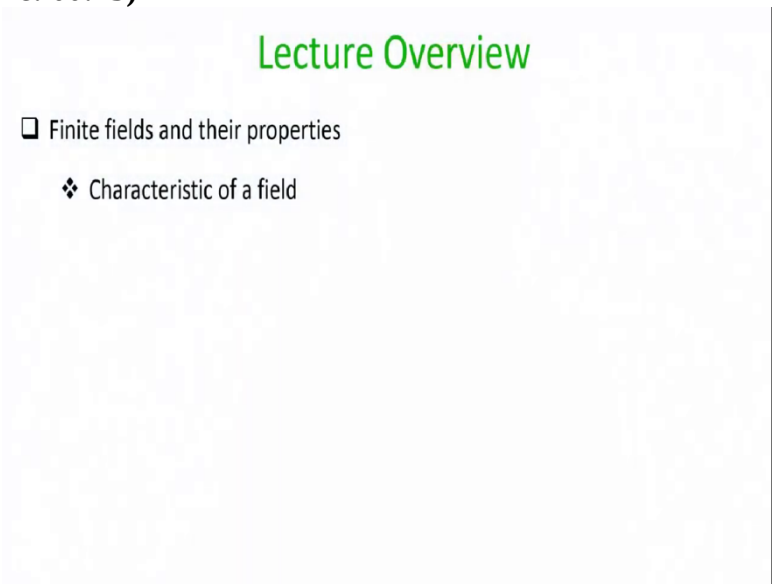
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

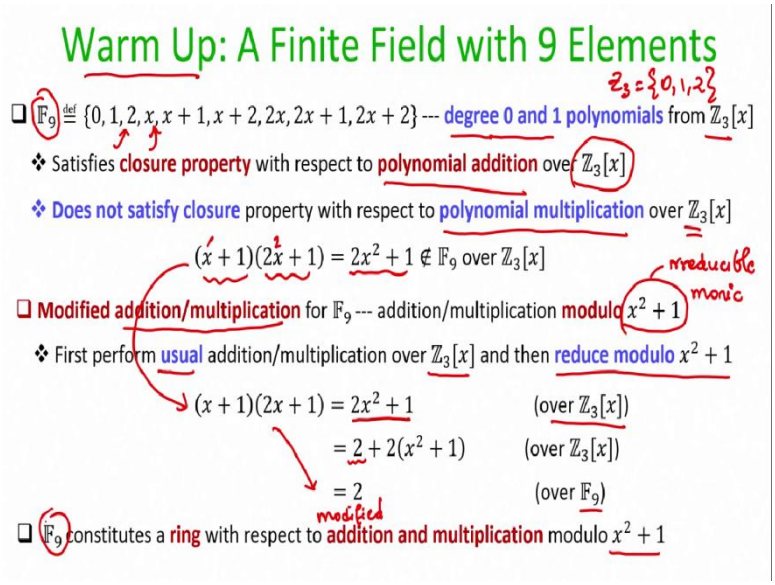
Lecture - 68
Finite Fields and Properties I

(Refer Slide Time: 00:23)



Hello everyone, welcome to this lecture. The plan for this lecture is as follows. In this lecture, we will discuss finite fields and their properties specifically we will discuss the characteristic of a field.

(Refer Slide Time: 00:33)



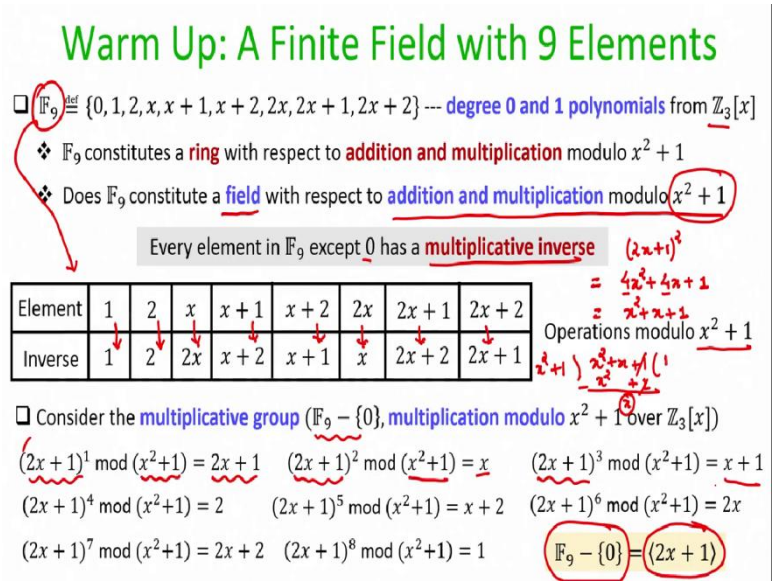
So, let us do some warmup and see how exactly we construct finite fields. So we will see a construction of a finite field with 9 elements. I denote set $\mathbb{F}_9$ which is a collection of these polynomials. So, these are basically polynomials of degree 0 and degree 1 where the

coefficients are from $\mathbb{Z}_3$ and remember $\mathbb{Z}_3$ is the set { 0, 1, 2 }. So, you can see that, if I consider the operation of polynomial addition over the set $\mathbb{Z}_3[x]$, then it satisfies the closure property namely, you take any 2 polynomials from this collection and add them you will get again a polynomial in the same set F_9 but it turns out that with respect to the operation of polynomial multiplication, the closure properties not satisfied namely, suppose I take these 2 polynomials (x + 2) (2x + 1) and if I multiply them, then remember that when I multiply polynomials over fields where my field is $\mathbb{Z}_3$, then the degree of the product polynomial will be the sum of the degrees of the individual polynomials. So, I have degree 1 polynomial here degree 1 polynomial here, so that is why the sum of the product polynomial will be 2 and this polynomial is not a member of the set F_9. So, that is why now, what I am going to do is I am going to define a modified addition and multiplication operation, where I will be doing all the addition and multiplication of the polynomial as I was doing earlier, but my resultant answer will be computed modulo this polynomial ($x^2 + 1$) and if you see closely here this is an irreducible polynomial; irreducible monic polynomial actually. So, the modified operation namely addition and multiplication is the following: I first do the usual addition and multiplication over $\mathbb{Z}_3[x]$.

And then I do a modulo $x^2 + 1$ and that will be my resultant answer. So, for instance, if I again perform the multiplication of these 2 polynomials over $\mathbb{Z}_3[x]$ as I said, I will obtain this polynomial ($2x^2 + 1$), but now what I am going to do is I am going to divide this polynomial by my $x^2 + 1$ and focus on the remainder. So, if you see $2x^2 + 1$, I can express as 2 times $x^2 + 1 + 2$.

So, 2 will be the remainder polynomial, namely the constant polynomial and hence as per the modified multiplication operation the product of these 2 polynomials will be 2 which is now a member of the set F_9. So, it turns out that with respect to the modified addition and multiplication operation namely addition and multiplication modulo this irreducible polynomial the collection F_9 satisfies my ring axioms.

(Refer Slide Time: 03:53)



Now, I would be interested to check whether this collection F_9 indeed satisfies the axioms of field as well, with respect to the addition and multiplication operation modulo this irreducible polynomial. And for field axioms we need that each non-zero element should have a multiplicative inverse. So I have to check whether every element of this set F_9 except the element 0 whether it has a multiplicative inverse.

And it turns out that indeed each non-zero element of this set F_9 has a multiplicative inverse. So, for instance the multiplicative inverse of 1 is 1 because if you multiply 1 with 1, you get 1 and then if you do a modulo $x^2 + 1$ you will get 1 in the same way, inverse of 2 is 2 because 2 into 2 is 4 and 4 you will first reduce over $\mathbb{Z}_3$ you will get 1 and then if you reduce 1 modulo $x^2 + 1$ you will get 1.

If you do the product of x and 2x you will get $2x^2$. Now, the coefficient 2 when reduced within $\mathbb{Z}_3$ will give you coefficient 2 itself and now if you reduce $2x^2$ modulo $x^2 + 1$ so, you will first multiply with 2; you will get this $(2x^2 + 2)$ and now, if you do a subtraction you will get -2 but -2 over $\mathbb{Z}_3$ is actually plus 1 which is the identity element; multiplicative identity.

So, like that you can verify easily that under each element I have written down its corresponding inverse element and each of the inverse element is actually a member of the collection F_9. So, that means each of the non-zero element here indeed has a multiplicative inverse. So, now I want to show you some another interesting property of this field F_9.
So, we have already proved now that this collection F_9 satisfies the field axioms with respect to the addition and multiplication operation modulo this irreducible polynomial, I have not

shown you the distributive property namely, addition distributes over multiplication. But it is easy to verify that, but I would like to show you another interesting property of this field. So, here I am going to focus on all the non-zero elements of this set F_9.

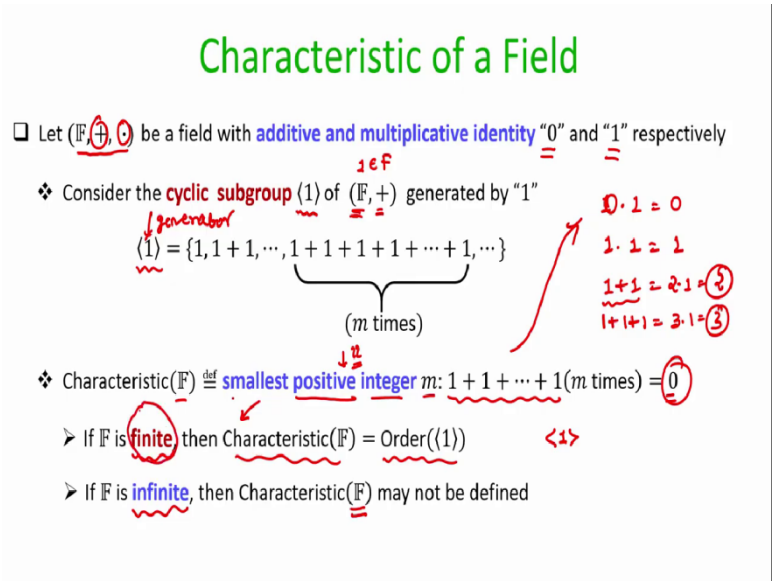
And now, what I have computed here is the following I have computed various powers of this element $2x + 1$, of course, modulo the irreducible polynomial. So, the polynomial $2x + 1$ power 1 will give you the same element $(2x + 1)^2$ modulo $x^2 + 1$ will give you what x so, if you want to verify that let us do that. So, you have $(2x + 1)^2$ so, you will first expand it so, you will get $4x^2 + 4x + 1$.

But each of the coefficients has to be first reduced over $\mathbb{Z}_3$ so 4 becomes 1. So, you get x^2, 4 becomes 1 again. So, you get x and then you get +1 and now, you have to reduce $x^2 + x + 1$ modulo $x^2 + 1$ that is the way we have defined our modified multiplication operation. So, you will get $x^2 + 1$ and now, if you subtract you get x; 1 and 1 cancels out.

Now, you cannot further divide x by $x^2 + 1$ because the degree is less. So, x will be the remainder. In the same way $(2x + 1)^3$ will give you $x + 1$ and so, on. So, what I have shown here is if you take the various powers of $2x + 1$ and compute the powers as per the modified multiplication operation, then you get basically all the non-zero elements of this collection F_9.

That means, I can treat this element $2x + 1$ as a generator which can generate all the non-zero elements of this collection F_9 and as per our notation of generators and cyclic group I can basically say here that if I consider the field F_9 and focus on the multiplication operation modulo $x^2 + 1$ then it is actually a cyclic group where $2x + 1$ is a generator. I will touch upon this fact later.

(Refer Slide Time: 09:05)



But this was just for your demonstration. So, now next we want to define what we call as characteristic of a field. So, imagine you are given an abstract field. So, this is your abstract plus operation and abstract dot operation; need not be your integer plus and integer dot operation and my elements 0 and 1 are the additive and multiplicative identity respectively. Again they are they need not be the numeric 0 and 1.

They are the representation of your additive and multiplicative identity element. Now, what I am going to focus on is the following. I will see what are the various elements I can generate as per the dot operation from this multiplicative identity element 1. I will be focusing on the cyclic subgroup as per the addition operation. So basically, I am going to add 1, 0 times, which will give me the element 0, so 0 times 1 will give me 0, 1 times 1 will give me 1 and 1 + 1 which is same as 2 times 1 will give me 2, 1 + 1 + 1 3 times will give me 3 times 1 which is same as 3 and so on. Again I am using; I am denoting 2, 3 as results but this may not be the element numeric 2, numeric 3 they are basically representation of the result of adding the multiplicative identity 1 to itself.

So, if I focus on the cyclic subgroup namely the various elements which I can generate by adding the element 1 to itself several times then that will be a subgroup of my original group. So remember, this collection F with respect to the plus operation constitutes a group, because that is one of the axioms of the field and since, I am taking an element 1 belonging to the set F and computing the various powers.

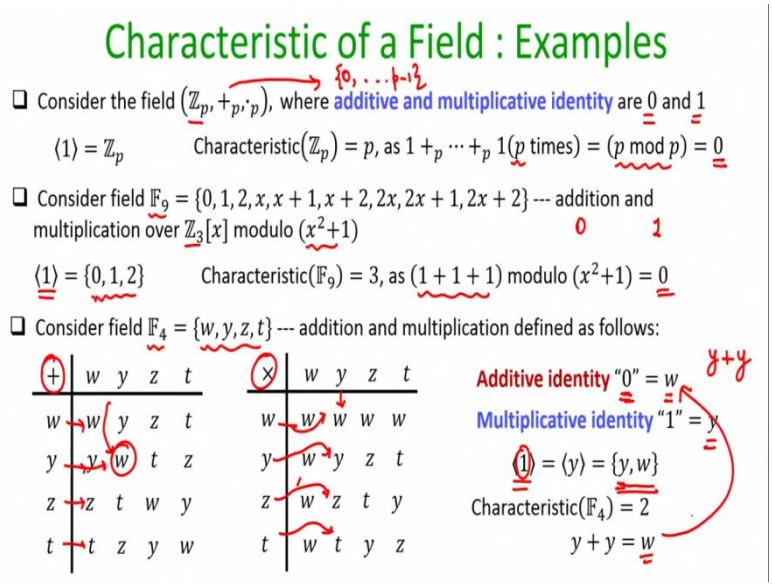
Then as per the rules of group theory, this will be considered as a subgroup and it will be a cyclic group where 1 is the generator. So, the characteristic of the field is the smallest

positive integer m such that 1 the multiplicative identity, 1 is added m times I get the element 0. So, why I am focusing on the positive integer and why not 0 is allowed here? because as per the definition here, 0 times 1 will of course, give you the element 0.

So, that is why I am interested in the smallest positive integer. So, it turns out that as per the definition of our characteristic, if your field F is a finite field then of course the subgroup; the cyclic subgroup generated by the element 1 also will be finite and in that case, what I can say is that the characteristic of the field is nothing but the order of the cyclic group generated by the element 1.

Because, whatever is the number of elements generated by this element 1 say if there are m number of elements that means, starting from the 0th power to the (m – 1)th power, I can generate all the elements and then as soon as I take the mth power, I will get back the identity element namely 0. Whereas, if the field F itself is infinite and the characteristic of F may not be well defined. So, typically we will be interested in the characteristic of a field when our field is a finite field.

(Refer Slide Time: 13:17)



So, let us see some examples of characteristic of a field. So, let us first take this example, namely the field consisting of the elements 0 to p - 1 that is my set $\mathbb{Z}_p$ and my plus operation is addition modulo p and my multiplication operation is multiplication modulo p and here the identity elements are indeed the numeric 0 and 1 respectively, the additive and multiplicative identity elements.

So, now let us try to find out the characteristic of a field. So, for that we have to focus on the size or the order of this subgroup namely the subgroup generated by the element 1 and if I consider the subgroup generated by the element 1 it will be the entire $\mathbb{Z}_p$ because 0 times 1 will give you 0, 1 added to itself only once we are going to give you the element 1. 1 added to itself again we will give you 2 and so on. So basically the characteristic here will be p because if I add 1 to itself p times and remember by add I mean addition modulo p. So, if I add 1 to itself p times the result will be p and p modulo p as per the plus modulo p operation will give me the element 0. So that is why the characteristic of this field will be p. Now let us consider the field that we had constructed at the beginning of this presentation, this lecture, this was the field consisting of 9 polynomials of degree 0 and 1 over $\mathbb{Z}_3$ and all my operations are modulo $x^2 + 1$ then here the additive identity is the numeric 0 or the constant polynomial 0 and the multiplicative identity is the constant polynomial 1. Now if I want to find out characteristic of the field F_9 basically I have to find out the size of the cyclic subgroup generated by the element 1.

And it is easy to see that subgroup generated by the element 1 will be the constant polynomial 0, polynomial 1, and polynomial 2. So there are 3 elements that is why the characteristic will be 3 indeed if you add 1 to itself thrice you will get 3. Now if you reduce 3 modulo 3 you will get 0 and now if you 0 modulo $x^2 + 1$ you will get the element 0. That is why the characteristic of this field is 3.

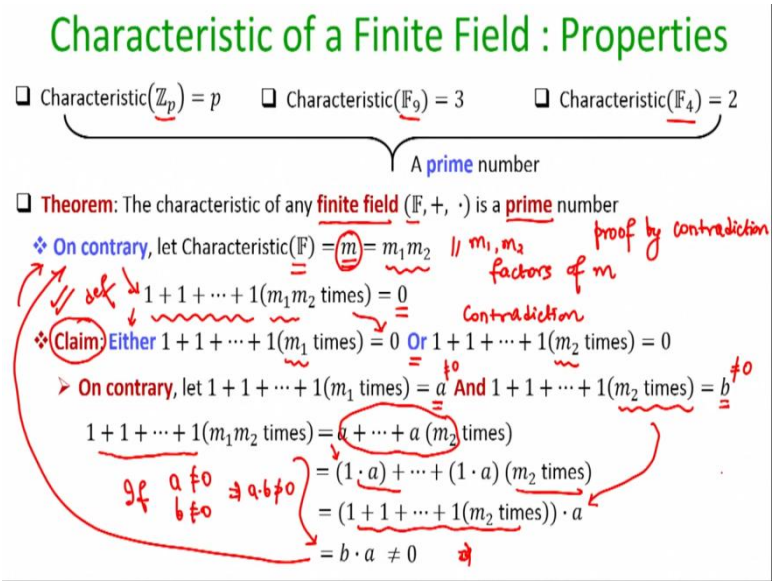
Let us consider an abstract field F_4 where my elements are letters here w, y, z and t. And now I define an addition and multiplication operation as per this table. So this table basically tells you the result of performing the plus operation and multiplication operation. So for instance if I consider this entry. This entry basically means that if I add y and z then my result is t. In the same way as per the multiplication table, the interpretation here is that if I multiply $\mathbb{Z}$ with the w my result is w and so on. That is the definition. That is my definition of the plus operation and the dot operation here and it is easy to verify that all the field axioms are satisfied: the closure property with respect to the plus is satisfied because you take any 2 elements of this collection F_4 and add them you will get again an element of the collection F_4.

Similarly dot or multiplication is closed. And you have the identity elements here. Let us identify the additive identity element 0, what exactly is the element 0 here the element 0 here is actually the element w, because you add w to any element you get the same element back so you add w with w you get w you add w to y you get y and so on. So even though w is additive identity whenever I want to refer to additive identity instead of saying w I will use the notation 0.

In the same way the multiplicative identity here is y because if you see the column under y in the multiplication table each element when multiplied with y gives you back the same element. So now what will be the characteristic of this field so finding the characteristic of this field; since the field is finite I will basically focus on the cyclic subgroup generated by this multiplicative identity element namely the elements generated by various powers of y.

So 0th power of y will give me the element y itself and y added to itself as per the additive table gives me the element w and that is all after that I cannot generate any new element. So that is why since there are 2 elements here the characteristic of this field is 2 and indeed you can check here that y additive to itself will give you the element w which is my 0 element.

(Refer Slide Time: 18:52)



So that is the definition of characteristic of a field. So we have seen examples of 3 fields in this lecture, the field $\mathbb{Z}_p$, the field F_9 and the field F_4 and the characteristic of each of these fields is a prime number. Now, you might be wondering, is it accidental, or is it in general always a case. So it turns out that this is not accidental and indeed, this is the case for every

finite field. So we can prove the following. That if you take any finite field F with an abstract plus and dot operation.

Then it's characteristic is always a prime number. It cannot be a composite number and at least the theorem is true with respect to the examples that we had seen already in this lecture. So now let us try to prove this theorem. So the proof will be by contradiction. So the theorem says that the characteristic should prime number but as per the proof by contradiction strategy, I will assume the contrary and I will assume that the characteristic is not a prime number. If it is not a prime number; so it is not a prime value then it will be composite. So let characteristic be m and suppose it is a composite value. Since it is a composite value it will have prime factors or some factors. So let m_1 and m_2 be the factors here and none of them is actually m because that is the definition of a composite number.

Now since the characteristic is m where m is the product of m_1 and m_2 that means in the field F, the element 1 when added m_1 m_2 times will give you the additive identity is 0. That is that comes from the definition. Now if this is the case then I am going to prove that either the element 1 added m_1 times will give you the element 0 or the element 1 added to itself m_2 times will give you the element 0.

That is what I am going to show next. Assuming that this claim is true then this goes against the assumption that the characteristic of the field was m_1 times m_2 because if 1 added to itself m_1 times gives you the element 0 then it implies that the characteristic is m_1 or if 1 added to itself m_2 times gives you the element 0 then that means the characteristic is m_2 and both m_1 as well as m_2 are individually less than m.

So that goes against the assumption that the characteristic of the field was m_1 times m_2 at the first place. So everything now boils down to proving this claim. That means assuming that 1 added to itself m_1 m_2 times gives you 0, I have to show that either this statement is true or this statement is true. And again I will use a proof by contradiction to prove this claim. So my goal is to show that 1 added to itself m_1 times or 1 added to itself m_2 times gives you 0 but on contrary assume that 1 added to itself m_1 times gives you a non-zero element a.

And 1 added to itself m_2 times gives you another non-zero element say b. Now if that is the case I have to arrive at a contradiction somehow and how do I arrive at a contradiction, so I utilize the fact that 1 added to itself m_1 m_2 times can be splitted as follows: I can say that let me add 1 to itself and m_1 times and then again let me add 1 to itself and m_1 times and then again let me add 1 to itself m_1 times.

And like that if I do this operation of adding 1 to itself m_1 times total m_2 times that will give me the effect of as if I have added element 1 to itself m_1 m_2 times. Now as per my assumption 1 added to itself m_1 times will give me a non-zero value a. In the same way the next operation of element 1 added to itself m_1 times will give me again element a and in the same way the last operation of performing the addition operation over the element 1 m_1 times will also give me the element a.

So what I can say is that the result of adding 1 to itself m_1 m_2 times is equivalent to adding this non-zero element a to itself m_2 times. Now what I can say is the following since the element a is a non-zero element I can say that as per the definition of multiplicative identity if I multiply the element a with the multiplicative identity namely the element 1 I will get the element a itself. So I can write a as dot of 1 and a and like that each of the a I can replace by 1 dot a and how many times I can do that: m_2 times. Now remember I am considering right now a field and over a field the plus and the dot operation satisfies the distributive property. So what I can say is the following I can take out this dot outside and distribute; inside I can collect all the plus.

And how many plus I have inside? m_2 because this whole operation of 1 dot a was performed m_2 times. Now I utilize the fact that 1 added to itself m_2 times will give me the non-zero element b that means this value is nothing but b and overall I get the conclusion that 1 added to itself m_1 m_2 times gives me the element b dot a and b dot a will not be 0 because as per my assumption a is not equal to 0, b is not equal to 0 and recall in a field if you have 2 nonzero elements then their dot is also not 0. So since b dot a is not 0, I get a contradiction that the characteristic of the field is m_1 m_2 because if the characteristic of the field was m_1 m_2 then the result of 1 added to itself m_1 m_2 times should give me the element 0. But what I have shown here is that 1 added to itself m_1 m_2 times is not 0. So I get a contradiction and that shows that my claim is correct and since my claim is correct, then that contradicts the assumption that I made here namely the characteristic is a composite number. That is an incorrect statement

that means the characteristic m was actually a prime number. So with that I conclude today's lecture: just to summarize in today's lecture we discussed about the characteristic of a field and we proved that if your field is a finite field then its characteristic is always a prime number.