Spread Spectrum Communications and Jamming

Prof. Debarati Sen
G S Sanyal School of Telecommunications
Indian Institute of Technology, Kharagpur

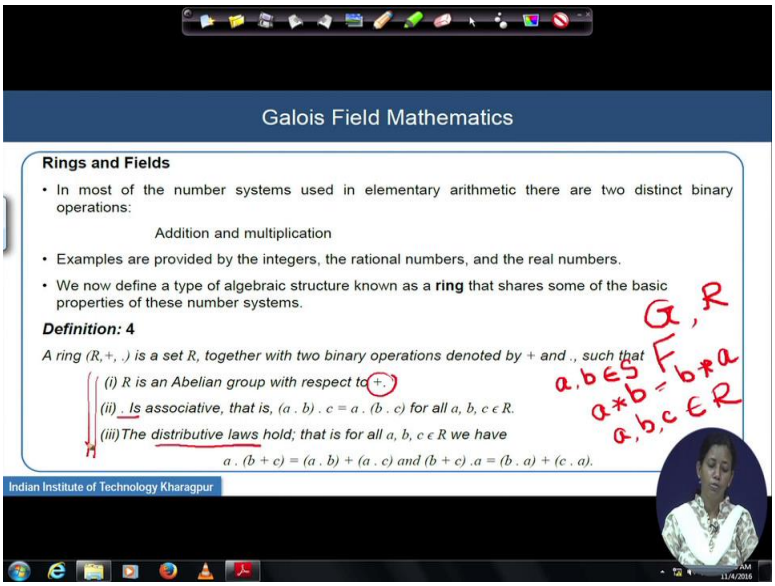
Lecture - 25
Galois Field Mathematics (Contd.)

Hello student. Today also we will continue with the Galois Field Mathematics. In the last module we have learned algebraic structure for a group. And we have seen also the several properties of a group. We have learnt how to test an abelian group. We have also at last; we have seen how to see the cyclic property of the group.

And we have also seen that a group we formed the group with respect to basically 2 operators. One is the multiplicative operator and another is the additive operator. And in the last part we have taken good example also to check the cyclic group. Some portions I left for your calculations and you are checking for checking the cyclic groups. And the example we have also taken and to check that to test how Z p star with respect to the prime numbers and with respect to the binary operator, multiplication binary operator and identity element one, how we can check and we can prove that it is a group. We have also checked that with respect to the number Z n, which is a set of the normal numbers natural numbers and natural integers, with respect to the additive operator and with respect to the binary with respect to the identity element 0, how that can form a group.

In this class, we will proceed from the group, and we will enter into ring. So, ring before entering into ring.

(Refer Slide Time: 02:01)



Let us the visit the conventional algebraic elementary arithmetic, where we are really very familiar about the 2 operation. One is the addition operation and as well as the multiplication operation. These 2 properties of this elementary arithmetic, you will find that that is having the maximum closeness or maximum resemblance in an algebraic structure in the Galois field, where actually which is called a ring. This basic property of all the elementary arithmetic, we will you will be able to see that we are recalling all those properties in the construction of a ring.

So, ring, we will write ring as a. So, usually in this whole lecture if I write G please remember that this is the symbol of a group if I write R. So, please remember that is the symbol of a ring if I write capital F, then it is a symbol of a field. So, group ring and field. So, ring is defined like this a ring R, with an operator here we have taken the both the operators plus, as well as the dot, is multiplicative operator and the additive operator. So, a ring with respect to this both the operators together, which are operated on this set are, is said to be ring if an only if R is an abelian group.

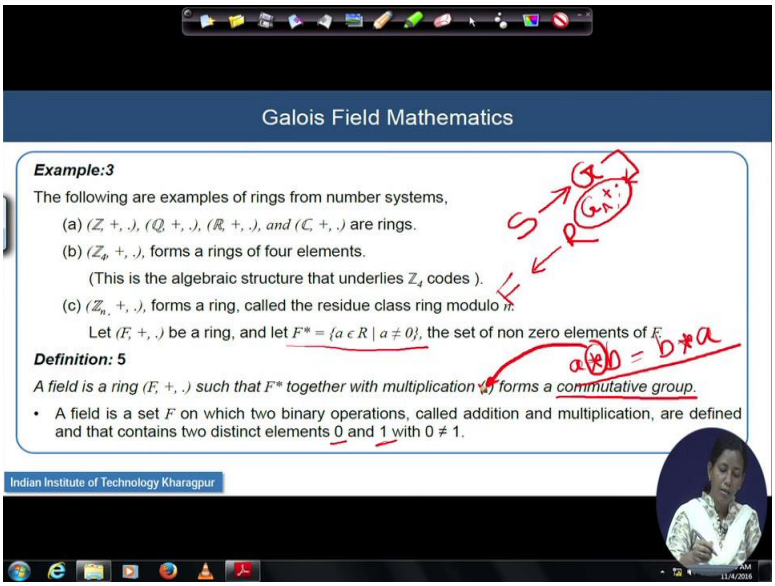
Please remember; what was the condition of declaring a group to be abelian group. We saw that we have the elements say a and b, which are belonging which are belonging to a set say S, and then if we see that the operator that is operating on that set S for that operator, this relation is true, where a star b is equal to b star a. We declared that the group is equal to an abelian group. So, ring is consisting of a set, this set should be an

abelian group with respect to the operation addition operation. So, with respect to additive operator the group needs to be proved to be an abelian group. It should say that set needs to be proven as a group and definitely that group needs to be proven as abelian group with respect to the additive operator. The set R should be proven associative with respect to the multiplicative operator such that I have taken 3 units at 3 elements from my set R.

So, a b c are the elements that belong to R, such a way that a star b is equal a star b dot c it will be a dot b star c. If it holds good. So, see the abelian group proof is coming with respect to the additive operator. The associativeness needs to be proved with respect to the multiplicative operator. So, if it is holding good, then also another law is applicable to declare some set as a ring, which is a distributive law. The distributive law says that for all these 3 elements a b c who are belonging to R, with respect to both the operators a plus and dot, this should be true. A dot b plus c should be equal to a dot b plus a dot c. And opposite thing if b plus c dot a is taken, then b dot a plus c dot a should be equal. So, 2 operators with respect to these 2 operators and if all this 3 are proven to be true, we can declare that this set is definitely a group and also a ring. So, this set is declared to be a ring, it is not only a group it is also an abelian group and also it is a ring.

So, if I tell that there exist a ring, and the background of your mind you should be able to connect, that this is also an abelian group. And they definitely it has 2 operators associated with it. And there exists the associative law and distributive law insight.

(Refer Slide Time: 07:05)



So, some example now once again; the set of real numbers, set of the integers, set of the real numbers, set of the complex numbers, rational numbers with respect to both the addition as well as the multiplication operator, they are all the rings. So, we are well known about the set if I take the set of all the complex numbers the rational numbers the real numbers and the normal integers, we will have said they are forming the ring with respect to these 2 operators. And we widely use actually this sets in our day to day life and then any other application of the mathematics elementary arithmetic.

Z 4 which is the set of the natural numbers after modulo n or modulo 4 operations. That set with respect to your additive operation as well as your multiplicative operations it forms another ring. And definitely how many elements will it have? It will have 4 elements only. If we come down we proceed from Z 4 to Z n, which is a basically after modulo n operation the set of the natural the set of the natural numbers, and that with respect to your additive as well as the multiplicative operator will also form a ring.

Now, let there is F plus dot. It is a ring associated. It will be called a ring. It is a ring basically and let F star, which is also where the element of all the field is actually all the set the elements of all the set of this F, which are a. They belong to this ring R given that is not equal to 0 and the set of the non 0 elements of a. So, let F be a ring then F star which is formed from F, and taking all the where all the elements belonging to R, and a is not equal to 0. It is also a set of the non 0 elements of all the F. If I start with a ring and

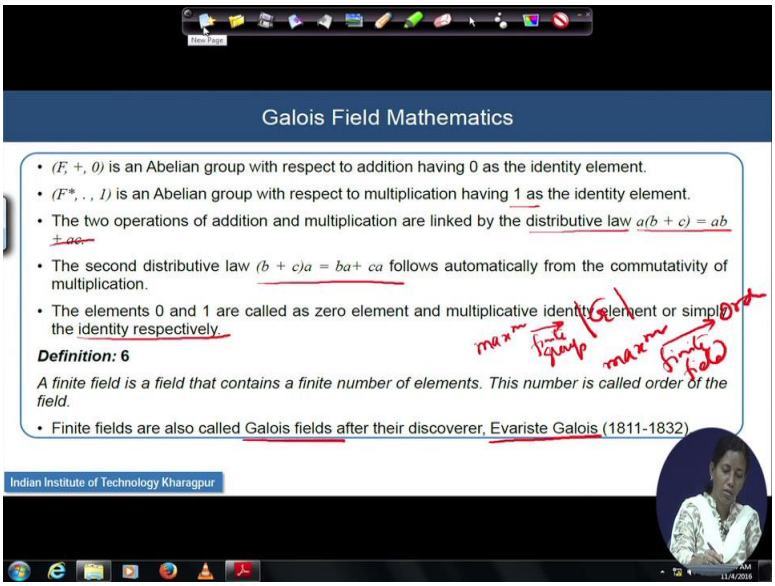
I can form actually F star by taking all the non 0 elements of this F. So, next definition the field is a ring such that a field can be a ring also such that the F star together with this multiplication is a commutative group.

So, to be commutative abelian group again we know that all the elements show with the respect to an operator should follow this expression should follow this relation a star b is equal to b star a. Here this star is basically with respect to the multiplication operation. So, you take a field which is F with respect to your addition operation and dot operator, and you take all the F star. How will you construct F star following this rule F star will be follow constructed following this rule and then with F star and F if I see actually that with respect to multiplication operation, they are commutative rule follows then we can say that this field can be also a ring.

A field it is also a set. On which this 2 binary operators called this addition and multiplications are defined. And that contains 2 distinct elements also which is actually 0 and 1. So, we came from the relation like this. So, we started with a set S. So, S with one or one operator either plus or dot we turned to be a group. A group with it is certain properties, I mean a set a group definitely a special kind of the group which is said to be abelian group if it is, and with the 2 operators we turn to be a ring. With ring from ring we came to field now.

So, if I see a field is also a ring. If we set ring is also a group. Definitely a field is a ring field is also a group and field is also a set. So, in the structure algebraic structure of the field if whatever the property a ring is satisfying it will be able to see, that all property of a group is satisfied in field all the property of a ring is also satisfied in a field. In addition, the field with field needs to prove and commutative group with respect to it is another set F star with the respective multiplication operation. So, that is the another constrain to declare a ring to be a field.

(Refer Slide Time: 12:28)



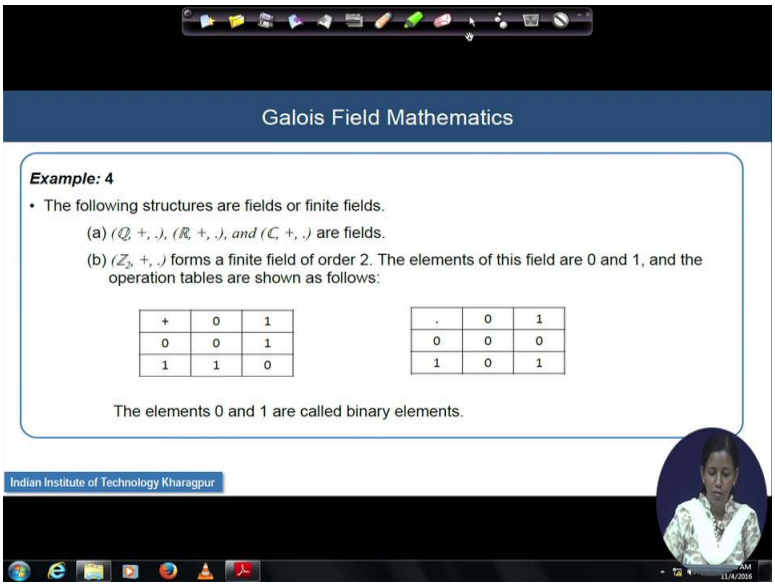
So, few more definitions and understanding F the field with respect to your additive operator and the 0 identity element is an abelian group. And with respect to abelian group with respect to some addition an having 0 as the identity element there. If star with respect to my multiplicative operator and identity element 1, it is also an abelian group with respect to multiplication and having 1 as the identity element. 2 operations like your which will have linked by the distributive law 2 operators and in this dot and this plus they are linked they can be linked with to prove the distributive law. The second distributive law that b plus c into a is equal to b a plus c a it follows automatically from the commutativity of the multiplication. And the elements the 0 and 1 they are called the 0 element and multiplicative identity element or simply the identity elements with respect to the operators.

So, with this field understanding of the field the question comes what is the definition of a finite field. So, we saw that a finite group will be constituting of finite number of the elements. In group also we saw there is a definition of finite group, infinite group and hence the order of the finite group there is no order in the infinite group definitely, but there is something called the order of the finite group. And similarly in a field also we will define the finite field, a field which contains all the finite number of elements will be called as a finite field. And the number of the elements maximum number of the elements that you are constituting or you are seeing inside the finite field which is called the order of the field. So, the maximum number of the elements that we see in a group in

a finite group, is the is a order of the group we saw we write it like this. So, maximum number of the elements that we find inside the finite group is the order of the group. And the maximum number of the element that you see in a finite field is also the order of the field.

So, this finite field was discovered by Galois. And that is why the field is named after him and we call it Galois field. So, that is why the name is. So, basically they had the finite fields which we are talking about and it goes after his invent the name of his inventor Galois.

(Refer Slide Time: 15:37)

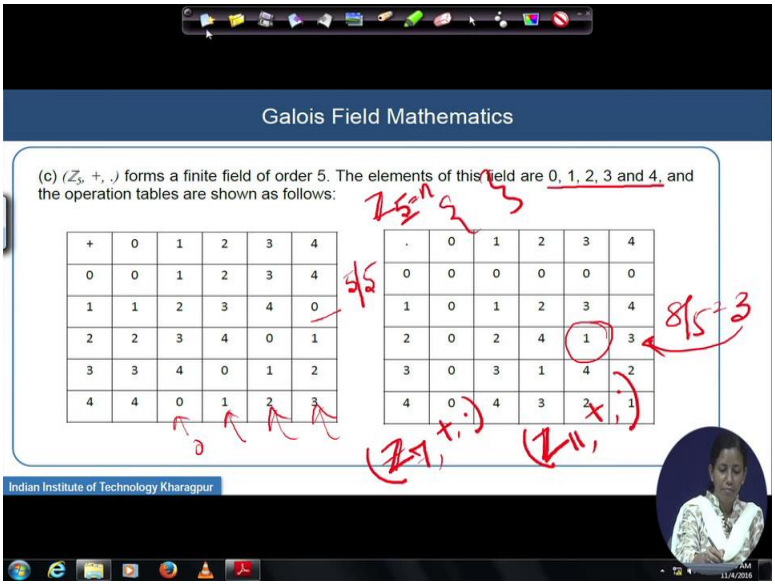


This is the time to take some example. We will see that there are the well-known sets which in form of with respect to other 2 operators can form the finite fields. Real numbers, with plus and minus operator they are complex set of complex numbers with respect to the additive operator and multiplicative operator of field. Q with respect to the positive operator as well as is as the multiplicative operator is also a finite field.

We will take an example of the natural numbers of with modulo 2 operations on it, with respect to your plus and dot operator, to see actually that it is a finite field of order 2, and then let us see the elements of this field and how the table operation table on it will be generated. This is a very well-known operation that we do in the first class of then a digital communication circuit and when we study all the gates in the digital communication and digital circuit also. So, the elements of this field Z 2 are only 2 and

though they are 0 and 1. So, with respect to plus and with respect to dot operators we will try to see how actually the operators are operating over the elements of this group, over elements of this field. So, this 0 and 0 with respect to the add operation it will lead like this and with respect to the dot operator it will lead like this. So, 0 and 1 are basically the binary elements of this field.

(Refer Slide Time: 17:39)



This is very simplistic example we started with and then let us see with higher number of the elements of a group and also of a field. Suppose we start with a Z 5 plus dot what is the meaning of it is, this Z 5. So, you take a set of the natural numbers and you each and every number you are dividing with the mod with the with 5 the n equal to 5 here, and whatever the remainder you are ending up with, you are then taking the n in a typical set. If that is the situation and then the elements of those fields are definitely you will be getting with 0 to 4, and the operation tables that we have shown here for both the operators are given by this.

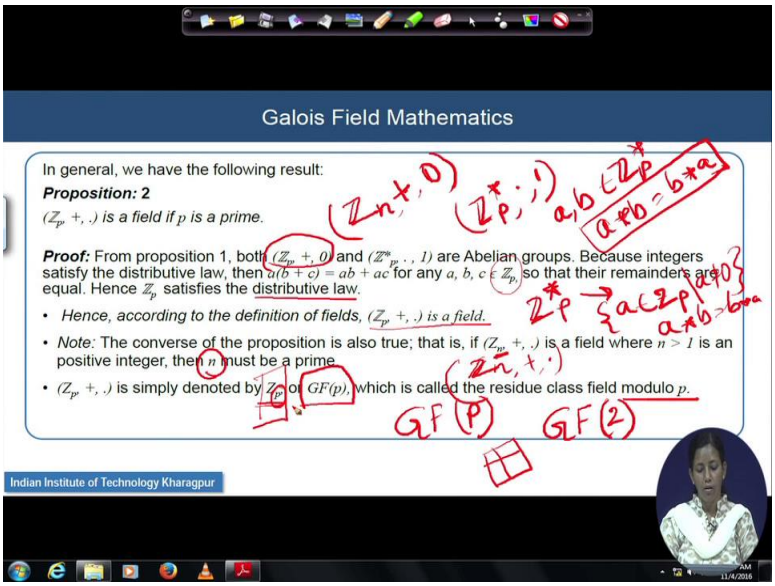
So, see with respect to the 0 the first row of the addition we understand. Once actually the operation with 1 is coming up now see beyond 3 when the addition is coming 5 which is not at all a number of this field element of this field. If we apply the modulo 5 operations for all this addition definitely it will come down here as 0. So, some operation after operation you are dividing it with a mod number you are ending up. So, currently if I come here. So, after this 4 plus 1 5 you are starting with the zeros and hence actually

this are all the remainders of the addition, after addition you are doing the mod operation, modulo operation. And you are ending up with all those numbers that is the way the whole operation table is written.

Now, I hope you have understood that the way the operator will operates it like this. Every element 5 element you do with respect to addition it is. So, you add the numbers and then divide it with the mod small n value with which actually it is constructed with. So, 0 plus 0 divided by 5 will lead you 0 no remainder remaining. And the you are done here the remainders are 0 only. The remainders will be 1 2 3 and zeros only, but once you are up to 4 you are fine, but once actually you are doing with one you are trying to add all of them. Because that is the way actually you have to perform the operation table. Once you are crossing the number added number with equal to greater than equal to 5 then your number will keep on changing your remainder values will keep on generating and you are filing it up with that.

The same thing holds good for multiplication. Multiplication with zeros in the first row will lead to you 2 0. With 1 will lead you to up to 4 with 2 you are fine, but to your 4 I mean 2, 2s are, but in this portion you are not because you have crossed the number 5. So, the remainder one will be 6. And you are ending up with the it remainder will be 1 and you are ending up with where. So, 4, 2s are 8 divided by 5 you will you the remainder 3. So, you are ending up. So, that is the way the whole operation table is filled up. You can try at home with some higher one. Suppose if it is a natural number with the mode 7 modulo operation 7 with respect to plus and dot operator try it out, to prepare this whole table, you can also try with some higher number we say Z 11, with respect to plus and dot and then you try to fill up all the tables.

(Refer Slide Time: 21:28)



So, in general we will find that they are 2 following results are generating. Proposition number 2 is Z p with respect to dot and we always respect to dot and with respect to plus and then it is a field, if an only if p is a prime. So, Z p any way we have learnt that if we write Z, Z is a set of the natural numbers and if I write it is p; that means, it is prime module after modulo p, p is the prime number and after the operation of the prime numbers on the numbers set, whatever the remainder is I am taking them out, and with that only I have prepared the set. That set with respect to your addition and the dot it is a field if an only if the p is the prime number. So, we have to proof that number one that it is to, I to come to be a field we have to proof that they are the follow all the properties of the field definitely.

So, from proposition 1, that we did earlier here, which we discussed in the last module, also I have not reproduced it here. We have also seen in the proposition 1 that Z p with respect to dot with respect to your additive operator and your identity element 0, and Z p star with respect to your multiplicative operator and your identity element one both are the abelian groups. If you remember that once we completed the description of our group, we prove this. We prove this and we also prove necessitation with that we also proof Z n dot 1, we also proved that Z p star dot 1 is a group we prove that Z n with respect to 1 and 0 and Z p star with respect to dot and 1 they are the groups. And we also in this process it was easy and we have also talked about that they are also the abelian groups; that means, all the elements of them each of them which belongs to either Z p or

Z n in case of my Z p star. If it belongs to the Z p star all that it Z p or elements they belong to this prove this this typical relationship. So, they were the abelian groups. So, we proved that they are the groups and we also there this relation holds good. So, they were the abelian groups also.

Extending the same logic, you can also show that the Z p with respect to your plus and 0 is also and abelian group. So, from the proposition we understand that the both of them are the abelian groups. And because all the integers, any integer value they satisfy the distributive law, such that this will hold good I mean a in to b plus c, if you do you will be ending up with a b plus a c, for any a b c which belong to the Z p. So, you can take an example also and you can see that this distributive law holds good for this Z p. So, that their remainders are all equal. So, hence this Z p satisfies the distributive law.

So, over fast criteria, to declare to be a field that is that that it should follow also the property of a ring. And in ring we saw that only the associative law it was not sufficient, you should be allowed it should be able to show that it is it follows the distributive law with respect to both the operators. So, with respect to both the operators here I am seeing that actually the components of this Z p. Set Z p they satisfy the distributive law. And according to the definition of the fields; this is also a field that we did earlier. The definition of a field says that you have to have another set prepared from this field from the ring if it is a ring already. So, Z p star where all the elements will be part of that ring earlier ring Z p, and given that a is not equal to 0. And the element by element wise it will form a commutative law.

So, the commutative law for the prime numbers is already proven. And hence we can declare that Z p with respect to your plus and dot it is definitely a field. Note here that one part is left. The converse of this proposition is also true that, if set of the natural numbers it should be written like this. If the set of the natural numbers with respect to the plus operator and dot operator is a field, where your n is greater than 1, and n is a positive integer, then n must be prime. I mean for if the p is the prime number then this is the field, this is the forward proof. And if this is the field, if given this is the field and n is the any greater than one number then to prove that it will be a field, definitely to proof that this should be a field. N should be a prime number.

So, it is vice versa. And we understand that this Z p plus n dot is simply denoted by Z p for either will be denoted simply by the Z p or we will write it as a Galois field p. So, remember that which is called the residue class field of modulo p whatever you say, because this is the modulo p operation on your natural numbers. So, when we write that the Galois field 2. So, it means that it contains the only 2 binary numbers only 2 numbers zeros and ones. And those numbers are the prime numbers and we can actually construct all the typical sets and all the typical working tables with respect to both the operators.

So, from now onwards when we will talk about the fields; so if they are the finite fields and they are of what is the modulo operation going on that field, we will either write in this form and preferably by the G F p, stating that these are the finite Galois fields with this with respect to their prime number p.