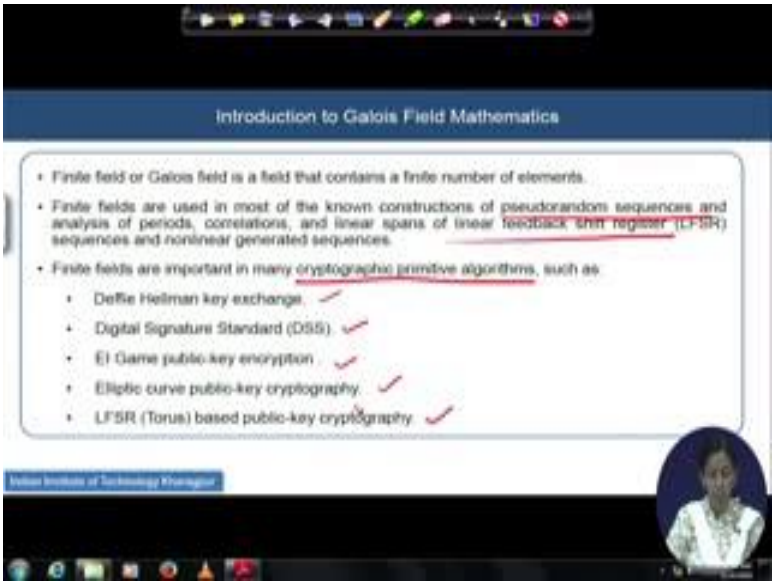
Spread Spectrum Communications and Jamming
Prof. Debarati Sen
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

Lecture - 24
Galois Field Mathematics

Hello students. Today we will start with introduction to Galois Field Mathematics. This say why we are entering here is, we have learnt a lot about the circuit design perspective of the generation of the codes, p n sequence codes, and as well as the maximum length sequence codes, through your linear feedback shift register architecture. But we have also discussed little bit about the mathematical analysis we have done, we have discussed little bit about the way the output codes and the bits of those codes are generated, but we I have not really gone into deep philosophy of designing and devising this codes and there on the form the fundamentals of the mathematics.

And in future if you try to design some code for secrecy, it will be you are for your own design. Then you need to understand that how to start what is the deep root of the mathematics from where actually the understanding and the framework should start with. To bridge that gap we will learn today little bit about the Galois field mathematics, and we will try to link up all the terms that usually is used for the code generation.

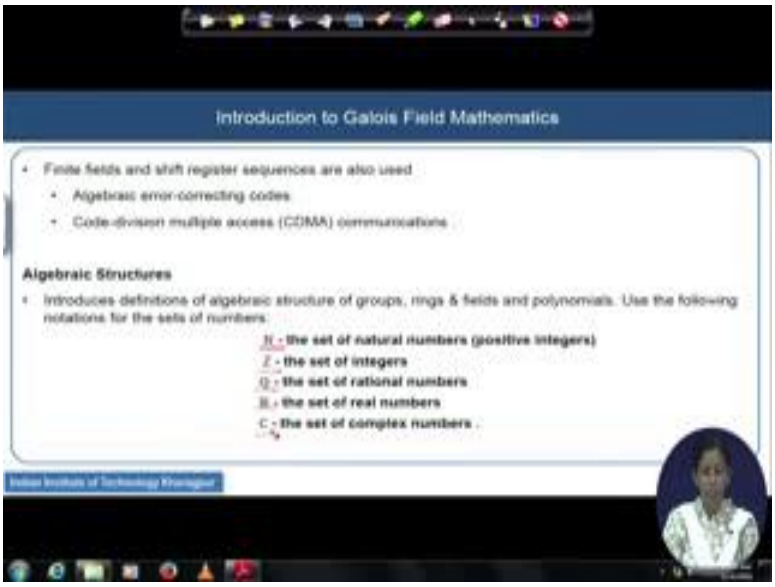
(Refer Slide Time: 01:45)



Galois field is a finite field, where you will see all the contents all the elements all the elements of that field contains the finite numbers. So, these finite fields are basically used for your code analysis, your analysis of the period's auto correlation cross correlation, generation of the p n sequence, p n random sequences and also the linear feedback shift register architecture non-linear sequences. We will specially see in the later module. So, how this finite field are really very important for the non-linear code generation? We will also link up the concept of the polynomials and the finite fields to the linear feedback shift register architecture at the end of the understanding of Galois field mathematics.

So, this is the one uses scenario where the finite fields are utilized for all this purposes and, but it has another important application in generating an in devising very lot of cryptographic primitive algorithms. I have given you some of the example of those cryptographic algorithms. For example, the Deffie Hellman key exchange algorithm digital signature standard algorithm, EI game public key encryption, elliptical curve, public key cryptography LFSR based public key cryptography. These are some of the examples where finite field is fundamental concept from where we start with.

(Refer Slide Time: 03:31)

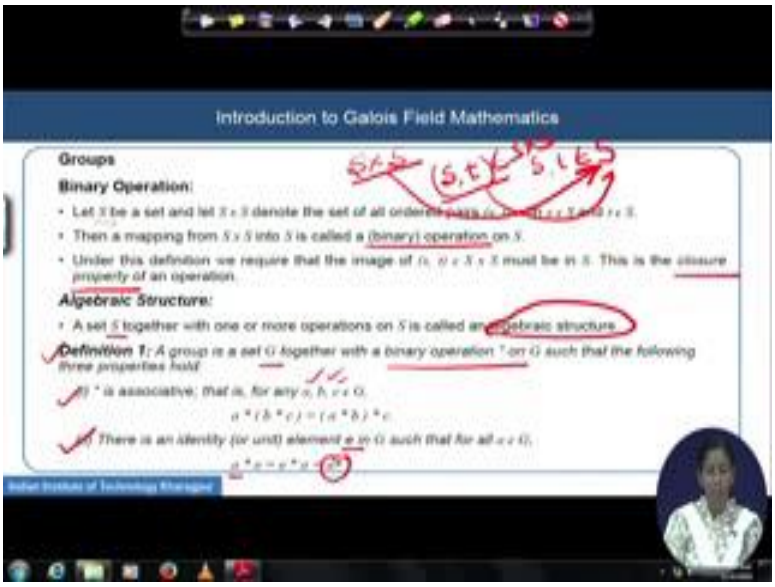


The finite fields and this shift register sequences; they are also used in other areas of the communication. For example, code for code division multiple access communications in devising the forward error control codes the FEC which we called the FEC and those

error control codes are designed it to give the protection against your channel burst errors as well as the channel errors. And all the whole family of the forward error control codes starting from your block code to all the codes that you can name off, the convolution code the RS code the concatenated code the LDPC which is mostly used in the modern communication systems. The generation and the algebraic architecture of all those codes roots down to the understanding of finite fields. It is beyond the scope of this codes to show you all the aspect of the finite fields and this application to those generations, but we will definitely relate the finite field it is relation of the finite, fields to the LFSR architecture and only near code generation architecture.

So, from now onwards we will talk about some specific algebraic architecture, and those algebraic structures of the architecture, so will be named as the group rings fields polynomials etcetera. But before describing the architecture we need to understand some of the definitions. So, we will use this following notation. Number one, this is n which will be the set of normal natural numbers Z, set of the integers Q, the set of the rational numbers R, the set of real numbers and the set of the complex numbers; natural number, integer, rational number, real number and the complex number.

(Refer Slide Time: 05:33)



So, now we are starting with the group. Before entering in to the algebraic structure of group we need to understand; what is the meaning of binary operation. That we seldom used in the digital communication, but what is the mathematical meaning of it is like this.

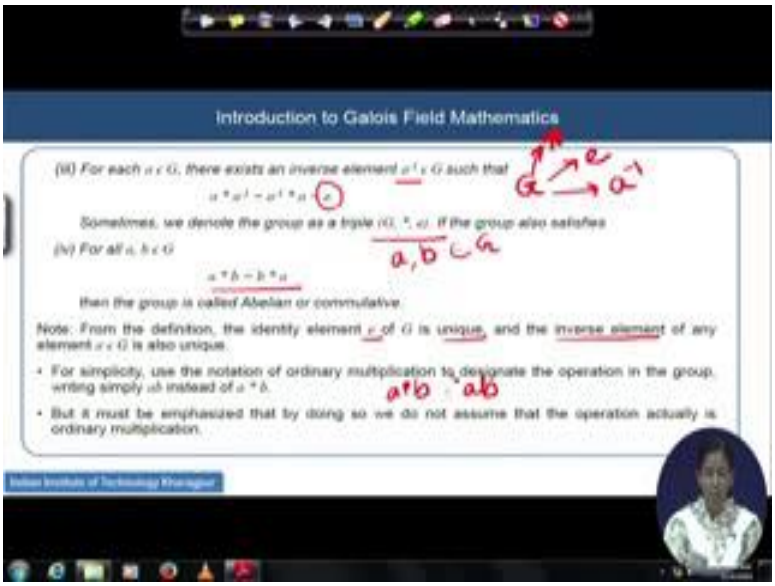
Let us consider that S is a set and there are S cross S, it denotes another set which is basically constituted by taking all the ordered pairs s comma t, which where s and t they belong to the original set S. So, I started with S I took all the ordered pairs who belong to S and I have put all the ordered pairs into another set which is S comma S cross S. So, then the mapping of this S cross S to S if I do some mapping from S cross S to S will be called a binary operation.

Remember one thing under this definition of this mapping and the binary called binary operation; we require that for each the image of all the components of this ordered pairs is called my t which belongs to your S cross S they should also be present in S. If I do a mapping from S cross S to S, then all the element that belongs to S cross S that are the ordered pairs must have an image on this that is assumption that has to be done. We call it the closure property. So, what we learnt? We learnt that what is the binary operation; and we learn what is the closure property of an operation. So now, the algebraic structure of the group can be defined, set now S and together with is one or more than one operation that we are declaring here, together with S, I mean that operations are running on S it is combine called algebraic structure.

So, I have a set and I have one or 2 binary operators and so, those binary operators together applied on s. Together will be called as a group. We can now set the definition of this group. A group is a set, with together with this operation star; the operation is symbolized as star. And so, the star operated on G will form a group if and only if the properties the following 3 properties hold good.

Property number one, the binary operator this star, it should be associative. That is suppose I have 3 elements, which belong to G. For them if I give the operation like this means b operated b with c b star c and then a star b star c should be equivalent to a star b star c. And there should be an identity or unit element called e in G in such a way that for each and every element a who belongs to G if I do that operation I if apply the binary operator in between a and this element e it should revert me back, which is equal to e star a also it will revert me back the element A. If it holds good, then we can declare e is the identity element of the group G.

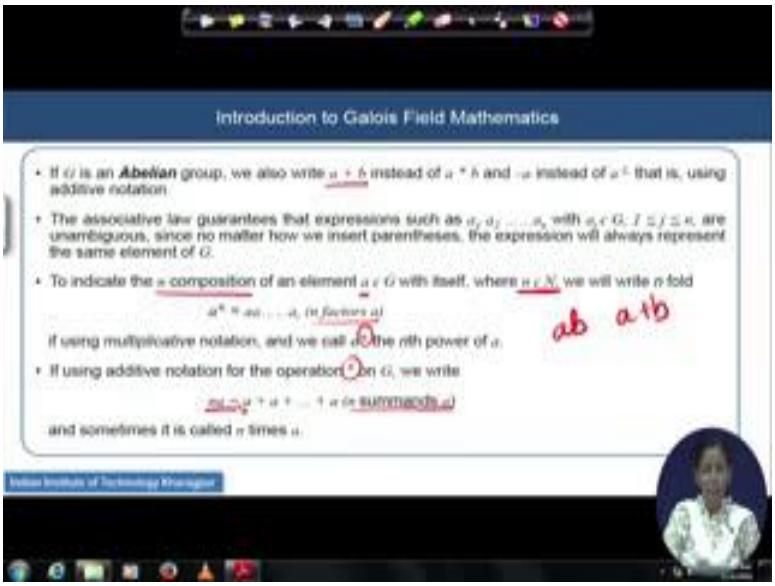
(Refer Slide Time: 09:02)



And the third element the third property says, that for each and every a that belongs to G there should be the another inverse element present in that group G. And to that such a way that a operator with that operator operating on jointly on a and a star will give you back the identity element e. So, hence we have 2 unique element associated with g. One is the identity element and another is the inverse of each and every element whoever is present inside the group. So, with respect and G is actually generating their identity element and there is inverse element with respect to a specific operator called the operator star.

So, group with it is binary operator and it is identity element sometimes, we write we prefer to write 3 of them jointly to denote a group. And we call it a triple, and if we find that for all the elements say a comma b who belongs to G, I can be finding a property like this that a star b is equal to b star a, then we can call that this g is a abelian group or commutative group. And from this definition the identity element e is definitely a unique element, and inverse element also is a unique element associated to a specific growth. For simplicity now we can proceed from now onwards saying that, there is instead of writing a star b we may use that a b, but remember that this a b is does not mean that the normal multiplication that we understand in the conventional arithmetic.

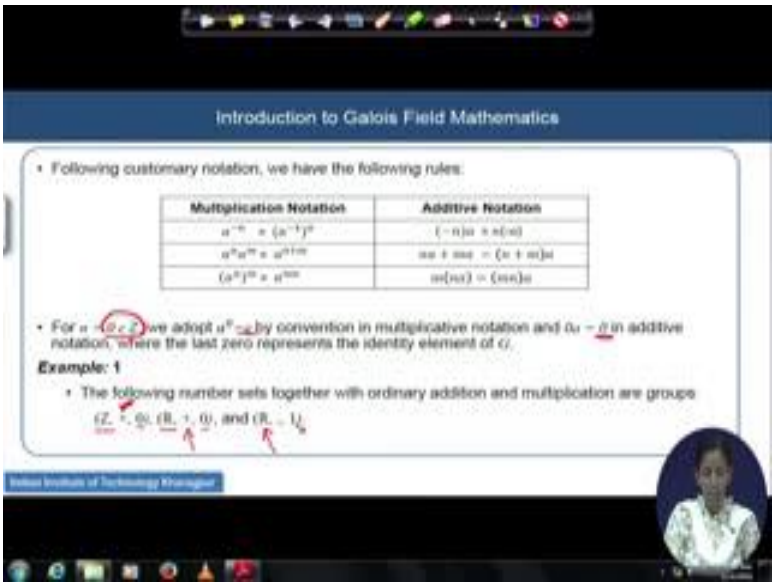
(Refer Slide Time: 10:46)



Similarly, actually the group is my abelian group, then for the operation of instead of writing a star b, and we can write a star a plus b instead of writing a star b, and we can also write minus a instead of your a inverse. And this additive notation they using this additive notation instead of my a star the operator we can try to this a plus b also. So, in in the whole Galois field he will receive that the elements are either said by a b or a plus b based on the operator is multiplicative operator or it is a additive operator.

Another important part to understand is the associative law, that guarantees that the expression such that a one to a in the way you are writing where all the a js belong to G and j is varying from my i to n. These are unambiguous. So, whatever we the we insert the parenthesis this expression will always represent the same element of the G of course, now we are coming to some details some more understanding. Suppose we wish to indicate the n composition of an element a, a is belonging to G with itself. And this small n can have it exist to be between a capital N any value within one to capital N it is. So, we will write the n fold of a if the if we utilize the multiplicative notation, and we call it an n factors of a which is basically a multiply by n times. And we call it the nth power. And if we use the additive notation then it will be like as a plus add it add it is n times. So, we call it n summands a and we will be ending up with n into a, and we calls sometimes it is an n times a also like the conventional system.

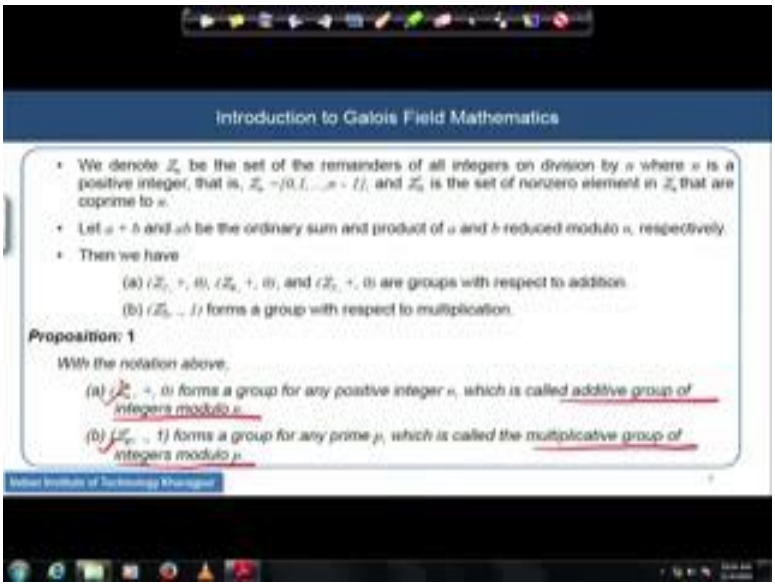
(Refer Slide Time: 12:49)



So, some customary notations here, some small operations we have shown. So, for multiplicative notation a to the power minus n can be equivalent to a to the power minus 1 into n. And equivalently here it will be minus n into a which is nothing, but n into minus m. Here actually multiplication of a to the power n into a to the power a m will be given by n plus m, whereas, in n a plus m a it should be is equal to n plus m into a. Here we are ending up with a to the power n whole to the power m, which is equal to a to the power n into m, and here it is ending up with m n a which is equal to m n in of a. For your n is equal to 0 which belongs to the integer group, and we adopt that a to the power 0 is a identity, it is identity element, by convention in case of our multiplication notation and 0 into a which is equal to fundamentally 0, this is the additive notation, where this 0 will be the identity element with respect to the additive operation is equal to additive.

So, once we understand the definition of the groups. So, we can now map that all the integers the group of the integers the set of the integers with respect to my positive I mean plus addition with respect to additive operator, and with respect to 0 with identity element is a group. Our set of my real numbers with respect to additive operator and 0 identity element is a group. All the real a set of real numbers with multiplicative operator and with our additive element one is also a group.

(Refer Slide Time: 14:47)



Now, let us define Z n. Z n be a set of the remainders of all the integers of the Z when it is divided by the number n. So, it is a modulo n. Z n is the modulo n, it is the integer with the modulo n of Z I should say and then Z n star is the set of the non-zero elements who are coprime to n. The definition of coprime is such that, suppose n is the prime number. Then actually any number between 0 to n if you pick up and if you try to find out that any number and that number let be a.

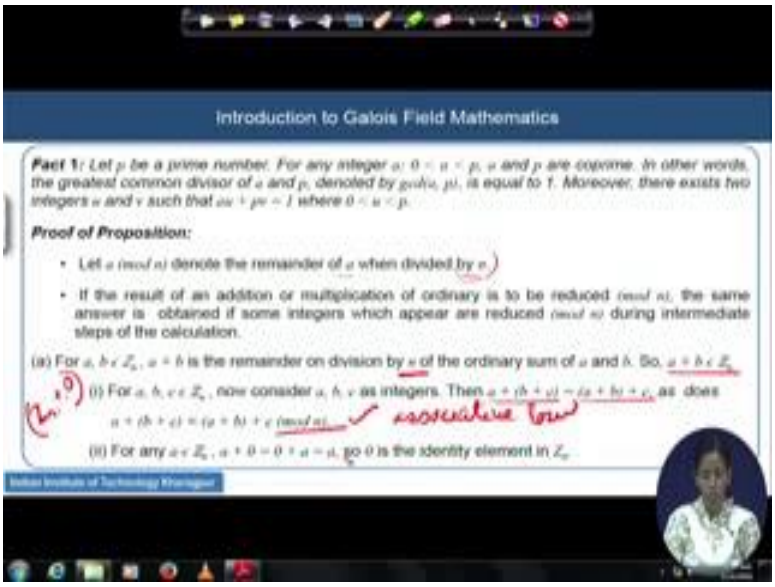
Then you will see that the greatest common divisor in between this number a and n is equal to only 1 if this happens than we say that a and n they are coprime. So, in this situation when Z n star will be the set you will of the no zero elements which are picked up from Z n. And then you will see that all the elements the coprime though elements of this should use constructed in such a way the elements of we are seeing of the Z n star they are the coprime to n. Let a plus b a b which we have already define they are the ordinary sum and products. If that is a situation to then for we can actually nicely construct this Z n and Z n star with respect to some known construct some known few known groups.

Like this, Z 2 it is called the remainder when the modulo 2 operations is non over the real numbers. With respect to my positive operator and my 0 identity element is a group. And this is also of modulo 6 operations with respect to my positive operator and 0 identity element, like this Z 5 plus 0 they are all the group with respect to addition. Then this Z 5

star with respect to my multiplicative operator and my identity element is equal to one, it forms another group with respect to the multiplication. So, now, we can propose some theorem. This theorem is respect to this notation we can propose that Z n plus 0, I mean with modulo n operation over the real numbers with additive operator and the identity element 0 will form a group of any positive integer n, and which we which is called as the additive groups of the integers modulo n. So, we have to prove that these form of group, and an I again all the prime numbers if p is the prime number. So, Z p star with multiplicative operator and identity element one. It will also form a group for any prime number of prime, which is called the multiplicative group of the integer modulo p.

We have to prove that this is a really group. We have to prove that this is really a group. So, we will do it in the next slide. So, in order to prove that it is a group, what we need to do we have to prove that the with respect to the binary operator, the elements are associative, we have to prove their existence identity element. And they are existing and inverse of that. So, identity element the inverse element as well as associative law we have to prove for both of them. To consider that yes the practice to that this will form a group.

(Refer Slide Time: 18:31)



And we have seen a fact from the definition of the coprime just now that I told, that it p is the prime number that then for any integer a which belongs to the 0 to p, a and p will be co prime because you will not find the greatest common divisor between a and p apart

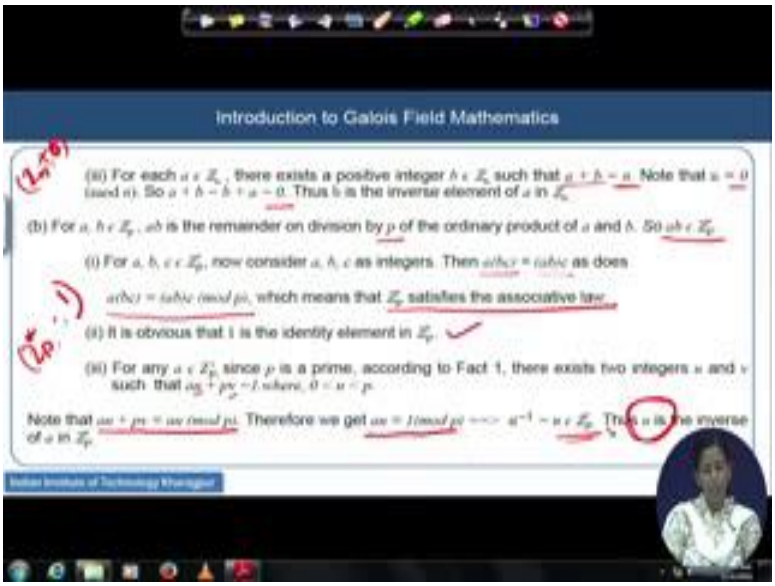
anything apart from than a. So, always it will be equal to a only. And moreover you will also find 2 other elements u and v, such that this a u plus p v will be always equal to one, where this u will vary between u or 0 to p u and also the v will vary between 0 to p. So, now, we will come back to the proof of the proposition that we did in the last slide. So, let a mod n denote the remainder of a when it is divided by the number n.

And if the result of an addition or the multiplication of the ordinary is to be reduced mod n, and then the same answer is obtained if some integers which appear are reduced mod n during the intermediate steps of the calculation. So, what is the meaning of this? Suppose I am getting a result after the addition or the multiplication of any ordinary number, which is reduced to mod n. And then same answer you will always get is obtained. If some integers which appear are reduced mod n during this intermediate calculation of this ordinary addition or multiplication of the number which is reduced mod n. It will get actually the results are coming same. Then now for my 2 elements a and b who are belonging to Z n, you will start with the a plus b and this is with respect to the first one. So, we are in we are our target is to prove that this Z n with respect to plus and the 0 is a group here we are.

So, suppose this a plus b, is the remainder on the division by n of the ordinary sum of a and b. So, definitely if it is a remainder definitely the remainder will belong to Z n, it is a where integer number. And if I take any 3 number a b c which belong to Z n and then now consider that a b c all are integer. Then if I operate in the normal operation, if additional operation if I do, for normal addition operation it holds good. If it holds good then it should be also hold good for this, means a plus b plus c should be also equal to a plus b plus c for when mod n operation is going on, for normal operation if it is true then with the mod n operation it will be also true, because we have already proof that this mod n will be after mod n operation that number belongs to the same set.

So, any a that is belonging to the Z n. So, it proves the associate, the first one proves the associative law, with modern operation. Second one if a is belonging to the Z n, and a plus 0 is equal to 0 plus a is equal to a of course, it will be always. So, 0 is always the identity element in Z n. So, identity element is also found.

(Refer Slide Time: 22:00)



Now, for each and every a that belongs to the Z n, there should exist a positive integer b, that also belongs to the Z n such a way that when this operation is going on it is equal to n. If n is we note that n is equal to 0 mod n. So, a plus b is equal to b plus a whatever you do is will be equal to 0. And such then in such a situation b is definitely a inverse element of a. So, hence you fall you could find the inverse, the identity element and you prove the associative law for this algebraic structure Z n, with respect to plus and with respect to 0. Hence it can be declared as a group. Let us see for the other one, p, Z p is the set of all the prime numbers. So, let a and b belongs to p and a b is a remainder of the division by p of the ordinary product of a and b.

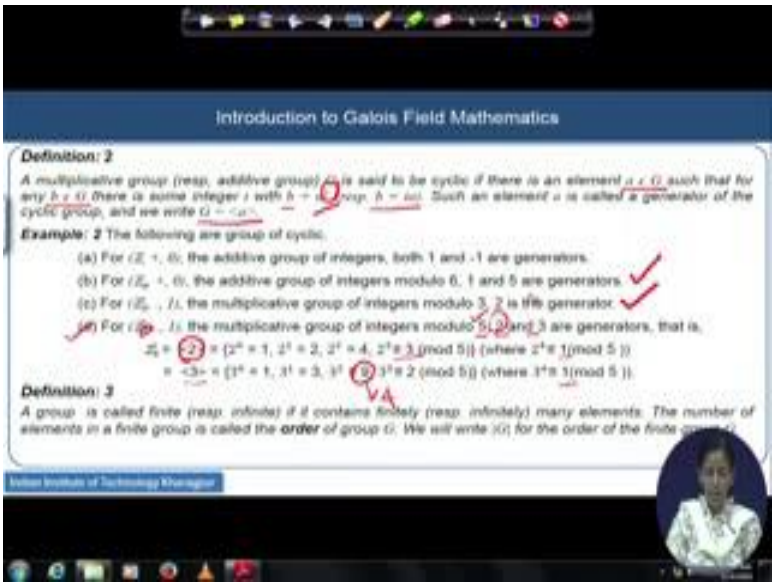
So, again by the going by the same logic a b should belong to the set Z p star. Now for a b c 3 elements, taken from the Z p star, we consider that a b c are the integers. If it is integers, then a into b c should be equal to a b into c. And it also through that the same law going by the same logic this can be also written. After modulo p operation they all belong to the same set, and hence it satisfies the associative law. It is obvious that one is the identity element because it is a product. So, wherever you go one will be the identity element for this whole set.

And for any element a Z p star which is a prime number, according to this fact one that we have declared earlier, there should exist 2 other number such u and v such that u plus p v will be equal to 1. And when you will be varying between 0 and p, and remember

that one fact that a u plus p v is also mod p a u mod p is equivalent to a u mod p. So, hence actually we will get a u is equal to 1 mod p, which will further give you that a inverse is equal to u nothing else. So, which is also belonging to Z p star, such that the u is the inverse of this any element a in Z p star. So, Z p star is also having identity element which is equal to 1, it will follow associative, all the components all the elements of this set follows the associative law.

And we have proved that it there exists a inverse element u for this set. So, hence Z p star with respect to your operators' dot and with identity element one will be considered as a group.

(Refer Slide Time: 25:01)



So, once we are here, the multiplicative group is a or any additive group. Now we understand the meaning of both of them. And it is said to be cyclic group if there is an element a which is basically a part of set G only or group G only, such that for any b any element b which also belong to G there is some integer, we could find a integer i in such a way that all the element b is can be reproduced equal to a to the power i in case of the multiplicative group, and b can be for your additive group b will be equal to i into a. Such an element a is called a generator of the cyclic group.

We write the generator of the cyclic group it is like this. It is a very important property of a group. We will take an example. For example, let us come to the example number d first. Then we will go up see this Z 5 star with respect to multiplicative operator and

identity element 1. It will be a multiplicative group and it is generator will be 5 2 and 3. How? So, with respect to 2, you see 2 to the power 0. So, what are the elements that you are having inside the Z 5 star you are having the elements up to 1 2 3 4. You cannot go beyond 5.

So, you start like this. 2 to the power 0 if you go, and you keep on increasing the value of this i, i is equal to 0 1 2 3. One by one you will be getting you're all the elements. So, 1 2 to the power 0 is 1, 2 to the power 1 is 2, 2 to the power 2 is 4 and 2 to the power 3 after mod 5 operation, the remainder will be it is basically 8, but if you divide it by 5 then it will be ending with the remainder 3. So, it is a n is this is the modulo operation that will go on the numbers. And if I increase 2 to the power 4, if I it is equal to 16, if I do the mod 5 operation I will end up with 1 which is the element of this.

So, hence you will come back to all the elements of this group if I do the modulo operation mod 5 operation on the number systems, and hence that is the best element on which you are doing that ith operation going on, that will be the generating element of that cyclic group. So, definitely it is the cyclic group, with respect to the generator 2 generating element or with respect to our generator 2. Similar stuff holds good for the elements 3. So, if I go ahead you will see that I will get all the elements back. This is equal to 3 square 3 to the power square is equal to 9, but if I do the mod 5 operation I will end with the file number 4.

And 3 to the power 27 with mod 5 operation will turn give you back number 2. 3 to the power 4 actually mod 5 operations will return you value 1. So, you are getting the values 1 2 3 4 4 only. So, 1 2 3 4 all the elements of this Z 5 star here. So, fundamentally the point is, I have not shown the calculation for your number 5, but you please do it by your own. You will be able to see that again you will be generating back all the elements of 1 2 3 4 only within this whole operation. So, we can declare that with respect to these 3 generators. This is basically a cyclic group.

Please do at home all the business with all the calculations with Z 3 star with Z 6, where I have already given the generators. But you can, but in exam there will be a question like given this kind of the group you have to find out your generator, and check whether this kind of group can be declared as a cyclic group or not. If you do not find any generator to generate all the elements inside that group, it cannot be a cyclic group. And

group the last definition in this module is related to the finite group. Group is called to be a finite group if it contains only the finite number of the elements and consecutively if a group is called to be infinite.

That means there are infinite elements inside that group. And the maximum number of the elements that you are finding inside that group will be called the order of the group. And the order of the group usually we write as mod of G for the finite group for the finite group, number for finite group actually we write the order to be written as mod G.