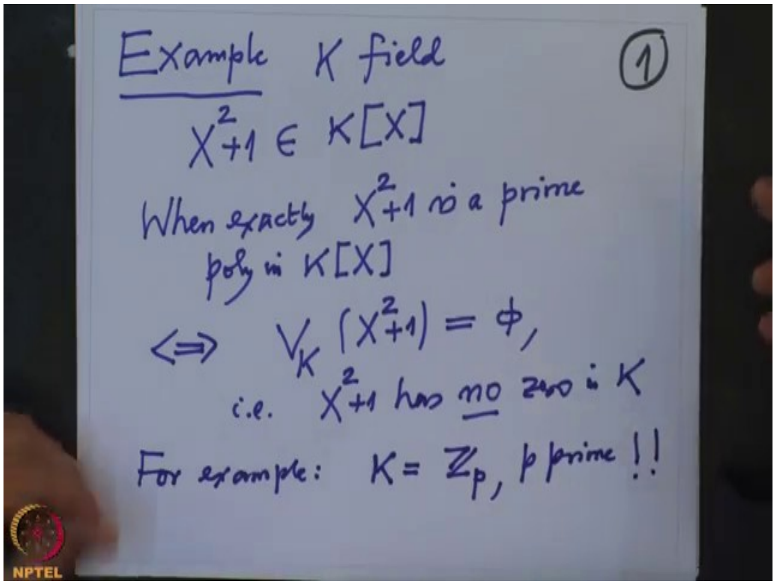
**Galois Theory**
**Professor Dilip P. Patil**
**Department of Mathematics**
**Indian Institute of Science, Banglore**
**Lecture 18**
**Examples**

Alright, in the last lecture we saw that particular polynomial degree 2 $X^2+1$, as a polynomial with real coefficients this polynomial is a prime polynomial and which is equivalent to the fact that this polynomial doesn't have a zero inside the field of real numbers I want to generalize this or I want to analyze for a general field when can this particular polynomial is prime polynomial in $K[X]$ or equivalently when can this polynomial has low zero inside the given field K.

(Refer Slide Time: 1:14)



Example K field 1

$X^2+1 \in K[X]$

When exactly $X^2+1$ is a prime poly in $K[X]$

$\Longleftrightarrow V_K(X^2+1) = \phi$,

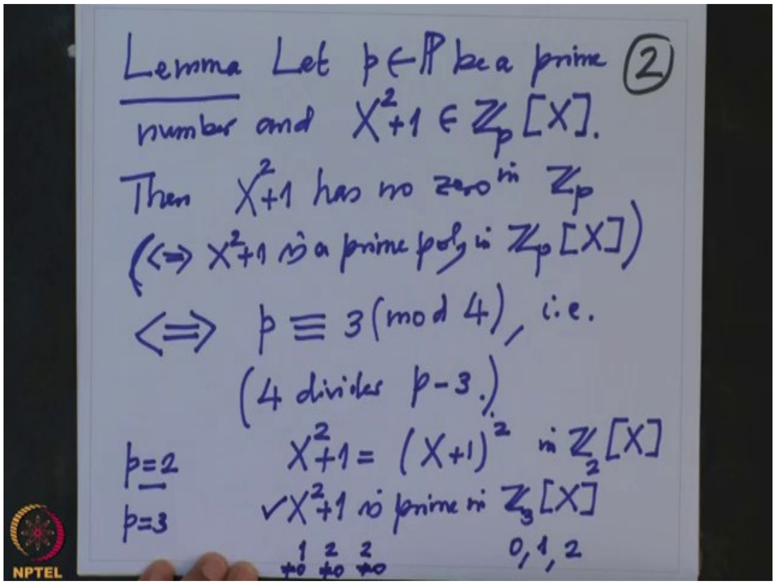
i.e. $X^2+1$ has no zero in K

For example: $K = \mathbb{Z}_p$, $p$ prime !!

So we are going in this example we are going to analyze this situation, example, K field and we consider this very special polynomial $X^2+1$, this is a polynomial of degree 2 in the field K over a field $K[X]$ over a field K, so it is a polynomial in $K[X]$. So when exactly $X^2+1$ is a prime polynomial in $K[X]$. This is equivalent to saying the zeroes of this polynomial inside K there is nobody, this is empty side. So this means so that is $X^2+1$ has no zero in K, this is what we want to analyze, for example when you take a field K to be equal to the finite field $\mathbb{Z}_p$ where p is prime, in this case we want to analyze.

So that will give us extensions of the field $\mathbb{Z}_p$ of degree 2, because this is a degree 2 polynomial, we prove the following lemma.

(Refer Slide Time: 3:07)



Lemma Let $p \in \mathbb{P}$ be a prime 2
number and $X^2+1 \in \mathbb{Z}_p[X]$.
Then $X^2+1$ has no zero in $\mathbb{Z}_p$
($\Leftrightarrow X^2+1$ is a prime poly in $\mathbb{Z}_p[X]$)
$\Longleftrightarrow p \equiv 3 \pmod{4}$, i.e.
(4 divides $p-3$.)

$p=2$ $\quad X^2+1 = (X+1)^2$ in $\mathbb{Z}_2[X]$

$p=3$ $\quad$ ✓ $X^2+1$ is prime in $\mathbb{Z}_3[X]$

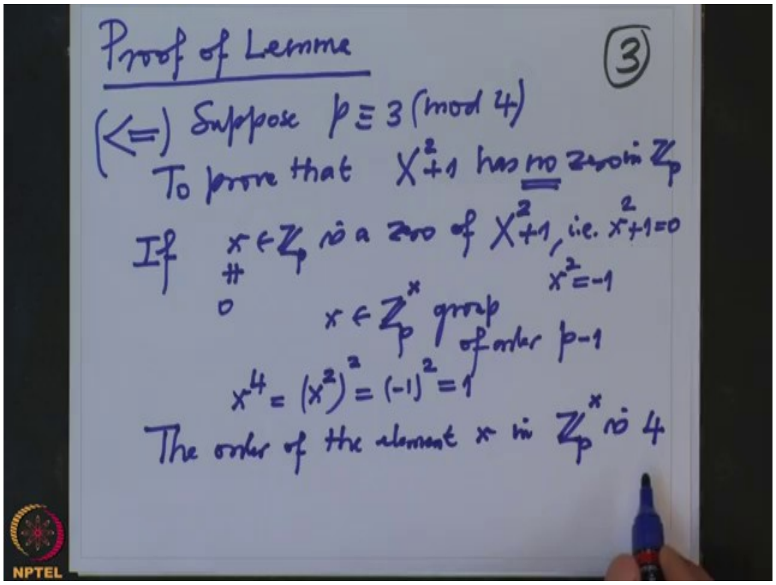
$\overset{1}{\neq 0}\ \overset{2}{\neq 0}\ \overset{2}{\neq 0}$ $\quad$ 0, 1, 2

So this is a lemma, let p be any prime number, p belong to P be a prime member and consider the polynomial $X^2+1$ as a polynomial in $\mathbb{Z}_p[X]$, then $X^2+1$ has no zero in $\mathbb{Z}_p$, we have seen that this is equivalent to saying $X^2+1$ is a prime polynomial in $\mathbb{Z}_p[X]$ this also we have seen we have just remarked about but this is equivalent to saying in terms of the numerals this (this is con) this is equivalent to saying p is congruent to 3 mod 4. So that is 4 divides p minus 3 that is equivalent to saying this alright.

So let us test for few small values of p, lets take p equal to 2 then p is not congruent to 3 mod 4, p is congruent to 2 mod 4 but then in this case $X^2+1$ is seen as X plus 1 whole square because p is a characteristic so it is this and therefore this polynomial actually has a zero one as a zero of X. So in $\mathbb{Z}_2[X]$, in $\mathbb{Z}_2[X]$ actually this $X^2+1$ splits into linear factors, alright. Where if such a thing then should test for p equal to 3 then p indeed congruent to mod 4, therefore by our observation this lemma is $X^2+1$ is a prime polynomial in $\mathbb{Z}_3[X]$, this you can test very easily because Z, this is a degree 2 polynomial, if it is not prime then it will have a zero and the only possibility for zero is 0, 1 and 2, because this are the only elements of $\mathbb{Z}_3$ and to check take each of them and plug it in here and see whether it is zero or not.

So when you plug it X equal to zero, this is one which is (now) which is not zero when should plus it in 1 then it is 1 plus 1 2 which is definitely not zero and if you plug it in 2 that is $2^2$ is 4, 4 plus 1 5, 5 mod 3 is 2 which is zero again. So therefore this is a prime polynomial in $\mathbb{Z}_3[X]$, alright.

(Refer Slide Time: 6:47)



Proof of Lemma ③

(⇐) Suppose $p \equiv 3 \ (\mathrm{mod}\ 4)$

To prove that $X^2+1$ has no zero in $\mathbb{Z}_p$

If $x \in \mathbb{Z}_p$ is a zero of $X^2+1$, i.e. $x^2+1=0$

$x \neq 0$ $\quad$ $x^2=-1$

$x \in \mathbb{Z}_p^*$ group of order $p-1$

$x^4 = (x^2)^2 = (-1)^2 = 1$

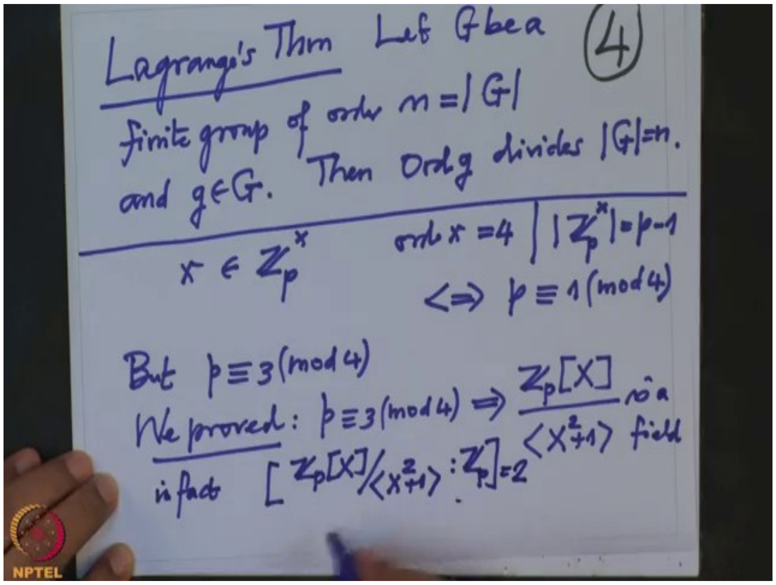
The order of the element $x$ in $\mathbb{Z}_p^*$ is 4

So we prove this, so proof of lemma, lemma is two parts so we will first prove this way that means we will suppose p is congruent to 3 mod 4 and we want to check that the polynomial $X^2+1$ is has no zero.

To prove that $X^2+1$ has no zero in $\mathbb{Z}_p$, no, alright. So suppose it is a zero, so suppose if x in $\mathbb{Z}_p$ is a zero of $X^2+1$ so that means when I plug it in capital X equal to small x it becomes zero, $X^2+1$ is zero but definitely this x is not zero because if x were zero then $X^2+1$ this is 1 and 1 equal to 0 is not possible, so x is definitely not zero and this equation will tell you $X^2$ equal to minus 1 but then x is non-zero element in the field, so x belong Z because this is a group because $\mathbb{Z}_p$ is a field and this is a group of order one less element in $\mathbb{Z}_p$ that $p-1$.

So this is a group under multiplication of order $p-1$ and x is a one element there, so that $X^2=-1$ so therefore $X^4$ will be equal to $X^2$ but $X^2-1$ and minus 1 square is 1. So x power 4 is 1, so this means the order of the element (order of the element) small x in the group is 4 because x is not null and $X^2-1$. So therefore the smallest power of x which becomes identity in the group is precisely 4. So order x is 4. But let me recall I have only used here very easy theorem (when) the in fact it is the first theorem in when one start studying finite groups.

(Refer Slide Time: 10:02)



4

Lagrange's Thm Let G be a finite group of order $n = |G|$ and $g \in G$. Then Ord g divides $|G| = n$.

$x \in \mathbb{Z}_p^{\times}$ ord $x = 4 \mid |\mathbb{Z}_p^{\times}| = p-1$

$\iff p \equiv 1 \pmod 4$

But $p \equiv 3 \pmod 4$

We proved: $p \equiv 3 \pmod 4 \Rightarrow \frac{\mathbb{Z}_p[X]}{\langle X^2+1 \rangle}$ is a field

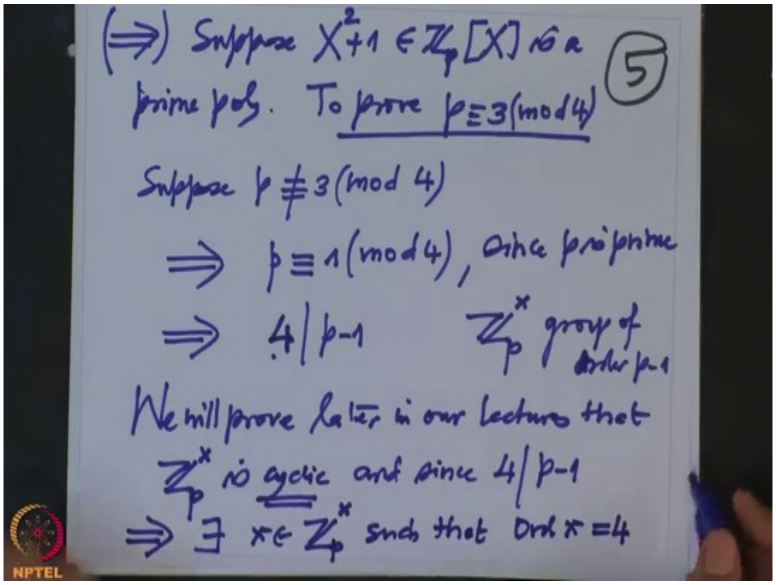
in fact $[\mathbb{Z}_p[X]/\langle X^2+1 \rangle : \mathbb{Z}_p] = 2$

The first is theorem is called, is due to Lagrange, so this is Lagrange's theorem that say that G if, let G be a finite group, G be a finite group of order n that is and if the cardinality of G and g is a an element in G then the order of g, small g divides order of G which is n, this is known as Lagrange's theorem, Lagrange have discovered this theorem while he was studying the relations between the roots of a polynomial and the coefficients of the polynomial and especially when he was dealing with rational functions fields in many variables and the permutation group operating on this and studying the fixed points etc-etc during that time he has guess the theorem which his offcourse very easy to prove but Lagrange never dealt with groups, ok.

So we have a situation x over an order an element in $\mathbb{Z}_p^x$ and order of x is 4 but then 4 should divide the order of $\mathbb{Z}_p^x$ but $\mathbb{Z}_p^x$ is order $p-1$ so 4 should divide $p-1$ but this is equivalent to saying p is congruent to 1 mod 4 but our assumption was (that our assumption was) was p was congruent to 3 mod 4 which contradicts our assumption that the polynomial $X^2+1$ has a zero inside this. So therefore we have proved one way implication. Now conversely so we have proved that so we have proved we proved if p is congruent to 3 mod 4 then $\mathbb{Z}_p[X]$ modulo ideal generated by $X^2+1$, this is a field.

It I an extension field of $\mathbb{Z}_p$ and degree of the field extension is true. So in fact the degree of $\mathbb{Z}_p[X]$ modulo the ideal generated by $X^2+1$ in this field over $\mathbb{Z}_p$ this degree is 2, this is exactly like real numbers, complex numbers.

(Refer Slide Time: 13:49)



(⇒) Suppose $X^2+1 \in \mathbb{Z}_p[X]$ is a prime poly. To prove $p \equiv 3 (\text{mod } 4)$ 5

Suppose $p \not\equiv 3 (\text{mod } 4)$

⇒ $p \equiv 1 (\text{mod } 4)$, since p is prime

⇒ $4 | p-1$ $\mathbb{Z}_p^\times$ group of order $p-1$

We will prove later in our lectures that $\mathbb{Z}_p^\times$ is cyclic and since $4 | p-1$

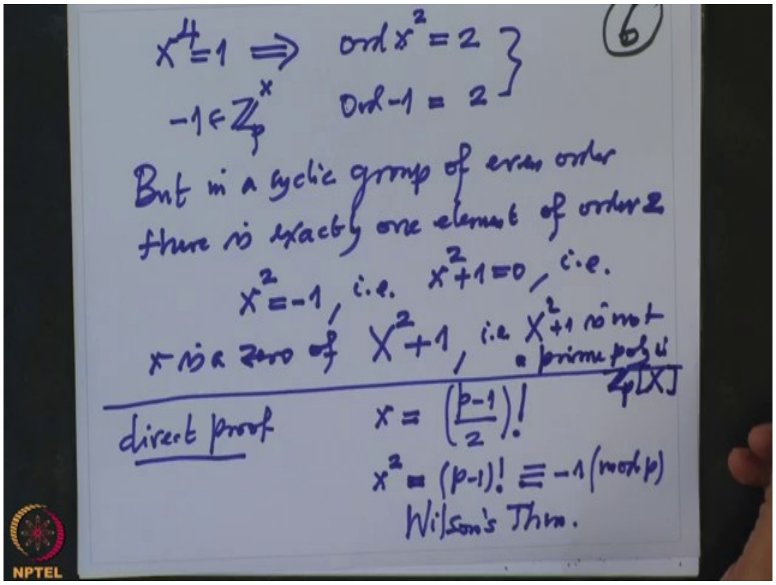
⇒ $\exists$ $x \in \mathbb{Z}_p^\times$ such that Ord $x = 4$

Now we want to prove the converse, so we want to prove this way, so that means we want to prove that so suppose $X^2+1$ in $\mathbb{Z}_p[X]$ is a prime polynomial and we want to prove, so to prove from here that p must be congruent to 3 mod 4, this is what we want to prove.

So suppose not, suppose p is not congruent to 3 mod 4, so what are the possibilities for p? Then p must be p cannot be congruent to 2 mod 4 because p is a prime number. So therefore only possibility is p has to be congruent to 1 mod 4, since p is prime. So once p is congruent to 1 mod 4 that means what? That means, 4 divides $p-1$ and we are in this group now $\mathbb{Z}_p^x$, this is a group of order $p-1$ and I want to use the fact that this group is cyclic. We are going to prove this we will prove later in our lectures that this group $\mathbb{Z}_p^x$ this group is cyclic and I have a prime we have a devisor 4 of these order of this group so and since 4 divides $p-1$ there exists an element x in this group such that order of that element order of x equal to 4.

This is true because in every cyclic group every divisor of the group order of the group in a cyclic group in a finite cyclic group every for every divisor of an order of the group there is an element of that order, so that is what I have used this is a cyclic group 4 here divisor of the order therefore there is an element x in that group of order 4.

(Refer Slide Time: 17:28)



(6)

$x^4 = 1 \Rightarrow \operatorname{ord} x^2 = 2$

$-1 \in \mathbb{Z}_p^\times \quad \operatorname{Ord} -1 = 2$

But in a cyclic group of even order there is exactly one element of order 2

$x^2 = -1$, i.e. $x^2+1=0$, i.e.

$x$ is a zero of $X^2+1$, i.e $X^2+1$ is not a prime poly in $\mathbb{Z}_p[X]$

direct proof $\quad x = \left(\frac{p-1}{2}\right)!$

$x^2 = (p-1)! \equiv -1 \pmod{p}$

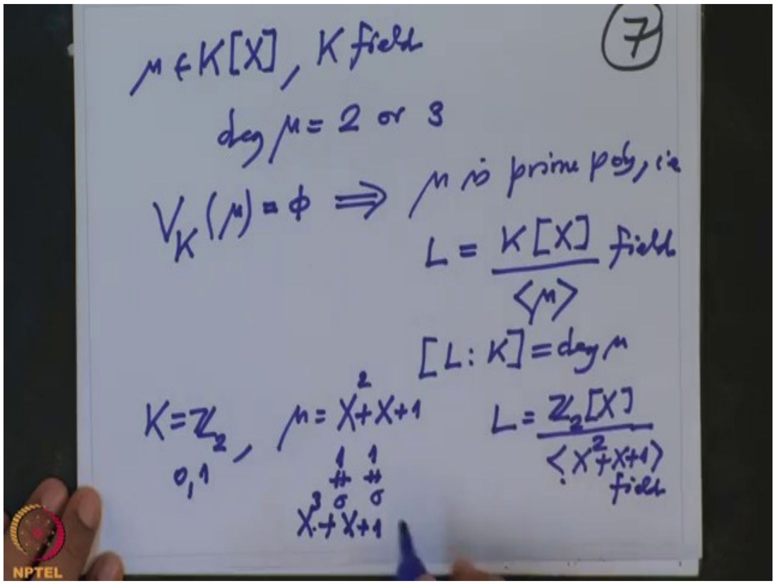
Wilson's Thm.

Once you have this order is 4, so x raise to 4 is 1 but then order of what will be the order of $x^2$ order of $x^2$ has to be 2 in minus 1 is an element in $\mathbb{Z}_p^x$ and what is the order of $-1$ ? Order of minus 1 is also 2 but then there is only in a cyclic group of even order that but in a cyclic group of even order there is exactly one element of order 2 but here we have likely the two elements $x^2$ is 1 and minus 1 is other 1 which are likely of order 2.

So therefore $x^2$ has to be minus 1 but that means this $X^2+1$ is zero so that means x is zero of the polynomial $X^2+1$. So that is what we wanted to prove, that is what we wanted to prove. So we finish this proof of this lemma that this proof also one can directly also see as follows. Direct proof, look at x, x equal to look at $p-1$ by 2 this factorial look at this element, then we know $x^2$ is $p-1$ factorial which is congruent to minus 1 mod p this is precisely Wilson's theorem.

So remember what we wanted to prove by assuring $X^2+1$ is a prime polynomial we wanted to prove p is congruent to 3 mod 4 by assuring p congruent 1 mod 4 we got a contradiction because this is zero of this polynomial that means this polynomial is not a prime polynomial that is $X^2+1$ is not a prime polynomial in general p x. This is contradiction to your assumption therefore p cannot be congruent to 1 mod 4 therefore p has to be congruent to 3 mod 4.

(Refer Slide Time: 21:19)



7

$\mu \in K[X]$, K field

$\deg \mu = 2$ or $3$

$V_K(\mu) = \phi \Rightarrow \mu$ is prime poly, i.e

$L = \dfrac{K[X]}{\langle \mu \rangle}$ field

$[L : K] = \deg \mu$

$K = \mathbb{Z}_2$, $\mu = X^2 + X + 1$ $\quad L = \dfrac{\mathbb{Z}_2[X]}{\langle X^2 + X + 1 \rangle}$ field

0, 1

1 1

≠ ≠

0 0

$X^3 + X + 1$

So altogether we have roved the lemma and the next question is, if I have a polynomial $\mu$ in with coefficients in the field, K field and degree of 2 a degree of $\mu$ is 2 or 3 how do we decide this polynomial $\mu$ has no zero inside K?

So that is no zero of there is no zero of $\mu$ inside K but which is if they may zero that will mean that this polynomial has to be $\mu$ is a prime polynomial because if $\mu$ is not prime it factors one of the factor has to be because the degree is 2 one of the 2 or 3 the degree of $\mu$ is 2 or 3 therefore one of the factor has to be linear if it factors. So that it cannot be because linear factors in corresponds to zero of $\mu$ inside K. So therefore if they were zero a $\mu$ is prime polynomial that means if I go modulo the polynomial ideal generated by the polynomial $\mu$ this must be a field, so you get a field extension and this field extension the degree of the field extension is equal to degree of $\mu$.

So again you can simply test let us take K equal to $\mathbb{Z}_2$ and let us take the polynomial $\mu$ to be equal to $X^2 + X + 1$ this is degree two polynomial and now we want to test whether L is field or not. This modulo $\mu$ so to test that you just have to test whether 0 and 1 they are zeroes of this polynomial $\mu$ but to check that I just put capital x equal to zero and test if I put capital X equal to 0 you get 1 which is not zero because capital X equal to 1 I put $1^2 + 1$ this is $1 + 1$ which is 2 which is 0 and the remaining one so this is not zero.

Therefore this are no zero therefore this L is a field, that is checks for the small values. Similarly you can check for the polynomial $X^3+X+1$ and in this case in the earlier case the degree of the field extension is 2 and it is over $\mathbb{Z}_2$ therefore the cardinality of L will be equal to 4, in this case once you check it is prime polynomial then the degree of L over K will be 3 and therefore L will have cardinality $2^3$ which is 8.

That is how one constructs finite fields with a bigger cardinalities, so with this we will stop here and continue with this lecture and remember two important things I have used in the above proof, one is easy one which is Lagrange's theorem for groups which relates the order of the elements and order of the group and other one is little bit more serious that the cyclic groups (the) if I take $\mathbb{Z}_p$ field and look at the multiplicative group of $\mathbb{Z}_p$ that is a cyclic group. This is what we have to prove in the coming lectures, thank you very much.