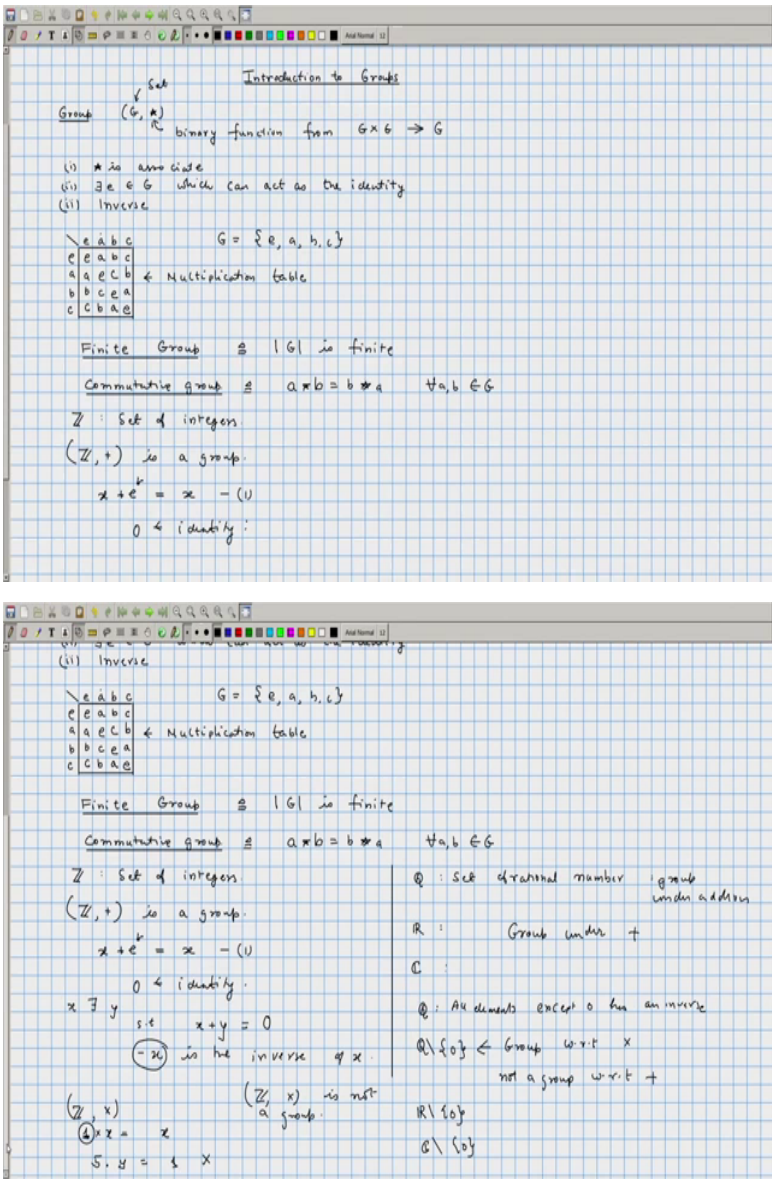
Discrete Mathematics.
Professor. Benny George
Department of computer Science and Engineering,
Indian Institute of Technology, Guwahati.
Lecture 38
Modular Arithmetic and Groups

So we will continue our study of groups.

(Refer Slide Time: 00:30)



A group is basically an algebraic structure it is denoted by G star. So it is two components the first is a set and the second object is a binary relation sorry binary function. From G cross G to G. So it takes two elements combines and gives an element of the set. So that it makes it a binary operation and this binary operation should have certain properties the first property is, it should be associative and the second requirement is there should be a an identity.

And the third property was that every element should have an inverse. These three properties have met for binary operation on G then we say that G together with the binary operation is a group. The examples that would be have seen that one of the example that we have saw, we can describe it by it is multiplication table. Then we specify the binary operation we basically need to tell each pair of elements, what is result of combining them?

So that can be given by a table so if it took G to be e, a, b, and we want to describe here the group that we used to solve our puzzle on reachable configuration on a solitaire board. The group can be describe as e as the identity and the other were the non-identity elements e multiplied by e or e combined with e gives you e and everything else combine everything else leaves the other elements unchanged and any element when combine with its self gives identity.

So a with a is identity b with b is identity c with c is identity, a combine with b gives c a combines with c gives b. So any two elements combine you get the result as a third elements, you can complete the table, this is what we would get. So this is a multiplication table, so that table that we would have a written is a multiplication table. It is called multiplication table because we chose to describe this operation as initially the group operation is viewed as multiplication though it could be very different from arithmetic operation of multiplication.

Now this group has third interesting properties first is it is a finite group, because there if only four elements in the group. So in general the finite group means the size of G is finite. A group with finitely many elements in the set corresponding to it that is called as a finite group. So this is an example of finite group, so for all the groups that we have seen are finite groups.

Now we could look at another property of this particular group namely this is a commutative group. In case of commutative group by definition what it means is a star b should be equal to b star a for all ab belonging to G. This is the case then it is called as a commutative group which is the clearly the case for this particular group that we have consider in fact all the groups that we have seen so far are finite groups.

Let us see some examples we will see that this algebraic structure that we define is without many cases in mathematics where you come across objects which behave in this particular manner familiar example for example if you take the set of integers, so this is the set of integers they do form a group but when we say group we ned to mention the operation as well. So z under, so with plus the usually arithmetic addition is a group. In case we can check

each and every property clearly you can add any two integer and the resultant is a new integer. So the operation the binary operation plus is well defined on the set of integer.

Further we can verify whether it is associative and we claim that there is an identity element that means there is a element x such that plus the identity will be x. SO there is a special elements e in the set of integers which makes this particular equation let us call it equation 1 and makes equation 1 true. So if we can show that there is one element then of course that elements is going to be a unique element.

So in particular here e will be 0. So if you look at the 0 integer that can act as a identity. So identity properties checked further we need to argue that for every element x there exist y such that x combine with y. So here combination operation is y. So this should be equal to identity which we discover it as 0 particular the integer minus x will do the task. So take x and add it to minus x you will get 0.

So every element has an inverse, so that was an easy example now just this if you look at the set of rational numbers they also form a group under addition. If you look at the set of the real number they also form a group under addition if you take a set of complex numbers they also form a group under addition. If you look at the set of real numbers they also form a group under addition if you take the set of complex numbers they also form a group under addition.

So these are examples of group under the usual arithmetic. But note that the addition operation is mean all though we refer to them as addition the addition operation on integers is different from the addition operation on rational numbers in it is again different from the addition not real numbers not complex numbers because if you think of them as operation their domains are very different of course when you restrict to the, because this is sub sets of there is a subset relationship between z, q, r, and c.

So if you restrict to if you restrict the addition to just the set of rational numbers then if you look at the addition on complex numbers and restrict that to just on rational numbers then of course we are talking about the same operation. Now let see some example of certain algebraic operations which will not be let say a group. For example, if we take the set of integers and if you look at multiplication this is the well-defined binary operation you can take any two integers and you can combine them when you combine them you will get an integer.

So, and clearly that operation is associative and is there an element which can act as identity of course there is if you look at the element 1, so 1 multiplied by any element is going to give you the same element even if x is 0 1 multiplied by 0 is going to be 0. So this is going to be trivially true. So 1 is the only element which will have this property, now if you look at the inverse property which should be satisfied by every group if you look at the element rather than 1 or may be minus 1 if look let us say 5.

Is there an element such that 5 times y is equal to 1 there are for example 1 by 5 can do the task but still one by 5 is not and integer. So this does not forma group under multiplication. So z under multiplication is not a group all though this is a well-defined operation, if you look at z under division that also is not a group because that is not even division you cannot take 2 integers and divide one by other.

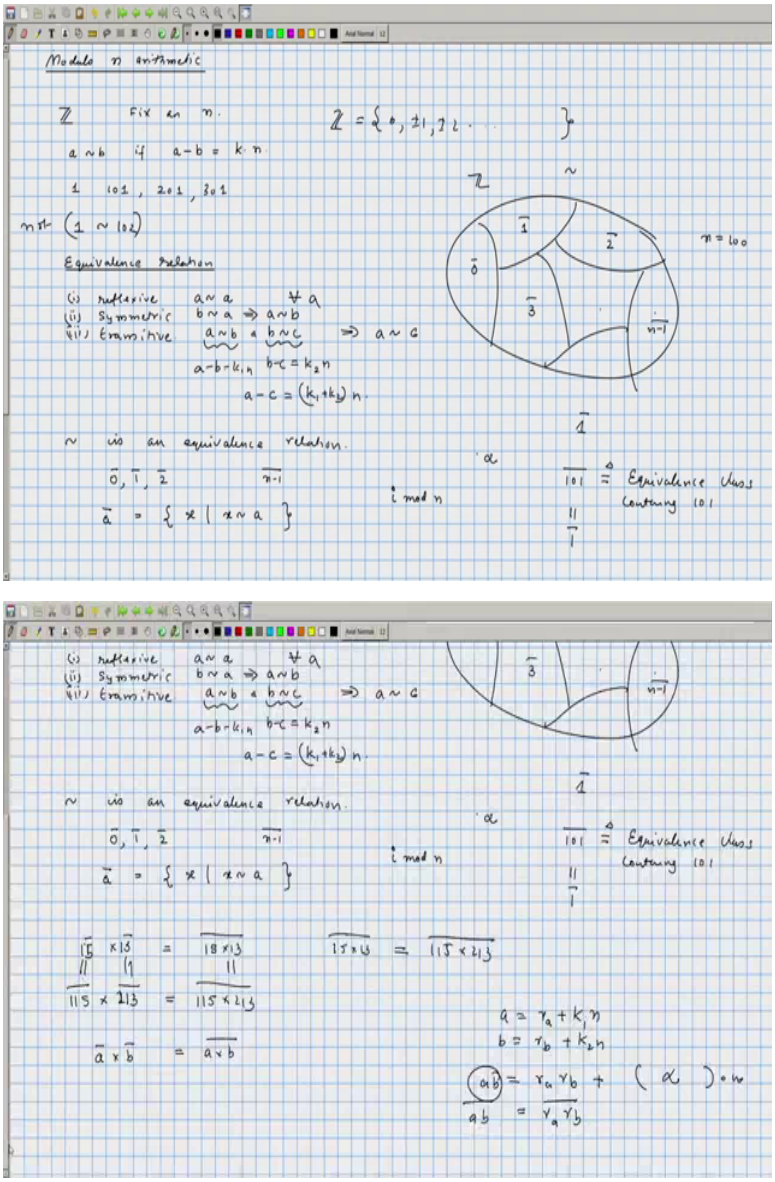
This particular when the number by which it divide is 0 that is not a well-defined operation and therefor that would not be a group. Now if you look at the set of rational numbers you still have you can look at all rational numbers you still have the associative property and 1 is going to so as the inverse means 1 is going to serve as the identity but all elements except 0 has sign inverse.

So this is almost a group but not quite there because of 0. So if you take q and remove this element 0 from it whatever you get is going to be a group under multiplication. But if look at the same set this is not going to be a group under addition. So this is a group with respect to the operation multiply, whereas it is not a group with respect to addition because the inverse identity and their addition was 0 and that is the element that we have removed from the set and now here other element can serve as no other element serve as the identity.

You can look at rational at real numbers that is not going to be a group under multiplication but if you remove 0 then we have a group under multiplication. Same with complex numbers if you remove 0 they will form a group under multiplication. So these groups all these groups we have looked at here they this nice property that they are infinite groups, z, q, r, and c they are all infinite groups.

So we have seen an examples of groups such are finite and infinite and these are groups are all both the finite groups we have consider and the infinite groups that we have considered are all commutative group later on see examples of non-commutative groups as well.

(Refer Slide Time: 13:29)



Now let us look at special group which arises out of number theory. So the operation is a very familiar operation it almost mimic's the addition. So we will look at modulo n arithmetic so that this will be used to define the special groups that we have interest with in. So let us look at the set of integers and we need to define a relationship between two integers we will say that a is related to b if a minus b is equal to k time n.

So if n divides a minus b then we will say that a and b are related. So we will start by fixing an n. So if your n was 100 then 1 and 101 are related because 1 minus 100 is minus 100 that is k times 100 for k equal minus 1. So 201, 301 all these elements are related to each other whereas 1 and 102 they are not related. So this relation is a special relation and since it is called as equivalence relation.

So as you have learned from your set theory lectures an equivalence relation is a relation which is this three properties it should be reflexive and it should be symmetric and the relation should be transitive. So if you look at the set of integers this is your z clearly for any n this relation that we have consider is reflexive because a is related to a for any a because a minus a is zero that is going to be 0 times n and it is symmetric if b is related to a this should imply that a is related to b.

Because b minus a and a minus b any of them is a multiple of n the other is also and it is transitive because a related to b and b related to c this would mean that a is related to c this can be seen by observing that if a related to b then a minus b is equal to k 19 and b minus c if look at it that is going to be equal to k to n and if you add this equations up you will get a minus c is equal to k1 plus k2 times n.

So this modulo n arithmetic if you we have not really talk about module or arithmetic act. If you look at this equivalence relation if you look at the relation tilde that is going to be an equivalence relation, and one thing we know about equivalence relation is if there is an equivalence relation then that is going to split up the underline set into different partition. So if this was you are set z if you look at tilde you will get all you can partition z into some number of parts here we can more specifically state what are the parts.

So we will call them as 0 prime or 0 bar 1 bar 2 bar up to n minus 1 bar. Where 0 bar let us say a bar consist of all element x such that x is related to a if you take all the element related to any particular element that forms one particular equivalence class and here therefore there can be only n minus 1 equivalence classes any other element has to be you take any arbitral element alpha it has to be related to one of these elements 0 one to up to minus 1.

Therefore, must fall in one of these equivalence classes. So here we started of with z and by looking at this equivalence relation we have partitioned z into a finite number of equivalence classes. So for any particular element i if you look at i mod n that is the remainder that you get when i is dived by n that is going to be the equivalence class containing.

So if you look at that number that number rethink of as a representative element of the equivalence class containing i. So these are class room 1, so all the way we are writing, so let us say our n think of it is 100 all though it say our classes are 1 bar 2 bar up to 99 bar we could say that 101 bar this can be define as the equivalence class containing 101 and that is going to be equal to 1 bar. So now what we have is a partition into equivalence classes let us see if we can do arithmetic with this classes which will mimic our normal arithmetic.

So I want to multiply to equivalence classes does it make sense. For example, what is going to be one bar into three bar I could define this to be equal to 1 let us say 5 into, so 15 bar into 13 bar I could define that as 15 into 13 whole bar. Now this is going to be a valid definition only if I take other elements let us say 115 which is in the same equivalence class and multiply it into let us say 213 bar by definition this should have been 115 into 213 the whole bar.

But since these both these classes are the same these classes also the classes on the right hand side also must be same in other words 15 into 13 the whole bar should be equal to 115 into 213 the whole bar if this arithmetic is to make sense can easily verify that, that is the case in case of both addition and multiplication. So we can say a bar into b bar is going to be equal to a into b the whole bar.

Because a bar is going to be all those elements which leave the remainder a and b bar has all those elements that leave a remainder b. So a bar you can think of a as let us say remainder a plus k times n and b is equal to remainder b plus k 2 times n and ab is going to be equal to remainder a remainder b plus all the other terms are going to contain n in them. So this is some expression alpha time n and this is just mean if you look at ab and consider the equivalence class of ab that is going to be same as the equivalence class of are ab.

So the remainder that a leaves when you divided by n alone is the alone determines the equivalence class contained containing a so you can work out the arithmetic and verify that the operation of addition and multiplication are indeed well defined. So early in all our example we started with an operation which is well define except in case of division we had a well define operation of addition our integers or complex numbers or rationales so on.

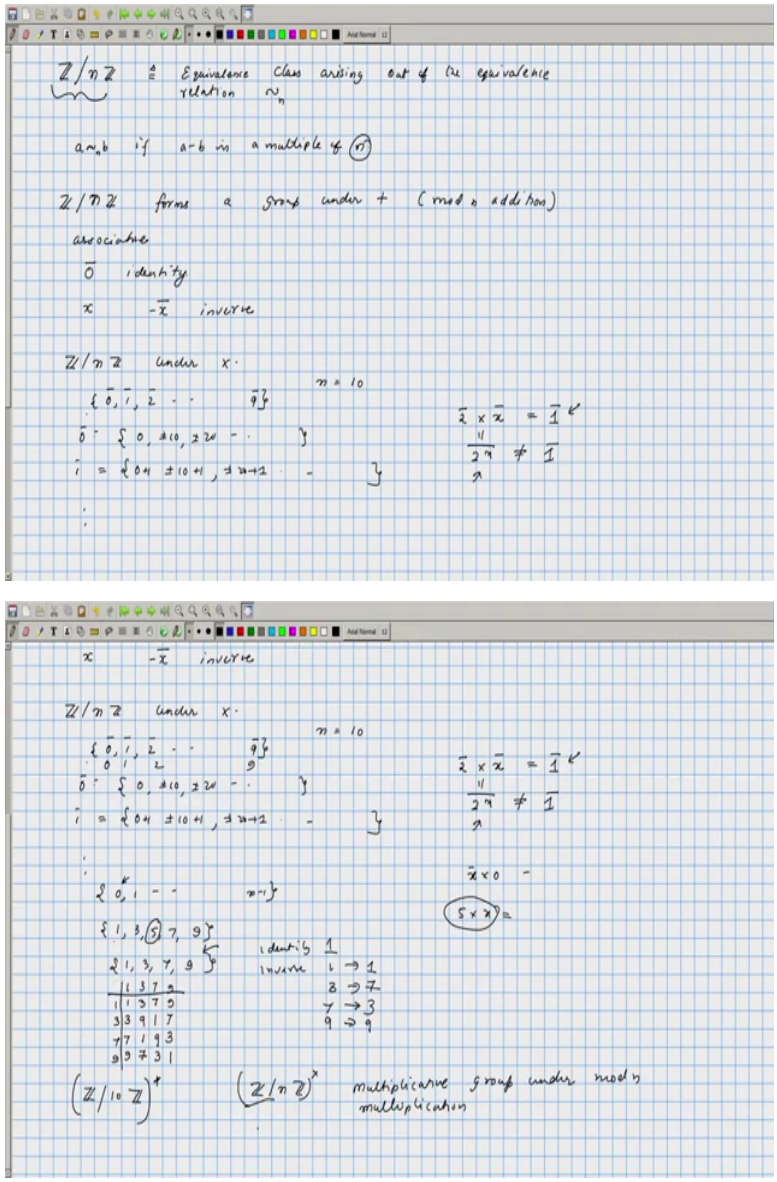
Here we have a new set which consist of equivalence classes and on theses equivalence class we have defined two operations one of additions and one of multiplication. In fact, we have defined infinitely many operations one for each number. Fix number and if n equals 100 you have a particular split into equivalence classes and if n is 113 we have yet another split into equivalence classes.

Once you fix the collection of sets or the equivalence classes you can multiply them you can add them in a certain way and those operations make sense they are valid binary operations on a finite set because each of these equivalence classes all though they might be infinite the number of equivalence classes is always going to be finite. If you are doing mod n arithmetic

if your equivalence relation is defined, let us say some number let us say some number finite number and the number of equivalence classes that you would have is a finite number.

And therefore this is a finite set on which we are operating. So we can ask our self this question is this finite operation? Along with this equivalence classes a group, so we see that under the addition they do form a group but under multiplication they do not but there is way of extracting a group out of these operations for multiplication as we will see that in the remainder of this lecture.

(Refer Slide Time: 24:46)



So let us first see the easy part, so we will first give some names to this. So Z mod n Z. This is an notation when we write Z slash n Z we what we mean is this is define as the equivalence classes arising out of the equivalence relation tilde. So I am going to write tilde n because we

say that a related to b a tilde and b if a minus b is a multiple of n. So this is dependent on the particular n that you chose.

And Z mod n Z that is how this is read. So Z mod n Z is going to be the equivalence classes arising out of this particular relation and if we look at the addition operation of these classes. So Z mod n Z forms a group under plus. So this is this plus is not the usual addition of numbers but this is the mod n addition. So you add to equivalences we added in the way we describe the layer ab that is same as the modulo n addition.

Why it is a group we need to check first of all that this is a valid binary operation that is something that we have seen earlier and clearly it is associative, and equivalence class corresponding to 0 will act as the identity and for any element x if you look at minus x or the equivalence class containing minus x that will be the inverse.

So we can easily verify inverse property also, so once you have a finite collection with the property of with the operation being associative and identity and inverse is being present we know that forms a finite group. Let us look at Z mod n Z the same Z under multiplication. So in this case if we look at, let us say so let us take an example if we take n is equal to 10 then our equivalence class is 0, 1, 2 up to 9.

So 0 bar, 1 bar, 2 bar, and 9 bar. So 0 bar consist of all the numbers the multiple of 0 one consist of all the number which are 1 more than multiple of 0 bar consist of all the multiple of 10, 1 bar consist of number which is one more than multiple of 10 so on. So 0 bar is 0 plus or minus 10 plus or minus 20 and so on. 1 bar is equal to 0 plus 1 plus or minus 10 plus 1 plus or minus 20 plus 1 and so on.

So these are your different equivalence classes and if we look at 2 bar that is one of the elements is there an element x such that two bar multiplied by x will give you identity clearly we need to check with only elements 1 to 9. But one thing we can observe is when you take two bar and multiplied with x and take the whole compliment and look at the equivalence cost containing 2x.

So this is equal to 2x bar, 2x is always going to be even number and here 1 bar we can check that if there is an identity then one has to be that identity, identity has to unique and it has to be 1 and 2 times x bar is going to consist of only even numbers and therefore this cannot be equal to 1 bar. So clearly this set of number cannot form a group at least when n is equal to 10. So in general it cannot be a group under multiplication operation.

Is there some way to extant out a sub set of these such that they form a group. So now we will stop pretending that the equivalence classes are going to be sets instead we will just work with the representative elements. That is much more convenient than just let us say thinking of these 1 bar,2 bar and so on we will just replace with number 0, 1, 2, up to 9 or when you are looking at the equivalence class corresponding to n when we are looking at mod arithmetic we will think of equivalence classes denoted by numbers 0 to n minus 1.

We will not put the bar above it and pretend that it is a set or it is an equivalence class. Instead whatever we do with the numbers themselves can be restated in the language of combining the sets by the other equivalence relation. So if we take these numbers 0 to n minus 1 can be somehow make this a group under multiplication may be the element 0 is going to be the trouble maker.

So let us first work out an example involving when n is equal to 10, so if you have 0 then clearly the multiplicative inverse is going to be difficult to combine because any element multiplied by 0 is going to or a multiple of 10. So x into 0 will always be equal to 0 it will never give you 1, so 0 cannot any have an inverse what are the other elements with may not have an inverse.

So we will try to remove the element which does not have an inverse an look at the remaining set and hope that will do the trick. Here at least the evenness is causing trouble, so let us say we remove all the even numbers then we will get 1, 3, 5, 7, 9. But 5 is also trouble maker here in the sense 5 times x is going to be and this is always going to be multiple of 5 so you will never get 1.

So maybe we will remove 5 as well and we will look at 1, 3, 7, 9. So now if we just have these four elements let us try and see, let us try and write multiplication table corresponding to it. So our elements are1, 3, 7 and then 9, 1, 3, 7, and 9 1 into 1 is 1 1 into 3 is 3 1 into 7 is 7 1into 9 is 9. This is going to be a commutative group, so we need to look at only half elements almost half the elements 3 into 3 is 9, 7 into 7 is 49 that is also going to 9, 9 into 9 is going to be 81.

So this almost look like our e a b c but that is not the case because 3 times 3 is not going to be 1 and 7 times 3 is going to be 1 because 7 time is 21 which is 1 mod 10 7 times 9 is going to be 3, 63 3 times 7 is 1 3 times 9 is 7 we can fill this up. So we get a multiplication table and from this table we can infer that all the properties that was required of the group is basically true. So this has identity which is one and inverse also there.

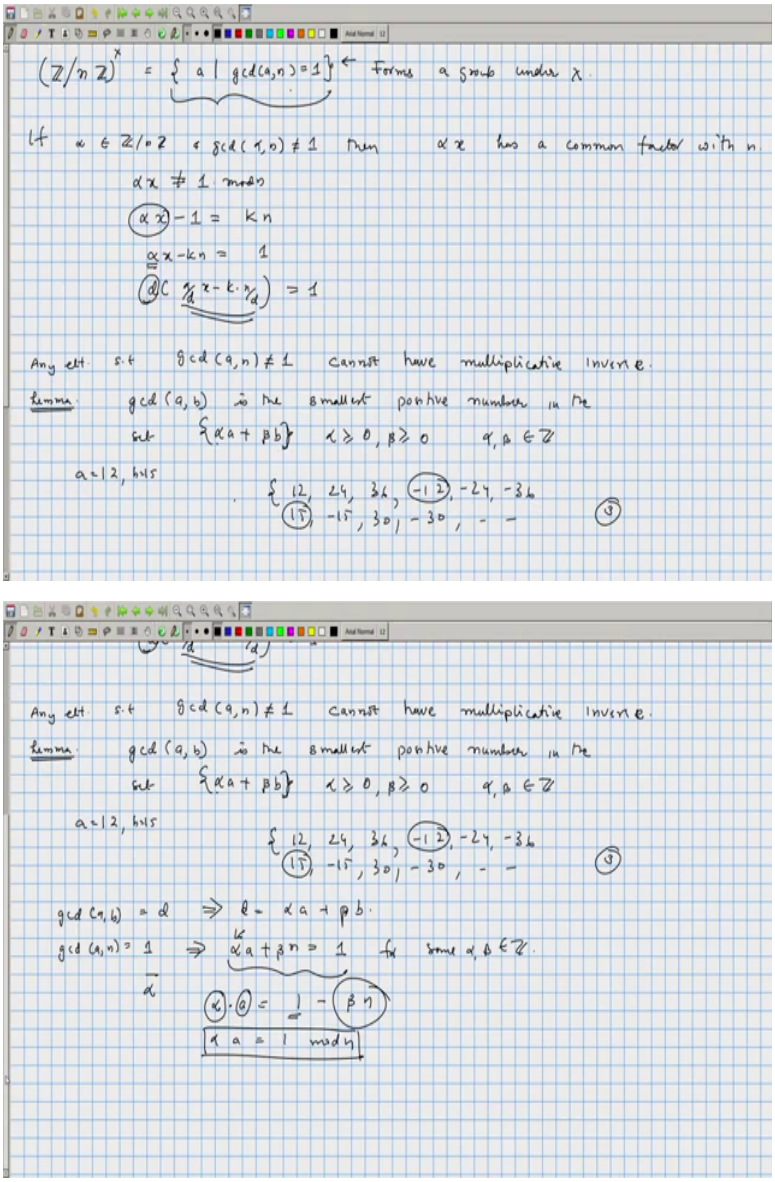
So namely the inverse of 1 itself of 3 is going to be 3 into 7 is 1. So inverse of 3 is 7 inverse of 7 is going to be 3 inverse 9 is going to be itself. So once you have verified identity and inverse associativity comes for free and check this valid operation therefore these elements form a group. So this is denoted by Z 10 because we were doing mod 10 operations 10Z the reason why we are writing it as this particular form Z divided by 10Z or Z mod 10 Z that will become clear and one of the later classes.

But right now we will just use it as a notation, so but we are not taking all the elements so when we write multiplication here this is what the although we are writing at Z divided by 10Z with the multiplication operation this basically means we are considering elements 1, 3, 7 and 9. So what is natural generalisation of this if it is n Z what does it mean which are the elements that stays which are the elements which will go out.

Here at least in case of 10 we could expand a sub set of elements which forma group among themselves. In case of general n can be do this we can do that and therefore when we write Z n Z star this is the multiplicative group under mod n multiplication. So what are the elements that goes into this we will make it clear in a short while, you can try to guess what are all the elements that are going to be there and Z divided by n Z.

It is going to have at most n minus 1 element because 0 is automatically not going to be present there. So the element from 1 to n minus 1 could be present and that is present in special cases try and figure out what is the special case.

(Refer Slide Time: 36:26)



But right now we will describe what precisely what explicitly what are the elements there in Z mod n Z under multiplication. So let us look at all the element a which are less than n and GCD of a n is equal to 1. So if you look at these collection we will show that this does form group under multiplication so this look at this collection will be proved that this forms group under multiplication.

But if you wanted to prove that Z divided by nZ is equal to this we need to show that our crosses was look at all the elements in Z divided by n Z the most n element 0 to n minus 1 from these all the elements which could possibly not have inverses with threw them out and whatever remains they will they will all have inverses and that is precisely this collection, why is this so?

So if you take any element let us say if alpha belongs to Z mod n Z and GCD alpha n is equal to is not equal to 1. Then clearly if you multiply if you look at alpha x has a common factor with n because alpha has a common factor with in alpha x will also have a common factor with n and therefore alpha x cannot be equal to 1 ever, because if this was equal to 1 mod n then alpha x minus 1 is equal to k times n alpha x has a factor.

So this would mean alpha x minus k n is equal to 1. Alpha x has a factor with n so if you take the common factor d out. So d into alpha by d x minus k into n by d this is equal to 1. So this is some number which is greater than 1 and this going to be an integer. So how can be multiply two integers with a different from 1 and of which at least one of them is different from one and get what so this is impossibly and therefore all the elements with are outside the set that we have describe here must be excluded.

In other words, any element such that GCD a, n is not equal to one cannot have multiplicative inverses. SO that is one part now we need to show that every element which satisfies the property that GCD is 1 GCD with n is 1 they will have inverse. So we will use the following Lemma if you look at the number so GCD ab is the smallest positive number in the set alpha a plus beta b.

If you look at alpha a plus beta b for alpha beta belong to integers and take all the possibilities, we will get we will get infinite set in that infinite set the smallest positive number is equal to the GCD you will not prove this statement it can be slip root from the basic number theoretic facts. But this is the so you can either treat this is the definition of GCD that is work out one example if you look at let us say 12 and 15 look at the numbers that you could form are (())(41:30) then 12 is possible 24 is possible 36 and the negative of this are all possible minus 12 minus 24 minus 36.

15 minus 15 30 minus 30 all these numbers are possible and this set has a nice property that look at number that form alpha a plus beta b if you take two of them and add them you still get another number in the collection for different alpha and beta. So minus 12 and 15 if you add you will get 3, so 3 is also going to be an element in the set you can argue that 3 is going to be the no other number smaller than 3 and strictly positive.

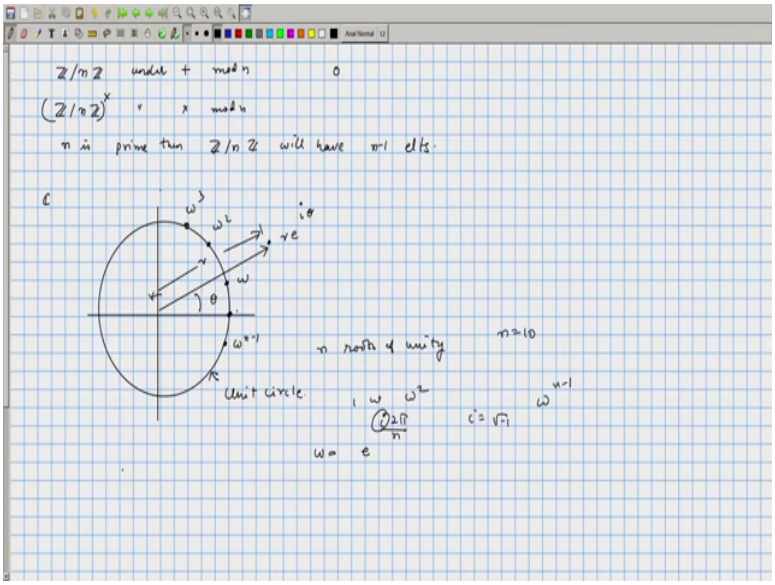
So at least in this case you can easily verify that the GCD is in fact the smallest positive number that can be obtained as a linear combination of 12 and 15. So we can use that fact that GCD ab smallest positive number of the form alpha a plus beta b. So if GCD ab is equal to d

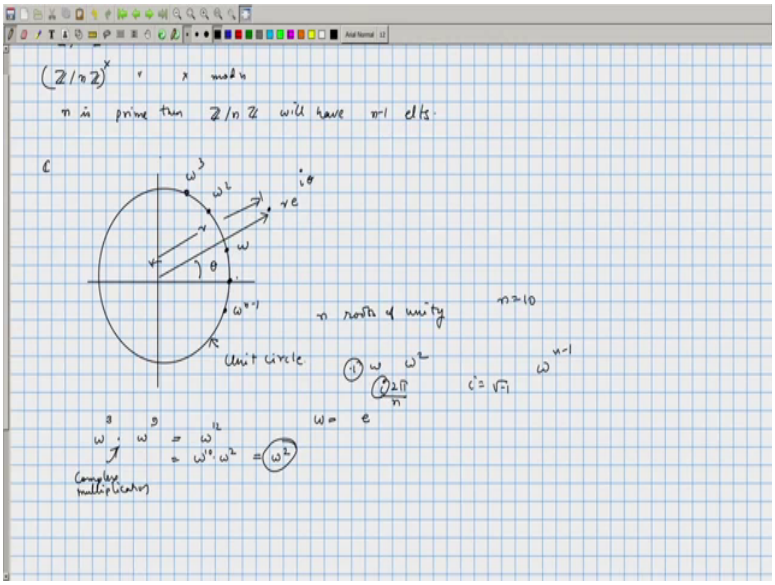
then d can be written as alpha plus beta b. So from this fact if GCD a n is equal to 1 this would imply that alpha a plus beta n is equal to 1 for some alpha beta belonging to integers.

So now if we look at this alpha is an integer look at the equivalence class which contains alpha if you look at alpha bar when the representative element for that class is going to be the inverse for a because that is clear from this equation alpha times a is equal to 1 minus beta n. So alpha and multiplied by a gave you 1 mod n so if look at this equation mod n. So alpha a is equal to 1 mod n.

So from this definition it straight forward that any element of the set define in this particular manner must have a multiplicative inverse in case we can, so if you look at the set we can look for multiplicative inverses we can look for associativity comes for free and identity 1 surely an element of this set because GCD 1 n is of course 1 and therefore this forms a group under multiplication.

(Refer Slide Time: 44:15)





So we have two new groups in fact infinitely new finite groups. So this under addition mod n and Z under multiplication mod n. So all though the arithmetic is mod n the sets are going to be different in both cases the first case surely the set will contain 0 an it will contain all the other n minus 1 as well, n minus elements as well as if you can consider the multiplicative group.

Multiplicative group will have strictly less elements than n if n is prime then only then Z n Z will have n minus 1 elements because if n is prime the numbers which are relatively prime to n or the number which have GCD with n as 1 are all the numbers less then n except the 0. So this gives us many examples of finite groups we will now see some other examples from the set of complex numbers.

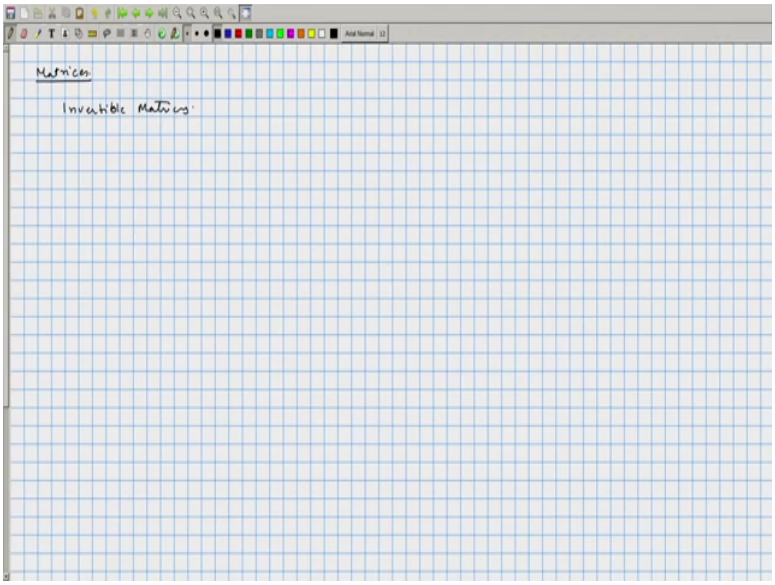
So let us look at the complex plain if you look at the complex plain then each complex number can be thought of as, so let us say r e raise to i theta, so this is he angle theta and this distance is r. Now if you look at roots of unity. So complex numbers if you remove the 0 complex number that is of course going to be a group under multiplication let us look at another example.

So let us look at the unit circle and let us look at let us say the n roots of unity. So let us say n is equal to 10. So consider the n roots of unity, so if the nth root is going to be let us say omega you can check that the other roots are going to be omega square omega Q went so on up to omega raise to n minus 1. So 1 omega, omega square omega raise to n minus 1 are going to be the n roots of unity where omega is e raise to i 2 pie by n where i is the where i is the square root of minus 1.

So now let us just focus on this numbers do they form a group of course we have to think what is the operation if you add two of them if you take omega raise 3 and let us say if n is 10 this multiplied by omega raise to nine this is going to be omega raise 12 this is going to be omega raise to 10 into omega square and that is going to be just omega square. So here the multiplication is a complex multiplication restricted to these ten numbers.

So we are looking at this ten numbers omega, omega square of 2 omega raise to 9 you can check that these complex numbers could be multiplied by us, this could be multiplied as complex numbers and the resultant is going to in lie in the same collection. So we have a valid binary operation on the set of nth roots of unity and that operation of because complex multiplication associative we have an associative operation you can verify that since one is there is a multiplicative identity and also every element here can be inverted as well and therefore these for a group under multiplication next example we will, so this is again a finite group which is a sub group of a infinite group.

(Refer Side Time: 49:03)



If you look at matrices if you look at the collection of all matrices that is not going to be a group in general because under matrix multiplication there is lot of matrices which cannot be inverted. So if you look at invertible matrices it can show that they also form a group under matrix multiplication. We will stop here for today and continue our discussion on groups in the next class