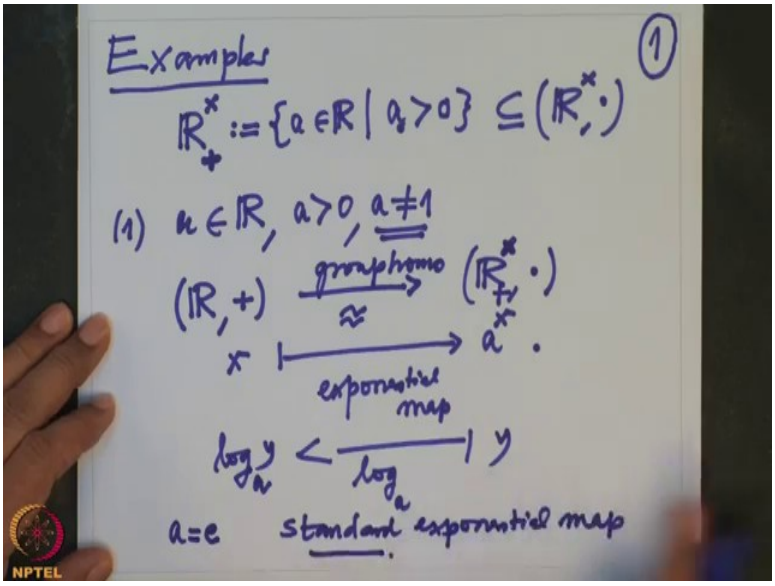
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 20
Some Examples and Characteristic of a Ring

Now we are discussing finite groups I also like to have some examples of the groups which are not finite but arguments etc so I would like to spend some time on explicit examples which are very useful not only in algebra but even analysis courses. Couple of such groups before I actually prove the theorem as stated I want to discuss some examples.

(Refer Slide Time: 00:59)



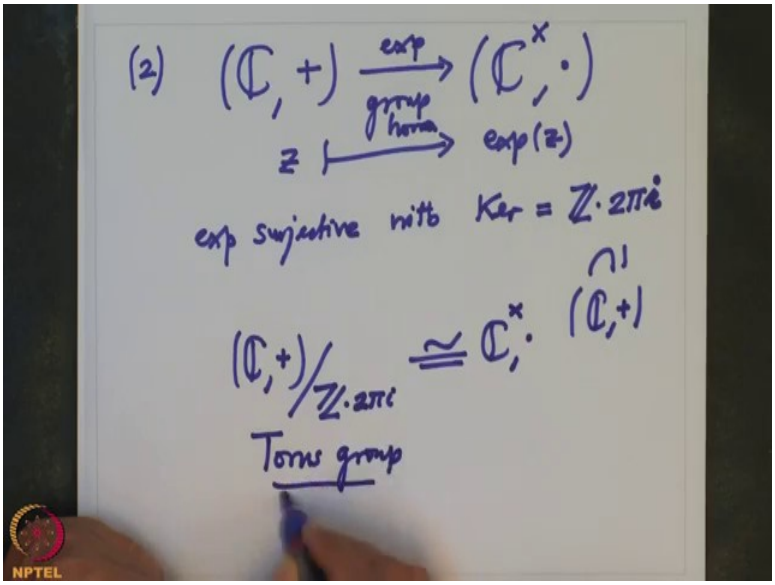
Alright so the examples that I want consider are for example the groups so let us let me write the groups these are groups R^x of course this is a group under multiplication but not only this, if I take the positive ones. So this are precisely the positive real numbers a real numbers in non-zero, non-zero I don't write because it is a positive this is clearly a group under multiplication this is a sub-group of R^x because if I take two positive real number then multiplication is also positive the inverse is also positive and so on. So this is a sub-group of this, so this sub-group so to understand this sub-group what is this sub-group? For example, see when one wants to understand groups one want to understand them in terms of the known groups.

For example I want to understand this group in terms of the additive group of real numbers so in terms of that so what do we do for that? So let us look at so let me write the number 1, so let us take any a which is a real number positive real number and did not equal to 1 you will see why I am assuming not equal to 1. What is the identity element in this group? One is identity element in this group alright so look at the map R under addition to R what is the map? Take any x in the real number and map it to a^x , x is a real number a is number which is not 1 and so this is a map.

What kind of a map it is this? When you have when you add the numbers and you take the exponential the exponential laws will tell you this map is actually a group homorphism . So there is this is a group homorphism to which group now, let us be more precise (R,+) to (R,.) and this will never be zero, so it will actually be a map from non-zero real (numb) inside the non-zero real number not only that this will never be negative. So therefore it is actually a map from R plus to this group we wanted to study this is called an exponential map.

This is the standard way to convert additive structure to multiplicative structure and I want to actually check that this map is an isomorphism this is a group isomorphism. So what do I do? For that I have to give the map in the other direction but the map in the other direction is clear y goes to $\log_a y$ this is and this is the $\log_a y$. So this two maps are inverses of each other so when you want to study this group it is equivalent to study the real numbers group and in particular one wants to study this one want to take a equal to e then you get a Euler's exponential map, this is a standard exponential map. Alright so that is one thing now the same thing if you do it for complex numbers, what do you get?

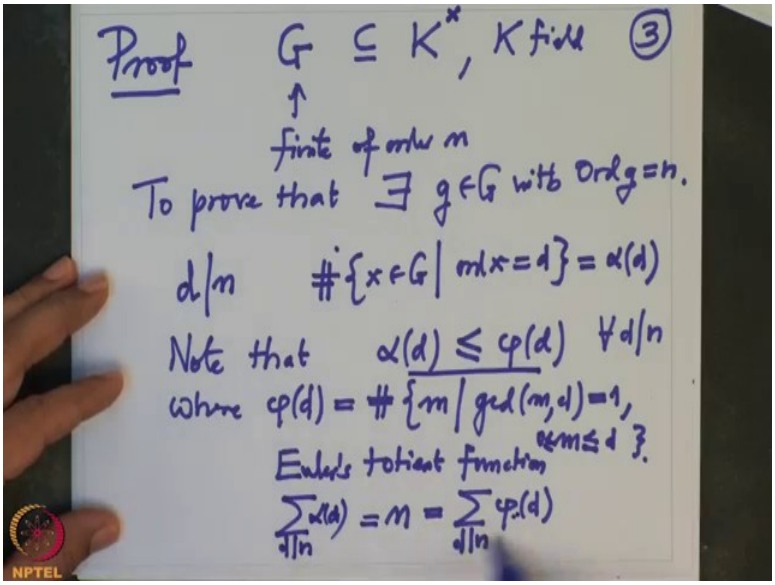
(Refer Slide Time: 5:50)



Now I will be little bit brief because I have to save some time. So now if you take the group ($\mathbb{C}$,+) and the whole multiplicative groups ($\mathbb{C}^x$,.) remember there is no positive negative in complex number what we did in real numbers and there is a natural map here namely z going to e^z and then obvious property tells you that this map is a group homorphism this is a group homorphism. So that the standard property of the exponential that we study in the (this is expo) the usual calculus first calculus course tells you this is a group homorphism this denoted by exp.

Now it is surjective this exp is surjective and the Kernel is what? Kernel is precisely (the kernel is precisely) generated is a sub-group generated by $2\pi i$, $\mathbb{Z}2\pi i$ that is this is additive sub-group of ($\mathbb{C}$,+) so that means that if I go mod the kernel ($\mathbb{C}$,+) mod this $\mathbb{Z}2\pi i$ this is isomorphic to ($\mathbb{C}^x$,.) multiplicative group. This group is often called a Torus group ok more than that I will not say right now. So this are two important groups which will come up in our study sometime ok now third one. Now I want to resume the proof that G is finite.

(Refer Slide Time: 8:14)



So proof, what we wanted to prove, we wanted to prove that if G is a sub-group of $K \times K$ is a field and the G is finite then G is cyclic alright. So what do we wanted to prove? G is finite let us say of order n then I want to prove that there is so to prove that there exists an element g in G with order of g equal to n, this is what we wanted to prove. Alright so note that if I take we have noted already that if I take elements of G and their orders they are divisors of the order of G this is precisely the Fermat's Little Theorem.

So we know on the other hand I want to know if d divides n, d is a divisor of n then I want to denote this set all those elements x in G such that order of x is d this set I want to denote by something I don't need to denote I want to denote the cardinality of this set by some it will depend on this d. So I want to denote it by $\alpha(d)$ this is the cardinality. Look it may happen that this set is empty and there is no element of order $\alpha(d)$ and our problem is to prove that if I take d equal to n then alpha of n is non-zero, non-zero means there is an element of that order.

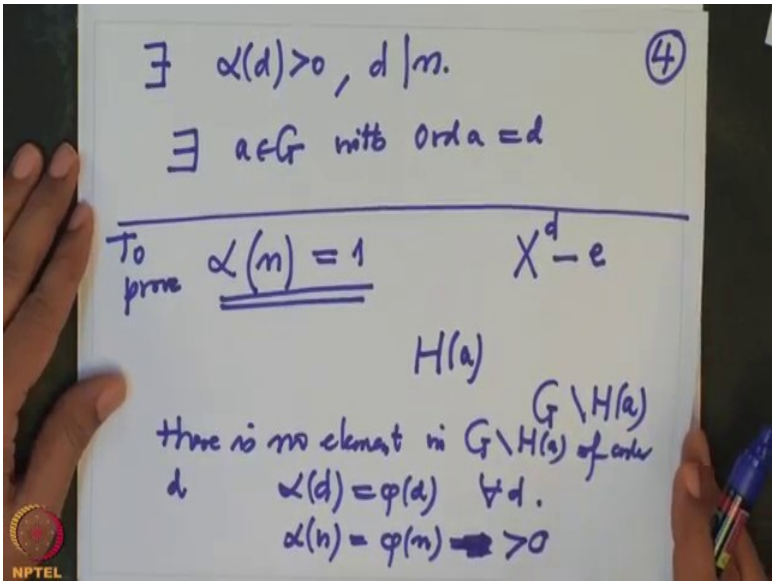
Ok so what do we know? Only element of d what is the what is the bound on $\alpha(d)$? $\alpha(d)$ note that $\alpha(d)$ is less equal to $\phi(d)$ where $\phi(d)$ is Euler's c function this is true for every d of n where $\phi(d)$ is Euler's this is the number of elements m such that GCD of m and d equal to 1 and m is small or equal to d. So this is called Euler's quotient function this is number of element which are smaller equal to d and of course positive not negative so that the GCD is 1

this is $\phi(d)$ and what do we know about this Euler's ϕ function the nice formula which I will prove when I introduce group actions.

So nice formula is if I take m this is same as the sum of all $\phi(d)$ where d divides n sum is runnign over all divisors of n this is $\phi(d)$ and how does one prove this formula? This is very easy to prove just use this for cyclic group of order n and then count the number of elements of order d there they are precisely the GCD co-prime etcetra so this formula I will take it under today. On the other hand if I take any divisor of d and take this $\alpha(d)$ and now in I have exhausted all the elements (so the) on the other hand this n is also same as $\alpha(d)$ where d divides n.

So I have this equality and also I have this so if all the numbers are strictly smaller than if all $\phi(d)$ they are strictly smaller than if $\alpha(d)$ are strictly smaller than $\phi(d)$'s then this cannot be equality.

(Refer Slide Time: 13:34)



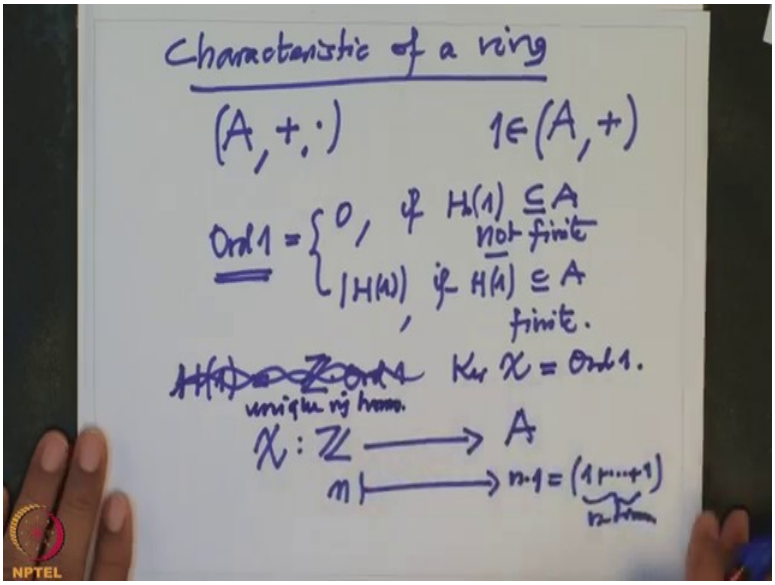
Therefore from this we conclude that (we conclude here from that) there is an element there exists an element as a divisor so that $\alpha(d)$ is positive d is some divisor of n. So that means what? There exists an element a in G with order of a to be d. If the order of d is to be alright so I want to actually prove that what do we want to prove? Let us analyze what we want to prove?

I want to prove that alpha of n is 1 I want to prove this is what we want to prove (to prove) alright so if there is some d so that $\alpha(d)$ is positive and then there is an element of order d then what happen? Then look at this equation X power d minus identity this equation. So in this equation definitely therefore if I remove if I look at the sub-group generated by a this is H a this sub-group of order d and all other elements of order d are also contained there because so therefore if I remove if I look at this equation in with G minus H a in this there is no element (no element) in G minus H of a of order d.

Therefore what we will conclude that is $\alpha(d)$ equal to $\phi(d)$ actually for every d in particular $\alpha(n)$ equal to $\phi(n)$ which is 1 and therefore there is an element of order no $\phi(n)$ is definitely non-zero because they are definitely co-prime numbers to n. So therefore $\alpha(n)$ is therefore positive that means there is an element of order n and therefore G as an element of order n and that is what we wanted to prove that will in particular say that G is cyclic, this proof also I am going to improve the problem here is I am not using so called group actions.

Once I start using group actions this proves will get even improved ok so I will not say much about it but now I want to prove the theorem that I wanted to prove that given a prime number p there is a field with cardinality p^n ok before I do that so let us say I need a concept of characteristic, characteristic of a field, of a field or a ring. So we have a ring a, a ring means we have two operations so that it is a ring and I will assume easily commutative so we have this ring and we have additive group this is a group and then an element here the (additive) identity is usually denoted by zero multiplicative identity is 1 so 1 be an element here.

(Refer Slide Time: 18:05)



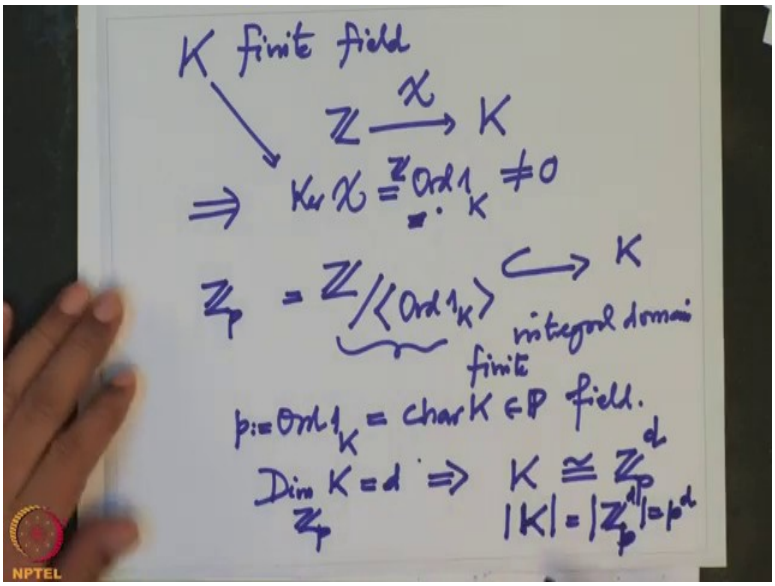
So it makes sense to talk about the order of 1, what is order of 1? Order of 1 is by definition you take a sub-group generated by 1 so take H of 1 this is additive sub-group of A and if it is finite the order is the cardinality if it is infinite if it is not finite then the order is 0, this zero if $H(1)$ is not finite and cardinality of $H(1)$ if $H(1)$ is finite. Let us see what $H(1)$ is, what is $H(1)$? $H(1)$ is a sub-group generated by 1 right that means we have to keep and remember then binary operation is plus. So you have to keep adding one. So if you if this was finite after adding one sufficiently many times it will become zero. So that is the case when this H a is $H(1)$ is finite.

Never becomes finite means no matter how many times you add one you will never get zero so that means the order of one is either zero or this set. So what is $H(1)$? $H(1)$ is precisely sub-group of A generated by 1 but that is precisely z times order 1 that is what will be said you know, so how many times it will go on if order 1 is not if it is this is not finite it is z otherwise it will be some Z mod order. So this is the order ok so in other ok so what is the characteristic? That is order 1, so that means this order 1 is a Kernel you remember this as a the map χ from $\mathbb{Z}$ to the ring A namely any m raise to n time 1 that means m and $1+1+\ldots$ either 1 n times or minus n times and the kernel of this is precisely the order.

So I am saying something wrong here, so this is not correct kernel of this χ is precisely the order of 1 so that means ok. So that is precisely the characteristic we defined in the earlier way

also in the earlier definition also it is a generator of the kernel of this χ map this χ is unique homorphism and the generator is called the characteristic that is order 1.

(Refer Slide Time: 21:47)



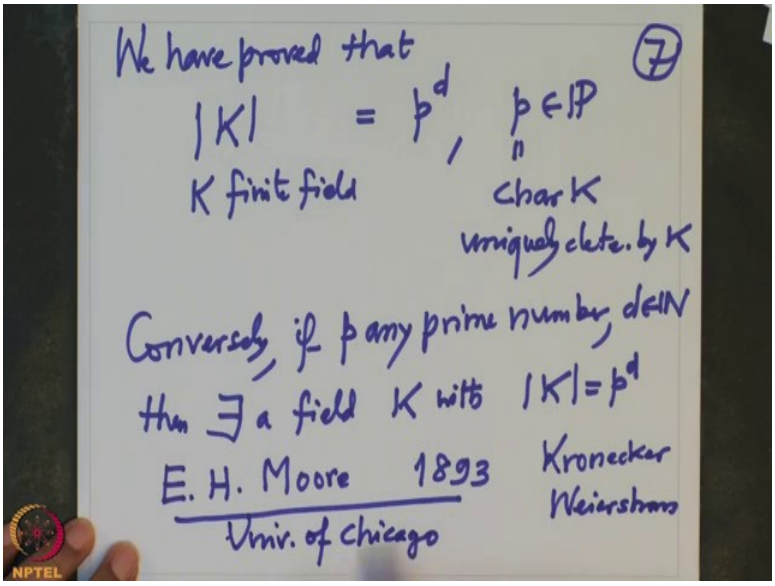
Ok so now if you have a finite field so let us take K to be finite (finite field) then this is a finite set and $\mathbb{Z}$ to K this χ map is definitely will have a non-zero kernel if it is in kernel is zero that means this $\mathbb{Z}$ is sits inside K injectiveley so that cannot happen $\mathbb{Z}$ is infinite K is finite so definitely because this K is finite Kernel of χ which is order of 1 this 1 is I K this is not zero, this is generated by the order of 1 which is not zero.

So therefore there is a injective map from $\mathbb{Z}$ mod let us call this as some number n so this $\mathbb{Z}$ mod generated by order 1 K this is inside goes inside K but K is a filed so therefore this is a sub-ring of the field which is also integral domain (integral domain) but is domain and it is finite because this is non-zero so this is finite integral domain, finite integral domains are fields so therefore this is a field and therefore this order of K order of 1 K which is precisely the characteristic of K which is a prime number this is P so this is small p let us call it, therefore we have plead that the characteristic of a finite field is always a prime number p and then we have K here and this is what?

This is nothing but $\mathbb{Z}_p$ in the notation this $\mathbb{Z}_p$ is a sub-field of this, this is finite therefore if you think this K as a vector space over $\mathbb{Z}_p$ the dimension of K as a vector space over

$\mathbb{Z}_p$ this is some d then what? Then that will mean that this K is isomorphic to $\mathbb{Z}_p$ vector space of dimension in this is Z power d that means cardinality of K is precisely cardinality of $\mathbb{Z}_{p^d}$ which is p^d . So therefore what did we prove? We have proved that if K is a finite field then the cardinality must be power of p.

(Refer Slide Time: 24:40)



So I will note it what we have proved so 7 we have proved that cardinality of a finite field K finite must be p power some d or p is some prime number and in fact that p has to be characteristic of K which is this p is uniquely determine by K.

Now I want to prove the conversely, converse is conversely if p ant prime number and d is any natural number then there exists a field capital K with cardinality p^d ok. So this was first proved by this was proved by E. H Moore in 1893 this Moore was a student of Kronecker and Weierstrass actually Moore was from Chicago University of Chicago and those there was it was not possible to do PhD in mathematics in America. So they were going to Europe especially to Germany and France they going there to do PhD's and E. H Moore was the first mathematician in America who has worked extensively on the fact that to start a PhD program in America and that was possible in the early 20th century after the big efforts of Moore.

This Moore is the one who proved this theorem I will continue this proof in the next lecture. So remember today I have only I have made a digression on the groups and ultimately our course

revolves around using group theory in theory of equations, solutions of equations. Solutions of equation was much more older than the group theory subject but nowadays group theory is much more taught that the theory of equation and I also want to stress more on theory of equations so we will come back to theory of equation we will keep coming back and going this whole course we keep a roller coaster between the group theory and theory of equations, thank you.