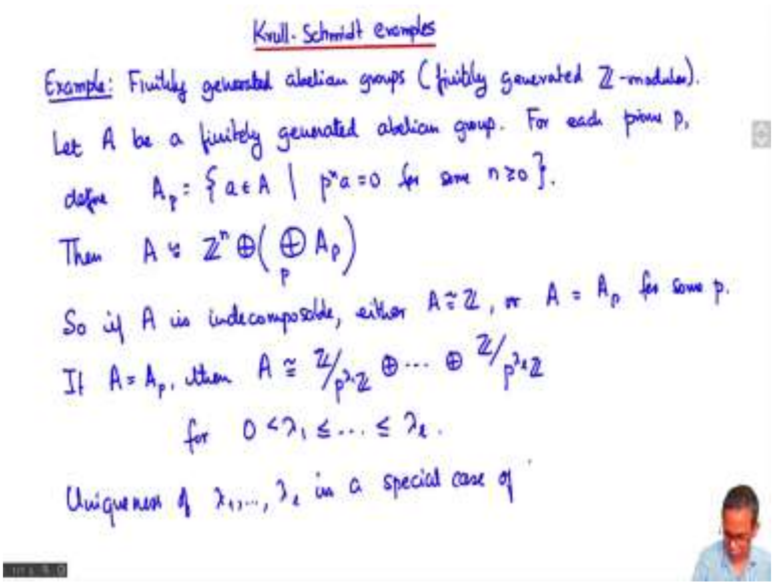
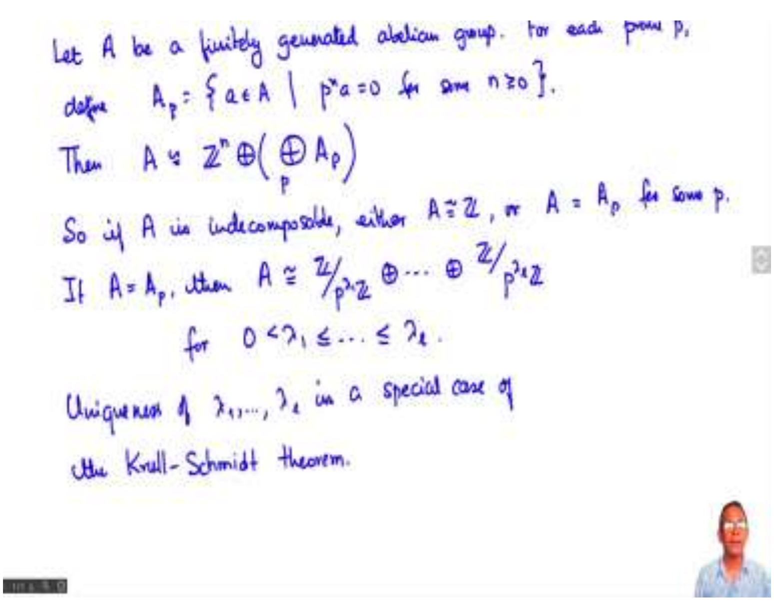
Algebra 2
Professor. Amritanshu Prasad
Department of Mathematics
The Institute of Mathematical Science
Krull-Schmidt Examples

(Refer Slide Time: 00:14)





Let us look at some examples related to the Krull-Schmidt theorem. So, first example what is the Krull-Schmidt decomposition when we look at finitely abelian groups or maybe I could even say a little more generally, finitely generated abelian or what we are also talking about, finitely generated Z modules, we want to see it in the language of modules.

These finitely generated abelian groups satisfy both the ascending chain condition and the descending chain condition and therefore, the Krull-Schmidt theorem applies. So, let us just see how the Krull-Schmidt works for this class of modules. So, suppose A is finitely generated abelian group, then define its p primary part to be those elements a in A such that p to the n a is 0 for some n greater than or equal to 0 for a fixed prime p. So, for each prime p, you make this definition.

Then we know from the theory of finitely abelian groups that A is isomorphic to Z to the power n, direct sum and then there is a sum over all primes p Ap and this part the only finitely key many non-zero, AP is nonzero for only finitely remaining p and so, this is going to be a finitely direct sum. So, all this follows from the structure theorem of finitely abelian groups.

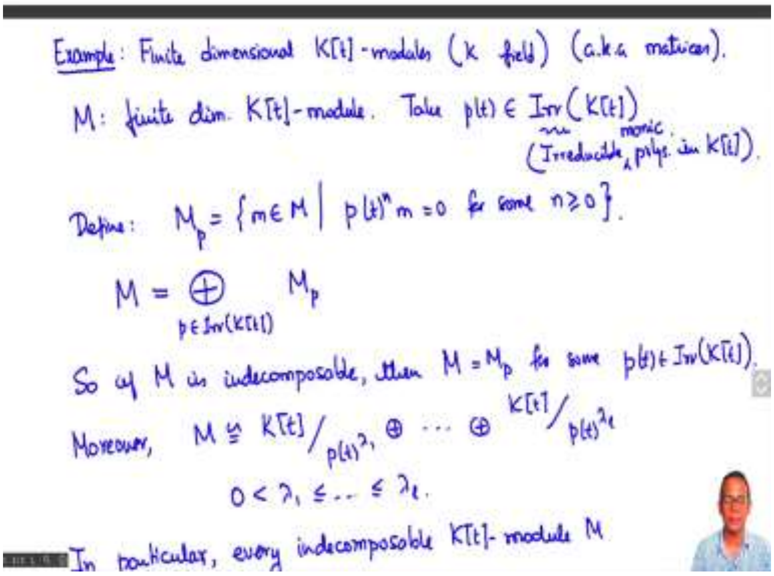
In fact, from this decomposition, you will be able to see that A satisfies the ascending chain condition and the descending chain condition. So, if A is indecomposable, either A is isomorphic to Z or A is Ap for some p, for some prime number p. So, either A is free and it is isomorphic to Z or A is what is known as p prime varying for some prime p.

And furthermore, if A is p primary, then the structure theorem for finitely abelian group says that A is isomorphic to Z mod p to the lambda 1 Z plus Z mod p to the lambda 2 Z and so on, Z mod p to the lambda l said for some integers 0 less than lambda 1 less than or equal to lambda 2 less than or equal to lambda l.

And, in fact, these integers are uniquely determined. That is the, that is a consequence on the structure theorem for finitely generated abelian groups. Now, in this decomposition the uniqueness of these integers p1, p2, pn can also be viewed as a consequence of the Krull-Schmidt theorem. We have already seen that every in decomposable finite where every decomposable finitely abelian group is in fact of the form Z mod some prime p and this is exactly a Krull-Schmidt kind of decomposition.

And seeing that, when arranged in weakly decreasing increasing order, these invariants lambda 1, lambda 2, lambda l are uniquely determined is in fact the statement of the Krull-Schmidt theorem. So, uniqueness of lambda 1 lambda l is a special case of the Krull-Schmidt theorem. Let us look at another example that we have encountered in algebra 1.

(Refer Slide Time: 05:42)



Which is finitely dimensional modules over a polynomial ring, K is a field and when we say finitely dimensional, we mean finitely dimensional over K. So, this is also known as, so finitely dimensional K t modules are in bisection with matrices. I will recall how this works in a bit, but you have seen this in algebra 1 if you took algebra 1.

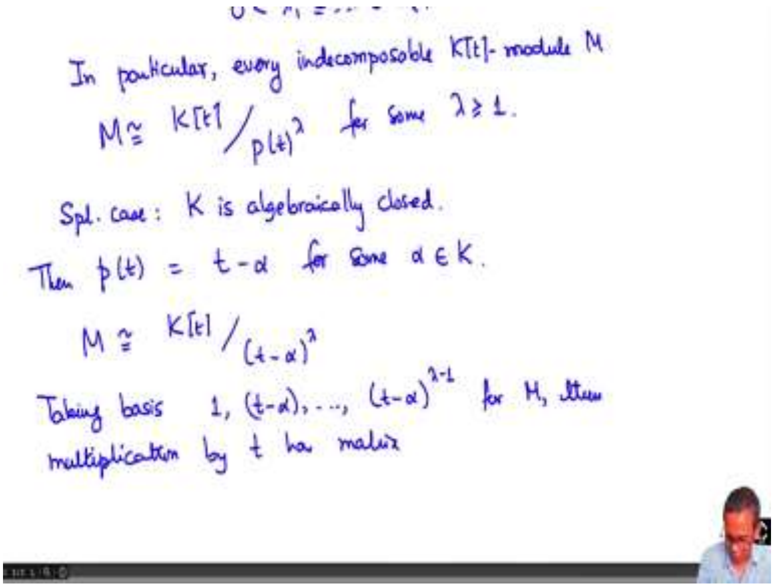
So, suppose M is a finitely dimensional K t module and take p t to be any irreducible polynomial in K t. So, by this I mean irreducible polynomials in K t, then define again the p primary part Mp equals m in M such that p t to the power n times m is equal to 0 for some and later than or equal to 0.

Then again we know from basic module theory that, if you want you can go back and look at the lectures on finitely regenerated modules over (())(07:43) M is going to be direct sum over p irreducible K t Mp and once again, this m being finitely dimensional only finitely many of these harm Mps will be nonzero and so this sum will actually be a finite direct sum.

So, you get a canonical direct sum decomposition of M there is no choice here and but then each Mp may not be in decomposable in general, but certainly if M is in decomposable, then M is equal to Mp for something. So, if M is indecomposable then M equals Mp for some polynomial, irreducible polynomial Kt.

Moreover, by the structure theorem M is isomorphic to K t mod p t to the lambda 1 plus K t mod p t to the lambda l and this again here we have 0 less than lambda 1 less than or equal to lambda 2 less than or equal to lambda l and the uniqueness of these invariance lambda 1 to lambda l is again can be viewed also as a consequence of the Krull-Schmidt theorem.

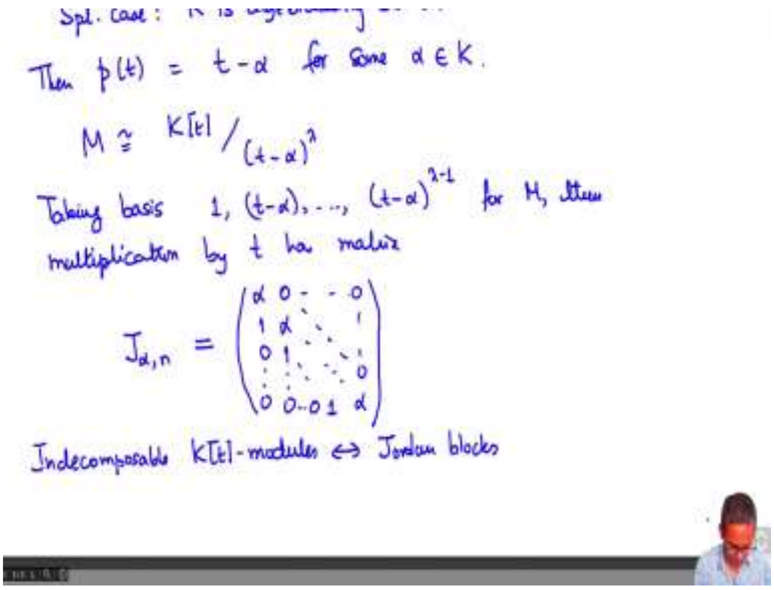
(Refer Slide Time: 09:33)



And in particular the in decomposable K t modules M is isomorphic to K t mod p t to the power lambda for some lambda greater than or equal to 1. So, these are precisely the indecomposable modules. Let us take a special case, when K is algebraically closed, in this case p t has to be of the form t minus alpha for some alpha in K. Here I should see that these p ts are only maybe we should say here, let us just to make this unique, we do not want to consider a polynomial and some K multiple of that polynomial. So, maybe here I should say irreducible monic polynomials, so we will only take polynomials with (())(11:08) term equal to 1.

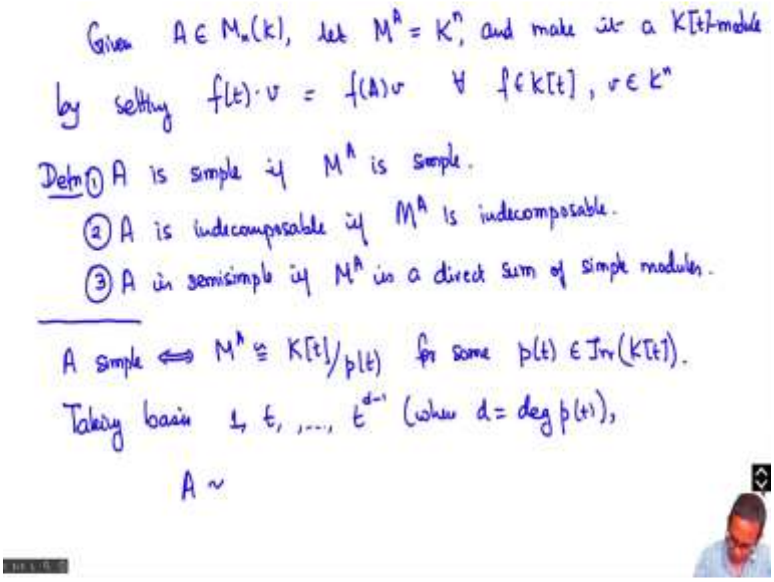
And so likewise here, every irreducible polynomial is linear and by scaling it, we can make it monic and hence of the have the form t minus alpha for some alpha in K. And in that case, M is isomorphic to K t mod t minus alpha to the power lambda. Now, if you take a basis, 1 t minus alpha t minus alpha to the power lambda minus 1 for M, then multiplication by t has matrix.

(Refer Slide Time: 12:10)



Given by 1 alpha 0, 0, 1. So, you have no, I think I got this wrong, it is alpha 1 0 0 alpha 1 0 0. So, you have alphas along the diagonal, you have 1 just below the diagonal and everything above the diagonal is 0. This is what is known as a Jordan block with eigenvalue alpha size M. And so in decomposable K t modules correspond to Jordan blocks, at least when K is algebraically closed. Now, we can turn this thing backwards and we can also say that.

(Refer Slide Time: 13:30)



Given A matrix M by n matrix in K, we can form a K t module. So, we just take MA to K to the power n and make it a K t module by allowing t act by K or so what I will say is by setting f t times a vector v to be f A b. So, this f A means you take the polynomial F and divide. So, f is a polynomial with coefficients in K you substitute for the variable t, the matrix

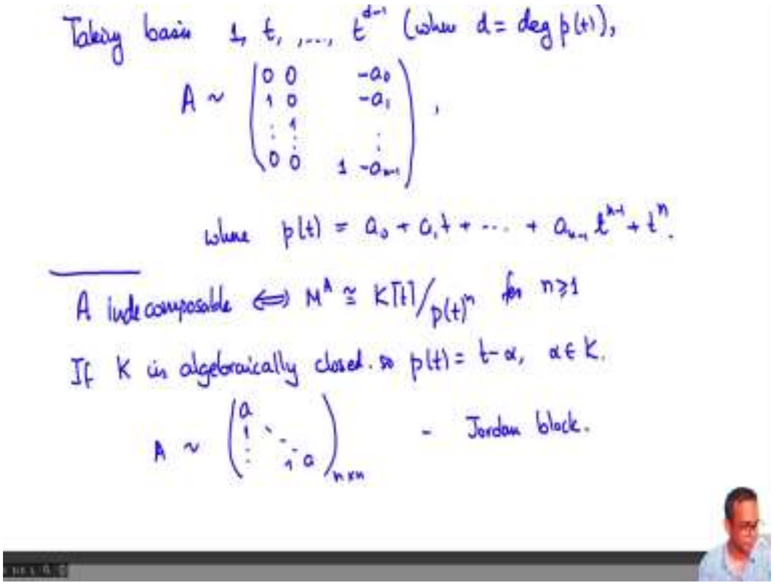
A and evaluated you will get n by n matrix and you can multiply it on the right, by any vector v thought of as a column vector.

Now, using this correspondence between matrices and Kt modules, we can transfer ideas from module theory to matrix theory. So, here are some definitions motivated by this. A matrix is simple, if MA is simple, we could say a matrix A is indecomposable, if MA is indecomposable and let me just introduce a new motion, a matrix A is semi simple if MA, a module is set to be semi simple if it is isomorphic to a direct sum of simple modules. So, is a sum of simple modules, is a direct sum of simple modules.

So, for example if A is simple, then that means that MA we just seen is isomorphic to K t, mod p t for some irreducible polynomial, irreducible monic polynomial. Well, we did not quite see this, but what we saw is that if M is in decomposable, then it is a form K t mod p t to the n and since every simple module is in decomposable, it is not difficult to see that the only simple modules among K t mod p to the n are the ones where n is equal to 1.

So, modules of the form K t mod p t and what this means is, if you taking basis, 1 t t to the power d minus 1, where d is the degree of p t, we get that A is similar to the matrix which has the following form.

(Refer Slide Time: 17:20)

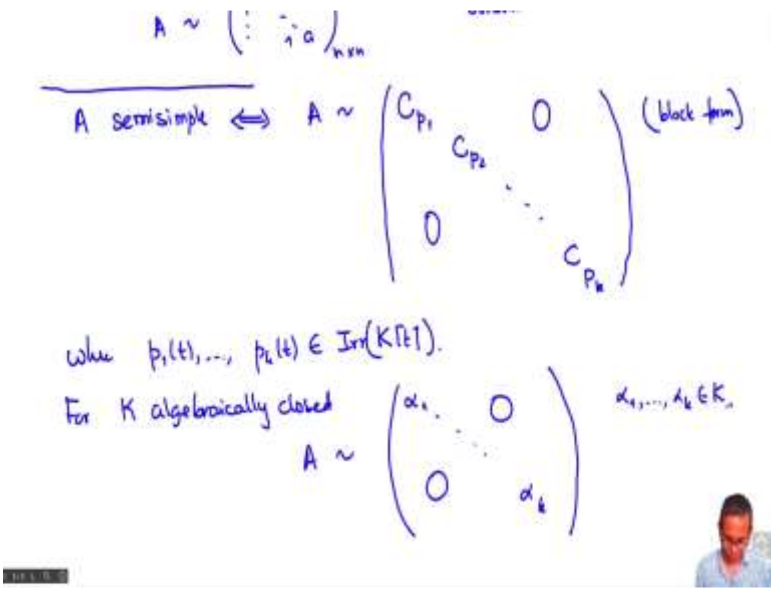


So, the first basis vectors 1 it goes to the vector t. So, it starts off like just with ones in the row just below the diagonal and so you have this last column left and there you put in the coefficients of pt. So, you put in minus A0 minus 1 minus A sub n minus 1, where p t is equal to A0 plus A1 plus An minus 1 t to the power n minus 1 plus t to the n, we assuming that p t is monic. So, that is what simple. So, simple matrices are always similar to (compan). This is called a companion matrix of pt.

Simple matrices are similar to companion matrices of irreducible polynomials. If the field K were algebraically closed, then p t would have degree 1 and this will just be a 1 by 1 matrix. Now, let us look at what happens to indecomposable modules give A is indecomposable, then that means that MA is isomorphic to K t mod p t to the power n for some n greater than or equal to 1.

Now, if K this could have a slightly complicated form though in most cases, especially when K is a perfect field, it can be simplified. But for now I just keep this simple and let us assume that K is algebraically closed. Then what we have seen is that just p t has to be of the form t minus alpha for some alpha in K and what we get is that A is similar to a 1, this Jordan block of some size, size n here and finally, let us look at the case A is semi simple.

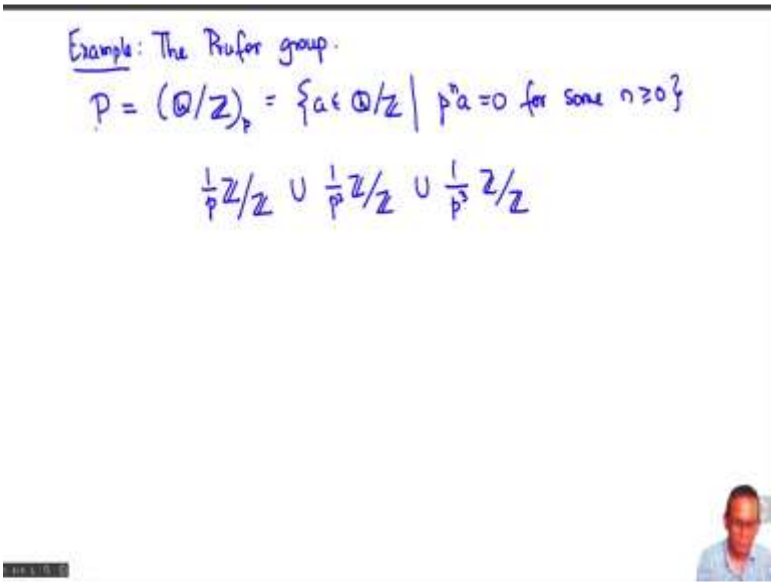
(Refer Slide Time: 20:03)

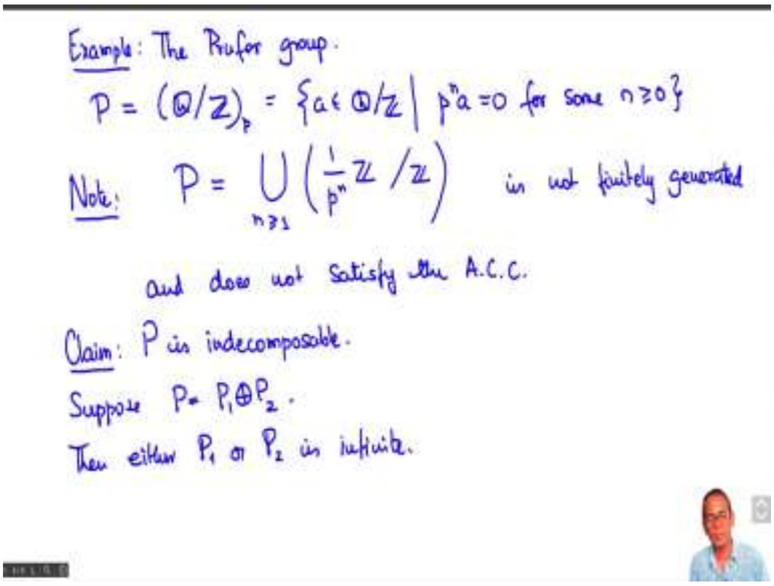


In this case, A similar to, so direct sum of simples and so is similar to Cp1, Cp2 to a block diagonal matrix, where the diagonal blocks are companion matrices of irreducible, monic irreducible polynomial and if K were algebraically closed this would mean that A is similar to alpha 1, alpha k, because these irreducible polynomials would be of the form t minus alpha 1 t minus alpha 2 t minus alpha for some alpha t, for some alpha 1 up to alpha K in K.

In other words, K, semi simple matrices in an algebraically closed field are precisely the diagonalizable ones. I will end this session with a very interesting example.

(Refer Slide Time: 21:49)





Which is called the proofer group, which we have briefly encountered during one of the lectures. So, this is Z module, it is an abelian group. So, the definition of this proofer group, which I will denote by P, is the P primary part of Q mod Z p of the group Q mod Z. What is this? So, these are those elements of Q mod Z which are killed by some power of p, if you ask what are the elements of Q mod Z that are killed by p, then that is 1 over p Z mod Z.

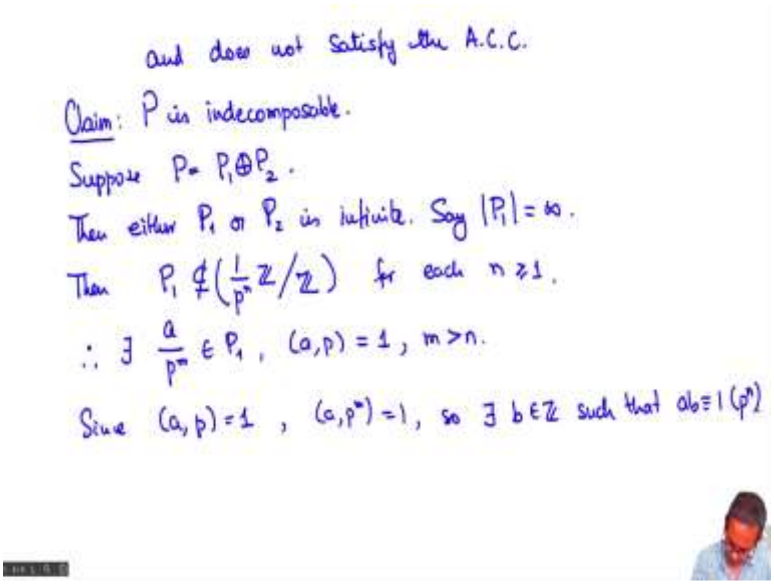
What are the elements that are killed by p squared, that is 1 over p squared Z mod Z. What are the elements that are killed by p cube, that is 1 over p cube Z on Z. So of course, this is an increasing chain 1 over p squared contains 1 over p squared Z contains 1 over p Z 1 over p cube that contains 1 over p squared Z and so on. So, these this is an increasing chain, but what we want is an infinitely union and that will give you the full proofer group.

So, what I am saying is that the proofer group P is equal to union n greater than or equal to 1, 1 over P to the n Z mod Z. So, it is a, this is an increasing union of subgroups of the proofer groups and this group 1 over p to the n Z mod Z is of course, just isomorphic to Z mod p to the n Z just scaling everything up by a factor of p to the n. And this is not finite, degenerated and it does not satisfy the ascending chain condition.

Well, that is obvious, because here is an ascending chain which never stabilizes. And it is not finitely generated because you took any finite subset of P, it could be contained in one of these subgroups and so, it could not generate all of P. Now, I claim that P is indecomposable. Suppose that, so what we need to show that if P can be written as a direct sum P1 plus P2. We need to show that one of these is equal to P and the other is 0.

Then, but we cannot have both. So, how to show that 1 of them is equal to P. Now, if P is P1 plus P2 we cannot have that both P1 and P2 are finite, because then P would be forced to be finite, but it is clearly infinite. So, then either P1 or P2 is infinite and I show that whichever 1 is infinitely is going to be all of P and the other 1 has to be 0.

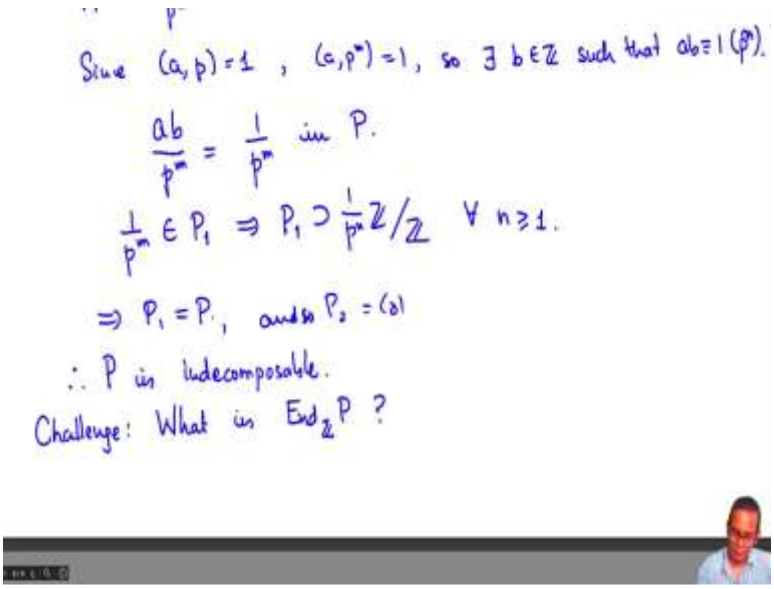
(Refer Slide Time: 25:37)



So, let us say that, say P1 is infinite. So, then, what we have is that since P1 is infinite, P1 cannot be contained in a finitely subgroups P1 is not contained in finite sub group so P1 is not contained in 1 over p to the n Z mod Z for any n. So, that means that there exists an element, a mod p to the m in P1, where a p the GCD of a is not divisible by p and m is greater than n.

Any element which is not of this form could be further reduced to the form where a, p is 1 and then if the m is less than or equal to n, then we would have inside this subgroup 1 over p to the n Z mod Z. So, there exists an element of this form since a, p the GCD of a and p is 1, the GCD of a, p to the m is also 1. So, there exists an integer b such that ab is congruent to 1 mod p to the m, p to the n let us say.

(Refer Slide Time: 27:21)



So, what I can do is I can write ab, maybe I should say ab is congruent to 1 mod p to the m. So, ab mod p to the m is going to be equal to 1 mod p to the m in the proofer group P and so, 1 mod p to the m belongs to this P1 which also implies that P1 contains 1 over p to the n Z mod Z this is because, every element in 1 mod p to the n Z mod Z is a multiple of 1, an integer multiple of 1 over p to the m.

So, since P1 is a subgroup, if it contains this element, it will contain every multiple of it and so it must contain this. So, what we see is that P1 contains 1 over p to the n Z mod Z for all n greater than or equal to 1. But this clearly that implies that P1 is equal to P, because P is precisely the union of these subgroups and P2 is 0. So, this means that the proofer group P is indecomposable. Now, here is a small challenge for you. What is this local ring and end Z of the proofer group, give it this, I will stop.