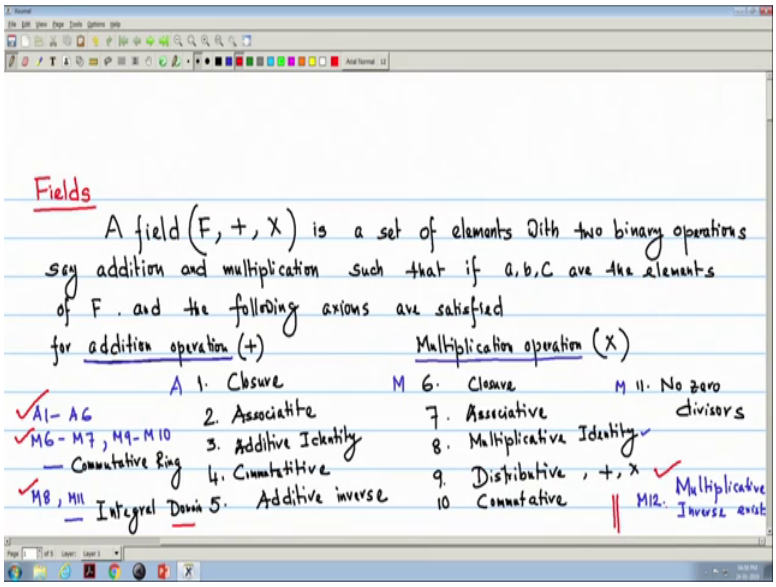
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 56
Finite Field and Applications

Today we will read the fields one algebraic systems and in particular our emphasis will be on finite fields, because as real life applications there are numerous application areas that where finite fields are used, particular that cryptography and the coding theory well mainly the finite fields are used. So, first we did that the field.

(Refer Slide Time: 01:02)



Since already we have read the number of algebraic systems and there we have seen that a; the general properties that they hold. Now, we based on those properties that we try to define the algebraic system field. So, a field F and normally a field is also with two binary operations like ring. So, we if we write that as if the addition and the multiplication is a set of elements with two binary operations like ring that we have read last day, say addition and multiplication, but as already we have read, we have seen that this addition and multiplication may not be the ordinary addition and multiplication.

And such that if a, b, c are the elements of F then the; and the following axioms are satisfied. If we remember that the these axioms are the properties that are the mainly the closure property, the associative, the identity element must be there and when we are

considering two binary operations then distributive property must be hold. So, if we see those properties say for addition we can write; that means, for addition operation now properties are say closure, then it has the associative, then it has additive identity should be there, then it must be commutative and additive inverse exists.

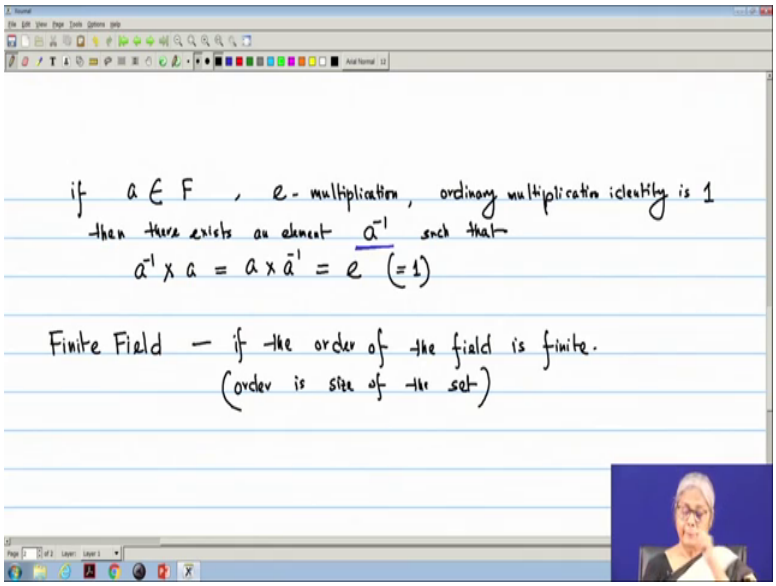
So, this is when we consider the addition operation and addition operation that is my here we have considered it is plus. Now similarly if I consider the; because field on field there are two operations are there. So, if I consider the multiplication operation; for multiplication operation then I should have the closure; that means, it should be closed under multiplication, then associative with respect to the multiplication operation, then multiplicative identity should be there, now the distributive property should be there, so, it should be distributive.

Now, if the multiplication is commutative then it can be a commutative ring, now we can also see that integral domain; that means, if it is multiplicative identity and the no divisors; that means, if I add another property we have seen that multiplicative identity and no divisors; no zero divisors; then it can it is the integral domain. Then it is so, we have seen that if it is say additive property we can write that it is A multiplicative M. So, if it is A 1 to A 6 it holds; then I can write M 6 to M 7 and M 9, M 10 then it is I can tell this is commutative ring that we have read lasting.

And now if I add two more that M 8 that multiplicative identity and the M 11 the no zero divisors then I can tell that this is the integral domain.. Now see for when we have considered the addition operation we have considered that additive inverse, but when we have considered all the multiplication operation the properties which are must be obeyed under multiplication say here closure, associative and multiplicative identity for integral domain it can be commutative and distributive when both addition and multiplication we have considered. So, distributive for both addition and multiplication, but multiplicative inverse we have not considered.

So, here for the field that in addition that must multiplicative inverse it must satisfied. So, we can write the additional thing that M 12 is the multiplicative inverse exist. So, over the properties satisfied by the competitive ring and the integral domain, if we see that multiplicative inverse exist; then it is a field.

(Refer Slide Time: 11:08)

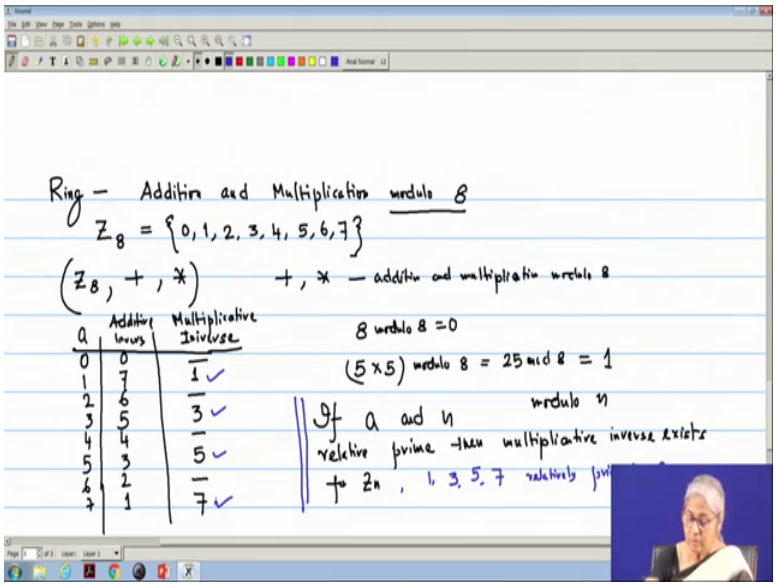


So, what is a multiplicative inverse; that means, if the if; a belongs to F the field and say multiplicative identity is e; this e is the multiplicative identity. So, which is for normal multiplication or ordinary multiplication it is 1; for ordinary multiplication identity is 1.

Then there must exist an element a inverse such that a inverse in multiplication if I take equal to a to a inverse equal to the multiplicative identity e equal to may be equal to 1 for ordinary multiplication. So, this a inverse must exist for the field and then we called that this is a field. Now if we remember and when it is finite field; finite field that if the order of the field is finite; that means, the number of elements in the set are finite. So, it is finite field if the order of the field is finite and order means we know order is the size of the set; that means, the number of set of elements ok.

And as I have already mentioned that infinite field is of very less use actually the real life applications like cryptography, coding theory the finite fields are used. So, mainly in our lectures we will be concentrating on the finite fields and their properties.

(Refer Slide Time: 14:07)



So, if we remember the in the lecture that or when we have read the ring we have taken some examples that addition and multiplication modulo; we have taken addition and multiplication modulo 8; one examples we have seen and what we have shown that under multiplication modulo 8; under multiplication modulo 8 it is a ring.

But the; when we have seen the operations the addition and multiplication modulo 8 then we have seen that it is the multiplicative inverse does not exist for all the elements. If we remember the what will be the set when we are taking the modulo 8 normally we have read that Z, now we give the notation that it is a Z 8 is the set, what is Z 8 because if I take the modulo 8; that means, it is nothing, but the remainder when some number is divided by 8.

So, remainder can be 0 to 7. 0, 1, 2, 3, 4, 5, 6, 7 so, this is the set Z 8 and we have seen that Z 8 and then the addition modulo 8 and the multiplication modulo 8. We have taken this here plus and star at the addition and multiplication modulo 8. Now when we have written that all the; or tabulated all the additions and the multiplication modulo 8 we have seen that if we remember that only since these are my set elements. So, some set a; if I write that this is 0, 1, 2, 3, 4, 5, 6, 7 then we got that additive inverse; we got that additive inverse.

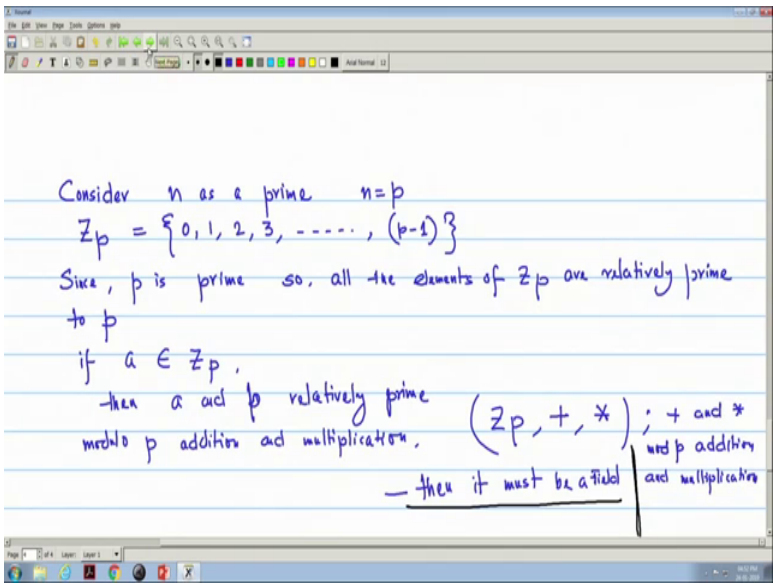
Additive inverse for 0 it is 0 because for additive identity is 0, this is 7, this is 6, 5, since modulo 8 modulo 8 is; 8 modulo 8 is 0. So, this is 4, 3, 2, 1. When we have taken the

same thing for the or multiplicative inverse; multiplicative inverse here multiplicative is that modulo 8 multiplication then we have seen that for 0 normally we do not get because 0 then there should not be zero divisors.

Then for 1 we get it is 1, for 2 we did not get any multiplicative inverse, for 3 it is 3, for 4 we did not get, for 5 it is 5, for 6 we did not get any inverse, for 7 it is 7. If we remember again then it is for say 5 this is we know that 5 into 5 modulo 8 modulo 8 equal to 25 mod 8 and this equal to 1; remainder is 1. So, similar way we can get the 1 and 7, now see and the conclusion we have made that if this a; if we remember that conclusion was that if a and n when we are taking modulo n or n multiplication, then a and n are relatively prime; then we get the then multiplicative inverse exist for Z n; this is for Z n.

So, and since here 2 4 and 6 are not relatively prime to 8 so, we did not get, but here say 1, 3, 5, 7 they are relatively prime to 8 relatively prime to 8 so, multiplicative inverse exist. So, that is why the ring under modulo addition or modulo multiplication or if we take the modulo 8 multiplication; that means, Z 8; Z 8 was not a ring or Z 8 is not a ring. Now, if it is a field that multiplicative inverse must exist. So, if I consider the n as a prime.

(Refer Slide Time: 20:17)



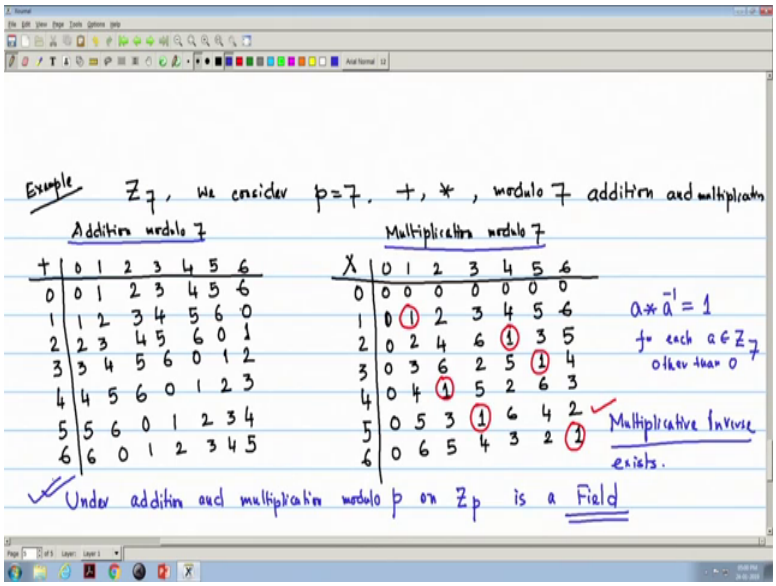
So, we consider n as a prime, then what will happen say if it is Z n or I write n equal to p normally that is the convention so, we write Z p. So, if it is Z p then Z p the set will be 0,

1, 2, 3 and up to p minus 1, then what is the relation between all these elements to p. Since p is a prime; so, all the elements of Z p are relatively prime to p except 0; we do not normally we consider that 0.

So, relatively prime to p; that means, I can take if a belongs to Z p other than 0 then a and n are relatively prime Then now if I do the modulo p addition and multiplication modulo; that means, the set I take the Z p and then plus and last day we have given this notation as the star that modulo addition under this; this isplus and star are modulo p or mod p addition and multiplication, then it must be a it must be a field.

So, we have considered the p and Z p and so that the set becomes 0 to p minus 1 since p is prime. So, all the elements are relatively prime and then the according to that example we have seen; that it must be; we must get that a multiplicative inverse.

(Refer Slide Time: 23:50)



Now, we take one example that where we take the Z 7 ; that means, we consider we consider p equal to 7 and the plus and star we give the modulo 7 addition and multiplication.

Now, if we tabulate the addition modulo 7 so, we first see the addition modulo 7 it will be only 7 elements and modulo 7. So, if we remember it would be same because addition will be similar 6 plus 1, 7 so, modulo 7. It is 0; again 7 modulo 7 it is 5, 6, now it will be

modulo 7. So, it will be giving 0 1 2 3 4 6 0 1 2 3 4 5. So, addition modulo will be 7 now addition modulo 7 this table will be.

Now, if I consider the multiplication modulo 7 on Z p, now since 0 multiplied by any element will be 0. Now it will be similarly it is multiplied by 1; this is because multiplicative identity is 1. Now I have to take that a into b modulo 7. So, 2 into 2 2 into 2 4, 4 modulo 7 is 4, 6 modulo 7 is 6, but 8 modulo 7 will be 1, similarly 10 modulo 7 will be 3 and 12 modulo 7 is 5. So, what lastly we have done modulo 8 now we are doing modulo 7.

Then it is 0 3 6 modulo 7 2 then it is 5 12 15 so, it is 1 now 18 so, this becomes 4, now 0 4 0 4 8. So, it is 1, then 12, it is 5, 16, it is 2, 16 modulo 7 remainder 2, then 20. So, it is 6 then it is 3, 5 5 modulo 7, 5 3 1 6 25 so, it is 4, then 30 so, it is 2, 6 modulo 6 0 6 module 12. So, it is 5, 4 24 then 30 so, 2 then 36 so, it will be 1.

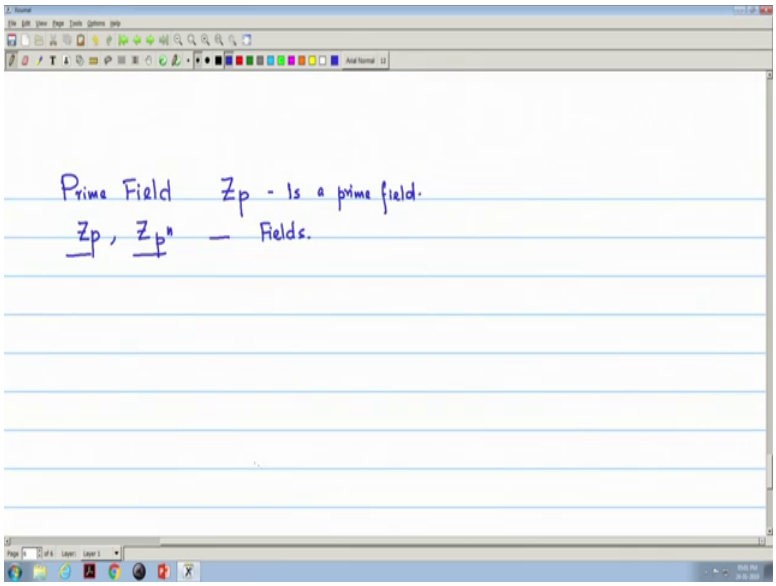
Now, we observe some of the seen; first thing is except 0 we are getting multiplicative identity for each element 1 because since multiplicative identity is 1. So, we are getting a a inverse equal to 1 for each or for all a belongs to F Z p, here it is I should write that for a belongs to Z 7. So, for each element of Z 7; I am getting and this is for other than other than 0.

So, multiplicative inverse exist since last day we have seen that for or when we have discussed that multiplicative inverse exists for other properties when the we have taken that addition modulo 8 and multiplication modulo 8 that for all properties that we have or the axioms that we have defined for field should follow that closure, associative, additive identity it is a commutative and then for since it is a commutative ring we have shown this is also integral domain.

So, up to these all these properties for addition these additive 1 to A 6 for multiplication for M 6 to M 7 commutative ring then it is integral domain everything is satisfied. Now what we show that these only these M 12 that multiplicative inverse that now we show that when we are taking that a prime number; that means, when Z 7; 7 is a prime then multiplicative inverse exist. Since all other all the elements of Z p or in this case Z 7 it is relatively prime to p.

So, we can we conclude that our under addition modulo p; addition and multiplication these are 2 binary operations multiplication modulo p where p is prime though on Z p, Z p is a set 0 to p minus 1 is a field. And this is a very good observation and based on that actually we will be forming that prime field.

(Refer Slide Time: 32:31)



So, normally when p is prime we call it is a prime field. So, on prime field so, Z p is a prime field and operation is and we will; mainly the next lectures we will be considering this prime field and the extension field that is Z p and some Z p n; that means, when this is p to the power n, the set of elements are 0 to p to the power n.

So, mainly our focus is on these two fields we will be discussing. So, in this lecture we have seen that how very basic concepts that how the Z p with the two binary operations the modulo operations addition modulo p and multiplication modulo p; how they are forming a field and how we are defining the prime field and then this p to the power n we call that is the extension field and mainly we will be concentrating on the studies of these two fields.