SEMESTER II MATHEMATICS GENERAL

LECTURE NOTE

**ABSTRACT AND LINEAR ALGEBRA**

TARUN KUMAR BANDYOPADHYAY, DEPARTMENT OF MATHEMATICS

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0301252.wmf

**TEXT**: (1) Abstract Algebra—Sen,Ghosh,Mukhopadhyay

(2) Abstract and Linear Algebra-- Mapa

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0292020.wmf

In case you face difficulty in understanding the following material , you may e-mail to me at [**tbanerjee1960@gmail.com**](mailto:tbanerjee1960@gmail.com) stating your Name and Roll No.

**DOWNLOAD SITE: WWW.SXCCAL.EDU**

**SECTION I: ABSTRACT ALGEBRA**

**SETS AND FUNCTIONS**

In Mathematics, we define a mathematical concept in terms of more elementary concept(s).For example, the definition of perpendicularity between two straight lines is given in terms of the more basic concept of angle between two straight lines. The concept of set is such a basic one that it is difficult to define this concept in terms of more elementary concept. Accordingly, **we do not define ‘set’** but to explain the concept intuitively we say: a set is a collection of objects having the property that given **any** abstract (the thought of getting 100%marks at the term-end examination) or concrete (student having a particular Roll No. of semester II mathematics general) objet, we can say **without any ambiguity** whether that object belongs to the collection(collection of all thoughts that came to one’s mind on a particular day or the collection of all students of this class) or not. For example, the collection of ‘good’ students of semester II will not be a set unless the criteria of ‘goodness’ is made explicit! The objects of which a set A is constituted of are called elements of the set A. If x is an element of a set A, we write **xA**; otherwise **xA**. If every element of a set X is an element of set Y,X is a subset of Y, written as X Y. X is a **proper** subset of Y if X Y and YX, written as. For two sets X = Y iff (if and only if, bi-implication) X Y and YX. A set having no element is called null set, denoted by .

**Example1.1** a≠{a} (a letter inside envelope is different from a letter without envelope{a}{a,{a}}, {a}{a,{a}}, A(the premise x of the implication x ⇒ x is false and so the implication holds **vacuously**), AA, for every set A.

**Set Operations: formation of new sets**

Let X and Y be two sets. Union of X and Y, denoted by **XY**, is the set {a| aX **or** aY **or** both}. Intersection of X and Y, denoted by **X**, is the set {a| aX **and** aY}. The set difference of X and Y, denoted by **X-Y**, is the set {a| aX **and** a Y}. The set difference U-X is called complement of the set X, denoted by **X/**, where U is the universal set. The symmetric set difference of X and Y, denoted by **X**, is the set (X-Y) U(Y-X). For any set X, the power set of X, ***P*(X)**, is the set of all subsets of X. Two sets X and Y are disjoint iff X = . The Cartesian product of X and Y, denoted by **X X Y**, is defined as the set {(x,y)| xX, yY} [ (x,y) is called an ordered pair. Two ordered pairs (x,y) and (u,v) are equal, written (x,y) = (u,v), iff x = u and y = v]. If we take X = {1,2} and Y = {3}, then X X Y = {(1,3),(2,3)} **≠**{(3,1),(3,2)} = Y X X. Thus Cartesian product between two **distinct** sets are **not necessarily** commutative (Is **?**).

**Laws governing set operations**

For sets X, Y, Z,

* **Idempotent laws**: X, XX = X
* **Commutative laws**: XY = YX, XY = Y
* **Associative Laws**: (XY)Z = X(YZ), (XY)Z = X(Y
* **Distributive laws**: X(YZ) = (X(XZ), X(YZ) = (X(XZ)
* **Absorptive laws**: X(XY)=X, X(XY)=X
* **De’ Morgan’s laws**: X-(YZ) = (X-Y)(X-Z), X-(YZ) = (X-Y)(X-Z)

**Note:** We may compare between usual addition and multiplication of real numbers on one hand and union and intersection of sets on the other. We see that the analogy is not complete e.g. union and intersection both are distributive over the other but addition is not distributive over multiplication though multiplication over addition is. Also A, for all set A but a.a = a does not hold for all real a.

**Example1.2** Let A, B, C be three sets such that AC = BC and AC/ = BC/ holds. Prove that A = B.

**»** A = AU (U stands for the universal set conerned) = A(CC/)(definition of complement of a set) = (AC)(AC/)(distributivity of over = (BC)(BC/)(given conditions)= B(CC/)(distributivity of =B.

**NOTE Make a habit of citing appropriate law at each step as far as practicable.**

**Example1.3** Let A, B, C be three sets such that AB = AC and AB = A, then prove B = C.

**»** B = B(AB) = B(A) = (BA)(BC) (distributivity of over) = (CA)(BC) = C(AB)= C(A) = C.

**Example1.4** A implies A = B: prove or disprove.

**NOTE: Proving** will involve consideration of **arbitrary** sets A,B,C satisfying the given condition, whereas **disproving** consists of giving counter-examples of three **particular** sets A,B,C that satisfies the hypothesis A but for which the conclusion A = B is false.

**»** This is a true statement. We first prove AB. Let xA.

**Case 1** xC. Then x (A-C)(C-A) = A = = (B-C)(C-B). Thus x Since xC, x.

**Case 2** xC. x (A-C) A = = (B-C)(C-B). Since xC, xC-B. Thus xB-C. So x.

Combining the two cases, we see A. Similarly, BA. Combining, A = B.

**Example1.5** Prove or disprove: (A-B)/ = (B-A)/.

**»** This is a FALSE statement. **COUNTEREXAMPLE**: Let U = A = {1,2}, B = {1}.Then (A-B)/ = {1} ≠ (B-A)/ = {1,2}.

**Example1.6** Prove: [(A-B)(AB)][(B-A)(AB)/] =

**»** By distributivity,[(A-B) (B-A)][(A-B) A B)/][(AB)][(AB)]= [(A-B)(A/B/)] = .

**PRACTICE SUMS**

1. Prove or disprove: A(B-C) = (AB) – (AC)
2. Prove or disprove: A-C = B-C iff AC = BC.( ‘IFF’ stands for’ if and only if’)
3. Prove :A X (BC) = (A X B) (A X C)

NOTATION: N,Z,Q,R,C will denote set of all positive integers, integers, rational numbers ,real numbers and the complex numbers respectively.

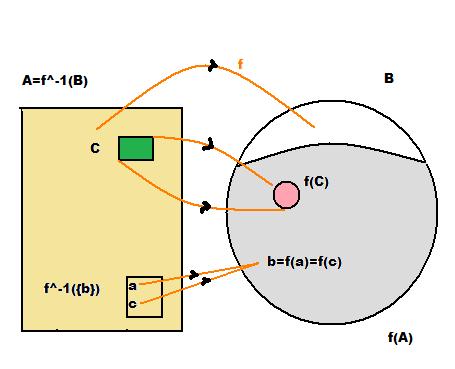
A **function** from a set A to a set B, denoted by f: AB, is a correspondence between elements of A and B having the properties:

* For **every** xA, the corresponding element f(x) f(x) is called the image of x under the correspondence f and x is called a preimage of f(x). A is called domain and B is called the **codomain** of the correspondence. Note that we differentiate between f, the correspondence, and f(x), the image of x under f.
* For a **fixed** xA, f(x) is unique. For two different elements x and y of A, images f(x) and f(y) may be same or may be different.

In brief, **a function is a correspondence under which**

* **both existence and uniqueness of image of all elements of the domain is guaranteed but**
* **neither the existence nor the uniqueness of preimage of some element of codomain is guaranteed**.

**NOTATION** Let f:AB. For yB, f-1({y}) = , if y has no preimage under f and stands for the set of all preimages if y has at least one preimage under f. For two elements y1,y2B, f-1({y1,y2})= f-1({y1}) f-1({y2}). For CA, f(C) = {f(c)| c f(A) is called the range of f.

  
*IMAGE SET AND PREIMAGE SET UNDER A FUNCTION f*

**Example1.7** Prove that f(AB) f(A)f(B) ; give a counterexample to establish that the reverse inclusion **may not** hold.

**»** y f(AB)y = f(x), x AB y = f(x), x A and xByf(A)and yf(B)y f(A)f(B). Hence f(AB) f(A)f(B). Consider the counterexample: f: RR,f(x) = x2, A = {2}, B = {-2}.

**Example1.8** Let f: RR, f(x) = 3x2-5. f(x) = 70 implies x = ±5. Thus f-1{70} = {-5, 5}.Hence f[f-1{70}] = {f(-5), f(-5)} = {70}. Also, f-1({-11}) = [x f-1({-11})3x2-5=-11x2=-2].

**Example1.9** Let g: RR, g(x) = . Find

g-1({2}).

**PRACTICE SUMS**

Prove that (1) f(AB) =f(A)f(B), (2) f-1(B1B2) = f-1(B1)f-1(B2), (3) f-1(B1B2) = f-1(B1)f-1(B2).

A function under which uniqueness of preimage is guaranteed is called an **injective** function. A function under which existence of preimage is guaranteed is called a **surjective** function. Put in a different language, f: AB is injective iff a1, a2A, f(a1) = f(a2) implies a1 = a2. f is surjective iff codomain and range coincide. A function which is both injective and surjective is called **bijective**.[..\Documents\104.jpg](../Documents/104.jpg)

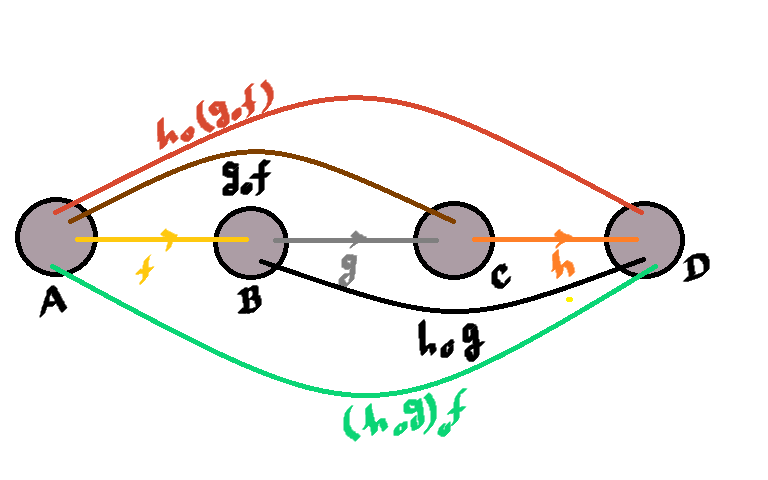
**NOTE:** The injectivity, surjectivity and bijectivity depends very much on the domain and codomain sets and may well change with the variation of those sets even if expression of the function remains unaltered e.g. f:ZZ, f(x) = x2 is not injective though g:NZ, g(x) = x2 is injective.

**Example1.10** f: RR, f(x) = x2 – 3x+4. f(x1) = f(x2) implies (x1-x2)(x1+x2-3) = 0. Thus f(1) = f(2) though 1≠2; hence f is not injective[Note: for establishing non-injectivity, it is sufficient to consider particular values of x]. Let yR and xf-1{y}. Then y = f(x) = x2 – 3x+4. We get a quadratic equation x2 – 3x+(4-y) = 0 whose roots, considered as a quadratic in x, give preimage(s) of y. But the quadratic will have real roots if the discriminant 4y-70, that is , only when y7/4. Thus, for example, f-1{1} = Hence f is not surjective.

If f:AB and g:BC, we can define a function g0f:AC, called the **composition** of f and g, by (g0f)(a) = g(f(a)), aA.

**Example1.11** f:Z Z and g: Z Z by f(n) = (-1)n and g(n) = 2n. Then g0f: Z Z, (g0f)(n)=g((-1)n) = 2(-1)n and (f0g)(n) = (-1)2n. Thus g0f ≠ f0g. Commutativity of composition of functions need not hold.

**Note**: Composition of functions, whenever is defined, is associative.



*ASSOCIATIVITY OF COMPOSITION OF FUNCTIONS*

**PRACTICE SUMS**

Let f:AB and g:B.Then prove that:

1. if f and g are both injective, then g0f is so.

[hints (g0f)(x)=(g0f)(y) ⇒g(f(x))=g(f(y)) ⇒f(x)=f(y) ⇒x=y]

1. If g0f is injective, then f is injective.
2. [hints f(x)=f(y) ⇒g(f(x))=g(f(y)) ⇒(g0f)(x)=(g0f)(y) ⇒x=y]
3. if f and g are both surjective, then g0f is so.

[hints cC⇒bB,c=g(b) ⇒aA,b=f(a) ⇒c=g(b)=g(f(a))=(g0f)(a)]

1. If g0f is surjective, then f is surjective.

Verify whether following functions are surjective and / or injective:

1. f:RR, f(x) = x
2. f: (-1,1)R, f(x) =

Let f:AB be a bijective function. We can define a function f-1: B A by f-1(y) = x iff f(x) = y. Convince yourself that because of uniqueness and existence of preimage under f ( since f is injective and surjective), f-1 is indeed a function. The function f-1 is called the **inverse function** to f. The graphs of f and f-1 for a given f can be seen here: [..\Documents\x8.mw](../Documents/x8.mw)

**Note** Graph of f-1 can be obtained by reflecting the graph of f about line x=y.

**Example1.12** Let f: (0,1)(1/2,2/3) be defined by f(x) = . Verify that f is bijective(DO IT).

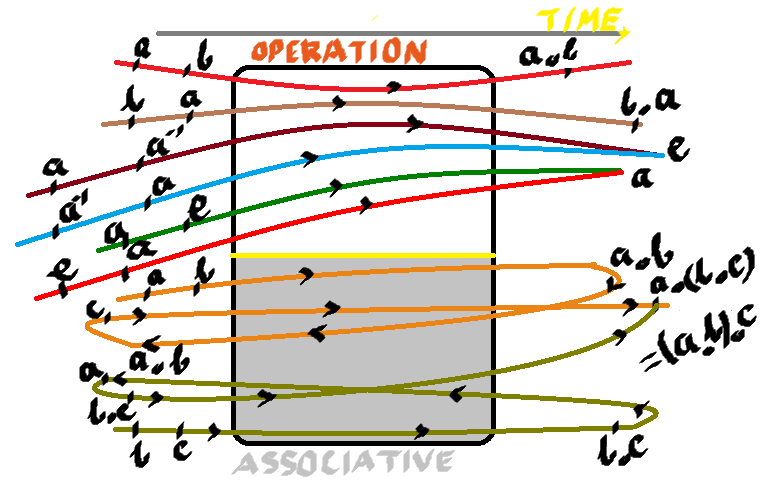
[explanation:f(x)=f(y)⇒=⇒x=y. Let c(1/2,2/3). If possible, let x be a pre-image of c under f, that is, f(x)=c. then c= implying x= (0,1) since -1/2<c-1<-1/3, -1/3<1-2c<0]. f-1: (1/2,2/3)is to be found. Now, let f-1(y) = x, y. Then f(x) = y. So =y and hence x = = f-1(y).

**BINARY OPERATIONS**

Let A≠. A **binary operation** ‘0’ on A is a function from A X A to A. In other words , a binary operation ‘0’ on A is a rule of correspondence that assigns to each ordered pair (a1,a2) A X A, some element of A, which we shall denote by a1 0a2. Note that a1 0a2 **need not be** distinct from a1 or a2.

**Example1.13** Subtraction is a binary operation on Z but not on N; division is a binary operation on the set Q\* of all nonzero rational number but not on Z.

Let 0 be a binary operation on A≠. 0 is **commutative** iff x0y = y0x holds ,for all x,yA. 0 is **associative** iff x0(y0z) = (x0y)0z holds for all x,y,zA. An element eA is an **identity** of the **system** (A,0) (that is, a nonempty set and a binary operation defined on the set) iff x0e = e0x = x holds for all xA. Let (A,0) be a system with an identity e and let x, yA such that x0y = y0x = e holds. Then y(x) is called an **inverse** to x(y respectively) in (A,0).



*BINARY OPERATION ‘MACHINE’: ASSOCIATIVE BINARY OPERATION IN PARTICULAR*

**Example1.14** Consider the system (R,0) defined by x0y = x, x,yR. Verify that 0 is non-commutative, associative binary operation and that (R,0) has no identity.

**Example1.15** Verify that subtraction is neither associative nor commutative binary operation on Z. (Z,-) does not have any identity.

**Example1.16** Consider the system (Z,\*) where the binary operation \* is defined by a\*b = , a,bZ. Verify that \* is commutative but not associative [ note, for example, that {(-1) \*2}\*(-3)≠(-1) \*{2\*(-3)}]. (Z,\*) does not have an identity.

**Example1.17** (R,+) is commutative, associative, possess an identity element 0 and every element of (R,+) has an inverse in (R,+).

**NOTE** From examples 1.12 to 1.15 it is clear that associativity and commutativity of a binary operation are properties independent of each other, that is, one can not be deduced from the other.

**Example1.18** Let 2Z denote set of all even integers. 2Z, under usual multiplication, form a system which is associative, commutative but possesses no identity.

**Example1.19** Let M2(Z) = . M2(Z) under usual matrix addition forms a system which is commutative, associative. (M2(Z),+) possesses an identity, namely the null matrix, and every element in (M2(Z),+) has an inverse in (M2(Z),+).

**Example1.20** Let GL(2,R) denote the set of all 2x2 real non-singular matrices under usual matrix multiplication. The system is associative, non-commutative, possesses an identity and every element has an inverse in the system.

**Example1.21** Let Zn = {0,1,2,…,n-1} and let +n be the binary operation defined on Zn by: for a,b Zn, a+nb is the smallest nonnegative remainder obtained by dividing a+b (usual addition in Z) by n. we can define the operation by the following **Cayley Table:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **+n** | **0** | **1** | **2** | **…** | **n-2** | **n-1** |
| **0** | **0** | **1** | **2** | **…** | **n-2** | **n-1** |
| **1** | **1** | **2** | **3** | **…** | **n-1** | **0** |
| **2** | **2** | **3** | **4** | **…** | **0** | **1** |
| **…** | **…** | **…** | **…** | **…** | **…** | **…** |
| **n-1** | **n-1** | **0** | **1** | **…** | **n-3** | **n-2** |

(Zn,+n) can be proved to be commutative and associative, possesses an identity element 0 and an element rZn has an inverse (n-r) for r≠0 and inverse of 0 is 0. Commutativity is clear from the symmetry of the table about the main diagonal.

**Example1.22** Let D = {zC| zn = 1} be the set of all n th roots of unity. D, under usual complex multiplication, forms a commutative, associative system possessing identity 1 and inverse of zD is 1/zD.

**DEFINITION** A nonempty setG with a binary operation ‘**.’**defined on G forms a **group** iff following conditions are satisfied: (1) **.** is associative, (2) (G,**.**) has an identity element, generally denoted by e and (3) every element xG has an inverse element x-1G. If, in addition, (G,.) is commutative , (G,.) is an abelian group.

**Note: x-1 is not to be confused with 1/x.** If the group operation is denoted by ‘+’, then inverse of x is denoted by – x.

Example of formation of **negation** of a mathematical statement: 

UNDER WHAT CIRCUMSTANCE DO WE SAY (G,.) IS **NOT** A GROUP?

**Example1.23** Verify whether (Z,0) defined by a0b = a+b – ab (usual operations on Z on the RHS) forms a group.

**»** (a0b)0c = (a+b – ab)0c = (a+b – ab)+c – (a+b-ab)c = a+b+c – ab – bc – ca+ abc

a0(b0c) = a0(b+c – bc) = a+(b+c – bc) – a(b+c – bc) = a+b+c – ab – bc – ca+abc.

So, (a0b)0c = a0(b0c), for a,b,cZ. Thus (Z,0) is associative.

Clearly, a00 = 00a = a, aZ. Thus (Z,0) possesses an identity 0Z.

Let az and bZ be an inverse to a. by definition, a0b = b0a = 0. Thus a+b – ab = 0. Hence , for a≠1, b = a/(a-1). But , in particular, for a = 3, b = 3/2Z. Hence (Z,0) does NOT form a group.

**Example1.24** Verify whether (R,0) defined by a0b =, a,bR forms a group.

**»** Verify that(R,0) is associative and commutative. If (R,0) has an identity eR, then a0e = e0a = a holds for all a R. Thus = a. hence = a - <0 for a<0, contradiction. Hence (R,0) has no identity element and hence does **NOT** form a group.

**PRACTICE SUMS**

Verify whether following system forms group or not:

1. (Z,0) , a0b = a, a,bZ
2. (Z,0) , a0b = a+b+2
3. (2Z+1,\*), a\*b = a+b-1 [2Z+1 stands for set of all odd integers]
4. Let S and *P*(S) be the power set of S. Consider (*P*(S),).
5. Let S and *P*(S) be the power set of S. Consider (*P*(S),).
6. Let Q[ = {a+ b| a,bQ}. consider (Q[-{0},.)

**Elementary properties of Group**

**Theorem 1.1** Let (G,.) be a group. The following properties hold:

1. Identity element e in G is unique
2. For a given element x of G, x-1 is unique
3. e-1 = e, (x-1)-1 = x, xG.
4. (Cancellation Laws) for a,b,cG, a.c = b.c⇒a = b(right cancellation property)

c.a = c.b⇒a = b(left cancellation property)

(5) (a.b)-1 = b-1.a-1, a,bG.

**»** (1) Let e,f be two identities of (G,.). Then e = e.f (f is an identity element) = f (e is an identity element)

(2) Let y and z be both inverse element of the element x in G. By definition, x.y = y.x = e and x.z = z.x = e. Then y = y.e = y.(x.z) = (y.x).z = e.z = z. hence x-1 for given x is unique.

(3) Since e.**e**= e and x.**x-1**= e, it follows from definition of identity and inverse element.

(4) a.c = b.c⇒(a.c).c-1 = (b.c).c-1⇒a.(c.c-1) = b.(c.c-1) (associativity) ⇒a.e = b.e⇒a = b.

(5) (a.b).(b-1.a-1) =a.(b.b-1).a-1 = (a.e).a-1 = a.a-1 = e. S**imilarly** (need be mentioned)(b-1.a-1).(a.b) = e. Hence.

**Notation:** Let G be a group, aG, nZ. a0=e(identity), an =(( a.a)…a)( n times, n),an = (a-1).(a-1)…(a-1) (-n times, -nN).

**Example1.25** Let (G,.) be a group such that (a.b)-1 = a-1.b-1, a,bG. Prove that G is abelian.

**»**For all a,bG, (a.b)-1 =a-1.b-1 = (b.a)-1. Hence a.b = [(a.b)-1]-1 = [(b.a)-1]-1 = b.a, a,bG.

**Example1.26** Let (G,.) be a finite abelian group and G={a1,a2,…,an}. Let x = a1.a2….an G. Prove that x2 = e.

**»** using commutativity and associativity of (G,.), x2 can be expressed as product of finite number of pair of elements of G, each pair consists of elements which are mutually inverse to each other. Hence the result.

**Example1.27** Let G be a group such that a2 = e, for all aG. Prove that G is abelian.

**»** For aa.a = a2=e = a.a-1⇒ a = a-1⇒a.b = a-1.b-1 = (b.a)-1 = b.a, for a,bG. Hence.

**Example1.28** Let G be a group such that for a,b,c , a.b = c.a implies that b = c. Show that G is abelian.

**»** (a.b).a = a.(b.a), for a,b,cG (by associativity) ⇒a.b = b.a

**Example1.29** Prove that G is abelian iff (a.b)2 = a2.b2, a,bG.

**» Sufficiency** a.(b.a).b = (a.b)2 = (a.a)(b.b) = a.(a.b).b⇒ b.a = a.b for a,bG.

**Necessity** If G is abelian, then (a.b)2 = (a.b).(a.b) = a.(b.a).b = a.(a.b).b = (a.a).(b.b) = a2.b2.

**Example1.30** In a group G, a.b.c = e⇒b.c.a = e.

**»**Try yourself.

**SUBGROUP OF A GROUP**

Let (G,.) be a group and HG. H is called a **subgroup** of G iff (1) for a,bHG, a.bH and (2) (H,.) is a group. Every group G≠{e} has at least two subgroups, namely G and {e}. These are called **trivial** subgroups; other subgroups are called **nontrivial** subgroups.

Note The system (N,+) satisfies (1) but is not a subgroup of the group(Z,+). It can be shown that if H is **finite** and satisfies (1), then H is a subgroup of G.

**Example1.31** (Q,+) is a subgroup of (R,+).(2Z,+) is a subgroup of (Z,+), (Z,+) is **NOT** a subgroup of (R-{0},.).{1,-1} is a subgroup of (Q\*,.), Q\* standing for set of all nonzero rationals. {0,4} is a subgroup of (Z8,+8). H = {zC| is a subgroup of the multiplicative group C\* of all nonzero complex numbers.

**Theorem 1.2** All subgroups of a given group (G,.) have the same identity.

**»** Let H be a subgroup of (G,.). Let eG and eH  be the respective identities. Then eH.eH = eh (eH considered as element of (H,.)) = eH.eG (eH considered as an element of G, eG being the identity of G) , by cancellation property in G, implies eG = eH.

**Corrolary** Intersection of all subgroups of a given group is nonempty.

**Theorem 1.3** Let H be a subgroup of the group G and let xH. Then xG-1 = xH-1.

**»** x. xG-1 = eG = eH = x.xH-1⇒ xG-1 = xH-1.

**Note**: For xH,x-1H. But for xG-H, x-1∉H; for, otherwise, x=H.

**Theorem 1.5 (Necessary and sufficient condition for a nonempty subset of a group to form a subgroup)**

Let G be a group and H be a **nonempty** subset of G. Then H is a subgroup of G iff for all a,bH, a.b-1H.

**Example1.33** Let G be a group and aG. Let C(a) = {xG|a.x = x.a}. Show that C(a) is a subgroup of G.

**»** eC(a). Thus C(a) ≠. Let x,yC(a). Then x.a = a.x, y.a = a.y. so (x.y)a = x.(y.a) = x.(a.y) = (x.a).y = (a.x).y = a.(x.y). Hence x.yC(a). Again xC(a) ⇒x.a = a.x⇒x-1(x.a).x-1 = x-1.(a.x).x-1⇒a.x-1 = x-1.a⇒x-1=C(a). Hence.

**Example1.34** Prove or disprove: the group (R\*,.) has no finite subgroup other than {1}.

**»** let H be a finite subgroup of (R\*,.) other than {1}. Let xH,x≠1 . Either or >1, call it y.Thus {y,y2,..}H with all the elements distinct, contradiction.

**Example1.35** Prove or disprove: Let G be a group and H be a nonempty subset of G such that a-1H for all aH.Then H is a subgroup.

**»**Try yourself.

**Example1.36** Prove or disprove: there does not exist a proper subgroup H of (Z,+) such that H contains both 5Z and 7Z.

**»** 1 = 3.7 – 5.4H, hence H = Z(since any integer can be obtained by finite number of addition of 1 or of -1 or by additionof 1 and -1.Note that since 1H and H is a subgroup, -1H).

**RINGS AND FIELDS**

**Definition** A nonempty set R with two binary operations ‘+’ and ‘.’ defined on R forms a **ring** (R,+,.) IFF

1. (R,+) is an **abelian** group: for a,b,cR,
2. (a+b)+c = a+(b+c)
3. 0R,aR such that a+0 = 0+a = a(**Caution:** interchange of the quantifiersand will be **disastrous**)
4. aR,(-a)R such that a+(-a) = (-a)+a = 0
5. (R,.) is associative: for a,b,cR, a.(b.c) = (a.b).c
6. ‘.’ is distributive over ‘+’: a.(b+c) = (a.b)+(a.c), (b+c).a = (b.a)+(c.a), a,b,cR.

**Note**: Assumptions corresponding to first named operation’+’ are many more than those corresponding to second named operation’.’. Imposing more conditions on ‘.’ results in special type of rings. A ring (R,+,.) is **commutative** iff a.b = b.a, a,b R. A ring (R,+,.) is **with unity** iff 1R such that a.1 = 1.a = a,a R. The identity with respect to the first operation is referred to as **identity** whereas the identity with respect to second operation is called **unity.**

**Example1.37** Verify whether (Z,+,.) forms a ring, where ‘+’ is the usual addition of integers and a.b = max{a,b}, a,bZ.

**Example1.38** Prove that (Z,0,\*) defined by a­0b = a=b – 1 and a\* b = a+b – ab forms a commutative ring with unity.

**Example1.39** Let 2Z be the set of all even integers. Define + as usual and . by a.b = ½ ab(usual multiplication on the right). Verify whether (2Z,+,.) forms a ring. Is there a unity in (2Z,+,.)?

**Example1.40** Let X≠. Prove that (*P*(X),Δ,) form a commutative ring.

**Theorem 1.6** Let R be a ring and a,bR .Then for a,bR, (1) a.0 = 0 = 0.a, (2) a.(-b) = (-a).b = -(a.b).

**»** (a.0)+0 = a.0 (0 is additive identity) = a.(0+0) = (a.0)+(a.0) (distributivity). By left cancellation property in the group (R,+), a.0 = 0.

Also [a.(-b)]+[a.b] = a.[(-b)+b] = a.0 = 0 and commutativity of + ensures that [a.b]+[a.(-b)] = 0. Hence a.(-b) =-(a.b). Similarly other part can be proved.

**Definition** A nonempty set F with two binary operations ‘+’ and ‘.’ defined on F forms a field iff

1. (F,+) is an abelian group(let 0 be the identity element)
2. (F-{0},.) is an abelian group(let 1 be the identity element)
3. ‘.’ Is distributive over ‘+’.

**Note: obviously 0≠1 in a field**, since (F-{0},.)s nonempty.

**Example1.41** The sets Q,R,C under usual addition and multiplication operations form fields.

**Subrings and Subfields**

**Definition** A nonempty subset S of a ring (R,+,.) is called a **subring** of the ring R iff (S,+) is a subgroup of the abelian group (R,+) and for all a,bS, a.bS.

**Example1.42** In the following chain , the former is a subring of the later(under usual addition and multiplication): Z Q . For any fixed natural n, nZ = {na|aZ} is a subring of Z.

**Example1.43** The set Z[ = {a+ b| a,bZ} is a subring of R.

**Example1.44** The ring of Gaussian integers {a+i b| a,bZ} is a subring of C.

**Theorem 1.7** Let R be a ring and S be a nonempty subset of R. A necessary and sufficient condition that S is a subring of R is a,bS implies a – b, a.bS.

**NOTE :** A ring with unity (multiplicative identity) may have a subring without a unity.The subring (2Z,+,.) has no unity whereas the ring (Z,+,.) has a unity 1.It may also happen that a ring R and one of its subring S may both have unity but 1S ≠1R. IN CONTRAST, every subring must share the same identity with the ring.

**Definition** Let F be a field. A subring S of F is called a subfield of F iff 1F S and for each 0≠aS, a-1S.

**Theorem 1.8** LetS be a subset of a field F. Then S is a subfield of F iff (1) a - bS, for all a,bS, and (2) a.b-1S, for all a and bS-{0}.

**Example1.45** T = {a+bw| a,bQ} is a subfield of C (w stands for an imaginary cube root of unity) .

**Example1.46** Prove that S = is a subring of the ring R = .

**Example1.47** Verify whether S = {0,2,4,6,8,10} forms a subfield of the field (Z11,+11,.11), where Z11 = {0,1,2,…,10}, a+11b and a.11b is defined to be the smallest nonnegative remainder obtained by dividing a+b and a.b respectively by 11, for a,bS.

**Example1.48** Verify whether Q[ = {a+ b| a,b} is a subfield of R.

SECTION II: LINEAR ALGEBRA

**MATRICES**

**Definition** A rectangular array of mn elements aij into m rows and n columns, where the elements aij belong to a field F, is called a matrix of order mxn over F. It is denoted by [aij]mxn or by . F is called field of scalars. In particular, if F be the field R of real numbers, a matrix over R is said to be a real matrix. The element aij appearing in the i th row and j th column of the matrix is said to be ij th element. If m=1, the matrix is said to be a **row matrix** and if n = 1, it is called a **column matrix.** If each element of a matrix is 0, it is called a **null matrix** and denoted by Omxn. If m=n, matrix is called a **square matrix**. Two matrices [aij]mxn and [bij]pxq are **equal** iff m = p, n = q and aij = bij for each i and j. A square matrix whose elements on the principal diagonal are all equal to 1 and all the elements off the main diagonal are 0 is called **identity matrix** and is denoted by In. If A = [aij]mxn, then **transpose of A**, denoted by AT, is defined as AT = [bij]nxm,where bij = aji, for each i and j. A square matrix is a **diagonal matrix** if all the elements not lying on the main diagonal are zero.

**OPERATION ON MATRICES**

Equality of matrices [aij]mxn=[bij]pxq iff m=p,n=q and aij = bij, for each i,j.

Multiplication by a scalar for a scalar c, c[aij]mxn = [caij]mxn

Addition two matrices [aij]mxn , [bij]pxq are conformable for addition iff m = p and n = q and in that case

[aij]mxn+[bij]mxn = [aij+bij]mxn

Multiplication two matrices [aij]mxn , [bij]pxq are conformable for multiplication iff n = p. in that case

[aij]mxn [bij]nxq = [cij]mxq, cij =.

**ALGEBRA OF MATRICES**

1. Matrix addition is commutative and associative.Try yourself
2. Matrix multiplication is NOT commutative : provide **counterexample.**
3. Matrix multiplication is **associative**. Let A = [aij]mxn, B = [bij]nxp, C = [cij]pxq. Then AB = [dij]mxp, where dij = . Thus (AB)C = [eij]mxq where eij = = . Again, BC = [fij]nxq, where fij = . Thus A(BC) = [gij]mxq where gij = = = eij, for all I,j. hence A(BC) = (AB)C.
4. Matrix multiplication is distributive over addition: **prove yourself.**
5. (AT)T = A
6. (A+B)T = AT+BT.
7. (AB)T = BTAT (supposing A,B are conformable for product). Let A = [aij]mxn, B = [bij]nxp. AB =[cij]mxp, where cij = . So (AB)T =[dij]pxm, dij = cji=. BT = [eij]pxn , AT = [fij]nxm where eij = bji,fij = aji. Hence BTAT = [gij]pxm, where gij ===dij. Hence.

**Symmetric and skew-symmetric matrix**

A square matrix A is **symmetric** iff A = AT. A square matrix A is **skew-symmetric** iff A = -AT.

**Results involving symmetric and skew-symmetric matrices**

1. If A and B are symmetric matrices of the same order, then A+B is symmetric.
2. If A and B are symmetric matrices of the same order , then AB is symmetric iff AB = BA.

**»** if AB is symmetric, then AB = (AB)T = BTAT = BA. If AB = BA, then AB = BA = BTAT = (AB)T, so that AB is symmetric.

1. AAT and ATA are both symmetric.
2. A real or complex square matrix can be uniquely expressed as the sum of a symmetric and a skew-symmetric matrix.

**»** let A be a square matrix. then A can be expressed as A = where is symmetric and is skew-symmetric. Uniqueness can be proved(Try yourself!)

PRACTICE SUMS

1. If A and B are square matrices of the same order, does the equality A2-B2 = (A+B)(A-B) hold good? Justify.
2. Three matrices A,B and C are such that AB = AC. Can we conclude B = C?
3. Three matrices A,B and C are such that AB = In, BC = In. Prove A = C.

DETERMINANT

Let M stand for the set of all square matrices over R. We define a function det: MR **inductively** as follows:

**Step 1** det X= a11=(-1)1+1a11, if X= [a11]1x1. det, if X=[aij]2x2= .

**Step 2** let us assume the definition is valid for a square matrix of order n: thus for X= (aij)nxn , det X=, where X1r is a matrix of order n-1, obtained from X by deleting the first row and r th column. We now consider X = (aij)(n+1)x(n+1). We now define det X =, where X1r is a matrix of order n, obtained from X by deleting the first row and r th column. By assumption, can be evaluated for all r. so the definition is valid for a square matrix of order (n+1).

Hence by induction, for a matrixX = (aij)nxn , we define det X =, where X1r is a matrix of order n-1, obtained from X by deleting the first row and r th column.

Following this definition , we can define det X, for any X M.

**Example 2.1** for the matrix X=, det X = (-1)1+1a11X11+(-1)1+2a12X12+(-1)1+3a13X13, where X1r is the determinant of the matrix obtained by deleting the first row and r th column of A. now X11 = (-1)2+2a22det(a33)+(-1)2+3a23det(a32) = a22a33-a23a32. Similarly value for X**12** and X**13** can be found and finally value ofdet X can be calculated.

**Properties of determinants**

1. detX = det X**T**, where X = . By actual calculation, we can verify the result.

NOTE: By virtue of this property, a statement obtained from an established result by interchanging the words ‘row’ and ‘column’ thoroughly will be established.

1. Let A be a matrix and B is obtained from A by interchanging any two rows (columns) of a matrix A,then detA = - det B.
2. If A be a matrix containing two identical rows (or columns), then det A = 0. Result follows from (2).
3. If elements of any row of a determinant is expressed as sum of two elements, then the determinant can be expressed as a sum of two determinants.

**Example** det=, which can be verified using definition and earlier properties.

1. If elements of any row of a determinant is multiplied by a constant, then the determinant is multiplied by the same constant

**Example**= c det , which can be verified using definition and earlier properties.

1. In an nxn matrix A if a scalar multiple of one row(column) be added to another row(column), then detA remains unaltered.

**»** det = det, [by property (4)] = det+c, [by property(5)] = det+c.0, [by property(3)] = det

1. In an nxn matrix A, if one row(column) be expressed as a linear combination of the remaining rows(columns), then detA = 0.

**»** det

= c1det+c2det=0.

**Example2.2**  Prove without expanding the determinant =0

**»** =+=

- +=0.

**Cofactors and Minors**

Let A = [aij]mxn. Mij, **minor** of the element aij, is the determinant of the matrix obtained by deleting i th row and j th column of the matrix A. Aij, cofactor of the element aij, is defined as (-1)i+jMij.

**Theorem2.1** For a matrix A=[aij]3x3, ai1Ak1+ ai2Ak2+ ai3Ak3 = det A, if i=k and = 0, if i≠k.

**»** a11A11+a12A12+A13 = a11(-1)1+1det+a12(-1)1+2det+a13(-1)1+3det=detA, by definition. Also, a11A21+a 12A 22+a13A 23 = a11(-1)2+1det+a12(-1)2+2det+a13(-1)2+3det

=det (by definition of determinant) = 0(by property (3)).

Similarly other statement can be proved.

**Multiplication of determinants**

**Theorem2.2** If A and B are two square matrices of the same order, then det(AB) = detA.detB= det AT.det B

**Note** In view of the above theorem, multiplication of determinants can be carried out either using ‘**row by row**’ rule or using ‘**row by column**’ rule.

**Example2.3**  prove =(a3+b3+c3-3abc)2

**»** we have =- (a3+b3+c3-3abc). Now = = . Hence.

**Example2.4**  Prove that =2(a-b)2(b-c)2(c-a)2.

We have = (a-b)(b-c)(c-a). now 2=-2

=. Hence.

**Definition** If A=(aij) be a square matrix and Aij be the cofactor of aij in det A, then det(Aij) is the adjoint of det A.

**Theorem2.3** If A=(aij)3x3, then det(Aij)=[det (aij)]2, if det (aij)≠0.

**»** =

= (det A)3. Hence det(Aij)=[det (aij)]2, if det (aij)≠0.

**Example2.5** Prove =(a3+b3+c3-3abc)2

**»**  we have =-(a3+b3+c3-3abc). Now = adj==RHS

**Adjoint of a square matrix**

**Definition** Let A = (aij) be a square matrix. Let Aij be the cofactor of aij in detA. The **adjoint** of A, denoted by Adj A, is defined as (Aij)T.

**Theorem2.4** Let A be a square matrix of order n. then A. (Adj A) = (Adj A).A = In.

**»** the i,j th element of A.(Adj A) is ai1A1j+ai2AI2+…+ainAnj which equals 0, if i≠j and equals , if i=j. Hence A. (Adj A) = = In. similarly other part.

**Definition** A square matrix is **singular** if=0 and is **non-singular** if ≠0.

**Definition** A square matrix of order n is **invertible** if there exists a matrix B such that AB= BA = In. B is called an inverse to A. If C be an inverse to A also, then AC = CA = In. using associativity of product of matrices, it is easy to verify that B = C. So inverse of a square matrix , if it exists, is unique. Note also that since AB and BA both are to be defined, A must be a square matrix.

**Theorem2.5** An nxnmatrix A is invertible iff it is non-singular.

**» Necessity** let Anxn be invertible. Then there exists Bnxn such that AB = BA = In. then ===1 so that ≠0.

**Sufficiency** Let≠0. we know that A. (Adj A) = (Adj A).A = In. hence A.= A = In, proving the result.

**Note** Inverse of a matrix can be easily obtained as in here: [..\Documents\x14.mw](../Documents/x14.mw)

**Theorem2.6** If A,B be invertible matrices of the same order, then AB is invertible and (AB)-1 = B-1A-1.

**»** ≠0, hence AB is invertible. Using associativity, (AB)(B-1A-1) = In=(B-1A-1)(AB). Hence.

**Theorem2.7** If A be invertible, then A-1 is also invertible and (A-1)-1 = A.

**»**  From AA-1 = A-1A = In, it follows from the definition of inverse that (A-1)-1 = A.

**Theorem2.8** If A be an invertible matrix, then AT is invertible and (AT)-1 = (A-1)T.

**»** AT.(A-1)T = (A-1A)T=InT = In = (AA-1)T = (A-1)T.AT. Hence (AT)-1 = (A-1)T.

**Orthogonal matrix**

**Definition** A square matrix A of order n is **orthogonal** iff AAT = In.

**Theorem2.9** If A is orthogonal , then A is non-singular and =±1.

**»**  implies.

**Theorem2.10** If A be an nxn orthogonal matrix, then ATA = In.

**»** AAT = InAT(AAT) = ATIn(ATA)AT = AT(ATA-In)AT = O(ATA-In)[AT(AT)-1] = O (A is orthogonalA is non-singularAT is non-singularAT is invertible)ATA = In.

**Theorem2.11** If A and B are orthogonal matrices of the same order, then AB is orthogonal.

**»**(AB)(AB)T = (AB)(BTAT) = A(BBT)AT =(AIn­)AT = AAT = In.

**Theorem2.12** If A is orthogonal, A-1is orthogonal.

**»** (A-1)(A-1)T=(A-1)(AT)-1= (ATA)-1 = I­n-1 = In.

**Note** : If A be an orthogonal matrix, AT = A-1.

**Rank of a matrix**

**Definition** Let A be a non-zero matrix of order mxn. Rank of A is defined to be the greatest positive integer r such that the determinant of the matrix formed by elements of A lying at the intersection of some r rows and some r columns is nonzero. Rank of null matrix is defined to be zero. **NOTE** Rank of a matrix can be obtained as here:[..\Documents\x15.mw](../Documents/x15.mw)

**Note** (1) 0<rank A≤ min{m,n}, for a non-zero matrix A.

(2) for a square matrix A of order n, rankA < n or =n according as A is singular or non-singular.

(3) Rank A = Rank AT.

**Elementary row operations**

An elementary operation on a matrix A over a field F is an operation of the following three types:

* Interchange of two rows(columns) of A
* Multiplication of a row (or column) by a non-zero scalar c F
* Addition of a scalar multiple of one row (or column)to another row(or column)

When applied to rows, elementary operations are called ***elementary row operations***.

**Notation** interchange of i th and j th row will be denoted by Rij. Multiplication of i th row by c will be denoted by cRi. Addition of c times the j th row to the i th row is denoted by Ri+cRj.

**Definition** an mxn matrix B is **row equivalent** to a mxn matrix A over the same field F iff B can be obtained from A by a finite number of successive elementary row operations.

**Note** Since inverse of an elementary row operation is again an elementary row operation, if B is row equivalent to A, then A is also row equivalent to B.

**Definition** an m x n matrix is **row reduced** iff

* The first non-zero element in a non-zero row is 1 and
* each column containing the leading 1of some row has all other elements zero.

**Example2.6**

**Definition** an m x n matrix A is **row reduced echelon matrix** iff

* A is row reduced
* Each zero row comes below each non-zero row and
* If first r rows are non-zero rows of A and if the leading element of row I occurs in column ki, then k1<k2<…<kr.

**Example2.7**

**Algorithm which row-reduces a matrix to echelon form**

**Step 1**  suppose that j1 column is the first column with a nonzero entry. Interchange the rows so that this nonzero entry appears in the first row, that is, so that ≠0

**Step 2** for each i>1, apply the operation Ri→-.

Repeat steps 1 and 2 with the submatrix formed by all the rows excluding the first.

**Theorem2.12** For a given matrix A , a row-reduced echelon matrix B equivalent to A can be found by elementary row operations.

**Example2.8**

**Theorem2.13** If a matrix A is equivalent to a row-reduced enhelon matrix having r non-zero rows, then Rank A = r.

**Example2.9** Find the rank of the matrix A =

**» first method** rank A≥ 1, since = 1≠0. Though det = 0, det≠0. Hence rank A≥ 2. Since

det A= 0, rank A is not equal to 3. hence rank A = 2.

**second method** A . Hence rank A = 2.

**SYSTEM OF LINEAR EQUATIONS**

A system of m linear equation in n unknowns x1,x2,…,xn is of the form

a11x1+a12x2+…+a1nxn = b1

a21x1+a22x2+…+a2nxn = b2

……

am1x1+am2x2+…+amnxn = bm, where aij’s and bi’s are given elements of a field.

An ordered n-tuple (c1,c2,…,cn) is a solution of the system if each equation of the system is satisfied by x1=c1,…,xn = cn. a system of equation is **consistent** if it has a solution; otherwise it is **inconsistent.**

**Matrix representation** Let **A** = (aij)mxn, **X** = (xj)nx1 and **B** = (bi)mx1.then the system can be written as **AX** = **B**. The matrix is called the augmented matrix, denoted by (**A**,**B**).

**Definition** two systems **AX**=**B** and **CX**=**D** are equivalent systems if the augmented matrices (**A**,**B**) and (**C**,**D**) are row equivalent.

**Theorem2.14** if **AX** = **B** and **CX** = **D** are equivalent systems and if (e1,e2,…,en) be a solution of **AX** = **B**, then (e1,e2,…,en) is also a solution of **CX** = **D**. If one of two equivalent systems is inconsistent, then the other is also so.

**Note** Consistency can be visually verified for a system of equations in three variables here: [..\Documents\x9.mw](../Documents/x9.mw)

**Example2.10** Solve, if possible, the system x1+2x2 – x3 = 10, -x1+x2+2x3 = 4, 2x1+x2 – 3x3 = 2.

**»** the augmented matrix . Thus the given system is equivalent to x1+2x2 – x3 = 10, 3x2+x3 = 14, 0 = -4, which is inconsistent. Thus the given system is inconsistent.

**Theorem2.15** a necessary and sufficient condition that a given system of linear equations **AX**=**B** is consistent is that rank **A** = rank(**A**,**B**).

**Exercise** Verify that the system of equation given above is inconsistent.

**Solution of a system of linear equations having same number of variables as that of equations in which coefficient matrix is nonsingular**

**METHOD 1: Cramer’s rule**

Let

a11x1+a12x2+…+a1nxn = b1

a21x1+a22x2+…+a2nxn = b2

………………………………..

an1x1+an2x2+…+annxn = bn

be a system of n linear equations in n unknowns where det A= det(aij)nxn≠0.Then there exists a **unique** solution of the system given by x1 = ,…,xn = , where Ai is the nxn matrix obtained from A by replacing its i th column by the column [b1 b2…bn]T, i = 1,2,…,n.

**»** x1detA =det = det

=det=det A1. Similarly others.

**Example2.11**  let us consider the system x+2y-3z = 1, 2x – y+z = 4, x+3y = 5.

Determinant of the coefficient matrix = = -22≠0. By Cramer’s rule,

x = =2, y==1, z==1.

**METHOD 2: Matrix Inversion method**

Let **A** = (aij)nxn, **X** = [x1,..,xn]T, **B**=[b1,b2,…,bn]T. Then the above system of linear equations can be written as **AX**=**B**,

where det**A** ≠0. Thus **A**-1 exists and **X** = **A**-1**B**.

**Example2.12**  3x+y = 2, 2y+3z = 1, x+2z = 3.

Let **A** =, **X**=. det**A**≠0. **A**-1 = = . **X**=**A**-1**B**=. Thus the solution is x = 1,y = -1,z = 1.

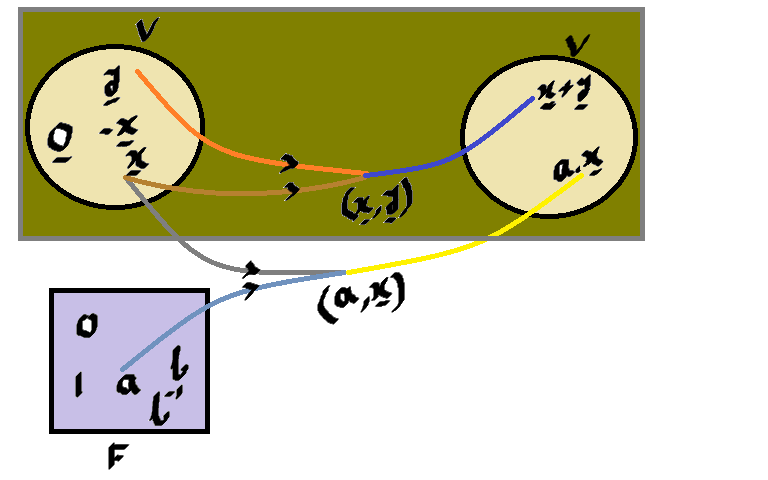
**VECTOR SPACES**

**Definition** Let (F,+,.) be a given field and let V≠. Let 0: VXVV be an **internal** binary operation and \*:**F**XVV be an **external** binary operation satisfying the following axioms:

1. (V,0) is an abelian group: (i)0 is associative, V,V,0=0 = , (iii)V,-)V, 0(-) = (-)0 = , (iv) V,0=0
2. a,bF, ,V,(i) a\*(0) = (a\*)0(a\*), (ii) (a+b)\* = (a\*)0(b\*), (iii) (a.b)\* = a\*(b\*), (iv) 1\* =

Then (V,0,\*) is called a **vector space** over the field (F,+,.).

The elements ,… of V are called **vectors** and the elements a,b,… of F are called **scalars**.



EXTERNAL AND INTERNAL BINARY OPERATIONS IN THE CONTEXT OF VECTOR SPACE

**NOTATION** Though the binary operations ‘0’ and ‘\*’ on V may or may not be same as that of the binary operations ‘+’ and ‘.’ on F, for simplification of notation we shall denote them by same notation ‘+’ and ‘.’. it will be clear from context which operations we are talking of. For example, the expression (a\*0[(a+0.b)\*(0)] in simplified notation becomes (a.)+[(a+0.b).(+)]. Clearly expressions like . or a+ are **meaningless**. Additive and multiplication identities of F will be denoted by 0,1 respectively and will stand for the identity of V.

**Theorem2.16** Let V be a vector space over a field F. Then for all a F,for all V,(1)0. = , (2) a.=,(3) (-1). = -, (4) a. = implies a= 0 or = .

**»** (1) +0. = 0. = (0+0). = (0.)+(0.). Thus ,by right cancellation in the group (V,+), 0.= .

(2) +a. = a.=a.() = (a.+(a. implies ,by right cancellation in the group (V,+), a.=.

(3) +(-1). = 1.+(-1). = [1+(-1)]. = 0. = = (-1).+ [ since (V,+) is abelian]. Hence (-1). = -.

(4) if a≠0,a. = , then = 1. = (a-1.a). = a-1.(a.) = a-1.=, by (2).

**Example2.13** in high school geometry, a vector in space is represented by a directed line segment. Two directed line segments of equal length and in the same direction represent the same vector. the sum of two vectors is obtained by parallelogram rule. the elements of R are called scalars. If aR and x is a vector, then ax is a vector parallel to x whose magnitude is changed by a factor of ; negative a means the reversal of direction. It can be verified that the set of all such vectors form a vector space over R.

**Example2.14** Fmxn,the set of all matrices of size mxn with entries from F is a vector space over F under the usual addition and scalar multiplication of matrices. In particular, Fnx1, the set of all column vectors of length n, is a vector space over F, denoted by Fn. in particular, F may be taken as R or C.

**Example2.15** Let F be a field and K be a subfield of F. Then F is a vector space over the field K under the usual addition and multiplication of F, that is, for aK and F, the scalar multiplication a. is the multiplication of a and in F. Thus C can be considered as a vector space over R(or over Q) and R can be considered as a vector space over Q. Note that Q is **not** a vector space over R, since for scalar R and vector 1Q, .1Q.

**Example2.16** Let V = R+, the set of all positive real numbers. Then V is an abelian group with respect to the usual multiplication of real numbers. Let us define scalar multiplication as follows: for V,aR, a. = xa. it can be verified that V, under the above operations, form a vector space. In this vector space, =1.

**PRACTICE SUMS**

1. Let V be a vector space over F. Show that , if for aF and V, a. = , then a = 1 or = .
2. Prove that Q[] = {a+b| a,bQ} forms a vector space over Q under usual addition and scalar multiplication.

**Subspaces**

Let V be a vector space over F. A subset W of V is a **subspace** of V if W itself is a vector space with respect to the addition and scalar multiplication of V. Since every subgroup of a group shares the identity of the group and since W is a subgroup of V under addition, the null vector W.

**Theorem2.17 (Necessary and sufficient condition for subspace of a vectror space**) Let V be a vector space over F. A nonempty subset W of V is a subspace of V iff a+bW,for all a,bF and ,W.

For a vector space V, the whole space V and {} are subspaces of V. A subspace W of V is proper if W≠V and nonzero if W ≠{}.

**Example2.17** Verify which of the following subsets of vector space R3is a subspace of R3:

1. W = {(x,y,z)| x+y+z = 0}
2. W = {(x,y,z)| xy = 0}
3. W = {(x,y,z)| y = x}
4. W = {(x,y,z)| z is an integer}

**»**  (2) (1,0,1) and (0,1,1) W but (1,0,1) + (0,1,1)=(1,1,2)W. Hence **NOT** a subspace.

1. W is **NOT** a subspace since (1,1,1) = ( ,)W.

**SPAN OF A SUBSET OF A VECTOR SPACE**

**Definition** Let S = {1,2,…,n} be a finite subset of a vector space V and a1,a2,…,an F. Then = a11+a22+…+ann is called a linear combination of the set S. If S is an infinite subset of V, a linear combination of a finite subset of S is called a linear combination of S. The span of S, written as [S], is the set of all linear combinations of S. If T is a subset of V such that V = [T], then T is called a **set of generators** of V.

**Example2.18** S = {(1,0,0),(0,1,0),(0,0,1)} is a subset of R3. [S] = {x(1,0,0)+y(0,1,0)+z(0,0,1)| x,y,z} = {(x,y,z)| x,y,zR} = R3.

**Example2.19** Show that in R2, (3,7) [(1,2),(0,1)] but (3,7)[(1,2),(2,4)].

**»** (3,7) [(1,2),(0,1)] since (3,7) = 3(1,2)+1(0,1). If possible, let (3,7)[(1,2),(2,4)]. Then there exists a,bR such that (3,7) = a(1,2)+b(2,4). Then a+2b = 3,a+2b = 7/2, inconsistent system of equations. Hence (3,7)[(1,2),(2,4)].

**Theorem2.18** If S is a nonempty subset of a vector space V, then [S] is the smallest subspace of V containing S.

**Note** [] = {}.

**Example2.20** let 1,2,3 be three elements of a vector space V. Then prove that (1) [{1,2}] = [{1-2,1+2}], (2) [{1,2}] =[{a11,a22}], a1,a2≠0, (3) if 3[{1,2}], then [{1,2,3}] = [{1,2}].

**Example2.21** Find the span in R3 of the set of points lying on (a) the x-axis and y-axis in R3, (b) the z-axis and the xy-plane and (c) x-axis and the plane x+y = 0.

**Theorem2.19** intersection of any collection of subspaces of the same vector space V is a subspace of V.

**Example2.22** Prove that the set of vectors (x1,x2,…,xn) of Rn which satisfies each of the following m equations form a subspace of Rn (aij:

a11x1+a12x2+…+a1nxn = 0

a21x1+a22x2+…+a2nxn = 0

………………………………..

an1x1+an2x2+…+annxn = 0

**Note** union of two subspaces **may not be** a subspace: Let X = [(1,0)] and Y = [(0,1)]. X and Y are subspaces of R2 but XY is not since 1(1,0)+1(0,1) = (1,1) XY.

**Basis and dimension**

A vector space V over a field F is **finite dimensional** if there are finite number of elements 1,2,…,n in V such that V = [{1,2,…,n}]. if no such finite number of elements exist in V, V is called **infinite dimensional**. A finite subset {1,2,…,n} of V is **linearly dependent** if there are scalars a1,a2,…,an, **NOT ALL ZERO**, such that a11+a22+…+ann = . {1,2,…,n} of V is **linearly independent** iff a11+a22+…+ann = ,a1,…,anF implies a1 = … = an=0. An arbitrary subset X(not necessarily finite) of a vector space V is linearly independent if every finite subset of X is linearly independent; on the other hand, if X contains at least one finite linearly dependent subset, then X is linearly dependent. Any subset of V that contains is linearly dependent(since 1.= but 1≠0: 1=0 will mean F ={0}, unacceptable). A set consisting of a non-zero vector is linearly independent. Any subset of a linearly independent set is linearly independent and a superset of linearly dependent set is linearly dependent.

Let V be a vector space over a field F. A subset B of V is a **basis** of V iff (1) V = [B] and (2) B is a linearly independent subset of V. If V is a finite dimensional vector space, it can be proved that any two basis of V contains same number n of elements. N is called dimension of V.

**Note** we can obtain a basis of a subspace generated by given finite number of vectors as seen here: [..\Documents\x13.mw](../Documents/x13.mw)

**Example2.23** show that the set {1,i} is linearly dependent subset of the vector space C over the field C but is linearly independent subset of the vector space C over the field R.

**»** there exists nonzero scalars 1,iC such that 1.+i. =, hence the first part. For real a,b, a.+b. = 0 = 0+i.0 implies a = b = 0, proving second part.

**Example2.24** if {,,} is linearly independent in V, prove that {+,+,+} is linearly independent.

**Theorem2.20** Let V be a vector space over a field F. A finite subset B of V is a basis of V iff every element of V can be expressed as a **unique** linear combination of elements of B.

**» Necessity** Let B = {1,…,n} be a basis of V. Let v = =, ai,biF. Using distributivity of **.** over**+**, we can write = , which because of linear independence of B, implies ai = bi, for all i. hence uniqueness.

**Sufficiency** To prove B is linearly independent. = = implying ai=0, for each i. hence.

**Theorem2.21** A linearly independent subset of a finite dimensional vector space can be extended to form a basis of the vector space.

**Corollary** If V is a vector space of dimension n and if X is a linearly independent subset of V with n elements, then X is a basis of V.

**PRACTICE SUMS**

1. Justify whether true/false: (1) every set of three vectors in R2 is linearly dependent, (2) the set {(1,1,0),(0,1,1),(1,0,-1),(1,1,1)} is linearly dependent and one of the vectors can be expressed as a linear combination of the preceeding vectors.
2. Let S be a finite subset of a vector space V, prove that (1) if S is linearly independent and every proper superset of S in V is linearly dependent, then S is a basis of V, (2) If S spans V and no proper subset of S spans V, then S is a basis for V.
3. Prove that (1) every one dimensional subspace of R3 is a straight line through the origin, (2) every two dimensional subspace of R3 is a plane through the origin. Deduce that the intersection of two distinct planes of R3 through the origin is a straight line through the origin.
4. Let S1 = {(1,2,3),(0,1,2),(3,2,1)} and S2 ={(1,-2,3),(-1,1,-2),(1,-3,4)}, find the dimension and a basis of [S1].

EIGEN VECTOR AND EIGEN VALUE CORRESPONDING TO A SQUARE MATRIX

Let A be an nxn matrix over a field F. A non-zero vector Fn is an **eigen vector** or a characteristic vector of A if there exists a scalar aF such that A = c holds. Thus (A-cIn) = O holds. This is a homogeneous system of n equations in n unknowns. If det(A-cIn) ≠ 0, then by Cramer’s rule, = will be the only solution .Since we are interested in non-zero solution, det(A-cIn)=0 (**2.1**).equation (2.1) is called the **characteristic equation** of A. A root of (2.1) , considered as an equation in a, is called an eigen value of A. We can plot eigenvectors of a given matrix as in here: [..\Documents\x7.mw](../Documents/x7.mw)

**Example2.25** letA =. The characteristic equation is =0, or ,a2-6a-7 = 0.thus eigen values are -1,7. The eigenvector corresponding to the eigenvalue -1 is given by =-1. Thus 2x+3y = 0, 4x+6y = 0. Thus x =-3y/2.hence the eigenvector corresponding to -1 is =, where k≠0. Similarly eigenvector corresponding to eigenvalue 7 can be found.

**Theorem2.22** The eigen values of a diagonal matrix are its diagonal elements.

**Theorem2.23** If c is an eigen value of a nonsingular matrix A, then c-1 is an eigen value of A-1.

**Theorem2.24** If A and P be both nxn matrices and P be non-singular, then A and P-1AP have the same eigen values.

**Theorem2.25** To an eigen vector of A, there corresponds a unique eigen value of A.

**»** if possible, let there be two distinct eigen values c1 and c2 of A corresponding to an eigen vector . Thus A = c1 = c2. hence (c1-c2) = ; but this is a contradiction since a1≠a2 and is non-zero vector. Hence.

**Theorem2.26** To each eigen value of A, there corresponds at least one eigen vector.

**Theorem2.27** Two eigen vectors of A corresponding to two distinct eigen values are linearly independent.

**Theorem2.28 (Cayley Hamilton theorem)**

Every square matrix satisfies its own characteristic equation.

**Example2.26** let A=. Verify that A satisfies its characteristic equation. Hence find A-1.

**»** The characteristic equation is x2 – 7x+7 = 0. Now A2-7A+7**I** =O can be verified by actual calculation. Hence Cayley Hamilton theorem is verified. Hence A=I2. Thus A-1 = =.

**REAL QUADRATIC FORM**

An expression of the form (i,j = 1,2,…,n) where aijare real and aij = aji, is said to be a real quadratic form in n variables x1,x2,…,xn. the matrix notation for the quadratic form is TA, where = T, A = (aij)nxn. A is a real symmetric matrix since aij = aji for all i,j. A is called the matrix associated with the quadratic form.

**Example2.27** x1x2-x2x3 is a real quadratic form in three variables x1,x2,x3. The associated matrix is .

**Definition** A real quadratic form Q=TA is

1. Positive definite if Q>0 for all ≠O
2. Positive semi definiteif Q≥0 for all ≠O
3. Negative definite if Q<0 for all ≠O
4. Negative semidefinite if Q≤0 for all ≠O
5. Indefinite if Q≥0 for some ≠O and Q≤0 for some other ≠O

**Example2.28** consider the quadratic form Q(x1,x2,x3) = x12+2x22+4x32+2x1x2-4x2x3-2x3x1 = (x1+x2-x3)2+(x2-x3)2+2x32≥0 and Q = 0 only when x1+x2-x3= x2-x3 = x3 = 0, that is, when x1=x2=x3 = 0. Thus Q is positive definite.

**Example2.29** Q(x1,x2,x3) = x12+2x22+2x32+2x1x3-4x2x3-2x3x1 = (x1+x2-x3)2+(x2-x3)2≥0 and Q = 0 only when x1+x2-x3= x2-x3=0.Thus Q(0,1,1)=0. Hence Q is semi-definite.

**Example2.30** Q(x1,x2,x3) = x12+x22+2x2x3 = x12+(x2+x3)2-x32. Since Q(1,1,0)>0 and Q(0,-1,1)<0. Thus Q is indefinite.

For a real quadratic form Q=XTAX where A is real symmetric matrix of rank r(≤n), there exists a non-singular matrix P such that PTAP becomes a diagonal matrix of rank r, where 0≤m≤r. thus by a suitable transformation X=PY, where P is nonsingular, the real quadratic form Q transforms to y12+…+ym2-ym+12-…-yr2 where 0≤m≤r≤n. this is called **normal form** of Q.

**Theorem2.29** The integer m which is the number of positive terms in the normal form of a real quadratic form Q, is invariant. Since the rank remains invariant under congruence, the signature of the matrix A, m-(r-m) = 2m-r is invariant.

**Theorem2.30** By the transformation = P , where P is non-singular , the character of a real quadratic form TA regarding positive definiteness etc. remains invariant.

**Theorem2.31** A real quadratic form of rank r and index m is

1. Positive definite, if r = n,m=r
2. Positive semidefinite, if r<n,m= r
3. Negative definite, if r = n,m = 0
4. Negative semidefinite, if r<n,m= 0
5. Indefinite, if r≤n,0<m<r

**Example2.31** Reduce the quadratic form 5x2+y2+14z2-4yz-10zx to its normal form and show that it is positive definite.

**»** The associated symmetric matrix is A=. Let us apply congruent operations on A to reduce it to the normal form.

A. The normal form is x2+y2+z2.the rank of the quadratic form is 3 and its signature is 3. Thus the quadratic form is positive definite.

C:\Program Files\Microsoft Office\MEDIA\CAGCAT10\j0286034.wmf