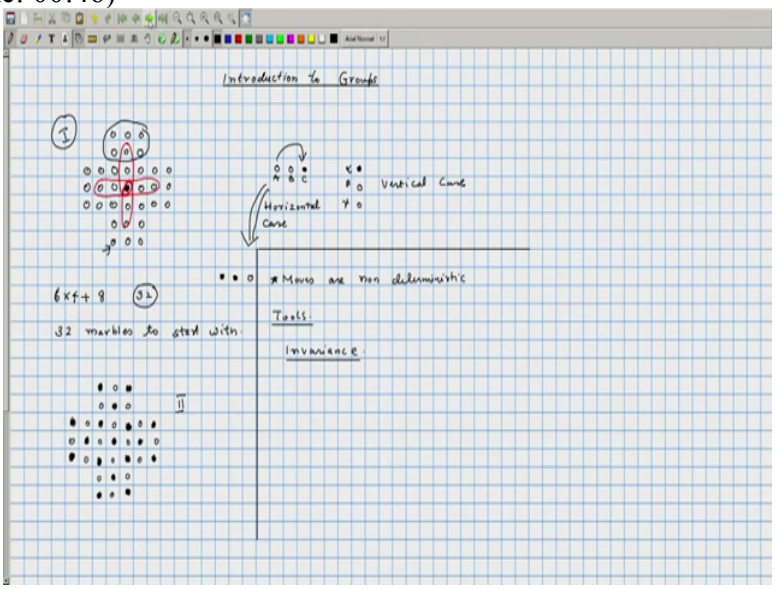
Discreet Mathematics
Professor Benny George
Department of Computer Science and Engineering,
Indian Institute of Technology, Guwahati.
Lecture 37
Introduction to Groups

(Refer Slide Time: 00:46)



We will begin our study of algebraic structures with an introduction to the algebra structure known as groups, we will understand this by solving and we will introduce a notion of groups by solving up puzzle and first describe a game that many of you may be familiar with, so this is known as the peg solitary game.

So this game is a single player game and it is played on a board which looks like this, so you can imagine these holes as places where a marble can be placed. So the initial configuration all the positions will contain marble. So let us say that the darken positions are divide of marbles.

So if I marked it in black that means there is no marble at that particular position. And, so this is the starting configuration there are marbles that all the positions except at the very center of the board, and there certain moves that is available and you can perform these moves in the board and the final configuration is given the question is whether you can reach that particular configuration.

Since we need to describe what the moves are, so center position is the only so the starting the standard starting configuration is 1 where is the center position is divide of any marbles,

so let us look what is a generalized move like so let us say there are 2 positions which are filled with marble and there is a weaken position next to it.

So that these positions are one after another they are adjacent position, they can either be in the horizontal position so this is horizontal case or you can have an arrangement where there is a vertical alignment of 3 positions such that 2 of them are filled with marbles and the third one is empty.

So this is the vertical case, so in this case what you can do is you can allow this is the move is described as the left most marble can jump to the weaken position and if you jump over a marble the middle one is removed, so from this configuration we will end at up at the following configuration wherein you have 2 empty positions and 1 position filled with a marble.

So basically if you name this as A, B and C where A, B are occupied positions and C is an unoccupied position, then the marble from position A can be transferred to the positions C which is empty and in the process you can remove of the marble that is there at position B, in case of vertical alignment also you can do the same thing.

So, if name these positions as alpha, beta and gamma the marble at gamma can jump over the marble at beta to the position alpha and in the process the marble let beta position is removed, now there are other moves as well for example here the move is left to right you can have it from right to left, top to bottom all those are fine.

So, basically any move is o the following kind you need to find 3 positions of the board which are next to each other they should be consecutive positions such that the extreme positions that is not if you find this 3 consecutive positions either horizontal or vertical the middle position should surely contain a marble and one of the sides should be empty, in that case you can transfer the marble to the empty position and remove the other 2 marbles, so that is the move.

The question is if you start with a particular configuration can you reach other configuration, note that any move horizontal or vertical will reduce the number of marbles on the board, so in this starting configuration there are along the arms there 6 so 6 into 4 plus 9 positions out of which 1 is empty so into 8 marbles are present let us 32 marbles are there on the table.

So 32 marbles to start with, and then the question is can you reach a configuration with exactly 1 marble. So you can try this out and may be after it is slightly difficult but you can figure out that there are configure, you can reach a configuration where there is only 1 marble remaining.

So, let me let just describe some configuration which you from which there are no moves. For example, so if you had marbles at the alternate positions let say marbles in the chess board pattern, so suppose after moving some number of marbles around you reach this particular configuration.

Here you can see that there is no further moves possible, so if you call this as first position and this is position number 2, in position number 1 there are many moves for example you can consider these 3 positions and make a move or you can consider these 3 an consider a move or you can consider these 3 or you can consider these.

So many moves are there and after the first move is made there are again many moves that are left so you could choose any of those things and keep on repeatedly doing, suppose we reach the configuration 2 then from there are the no further moves possible and there are undo so that is that will be a positions in which you get stuck.

Also if you have just 1 marble there is no way you can move anything around so that is also a dead end, so question is starting from 1 can you reach a position a configuration precisely 1 marble the answer to this question is as there are you can do that but what we will consider in this lecture is a little is a variant of this in the sense can be reach a configuration where there is only 1 marble but that is at let this corner position.

So, the only marble remaining is appearing at one of the corners is this possible and to this question if we want to list out all the possible moves the first move itself there are 4 possible moves and in between there could be a multiple number of moves so it could be a very large number of moves to explore if you wanted to conclude that there are that it is impossible to reach a particular configuration.

You can model it as a search through the configuration space so with each configuration can be describe by a let us say a bit vector with 33 positions each 33 a bit vector of length 33 tells weather a marble is present at a position or not and from each bit vector you can move to certain other bit vectors you can move from one position to another, if there is a valid move which will take you from one to other.

And then this can be a reformulated as a search problem on a graph but the search space is really huge here so we can not really hope to do a computerized check to figure out whether certain configuration are reachable or not and if the same configuration if it is imagine on the I mean the same game if it is imagine on the larger board with more positions then it is hopelessly intractable.

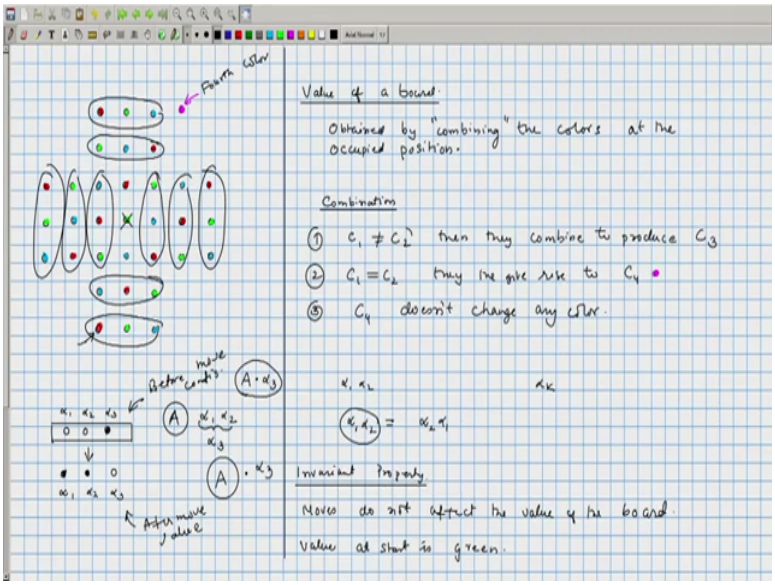
We will see that in some cases we can use some cleaver arguments to say that you cannot reach certain configurations, so we will use some standard tools from computer science while we argue about these the moves are non-deterministic. In the sense we have no control over the choices made by some player while he is playing this particular game.

So in order to argue that none of the sequence is of moves can reach a certain configuration we need to answer about all possible moves, the tools that we will use to solve this the main thing as a this a key thing that is used in many proofs this is called as invariance, so here we have some particular we think of this as an algorithm so somebody some adversary is performing some sequence of operations on some configuration space and each configuration has to follow certain rules it is either the horizontal case or the vertical case.

But we will identify some quantity associated with each configuration such that, that quantity remains in invariance it does not change even after the moves is made. And once we have established the invariant what we can argue is that no matter what are the moves done by the adversary the first configuration and the last configuration whatever are the sequence of steps that take you to the last final configuration.

The invariant must be satisfied and if we can argue that the configuration that we want to end up with does not have the invariant property then we can say that look that is a configuration that is unreachable, so let us identify what is invariant property here.

(Refer Slide Time: 13:14)



So in order to describe the invariance what we will need is the idea of groups, we will not initially formulated in terms of group theory but we will explain it via simpler methods. So let us so what you can do is a following, so look at these positions we going to number this position in a certain way and based on the numbers that we give this positions and the presence or absence of marbles or individual position based on that we will come up with a numerical quantity.

So there are 33 positions of the board so what we will do is we will look at this board configuration and to each positions and the board we will give a certain colour, so this colours, let us called the colours is A, B and C so this positions gets colour A the next one gets B and the next one gets C, and we do this systematically.

So A, B, C this will so this is again going to be A. A, B, C, A, B, C, A, A, B, C this is also going to be an A this is going to an B and these position are going to be the C positions, so we look at the board position and we give colours or we label each of this positions as A, B and C.

Now we are in position to determine the value of the board, so the value of the board is determined by combining the colours given to the positions which have marbles in that, so let us say the positions which do not have marble we can probably cross it out. So initially these positions did not have a marble, and all the other positions contain marble.

So, at any positions the value of the board is obtained by combining the values of the positions the value of the board is determine by combining the colours at the positions were there are marbles. So initially there are 32 such positions they are combined and we get a value.

Now how are these colors combine, so we will follow the simple rule that whenever 2 distinct colours combine you get the third colour, so if the red and the green combined you will get a blue so blue and the red combine you will get a green and so on, so 2 distinct colours when they combine you get the third colour, and if a colour combines with itself you will get a brand new colour.

So there is a fourth colour in the picture lets denote it by pink, so this is the fourth colour. So let us just write our setup so we define what is the value of a board, this is obtain by combining the colours at the occupied positions. So we have defined the value of a board by combining the colours at the occupied positions.

So given any board we know how to compute the value, now this combination means the following if you think of C1 and C2 as a colour and if C1 not equal to C2 then they combine to produce C3 and if the colour is same if C1 is equal to C2 then they give rise to C4. So C4 is a new colour.

Now this combination rule 1 when you think about it this applies only to colours red, green and blue, if it was a fourth colour if it was the pink colour then that colour combines with any colour it does not change anything, so that is third rule C4 does not change any colour, in the sense if you combine a red and the pink what you will get is a red if you combine a green and a pink you will get a pink if you combine a blue and a pink then you will get a pink colour.

And pink and pink when they combine will still get a pink colour. So we have described the rules of combining colours there are 3 colours on the board but when you determine the value we have introduced a fourth colour so 2 colour combines and give rise to the colour which is not present if these 2 colours are red, green and blue.

The fourth colour was used at any time that will not change the colour of anything that it combines with, so now we have define formally what is the value of a board. Now let us look at the initial value of the board, so the way in which this are colours combine does not really matter because all that matter when if you have let us say, so you can convince yourself that

the order of combinations do not really matter, that means weather a red first combines with the blue and then combines with the green or the other way really does not matter.

Because, so let us say we write down these colours C1 so if you arrange them as alpha 1, alpha 2, alpha k these are the colours now at any point alpha 1, alpha 2 same as if you combine alpha 1 and alpha 2 that is the same as combining alpha 2 and alpha 1, so any rearrangement of colours is still ok so any order of combining them will give rise to the same colours.

So for this board what is the initial value of the board, think about it for a few seconds. So we can determine it by looking at the rose looking at this diagram carefully, so if you look at the top most row the red and green combines to give a blue. Blue and blue combines to give a pink, so any 3 of them because all these were occupied positions all these give rise to pink and the pinks when they combine with each other they do not do anything there would not bring in any change, so you going to get a pink by combining this.

And the red and blue where occupied positions where is a green and the center was unoccupied so the total product is going to be just the product of or the total value of the board is going to be the value that you get when you combine a red with a blue and that is going to be a pink, and the other combine and give a pink. Pink and pink combines to give you a pink, so the initial value is going to be pink.

Now here is a crucial observation which is where we use a invariant property moves do not affect the value of the board, so look at the value of a board before and after a move is performed the value remains the same, why it is so because let us look at any move think of it is horizontal, vertical is similar. So if 3 positions, so let us say we denote them by alpha 1, alpha 2 and alpha 3. Two of them are going to be occupied let say the occupied positions is what we call as alpha 1 and alpha 2 and alpha 3 is the unoccupied position.

So this is the unoccupied position and this will change to 2 unoccupied positions and 1 occupied position. The initial value of the board is going to be obtained by looking at the other positions so let us say this is initial board or let say before move configuration, so let us say A denote the remaining of the board and then there are this positions alpha 1 and alpha 2.

The occupied positions inside this they will combine and let us say it will give some value A, when alpha 1 and alpha 2 combine what you will get is clearly alpha 3, so the initial value is A combined with alpha 3 so I will write as A followed by alpha 3 so this is the initial value,

and after the move these 2 positions are unoccupied whereas the other positions remain unchanged.

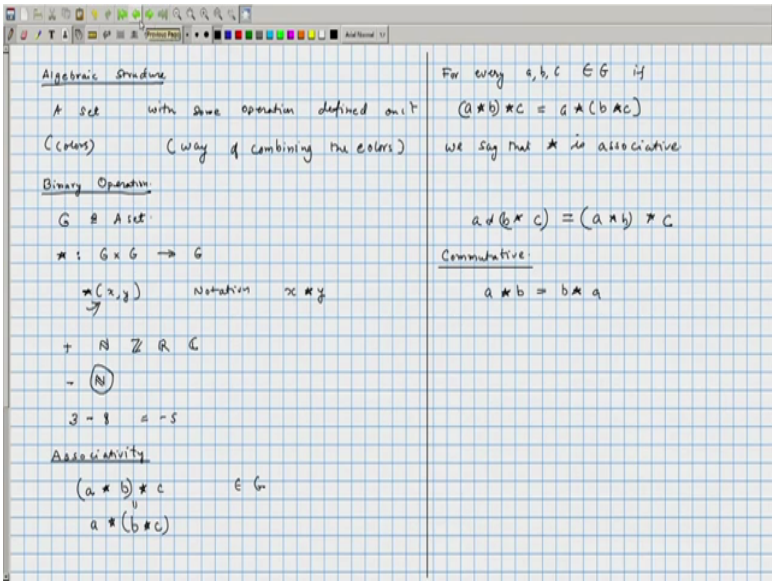
And alpha 3 which was an initially unoccupied now becomes an occupied positions so the value after the move is going to be again A those were the other positions the positions other than alpha 1 and alpha 2 and alpha 3 there value if we denote it by A that followed by the only occupied position that is alpha 3.

So if you combine this whatever value get that is going be the values of board, so you look at any individual move that does not change the value of the board and we argued at this torque the value is B, so after any move no matter what move you perform what order you perform the value of the board should still remain B or green.

So if you call this as green position the value of the final board should be green, so now if we asked whether we can obtain a board position with precisely 1 marble at this position we can say that is not possible because that would be a board position whose value is red, but the only allowable board positions are the once in which the value is green.

So this was a neat little puzzle wherein we solved by identifying a crucial invariant property what is this got to do it group theory. So here we talked about objects combining in a certain way, it an another arbitrary way of combining objects we found combining method very useful to solve our problem but many different objects I mean can be studied by this kind of methodologies wherein we identify some structures in the problem and use that to solve certain problems.

(Refer Slide Time: 26:30)



So, what we have in an algebraic structure, so let say what is an algebraic structure. So an algebraic structure is a set in our case this is colours and some operations on it and that was the way of combining, so depending upon what are the properties that you insist of the operation you will get various algebraic structure.

So in our case we had we had a set of colours 4 colours and we told how 2 of them can combine to give rise to a third colour, so the particular thing that we used can also be called as a group so let us understand what are groups.

So formally we need to understand what are binary operations because this combining we are restricting to combining 2 at a time you can combine more at a time you will get more complex objects but we will restrict ourselves to binary operations. So let us understand what are binary operations.

So you have a set let us called set as G and a binary operation so we could use any symbol let say plus, multiplication, subtraction all these are examples of binary operation, so that would be thought of as a function from G cross G to G, that means take 2 elements then map into a third elements of the set, so it can be thought of as a function which takes a pair of objects from a set and gives rise to an element of the set, in the functional form this can be written as star followed by x, y that means it is combining x and y and it is a function with 2 parameters x and y.

But when we look at algebraic structures the most common notation for writing stars x, y is x star y we will write it in between and use it functional notation, so the usual binary operation

that we will think of plus define on either as a set of natural numbers or the set of integers or the set of real numbers or complex numbers and so on.

So that is a binary operation, it takes 2 elements combines them and gives a third element in the same set. Now if you think of the subtraction operation on the set of natural numbers that is not well define so we should not really talk about subtraction on natural numbers because if you subtract 3 and 8 if you look at 3 minus 8 the result is not really natural numbers.

So we want when we say binary operations by definition they take 2 elements and return a third element so 3 minus 8 the answer is minus 5 and that is not an element of n so minus cannot be viewed as a binary operation on this particular set but of course it can be viewed as a valid binary operation on the set of integers.

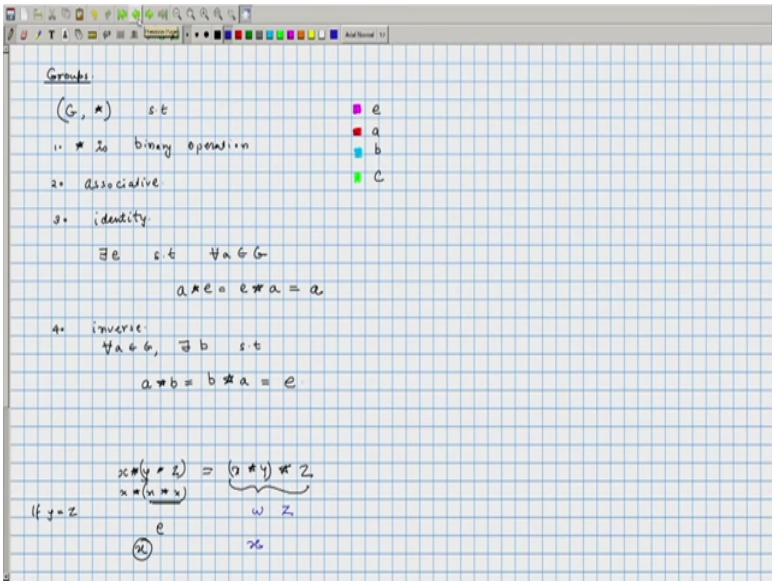
So when in order to define what are groups we will need another property known as associativity, so if you have let us say element A, B and C belonging to G we could first combine A and B and then combine it with C or we could have first combine B and C and A is combine with the result of that, if these are both equal then we say that the operation is associative.

So formally for every A, B, C belonging to G if A star B star C is equal to A star B star C use parenthesis to indicate which of the operations is done first if this is equal then we say that star is associative, so note that in our colour combination example the operation was indeed associative if you had first combined let say if A, B, C where 3 colours some of them may be equal or unequal each of them could be one of the 4 colours.

So if you can verify that A star B star C is equal to A star B star C so that was indeed a an associative operation, infact it had an additional property weather you I mean be with just bothering about combining 2 colours which one is written as a first colour and which one is written as a second colour does not really matter, so that is called as commutatively property.

So A star B is same as B star A, so then we looked at the binary operation that was taking 2 parameters and when you talk about 2 parameters what is the first parameter and what is the second parameter is important but if it is commutative then the order does not really matter A star B is equal to B star A, by our definition of combining colours we did not really think of it in the functional way because this operation we want it to be commutative. So now after we understood what is binary operations what is associative and what is commutative we can define what is a group.

(Refer Slide Time: 32:55)



So the formal definition, a group is a set G with an operation star we call it as star you can use any other symbol so it is a pair the first is a set and the second is an operation such that this is 4 properties. First starts a binary operation, so some books might say that this operation star is there is closure but that is when you say binary operations let us take an care of.

So this is the binary operation and you want this to be associative that means for any 3 elements from G A, B and C. A star B star C no matter how you parenthesis it you will get the same result. And the third property is I did not exist in of a identity that means there exist an element let call that it is e such that for all A belonging to G a star e is equal to e star a and that is equal to a.

So there is a special element we will later on prove that there can be only once such benefits it is a group then there cannot be 2 such elements so here when we say the definition we say that there is an element the property of identity says that there exist as special element such that any element that the group when multiplied with that element will give rise to the same element does not change things.

And the fourth property is that of inverse so formally this means for every element A belonging to G their exist an element b such that ab a multiplied by b or a star b is equal to b star a and that will be equal to identity, so if you can find a set equipped with a binary operation which has these properties that is this is associative it has an identity and every element as an inverse then we say that this is a group.

So let us look at our example we had 4 colours let call these colours as by letters, so this is our special colours which we will which will do the role of e or the identity and let us call this as a, b and c you check that for any 3 elements so let us say x, y, z. so x star y star z is equal to x star y star z, if x is identity so we have to verify for all cases if x identity then what we have here is y star z that is because e combines with anything to leave it unchanged.

So if x is e then this is going to be the left hand side is going to be y star z and the right hand side x combines with y is going to be y and the entire product is going to be or the entire expression on the right hand side is going to y star z. so when x is equal to e this is clear when anyone of y and z if any of them is e then the same reasoning works out.

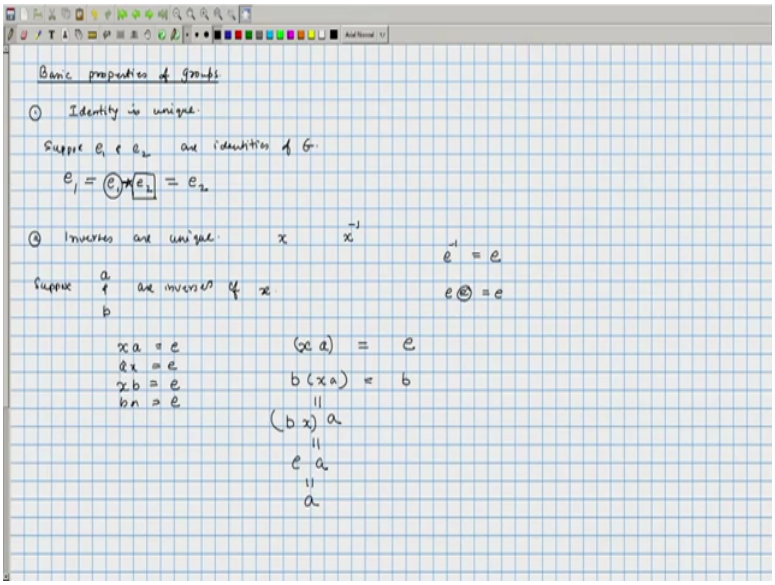
So we may assume that they are all different from e and if 2 of them are the same so one case when all 3 of them are the same for all 3 of them are the same then does not really because left hand side and right hand side they all give rise to so let us say x star x star x x star x is going to give you e and x star e is going to be x and the other side is also going be the same thing.

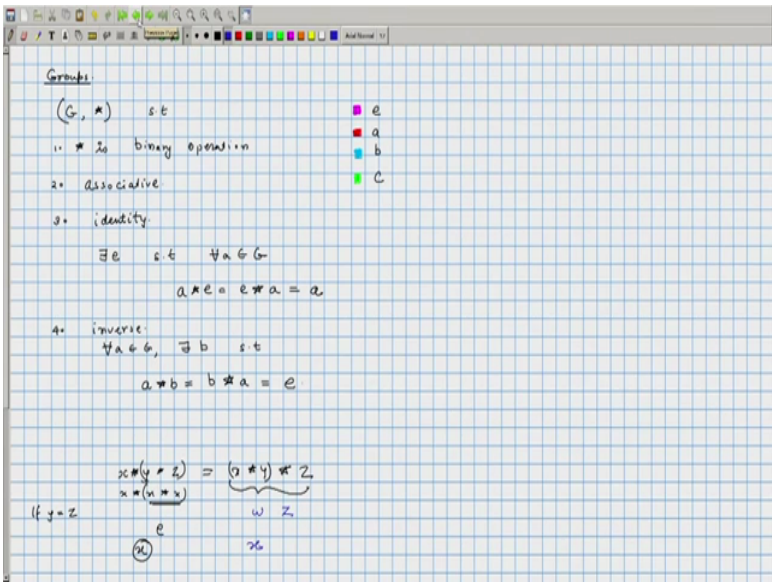
So when all them are the same does not matter if all of them are distinct then x, y and z when they are all distinct y, z will combine to give x and the entire product is going to e and the right hand side is similar x star y is going to be z, z star z is going to e. so when all of them are same all of them are different those cases are taken care of the only remaining case is when 2 of them are the same.

So if y equals z and y star z will give you e and x star e is going to be x if y is equal to z then the left hand side is going to x whereas the right hand side x into y will be the third missing element which we will call by w and w multiplied by z will give you the missing element here which is nothing but x.

So in that case also things are going to be the same so here we assume the y and z are equal if x and y are same then the same reasoning applies and so on, so we can verify in a systematic manner that the operation is associative and then the pink colour or e automatically serves as the identity and every element has an inverse namely the element itself is the inverse mean take you any element it is inverse is itself, because you multiply e to itself you will always get identity, or combine it with itself you get identity. So in our example in solitary problem we had basically assign an element of group to each position and the board and the value of the board was a product of the occupied positions.

(Refer Slide Time: 40:09)





So let us look at some properties of groups, the first property that we will state is that the identity is unique, every group will have a unique identity. Look at the definition we just said that there exist an element there could be multiple how do we rule out that case, so suppose e1 and e2 where both identities of a group and we want to show that e1 is equal e2.

So we just need to look at e1 star e2 because e1 is the identity this has to be equal to identity multiplied by any other element should leave the other element unchanged so they should be equal to e2, also because e2 is an identity we can say that e1 combine with e2 should leave e1 unchanged so they should be equal to e1 and therefore e1 is equal to e2, so there is a unique identity.

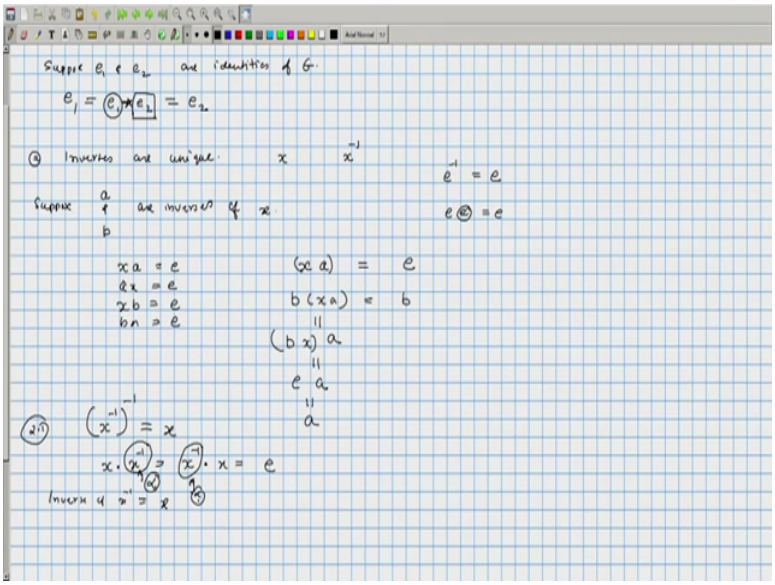
The next property is that the inverses are also unique, so the inverse we will denote it we will have a notation so if you have an element x since it is inverse is unique there is a specific element we will once we have this particular fact proven we can denote it by x inverse that will be the unique inverse of any elements x, how do we prove that?

Suppose let us say a and b are both inverses so what do we know because of this we can say that xa is equal to identity ax is equal to identity, xb is identity and bx is also equal to identity. From these somehow we need to argue that a and b are same. So lets us look at this equation xa is equal to identity now if we multiply with b on the left what we will get is b times xa or b star xa, so when I write xa it means I am just following of the star, instead of writing star e time I will just write the letter.

So when I write bxa it means b star x star a and associativity grantees that the order really does not matter, so bxa that should be equal to b times e and that is b, but here bxa we can write it as b times x and a and since bx is identity this is equals to identity times a and that is equals to a, so we get a is equal to b.

So every element x will have a unique inverse in particular you if you look at the element a the identity element its inverse has to be itself because it satisfies the property that so e times e is equal to e therefore e is an inverse of e and since it is the it there is only 1 inverse e has to be it on unique inverse.

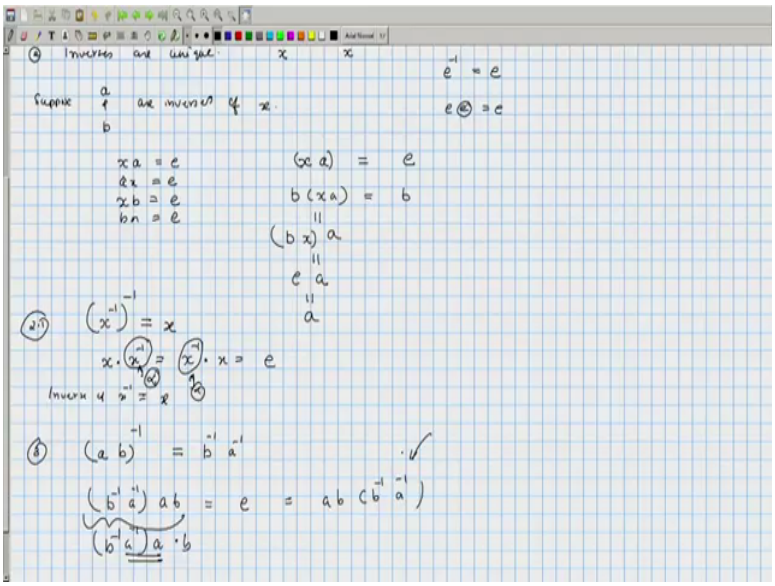
(Refer Slide Time: 44:18)



And another property of inverse is this if you look at x inverse is if you look at x inverse that some particular element its inverse is equal to x that is straight forward because by definition of inverse x times x inverse is equal to x inverse times x is equal to identity. Now if you let x inverse play the role of x then this equation says that the inverse of x inverse is equal to x.

Because if you denote this by let us say alpha if you denote x inverse by alpha, alpha times x is equal to x times alpha and that is equal to identity. Therefore the inverse of alpha must be x.

(Refer Slide Time: 45:12)



The third property of inverse is if you multiply 2 elements a and b and take their inverse that is going to be equal to the product of the inverses is but done in the inverted fashion, so this would not be equal to a inverse times b inverse unless the group is commutative but in any case it will be equal to b inverse times a inverse.

That is because if you look at the product b inverse, a inverse times ab this will be equal to identity and this will also be equal to ab times b inverse a inverse. So this has been bracketed in a certain way but because of associativity properties we can just bracket in other ways and you can combine them and see that they will give identity.

So, we just need to look at b inverse times a times b, so the initial combination of a inverse and a will give you identity, b inverse times identity will give you b inverse that multiplied by b gives identity same thing applies on the other side will again give you identity. So ab inverse is b inverse times a inverse, so we will stop here and will continue our exploration of algebraic structures in the coming class.