Discrete Mathematical Structures

Dr. Kamala Krithivasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

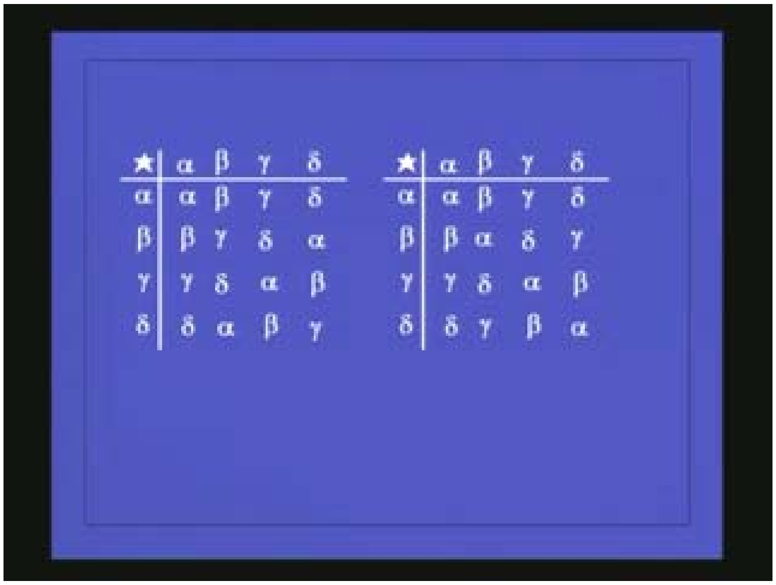
Lecture # 37

Algebras (Contd…)

In the last lecture we saw about groups. We also saw what is a subgroup and under what conditions a subset of a set under a particular binary operation can be called a subgroup. We saw that it is enough if we check for the closure property. So once the closure property is satisfied the other axioms will be automatically satisfied, that is what we saw in the last lecture. We also saw what is meant by an Abelian group.

A group has to satisfy four properties; the closure property, the associative property, existence of an identity and for each element you should have an inverse element. These are the four conditions for a group. Now, if in addition the commutative property is also satisfied then the group is called an Abelian group or a commutative group. So usually we denote a group by the underlying set under operation star. So if this binary operation satisfies the commutative property also then it is called an Abelian group. We also saw that there can be only one non isomorphic group of order two but when you consider four there are two non isomorphic groups and they are given by these two tables.

(Refer Slide Time: 02.54)



★	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ

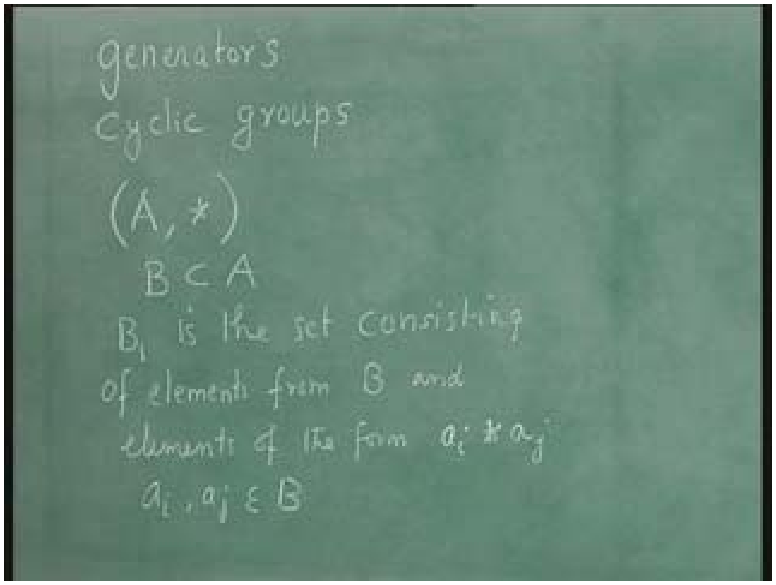
★	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	α	β
δ	δ	γ	β	α

For two the table will be like this; a b a b then a is the identity element so the table will be like this. For three the table will be like this; a b c and a b c where a is the identity element. Now you can see that here a is its own inverse and b is its own inverse, here a is its own inverse and b is the inverse of c and c is the inverse of b in this table. Not only that you see that these tables are symmetric, if we look it as a matrix it is symmetric about the diagonal so they are commutative groups. If it is symmetric about the diagonal it is a commutative group.

You can very easily see that if you look at groups of order four there are two non isomorphic groups. In this one alpha is the identity element and gamma is its own inverse, beta is the inverse of delta and delta is the inverse of beta. In this table alpha is its own inverse it is the identity element, beta also is its own inverse, gamma also is its own inverse and delta also is its own inverse, that is why you are having alpha, alpha, alpha in the diagonal.

Now you look at the diagonal and you see that it is these matrices are symmetric about the diagonal and so again these two groups are commutative groups or Abelian groups. We have also seen an example of a non commutative group by taking non singular 2 by 2 matrices in the last class which is an example of a non commutative group under matrix multiplication. Now, let us see what generators of a group are and what cyclic groups are. Take a group with a set A and an operation (A, star) and consider a subset B of A. Let B_1 be the set consisting of elements from B and elements of the form a i star a j where a i a j belong to B. Consider a subset B of A and then take the set B_1 which consists of B as well as elements obtained by performing the operation on elements from B.

(Refer Slide Time: 07.01)



generators

cyclic groups

$(A, *)$

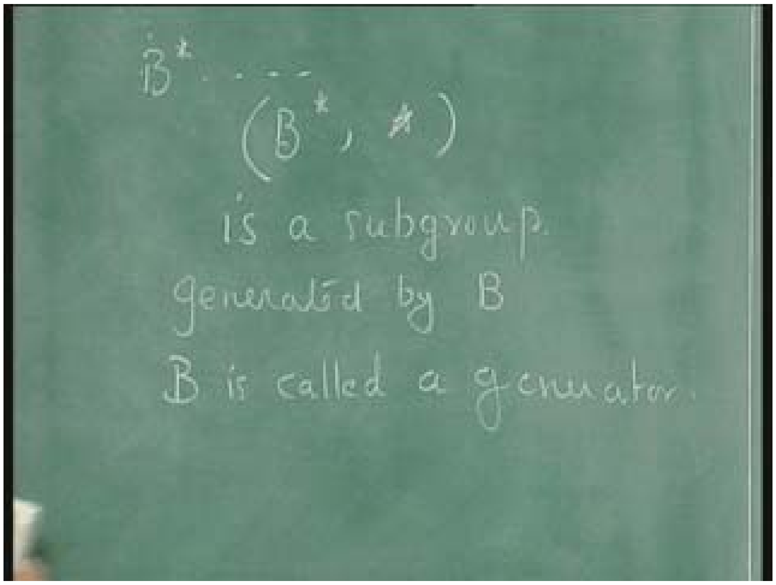
$B \subset A$

B_1 is the set consisting of elements from B and elements of the from $a_i * a_j$

$a_i , a_j \in B$

Take B_1 and perform the set B_2 like this, construct the set B_2 from B_1 and B_3 from B_2 and so on. B power star is the union of all or in the end you get B power star. B power star is the union of all these things so you consider (B power star, star). B power star is a closed set, it is closed under this operation. Now you must also consider that B should also contain the identity element then (B power star, star) is a subgroup and that is generated by B. B contains the identity element of (A, star) also then (B power star, star) is closed so because it is closed you get it is a subgroup generated by B. For example B is called a generator.

(Refer Slide Time: 08.58)



$B^* \ldots$

$(B^*, *)$

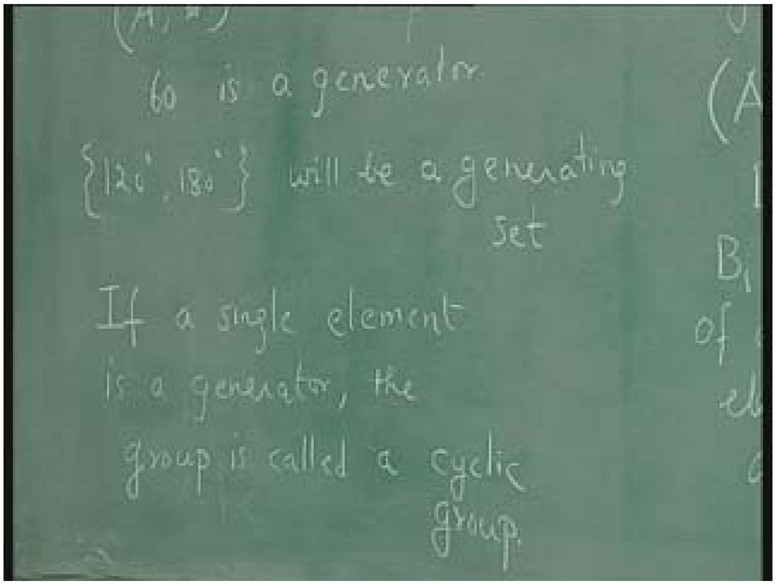
is a subgroup.

generated by B

B is called a generator.

Look at this example of rotations about a plane; the set A is taken as a set of rotations 0 degree, 60 degrees, 120 degrees, 180 degrees, 240 degrees, 300 degrees. We have seen that under composition of rotation which is denoted by this symbol this is a group. And you can see that 60 is a generator for this because when you combine 60 with 60 you get 120 and with that you combine 60 you get 180 and so on so 60 is the generator for this. Similarly, the set 120 and 180 will be a will be a generating set, 120 alone is not a generator because with 120 if you have 120 you can have 240 and 0 and you will not able to get 60, 180 and 300. So this is a generator for this group and this combines it as a generating set for the group A star. Now if you have a single element as a generator the group is called a cyclic group.

(Refer Slide Time: 11.16)



(A, *)

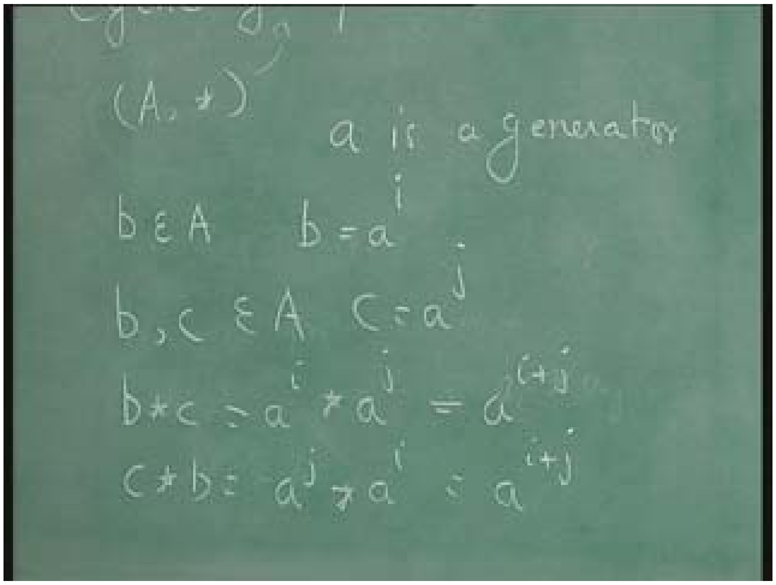
60 is a generator

{120°, 180°} will be a generating set

If a single element is a generator, the group is called a cyclic group.

Now, for example, this is a cyclic group and 60 degrees is a generator for this. so in a cyclic group suppose I have a group A star and a generator then if you take any element b belonging to A then b will be of the form a power I, that is for some i b you can express as a power i because a, a squared, a cubed everything belongs to the set A so if you take any element b you can write b as a power i. And because of this property what do you get? If you take two elements b and c belonging to A probably you can write b as b equals a power i and c you can write as a power j, any element you can write in this form. So what can you say about B power star c? Here B power star c will be a power i star a power j and you can write that as a power i plus j. And that is the same as if you take c star b that is a power j star a power i equals a power i plus j.

(Refer Slide Time: 13.03)



$(A, *)$

a is a generator

$b \in A \quad b = a^i$

$b, c \in A \quad c = a^j$

$b * c = a^i * a^j = a^{i+j}$

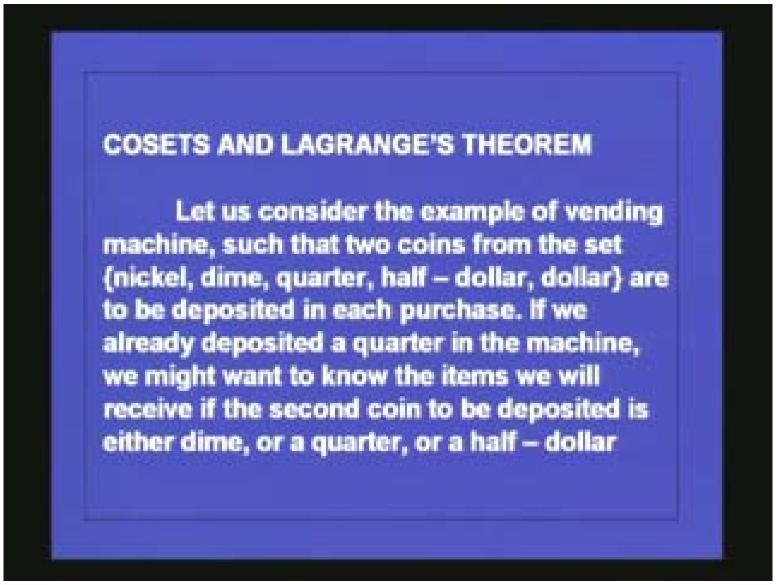
$c * b = a^j * a^i = a^{i+j}$

If you take any two element B power star c equals c star b you get this result. That is, the group is commutative. So any cyclic group is commutative but it is not the other way round that any commutative group need not be cyclic. So look at these two tables what is alpha? Alpha is the identity element. Take beta, what is beta squared? Beta squared is gamma and what is beta cubed? Beta cubed is beta squared into beta that is gamma into beta delta, what is beta power 4? That is beta cubed into beta, beta cubed is delta so beta cubed into beta will be alpha. So from beta you are able to get all the elements. When you just take beta it is beta, beta squared will be or beta into beta will be gamma, beta cubed will be delta and beta power 4 will be alpha. So beta is a generator for this group, so this is an example of cyclic group and you can very easily see that it is also commutative.

Look at this, this is commutative group it is an Abelian group but does it have a generator? Take beta can it be a generator? Beta squared is alpha, beta cubed is alpha into beta beta, beta power 4 is again alpha and so on. So with beta you will be able to get only beta and alpha you will be not able to get gamma and beta so beta cannot be a generator. Take gamma can it be a generator? Gamma into gamma is alpha, gamma squared is alpha, gamma cubed will be alpha into gamma gamma, gamma power 4 again will be alpha and so on. So with gamma you will able to generate only gamma and alpha, look at these elements alpha gamma gamma alpha, so with gamma you will not be able to generate beta or delta.

Similarly, take delta, delta squared is alpha, delta cubed is delta, delta power 4 is alpha and so on. So look at these four elements alpha, delta, delta, alpha. So with delta you will be able to generate only delta and alpha and not beta and gamma. So none of the three elements beta, gamma, delta can be a generator. So you realize that this is not a cyclic group but is a commutative group. We see that every cyclic group is commutative but it is not necessary that every commutative group should be cyclic this is one reason. Next we shall see what is meant by a coset and what LaGrange’s theorem is. So let us consider what is meant by a coset.

(Refer Slide Time: 16.59)

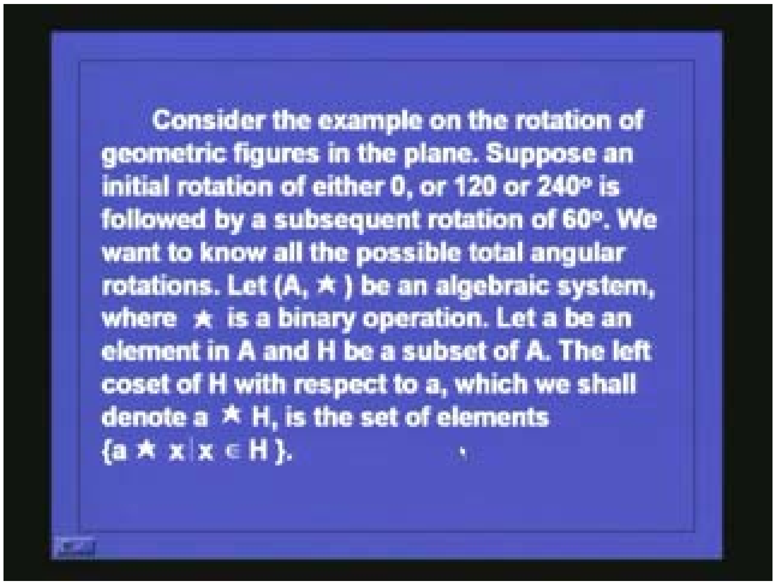


COSETS AND LAGRANGE’S THEOREM

Let us consider the example of vending machine, such that two coins from the set {nickel, dime, quarter, half – dollar, dollar} are to be deposited in each purchase. If we already deposited a quarter in the machine, we might want to know the items we will receive if the second coin to be deposited is either dime, or a quarter, or a half – dollar

Let us consider the example of a vending machine, such that two coins from the set nickel, dime, quarter, half-dollar, dollar are to be deposited in each purchase. If you already deposited in the machine, we might want to know what items we can receive if the second coin to be deposited is either a dime or a quarter or a half-dollar.

(Refer Slide Time: 17.27)



Consider the example on the rotation of geometric figures in the plane. Suppose an initial rotation of either 0, or 120 or 240° is followed by a subsequent rotation of 60°. We want to know all the possible total angular rotations. Let $(A, \star)$ be an algebraic system, where $\star$ is a binary operation. Let a be an element in A and H be a subset of A. The left coset of H with respect to a, which we shall denote $a \star H$, is the set of elements $\{a \star x \mid x \in H\}$.

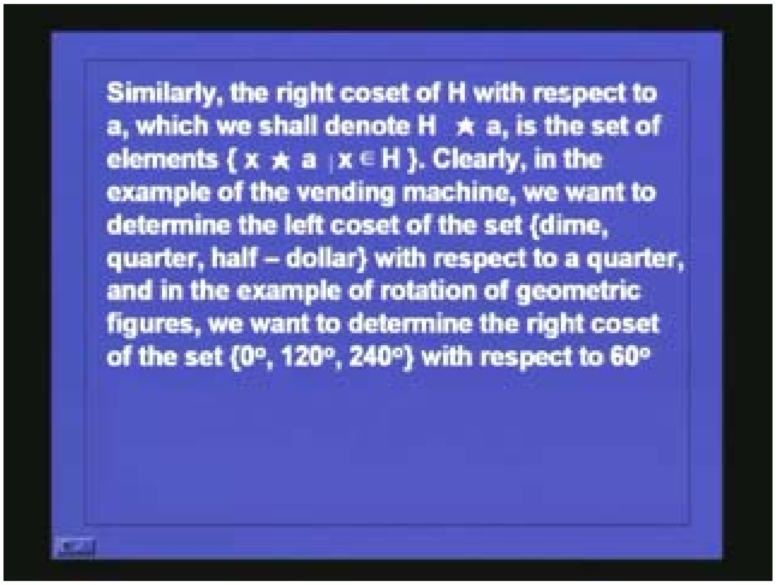
Similarly, you look at the example of a rotation of the geometric figures in the plane. This we have considered again and again. Suppose an initial rotation is either 0 degrees or 120 degrees or 240 degrees afterwards it is followed by a subsequent rotation of 60 degrees. Then what is the result?

With 0 and 60 you get will get 60 with 120 and 60 you will get 180 with 240 and 60 you will get 300. We want to know all the possible total angular rotations obtained like this. So in general what we want is this, putting in a formal manner what we want is this; let (A, star) be an algebraic system where star is a binary operation. Let a be an element of A and H be a subset of A. The left coset of H with respect to a which we shall by denote a star H is a set of elements of form a star x where x belongs to H.

I will repeat this definition;

Let A star be an algebraic system where star is a binary operation and let a be a particular element of A and H be a subset of A. Then the left coset of H with respect to a is defined in this manner, it is defined as a star H and it consists of the set of elements a star x where x belongs to H.

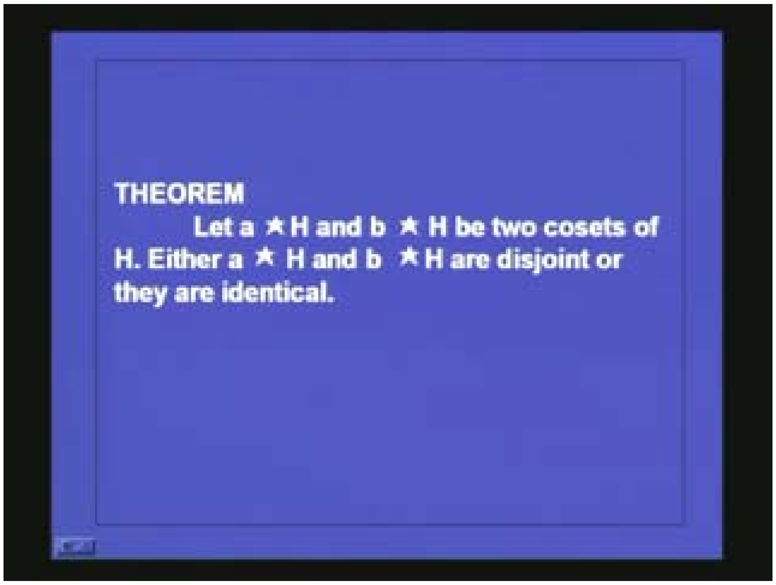
(Refer Slide Time: 19.12)



Similarly, the right coset of H with respect to a, which we shall denote H $\star$ a, is the set of elements $\{ x \star a \mid x \in H \}$. Clearly, in the example of the vending machine, we want to determine the left coset of the set {dime, quarter, half – dollar} with respect to a quarter, and in the example of rotation of geometric figures, we want to determine the right coset of the set {0°, 120°, 240°} with respect to 60°

Similarly, the right coset of H with respect to a is denoted as H star a is the set of elements of the form x star a where x belongs to H. So, if you look at the examples which you considered in the case of vending machine first you deposited a quarter and then you want to know what is the result when you deposited a dime quarter or a half dollar. It is in essence you are finding the left coset of the set dime, quarter, half dollar with respect to a quarter. And the case of the rotations of the geometric plane you have seen, the first initial rotation is 0, 120 or 240 followed by a rotation 60 degrees. That is in essence you want to determine the right coset of the set 0, 120 or 240 with respect to 60 degrees. So this is the essence of right coset and left coset which we have seen now.

(Refer Slide Time: 20.15)



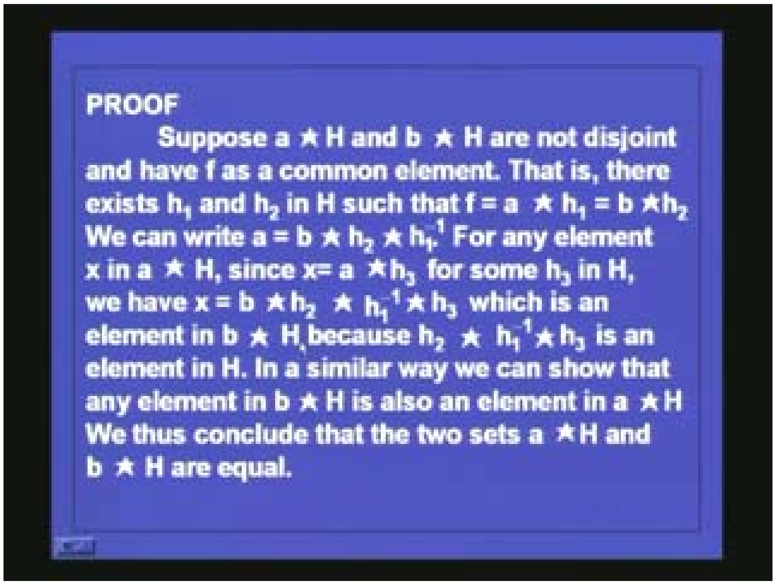
THEOREM

Let $a \star H$ and $b \star H$ be two cosets of H. Either $a \star H$ and $b \star H$ are disjoint or they are identical.

Immediately we get one small result: Let a star H and b star H be two left cosets of H with respect to two elements a and b. Then either a star H and b star H are disjoint or they are identical. First of all we have to specify what H is? What is a? What is b?

That is, you are considering a group A star and a subgroup H star with respect to the same operation and H is contained in A. Now a and b are two elements belonging to A. Now we are considering a star H and b star H. These two are either disjoint or they are identical. How do you go about proving this?

(Refer Slide Time: 24.15)



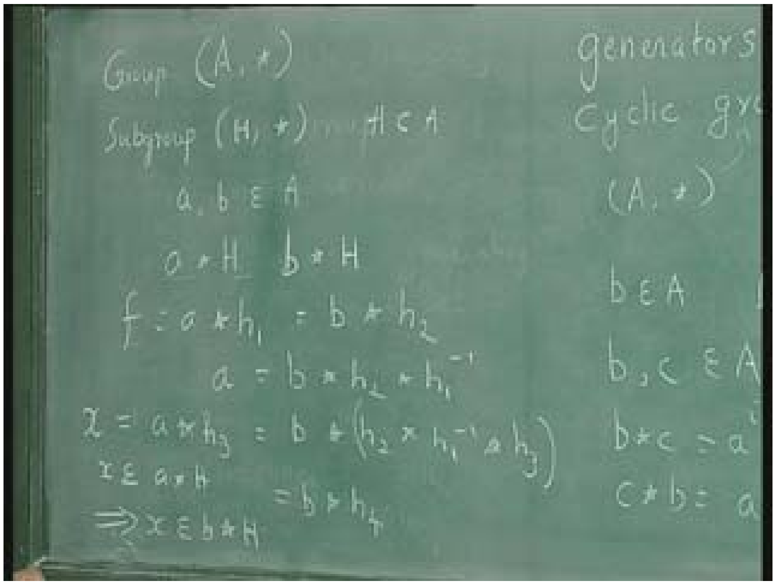
PROOF

Suppose $a \star H$ and $b \star H$ are not disjoint and have f as a common element. That is, there exists h_1 and h_2 in H such that $f = a \star h_1 = b \star h_2$ We can write $a = b \star h_2 \star h_1^{-1}$ For any element x in $a \star H$, since $x= a \star h_3$ for some h_3 in H, we have $x = b \star h_2 \star h_1^{-1} \star h_3$ which is an element in $b \star H$, because $h_2 \star h_1^{-1} \star h_3$ is an element in H. In a similar way we can show that any element in $b \star H$ is also an element in $a \star H$ We thus conclude that the two sets $a \star H$ and $b \star H$ are equal.

Suppose a star H and b star H are not disjoint they have a common element f, in this case you show that a star H and b star H are identical, that is a star H contains an element f if also is in b star H. Therefore there exist h_1 and h_2 in H such that f equals a star h_1 equals b star h_2. So you have f is equal to a star h_1 is equal to b star h_2. So what can you say about a? a is equal to b star h_2 star h_1 inverse because of group property you can have like this, a is this.

Now take some element in a star H it will be of the form a star h_3. Any element here will be of the form a star h_3 and that will be of the form b star (h_2 star h_1 inverse star h_3). Now you look at this because of the associative property I can group like this; h_2 h_1 h_3 are all elements of H so this will be an element of H so this you can write as a b star and some h_4. So if you take an element a star h_3 some element x which belongs to this you can also write x as this so if x belongs to a star H implies s belongs to b star H.

(Refer Slide Time: 24.42)



Group $(A, *)$

Subgroup $(H, *)$ $H \subset A$

$a, b \in A$

$a * H$ $b * H$

$f = a * h_1 = b * h_2$

$a = b * h_2 * h_1^{-1}$

$x = a * h_3 = b * (h_2 * h_1^{-1} * h_3)$

$x \in a * H$ $= b * h_4$

$\Rightarrow x \in b * H$

generators

Cyclic gr

$(A, *)$

$b \in A$

$b, c \in A$

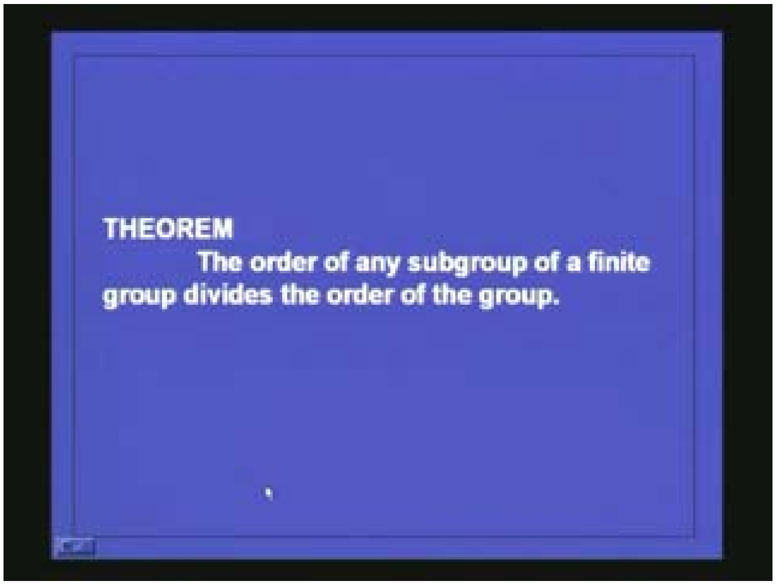
$b * c = a^i$

$c * b = a$

Look at this for any element x in a star h since x equals a star h_3 for some h_3 in H we have x equals b star h_2 star h_1 inverse star h_3 which is an element in b star H because this whole thing h_2 star h_1 inverse h_3 is an element in H. That means x belongs to a star H implies x belongs to b star H. In a similar manner you can prove that if x belongs to b star H, x belongs to a star H, you can prove the other way round or the converse of this that means these two are identical. So we show that if they are not disjoint they are identical. In a similar way we can show that any element in B power star H is also an element in a star H.

Thus we conclude that the two sets a star H and b star H are equal in the case when they are not disjoint there could be disjoint. So either they are disjoint or if they are not disjoint they will be equal they will be identical.

(Refer Slide Time: 25.20)



THEOREM

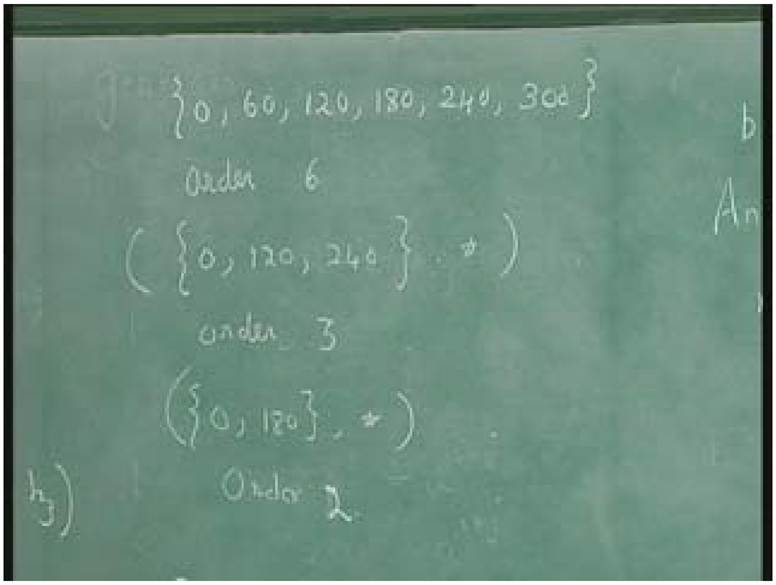
The order of any subgroup of a finite group divides the order of the group.

This gives you the result that the order of any subgroup of a finite group divides the order of the group. Now we are considering only finite groups. Let us take the example of the rotation again. You have 0, 60, 120, 180, 240 and 300, what is the order of the group? Order is a number of elements here, it is 6.

What are the subgroups here?

It is 0, 120, 240 is a subgroup with the same rotation operation, this star is a subgroup. And what is the order of this? The order of this is 3, again 0, 180 with the same operation of rotation is a subgroup and what is order of this? The order is 2 here. So you see that the order of the subgroup divides the order of the group. Here also the order of the subgroup divides the order of the group.

(Refer Slide Time: 26.50)



So, as an example we have verified and we can prove that if you have finite groups the order of any group of a finite group divides the order of the group. This follows from the previous result that if you have H as a subgroup then a star H and b star H are either disjoint or they are identical. Now, take a group A star this is a group, take a subgroup H star, now let the order of this be k then the order of this is l. Now you have to show that l divides k.

If you consider the left cosets of this with respect to each element what can you say about the size of this?

This is a sub set of A because this should be a sub set of A. What can you say about the size of this?

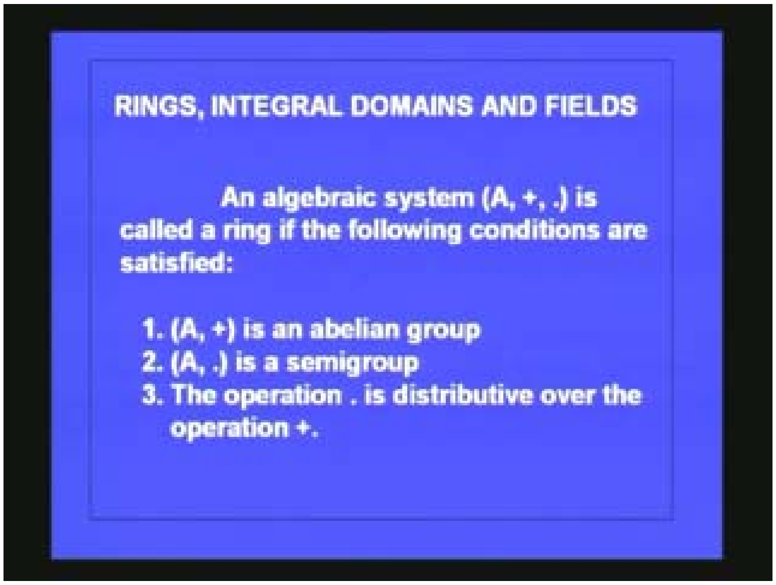
This will be l because you cannot have some a star h_1 equals a star h_2 because in that case because of left cancellation h_1 and h_2 will become equal. So different elements in H when you premultiply by a will give you different elements. So the size of this coset a star H will be l. So you should take any left coset of H the size of that will be just l the same as the size of the subgroup. And we know that from the previous result that the left cosets are either disjoint or identical. So what h does is H partitions A into blocks of size l.

Now one question one may ask is, is every element of A taken care of?

Every element of A will belong to one of these left cosets because H contains the identity element. So if you take any element a star e equals a every element a belonging to a will be in one of the left cosets. So you can see that h partitions A into blocks of size l. Suppose number of such blocks is m then you see that m into l equals k or l divides k, m is a integer because the number of blocks is an integer so you get the result l divides k or the order of a subgroup divides the order of the group if they are all finite. And this example again illustrates this group has order six we have two subgroup one is of order

three and three divides six and you have another subgroup of order two and two divides six.
You can take any other example and verify if you have a group of a finite order and subgroup of that then the order of the subgroup will divide the order of the group. This is known as LaGrange's theorem. So far we have seen few results about groups, there are so many other results about groups. But our idea in this course is to give a brief glimpse what is meant by a group and how the concept will be useful and also a few main important results. Next we shall see what is meant by a ring, an integral domain and a field.

(Refer Slide Time: 32.04)



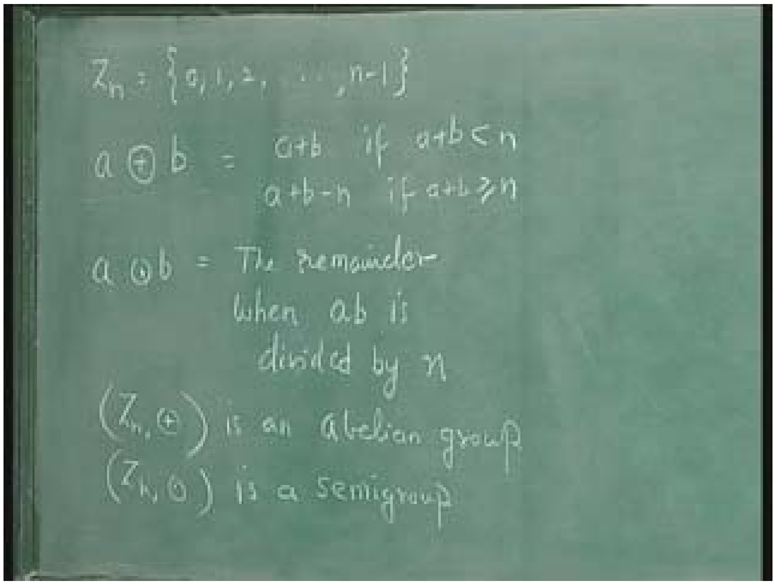
RINGS, INTEGRAL DOMAINS AND FIELDS

An algebraic system (A, +, .) is called a ring if the following conditions are satisfied:

1. (A, +) is an abelian group
2. (A, .) is a semigroup
3. The operation . is distributive over the operation +.

So far we have considered one binary operation, a set with one binary operation per semigroup, monoid and group. Now we will consider two binary operations and see what a ring is. An algebraic system (A, plus). These are binary operations, this is the underlying carrier is called a ring if the following conditions are satisfied. A along with this binary operation is an Abelian group, A along with other binary operation is a semigroup, the operation dot is distributive over the operation plus. If these there conditions are satisfied the system is called the ring. An example of that will be this; consider Z_n which is integers from and a plus b mod and addition equals a plus b; if a plus b is less than n equals a plus b minus n if a plus b is greater than or equal to n that is mod n addition. And a dot b is the remainder when ab is divided by n.

(Refer Slide Time: 35.09)



$Z_n = \{0, 1, 2, \ldots, n-1\}$

$a \oplus b = a+b$ if $a+b < n$
$\quad\quad\quad\; a+b-n$ if $a+b \geq n$

$a \odot b$ = The remainder when ab is divided by n

$(Z_n, \oplus)$ is an abelian group

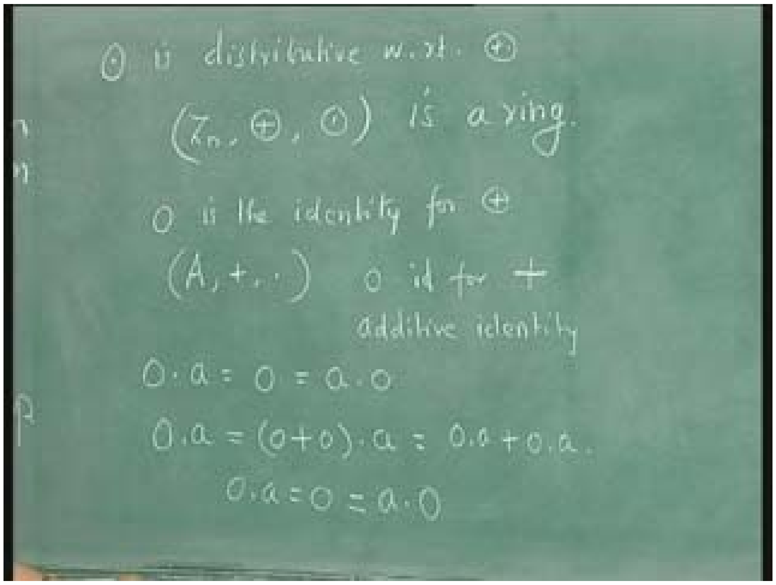
$(Z_n, \odot)$ is a semigroup

If you define these two operations that mod n division this is mod n multiplication and this is mod n addition. We have already seen that this is a group and this operation is also commutative so without loss of generality we see that Z_n dot is an Abelian group. Consider Z_n dot, we can see that with respect to this operation this is closed, if you multiply two and then divide by n you get another element.

The reminder will always be one of the elements between 0 and n minus 1 so it is closed with respect to this mod n multiplication and we can also prove the associative property without much difficulty. So this is a semigroup. Then you can show that this operation is distributive with respect to this. This again also is a routine procedure and without any difficulty we can prove that this is distributive with respect to plus. So, all these three conditions are satisfied so this example Z_n, dot. This is a ring, this gives you an example of a ring. Now, in this case 0 is the identity for this operation. In general, if you take this ring and 0 the identity for plus operation called as the additive identity 0 is the additive identity then you can see that 0 dot a equals 0 equals a dot 0.

How do you get this?
It is 0 dot a equals 0 you can write as 0 plus 0 dot a and because of distributivity this you can write as 0 dot a plus 0 dot a. So 0 dot a is 0 dot a plus 0 dot a that is 0 dot a becomes the additive identity but you know that the additive identity is 0 so 0 dot a equals 0. And similarly you can prove that this is also equal to a dot 0. So the additive identity becomes the 0 element for this operation. We can call this as multiplication and this as addition.

(Refer Slide Time: 37.33)



$\odot$ is distributive w.r.t. $\oplus$

$(Z_n, \oplus, \odot)$ is a ring.

0 is the identity for $\oplus$

$(A, +, \cdot)$ 0 id for $+$

additive identity

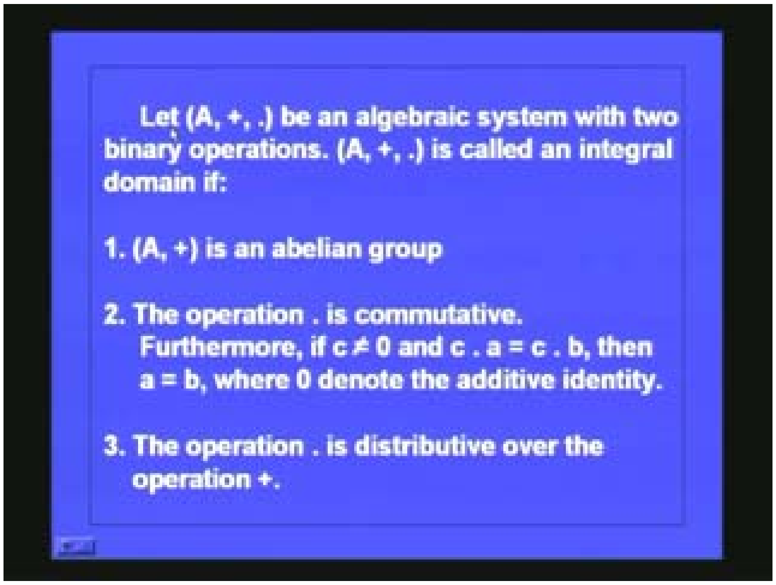
$0 \cdot a = 0 = a \cdot 0$

$0.a = (0+0) \cdot a = 0.0 + 0.a.$

$0.a = 0 = a \cdot 0$

So the additive identity becomes 0 for the multiplication operation. So with this let us see what is meant by an integral domain.

(Refer Slide Time: 37.40)

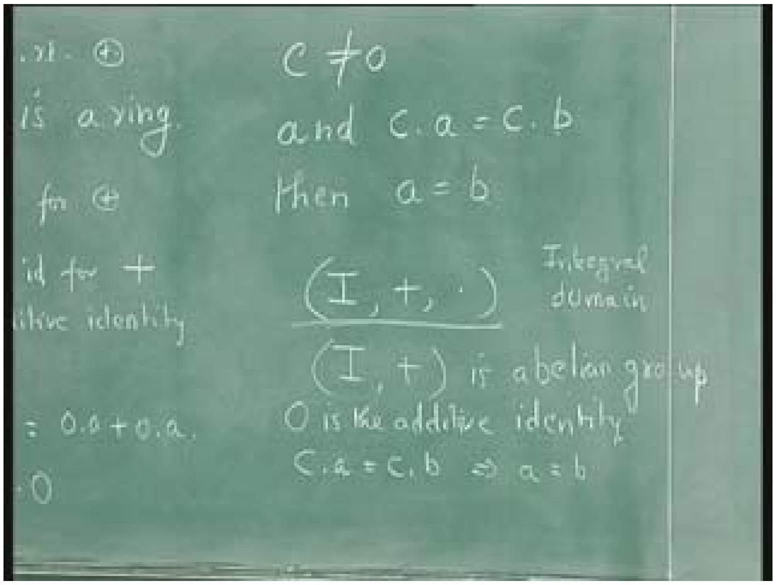


Let (A, +, .) be an algebraic system with two binary operations. (A, +, .) is called an integral domain if:

1. (A, +) is an abelian group
2. The operation . is commutative. Furthermore, if $c \neq 0$ and $c . a = c . b$, then $a = b$, where 0 denote the additive identity.
3. The operation . is distributive over the operation +.

Again you have a set with two operations (A, plus). We call this as addition and multiplication, it is an algebraic system with two operations and this is called an integral domain if the following conditions are satisfied. The first condition is same as for ring (A, plus) is an Abelian group. Then the second condition is dot which is a commutative operation. Furthermore if c is not equal to 0 and c dot a equals c dot b then a equals b. You are allowing left cancellation, (0) is the additive identity, the operation (dot) is distributive over the operation (plus), that is the third condition. An example of an integral domain is a set of integers with (plus) and (into), you know that (I, plus) is an Abelian group where 0 is the additive identity and if c is not 0, c multiplied by a number a and c multiplied by a number b will imply a equals b and this condition will be satisfied and multiplication is distributive with respect to addition. So all the three condition are satisfied therefore this is an example of an integral domain.

(Refer Slide Time: 39.58)



is a ring.

for ⊕

id for +

itive identity

= 0.a + 0.a.

0

$c \neq 0$

and $c.a = c.b$

then $a = b$

$\underline{(I, +, \cdot)}$ Integral domain

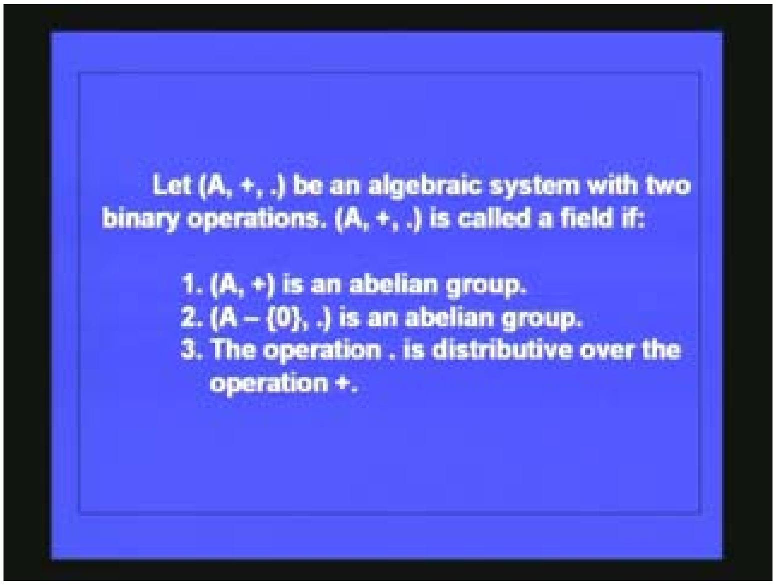
$(I, +)$ is abelian group

0 is the additive identity

$c.a = c.b \Rightarrow a = b$

Next we shall see the definition of a field. What is a field?
Again we have two operations addition and multiplication.

(Refer Slide Time: 40.16)



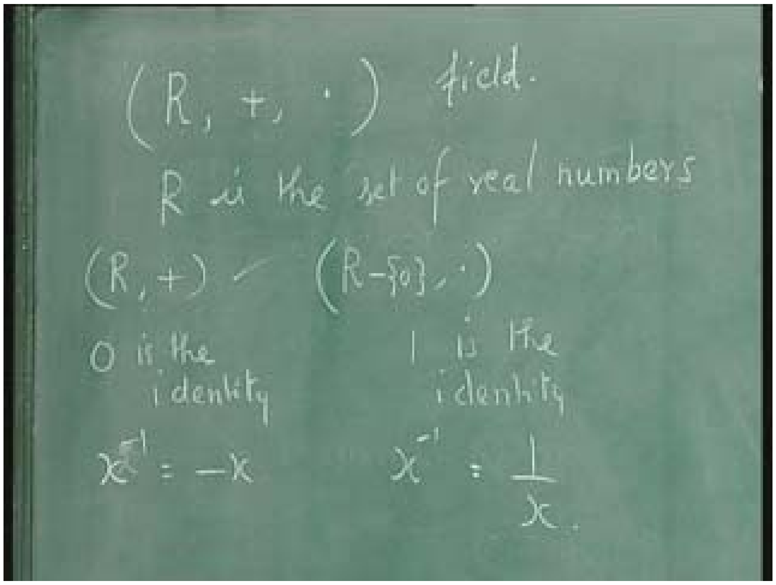
Let (A, +, .) be an algebraic system with two binary operations. (A, +, .) is called a field if:

1. (A, +) is an abelian group.
2. (A – {0}, .) is an abelian group.
3. The operation . is distributive over the operation +.

Let (A, plus, dot) be an algebraic system with two binary operations. This is called a field if (A, plus) is an Abelian group and 0 is the additive identity then (A minus {0}, dot) is an Abelian group the operation dot is distributive over the operation plus. If these three conditions are satisfied it is called a field. Consider a set of real numbers the plus operation and let us say addition and multiplication. R is the set of real numbers. Then you see that R, plus is an Abelian group that condition is satisfied. What is the additive identity? Here 0 is the additive identity and (R minus {0}, dot) will be a group where 1 is the multiplicative identity. Here 0 is the identity and here 1 is the identity. And the inverse of x will be minus x here and here x inverse will be 1 by x so inverse exists. This is again an Abelian group.

Both addition and multiplication are commutative operations so this is an Abelian group, this is an Abelian group and you know that the multiplication is distributive with respect to addition so the third condition is also satisfied so this is an example of a field.

(Refer Slide Time: 42.20)



$(R, +, \cdot)$ field.

R is the set of real numbers

$(R, +)$ ✓ $(R - \{0\}, \cdot)$

0 is the identity

1 is the identity

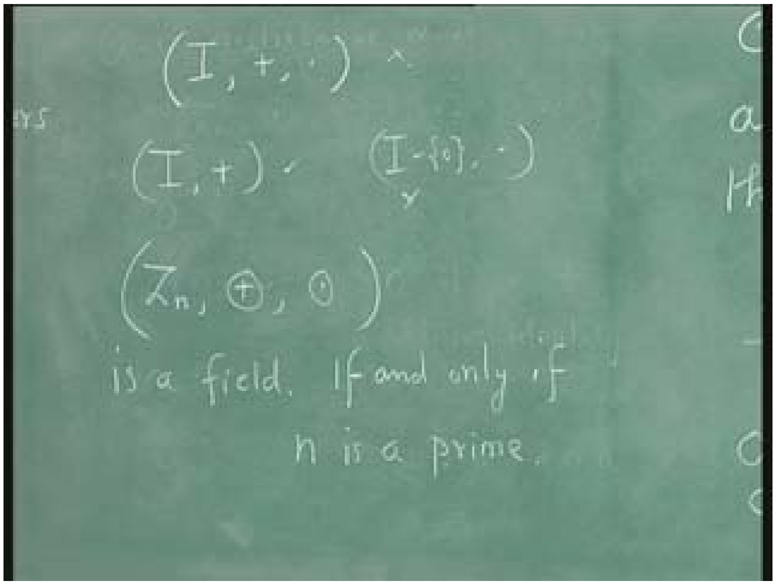
$x^{-1} = -x$

$x^{-1} = \frac{1}{x}$.

And similarly you can see that, take the set of complex numbers, the plus operation, the multiplication operation this is also a field. And if you take the set of rational numbers which usually you denote by (Q, plus, dot) is a field. Q is a set of rational numbers. Now, look at this, is this a group? The set of integers plus dot, is this a field? This is not a field because the first condition I plus is a group is okay but (I minus {0}, dot) is not a group because if you take some element 3 what will be the inverse of 3?
You have to define it has 1 by 3 because 1 is the multiplicativity identity but that is not an integer. So here we cannot prove the existence of inverse so this is not a group. So because of that this is not a field it is an integral domain but not a field.

Similarly, if you consider (Z_n, plus, dot) then this is a field, you can check this, this is a field if and only if n is a prime. If n is a prime certain properties will be evaluated and you will not be able to get a field. So this is a field if and only if n is a prime. So we have seen the definition of ring, integral domain and field and some examples.

(Refer Slide Time: 44.21)



$(I, +, \cdot)$

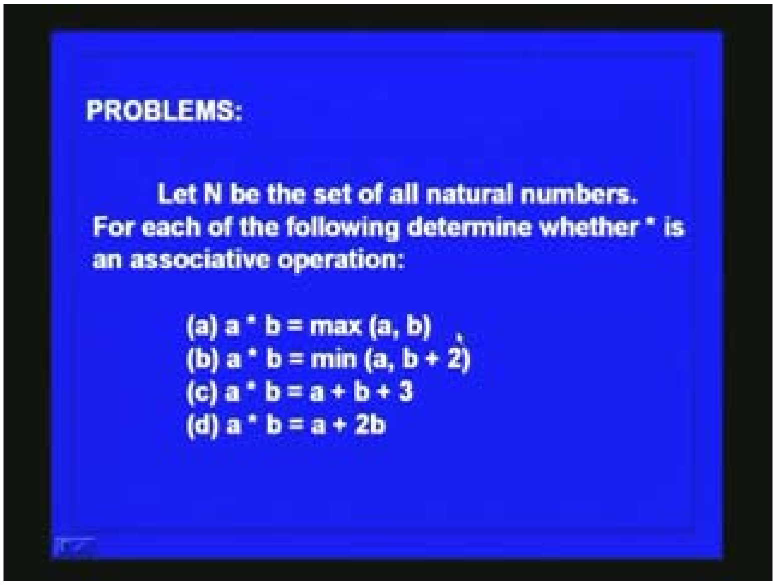
$(I, +)$ ✓ $(I - \{0\}, \cdot)$ ✗

$(Z_n, \oplus, \odot)$

is a field. If and only if n is a prime.

Next we shall consider a few problems. Look at this problem; let N be the set of all natural numbers. For each of the following determine whether star is an associative operation. Take a, a star b is defined as maximum of a and b.

(Refer Slide Time: 44.50)



PROBLEMS:

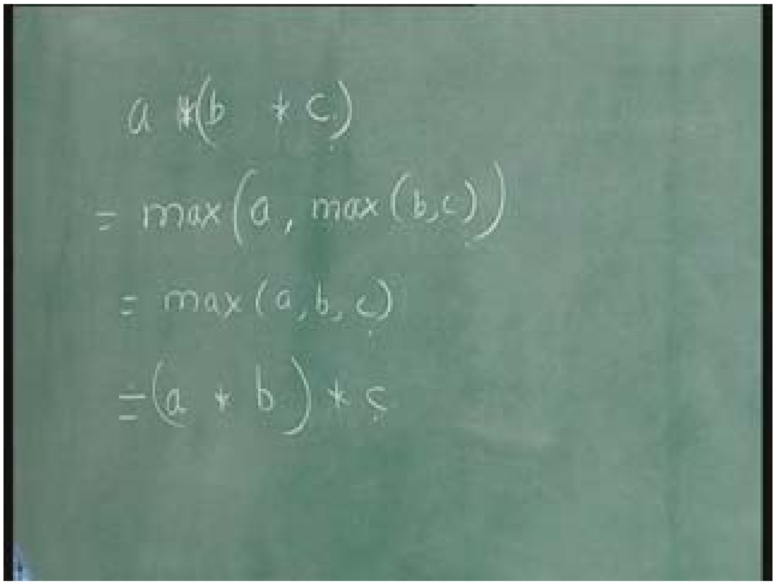
Let N be the set of all natural numbers. For each of the following determine whether * is an associative operation:

(a) a * b = max (a, b)
(b) a * b = min (a, b + 2)
(c) a * b = a + b + 3
(d) a * b = a + 2b

You can very easily see that this is an associative operation because a star B power star c you take this will be the maximum of a, maximum of b, c. In essence you will be really finding the maximum of a, b, c. Similarly, this will be equal to a star B power star c.

Again you will be finding the maximum of these three elements so this is an associative operation.

(Refer Slide Time: 45.26)



$$a * (b * c)$$

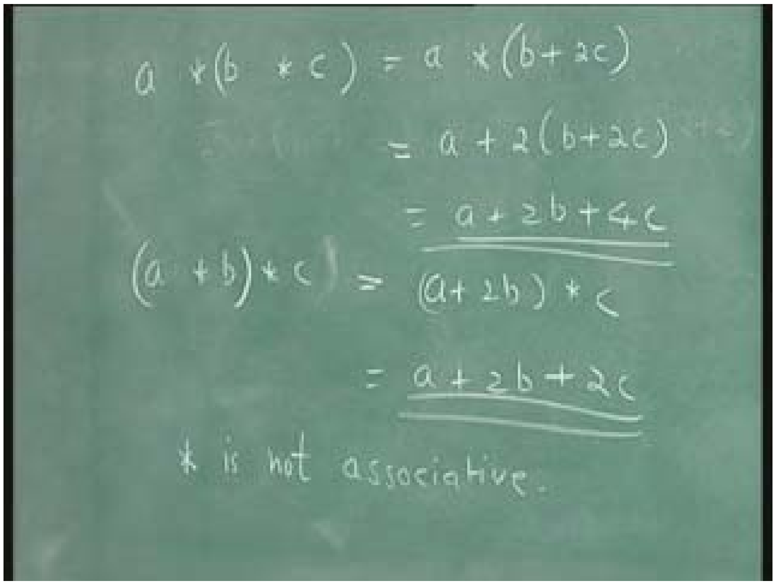
$$= \max(a, \max(b,c))$$

$$= \max(a,b,c)$$

$$= (a * b) * c$$

Take the fourth one a star b is defined as a plus 2b. So what is a star B power star c? That will be a star (b plus 2c) and that will be equal to a plus 2 (b plus 2c) that will be a plus 2b plus 4c. What can you say about (a star b) star c and that is equal to (a plus 2b) star c equals a plus 2b plus 2c. You can see that this is different from this so in this case, star is not associative.

(Refer Slide Time: 46.42)



$$a * (b * c) = a * (b + 2c)$$

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

$$= \underline{\underline{a + 2b + 4c}}$$

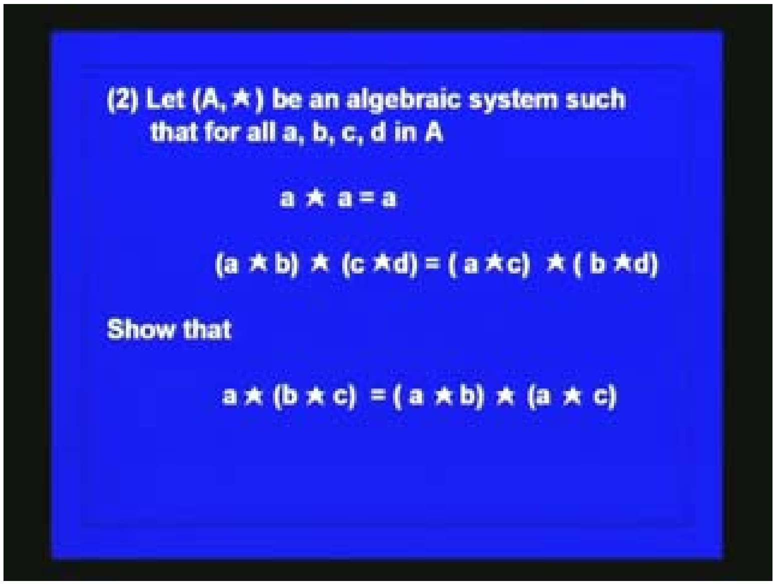
$$(a + b) * c = (a + 2b) * c$$

$$= \underline{\underline{a + 2b + 2c}}$$

$*$ is not associative.

You can try the other two portions. Let us consider one more example; Let (A, star) be an algebraic system such that for all a, b, c, d in A.

(Refer Slide Time: 46.59)



(2) Let $(A, \star)$ be an algebraic system such that for all a, b, c, d in A

$$a \star a = a$$

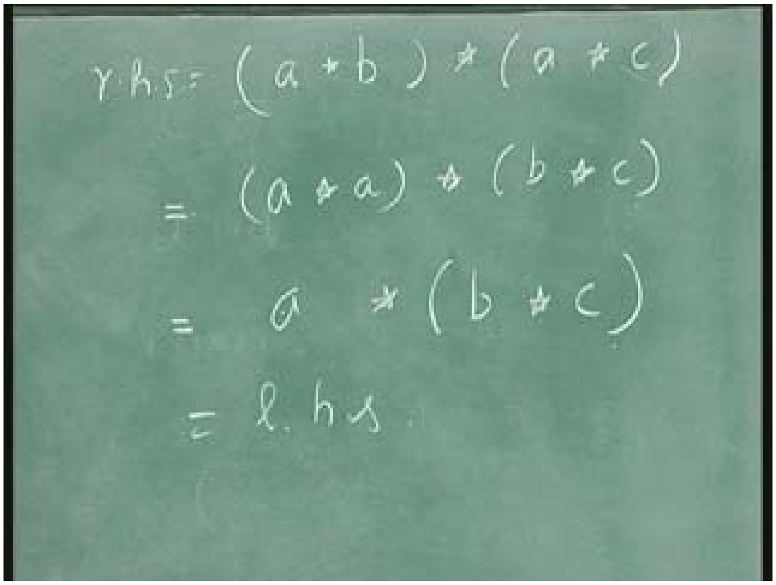
$$(a \star b) \star (c \star d) = (a \star c) \star (b \star d)$$

Show that

$$a \star (b \star c) = (a \star b) \star (a \star c)$$

a star a equals a and (a star b) star (c star d) equals (a star c) star (b star d). Show that a star (b star c) equals (a star b) star (a star c). Let us take the right hand side of the result we want to prove. The right hand side is (a star b) star (a star c). Now use this rule, this rule is (a star b) star (c star d) equals (a star c) (b star d). You use this rule and you will get this is equal to (a star a) star (b star c). But we are also given that a star, a is A so make use of that then you will get a, this is replaced by a star (b star c) which is the left hand side, so we have proved the result.

(Refer Slide Time: 48.12)



$r.h.s = (a \star b) \star (a \star c)$

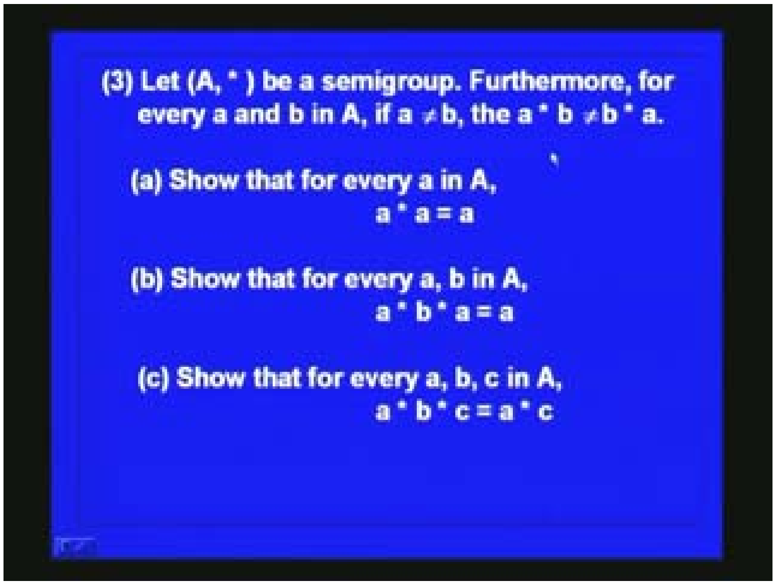
$= (a \star a) \star (b \star c)$

$= a \star (b \star c)$

$= l.h.s.$

Let us consider some more examples; Let (A, power star) be a semigroup. Furthermore for every a and b in A if a is not equal to b then (a power star b) is not equal to (b power star a).

(Refer Slide Time: 48.36)



(3) Let (A, *) be a semigroup. Furthermore, for every a and b in A, if $a \neq b$, the $a * b \neq b * a$.

(a) Show that for every a in A,

$$a * a = a$$

(b) Show that for every a, b in A,

$$a * b * a = a$$

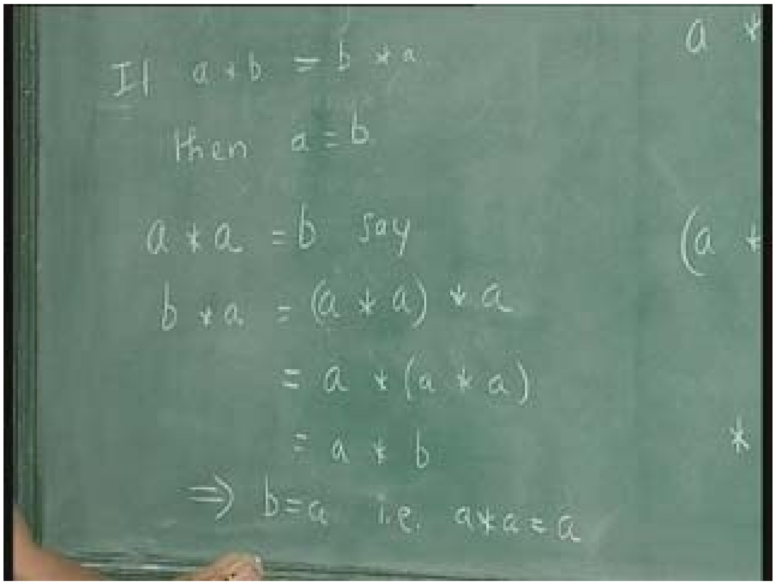
(c) Show that for every a, b, c in A,

$$a * b * c = a * c$$

Or if a power star b equals b power star a that will imply a equals b, so this is a semigroup. For a semigroup the closure and associative property hold and the condition given here is a not equal to b means a star b not equal to b star a. Or you can say it the other way round, if a star b equals b star a then a equals b this is a contrapositive. So three results you have been asked to prove.

Show that for every A in a power star a equals a. So a power star a equals b then what can you say about b power star a? B power star a is a star a star a and because of associtivaity you can write it as a star a star a, that is equal to a star b. So you have b power star a equals a star b which implies b equals a, that is a power star a equals a.

(Refer Slide Time: 50.10)



If $a * b = b * a$

then $a = b$

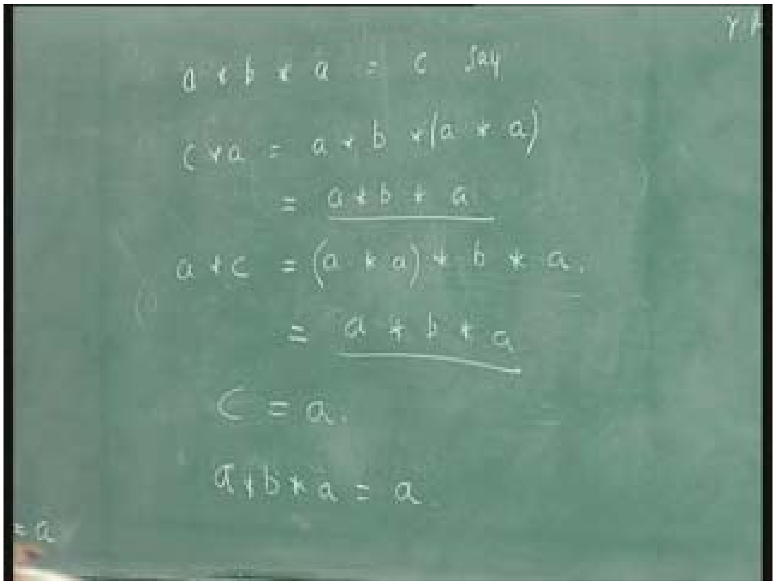
$a * a = b$ say

$$\begin{aligned} b * a &= (a * a) * a \\ &= a * (a * a) \\ &= a * b \end{aligned}$$

$\Rightarrow b = a$ i.e. $a * a = a$

In the similar we can prove two and three also, the second part and the third part. What is the second part?
Show that for every ab in A, a star b star a equals a. Look at a star b star a. Suppose this is c then c star a is a star b star a star a but because of associtivaity you can write like this; a star a is a by the first part so this will be a star b star a. What can you say about a star c?
a star c is a star a star b star a and because of associtivaity you can group like this by the first part a star a is a so a star b star a. These two are equal, c star a equals a star c which implies c equals a. That is a star b star a equals a, this is the second portion.

(Refer Slide Time: 51.43)



$a * b * a = c$ say

$c * a = a * b * (a * a)$

$= \underline{a * b * a}$

$a * c = (a * a) * b * a.$

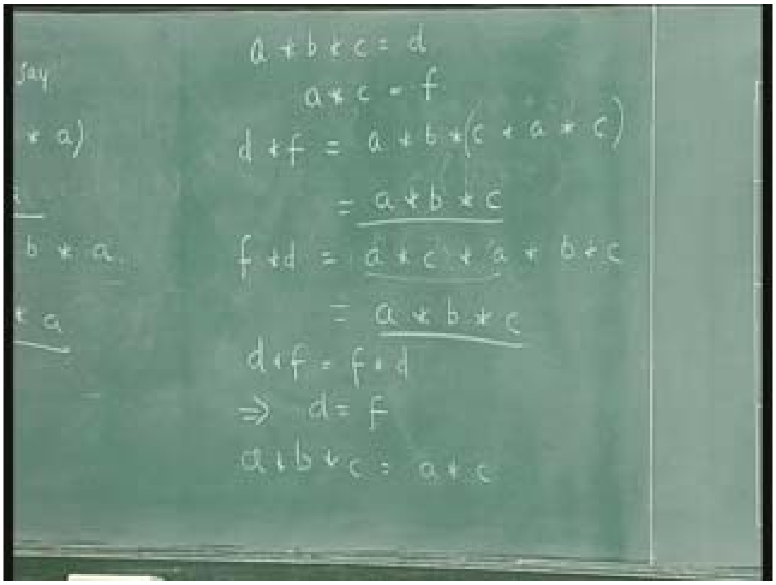
$= \underline{a * b * a}$

$c = a.$

$a * b * a = a$

Let us look at the third portion. Show that for every a, b, c in a star b star c equals a star c. Let a star b power star c equal to some d and a star c is some f then d star f equals a star b star (c star a star c) because of associativity we need not put parenthesis. But you know that c star a star c by the previous part the second part so this will be equal to c. Now what can you say about f star d? That will be a star c star a star b power star c it is like this. And because of associativity you can remove the parenthesis and write like this. Now if you take this alone it is a star c star a. So by the second result it will be a, this portion will be a so you get a star b power star c. So you find that these two are equal, that is d star f equals f star d which implies d equals f. This implies d equals f that is a star b power star c equals a star c.

(Refer Slide Time: 53.34)



$a * b * c = d$

$a * c = f$

$d * f = a * b * (c * a * c)$

$= \underline{a * b * c}$

$f * d = \underline{a * c * a} * b * c$

$= \underline{a * b * c}$

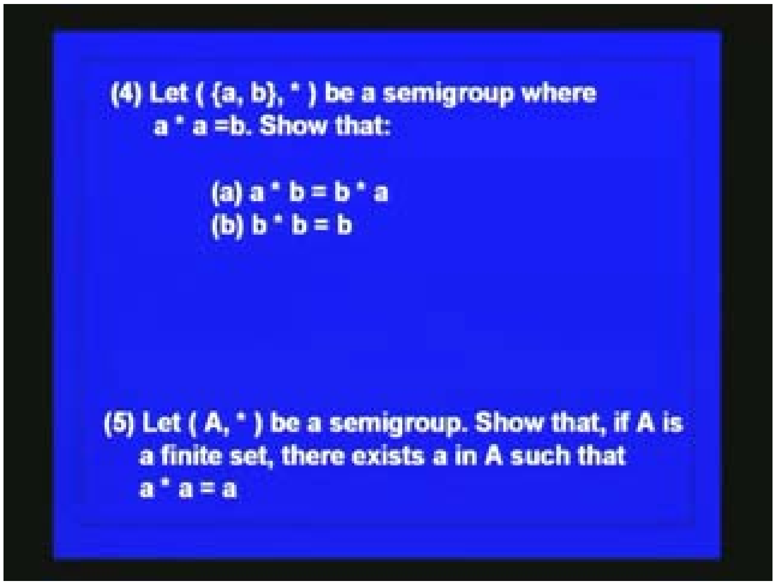
$d * f = f * d$

$\Rightarrow d = f$

$a * b * c = a * c$

So we have proved the third part also. There are some more examples which you can try as exercise. One is, let ab there are only two elements in the set and star is a binary operation.

(Refer Slide Time: 53.51)



(4) Let ({a, b}, *) be a semigroup where $a * a = b$. Show that:

(a) $a * b = b * a$
(b) $b * b = b$

(5) Let (A, *) be a semigroup. Show that, if A is a finite set, there exists a in A such that $a * a = a$

And we also have a power star a equals b. You are asked to show a power star b equals b power star a and you are also asked to show b power star b equals b. This is again a very simple example which will immediately follow by the associative property of the semigroup. Now this a star a is a semigroup, show that if A is a finite set there exists a in A such that a power star a equals a. This is not as simple as this; this is slightly more involved because if you take all the powers of an element that belongs to the semigroup because of the closure property and you are also given that it is a finite set that has to be taken into account.

So in this lecture we have seen LaGrange’s theorem and a few more properties of groups and how to tackle some problems about groups. So this covers the topic algebra and varieties of algebra.