

**Algebra - II**  
**Professor S Viswanath**  
**Department of Mathematics**  
**The Institute of Mathematical Science**  
**Lecture 34**  
**Artin's Theorem – Part II**

(Refer Slide Time: 00:14)

Artin's Theorem

Theorem: Let  $K$  be a field and  $\Gamma \subseteq \text{Aut}(K)$  be a finite subgroup. Then  $[K : K^\Gamma] = |\Gamma|$

Proof:  $F := K^\Gamma = \{a \in K \mid \sigma(a) = a \ \forall \sigma \in \Gamma\}$

$\begin{array}{c} K \\ | \\ F \end{array}$

Claim 1:  $|\Gamma| \leq [K : K^\Gamma]$

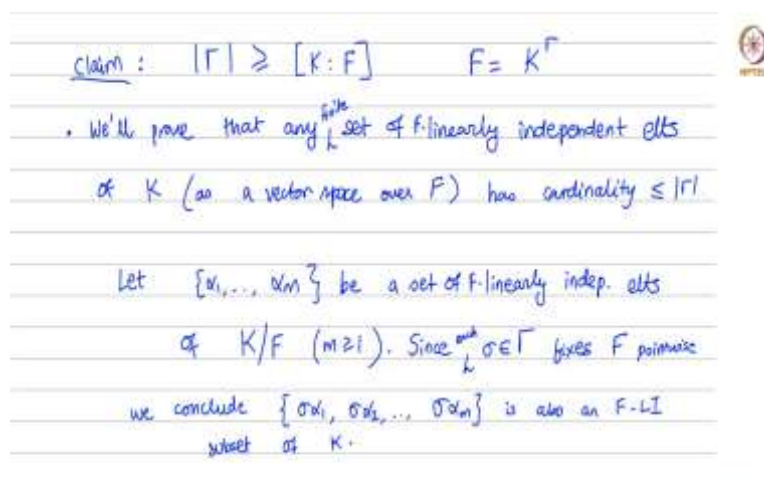
PF: If  $[K : K^\Gamma]$  is infinite, then done.

$\therefore$  we may suppose  $[K : K^\Gamma] < \infty$ .



In the previous video we proved one half of our Artin's theorem. So, recall the statement; it says if  $K$  is a field and if  $\Gamma$  is a finite subgroup of the group of field automorphisms of  $K$ , then  $K$  over the fixed field  $K^\Gamma$  is where it is a finite extension of degree equal to the cardinality of  $\Gamma$ . And we proved the inequality which showed that the cardinality of  $\Gamma$  is less than or equal to the (cardinal) the degree of the extension  $K, K^\Gamma$ . What we will do this time is to prove the other half.

(Refer Slide Time: 00:51)



claim:  $|\Gamma| \geq [K:F]$   $F = K^{\Gamma}$

• We'll prove that any finite set of  $F$ -linearly independent elts of  $K$  (as a vector space over  $F$ ) has cardinality  $\leq |\Gamma|$

Let  $\{\alpha_1, \dots, \alpha_m\}$  be a set of  $F$ -linearly indep. elts of  $K/F$  ( $m \geq 1$ ). Since  $\sigma \in \Gamma$  fixes  $F$  pointwise we conclude  $\{\sigma\alpha_1, \sigma\alpha_2, \dots, \sigma\alpha_m\}$  is also an  $F$ -LI subset of  $K$ .



So, I now claim that the reverse inequality holds, in other words that the cardinality of gamma is greater than or equal to the degree of the extension  $F$ , remember is the fixed field of gamma. And how are we going to prove this? We will prove the following, we will prove that any set of linearly independent elements, any set of linearly independent elements of  $K$  thought of as a vector space, as a vector space over  $F$ .

So, maybe to emphasize the field  $F$  I will say  $F$  linearly independent elements. So, I think of it as case a vector space over  $F$  and if we show that any set of linearly independent elements has cardinality at most, the cardinality of gamma. And now, if you show this, then you are done, because this would imply two things number one, that  $K/F$ ,  $K$  over  $F$  is a finite extension, because otherwise there will be infinitely many linearly independent elements possible.

Secondly, the dimension of this vector space is at most the cardinality of gamma because we just take a basis of this vector space, that is a set of linearly independent element and that can have cardinality at most gamma. So let us try and prove this statement. So, let us begin with a set of let  $\alpha_1$  through  $\alpha_m$  be a set of linearly independent elements.

So again, let me say  $F$  linearly independent elements of the vector space  $k$  thought of as a vector space over  $F$ . And of course, I will assume  $m$  is at least 1 here. So, some finite, some finite number of  $m$ . Now, let us show that, so maybe I should say any finite set. Now, what

do we know since this is linearly independent from this we can get many other linearly independent sets as follows.

Since each sigma and gamma fixes, so you pick elements sigma and gamma, since it fixes the field F pointwise. In other words, since it is a fixed field, sigma acting on an element of F gives you back that same element. We conclude the following that the collection sigma alpha 1, you just apply sigma to all these earlier fellows.

Alpha m, this is also F linearly independent, is also an F linearly independent. So just use LI for linearly, it is an F linearly independent subset of K. So, we have manufactured in some sense many linearly independent subsets starting with the first one.

(Refer Slide Time: 04:17)

Define map:  $\psi^\sigma: K^m \rightarrow K$   
 $(\sigma \in \Gamma) \quad (\beta_i)_i^m \mapsto \sum_{i=1}^m \beta_i (\sigma \alpha_i)$

Properties: (1)  $\ker \psi^\sigma := \left\{ (\beta_i)_i^m \mid \sum_{i=1}^m \beta_i (\sigma \alpha_i) = 0 \right\}$   
 Then  $\ker \psi^\sigma \cap F^m = (0)$  (by F-LI of  $\{\sigma \alpha_i\}_i^m$ )

(2)  $\psi^\sigma$  is K-linear i.e.  $\psi^\sigma((\beta_i)_i^m + (\beta'_i)_i^m) = \psi^\sigma((\beta_i)_i^m) + \psi^\sigma((\beta'_i)_i^m)$

And now comes the sort of important step non-obvious step. Let us define maps as follows. So, we have a bunch of linearly independent sets and we are going to define maps from  $K^m$  to  $K$  as follows. So I will call this map as psi, but this map will also depend on the sigma as follows; so given an M tuple beta i have numbers in K, I will map this to the corresponding linear combination of the linearly independent set sigma alpha i.

So remember sigma alpha i is linearly independent. And I just map the collection beta i to the corresponding linear combination. So, observe there is therefore, this is maps, one for each element of gamma. Now what are the key properties of these maps? Well, the first property the sigma alpha i are linearly independent thought of as an over the base field F. So, the linear independence tells you the following; if you look at the kernel of this map.

So if I ask what is the kernel of this map? In other words, what is the collection of  $m$  tuples which maps to 0,  $i$  equals 1 to  $m$ . Well, in general, there will probably be many of these, but if we take this to be the kernel, then observe the following; the kernel of  $\sigma \psi$ ,  $\psi \sigma$  does not intersect  $F^m$ . In other words, if all the  $\beta_i$  is come from  $F$ , then this linear combination can never be 0 unless all the  $\beta_i$  are 0 themselves.

This is exactly linear independence. So, by the  $F$  linear independence of the  $\sigma \alpha_i$ . So, the  $\beta_i$  cannot all simultaneously come from the base field  $F$ . Property two; observe that  $\psi \sigma$  is actually a  $K$  linear map. So, what sort of map is this? You can think of it. So now, the  $K$  to the  $n$  and  $K$ . If I think of them as vector spaces over  $K$  and then  $\psi \sigma$  is just a linear transformation of these  $K$  vector spaces. So this is  $K$  linear. In other words, if I add two guys, it will become the sum.

So if we take  $\beta_i$  plus the tuple  $\beta_i$  dash, which means component wise addition, then reduce give me  $\psi$  on  $\beta_i$  plus  $\sigma \beta_i$  dash. And I mean, that is more or less obvious, because you will substitute in place of  $\beta_i$ , you will have to substitute  $\beta_i$  plus  $\beta_i$  dash and so it is split up into two pieces.

(Refer Slide Time: 07:42)

Define map:  $\psi^\sigma: K^m \rightarrow K$   
 $(\sigma \in \Gamma) \quad (\beta_i)_i \mapsto \sum_{i=1}^m \beta_i (\sigma \alpha_i)$

Properties: (1)  $\ker \psi^\sigma := \left\{ (\beta_i)_i \mid \sum_{i=1}^m \beta_i (\sigma \alpha_i) = 0 \right\}$   
 Then  $\ker \psi^\sigma \cap F^m = \{0\}$  (by F-LI of  $\{\sigma \alpha_i\}_i$ )

(2)  $\psi^\sigma$  is  $K$ -linear i.e.  $\psi^\sigma((\beta_i)_i + (\beta'_i)_i) = \psi^\sigma(\beta_i) + \psi^\sigma(\beta'_i)$



And similarly, if I replace  $\beta_i$  by a multiple of  $\beta_i$ , in fact, a multiple coming from  $K$  scalar multiples that second property, if I apply  $\psi \sigma$  to  $\lambda$  times the  $\beta_i$ . So, let me just verify this  $\psi \sigma$ , this is just the  $m$  tuple  $\lambda \beta_i$  by definition and this is just  $\lambda \beta_i$  times  $\sigma \alpha_i$ . This is  $i$  goes from 1 to  $n$ .

So, observe this product is taken in  $F$  and  $\lambda$  and  $\beta_i$  are in  $F$ . So,  $\lambda \beta_i$  is another element of  $F$ .  $\sigma \alpha_i$  is of course, an element of  $F$  and so now by the associativity of the multiplication and the field, I can just pull the  $\lambda$  out. So, you will give me  $\beta_i \sigma \alpha_i$ . Can so this is true, in fact, for all  $\lambda$ 's coming from the field  $K$ .

So, this map is a  $K$  linear map. It satisfies additivity and scalar multiplication. It respects both operations. Now, that is the second property. So what do we know that for about the kernel of the map? So, so by the way, here is one property we know about the kernel. But now, because it is a  $K$  linear map from  $K^m$  to  $K$ , so this is what you would call a linear functional on the, the vector space  $K^m$ .

(Refer Slide Time: 08:56)

$$\begin{aligned} \psi^\sigma(\lambda(\beta_i)_m) &= \psi^\sigma((\lambda\beta_i)_m) = \sum_{i=1}^m (\lambda\beta_i)(\sigma\alpha_i) \\ &= \lambda \sum_{i=1}^m \beta_i \sigma\alpha_i \quad \forall \lambda \in K. \end{aligned}$$

ker  $\psi^\sigma$  is a  $K$ -subspace of  $K^m$ .

③ If  $(\beta_i)_m \in \text{ker } \psi^\sigma$ , then  $\sum_{i=1}^m \beta_i \sigma\alpha_i = 0$   
 Apply  $\tau \in \Gamma \cong \text{Aut}(K) \Rightarrow \tau(\sum_{i=1}^m \beta_i \sigma\alpha_i) = 0$



The kernel is a piece of subspace. It is a subspace of  $K^m$ . So again, just to emphasize that I'm talking about vector spaces over the field  $K$ , I will say it is a  $K$  subspace of  $K^m$ . So here, you know, there are two fields  $K$  and  $F$  in play and sometimes you may think of something as a vector space over  $K$ , sometimes over  $F$ .

So just to ensure we are not getting ourselves mixed up, I am just emphasizing the  $K$  or the  $F$ . So the kernel is a  $K$  subspace. So that is the second property. This  $K$  subspace is interesting. It does not intersect  $F^m$ , where  $F$  is the base field. And what is the third property and this is somehow the most important, one of the most important properties of these maps.

And this really uses the fact that  $\Gamma$  is a group. So I observe that the earlier half of Artin's theorem, did not really use the fact that  $\Gamma$  is a group of automorphisms. The

group structure was not used but now we are going to use it. So here is the, here is the observation.

So suppose I pick an  $m$  tuple  $\beta_i$  from 1 to  $m$ , which is in the kernel of  $\sigma$ ,  $\psi \sigma$ . Then what does that mean? It just says that the sum,  $\beta_i \sigma \alpha_i$  is 0. Now, what I can do is I can apply an element of  $\Gamma$  and auto morphism. Here, remember,  $\Gamma$  is a subset of the auto morphism group of the field  $K$ . So, I will apply  $\tau$  to this equation. So, what does that mean? It will give me summation, so, it is  $\tau$  acting on this sum is 0.

(Refer Slide Time: 10:47)

$$\sum_{i=1}^m \tau(\beta_i) \tau(\alpha_i) = 0 \Rightarrow (\beta_i)_i^m \in \ker \psi^{\tau\sigma}$$

$\tau(\beta_i) \in K$        $\tau(\alpha_i) \in \Gamma$

$$(\beta_i)_i^m \in \ker \psi^\sigma \Rightarrow (\tau\beta_i)_{i=1}^m \in \ker \psi^{\tau\sigma} \quad \forall \sigma, \tau \in \Gamma$$

let  $W := \bigcap_{\sigma \in \Gamma} \ker \psi^\sigma \subseteq K^m$ . Then  $(\beta_i)_i^m \in W \Rightarrow (\tau\beta_i)_i^m \in W \quad \forall \tau \in \Gamma$

But  $\tau$  being an auto morphism this can be written as the sum of  $\tau$  of  $\beta_i$  into  $\tau$  of  $\sigma$  of  $\alpha_i$ . So, I have used the fact that  $\tau$  respects both addition and multiplication. And now observe  $\tau \sigma$  is just another element of  $\Gamma$ . So what does that mean? It says that, if I look at these numbers,  $\tau \beta_i$ , so maybe I will give them a different name now,  $\beta_i$  dashes you wish, then it says that; so this says that these  $\beta_i$  dashes, this new  $m$  tuple is actually also in the kernel of  $\psi$  or not of  $\psi \sigma$ , but  $\psi$  of  $\tau \sigma$ .

That is exactly what this equation implies. So, here is the conclusion, if  $\beta_i$  belongs to the kernel of  $\psi \sigma$ , then  $\tau \beta_i$ , so let me just again call  $\beta_i$  dashes as  $\tau \beta_i$  is. So, if we apply  $\tau$  to each component, then the resulting  $m$  tuple is in the kernel of  $\psi$  of  $\tau \sigma$ . And this is true for all  $\sigma \tau$  coming from  $\Gamma$ .

So, this is the third important property that we need. Now, what does this imply, this third property especially, it says the following; if we take the intersection of all these kernels; so,

let  $W$  denote the intersection of all the kernels. What is this is some subset of  $K$  power  $m$  then this intersection has the following property.

So, just look at what this says; if you have something in one kernel and you apply an element to it, it lies in a different kernel, one of the other size, but if something comes from the intersection of all the size, then if you apply  $\tau$  to it, the answer is again and the intersection of all the  $\tau$ s all the sides.

So, if  $W$  is defined like this, then the conclusion is the following;  $W$  is invariant under  $\gamma$ . This means the following, then if I apply  $\tau$  to  $W$ , the answer is again in  $W$ . So,  $\beta_i$  belongs to  $W$  and so does  $\tau \beta_i$ . So, this invariance under the action of  $\gamma$ , I should say this is for all  $\tau$  in  $\gamma$ .

(Refer Slide Time: 13:24)

②  $W$  is a  $K$ -subspace of  $K^m$

③  $W \cap F^m = (0)$ .

Claim:  $W = (0)$ .

Proof: Suppose  $\exists \beta \in W$  with  $\beta_j \neq 0$  for some  $1 \leq j \leq m$ .

Since  $W$  is a  $K$ -subspace, by rescaling  $\beta$  by  
 elems of  $K$  (replace  $\beta$  by  $c\beta$  for  $c \in K$ )  
 we may assume  $\beta_j = \lambda$  (where  $\lambda \in K$  is fixed)

So, we are going to use this this invariance under the action of  $\gamma$ . So this is this is one property again. So, this is the first property of  $W$ . And of course, the other properties come from the previous statements, which is that  $W$  is of course, an intersection of subspaces. So, it is a subspace. It is a subspace of  $K$  power  $m$ . And in fact, every one of the size itself does not intersect  $F$  power  $m$ .

So, in particular,  $W$  does not intersect  $F$  power  $m$ . So, these are the three important properties of  $W$ . Now, what does this, what does this give us? Well, I claim that you really cannot find a  $W$  satisfying these properties. Claim is the only possibility for  $W$  is just the  $0$  subspace. These three properties are just too strong.

So proof, let us quickly prove this. So, suppose there exist a nonzero element. So, if there exists beta i 1 to m in W, with which is nonzero with say, with some beta i, say the ith term, maybe we should call it beta j with some nonzero element with beta j, not 0 for some j between 1 and m. So it is a nonzero element of W. Then will you we will get a contradiction.

So observe that, since W is a subspace, K subspace. So maybe I will call this m tuple as beta. Since W is a K subspace meaning it is closed under scalar multiplication by K, what you can do is the following; you can scale this element beta. We can scale beta by various scalars by elements of K. In other words, you can take beta multiplied by various Cs.

So, in other words, replace beta by a scalar multiple of beta, where the scalar comes from the field K and when you scale beta and we can scale beta by elements of K and so maybe I should say by rescaling beta we may assume that this nonzero element beta j, we may assume beta j is any given element of my it is an element beta j is lambda where lambda is some fixed, let me fix somewhere lambda belongs to K is some fixed element.

In other words, I can by rescaling I can ensure beta j is anything, any element I want, any element of K. So I am going to fix lambda and I will rescale beta so that beta j equals the value lambda.

(Refer Slide Time: 16:38)

Handwritten notes on a slide:

Let  $(\alpha_i)_{i=1}^m \in W$   $\neq 0 \in \Gamma$  } consider their sum

$\sigma := \sum_{i \in \Gamma} \alpha_i \in W \subseteq K^m$

$\sigma \sigma = \sum_{i \in \Gamma} \sigma \alpha_i$

$= \sigma$

$\sigma \sigma = \sigma \neq \sigma \in \Gamma$

$\sigma = (\sigma_i)_{i=1}^m \Rightarrow (\sigma_i)_{i=1}^m = (\alpha_i)_{i=1}^m \Rightarrow \sigma_i = \alpha_i$   
 $\forall i=1, \dots, m$   
 $\neq \sigma \in \Gamma$

Now, what is the, what is the point of this? So now, let us apply the three properties of tau. So observe, first I apply sorry, three properties of W. So now let us look at this property here.



We know that if you apply tau to beta  $i$ , this answer is  $W$ . So we know this was property 1 that I mentioned of  $W$ , for all tau in gamma.

Now, here is a standard sort of trick that one uses to construct elements which are invariant under actions of finite groups. Let us consider the sum of all these tau beta  $i$ s. So let me call this new element a zeta maybe. The zeta denote the sum of all these tau betas. Sorry, tau belongs to gamma.

So this, this  $m$  tuple, I am calling as tau beta. So, this is now  $m$  tuple. When I write tau beta, I really mean an  $m$  tuple here. So maybe we will put a underscore into the beta to say it is like a vector. So, look at this, this new element, this is an element of  $K$  power  $m$  and what more do I know about it? The key property is that this is invariant under the action of sigma.

So, consider there is some zeta, not only is it in  $K$  power  $m$ , it is actually in  $W$ . Why, because each of the tau betas is in  $W$ . So they have some missing  $W$ . Now, the important properties if I apply any element sigma to zeta where sigma is, so let sigma be an element of the group gamma. If you apply sigma to zeta, then the answer is the sigma tau beta.

But when tau runs over gamma, sigma Tau also runs over gamma possibly in a different order. So, this is actually the same as zeta again. This is just the same sum except that the terms may appear in some other order. So, this is the, this is the key property. So, sigma zeta is actually equal to zeta for all, for all elements sigma and gamma. So, what does that mean?

If I write zeta as I say zeta  $i$  equals 1 to  $m$ , the same tuple, then it means if I apply sigma to these components, so then sigma zeta  $i$ . So, the  $m$  tuple sigma zeta  $i$  coincides with zeta  $i$ , means that each of the components when I apply sigma to the zeta  $i$ , I get zeta  $i$  for all  $i$  equal to 1 to  $m$ , this is true for all sigma and gamma. So, now we stare at this last equation here.

It says that the zeta is that I have, they are fixed by every element of gamma, they are elements of  $K$ , but they are fixed by every element of gamma.

(Refer Slide Time: 19:56)

$$\Rightarrow \alpha_i \in K^r \quad \forall i=1, \dots, m$$

$$\Rightarrow \alpha = (\alpha_i)_i \in F^m \cap W = (0)$$

$$\Rightarrow \alpha_i = 0 \quad \forall i=1, \dots, m$$

$$\Rightarrow \text{In particular: Take } \alpha_j: \alpha_j = \sum_{c \in F} c \beta_j = \sum_{c \in F} c \alpha_j$$

$$\Rightarrow \sum_{c \in F} c \alpha_j = 0; \quad = 0$$

②  $W$  is a  $K$ -subspace of  $K^m$

③  $W \cap F^m = (0)$ .

Claim:  $W = (0)$ .

Proof: If  $\exists (\beta_i)_i \in W$  with  $\beta_j \neq 0$  for some  $1 \leq j \leq m$ .

Since  $W$  is a  $K$ -subspace, by rescaling  $\beta$  by

elts of  $K$  (replace  $\beta$  by  $c\beta$  for  $c \in K$ )

we may assume  $\beta_j = 1$  (where  $\lambda \in K$  is fixed)

$(z_i)_{i=1}^m \in W \quad \forall z \in \Gamma$

consider their sum

$$z := \sum_{\tau \in \Gamma} \tau z \in W \subseteq K^m$$

$$\sigma z = \sum_{\tau \in \Gamma} \sigma \tau z$$

$$= z$$

$$\sigma z = z \quad \forall \sigma \in \Gamma$$

$z = (z_i)_{i=1}^m \Rightarrow (\sigma z_i)_{i=1}^m = (z_i)_{i=1}^m \Rightarrow \sigma z_i = z_i$   
 $\forall i=1, \dots, m$   
 $\forall \sigma \in \Gamma$

In other words, the zeta is all in the fixed field gamma. This is true for all i equals 1 to m but the fixed field is exactly what we are calling F. So, to summarize what the trick finally does, we have one element beta in W. Now, we know that W is invariant under applying elements of gamma. So you apply all the elements of gamma, the tuas, and you get many vectors, tau betas.

Now when you add those vectors up, the final answer is definitely invariant under, I mean it is fixed by the action of gamma because you have taken a sum. Now, this implies that the zeta is all in F. So what does that mean? We have constructed so zeta therefore, which is the tuple of zeta is an element of F power m and remember, zeta was an element of W to begin with.

And now, recall that was the second property which said, W has no elements whose components are all in F. So we have constructed one such element, which means that the zeta must actually be the 0. So zeta i had better be 0 for all i equals to 1 to m. So, what does this mean? This says in particular, so in particular, let us just apply it to the jth component.

So, remember we know that at least one component beta j was not 0. So, take i to be the jth component, where beta j was the given lambda that we fixed. So then what is zeta j by definition? It is summation tau beta j, tau ranging over gamma. This is what we called summation tau lambda; lambda was the value of beta j gamma, this is 0.

So, what does this mean? This says that summation tau of lambda is 0, tau belongs to gamma. But now here is the interesting thing. Remember, the lambda was arbitrary to begin with. So

we could have chosen any element  $\lambda$  of the field  $K$  and why was that? Because  $\beta_j$  was nonzero to begin with, so you could scale and change its value to any element of  $K$ .

(Refer Slide Time: 22:25)

But  $\lambda \in K$  was arbitrary  $\Rightarrow \sum_{\tau \in \Gamma} \tau(\lambda) = 0 \quad \forall \lambda \in K$   
 $\Rightarrow \sum_{\tau \in \Gamma} \tau = 0 \quad (\in \text{Maps}(K, K))$   
 But  $\Gamma \subseteq \text{Maps}(K, K)$  is  $K$ -linearly indep.  
 $\Rightarrow \sum \tau = 0 \Rightarrow \Gamma$  is linearly dependent.  
 Contradiction!

But  $\lambda$  is arbitrary but  $\lambda$  in  $K$  was arbitrary to begin with. So, this implies that summation  $\tau$  when evaluated on  $\lambda$  is 0 for all  $\lambda$  in the field  $K$ ,  $\tau$  coming from  $\Gamma$ . This means that if you think of these as just maps from  $K$  to  $K$ , so this identity is this identity is when I am thinking of all the  $\tau$ s as being maps from  $K$  to  $K$ .

It is, it is the linear combination of the  $\tau$ s that just the sum of the towers is just the 0 map. That is what this just means. But recall, we have proved linear independence of characters. The  $\tau$ s after all are characters and you know, of the the multiplicative group of the field and so on.

So remember, one of our corollaries of the linear independence of characters said that the auto morphism group of a field is always a linearly independent subset of maps  $K \rightarrow K$ . But recall that  $\Gamma$  is in fact  $K$  linearly independent. But then this thing here contradicts that. This is a contradiction. But summation  $\tau$  is 0, means they are linearly dependent, means  $\Gamma$  is linearly dependent.

This is a linear dependence relation among the elements of and that is your contradiction. So this proves the second half of Artin's theorem. So what we have really shown is that the, well, sorry I should not write, there is still one little thing that we need to do.

(Refer Slide Time: 24:22)

$$\begin{aligned} \therefore W &= (0) && \text{where } \{ \alpha_1, \dots, \alpha_m \} \text{ F.L.I. subset of } K \\ &&& \text{where } m \leq |\Gamma| \end{aligned}$$

Now:  $K^m \xrightarrow{\Psi} K \oplus K \oplus \dots \oplus K = K^n \quad (n = |\Gamma|)$

$$\beta \rightarrow (\psi^{\sigma_1}(\beta), \psi^{\sigma_2}(\beta), \dots, \psi^{\sigma_n}(\beta))$$

where  $\Gamma = \{ \sigma_1, \dots, \sigma_n \}$

- $\Psi$  is  $K$ -linear map
- $\ker \Psi = \bigcap_{\sigma \in \Gamma} \ker \psi^{\sigma} = W = (0)$



We are almost there. So, what does this prove? So, we only proved that  $W$  is 0. So therefore, our conclusion is that  $W$  is 0 but that is not what we wanted to prove the starting. So recall at this point, let us just remember what did we want to prove? We had, we started out with so, recall one,  $\alpha_1$  through  $\alpha_m$ , was our original linearly independent subset, this was the  $F$  linearly independent subset of  $K$ .

We wanted to show that this number  $m$  is at most the cardinality of  $\Gamma$ . This is what we wanted to prove. Now along the way, we have sort of shown, constructed a certain subspace  $W$  and shown that that subspace  $W$  is zero. So how does this subspace being 0 tell us that  $m$  can be at most of the cardinality of  $\Gamma$ . That is the last step that we need to complete.

So now consider the following map. So I had remembered, from  $K^m$  to  $K^n$ , I had a map say called  $\psi^\sigma$ . But now I am going to stitch all those maps together. So I am going to define from  $K^m$  to  $n$  copies of  $K$ . So this I will write as, so let us just keep it like this for the moment.

So what is  $\psi^\sigma$ ? It is the following. I take an element  $\beta$ , and I map it to the first component, I will map it to  $\psi^{\sigma_1}(\beta)$ ,  $\psi^{\sigma_2}(\beta)$  and so on.  $\psi^{\sigma_i}$ , what name shall we give  $n$  maybe  $\sigma_n$  of  $\beta$ , where  $\Gamma$  is the set  $\sigma_1, \sigma_2, \dots, \sigma_n$ . So I had a map  $\psi^\sigma$ , one for each element of my group  $\Gamma$ .

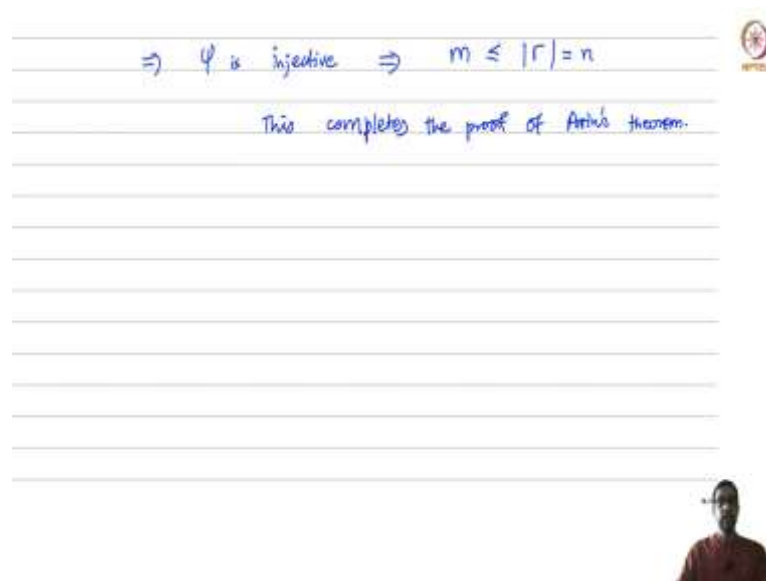
Now I am just stitching together all those maps forming one single map from  $K^m$  to  $K^n$  how many copies of  $K$ . This is  $K^n$ , where  $n$  is the cardinality of  $\Gamma$ . So I have a

map and remember that, that starting look like what we want to show that  $m$  is at most  $n$ , if we show that this map is injective for example, it will prove that the domain has to have dimensions smaller than the range.

And that is what we will show. Now observe  $\psi$  is, so we are almost done,  $\psi$  is a  $K$  linear map between these two  $K$  vector spaces. What is the kernel of  $\psi$ ? So this is obvious, the  $K$  linearity because each component is  $K$  linear and the kernel of  $\psi$  is, well all those  $\beta$ s which map  $2 \ 0 \text{ comma } 0 \text{ comma } 0 \text{ comma } 0$  and so on.

That just means that  $\beta$  should live in the kernel of each of the  $\sigma$  is but remember, that is exactly what we call kernel  $\sigma$   $\psi$ ,  $\psi$  belong belongs to  $\gamma$ , maybe write it like that. That is exactly the subspace  $W$ . It is the intersection of all these kernels of the  $\psi$   $\sigma$ s and now, where does that leave us? We just showed that  $W = 0$ . That was the whole point of the proof. And so it means that this map  $\psi$  is actually an injector map.

(Refer Slide Time: 27:45)



The slide shows a handwritten mathematical proof on a white background with horizontal lines. The text is written in blue ink. The first line reads:  $\Rightarrow \psi \text{ is injective} \Rightarrow m \leq |\Gamma| = n$ . The second line reads: "This completes the proof of Artin's theorem." There is a small circular logo in the top right corner of the slide. At the bottom right, there is a small inset image of a person's head and shoulders.

It is kernel is  $0$ , therefore,  $\psi$  is injected, or a 1 to 1 map. Now, an injective map between two  $K$  vector spaces means that the domain vector space must have dimension that is at most the dimension of the codomain or the range. So in this case,  $m$  can be at most the cardinality of the mod  $\gamma$ , which is what we call  $n$  on the left hand side. So that now completes. So this completes the proof of Artin's theorem. So next time, we look at some consequences of this theorem.