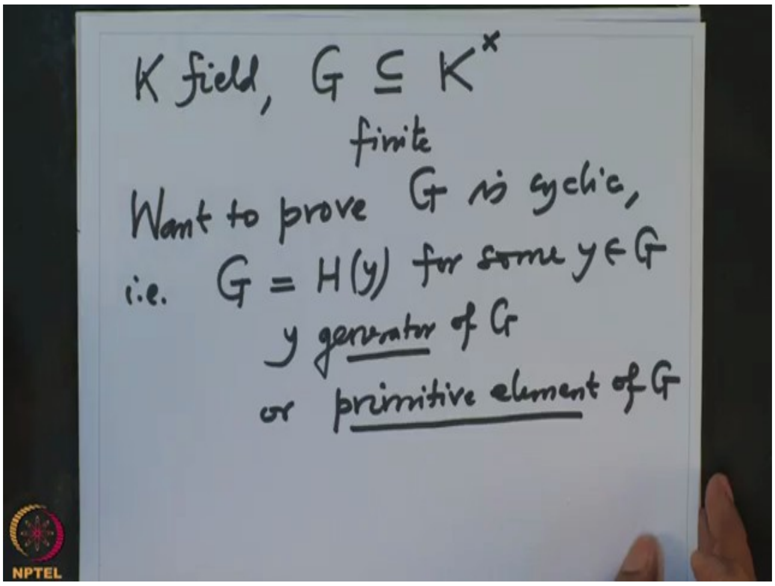
Galois Theory
Professor Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 21
Finite subgroups of the Unit Group of a Field

We will continue our study of Structure of finite groups of the multiplicative group of a field and today we will prove that these subgroups are cyclic.

(Refer Slide Time: 0:45)

!

K field, $G \subseteq K^{\times}$ finite

Want to prove G is cyclic,

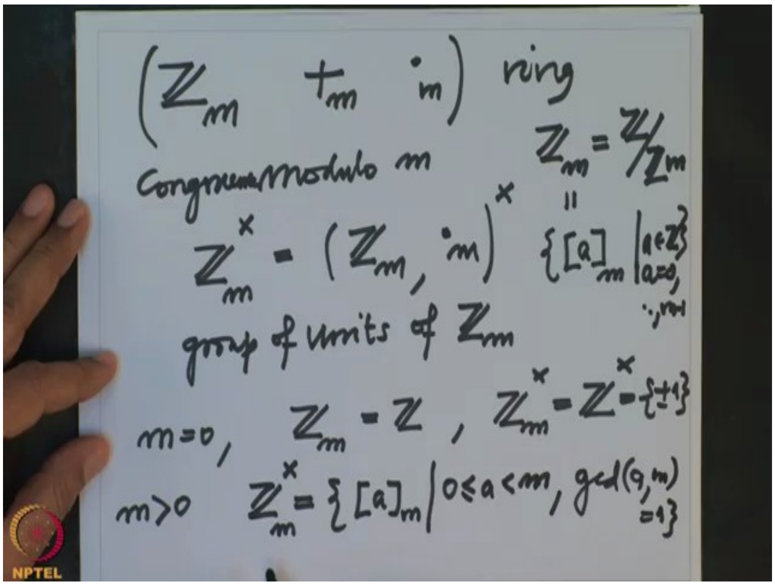
i.e. $G = H(y)$ for some $y \in G$

y generator of G

or primitive element of G

So (what) we will prove is that if K is any field and G is a subgroup of K^{x}, K^{x} is a multiplicative group of the field K and if G is finite then we want to prove G is cyclic, that means we want to prove that G is generated by one element that is in our notation G is $H(y)$ for some y, such a y may not be unique and such a y is also called a generator of G or also called primitive element of G. So cyclic group has primitive element and there may not be unique, there may be many primitive elements this what we want to prove but for the proof of this we will need some preliminary results on finite groups that I will recall, some of the results I will recall with the sketch of proofs and some of the them I will recall without proofs.

(Refer Slide Time: 02:33)



$(\mathbb{Z}_m \quad +_m \quad \cdot_m)$ ring

Congruence modulo m $\qquad \mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}m$

$\mathbb{Z}_m^{\times} = (\mathbb{Z}_m, \cdot_m)^{\times}$ $\qquad \{[a]_m \mid a\in\mathbb{Z}, a=0, \dots, m-1\}$

group of units of $\mathbb{Z}_m$

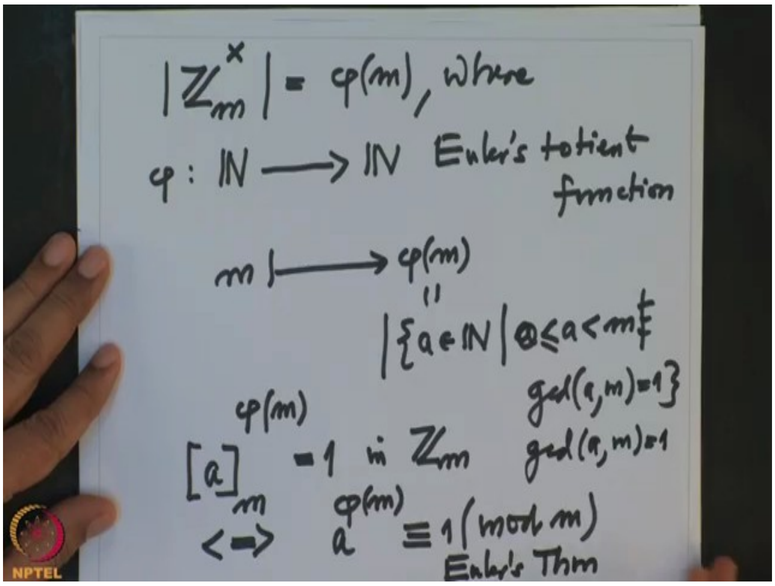
$m=0$, $\mathbb{Z}_m = \mathbb{Z}$, $\mathbb{Z}_m^{\times} = \mathbb{Z}^{\times} = \{\pm 1\}$

$m>0$ $\quad \mathbb{Z}_m^{\times} = \{[a]_m \mid 0 \le a < m, \gcd(a,m) = 1\}$

So for example let us started typical finite group for example we have seen $\mathbb{Z}_m$, this is modulo m operations, congruence modulo m. So there two operations plus and dot And with respective that we have seen it is a ring and whenever we have a ring we talk about the unit group of the ring that is usually denoted in this case $\mathbb{Z}_m^x$ this means you take the multiplicative monoid $(\mathbb{Z}_m,.)$ And take units in multiples element in their monoid that is obviously a unit that obviously subgroup of the multiplicative monoid of $\mathbb{Z}_m$ this is called group of units, group of units of $\mathbb{Z}_m$ and for example when m is 0 hiss $\mathbb{Z}_m$ is Z and therefore $\mathbb{Z}_m^x$ is Z cross which is only plus minus 1.

So it is obviously cyclic of order two more generally if m is positive remember also when we did the definition etcetera for $\mathbb{Z}_m$, $\mathbb{Z}_m$ as also same as Z additive group of integers a modulo the subgroup generated by m that is this, so this are the cosets and there given by the remainders of when you divide by m so there precisely m remainders from 0 to m minus 1, so therefore elements of $\mathbb{Z}_m$, $\mathbb{Z}_m$ also we are denoting this as residues that or equivalence classes so the notation is this, these are precisely the residues and there are precisely residues are from 0 to $m-1$, so these are precisely equivalence classes of 0, 1, 2 up to $m-1$ with the congruence modulo m relation, so when m is positive the units are precisely $\mathbb{Z}_m^x$ these are precisely all those remainders and we can assume them they are from 0 to m minus 1 and gcd of a and m should be 1 they are co prime to m, they are precisely the units in $\mathbb{Z}_m$ and then how many of them are there that this is a very famous notation for that due to Euler.

(Refer Slide Time: 05:56)



$|\mathbb{Z}_m^{\times}| = \varphi(m)$, where

$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ Euler's totient function

$$m \longmapsto \varphi(m) = |\{a \in \mathbb{N} \mid 0 \leq a < m,\ \gcd(a,m)=1\}|$$

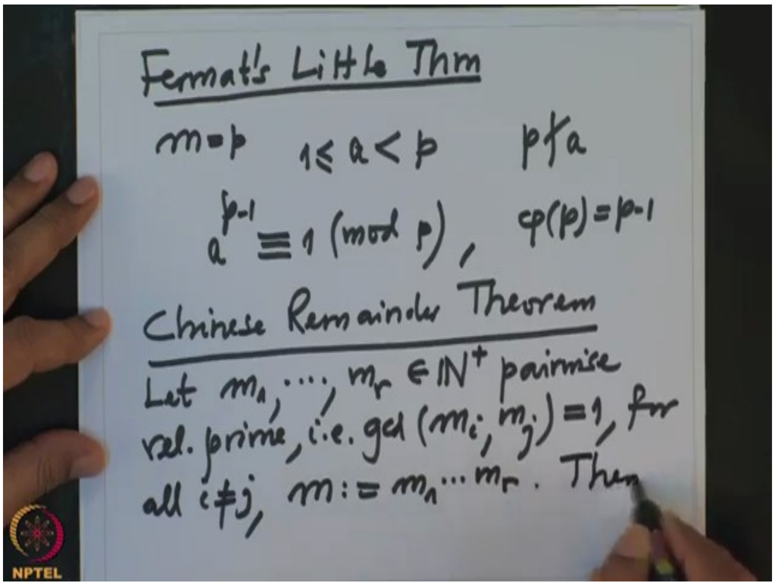
$$[a]_m^{\varphi(m)} = 1 \text{ in } \mathbb{Z}_m \quad \gcd(a,m)=1$$

$$\Longleftrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$$

Euler's Thm

That is say that cardinality of $\mathbb{Z}_m^x$ is precisely $\phi(m)$ where this ϕ is Euler's totient function this is Euler's totient function which maps any natural number m to $\phi(m)$ and $\phi(m)$ is by definition cardinality of all the integers, all the natural numbers a, $0 \leqslant a < m$ and gcd of a and m is 1; the number of coprime integers that is the $\phi(m)$, so the first thing to note is that because this is a group and order is $\phi(m)$ dividing any element there any element will look like any element is a residue and then if I raise to the power phi power m that should be 1 in these in $\mathbb{Z}_m$ but this is precisely writing this is equivalent to writing that if I raise $a^{\phi(m)}$ that is congruent to 1 mod m this is also called Euler's theorem, so this is under the assumption that gcd of a and m is 1, so this is Euler's theorem.

(Refer Slide Time: 07:54)



Fermat's Little Thm

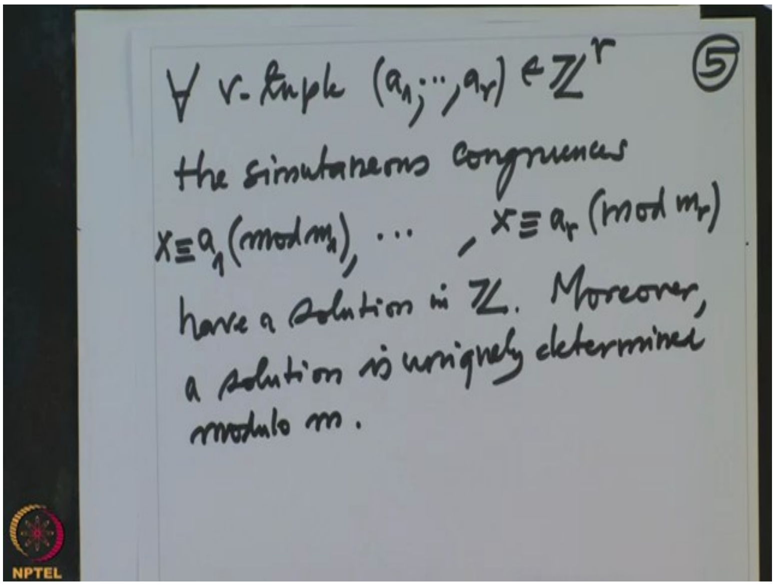
$m = p \quad 1 \leq a < p \quad p \nmid a$

$a^{p-1} \equiv 1 \pmod{p}, \quad \varphi(p) = p-1$

Chinese Remainder Theorem

Let $m_1, \ldots, m_r \in \mathbb{N}^+$ pairwise rel. prime, i.e. $\gcd(m_i, m_j) = 1$, for all $i \neq j$, $m := m_1 \cdots m_r$. Then

(Refer Slide Time: 09:55)



$\forall$ r-tuple $(a_1, \ldots, a_r) \in \mathbb{Z}^r$

the simultaneous congruences

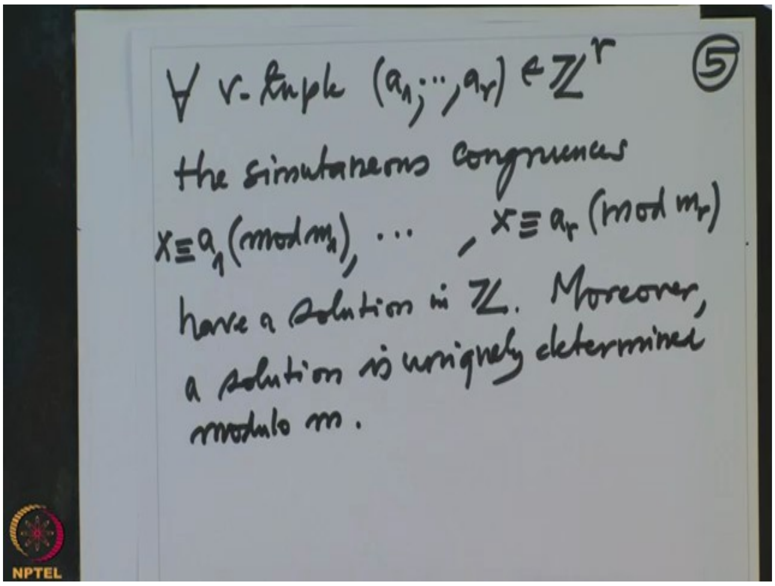
$x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$

have a solution in $\mathbb{Z}$. Moreover, a solution is uniquely determined modulo m.

(pa) Particular case we have seen earlier that is the famous Fermat's little theorem that says m is p here now any a smaller than p and bigger equal to 1 these are coprime to p does not divide a so therefore a^{p-1} is congruent to 1 mode p note that in this case $\phi(p)$ is $p-1$ because everybody is coprime to p, smaller than p so that is the Fermat's little theorem, ok now.

Now I want to recall what is called Chinese remainder theorem so Chinese remainder theorem this is about the solutions of simultaneous congruences simultaneous solution of a simultaneous congruences relations, so let m_1 to m_r be positive integers $\mathbb{N}^+$ which are pairwise relatively prime that simply means if I take any pair m_i and m_j they do not have any common factors that is gcd is 1 for all $i \neq j$ and let us take m is the product m_1 to m_r , then for every tuple of integers r tuple $(a_1, ..., a_r)$ of integers the simultaneous congruences X congruent to a_1 mod m_1 ,..., X congruent to a_r mod m_r have a solutions in Z. this simply means there exist in integers X so that X is congruent to a_1 mod m_1 , X is congruent to a_2 mod m_2 and so on X is congruent to a_r mod m_r , definitely there is a solution moreover a solution is uniquely determined modulo m solution may not be unique but when you go mode m that is unique solution. So this in the notation we can simply reformulate neatly as follows.

(Refer Slide Time: 11:31)



$\forall$ r-tuple $(a_1, \dots, a_r) \in \mathbb{Z}^r$ 5

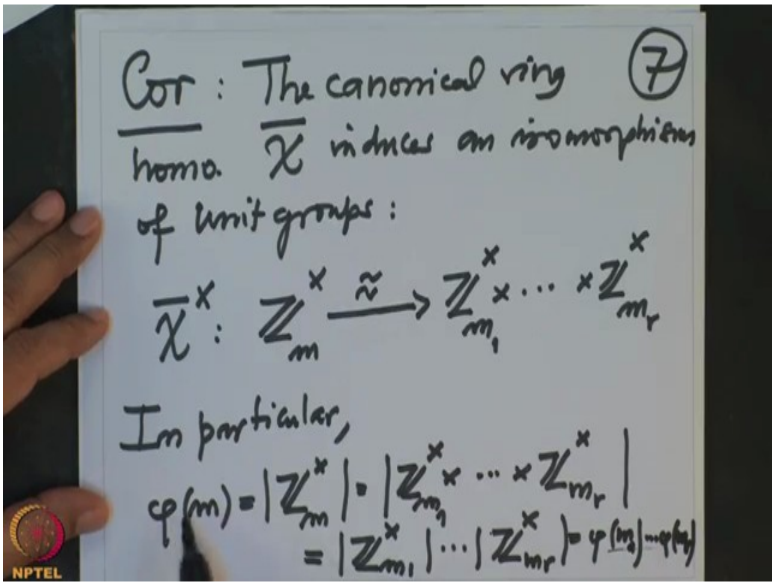
the simultaneous congruences

$X \equiv a_1 \pmod{m_1}, \dots, X \equiv a_r \pmod{m_r}$

have a solution in $\mathbb{Z}$. Moreover, a solution is uniquely determined modulo m.

So reformulation of CRT Chinese remainder theorem the canonical ring homomorphism $\bar{\chi}$ which is homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$, this is a product ring the component wise operations so any residue here a suffix m this maps to take that a and take the residues mode m_1 etcetera mode m_r this is a canonical map you just taking the residues this is an a isomorphism of a ring and surjetivity is what the existence of solution and the injectivity of this map is precisely uniqueness model, so this is also I will keep calling as Chinese remainder theorem, so proof is not very difficult so proof I am not going to prove this but I will note down some corollaries.

(Refer Slide Time: 13:17)



7

Cor: The canonical ring homo. $\overline{\chi}$ induces an isomorphism of unit groups:

$$\overline{\chi}^{\times} : \mathbb{Z}_m^{\times} \xrightarrow{\approx} \mathbb{Z}_{m_1}^{\times} \times \cdots \times \mathbb{Z}_{m_r}^{\times}$$

In particular,

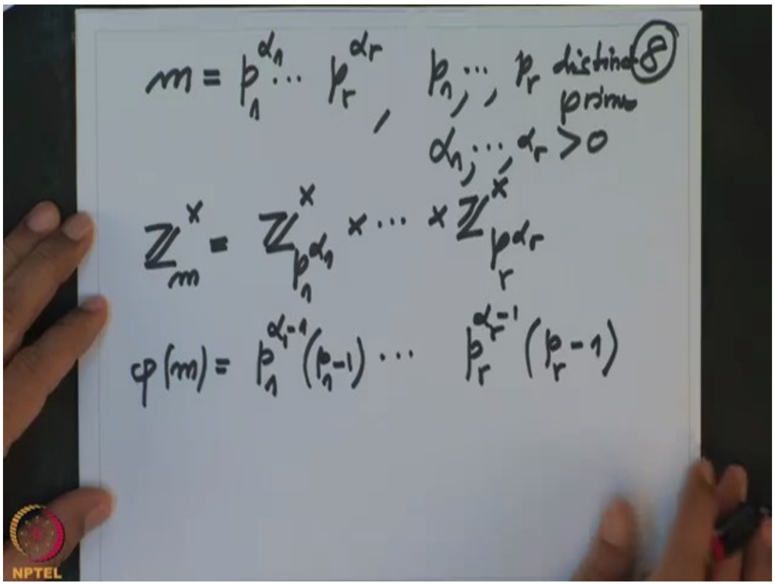
$$\varphi(m) = |\mathbb{Z}_m^{\times}| = |\mathbb{Z}_{m_1}^{\times} \times \cdots \times \mathbb{Z}_{m_r}^{\times}| = |\mathbb{Z}_{m_1}^{\times}| \cdots |\mathbb{Z}_{m_r}^{\times}| = \varphi(m_1) \cdots \varphi(m_r)$$

So for example, 1 corollary the canonical these canonical ring homomorphism $\overline{\chi}$ induces an isomorphism of unit groups that means this chi bar was from $\mathbb{Z}_m$, so the unit group of so that notation is $\overline{\chi}(x)$ this is $\mathbb{Z}_{m_x}$ to obviously the product ring the units are precisely the units in each component that means these are the this is a unit group of that product ring this is an isomorphism because at the ring level it is isomorphism so unit level it is an isomorphism.

So in particular the order of this group that we know it is phi m which is the order of the group $\mathbb{Z}_m^x$ but that is same as the order of this group $\mathbb{Z}_{m_1}^x \times ... \times \mathbb{Z}_{m_r}^x$ but these products is obviously the product of the unit group of $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_r}$ but obviously these is $\phi(m_1)...\phi(m_r)$ so therefore this means that ϕ is multiplicative function that means whenever you have relatively prime integers and when you apply ϕ to their product it is the product of the ϕ s.

So that was the (consequence) that is the property of the Euler's ϕ function.

(Refer Slide Time: 15:39)



8

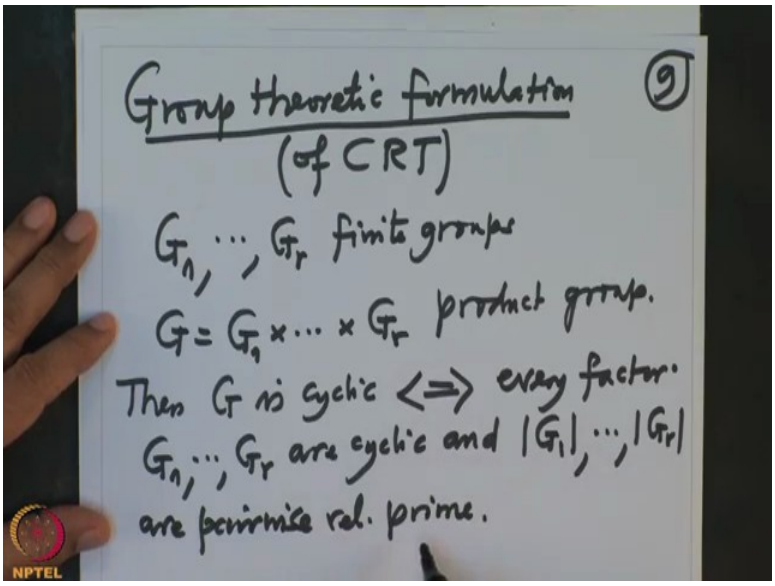
$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $p_1, \cdots, p_r$ distinct primes

$\alpha_1, \cdots, \alpha_r > 0$

$\mathbb{Z}_m^{\times} = \mathbb{Z}_{p_1^{\alpha_1}}^{\times} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}^{\times}$

$\varphi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$

(Refer Slide Time: 16.55)



9

Group theoretic formulation (of CRT)

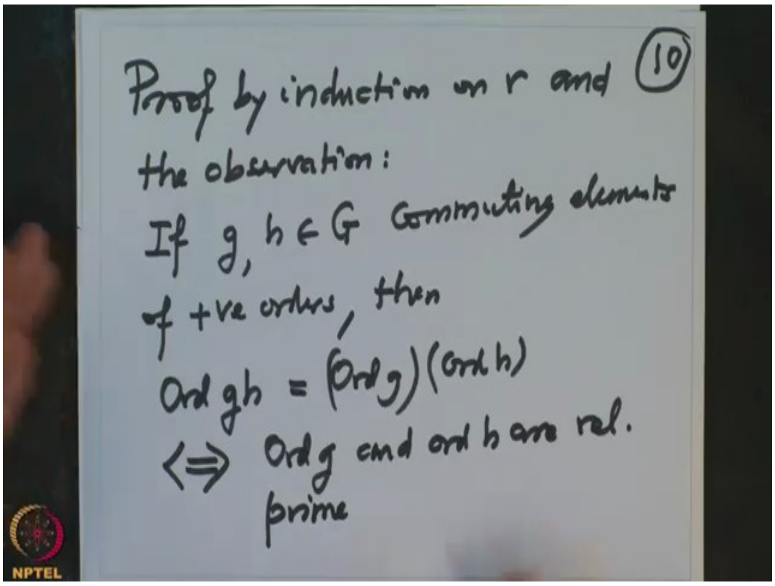
$G_1, \cdots, G_r$ finite groups

$G = G_1 \times \cdots \times G_r$ product group.

Then G is cyclic $\iff$ every factor $G_1, \cdots, G_r$ are cyclic and $|G_1|, \cdots, |G_r|$ are pairwise rel. prime.

So further if I specialized if I take precisely if I take m equal to look at the prime decomposition of $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ where p_1 to p_r are distinct primes and α_1 to α_r are positive natural numbers then $\mathbb{Z}_m^x$ is precisely $\mathbb{Z}_{p_1^{\alpha_1}}^x \times \ldots \times \mathbb{Z}_{p_r^{\alpha_r}}^x$ therefore their orders are equal that is $\phi(m)$ equal to modular of these group that is obviously $p_1^{\alpha_1 - 1} \times (p_1 - 1) \ldots p_r^{\alpha_r - 1} \times (p_r - 1)$ so nice formula for ϕ , also we can also formulate the Chinese remainder theorem completely in group theoretic terms so let me do it, so group theoretic formulations of CRT Chinese remainder theorem, so that is a following suppose you have G_1 to G_r are finite groups and let us denote G to with a product group with the component wise binary operation product group, ok then G is cyclic product group is cyclic that means it has primitive element if and only if a each factor every factor G_1 to G_r are cyclic and there orders are coprime and G_1 to order of G_1 to order of G_r are pairwise relatively prime.

(Refer Slide Time: 18:44)



Proof by induction on r and

the observation:

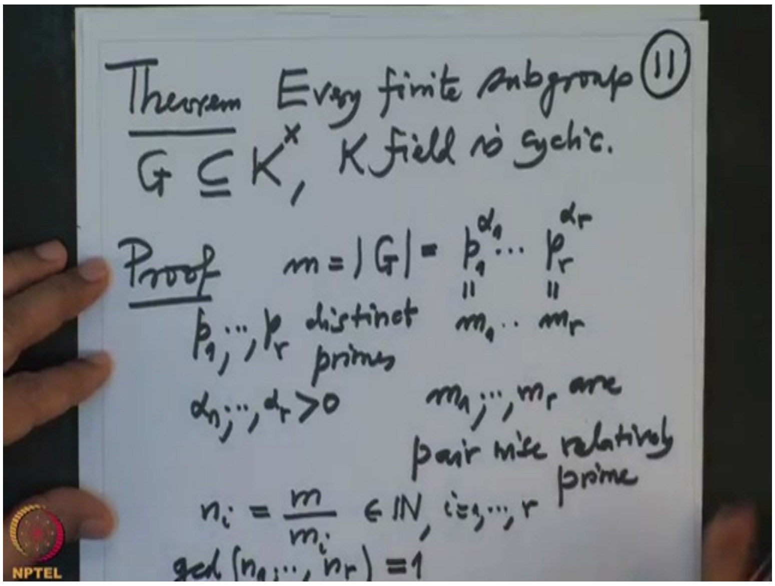
If $g, h \in G$ commuting elements of +ve orders, then

$$\text{Ord } gh = (\text{Ord } g)(\text{Ord } h)$$

$\Longleftrightarrow$ Ord g and ord h are rel. prime

So that this again I will not prove but this depends on this one can prove this I will just make one comment this can proved easily (by using) by induction proof by induction by induction on r and the observation following observation about the orders if g and h are two elements in a group commuting elements of positive orders then order of the product equal to product of the orders if and only if order g and order h are relatively prime this is this observation is very simple very easy to prove, so I leave it for you to check and now with this I will prove the theorem I wanted to prove.

(Refer Slide Time: 20:07)



Theorem Every finite subgroup (11)

$G \subseteq K^{\times}$, K field is cyclic.

Proof $m = |G| = \underset{m_1}{\overset{\shortparallel}{p_1^{\alpha_1}}} \cdots \underset{m_r}{\overset{\shortparallel}{p_r^{\alpha_r}}}$

$p_1, \dots, p_r$ distinct primes

$\alpha_1, \dots, \alpha_r > 0$ $m_1, \dots, m_r$ are pair wise relatively prime

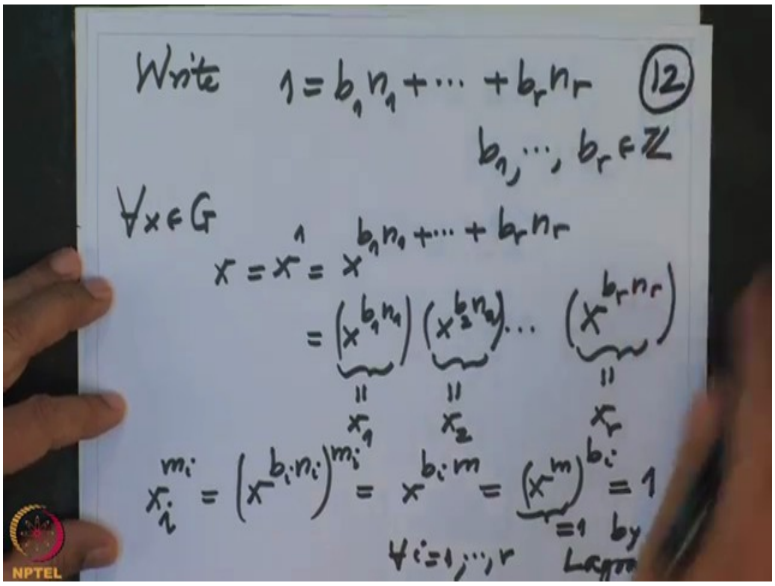
$n_i = \frac{m}{m_i} \in \mathbb{N}, i = 1, \dots, r$

$\gcd(n_1, \dots, n_r) = 1$

So that is the theorem every finite subgroup G of K^{x} where K is a field is cyclic, these what we wanted to prove, ok. K may not be a finite field, K may be infinite field also for example $K=\mathbb{C}$ or $K=\mathbb{R}$, so proof so let us look at the order of G, m is the order of G which is I will write other prime decomposition $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ where these p_1 to p_r are distinct primes and α_1 to α_r positive natural numbers.

So I will call these $p_1^{\alpha_1}$ as m_1 and $p_r^{\alpha_r}$ as m_r, so $m_1 \dots m_r$ are relatively prime down pairwise m_1 to m_r are pairwise relatively prime, so and now I define n_i to be equal to $\frac{m}{m_i}$, m is the product and I am just this mean that I am omiting m_i in the product, so these are integers, these are natural numbers i is from 1 to r and it is obvious that the gcd of n_1 to n_r is 1, So that means I can write 1 is a combination of n_1 to n_r.

(Refer Slide Time: 22:37)



Write $1 = b_1 n_1 + \cdots + b_r n_r$ $\boxed{12}$

$b_1, \cdots, b_r \in \mathbb{Z}$

$\forall x \in G$

$$x = x^1 = x^{b_1 n_1 + \cdots + b_r n_r}$$

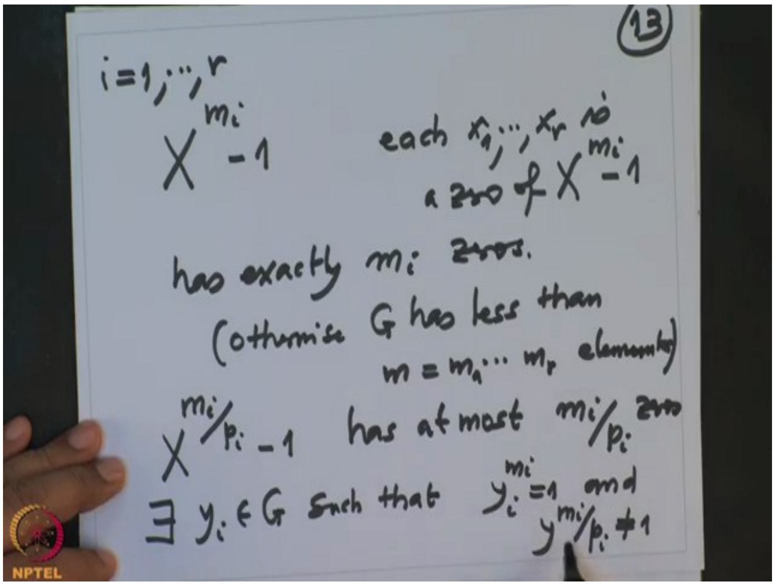
$$= \underbrace{(x^{b_1 n_1})}_{\substack{\parallel \\ x_1}} \underbrace{(x^{b_2 n_2})}_{\substack{\parallel \\ x_2}} \cdots \underbrace{(x^{b_r n_r})}_{\substack{\parallel \\ x_r}}$$

$$x_i^{m_i} = (x^{b_i n_i})^{m_i} = x^{b_i m} = \underbrace{(x^m)}_{=1 \text{ by Lagra}}^{b_i} = 1$$

$\forall i = 1, \cdots, r$

So write $1 = b_1 n_1 + \ldots + b_r n_r$, b_1 to b_r are integers and therefore if I take any x, so for every x in G therefore $x = x^1 = x^{b_1 n_1 + \ldots + b_r n_r}$ which is same as now these is same as $x^{b_1 n_1} x^{b_2 n_2} \ldots x^{b_r n_r}$ and these elements I want to call $x_{1,} x_2$ and x_r , so therefore every element we have written that is the product of r element x_1 to x_r and what is what about $x_i^{m_i}$ these is x_i is $x^{b_i n_i}$ and then raise it to the power m_i but that is same thing as $x^{b_i n_i m_i}$ is precisely m so these is $x^{m b_i}$ but this x^m element in group G whose order is m therefore this x^m is identity, so this is also identity and I am denoting identity by 1 because it is subgroup of K^x where 1 is identity, so this is true for every i from 1 to r these is if you like these is equal to one by Lagrange's theorem

(Refer Slide Time: 25:10)



13

$i = 1, \cdots, r$

$X^{m_i} - 1$ each $x_1, \cdots, x_r$ is a zero of $X^{m_i} - 1$

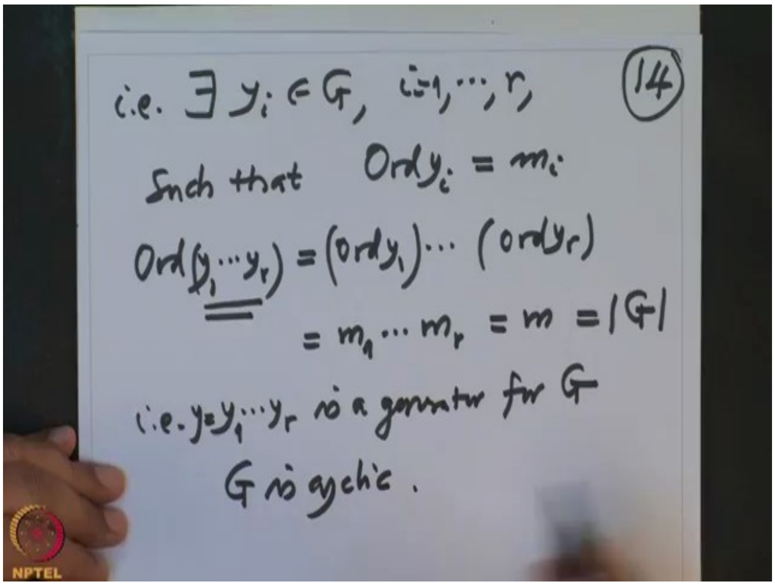
has exactly m_i zeros.

(otherwise G has less than $m = m_1 \cdots m_r$ elements)

$X^{m_i/p_i} - 1$ has at most m_i/p_i zero

$\exists\, y_i \in G$ such that $y_i^{m_i} = 1$ and $y^{m_i/p_i} \neq 1$

(Refer Slide Time: 28:32)



14

i.e. $\exists\, y_i \in G$, $i = 1, \cdots, r$,

Such that $\operatorname{Ord} y_i = m_i$

$\operatorname{Ord}(\underline{\underline{y_1 \cdots y_r}}) = (\operatorname{ord} y_1) \cdots (\operatorname{ord} y_r)$

$= m_1 \cdots m_r = m = |G|$

i.e. $y = y_1 \cdots y_r$ is a generator for G

G is cyclic.

So therefore $x_i^{m_i}$ is 1 for all 1 to r that is what we have checked but then remember we are over a field so now look at this polynomial, fix i from 1 to r and look at the polynomial $X^{m_i - 1}$ these polynomial we know because its polynomial or a field it has at most m_i zeros and I already know that each exercise is zero of these polynomial each x_1 to x_r is a zero of these polynomial it has at most m_i zeros and I know it has so many zeros if it has less number of zeros I want to claim that it has exactly m_i zeros because if it has less number of zeros then G will have you see here we have proved that every element of G is a product of x_1 to x_r , so if the number of zeros are of these polynomial is less than m_i than this meaning components are less, so by cardinality argument (it will) G will have less number of element, so these polynomial has exactly m_i zeros say otherwise would have less number of zeros otherwise G has less than m element m is $m_1 m_2 \ldots m_r$ elements.

So therefore G has these polynomial exactly has m_i zeros also moreover look at this polynomial $X^{\frac{m_i}{p_i}}-1$, these polynomial has at most $\frac{m_i}{p_i}$ zeros, so therefore we can find there exists an element y_i and G such that $y_i^{m_i}$ is 1 and $y_i^{\frac{m_i}{p_i}}$ is not 1, that is because you see these has to be the zero of these polynomial, so it is these and these has more zeros than these, so therefore I can find an element y which is zero of these but not zero of these that means y_i I can find so that $y_i^{m_i}$ is 1 and $y_i^{\frac{m_i}{p_i}}$ is not 1, But then this means the order of y_i so that is there exists $y_i \in G$, i from 1 to r such that order of y_i is precisely m_i because $y_i^{m_i}$ is 1 and $y_i^{\frac{m_i}{p_i}}$ is not 1 therefore order has to be m_i and these is to for every 1 to r and y_i is so therefore order of y_1 to y_r these product as earlier noted that is orders of products of the orders of y_1 to order of y_r and these is m_1 to m_r which is m which is order of G therefore these elements has to be a generator of a G.

So that is $y_1 \ldots y_r$, $y = y_1 \ldots y_r$ is a generator for G, so G is cyclic, this is what we wanted to prove, So we have proved that all finites of groups of the multiplicative group of a field is finite and we will used these fact in the next lecture to construct field arbitrary fields of cardinality p^n , so we will continue after the break.