

Galois' Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bangalore
Lecture 47

Digression on Symmetric and Alternating group

In the last lecture we have been studying symmetric polynomials and we have proved the fundamental theorem on symmetric polynomials which says that every symmetric polynomial in n variables is a polynomial in elementary symmetric polynomials, this is a very important theorem which was proved essentially by Newton and today I will discuss about the discriminants of a polynomial. So in general we have been dealing with discriminants of small degree polynomials in school and colleges but today I will define discriminant for a general polynomial of any degree and we will use it to study the Galois groups of some polynomials.

(Refer Slide Time: 01:23)

①

$$f_n = (X - X_1) \cdots (X - X_n) \in K(X_1, \dots, X_n)[X]$$

$$= X^n - S_1 X^{n-1} + \cdots + (-1)^r S_r X^{n-r} + \cdots + (-1)^n S_n$$

$S_0 = 1$ S_1, \dots, S_n elementary Symm. polynomials

general poly of degree n

So as usual K is our base field and we have general polynomial of degree n that I have denoted f_n , this is a polynomial, $(X - X_1) \cdots (X - X_n)$ and we consider this as a polynomial over the rational function field in X_1, \dots, X_n and X this is what we consider this is a polynomial in X with co-efficient in the rational function and we have seen that this polynomial has when you expand it, it is $X^n - S_1 X^{n-1} \dots$, etc. etc. middle term is $(-1)^r S_r X^{n-r}$ and the last term is $(-1)^n S_n$, where this S_1 to S_n are elementary symmetric polynomials and for safety I will define S_0 equal to 1, so I have these, this is a general polynomial of degree n .

(Refer Slide Time: 03:43)

Let $V = V(X_1, \dots, X_n)$ (2)
 (Vandermonde's determinant)
 $= \text{Det} \begin{pmatrix} X_1^0 & X_1^1 & \dots & X_1^{n-1} \\ X_2^0 & X_2^1 & \dots & X_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ X_n^0 & X_n^1 & \dots & X_n^{n-1} \end{pmatrix}$
 $i=0, \dots, n-1$
 $j=1, \dots, n$
 Verify $= \prod_{1 \leq i < j \leq n} (X_j - X_i)$
 $\in K[X_1, \dots, X_n]$

So when I have a polynomial in one variable over some field then I will satisfy this capital X_i equal to the roots of that polynomial and get back the original polynomial that is the idea. Now I consider these so let V which is $V(X_1, \dots, X_n)$, you will see why I chose the name V , this is precisely Vandermonde's determinant, I will write here Vandermonde's determinant and what is that?

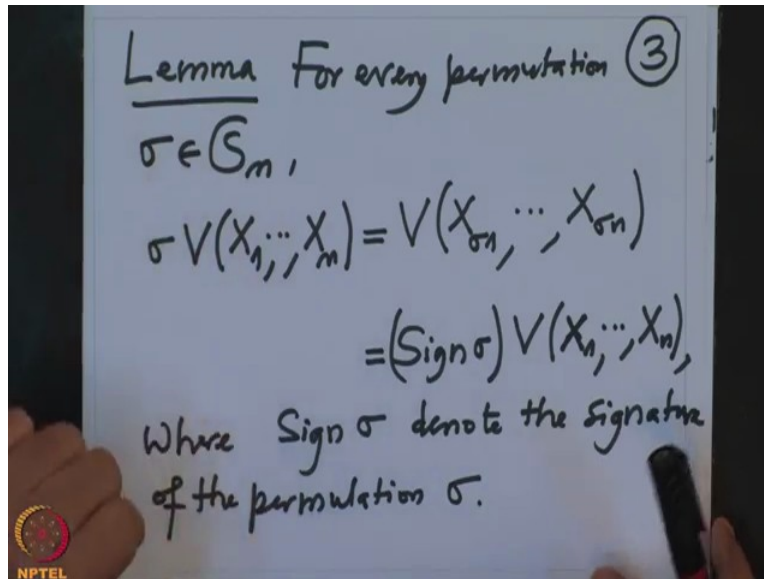
That is you take the matrix X_j^i , i is varying from 0 to $n-1$ and j is varying from 1 to n , so it is to get our hands so for example the first column is j is 1 right and i is varying so $1, X_1, X_1^2, \dots$ etc. etc. it goes on to X_1^{n-1} , this is the first column, the j th column will be $1, X_j, X_j^2, \dots$ etc. etc. X_j^{n-1} and so on, this is a big matrix, it is n cross n matrix and therefore determinant of that make sense.

These determinant you would have studied well in the college days, this determinant is I am denoting by V , so it is a polynomial in the variables X_1 to X_n , okay when you solve this determinants you would have realized this is the value of this determinant is product, product is running over the indices $1 \leq i < j \leq n$ and the product $X_j - X_i$, I will just indicate how it is solved you just subtract the column 1 from column 2 let us say and then you take out the common factor $X_2 - X_1$ and so on and that is what you do.

So this I would simply say this equality you verify, that is not too difficult so this is the Vandermonde's determinant and this is called Vandermonde determinant of X_1 to X_n and remember it is a polynomial over a field K , you can take any field X_1 to X_n , it is a polynomial

there, also therefore you can think it is a rational function, okay and the first important observation now I want to make in the following lemma.

(Refer Slide Time: 06:55)

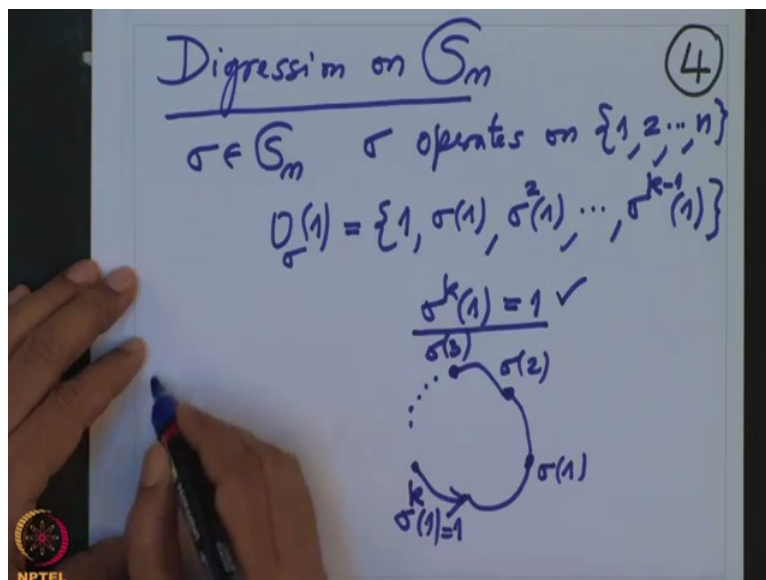


The image shows a whiteboard with handwritten text in black ink. At the top, it says "Lemma For every permutation (3)". Below that, it says " $\sigma \in S_m$ ". The main equation is " $\sigma V(X_1, \dots, X_m) = V(X_{\sigma 1}, \dots, X_{\sigma m})$ ". Below the equation, it says " $= (\text{Sign } \sigma) V(X_1, \dots, X_m)$ ". At the bottom, it says "Where $\text{Sign } \sigma$ denote the signature of the permutation σ ". There is a small NPTEL logo in the bottom left corner of the whiteboard image.

So lemma for every permutation $\sigma \in S_n$, if I permute variable in the Vandermonde determinant according to σ that means I am taking σ of this, so this was by definition what, this was by definition V of permute the variables according to σ , this is $X_{\sigma 1}, \dots, X_{\sigma n}$, now if it is equal to V then V will be symmetric that was the definition of a symmetric polynomial right but this is not symmetric so what comes out is $\text{sign } \sigma$ times $V(X_1, \dots, X_n)$, where $\text{sign } \sigma$ denotes the signature of the permutation σ .

Now I should digress little bit on the definition and some easy properties of the signature that I do it before I prove this lemma and we will come back to the proof of this lemma, so this says that this Vandermonde determinant is not a symmetric polynomial but it is almost like a symmetric polynomial.

(Refer Slide Time: 08:49)

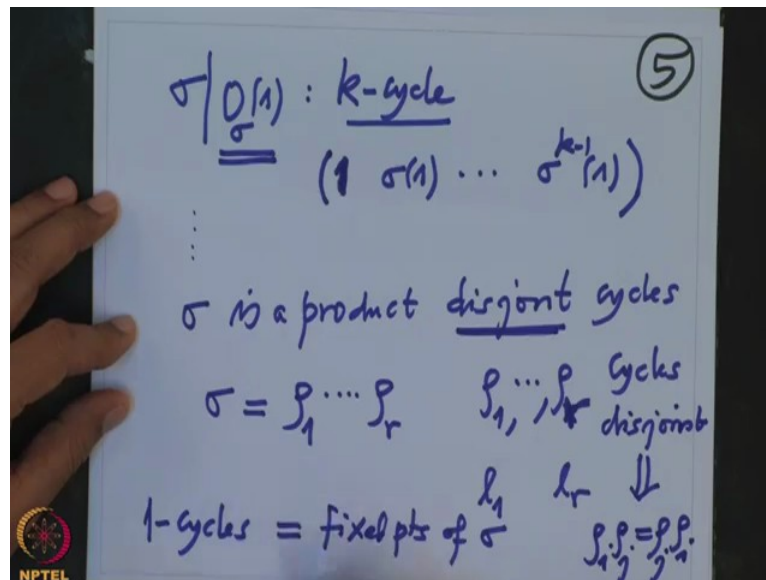


Okay so before we go on now this is Digression on the group S_n essentially, so the elements of the permutations we know, so σ any element, now note that the σ is a permutation so therefore this σ operates on the set 1 to n, so therefore I can talk about orbits, so when I say orbit of $O_\sigma(1)$, what does it mean? This means it should orbit of 1 under σ that means it starts with 1 then let us go to $\sigma(1)$, if it is different from 1 stop it, then if it is then go to $\sigma^2(1)$ and so on.

Now you will come to the power $\sigma^{k-1}(1)$, 1, and then I have chosen in such a way that these elements are distinct then you note that if I look at $\sigma^k(1)$ it has to be equal to 1, it has to be return to 1 so pictorially it start like this, 1 will start with 1 then $\sigma(1)$ then go to $\sigma(2)$ then go to $\sigma(3)$ and keep doing this, ultimately you will come back to 1, this is $\sigma^k(1)$ that will be 1 and just 1 before so why does it come back to 1?

Because if it does not come back to 1 then it will be some smaller power of σ but σ has a inverse so just cancelling that you will get a contradiction to the fact that these elements are distinct therefore σ power 1 is 1 so this is called a orbit of 1 now you choose an element outside this and do the same process, so therefore what it means is and if I restrict σ to this set so σ restricted to, so I will write on the next page.

(Refer Slide Time: 11:30)

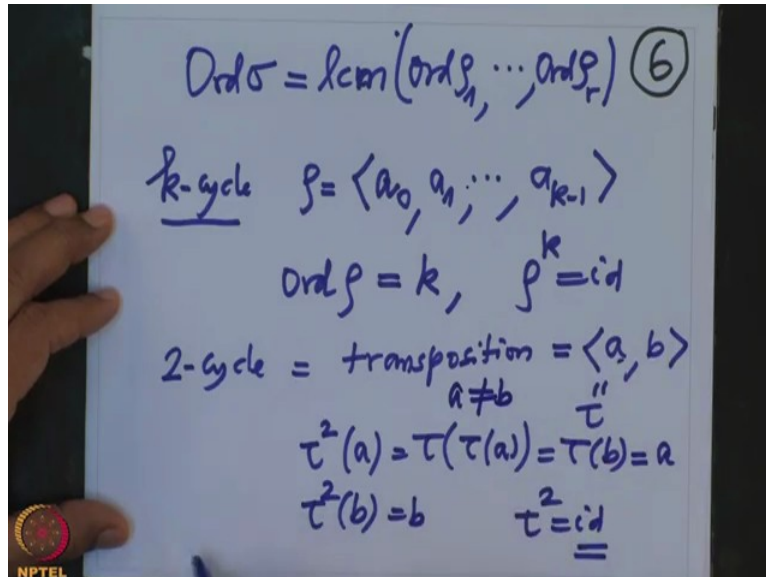


σ if I restrict to the orbit of 1, it is a very nice, it is actually a what is the k cycle, what does that mean, that means we can write this as only elements which are disturbed under this is 1, start with 1 then it goes to $\sigma(1)$ and so on, it goes to $\sigma^{k-1}(1)$ and then it comes back to 1 so you can complete it here, so therefore to this subset, if I restrict σ then it is a k cycle, the remaining element under these are fixed.

So I can do now if 1 to σ^{k-1} is exhausted all the latest I keep quit, otherwise I choose an element outside these and do the same thing that means this means if I continue like this, this means σ is a product of disjoint cycles, I will define what is a cycle, so that means I have written σ as a product of disjoint that means they do not have anybody in common, this I have written it as some $\rho_1 \dots \rho_r$ where ρ_1, \dots, ρ_r are cycles and this may have length l_1, \dots, l_r , that means this is l_1 cycle, this is l_r cycle and some of them could be one cycles, one cycles means they corresponds to the fixed point.

So 1-cycles they correspond to the fixed points of σ , so if one wants to understand a permutation one has to understand each cycles carefully and they do not middle with each because they are disjoint therefore they commute, so disjoint will mean that they commute so cycles disjoint and that means they commute $\rho_y \rho_j$ will be equal to $\rho_j \rho_y$ so as far as finding the order of the permutation σ in the permutation group, if we know the orders of these guys then we will know order of the σ because they commute therefore the order of the product will be the LCM.

(Refer Slide Time: 14:24)



So the advantage is our calculation becomes easier, comfortable so from these we will know that order of σ will be equal to LCM of orders of ρ_1 to order of ρ_r and therefore we only have to know what is the order of a cycle so if you take a k-cycle that means what, it is like this, in general it is $\langle a_0, a_1, \dots, a_{k-1} \rangle$, it has $k - 1$ elements in that.

These are the elements which are moved under these k-cycle remaining elements which are not here they are fixed so the order will be precisely order of these if you call these k-cycle as rho then order of rho will be nothing but k that means rho power k is identity that is easy because once rho square will, ρ maps is a_0 to a_1 , ρ^2 will map a_0 to a_2 and so on when you take k times composition of ρ with itself you get back identity.

So for example order of, if you take 2-cycle. 2-cycle is also called a transposition, the transposition looks like a, b, the only two elements which move under the transposition a and b remaining elements are fixed so this is usually denoted by τ so τ^2 if I want to compute, look at $\tau^2(a)$, $\tau(a)$, this is $\tau(\tau(a))$, but $\tau(a)$ is b, so this is tau b but tau b goes back to a so it is a.

Similarly $\tau^2(b)$ is b therefore a and b are fixed and the remaining are already fixed therefore we conclude that tau square is identity and if a when one writes transposition usually a is not equal to b otherwise it is added so therefore order of a 2-cycle is order of tau is 2, so if you go on then it is clear that order of a k-cycle is k.

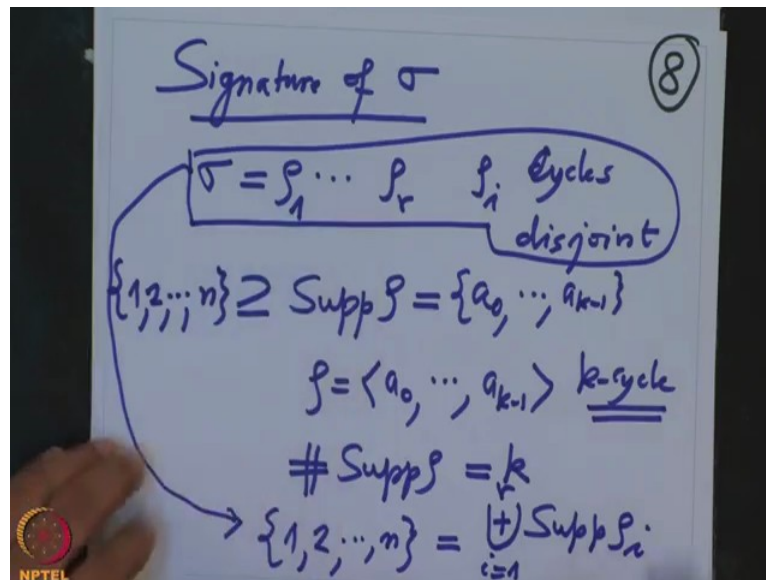
(Refer Slide Time: 16:53)

$\sigma = \rho_1 \cdots \rho_r$ ρ_i cycles (7)
disjoint
 $\text{Ord } \sigma = \text{Ord}(\rho_1 \cdots \rho_r)$
 $= \text{LCM}(\text{Ord } \rho_1, \dots, \text{Ord } \rho_r)$
3-cycle $\rho = \langle a, b, c \rangle$ 3-cycle
 $\text{Ord } \rho = 3$
1-cycles = id

And therefore if you would have written σ as a product of disjoint cycles ρ_1 to ρ_r these ρ_i 's are k -cycles of disjoint, disjoint is very important. Then the order of σ is order of this product, order of the product element in the group is not so easy to compute in general but when they are commuting then that order is nothing but LCM of orders of those elements, so this is easy to check so one more, what is the 3-cycle?

3-cycle is look like this a, b, c that means a, b, c are moving and this notation means a goes to b , b goes to c , so if this is ρ , this is 3-cycle. So order of these 3-cycle will be 3, that is in general. So we can easily compute if I give you the permutation, I first decompose that permutation into disjoint cycle and read the order, now what is a signature? So I would have to define signature in the same way so and also I should have mentioned earlier 1-cycles are identity okay.

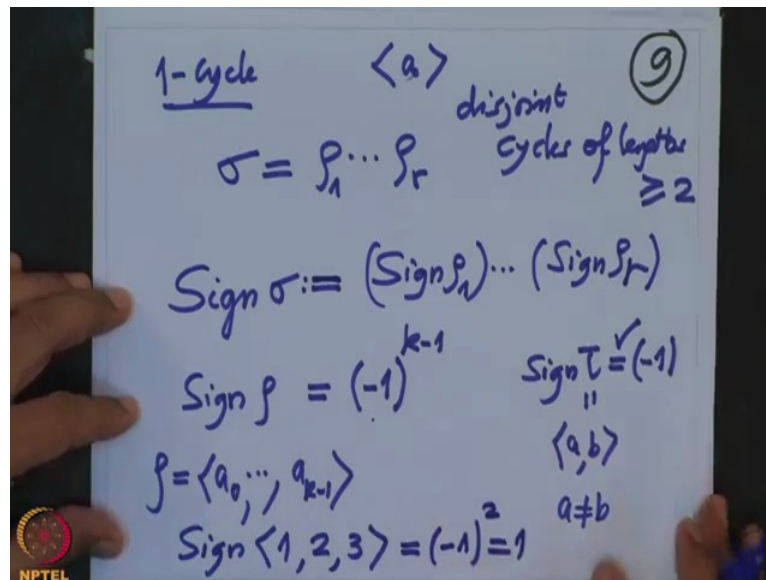
(Refer Slide Time: 18:41)



So to define a signature of permutation σ what is it, you first decompose into disjoint cycles, ρ_1 to ρ_r , ρ_i cycles and their disjoint, so therefore support, what is support of a cycle? Support of any cycle ρ is precisely the elements which it moves that means the elements which it contains.

So if ρ is this a_0 to a_{k-1} , this is a k -cycle, the support of ρ is precisely this subset a_0 to a_{k-1} , so if ρ is a k -cycle then the support of ρ has cardinality precisely, cardinality of the support is precisely k , since support is a subset of 1 to n and if you take their unions, unions of the support, so if σ is this written as a product of disjoint cycles then we know that this set 1 to n is precisely the disjoint union of supports of ρ_i , i is from 1 to r , disjoint union because they are disjoint and therefore we have decomposed this set into this.

(Refer Slide Time: 20:46)

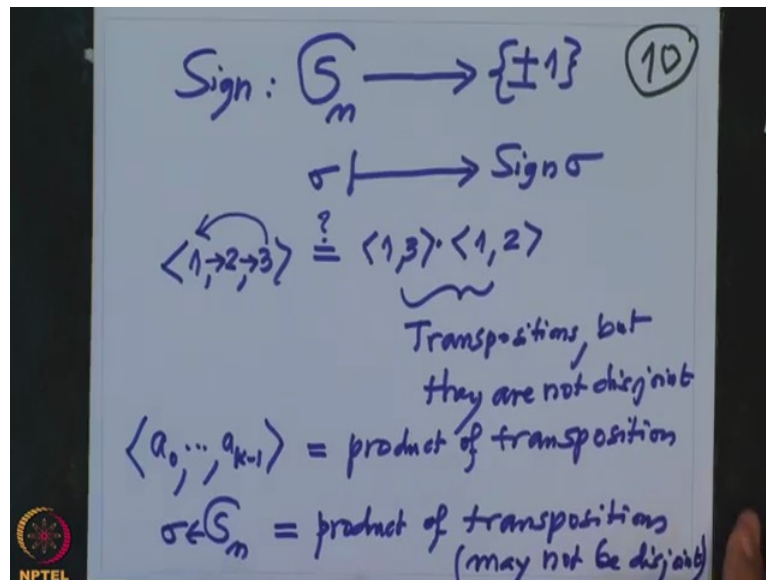


Now some supports may have only the singleton, the 1-cycles are precisely the identity element so they are 1-cycles will correspond to the fixed points so note that when you write 1-cycle, 1-cycle simply means like this but this is equivalent to saying a goes to a so this is like identity, so when we do this calculation we might as well assume that σ is rho 1 to rho r and they are cycles, disjoint of course of length big or equal to 2 because that is not playing any role here, so those are precisely the fixed points.

So therefore to define a sign of σ I want to define sign of cycle first where rho is k-cycle and this I define it to be equal to minus 1 power k minus 1, the number of elements minus 1 so this will give us sign of tau, where tau is a transposition, a not equal to b then this sign is minus 1 power 2 minus 1, this is so it is minus 1 so sign of a transposition is minus 1, sign of a k-cycle is minus 1 power k minus 1 and then you define sign of σ to be the product of the signs, this you define this, this is the definition, so that is a signature of a permutation.

Now what is sign of a 3-cycle, sign of say permutation 1, 2, 3 this means 1 goes to 2, 2 goes to 3 and 3 goes back to 1 and remaining guys are fixed, so this is therefore 3-cycle therefore sign is minus 1 power 2 which is 1.

(Refer Slide Time: 23:11)

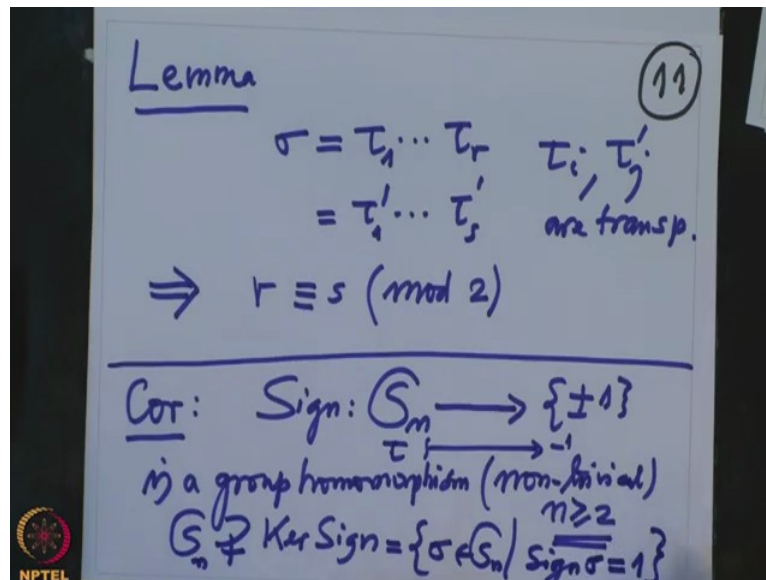


So the permutations we have which we have sign, sign is therefore we have define in a map, this is a map from the group S_n to the two elements with plus minus 1 so any σ goes to sign σ and what is more important is every cycle you can write it as a product of transposition for example so for example if I have cycle 1, 2, 3 this is a product of 1 goes to 2 composed with 1 goes to 3 is clear, so one has to be little careful how do you calculate.

So first you go from right to left, that is like a composition, so here 1 to goes to 2, 2 is fixed so 1 goes to 2, I am checking this equality, 1 goes to 2, 2 is fixed so 1 goes to 2, where do 2 go? 2 goes to 1 then 1 goes to 3 so 2 goes to 3, where do 3? 3 is fixed under this and 3 goes to 1, so this 3 goes to 1, so that is how 1 decompose cycle into product of transposition but remember these are not, these are transpositions but not disjoint, they are not disjoint.

So similarly you can decompose any k-cycle into product of transpositions and this way we would have decomposed any σ in S_n is a product of transpositions but we cannot say now the product of these transpositions is disjoint that we cannot say, may not be disjoint.

(Refer Slide Time: 25:38)



But what we can assert is the following easy lemma which I am not going to prove, I will leave it as an exercise so if σ is a product of disjoint transpositions in two ways, τ_1 to τ_r and τ'_1 to τ'_s where τ_i, τ'_j are transpositions then these r and s they are equal mod 2, this is easy verification which I am not going to do but this will allow us therefore once important consequence will be, corollary will be the sign map from S_n to plus minus set, now this is a group under multiplication, this is also group under composition and this map is a group homomorphism.

So signature is a map and therefore kernel makes sense, kernel of sign, this and obviously this group homomorphism is non-trivial, non-trivial means where n is at least 2, non-trivial means everybody does not go to 1, at least one element here goes to 1 well where the transpositions are going to minus 1 and because n is at least 2 there are transpositions and therefore kernel of this homomorphism is not the whole group, it is properly contained in S_n and these are precisely all those permutations σ such that sign of that σ is 1.

(Refer Slide Time: 27:59)

$\text{Ker Sign} =: A_n \subseteq S_n$ (12)
 $\{ \sigma \in S_n \mid \text{Sign } \sigma = 1 \}$
 $\{ \sigma \in S_n \mid \sigma \text{ is a product of even number of transp.} \}$
 A_n is normal subgroup of S_n of index 2;
 $S_n = A_n \cup \tau A_n$ where τ any transp.
 $S_n / A_n \cong \{ \pm 1 \}$

And sign is 1 means the σ is a product of even number of transpositions and therefore this group is very important and that group is called, so kernel of sign this is the definition, this is a subgroup of S_n and this is precisely all those permutation σ in S_n such that sign of σ is 1 but this is same as all those permutation σ in S_n such that σ is a product of even number of transpositions.

And it is also clear that this is a normal, normal subgroup of S_n because it is kernel of a group homomorphism and of index 2, in fact it is very easy to see that this group A_n is same thing as a disjoint union of any transposition times A_n , where τ is any transposition, that is very clear because we know that A_n is a kernel therefore what we know is S_n modulo the kernel that is A_n , these group is isomorphic to the group plus minus 1.

This group has kernel into 2 therefore these quotient set as kernel into 2 that is the meaning that it is index 2 and therefore this decomposition there only 2 cosets of A_n in S_n and they are precisely this, with this I will prove the lemma in a next half and we will continue after this digression of a group to study.

I have not yet come to the definition of a discriminant so I will study the Vandermonde determinant under, we want to check that if you apply, if I permute the variables in the Vandermonde determinant what happens to that determinant is it changes the sign according to the sign of that permutation. So I will continue after the break.