Linear Algebra

Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

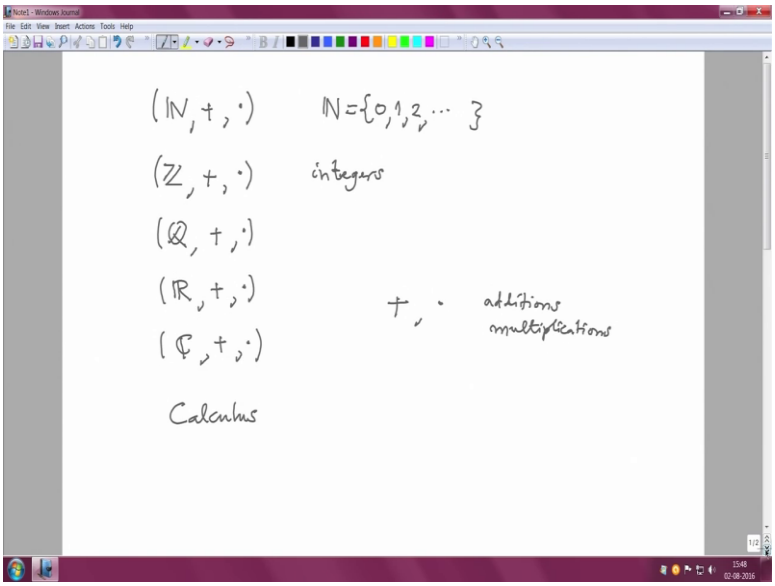
Lecture – 01
Introduction to Algebraic Structures - Rings and Fields

Welcome to this course on Linear Algebra. First I want to give a little introduction; we will be dealing with vector process and linear maps among them. As you are aware the origin of the concept vectors is most notably in physics and clearly described and developed in the geometry of real three, space which I keep calling the universe that we live in. Today in general, we understand a vector is an element of a vector space. In this sense the concept of vectors and vector spaces plays its fundamental role in all branches of mathematics, science as well as engineering.

We will start this course with the abstraction point and conveniently pass on to geometric thinking. More over such geometric perceptions are also beneficial in the frame work of abstract theory. Foundations of geometry are most efficiently formulated in terms of the algebraic structures, inheriting the geometry. It motivates, drawing suitable pictures and the source of inspiration for proving general results. With this in the first half today, I would like to introduce abstract vector spaces, but before that I would like to point out what prerequisites that one will lead for this course? And what exactly we will study in the whole course.

So, first a, prerequisites I will assume that all of you are familiar with set theory, especially concepts of sets, maps and various operations on the sets and subsets. I also will assume that you are familiar with number systems; natural numbers, integers, rational numbers, real numbers, complex numbers and the standard natural operations of addition and multiplication on them.

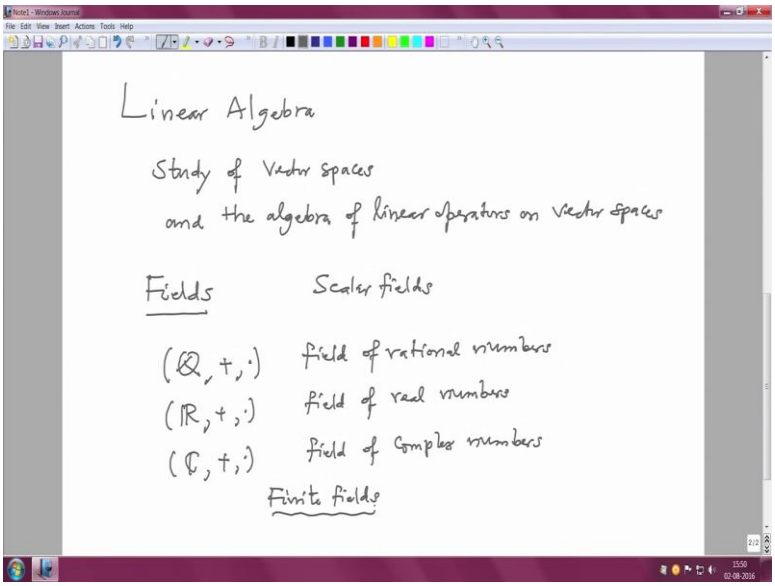
(Refer Slide Time: 02:53)



These systems I will keep denoting by N plus dot, this will be for the set of natural numbers and I will also remind you that in the natural numbers, I would like to add 0 as a natural number. In general song books or some references it is not added usually, but I will insist that 0 is a natural number. Integers I will denote by Z plus dot, they are integers and rational numbers Q plus dot or real numbers R and C plus dot, these are the real numbers and complex number system.

This plus and dot, they are the usual additions and multiplications on these sets and I will assume that all of you are familiar with this number systems and their basic properties. In any case, if some properties are needed specifically I will mention it at the time when you need it and I will also assume that you are familiar with the basic concepts of the calculus.

(Refer Slide Time: 04:30)

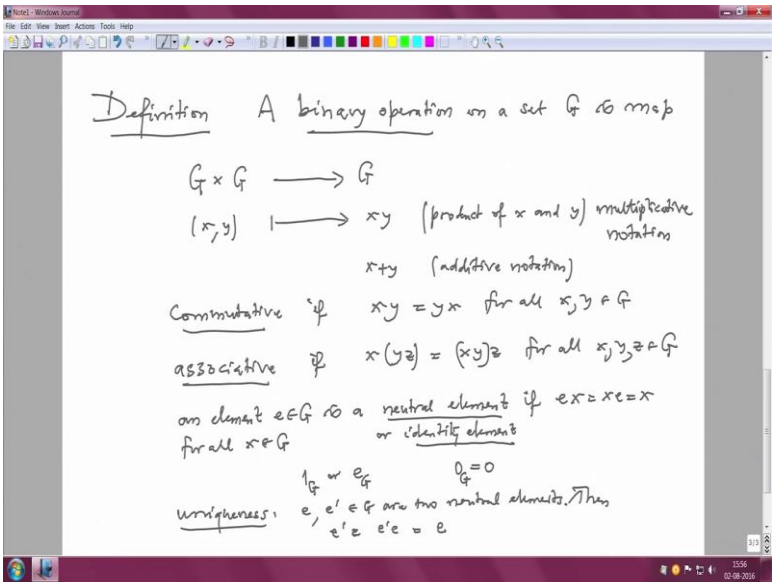


With this, I would like to start linear algebra and say that we are going to study of vector spaces and the algebra of linear operators on vector spaces. Usually one studies vector spaces or real numbers, but I am going to study over arbitrary fields, this is because in the present day applications of linear algebra is more important even for the case of finite fields and to define the first half I will define abstract vector spaces and for that I will need concept of a field. So, I would like to recall, what are fields this fields? These fields, so to define a vector space we need a field, these fields are also called as scalar field of that vector space.

So, already the familiar examples as I mentioned among the number system that you are probably aware that Q plus dot these are my field or real this is called a field of rational numbers and R pus dot, this is field of real numbers. Again, C complex numbers is called field of complex numbers, in addition to these fields I will also would like to recall, what is a finite field? So, to recall this I will go on to recalling the concepts of binary operation first.

So definition; so, the idea of the definition is to make things more general and also developed some notation, which will be using throughout the course, throughout this course.

(Refer Slide Time: 07:05)



So, a binary operation on a set G is a map, from the product say G cross G to G. The image of an order pair x comma y under this map, I will keep denoting this by x, y and maybe call into a product of x, y. Our standard notation sometimes will be the addition notation x plus y, this will called as additive notation and this earlier will be called multiplicative notation. So, such a map is called a binary operation, we will say binary operation is commutative if x times y equal to y times x for all x and y in G. As we are aware that, that the natural addition and multiplication operations on the number systems are commutative.

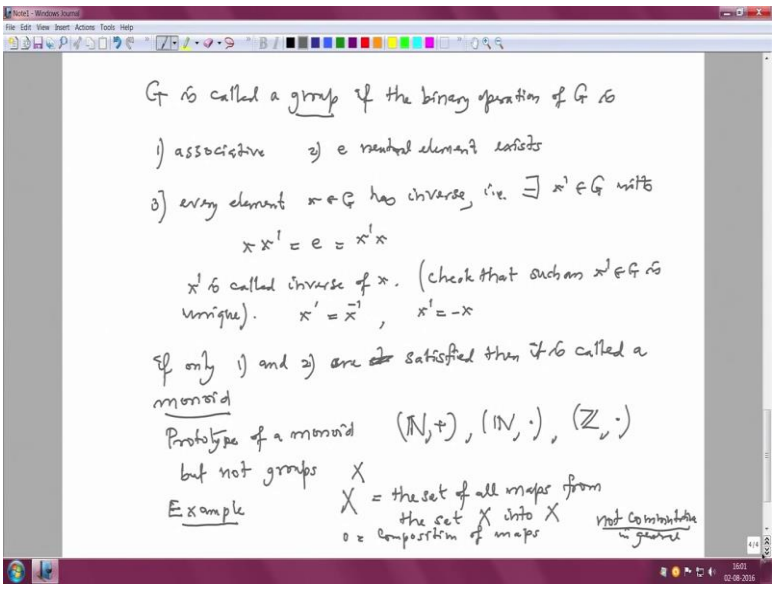
Further, we will say that the operation is associative if x times y, z in bracket is equal to x y times z for all x, y, z in G. So, this means this is a very important property that we need it all the time because it is independent of the bracket we put it and therefore, it is very important for the calculation purpose. Further, we will say that an element e in R is an neutral element, if e times x equals to x times e equal to x for all x G. Then such an element is called neutral element or also it is called identity element. For example, 0 will be additive, identity elements in the set of natural numbers and it is also additive element, additive neutral element in the integers also rational numbers, real numbers complex numbers and so on.

One is a multiplicative neutral element in natural numbers, integers, rational number, real numbers and complex numbers these we have been seen from the school days. Also one,

if I use multiplicative notation usually, I will denote the neutral element here 1, 1 G or e G, in general. In case of multiplicative notation I will denote it by 1 G, in case of additive notation I will denote it by 0 G or simply, when there is no chance of any confusion. Immediately after the definition, I would like you to show you that the neutral element if it exist it as to be unique, uniqueness. For the uniqueness we need to assume that the operation is associative.

Suppose e and e prime are two neutral elements then in G are two neutral elements, then e prime equal to e prime times e which is e prime. On one hand it is e prime because it is e prime, e is a neutral elements on the other hand it is e because e prime is identity, a neutral elements. See, e prime equal to e prime e because e the identity, e the neutral element and because e prime is a neutral element, e prime times e equal to e. So, e equal to e prime. So, that shows that, if neutral elements exist it is unique.

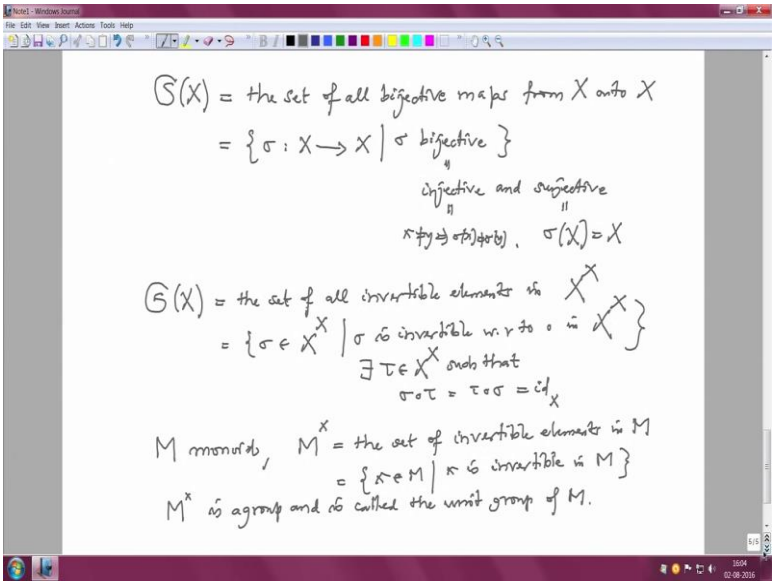
(Refer Slide Time: 13:26)



Next, we will call G a group, G is called a group; if the binary operation of G is associative 2; e exists, neutral element exists and 3; every element of G, x G has inverse; that means, there exist an element x prime in G with x times x prime equal to e also equal to x prime times x. If such a x prime exists then, that elements x prime is called the inverse of G a inverse of x, x prime is called inverse of x and to check that such an x prime is unique. In the multiplicative notation is x prime is usually denoted by x inverse, in the additive notation it is denoted by minus x.

So, G if the binary operation with these three properties is called a group, if only first two properties are satisfied then it is just called a monoid. If only one and two are satisfied then it is called a monoid. A typical example of a monoid prototype of a monoid is N plus N dot or Z dot, these are just monoids and they are no groups. They are monoids, but not groups. Another example, we will read later is the set of maps from X to X; this is the set of all maps from the set X into X and the binary operation is in the composition. Circulate denoted in the composition of maps, this is a monoid and all elements of this monoid are not invertible. These monoid is also not in general commutative, not commutative in general.

(Refer Slide Time: 17:38)



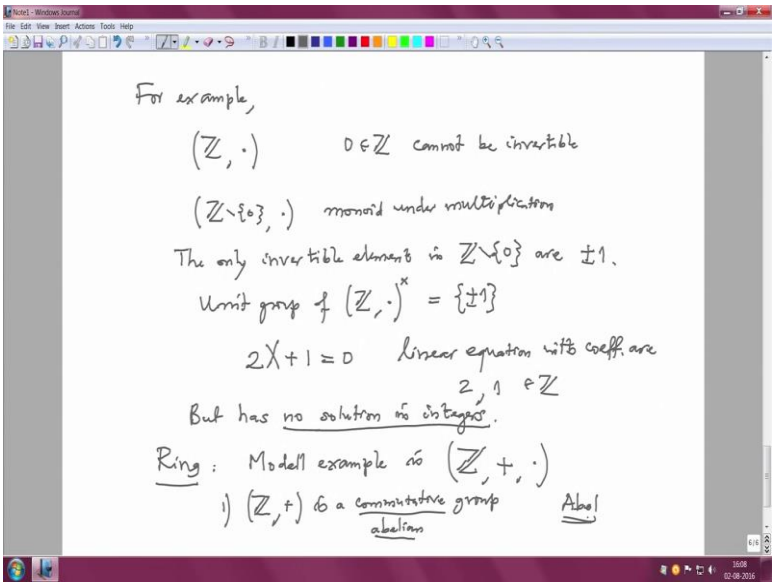
From the last monoid, we can actually, can set a group or we can extract a group namely the set of all not all, but set of all bijective maps on X to X. This is the set of all bijective maps from X to X, from X on to X. In the notation I will write, sigma from X to X, sigma is bijective; bijective means injective and surjective Injective means different elements have different images and surjective means everybody makes is in the image of sigma. So, surjective means image of sigma which is sigma X is X and injective means if x is not equal to y then sigma x is not equal to sigma y.

I will keep using this (Refer Time: 18:47) terms all the time without any reference. So, this is precisely. In fact, S X is precisely all this is the set of all invertible elements in the monoid X power X. So, that is sigma belong to X power X, sigma is invertible with

respect to composition in the X power X. This simply means there exist a tau in X power X, such that sigma of a, sigma compose tau equal to tau compose sigma which is equal to identity map of X. It is well known or you would have seen earlier that such maps are precisely the bijective maps from X to X.

So, I will not get into more into this. Just to comment that if you have a monoid in general, monoid then M cross this is the set of invertible elements in M. This is the notation it is although X is M, such that X is invertible in M. This is a group M cross with the given binary operation of M is a group and this group is called unit group of M. It is very important to on the unit group as you will see in the next example I want to do.

(Refer Slide Time: 21:14)



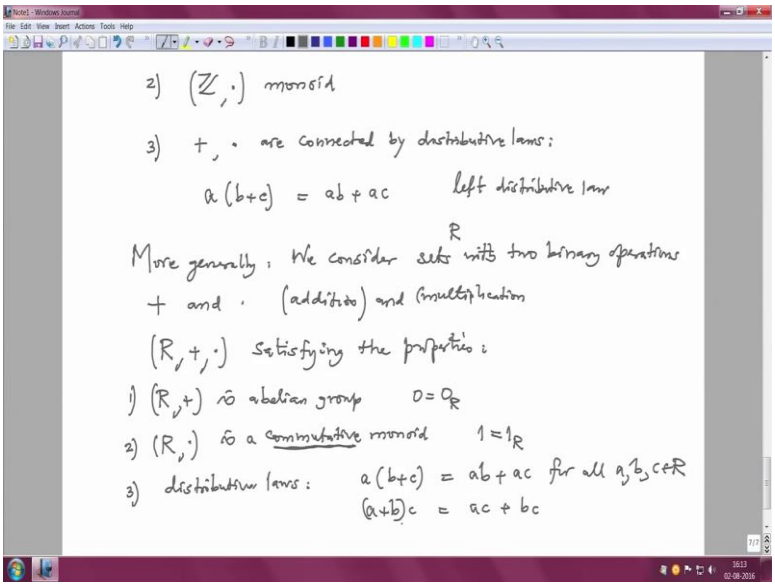
For example, if you take the monoid under multiplication integer, monoid of integers under multiplication this monoid; obviously, you cannot expect the additive identity which we are denoting by 0, this 0 in Z cannot be invertible with respect to multiplication of course.

So, but even if you remove 0, that is Z minus 0 and this is still a monoid under the multiplication and now only invertible elements in this monoid in Z minus 0 are plus minus 1. So, the unit group Z dot, this is precisely only plus minus 1; which is too small compared to this set of integers and that is one of the reason that we cannot solve the equations like, 2 times X plus 1 equal to 0. This is a linear equation with coefficients. So,

this is a linear equation with coefficient; coefficients here are 2 and 1 which are integers, but as no solution in integers.

So, that is a reason that we need a system, we need a field which as maximum number of invertible elements with respect to the field, with respect to the multiplication. So, now I will define the concept of field; or first I will define a concept of a ring and the model example is the set of integers; set of integers as two operations, plus and multiplication and what we are noted so far is 1, Z with respect to the operation plus is a commutative group. Sometimes commutative group is also called Abelian group. This Abelian adjective is attributed to the famous mathematicians Abel.

(Refer Slide Time: 24:56)



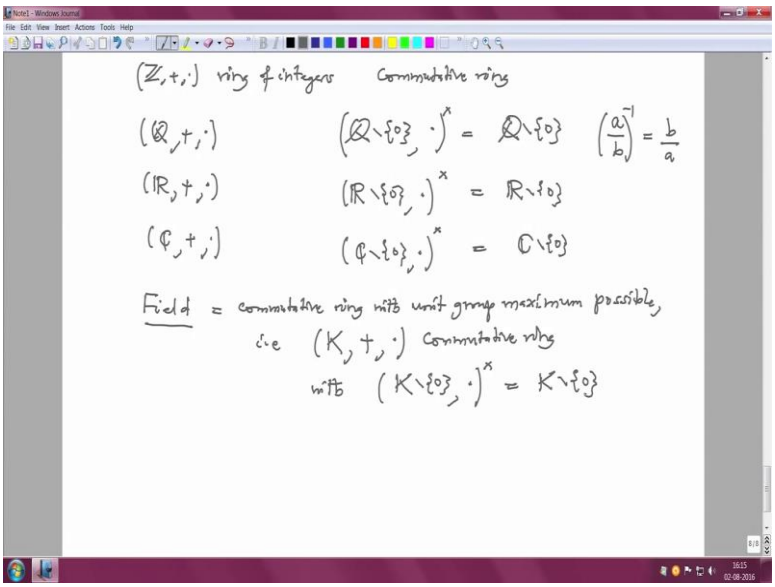
Second property that you have observed in this with respect to multiplication it is a monoid and third one, how this plus and multiplication are connected by so called distributive laws? Namely a times b plus c is same as a b plus ac and because it is commutative I write only one way. So, this is usually called a left distributive law or operation is commutative. So, I do not want to write it the other. So, this should be called left distributive. So, we are interested in sets which as two binary operation. So, more generally, we consider sets with two binary operations. We will denote them by plus and dot called addition and multiplication.

So, we are considering the sets are with two binary operation plus and dot. So, I will denote this as a triplet, satisfying the properties R plus 1 is an Abelian group; that means,

this operation plus is associating it has the neutral element and for every element of R there is a inverse with respect to plus. So, the neutral elements with respect to plus I will keep denoting by 0 when, there are more rings under consideration I will write it 0 R. 2, R with multiplication is a commutative monoid and neutral elements of this will be denoted by 1 or 1 R and remember I am putting this in a definition commutative.

So, I am defining what is called commutative ring? If this was not commutative then one would like to call it a ring in general, but in this course we will never deal with non commutative rings. We will mostly deal with commutative rings and we deal with it I will remind you that now we are considering a non commutative ring. 3, the plus and dot, additional multiplication are connected by distributive laws; a times b plus c equal to a b plus a c for all a b c in R. Similarly, one should write a plus b times c equal to a c plus b c, but because the operations are commutative in our case it is enough to write only one distributive law.

(Refer Slide Time: 29:25)



So, with this just note that all our standard examples, the model examples is Z plus dot. This is called a ring of integers and Q plus dot, R plus dot, C plus dot this is a commutative ring, ring of integers is a commutative ring. So, all these rational numbers, real numbers, complex numbers with our usual operations of plus and multiplication, they are all commutative rings, but they are more than commutative rings namely; if I

take the unit group of the multiplicative monoid of cube; obviously, we will have to omit 0 because we have no chance that 0 is invertible with respect to multiplication.

So, the unit group of rational numbers is all nonzero rational numbers. So, if you have a rational number a by b or basically the inverse of a by b with respect to multiplication will be b by a and we need nonzero rings because a as to be nonzero to come in the denominator therefore, you need a nonzero rings.

Similarly, for real numbers the younitu need group of nonzero real numbers is precisely all of them, all nonzero real numbers. Similarly for complex numbers, so these are called fields. So, field is by definition, it is a commutative ring with unit group maximum possible. That is field is a triplet k plus dot. So, it Is a commutative ring with the unit group of the multiplicative monoid after omitting 0, this is everybody or nonzero elements, so all nonzero elements in a field as inverses.

We will continue after the break.