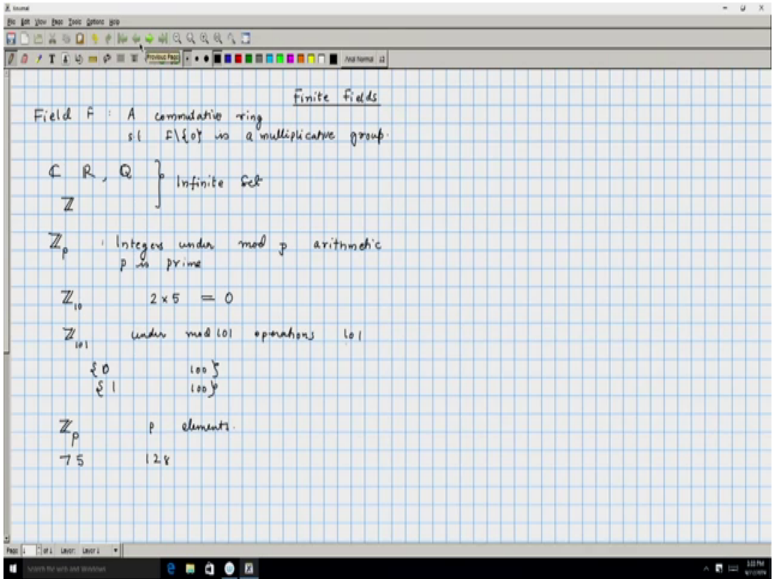
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Lecture 43
Construction of Finite Fields

(Refer Slide Time: 0:39)



Finite fields

Field F : A commutative ring
s.t. $F \setminus \{0\}$ is a multiplicative group.

$\left.\begin{matrix} C \quad R, \quad Q \\ \mathbb{Z} \end{matrix}\right\}$ Infinite set

$\mathbb{Z}_p$: Integers under mod p arithmetic
p is prime

$\mathbb{Z}_{10}$ $2 \times 5 = 0$

$\mathbb{Z}_{101}$ under mod 101 operations 101

$\{0$ $100\}$
$\{1$ $100\}$

$\mathbb{Z}_p$ p elements.
75 128

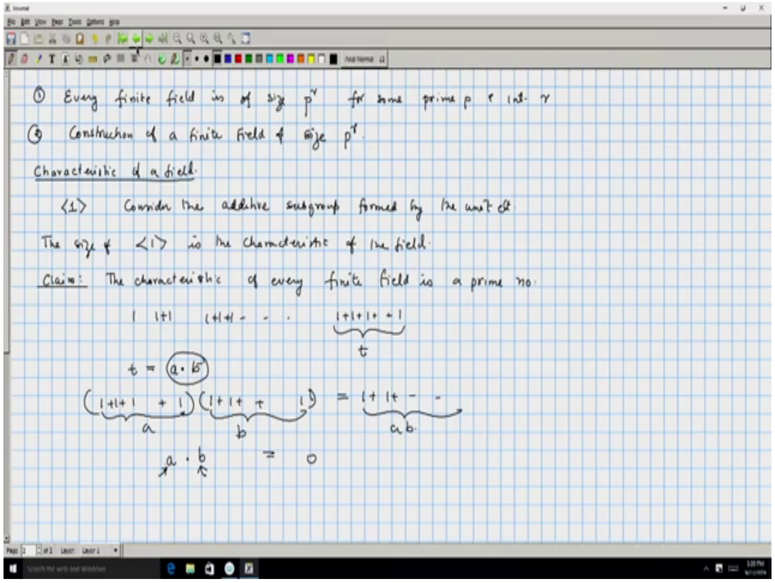
So we will study about the finite fields in this lecture. A field is a commutative ring such that the non-zero elements form a multiplicative group. The examples are the set of complex numbers, the set of real numbers and the set of rational numbers okay and the non-examples are the set of integer, if you look at the set of integers, they do form commutative ring but the elements are not invertible. All these are infinite sets, okay so these are examples, C, R and Q are examples of infinite fields and in this lecture what we will concentrate is on trying to understand the finite fields.

An example of a finite field is integers under mod P multiplication, mod P addition and mod P multiplication. And here we have to insist that P is prime. If we look at elements in Z10, so doing mod 10 arithmetic they do form a commutative ring but since 10 is not a prime number, this will not be a field. If you multiply 2 and 5, they are non-zero elements and they multiply to give you 0. So this would in particular mean that 2 is not going to be invertible, there is not going to be any element with which you can multiply 2 or 5 and get identity.

Okay because 2 and 5 are both factors of 10, whereas Z 101, 101 is a prime number so you can verify that under mod 101 operations these form a field of size 101. Okay the elements (1 to) 0 to 100 forms an additive group and the elements, the non-zero elements, 1 to 100 they will form a multiplicative group, every element you can check is invertible mod 101.

So if you take any prime P, if and you look at ZP, this will have P elements, so that is a finite field of size P. Can we have finite fields of size say 75? Can we have finite fields of size 128? Okay so finite fields of what size is exist? That is a question to which we will try to answer. We will provide some partial answers to this particular claim, this particular question.

(Refer Slide Time: 3:30)



① Every finite field is of size p^r for some prime p & int. r

② Construction of a finite field of size p^r.

Characteristic of a field.

$\langle 1 \rangle$ Consider the additive subgroup formed by the unit elt.

The size of $\langle 1 \rangle$ is the characteristic of the field.

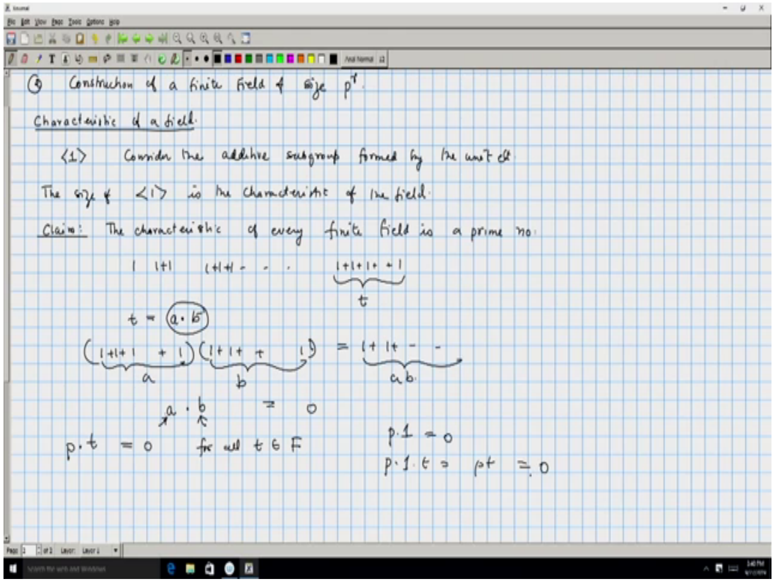
Claim: The characteristic of every finite field is a prime no.

$$1 \quad 1+1 \quad 1+1+1 \cdots \quad \underbrace{1+1+1+\cdots+1}_{t}$$

$$t = \boxed{a \cdot b}$$

$$\underbrace{(1+1+1 \quad + 1)}_{a}\underbrace{(1+1+ \quad + \quad 1)}_{b} = \underbrace{1+1+ \cdots}_{ab}$$

$$a \cdot b = 0$$



② Construction of a finite field of size p^r.

Characteristic of a field.

$\langle 1 \rangle$ Consider the additive subgroup formed by the unit elt.

The size of $\langle 1 \rangle$ is the characteristic of the field.

Claim: The characteristic of every finite field is a prime no.

$$1 \quad 1+1 \quad 1+1+1 \cdots \quad \underbrace{1+1+1+\cdots+1}_{t}$$

$$t = \boxed{a \cdot b}$$

$$\underbrace{(1+1+1 \quad + 1)}_{a}\underbrace{(1+1+ \quad + \quad 1)}_{b} = \underbrace{1+1+ \cdots}_{ab}$$

$$a \cdot b = 0$$

$p \cdot t = 0$ for all $t \in F$

$p \cdot 1 = 0$

$p \cdot 1 \cdot t = pt = 0$

What we will show is the following. The first thing that we will show is every finite field is of size P to the r for some prime P and integer R. In particular, after this we can conclude that there will not be a finite field of size 75, because 75 is not a prime power. And then we will give a construction of a finite filed of size P to the r okay and what is true but we will not show in this lecture is that there is only one finite field of a given size.

That means if we construct a finite field of size P to the r, that field can be thought of as a representative finite field of that size. Every other finite field of that side is isomorphic to the one that we will construct. So let us continue with this thread, first define an ocean of a characteristic of a field. Look at the identity element okay and keep on adding it to itself. In other words, consider the additive subgroup formed by the unit element. This is clearly a finite collection because every element that you generate is going to belong to the field and a field itself is a finite collection and therefore this is going to be a finite cyclic group.

The size of this particular cyclic group is what we called as a characteristic of the field. Now that when you consider infinite group, the additive subgroup formed by the unit element could possibly be infinite. Okay so in that case we might refer to the field as having characteristic 0 or infinite but here we are restricting ourselves to finite fields, therefore the characteristic is always a positive integer.

Now we will claim the following thing about characteristic. The characteristic of every finite field is a prime number okay, how do we show that? So by definition basically considering 1, 1 plus 1, 1 plus 1 plus 1 and so on okay look at the first time when it becomes 0. Because this is a cyclic group and it should, the process should some, at some stage give rise to 0 and that can be thought of as the characteristic. Okay beecause these are the distinct elements, after 0 has been generated if you add 0 the same structure is going to repeat again and again.

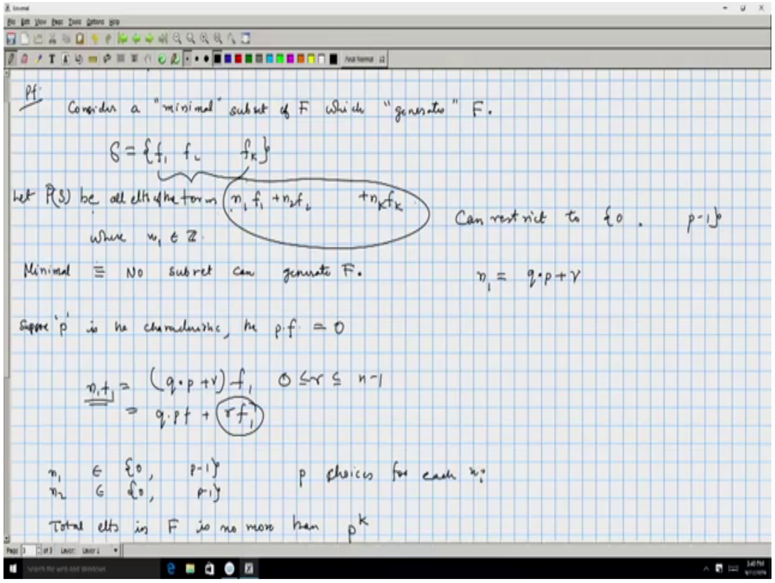
So the number of times 1 is being added to itself, to get 0 that can be thought as of the characteristic of the field. So let us say this t and t can be the smallest such number okay this minimum number of times that you have to add 1 to itself so that you get 0. Now if t is not a prime, we can write t is equal to a into b and then we can look at this particular equation 1 plus 1 plus 1 a times multiplied by 1 plus 1 plus 1 b times.

By the distributive law this should exactly be equal to 1 plus 1 plus 1 added ab times okay and 1 added to itself a times we can denote that by a and 1 added to itself b times we can call it as b, so these are two elements of the fields, two non-zero elements of the field because if either of them were 0 then we know that t is not the smallest number such that 1 when added t times gives rise to 0. So a and b we may assume is smaller than t and therefore now we have two non-zero numbers which multiply and give rise to 0 okay.

And that is not possible in a field, unless one of a and b are 0 okay which we had, neither of a and b can be 0 because we assumed the t was the smallest. So this contradicts the assumption the t could have been written as product of 2 things which are not mean product of a and, so this contradicts the assumption that t was a composite number. So the characteristic of every finite field is P, I mean a prime number and if you look at P times t this is equal to 0 for all t belonging to the field.

So take an a element of the field, multiply it with P, you will get 0 because P times 1 is 0 okay and P times 1 times t is equal to P times t, that is also going to be 0.

(Refer Slide Time: 9:46)



Pf:

Consider a "minimal" subset of F which "generates" F.

$S = \{f_1, f_2 \quad f_k\}$

Let R(S) be all elts of the form $n_1 f_1 + n_2 f_2 \quad + n_k f_k$

where $n_i \in \mathbb{Z}$.

Can restrict to $\{0, . \quad p-1\}$

Minimal ≡ No subset can generate F.

$n_1 = q \cdot p + r$

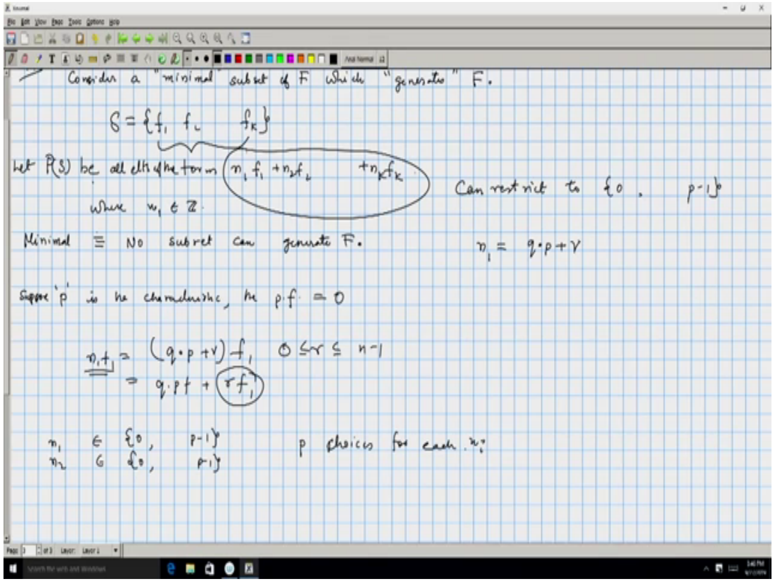
Suppose 'p' is the characteristic, the $p \cdot f = 0$

$$n_1 f_1 = (q \cdot p + r) f_1 \quad 0 \le r \le n-1$$
$$= q \cdot pf + rf_1$$

$n_1 \in \{0, \quad p-1\}$
$n_2 \in \{0, \quad p-1\}$

p choices for each n_i

Total elts in F is no more than p^k



Consider a "minimal" subset of F which "generates" F.

$S = \{f_1, f_2 \quad f_k\}$

Let R(S) be all elts of the form $n_1 f_1 + n_2 f_2 \quad + n_k f_k$

where $n_i \in \mathbb{Z}$.

Can restrict to $\{0, . \quad p-1\}$

Minimal ≡ No subset can generate F.

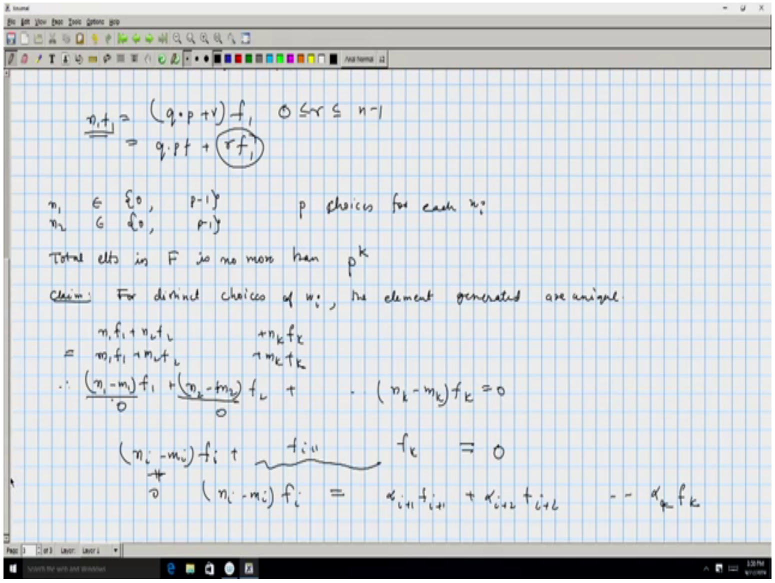
$n_1 = q \cdot p + r$

Suppose 'p' is the characteristic, the $p \cdot f = 0$

$$n_1 f_1 = (q \cdot p + r) f_1 \quad 0 \le r \le n-1$$
$$= q \cdot pf + rf_1$$

$n_1 \in \{0, \quad p-1\}$
$n_2 \in \{0, \quad p-1\}$

p choices for each n_i



$$\underline{\underline{n_1 f_1}} = (q \cdot p + r) f_1 \quad 0 \leq r \leq n-1$$

$$= q \cdot pf + \boxed{r f_1}$$

$n_1 \in \{0, \quad p-1\}$ $\quad$ p choices for each n_i

$n_2 \in \{0, \quad p-1\}$

Total elts in F is no more than p^k

Claim: For distinct choices of n_i, the element generated are unique

$$n_1 f_1 + n_2 f_2 \quad + n_k f_k$$

$$= m_1 f_1 + m_2 f_2 \quad + m_k f_k$$

$$\therefore \underset{0}{\underline{(n_1 - m_1)}} f_1 + \underset{0}{\underline{(n_2 - m_2)}} f_2 + \quad \cdot (n_k - m_k) f_k = 0$$

$$(n_i - m_i) f_i + \underbrace{\quad f_{i+1} \quad} \quad f_k = 0$$

$$\underset{0}{\ne} \quad (n_i - m_i) f_i = \alpha_{i+1} f_{i+1} + \alpha_{i+2} f_{i+2} \quad - - \alpha_k f_k$$

So now we are in a position to show, why every finite field is of size P to the r for some integer r and prime P. So let F be a finite field and let us look at a collection of elements of F which generates F. Consider a minimal collection or minimal subset of F which generates F and what does it mean for a collection to generate F? So we are looking at a set f1 f2 fk, some finite set such that if we consider these elements and add them up, add them up enough number of times we can generate the entire collection. Okay so we are looking at n1 f1 plus n2 f2 plus nk fk.

Consider all, suppose S is the set f1 f2 fk, so let P be the set of all elements of the form m1 f1 plus n2 f2 plus nk fk where n1 is an integer. Okay so that will be the set generated by S and we are looking at a set which generates the complete set F and we want that set to be the smallest. Smallest or the minimal one in the sense, none of its subsets can generate F, so this definition of minimal means, no subset can generate F. Clearly there are such sets which generates the entire collection, if you take the entire F that will generate F because we can mean n1 n2 can all be 1 or mean 1 and 0s.

So if you take the full collection, the full field, that can generate itself, so you can prove of elements systematically and probably get a small subset such that no smaller subset can generate the entire F. So let S be one such collection and further our previous observation that if p was the characteristic then p times any f is going to be equal to 0. So while we are considering elements of this form we can restrict to 0 to p minus 1 because n1 if we write it as say q times p plus r then n1 f1 is going to be q times p plus r times f1 which can be written as q times p f plus r times f1, so n times f1 is nothing but r times f1, where r is lying between 0 and n minus 1.

So when we are looking to generate the set F these coefficients of f1, f2, fk can be chosen from 0 to p minus 1 okay. So now if you look at f1, f2, fk and look at everything that is generated by f1, f2, fk, the possibilities are, the n1 could belong to 0 to p minus 1, n2 should can belong to 0 to p minus 1, so there are p possibilities or p choices for each ni. So in all the total number elements that we can form is no more than F, so the total elements in F is no more than p to the k. Because each one of these n1, n2, nk you can select it from 0 to p minus 1.

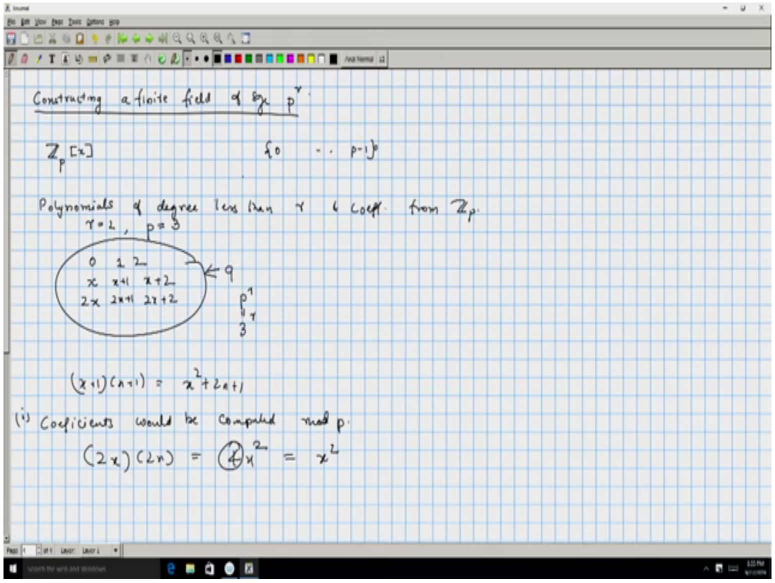
And what we will show now is that, it is exactly p to the power k. So our claim is for distinct choices of ni the element generated are unique. Why is this so? So suppose this is not the case then let us say n1 f1 plus n2 f2 plus nk fk this is equal to let us say m1 f1 plus m2 f2 plus mk fk. And we are assuming that n1, n2, nk if consider that as a tuple that is different from m1. m2, mk considered as a tuple. And since these two expressions generate the same element, if you subtract them you will get 0.

So therefore we can rewrite this as n1 minus m1 times f1 plus n2 minus m2 times f2 plus all the way up to nk minus mk times fk must be equal to 0. Now since ni is, ni minus mi, at least one of them should be non-zero because if all of them were 0, the ni's and mi's are equal. So look at the first non-zero entry, okay so let us say this is 0, this is 0, so ni minus mi is not equal to 0 okay so times fi plus some other terms, involving fi plus 1 all the way up to fk, this is going to be equal to 0.

We can rewrite this equation by taking ni minus mi times fi on one side, this is equal to let us say alpha i plus 1 fi plus 1 plus alpha i plus 2 fi plus 2 all the way up to alpha k fk, multiply with the inverses of ni minus mi on both sides, we can do that because ni minus mi is some number between 0 to p then it has an inverse, multiply that and we can express fi as linear combination of fi plus 1 up to fk. This would mean that in this collection f1 into fk, which we assumed as minimal, one of the elements can be expressed as linear combination of the other elements.

So there is a smaller set, namely s minus fi which generates the same collection, okay that is a, that contradicts our initial assumption, that s was the minimal subset okay and therefore we can conclude that our claim is valid. Okay that there cannot be two distinct choices for n1, for the tuples and them, such that they generate the same element. So this basically means that take any finite field, its size had to be of the form p to the power k or p to the power r where p is some particular prime

(Refer Slide Time: 18:18)



Constructing a finite field of size p^r.

$\mathbb{Z}_p[x]$ $\{0 \cdots p-1\}$

Polynomials of degree less than r & coeff. from $\mathbb{Z}_p$.

$r=2, \; p=3$

0	1	2
x	$x+1$	$x+2$
$2x$	$2x+1$	$2x+2$

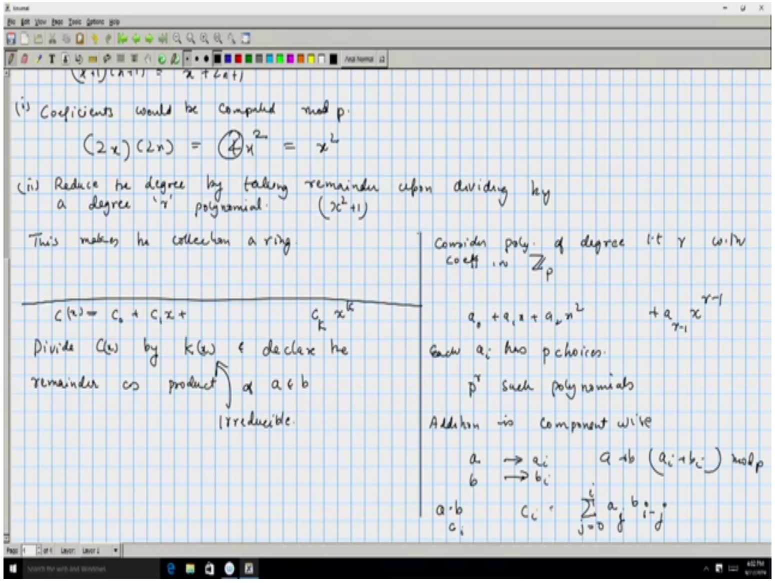
$\leftarrow 9$

$p^r = 3^r$

$(x+1)(x+1) = x^2+2x+1$

(i) Coeficients would be computed mod p.

$(2x)(2x) = \boxed{4}x^2 = x^2$



$(x+1)(x+1) = x^2+2x+1$

(i) Coeficients would be computed mod p.

$(2x)(2x) = \boxed{4}x^2 = x^2$

(ii) Reduce the degree by taking remainder upon dividing by a degree 'r' polynomial. (x^2+1)

This makes the collection a ring.

$c(x) = c_0 + c_1 x + \qquad c_k x^k$

Divide $C(x)$ by $k(x)$ & declare the remainder as product of a & b

Irreducible.

Consider poly. of degree l.t r with coeff in $\mathbb{Z}_p$

$a_0 + a_1 x + a_2 x^2 \qquad + a_{r-1} x^{r-1}$

Each a_i has p choices.

p^r such polynomials

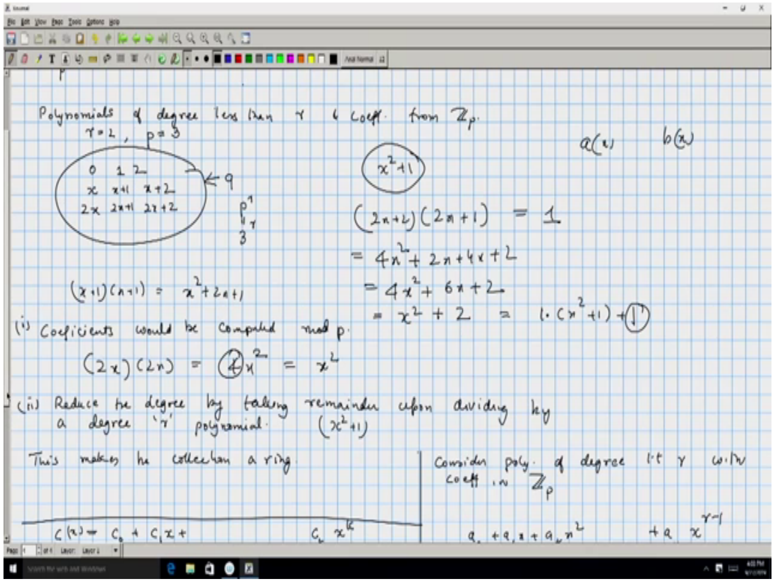
Addition is component wise

$a \rightarrow a_i$
$b \rightarrow b_i$

$a+b \; (a_i+b_i) \bmod p$

$a \cdot b$ c_i

$c_i = \sum_{j=0}^{i} a_j b_{i-j}$



Polynomials of degree less than r & coeff. from $\mathbb{Z}_p$.

$r=2,\ p=3$

$0\quad 1\quad 2$

$x\quad x+1\quad x+2$

$2x\quad 2x+1\quad 2x+2$

$\leftarrow 9$

p^r

3^2

$(x+1)(x+1) = x^2+2x+1$

(i) Coeficients would be computed mod p.

$(2x)(2x) = \boxed{4}x^2 = x^2$

(ii) Reduce the degree by taking remainder upon dividing by a degree 'r' polynomial. (x^2+1)

This makes the collection a ring

$\boxed{x^2+1}$

$a(x)\quad b(x)$

$(2x+2)(2x+1) = 1$

$= 4x^2+2x+4x+2$

$= 4x^2+6x+2$

$= x^2+2 = 1\cdot(x^2+1)+\boxed{1}$

Consider poly. of degree l.t r with coeff in $\mathbb{Z}_p$

$c(x) = c_0 + c_1x + \quad c_k x^k$

$a_0 + a_1x + a_2x^2 \quad + a\ x^{r-1}$

So the next question is, can we really generate that particular field? Okay so that is the last part of this lecture constructing a finite field of size (p to the k), no p to the r. So let us consider polynomials, so the way we will do this is, we will construct a set of polynomials and we will define a multiplication and addition on polynomials and with respect to that addition and multiplication, this collection of polynomials will basically be a finite field.

So the set basically consist of polynomials whose coefficients are from 0 to p minus 1, so consider Zp and look at polynomials whose coefficients are in Zp. So if you take p equals 3, the polynomial Zp we will consider are polynomials of degree less than r and coefficients from Zp.

So if I, if we choose r is equal to 2 and p is equal to 3, then our polynomials are going to be 0, 1, 2 this is the constant polynomials and then we have the polynomial x, x plus 1 and x plus 2 then 2x, 2x plus 1 and 2x plus 2. There are 9 elements here, namely p to the r, where p is 3 and r is 2. This is the collection of polynomials, of course if you multiply two of these polynomials their result is not going to be one of these collection, for example if I take x plus 1 into x plus 1 that is going to x square 2x plus 1, that is not an element of this collection.

So under the normal multiplication these do not form a finite field. So you have to define a new multiplication and addition. So the first thing is coefficients would be computed mod p, so in particular if multiply 2x and 2x we will get 4x but 4 mod 3 is 1, so that will be, sorry 4x square and that will be x square. But x square is still not an element of this collection. So what we will do is, we will reduce the degree by taking remainder upon dividing by a degree two polynomial or degree r polynomial.

This cannot be an arbitrary polynomial but let us say for the time being, let just say we will divide it with x square plus 1, okay so when you multiply two of these polynomials, what we do is, whatever is the resultant, we will convert the coefficients into mod p and whatever is the resultant polynomial that is being divided by a polynomial of degree r. When you divide a polynomial ax by another polynomial bx the remainder is going to be polynomial whose degree is going to be less than the degree of bx.

So when we do this, when we divide by r whatever we get will be of degree at most r minus 1. So now at least what we have is, we have a valid addition and multiplication operation defined on this collection. We need to verify that this is indeed a group, I mean this indeed a field. So it will not be a field when this is an arbitrary polynomial, so this makes it a ring. Because the addition is well defined, addition is invertible whereas multiplication may not be invertible.

We will introduce a concept called as irreducible polynomial and if the polynomial by which we are dividing is an irreducible polynomial then we will show that, these collection of polynomials will basically be a field. So before we introduce a notion of irreducible polynomial, let me just state whatever we were doing in a generalized setting. So what we do is consider polynomials of degree less than r with coefficients in Zp.

So we are looking at a0 plus a1x plus a2x square all the way up to a r minus 1 x raise to r minus 1. Each ai has p choices and each of those polynomial is a different polynomial when you are dividing by a degree r polynomial. Okay so these are distinct polynomials, they are precisely p raise to r such polynomials, okay.

Addition is component wise in the sense if you have a and b, so a is a sequence or a polynomial and b is another polynomial of degree r then so let us just say this corresponds to the coefficients are ai, coefficients of b are bi then a plus b is basically ai plus bi mod p, okay that is simple enough. And a times b is the normal polynomial multiplication, so if we denote it by ci, ci is equal to summation j going from 0 to i ai b i minus, sorry aj b i minus, so ci is aj b i minus j summed up over all values of j.

That will be the normal polynomial multiplication and then whatever polynomial you get, so let us just say c is the polynomial which we obtained as c0 plus c1x plus all the way up to ck x raise to k, now this k note that it could be greater than r. Now divide cx by a special polynomial kx and declare the remainder as product of a and b. And this kx has to be an irreducible polynomial, we have been defined what is an irreducible polynomial, we will come to that.

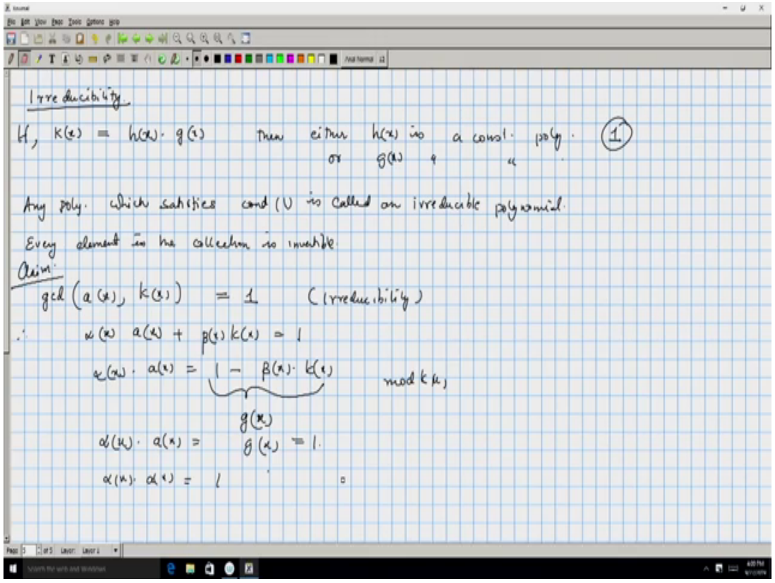
And then we do this, the property of irreducibility, makes sure that the collection forms a field. So in case of our field of size 9, if you looked at these particular polynomials and x square plus 1 happens to be an irreducible polynomial. So let us see at the example of one particular multiplication, if you took 2x plus 2 and multiplied with 2x plus 1, this is going to be 4x square plus 2x plus 4x plus 2. That is going to be 4x square plus 6x plus 2 and mod 3, the coefficients have to be converted to mod 3, you will get x square.

Because 3x square 3 is 0 and 6x is 0 times x, so that is gone and we will get this as x square plus 2. When we divide this by x square plus 1, okay this can be written as 1 into x square plus 1 plus 1, so 2x plus 2 into 2x plus 1 is will be reported as 1. So this will be 1 because mod x square plus 1, when you divide it by x square plus 1, the remainder is 1 and that happens to be one of the elements in the collection.

So whatever you multiply, since we are taking the remainder when you divide by x square plus 1, where the division is now a polynomial division, the remainder is going to be a polynomial of degree less than x square plus 1 that is going to be a polynomial of degree utmost 1. And we have listed out all the degree 1 polynomial in our collection. This is a well-defined operation. The only thing we need to really check is that, under this multiplication, every element in this collection has a multiplicative inverse.

This collection of polynomials is general collection, will be a ring, irrespective of whether x square is reducible or irreducible but the reducibility property will ensure that each element has an inverse.

(Refer Slide Time: 28:43)



Irreducibility

If, $k(x) = h(x) \cdot g(x)$ then either $h(x)$ is a const. poly. $\boxed{1}$
or $g(x)$ " "

Any poly. which satisfies cond (1) is called an irreducible polynomial.

Every element in the collection is invertible

Aim:

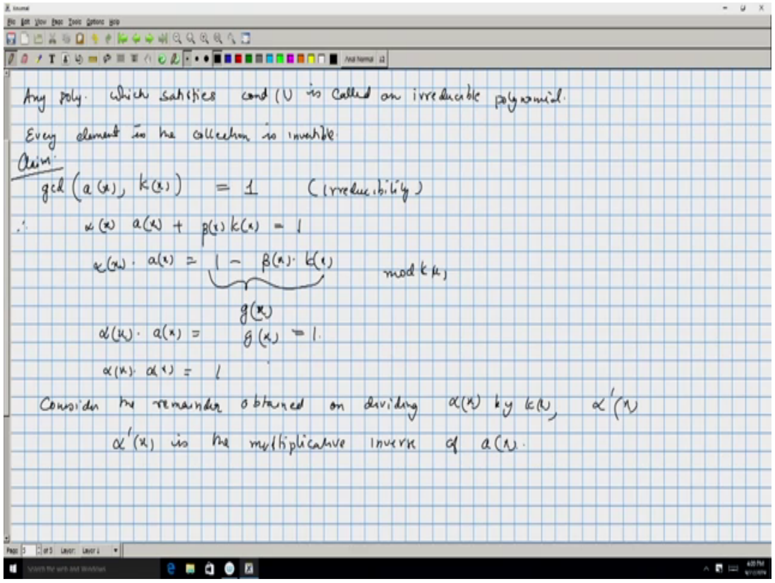
$\gcd(a(x), k(x)) = 1$ (irreducibility)

$\therefore \alpha(x)\ a(x) + \beta(x)\, k(x) = 1$

$\alpha(x) \cdot a(x) = \underbrace{1 - \beta(x) \cdot k(x)}_{g(x)}$ mod $k(x)$

$\alpha(x) \cdot a(x) = g(x) = 1.$

$\alpha(x) \cdot a(x) = 1$



Any poly. which satisfies cond (1) is called an irreducible polynomial.

Every element in the collection is invertible

Aim:

$\gcd(a(x), k(x)) = 1$ (irreducibility)

$\therefore \alpha(x)\ a(x) + \beta(x)\, k(x) = 1$

$\alpha(x) \cdot a(x) = \underbrace{1 - \beta(x) \cdot k(x)}_{g(x)}$ mod $k(x)$

$\alpha(x) \cdot a(x) = g(x) = 1.$

$\alpha(x) \cdot a(x) = 1$

Consider the remainder obtained on dividing $\alpha(x)$ by $k(x)$, $\alpha'(x)$

$\alpha'(x)$ is the multiplicative inverse of $a(x)$.

So now let us define the notion of irreducibility. So let us look at the polynomial kx, suppose we can write kx is equal to hx times gx, then either hx is a constant polynomial or gx is a constant polynomial. The polynomials which satisfies this condition is called as irreducible polynomial. So let us call this as condition 1, any polynomial which satisfies condition 1 is called an irreducible polynomial okay. So this is a notion very similar to that of primality, a prime number if you write it as product of two objects, mean two numbers then one of the numbers is 1.

It is (always), mean one of the, mean if a number is written as a into b and if a or b is 1, means it is always the case then we say that the number p is prime. The only way in which you can write a prime number as product of two other elements is by choosing one of those elements as 1 but here instead of 1, we have what is a constant polynomial. So the only factorization possible for kx, involves a constant polynomial then we will say k is an irreducible polynomial.

In other words, this does not have common factors with any other polynomial other than the constant factors. So now let us see how the notion of irreducibility helps us in constructing the finite field. So the condition that we have to prove is that every element in the collection is invertible, this is what we need to prove. So let us say ax is one particular element, since kx is an irreducible polynomial, if we look at the greatest common divisor of ax and kx, this must be equal to 1.

We can adjust the constant polynomial, so that the coefficients are, means it is not anything different from 1, it is exactly 1. Here the definition of your reducibility we could have constant factor which is a constant polynomial but we can adjust the constant polynomial to be 1. So GCD of ax and kx, if it is equal to 1 because kx is a irreducible polynomial okay reason is reducibility. Because if it is anything other than 1 then ax and kx has a common factor and that common factor is a common, is a factor of kx, so GCD ax and ax kx equals 1 and the definition of GCD is the smallest positive linear combination, okay.

So what this also means is, we can find alpha x and beta x such that alpha x ax plus beta x kx is equal to 1. Now this would mean that alpha x into ax is equal to 1 minus beta x times kx okay so if you look at this particular polynomial, that is called that as gx. What we know is, alpha x when multiplied by ax gives gx and if we look at this mod kx, this gx is nothing but 1. So alpha x into ax is 1 mod kx. So that means if we look at the polynomial corresponding to alpha x means consider the remainder obtained on dividing alpha x by kx, let us call that as alpha prime x, alpha prime x is the multiplicative inverse of ax.

So we took an arbitrary polynomial from our collection and since GCD with kx is 1 we can find a linear combination of ax and kx, which gives us 1and from that we can extract an inverse of ax, okay that means that every element is invertible and therefore this collection forms a group. What needs to be further shown is that for every degree, there is an irreducible polynomial, it is little beyond the scope of this course, so we would just assume that, that for any particular degree there is an irreducible polynomial of that degree. So that is the end of this lecture.