**Definition 1.5:**

The number of elements of a group (finite or infinite) is called its order. We will use |G| to denote the order of G.

**Example 1.2**: The group Z of integers under addition has infinite order, whereas the group U(10) = {1, 3, 7, 9} under multiplication modulo 10 has order 4.

3

**Order of an Element**

**Definition 1.6**:

The order of an element g in a group G is the smallest positive integer n such that gn = e (In additive notation, this would be ng =0.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by |g|.

**Example 1.3**:U(15) ={1, 2, 4, 7, 8, 11, 13, 14} under multiplication modulo 15

order of the element 7 is 4. Since 71=7, 72=4, 73=13, 74=1.

**Subgroup**

**Definition 1.7**:If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G. We use the notation H G to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write H G. Such a subgroup is called a proper subgroup.

**Example 1.4**:The set {1,-1} is a subgroup under multiplication of the group {1,-1,i,-i} under multiplication

**Subgroup Tests**

* **One-Step Subgroup Test**

Let G be a group and H be a nonempty subset of G. If ab-1 is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if a - b is in H whenever a and b are in H, then H is a subgroup of G).

* **Two-Step Subgroup Test**

Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a-1 is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

* + **Finite Subgroup Test**

Let H be a nonempty finite subset of a group G. If H is closed under

the operation of G, then H is a subgroup of G.

4

**Cyclic Group**

**Definition 1.8**:

A group G is called cyclic if there is an element a in G such that G = {an | n Z}. Such an element a is called a generator of G, where G is denoted by G = <a>.

**Example 1.5**:

* The set of integers Z under ordinary addition is cyclic. Both 1 and -1 are generators.
* The set Zn = {0,1,2,…,n-1} for n 1 is a cyclic group under addition modulo n. Again, 1 and -1=(n – 1) are generators .Unlike Z it has other generators too.For instance Z8={0,1,2,3,…,7} where 1,3,5,7 are generators of Z8.

**Non cyclic group**

**Example 1.6**: U8={1,3,5,7} under multiplication modulo 8 is not a cyclic.

**We present some theorems based on a cyclic group**

**Theorem 1**:

Order of a cyclic group is equal to the order of its generators.

**Theorem 2**:

A subgroup of cyclic group is cyclic.

**Theorem 3**:

Every cyclic group is abelian.

**Converse of the above theorem is not true.**

**Statement:**

An Abelian group need not be a cyclic group.

**Example 1.7**:<Q,+> ,Suppose m/n Q and generator of Q. Then an element of Q should be multiple of m/n , 1/(3\*n) k\*(m/n) for some k, 1/3=k\*m which is not possible as k and m are integers.

**5**

**Coset of H in G**

**Definition 1.9:**

Let G be a group and let H be a nonempty subset of G. For any a G,the set {ah | h H} is denoted by aH.

Analogously, Ha = {ha | h H}and aHa-1 ={aha-1 | h H}. When H is a subgroup of G, the set aH is called the left coset of H in G containing a, whereas Ha is called the right coset of H in G containing a.

**Example 1.8:**

Let G = S3 and H = {(1), (13)}. Then the left cosets of H in G are

(1) H = H.

(12) H = {(12), (12)(13)} ={(12), (132)} = (132)H.

(13) H = {(13), (1)} = H.

(23) H = {(23), (23)(13)} = {(23), (123)} = (123)H.

**Lagrange’s theorem:**

**Statement:**

If G is a finite group and H is a subgroup of G, then |H| divides |G|.

We would like to point out that the converse of the Lagrange’s theorem is not true.

For example,

The alternating group G=A4 which has 12 elements has no subgroup of order 6.

**Remark:**

The converse of Lagrange theorem is true, when the group is Abelian.

6

**CHAPTER 2**

**RING THEORY AND INTEGRAL DOMAIN**

**Introduction**

Many sets associated with two binary operations addition and multiplication. When we considering these sets as groups then we consider either of binary operation addition or multiplication. But one may wish to take both the binary operations. So the ring concept comes into picture. This notion was originated in mid nineteenth century by Richard Dedekind, although its first formal abstract definition was not given until Abraham Fraenkel presented it in 1914. In this chapter, we give few definitions with examples and some results.

**Definition 2.1:**

A ring R is a set with two binary operations, addition (denoted by

a + b) and multiplication (denoted by ab), such that for all a, b, c in R:

1. a + b = b + a.

2. (a + b) + c = a + (b + c).

3. There is an additive identity 0. That is, there is an element 0 in R such that a + 0 = a

for all a in R.

4. There is an element -a in R such that a + (-a) = 0.

5. a(bc) = (ab)c.

6. a(b + c) = ab + ac and (b + c) a = ba + ca.

**Example 2.1:** The set Z of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of Z are 1 and -1.

**Commutative ring**

**Definition 2.2:**

When R satisfies commutative property w.r.t multiplication then R is called commutative ring.

**Example 2.2:** The set *Zn* = {0, 1, . . . , *n* - 1} under addition and multiplication modulo *n* is a commutative ring.

7

**Unity**

**Definition 2.3:**

When a ring other than {0} has an identity under multiplication, we say that the ring

has a unity.

**Example 2.3:** The set *Z*[*x*] of all polynomials in the variable *x* with integer coefficients under ordinary addition and multiplication is a commutative ring with unity *f*(*x*) = 1.

**Unit**

**Definition 2.4:**

If a 0 ∈ R and a-1 exist then a is a unit of R.

**Example 2.4:**

The set *Z* of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of *Z* are1 and -1.

**Some Properties of Rings**

1.Let a, b, and c belong to a ring R. Then

* a0 = 0a = 0.
* a(-b) = (-a)b = -(ab).
* (-a)(-b) = ab.
* a(b - c) = ab - ac and (b - c)a = ba - ca.

2.Furthermore, if R has a unity element 1, then

* (-1)a = -a.
* (-1)(-1) = 1.

**Uniqueness of the Unity and Inverses:**

If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

**Note:**

If a, b, and c belong to a ring, a 0 and ab = ac, we cannot conclude that b = c. Similarly, if a2 = a, we cannot conclude that a = 0 or 1.

**8**

**Subring**

**Definition 2.5:**

A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

**Subring test**

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication—that is, if a - b and ab are in S

whenever a and b are in S.

**Example 2.5:**

For each positive integer n, the set

nZ ={0, n, 2n, 3n, . . .} is a subring of the integers Z.

**Zero-Divisors**

**Definition 2.6:**

A zero-divisor is a nonzero element ‘a’ of a commutative ring R such

that there is a nonzero element b R with ab = 0.

**Integral Domain**

**Definition 2.7:**

An integral domain is a commutative ring with unity and no zero- divisors.Thus, in an integral domain, a product is 0 only when one of the factors is 0; that is, ab = 0 only when

a = 0 or b = 0.

Let a, b, and c belong to an integral domain. If a 0 and ab = ac,

then b = c.

**Example 2.6:**

* The ring Zp of integers modulo a prime p is an integral domain.
* The ring Zn of integers modulo n is not an integral domain
  + - when n is not prime.

9

**Characteristic of a Ring**

**Definition 2.8:**

The characteristic of a ring R is the least positive integer n such that nx = 0 for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

**Example 2.8**:The ring of integers has characteristic 0, and Zn hascharacteristic n.

**Characteristic of a Ring with Unity**

**Theorem 2.1:**

Let R be a ring with unity 1. If 1 has infinite order under addition,then the characteristic of R is 0. If 1 has order n under addition,then the characteristic of R is n.

**Proof:**

If 1 has infinite order, then there is no positive integer n suchthat n . 1 = 0, so R has characteristic 0.

Now suppose that 1 has additiveorder n. Then n . 1 = 0, and n is the least positive integer with this property. So, for any x in R, we have

n . x = x + x + . . . +x(n summands)

= 1x+1x+. . . +1x(n summands)

= (1+1+ . . . +1)x(n summands)

= (n.1)x=0x=0

Thus, R has characteristic n.

**Characteristic of an Integral Domain**

**Theorem 2.2:**

The characteristic of an integral domain is 0 or prime.

**Proof:** By Theorem 2.1, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that n = st

10

where 1 s,t n. Then, we know that

0 = n . 1 = (st) . 1 = (s . 1)(t . 1).

So, s . 1 = 0 or t . 1 = 0. Since n is the least positive integer with the

property that n .1 = 0, we must have s = n or t = n.

Thus, n is prime.

**Note:**

In the ring, the zero of the polynomial causes unusual results, since it does not satisfy zero divisors.

**Example 2.9:**

x2-4x+3=(x-3)(x-1)=0, In Z12 has x=3, x=1, x=7, x=9.

11

**CHAPTER 3**

**FIELD THEORY AND EXTENSION**

**Introduction**

An archaic name for field is rational domain. Fields have been used implicity ever

since the discovery of addition, subtraction, multiplication and division. Cardan’s formula dating from 16th century used Q, R, C. Lagrange used the field of rational functions in

n-variable in his 1770 study of roots of polynomials. The first truely abstract notion of field is due to Dedekind. In 1877, he gave the following definition:

“I call a system A of numbers (not all zero) a field when the sum, difference, product and quotient of any two numbers except 0 in denominator in A also belongs to A. ”This is not completely general for the numbers. Taking into account ring definition, a field can be defined as “A commutative ring with unity in which every nonzero element has a multiplicative inverse.”OR, “ A field is a commutative ring in which we can divide by any nonzero element.” In fact in 1893, Dedekind’s student Weber gave the first fully abstract definition of field which we use today.

**Definition 3.1:**

A field is a commutative ring with unity in which every nonzeroelement is a unit.

**Theorem 3.1:**

A finite integral domain is a field.

**Proof:**

Let D be any finite integral domain. Let a ( 0) ∈ D. We have to show that a-1 exist or a is unit. If a = 1, a is its own inverse. If a 1, then a1,a2,a3, ..... ∈ D, but D is finite. So there must be two positive integer i and j such that i > j and ai = aj ⇒ ai-j=1

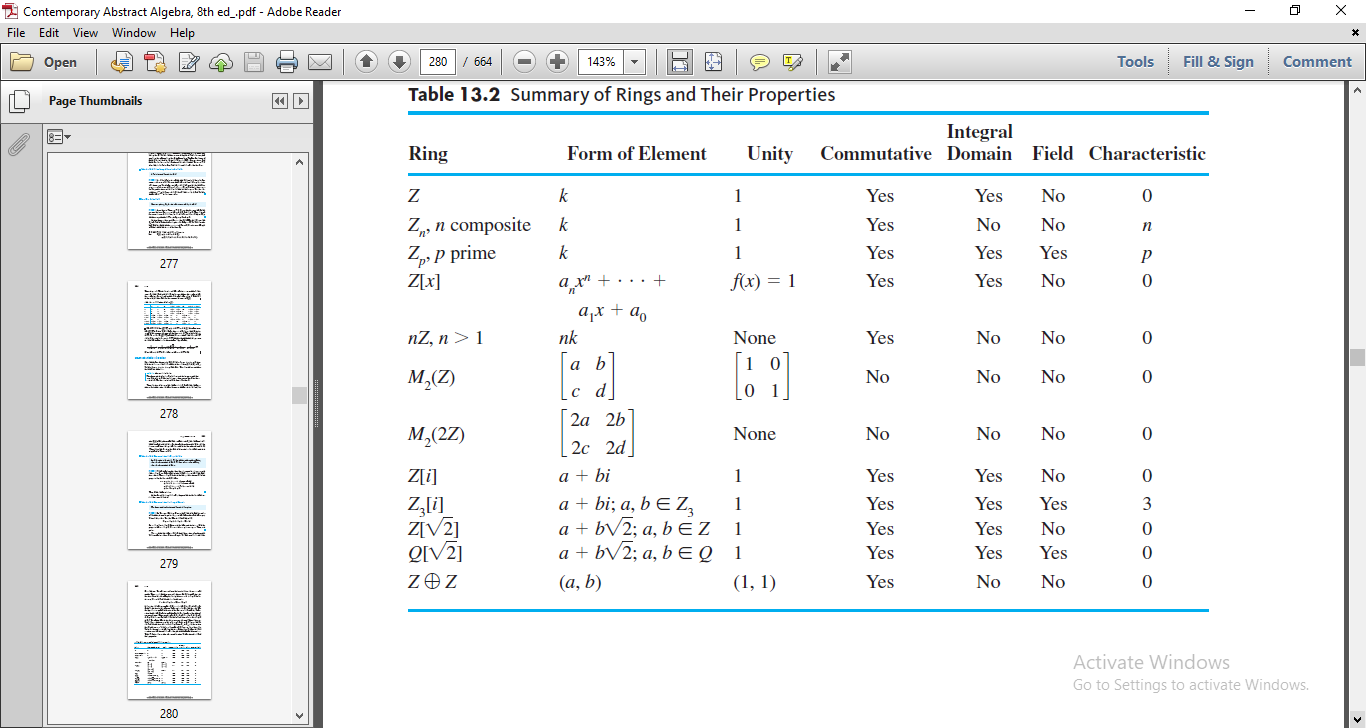
⇒ ai−j−1=a-1. So a-1 exists.

**Example 3.1:**

* Zp Is a Field ,for every prime p, Zp, the ring of integers modulo p is a field.
* Field with Nine Elements.Let Z3[ i ]={a + bi | a, b Z3}= {0, 1, 2, i, + 1 i, 2 + i, 2i, 1 + 2i, 2 + 2i}

**12**

**Summary of Rings and properties**



**Homomorphism**

**Definition 3.2:**

The word homomorphism comes from Greek words ‘homo’ means ‘like’ and ‘morphe’

means ‘form’.

**Similarity with photography**

A photograph of a person cannot tell us the person’s exact height, weight and age.

But it may be possible to decide from a photograph that the person is tall or short, heavy or thin, old or young, male or female. Like this a homomorphic image of a group gives us some information about the group not the exact property of the group.

**Ring homomorphism**

**Definition 3.3:**

A ring homomorphism is a map from one ring to another that preservers the binary operations addition and multiplication.

13

Let R and S be rings, ϕ : R → S satisfying

(i)ϕ(a + b) = ϕ(a) + ϕ(b) ∀ a, b ∈ R.

(ii)ϕ(ab) = ϕ(a)ϕ(b) ∀ a, b ∈ R. Then ϕ is called a ring homomorphism.

**Monomorphism**

If a ring homomorphism is one-one then it is called monomorphism.

**Etimorphism**

If a ring homomorphism is onto then it is called etimorphism.

**Isomorphism**

If a ring homomorphism is one-one and onto then it is called isomorphism.

**Example 3.2**:

Let ϕ : Z → Zn, defined by k → k mod n, nZ+ a,b∈ Z

ϕ(a + b) = (a + b) mod n

= ((a mod n) + (b mod n)) mod n

= a mod n + b mod n

= ϕ(a) + ϕ(b).

**Extension Field**

**Idea behind to develop extension fields**

Some polynomials don’t have zeros in the base field. The zeros of those polynomials

are exist in some other field which is lager than the base field. Those fields are called

extension fields.

**Definition 3.4**:

Let F be a field and E be a field containing F as a subfield. Then E is called an extension of F and can be regarded as vector space over F. F is called base field of the extension E.

**Examples 3.3:**

The extension field of Q is R and extension field of R is C.

14

**CHAPTER 4**

**REDUCIBLE AND IRREDUCIBLE POLYNOMIAL**

**Introduction**

In high school, students spend much time factoring polynomials and finding their zeros. In this chapter, we consider the same problems in a more abstract setting.

**Definition 4.1**:

Let R be a commutative ring. The set of formal symbols

R[x] = {anxn + an-1xn-1 + . . . + a1x + a0 | ai R, n is a non-negative integer} is called the ring of polynomials over R in the indeterminate x.

Two elements

anxn + an-1xn-1+ . . . + a1x + a0

and

bmxm + bm-1xm-1+ . . . + b1x + b0

of R[x] are considered equal if and only if ai =bi for all nonnegative integers i.

**Addition and Multiplication in R[x]**

**Definition 4.2:**

Let R be a commutative ring and let

f (x) = anxn+an-1xn-1+. . .+a1x+a0

and

g(x) =bnxn+bn-1xn-1+. . .+b1x+b0

belong to R[x]. Then

f (x) + g(x) = (as+bs)xs + (as-1 + bs-1)xs-1 + . . . + (a1+b1)x+ (a0+b0),

where s is the maximum of m and n, ai =0 for i n, and bi =0 for

i m. Also, f (x)g(x) = cm+nxm+n+cm+n-1xm+n-1+. . .+c1x+c0

where ck=akb0+ak-1b1+ak-2b2+… +a0bk

for k = 0, . . . , m + n.

**Example 4.2:**Let F(x)=2x3+x2+2x+2, g(x)=2x2+x+1

15

F(x)+g(x)=(2+0)x3+(1+2)x2+(2+2)x+(2+1)=2x3+0x2+x+0 =2x3+x

F(x).g(x)=(0.1+0.2+2.2+1.0+2.0+2.0)x5+(0.1+2.2+1.2+2.0+2.0)x4

+(2.1+1.2+2.2+2.0)x3+(1.1+2.2+2.2)x2+(2.1+2.2)x+2.1

=x5+0x4+2x3+0x2+0x+2

=x5+2x3+2

**Factorization of polynomials**

**Irreducible and Reducible Polynomial**

**Definition 4.3:**

Let D be an integral domain. A polynomial f(x) from D[x] that is neither the zero polynomial nor a unit in D[x] is said to be irreducible over D if, whenever f(x) is expressed as a product f(x) = g(x)h(x), with g(x) and h(x) from D[x], then g(x) or h(x) is a unit in D[x]. A nonzero, nonunit element of D[x] that is not irreducible over D is called reducible over D.

**Example 4.3:**

* The polynomial f(x) =2x2+4 is irreducible over Q but reducible over Z, since 2x2+4=2(x2+2) and neither 2 nor x2+2 is a unit in Z[x].
* The polynomial f(x)=2x2+4 is irreducible over R but reducible over C.

**Primitive Polynomial**

**Definition 4.4:**

The content of a nonzero polynomial anxn+an-1xn-1+. . .+a1x+a0 where the ai’s (i=0,1,2. . . n) are integers, is the greatest common divisor of theintegers an, an-1, . . . , a0. A primitive polynomial is an element of Z[x] with content 1.

**Gauss’s Lemma**

**Theorem 4.1:**

The product of two primitive polynomials is primitive.

**Proof:** Let f(x) and g(x) be two primitive polynomials.

16

We have to prove f(x)g(x) is primitive.If possible, let f(x)g(x) is not primitive. So let p be a primitive divisor of the content of f(x)g(x), and let the polynomials (x)(x) and )obtained from f(x), g(x) and f(x)g(x) respectively, by reducing the coefficients modulo p. Then (x) and (x) ∈ Zp[x] and(x)(x) =) = 0, the zero elements of Zp[x]. So, either (x) = 0 or (x) = 0, (Since these are in integral domain). This means that either p divides every coefficient of f(x) or p divides every coefficient of g(x). Therefore, either f(x) is not primitive or g(x) is not primitive, which is contradiction to the assumption.

So f(x)g(x) is primitive

**Reducibility test**

**Reducibility Test for Degrees 2 and 3**

**Theorem 4.2:**

Let F be a field. If f(x)F[x] and deg f(x) is 2 or 3, then f(x) is

reducible over F if and only if f(x) has a zero in F.

**Proof:**

Suppose f(x) is reducible. So deg f(x) = deg g(x) + deg h(x), degree of f(x)=2 or 3, so

at least g(x) or h(x) has degree 1. g(x) = ax + b, therefore ax + b = 0 =⇒ x = −a-1b

is a zero of g(x).–a-1b is a zero of f(x). Conversely, suppose that f(a) = 0, a ∈ F. So

x − a is a factor of f(x). Therefore f(x) is reducible over F.

**Example 4.4:**The polynomial f(x)=2x2+4 is irreducible over R but reducible over C

**Reducibility over Q Implies Reducibility over Z**

**Theorem 4.3:**

Let f(x) Z[x]. If f(x) is reducible over Q, then it is reducible over Z.

**Proof:**Given that f(x) is reducible over Q. So we can write f(x) = g(x)h(x), where g(x) and h(x) ∈ Q[x]. We may assume that f(x) is primitive because we can divide both f(x) and g(x)h(x) by the content of f(x). Let a be the least common multiple of the denominators of the coefficients of g(x) and b be the least common multiple of the denominators of the coefficient of h(x). Then abf(x) = ag(x).bh(x), where ag(x) and bh(x) ∈ Z[x]. Let c1 be the content of

17

ag(x) and c2 be the content of bh(x). Then ag(x) = c1g1(x) and bh(x) = c2 h1(x), where g1 (x) and h1(x) both are primitive and

abf(x) = c1 c2 g1(x)h1 (x). (4.1)

f(x) is primitive so content of abf(x) is ab and g1 (x)h1(x) is primitive since product of

two primitive polynomials is primitive.

So content of c1c2 g1 (x)h1(x) is c1c2 Thus from equation (4.1), ab = c1c2,

f(x) =g1(x)h1(x), where g1(x) and h1(x) ∈ Z[x] and deg g1 (x) = deg g(x) and

deg h1(x) = deg h(x). f(x) is reducible over Z.

**Irreducibility Tests**

**Mod p Irreducibility Test**

**Theorem 4.4:**

Let p be a prime and suppose that f(x) Z[x] with deg f(x) 1. Let (x) be the polynomial in Zp[x] obtained from f(x) by reducing all the coefficients of f(x) modulo p. If (x) is irreducible over Zp and deg f (x) = deg(x), then f(x) is irreducible over Q.

**Proof:**

Let f(x) ∈ Z[x]. If possible, let f(x) be reducible over Q, then we have f(x) = g(x)h(x)

with g(x), h(x) ∈ Z[x] and both g(x) and h(x) have degree less than that of f(x). Let

(x), (x) and (x) be the polynomials obtain from f(x), g(x) and h(x) by reducing all the

coefficient modulo p. Since deg f(x) = deg (x), we have deg (x) ≤ deg g(x) < deg (x). Again deg(x) ≤ deg h(x) < deg(x), but (x) =(x)(x).(x) is reducible over Zp,

which is contradiction. Hence, f(x) is irreducible over Q.

**Example 4.5:**

Let f(x) = 21x3-3x2+2x+9. Then over Z2, we have (x) =x3+x2+1 and since (0)=1 and (1)=1 we see that (x) is irreducible over Z2. Thus, f (x) is irreducible over Q.

Note that over Z3, (x) = 2x is irreducible, but we may not apply above theorem to conclude that f(x) is irreducible over Q.

**18**

**Converse need not to be true**

**Example 4.6:**

f(x)=21x3-3x2+2x+8,then over Z2, (x)=x3+x2=x2(x+1) .Therfore f(x) is reducible over Z2. But it is irreducible over Q.

**Eisenstein’s Criterion :**

**Theorem 4.5:**

Let f(x) = anxn+an-1xn-1+ . . .+a0 Z[x]. If there is a prime p such that p does not divide an ,

p | an-1, . . . , p | a0 and p2 does not divide a0, then f(x) is irreducible over Q.

**Proof:**

If possible let f(x) be reducible over Q. Then we know that ∃ elements g(x) and h(x) in

Z[x] such that f(x) = g(x)h(x) and deg g(x) ≥ 1, deg h(x) < n.

Say g(x) = brxr+br-1xr-1+. . .+b0 and h(x) = csxs+cs-1xs-1+. . .+c0. Then since p | a0 and p2 does not divide a0 and a0 = b0c0, so p divides one of b0 and c0 but not the both.

Let us consider the case p | b0 and p does not divide c0, since p does not divide

an ⇒ p does not divide brcs ⇒ p does not divide br or p does not divide cs. If p does not divide br so there exist a least integer t such that p does not divide bt. Now consider

at = btc0 +bt−1c1 +. . .+b0ct.

By assumption, p|at and by choice of t every summand on the right hand side after the

first one is divisible by p .Then it is true that p to divides btc0, this is impossible.

p is prime and p divides neither bt nor c0, which gives contradiction.

Hence the statement.

**Irreducibility of pth Cyclotomic Polynomial**

**Theorem 4.6:**

For any prime p, the pth cyclotomic polynomial is p(x)=(xp-1)/(x-1)=xp-1+xp-2+. . .+x+1 is irreducible over Q.

**Example 4.7:**

The polynomial 3x5 + 15x4- 20x3 + 10x + 20 is irreducible over Q because 5 does not divide 3 and 25 does not divide 20 but 5 does divide 15, -20, 10, and 20.

19

**CHAPTER 5**

**SYMMETRY ANALYSIS OF DIFFERENTIAL EQUATIONS**

**Introduction**

A Lie group of transformations admitted by a differential equation corresponds to

a mapping of each of its solutions to another solution of the same differential equation.

There are an infinite number of ways of representing such a mapping by allowing an

arbitrary change of independent variables. The representation is unique if the independent variables are kept fixed.

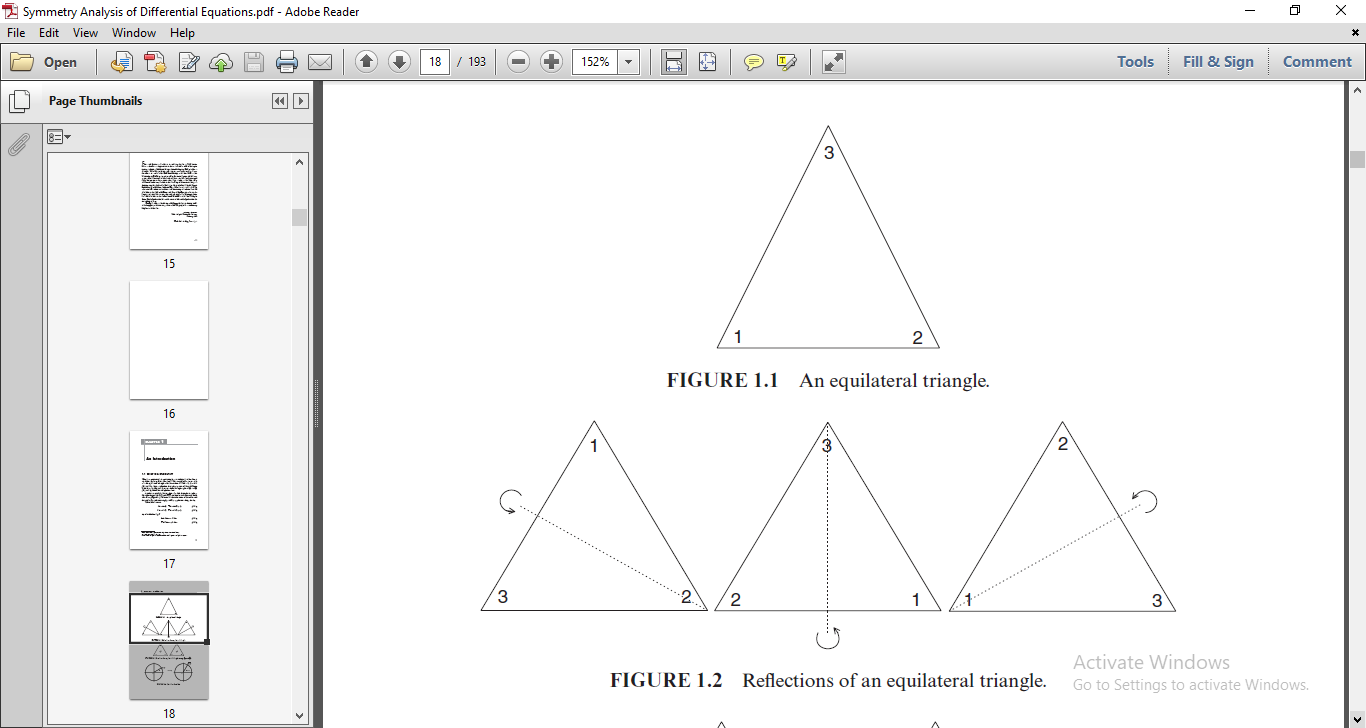
**Symmetry of planar objects**

**Definition 5.1:**

A symmetry of a geometrical object is a transformation whose action leaves the object apparently unchanged.

**Example 5.1:**

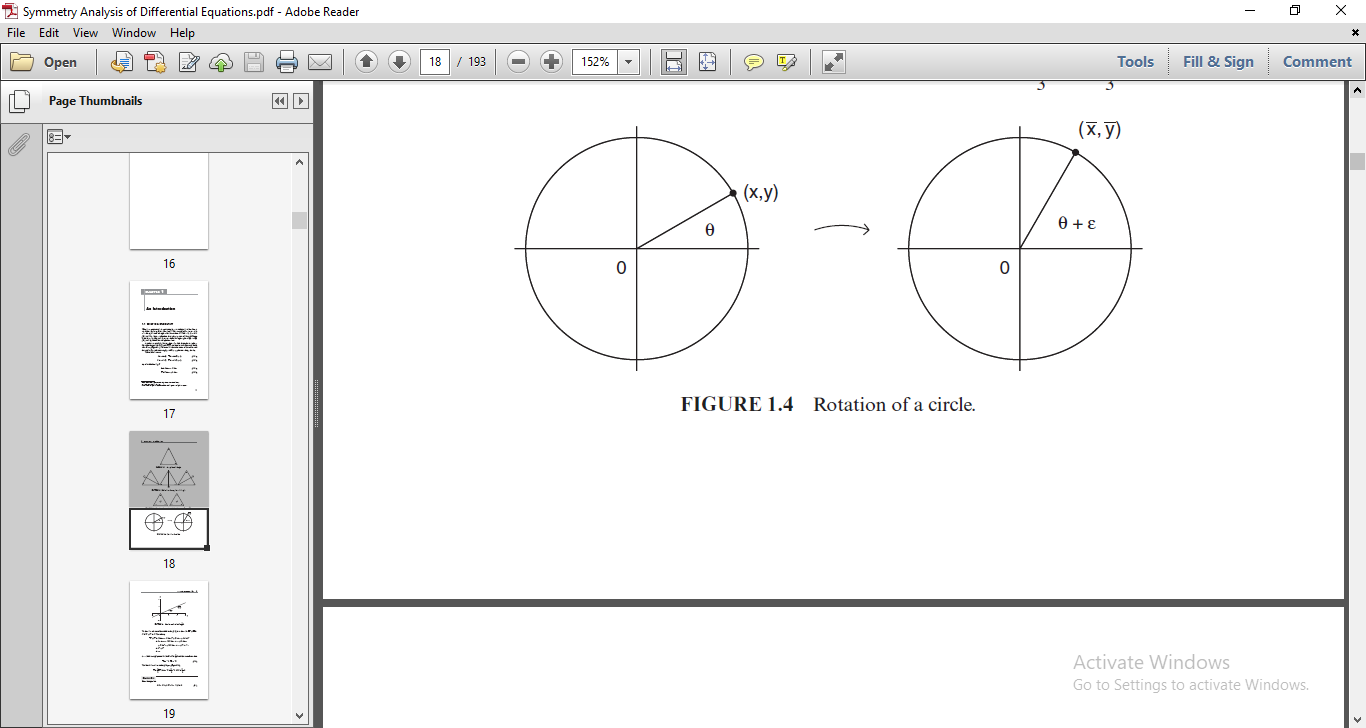
1. Rotating an equilateral triangle anticlockwise about its centre. After a rotation of 2/3, the triangle looks the same as it did before the rotation, so this transformation is a symmetry. Rotations of 4/3 and 2 are also symmetries of the equilateral triangle.The equilateral triangle has the trivial symmetry, the rotations described above, and flips about the three axes. These flips are equivalent to reflections in the axes. So an equilateral triangle has six distinct symmetries.



20

2) The rotation of a disk through an angle 𝜀. Consider the points (x, y) and (, ), on the circumference of a circle of radius r We can write these in terms of the radius and the angles 𝜃 (a reference angle) and 𝜃 + 𝜀, (after rotation), that is, These then become

x = r cos 𝜃, = r cos(𝜃 + 𝜀),

y = r sin 𝜃, = r sin(𝜃 + 𝜀), **Group of transformations**

**Definition 5.2:**

A group G is a set of elements with a law of composition between elements satisfying the following axioms:

(i) **Closure property**: For any elements a and b of G, (a, b) is an element of G.

(ii) **Associative property**: For any elements a, b, c of G:(a, (b, c)) = ((a, b), c).

(iii) **Identity element:** There exists a unique identity element e of G such that for any

element a of G: (a, e) = (e, a) = a.

(iv) **Inverse element**: For any element a of G there exists a unique inverse element a-1 in G such that (a,a-1) =(a-1,a) = e.

**Abelian Group**

**Definition 5.3**:

A group G is Abelian if (a, b) = (b, a) holds for all elements a and b in G.

**21**

**Subgroup**

**Definition 5.4:**

A subgroup of G is a group formed by a subset of elements of G with the same law of composition .

**Examples of group transformation**

**Example 5.2:**

(1) G is the set of all integers with (a, b) = a + b. Here, e = 0 and a-1=-a.

(2) G is the set of all positive reals with (a, b) = a . b. Here, e = 1 and a-1=1/a

(3) G is the set of symmetries(transformations) which leave invariant an equilateral

triangle ABC with both faces painted in the same color .

**Definition 5.5:**

Let x=(x1,x2, . . . ,xn) lie in the region D ⸦ Rn. The set of transformations

x\* = X(x;),

defined for each x in D and parameter in set S ⸦ R, with ( , δ) defining a law of

composition of parameters and δ in S, forms a one-parameter group of transformations

on D if the following hold:

(i) For each in S the transformations are one-to-one onto D. [Hence, x\* lies in D.]

(ii) S with the law of composition forms a group G.

(iii) For each x in D, x\*= x when0 corresponding to the identity e, i.e.,

X(x;0 ) = x.

(iv) If x\* = X(x;), x\*\* = X(x\*; δ), then

x\*\* = X(x;( , )).

**One-parameter lie group of transformations**

A one-parameter group of transformations defines a one-parameter

Lie group of transformations if, in addition to satisfying axioms (i)–(iv) of definition 5.5:

(v) is a continuous parameter, i.e., S is an interval in R. Without loss of generality,

= 0 corresponds to the identity element e.

(vi) X is infinitely differentiable with respect to x in D and an analytic function of in S.

(vii) ( , ) is an analytic function of and δ, S,S.

22

If one thinks of as a time variable and x as spatial variables, then a one parameter

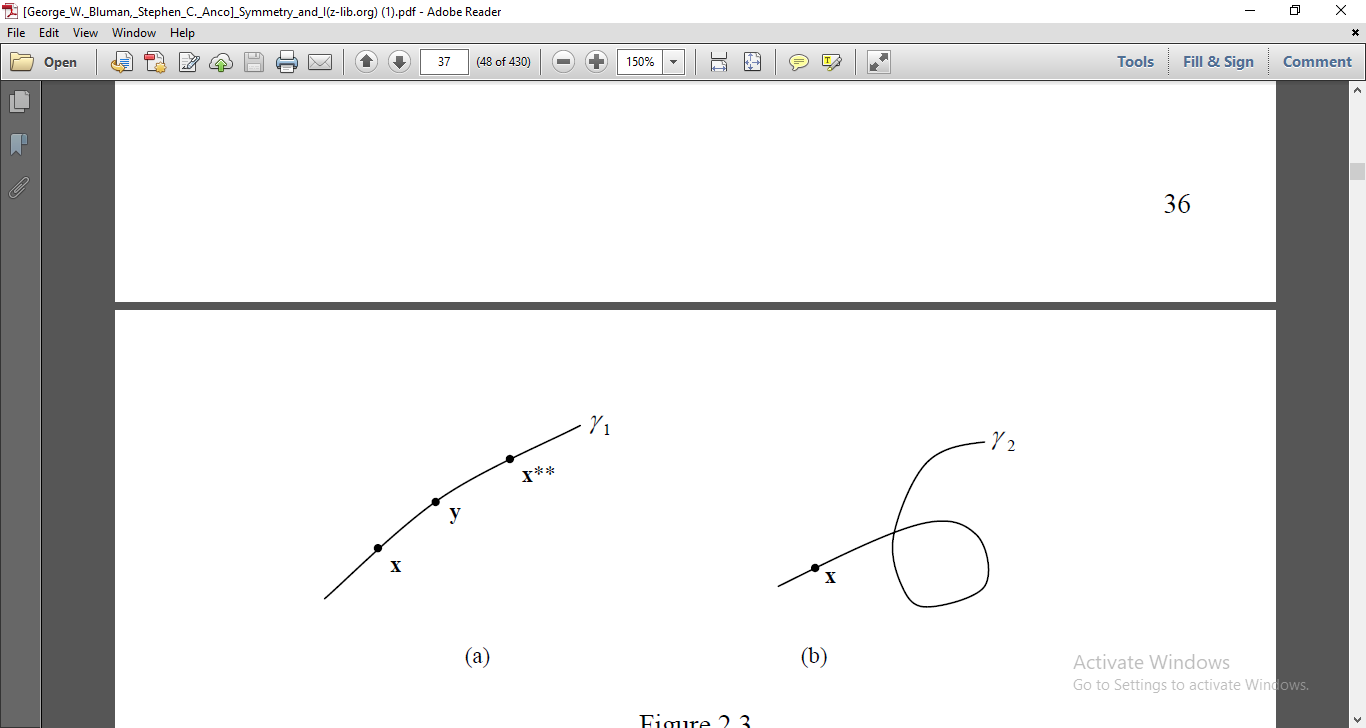
Lie group of transformations, in effect, defines a stationary flow.

Let X(x; ε ) (5.1)

define the evolution of x over all elements S. This defines a curve γ1 [Figure(a)].

Now let y = X(x;) represent a point on γ1. Then x \*\* = X(y; ) =X(x; (, )) must lie on γ1. Note that the self-intersecting curve γ2 [Figure(b)] cannot represent the evolution defined

by (5.1)



**Examples of one-parameter lie groups of transformations**

**Example 5.3:**

(1) Group of Translations in the Plane

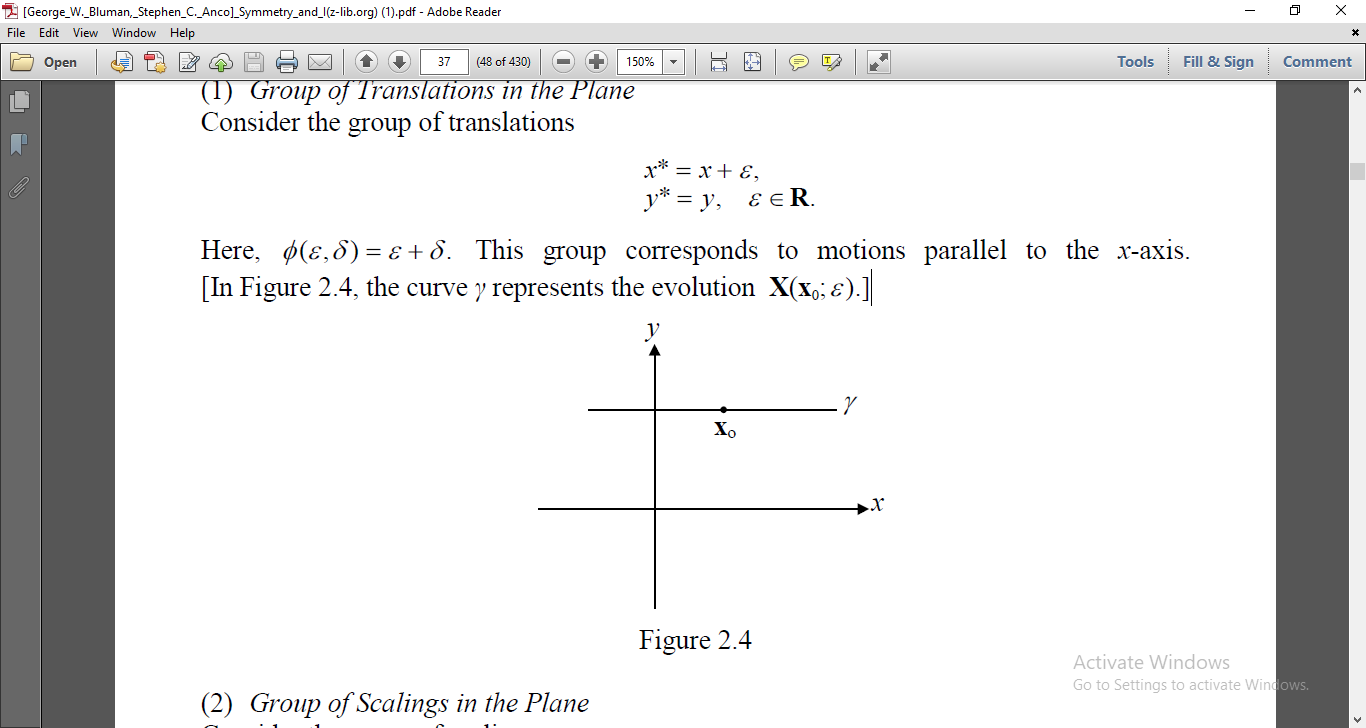
Consider the group of translations

x\*=x+,

y\*=y, R

Here, (,) =+ .This group corresponds to motions parallel to the x-axis.

[In Figure 2.4, the curve γ represents the evolution X(x0;).]



(2) Group of Scalings in the Plane

Consider the group of scalings

23

x\*=

y\*=2y ,0 < <

Here(,)=, and the identity element corresponds to =1. This group of

transformations can also be reparametrized in terms of =-1:

x\* = (1+)x,

y\*= (1+)2y, -1 < <

so that the identity element corresponds to =0 with the law of composition of parameters

given by

()=++

**Infinitesimal transformations**

**Definition 5.6:**

Consider a one-parameter () Lie group of transformations

X\* = X(x;) (5.2)

with the identity = 0 and law of composition . Expanding (5.2) about = 0, in some neighbourhood of = 0, we get

x\*=x+++ . . .x++O().

ξ(x)=.

The transformation x +ξ(x) is called the infinitesimal transformation of the Lie group

of transformations (5.2). The components of ξ(x) are called the infinitesimals of (5.2).

**Example 5.4:**

Consider the ordinary differential equation

=0 (5.3)

The solution to (5.3) is y = c; c R. This yields that the graph of solutions of (5.3) are horizontal lines in the plane.

Thus, for a parameter R , one symmetry of (5.3) is translations in the y-direction,

i.e. (; ) = (x; y+). This is true since the transformation maps the solution y = c to the solution y = c + , which also satisfies (5.3).

24

Another symmetry that (5.3) possesses is the scaling (; ) = (;), since it maps horizontal lines to other horizontal lines. For 0, these transformations will stretch or shrink the lines, but horizontal lines will be preserved as sets. Moreover, for the symmetry of translations in the x-direction. i.e. () = (x +, y), every solution curve is mapped to itself. This is a trivial symmetry.

**Example 5.5:**

Consider the simplest second-order ODE,

= 0 (5.4)

Let us assume that (5.4) is invariant under a one parameter () continuous

point transformations

= +ξ(x,y)+O()

= +(x,y)+O()

=+(1)+ O()

=+(1)+ O()

Therefore, the linearized symmetry condition of (5.4) is (2)=0 when = 0

that is,

+(2-)+(-)-=0

As ξ and are independent of, the linearized symmetry condition splits into the following system of determining equations:

,  2-=0,-=0,=0 (5.5)

The general solution of the last of (5.5) is

ξ (x, y) = A(x)y + B(x);

for arbitrary functions A and B. The third of (5.5) gives

(x; y) = (x)y2 + C(x)y + D(x);

where C and D are also arbitrary functions.

Then the remaining equations in (5.5) amount to

(x)y2 + (x)y + = 0; 3(x)y + 2- = 0; (5.6)

25

Equating powers of y in (5.6), we obtain a system of ODEs for the unknown functions A, B, C, and D: These ODEs are easily solved, leading to the following result. For every one parameter Lie group of symmetries of (5.4),the functions ξ and are of the form

ξ(x; y) = c1+ c3x + c5y + c7x2+ c8xy; (5.7)

(x; y) = c2 + c4y + c6x + c7xy + c8y2; (5.8)

and c1,c2, . . .c8 are arbitrary constants. Thus, the given ODE (5.4) is invariant under

=+(c1+ c3x + c5y + c7x2+ c8xy) (5.9)

=+(c2 + c4y + c6x + c7xy + c8y2) (5.10)

FactorizatiTherefore, the most general infinitesimal generator take the form

X=

= ======xy+.

26

Biblilography

1)Joseph A.Gallian: Contemporary Abstract Algebra,

Cengage Learning,Ninth edition.

1. George.W.Bluman and Stephson K Anko:Symmetry and Integration methods for Differential equation, Springer.
2. I.N. Herstein: Topics in Algebra, Wiley Student

edition,Second edition.

1. Peter.E.Hydon:Symmetric methods of Differential

Equation ,Cambridge Text in Applied Mathematics.

27