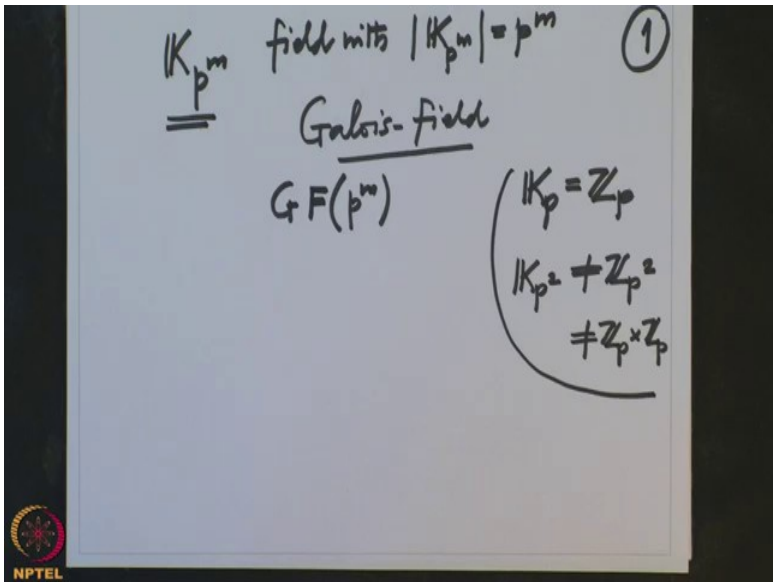
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics,
Indian Institute of Science, Bangalore.
Lecture No. 23
Digression on Group action - 1

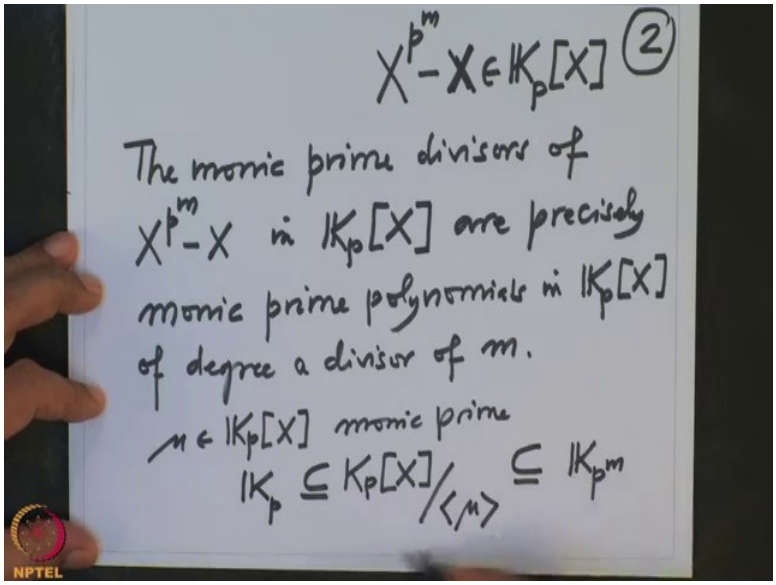
(Refer Slide Time: 0:51)



We have seen that given the prime number p and a positive natural number m, there is a field with which early p^m element and to such field are uniquely determined up to an isomorphism, such a field use a rotation for such a field is therefore, I am going to denote by double line K_{p^m} this is field with cardinality p^m, such a field is also called as a Galois field and some people also denoted by the notation $GF(p^m)$, G for Galois and F for the field, but I will denote by this, so for example in this notation K_p is nothing but $\mathbb{Z}_p$ and note that K_{p^2} is not $\mathbb{Z}_{p^2}$ because $\mathbb{Z}_{p^2}$ is not a field or not even $\mathbb{Z}_p \times \mathbb{Z}_p$, this is a vector space of dimension two.

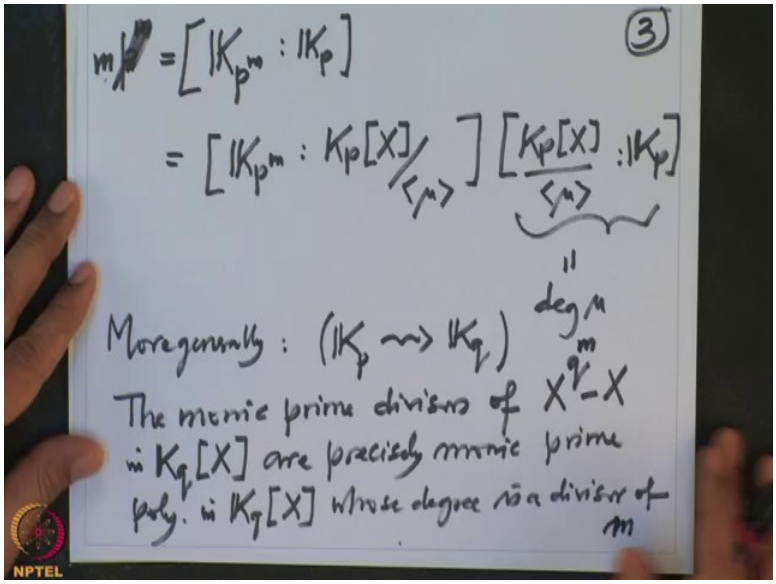
So as a vector space it is this but not as a field, so remember this, this very important. Okay, now I want to deduce two important consequences of the above proof, the proof we have given that such fields are uniquely determined namely, we have deduce, we have use in the construction, we have used this polynomial.

(Refer Slide Time: 2:33)



$X^{p^m} - X$ and this is a polynomial in $K_p[X]$; okay, so the statement I want to write is, the monic prime divisors of is polynomial $X^{p^m} - X$, in of course in this ring, in $K_p[X]$ are precisely monic prime polynomials in $K_p[X]$ of degree a divisors of m, so what I am writing, that means monic polynomial prime and the degree of that polynomial has to be divisor of m, why is that? Because if you take such a monic polynomial in μ, μ in $K_p[X]$ which divides μ monic, monic prime, then $\frac{K_p[X]}{\mu}$, it is a it is a field of this K_{p^m}, but this is a field which contain K_p, so the degree, this degree is m I know.

(Refer Slide Time: 5:07)



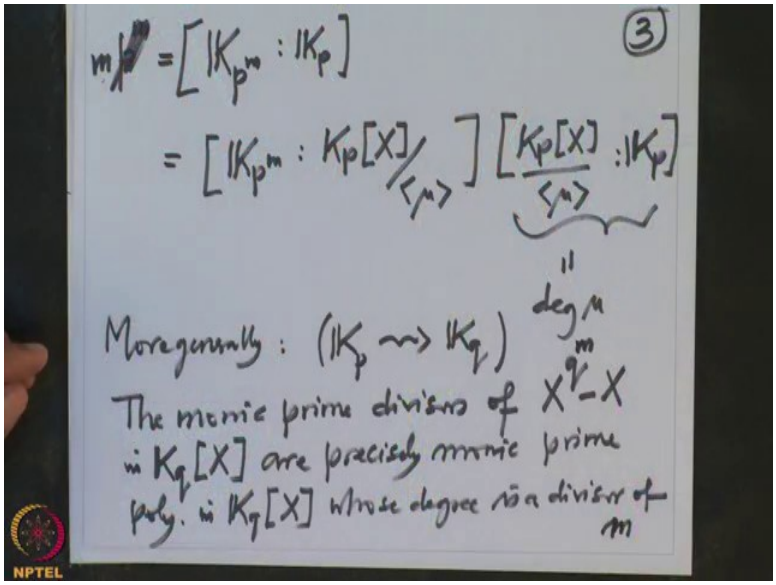
So you see the degree of K_{p^m} over K_p these degrees p^m, but these degrees is same thing as K_{p^m} : $\frac{K_p[X]}{\mu}$ and this degrees is $\frac{K_p[X]}{\mu}$ over K_p this degree is nothing but degree of μ, so degree of μ has to be the divisors of this, no actually it is a divisors of m, (this is not) this is not p^m, this is M, this degree is m, because it is a degree m extension, because this has cardinal p^m, so this is m and this is degree in μ, so μ, degree μ divides m.

So their same m conversely we have any minimal monic prime polynomial of degree is some degree, then this is a field and there has to divide this, so (the) that justify the earlier statements. The prime divisors of $X^{p^m} - X$ are precisely the monic prime polynomial of degree which are divisors of m.

Okay, this is one observation and this is not only true for p power, so this is more generally you could write if I have not only for $\mathbb{Z}_p$, not only for K_p, I want to write a statement for more generally the same proof, I want to replace K_p by any finite field with cardinality q, the q has to be power of p of course.

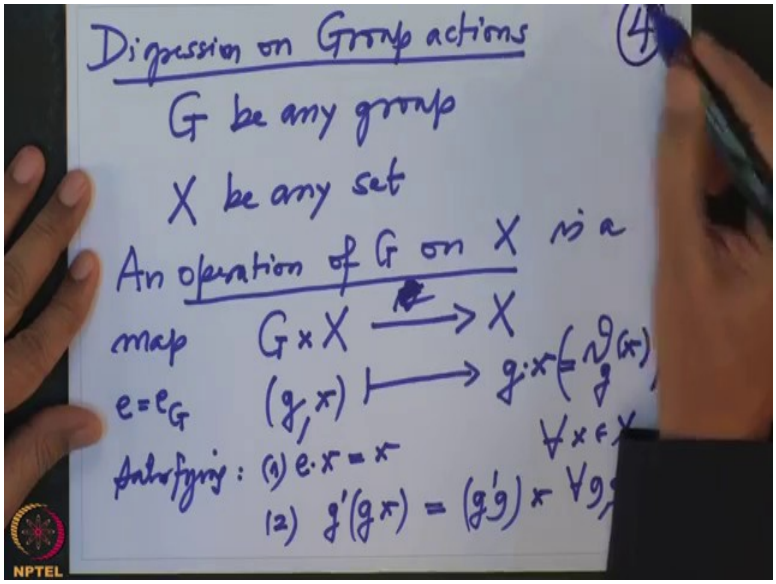
So, so the monic prime divisors of $X^q - X \in K_q[X]$ are precisely monic prime polynomials in $K_q[X]$ whose degree is a divisors of m, where q is course p power q power q power m, so I just replace the field K_p by K_q and the same statement and the proof is also same; okay, so that two important observations, now as one realises that to studies zeros of the polynomials.

(Refer Slide Time: 8:50)



Finite group theory plays very important role, another concept where this course will centre around is so-called the concept of group actions.

(Refer Slide Time: 9:02)



This is a digression on Group actions, we do not need in this digression we know, we do not need G to be a finite group, so take G be any group and X be any set, so an operation of G on X is a map from $G \times X \rightarrow X$ and this map is denoted by (g,x) goes to simply, this is simply a notation gx .

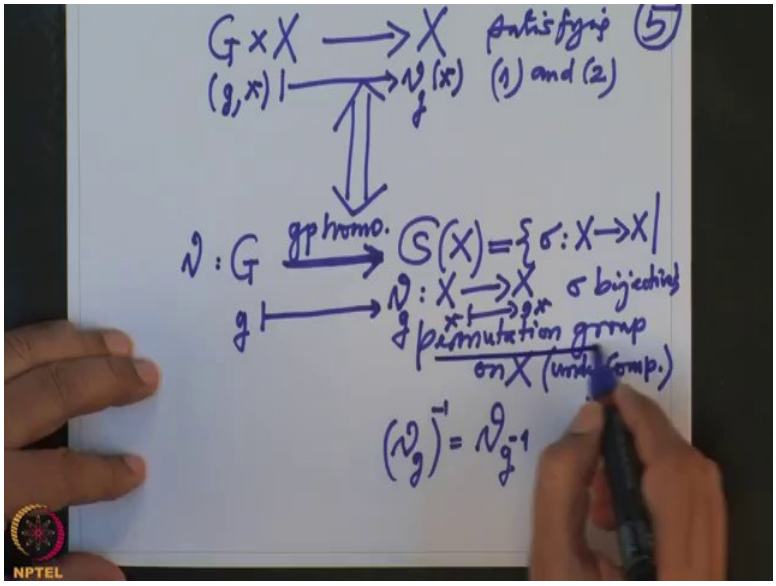
Satisfying the two properties, so this is simply just a notation or one also denotes just not to get confuse, one also denotes this as theta, so for g we valuated at x, so this is a map theta, do

not give, this is just a notation, just gx that is just a image of the (g, x) and what properties it should satisfy namely identity times x, whereas is e identity in G this should be x, this is property 1 and 2, if I take gx, I will also stop writing that dot in between and then, this is an element of x, these are multiplied by another element of the group G, g' that should be $g'gx$, now this is an operation in g and this operation we are defining.

So, it is clear from the context what we are writing and these equations are true for all $x \in X$ and for all $g, g' \in G$, in such map is called an operation of G on X, also I know this is actually called a left operation of G, G is written on the left, on the right it will be called a right action, but we will consider only a left operation, so this is a typical example.

Let us see some examples, so before I give more example I will just reach translate this a definition, so for an example on the set X, G may operate the same group, G may operate in a different way, for example, one obvious operation in their it is a trivial operation namely, G times X is X for every G, so that is a trivial operation or so the two, the same group G can operate on the same set in a different way, but giving an operation of G on X.

(Refer Slide Time: 12:53)



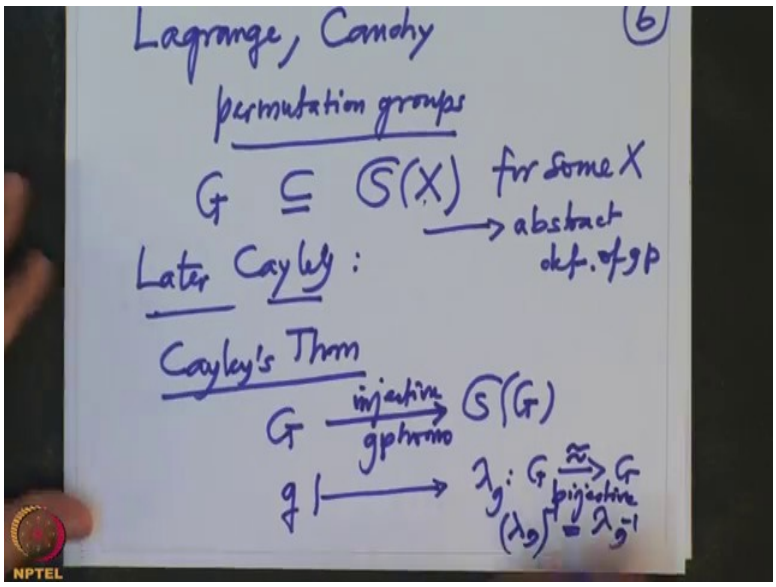
So $G \times X \to X$ giving such a map satisfying one and two, this is an equivalent to giving a group of homomorphism from G to the group $S(X)$, $S(X)$ this is a group of all bijections from X to X, σ from X to X a map, σ bijection, this is called a permutation group on X, this is a group under composition, the identity element in this group is either identity map of

X and inverse of element is either is set theoretic inverse of the map σ and giving such an operation is giving equivalent to giving a group homomorphism.

So what is the identification, so any g you can, you want to define a map which is a bijective, so that is, we want to define a Θ_g and Θ_g should be bijective map from X to X and that is precisely this x going to gx, now you check that this is bijective, that is very easy because $\Theta_{g^{-1}}$ is nothing but $\Theta_{g^{-1}}$ is obviously the inverse because of the property one and two and conversely if you have given such a map Θ, then we have the operation namely g,x where does it go, it goes to $\Theta_g(x)$.

So to give an operation is equivalent to give a group of homomorphism, so this is important in a group theory setup that we need a group of homomorphism and a property that it is a group of homomorphism is encoded in one and two; and one and two implies it is a group of homomorphism and so, so these permutation group is very important.

(Refer Slide Time: 15:28)



And let me remind you the Lagrange, was the one who started with the permutation group studying permutation group is early with a, he did not mention it explicitly but essentially he was studying permutation group. And Lagrange and Cauchy, later Cauchy, these are the people who started studying permutation group more and more intimately.

Infect those days by definition of a group G was always a subgroup of the permutation group for some X, this was a essentially a definition, so this simply means, G is operating on X because this naturally inclusion will give you operation of G on X.

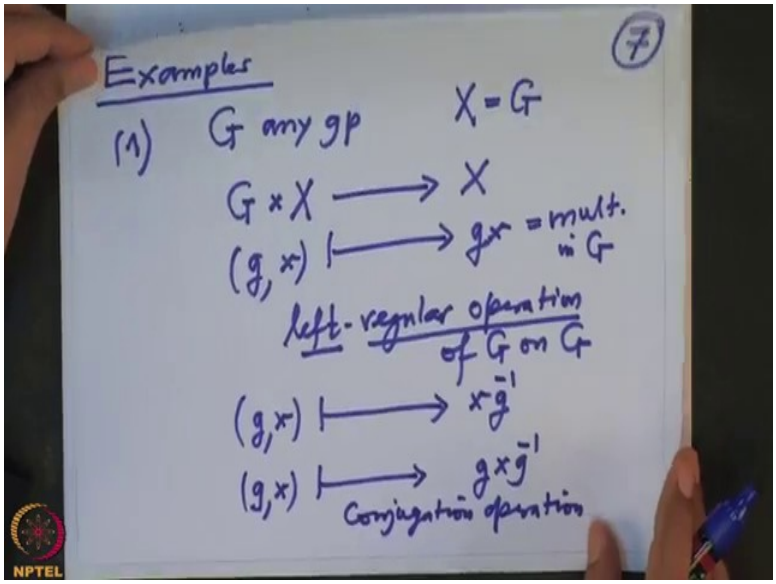
So later on Cayley proved that, later Cayley proved that a in between there was an abstract definition of a group, abstract definition of group, namely what we are used to the G they said in the binary operation where there is an associated activity identity exits and every element has inverse this was an abstract definition of a group, it came much later than this definition but later Cayley prove that this two definitions are equivalent by proving Cayley's theorem.

So Cayley's theorem, Cayley proved that if I take G and if I take a permutation group of G this they injective map here natural injective map, injective group homomorphism, that means G is a subgroup of this permutation group but these G maybe two big set, maybe you want to find a smaller and smaller set where G is a subgroup of the permutation group on that symbols.

So that requires more efforts but just a subgroup is trivial because in it take in g and take a multiplication map on g by G and obviously these G is, this λ_G is a bijective map not isomorphism but bijective map because the inverses $\lambda_{G^{-1}}$ nothing but $\lambda_{G^{-1}}$ and therefore that gives an inverse, so that means they are bijective maps, so this is a trivial theorem.

So and this map is injective is also trivial theorem, so but importantly says that the modern and old definitions are equivalent, now I want to give a some few examples important examples of a group actions.

(Refer Slide Time: 18:36)



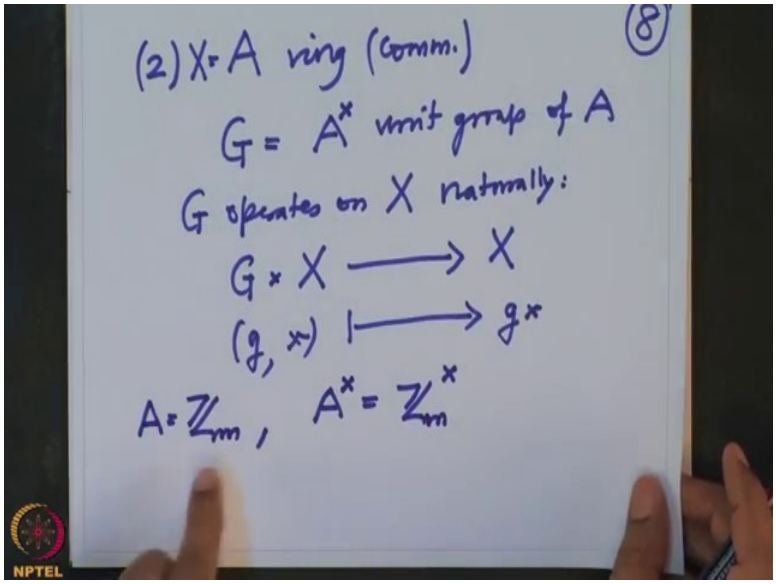
So examples, one a so first of all take any group G, G is any group and X is also G, so now I want to give you operation, so G I want to give you a map from G cross, I will still write X for psychological reason to X and then the pair (g,x) goes to gx, this is now a multiplication, this is a multiplication in G because x and g both are elements of G, this is a binary operation in G multiplication but it is clearly it satisfy the one property one says that E is an identity in property and the second property says that it is associated activity.

So therefore G operates on G by left multiplication, so this is called left regular operation of G on G, left because it is a left multiplication. If I want to give you the right one then I want to give I want to multiply G on the right side but then to make one and two property will have to say that multiplied on the right not by G by G^{-1}.

So g, x mapping to xg^{-1} because a property two should satisfy, so this is also operation, on G this is a right operation, we can combine the both two, then we can give another one (g,x) goes to gxg^{-1}, this is, conjugation operation, so you see on the same set G, G is operating on many ways.

Okay, so this was one example and more and more examples I will keep collecting it when we go on according to our need but one very important I want to say it now is second example.

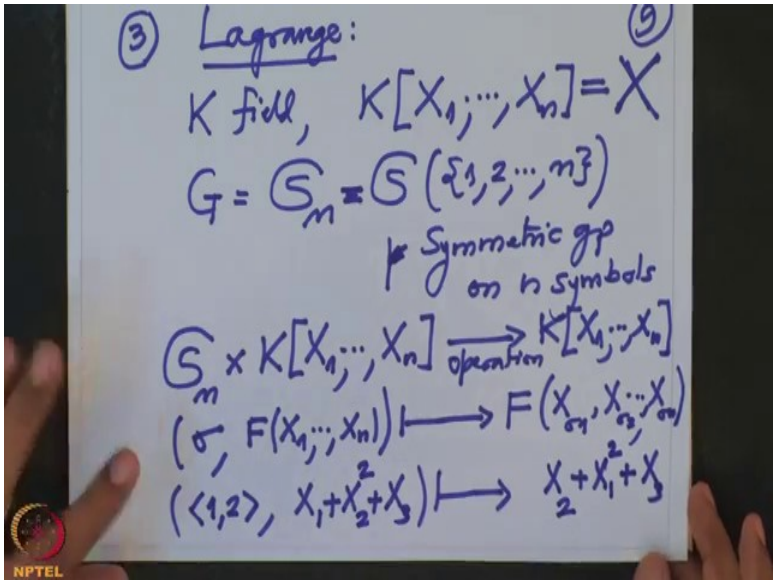
(Refer Slide Time: 21:19)



Suppose A is any ring, you take commutative ring and then I know the group G, G is the unit group of A, A^x , this is the unit group of A, then this A^x operates on A naturally, A is my set X, so X is my A, so G operates on X naturally, how then that means you have to give map $G \times X \to X$, so take any g, take any x and just multiply gx this is a multiplication in the ring now, so this is an operation which satisfy one and two it is very clear, if g is identity of the group that is identity in the ring A and therefore one X is X and so on, so this is a natural operation.

In particular you see if I take the ring $\mathbb{Z}_m$ this is my ring A and what is my group G than A^x , A^x is nothing but $\mathbb{Z}_m^x$ that is a group that we know and then this group operates here, it is very natural and one wants to understand this operation well and I want to introduce some more definition to understand what we have to understand.

(Refer Slide Time: 22:56)



Now another important example is, this is Lagrange, so you take a field K and take a polynomial ring in many variables $X_1,\ldots,X_n$, this is my set capital X, this is the set I want to and the group G is a permutation group on n symbols, so this is same as S of the set $\{1,2,..,n\}$ bijective maps from one two n the abbreviation for this symbol is just S_n.

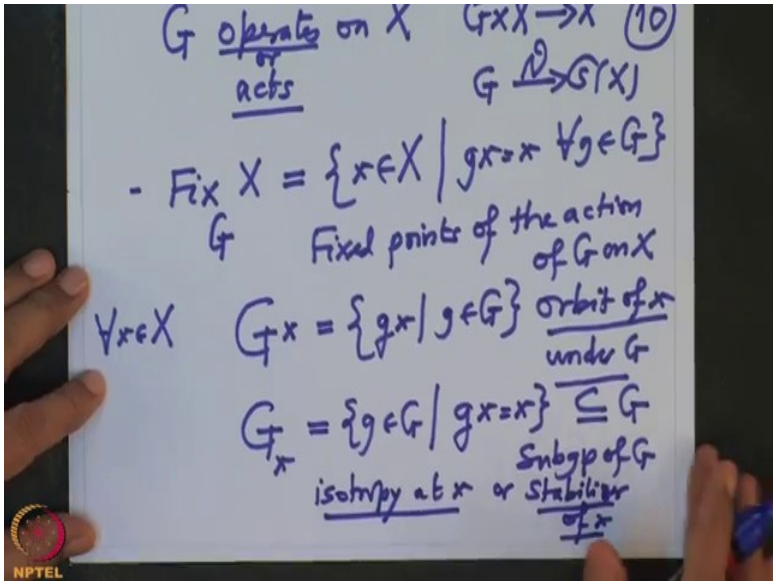
This is permutation symmetric group is also called symmetric groups on n symbols or n letters and how does this group operates on the polynomials, so that means I want a map from S, S_n cross polynomials in n variable to again a polynomial variable, so that means given permutation σ and a polynomial F in n variables I want to get new polynomial, so this should go you take the same polynomial and permute the variables according to σ.

So $F\left(X_{\sigma(1)},X_{\sigma(2)},\ldots,X_{\sigma(n)}\right)$, so just you have to check that this is an operation, operation of the group on the polynomials that is very easy because when σ is identity polynomial does not change and when you have two permutations you first apply one permutation and then apply another permutation that is like applying composition of the permutation.

So to say that, if I take say for example σ is the transposition $(1,2)$ and if I take the polynomial $X_1+X_2^2+X_3$ where will this go, this pair will go to this polynomial I have to change variables according to this permutation, so 1 is going to 2, 2 is going to 1 and remaining in this is are fixed, so first of all X_3 is fixed, X_1 is going to X_2 so this polynomial is going to X_2 and X_2 is going to X_1, so this is $X_1^2+X_3$.

So you permute the variables according to the permutations, so Lagrange was studying this group actions was studying the solutions of the roots of the polynomials in the one variable and relating to it questions, so this I will do this more precisely when we are in a flocabulary but right now, I need to introduce more for flocabulary about group actions, so whenever we have a group action.

(Refer Slide Time: 26:28)

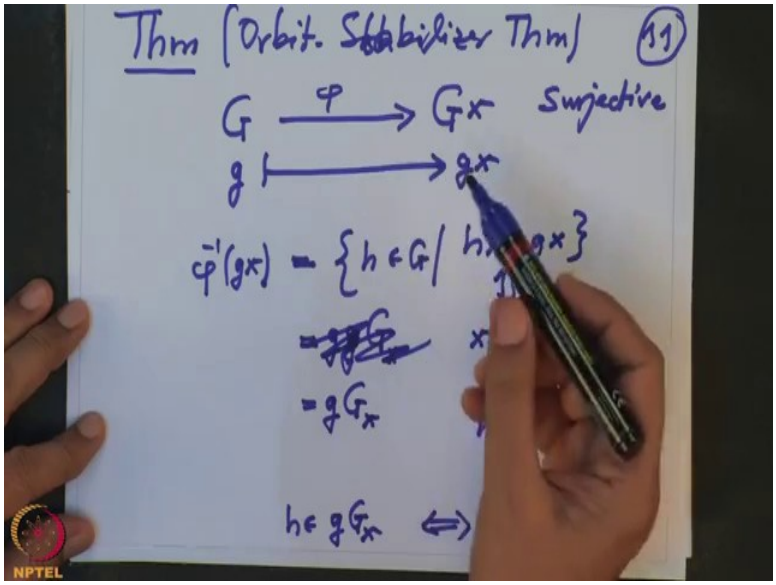


Now we will say that G operates on X or I will also say that G acts on X, these are the same thing, operation will mean that the map $G \times X \to X$ and action will mean that G to $S(X)$ both these are equivalent only the words are different, so when G operates on this, that means think of this, this is a G to $S(X)$, there is a group homomorphism, this is theta, so what is a fix? If I rate fix points of X under G that means by definition all those $x \in X$ such that gx equal to x for all G, these are called a fixed points of the action of G on X, that is one thing.

Another definition I need is for every $x \in X$, I have the orbit Gx this is all the G multiples of x, so gx as g whereas in G, so this is orbit of g, orbit of x under G or G multiples of x, similarly I have G_x, these are all those elements in g in G such that G do not move x, so that gx is x, this is a subset of G, this is clearly a subgroup of G that is easy to check from the group action property 1 and 2 and a also this is called isotropy at x or stabiliser of x.

Both these a terms come from physics actually because a stabiliser, it is stabiliser this x and it is isotropy at x, so and the basic relations between the two I just want to write which is called orbit stabiliser theorem.

(Refer Slide Time: 29:05)

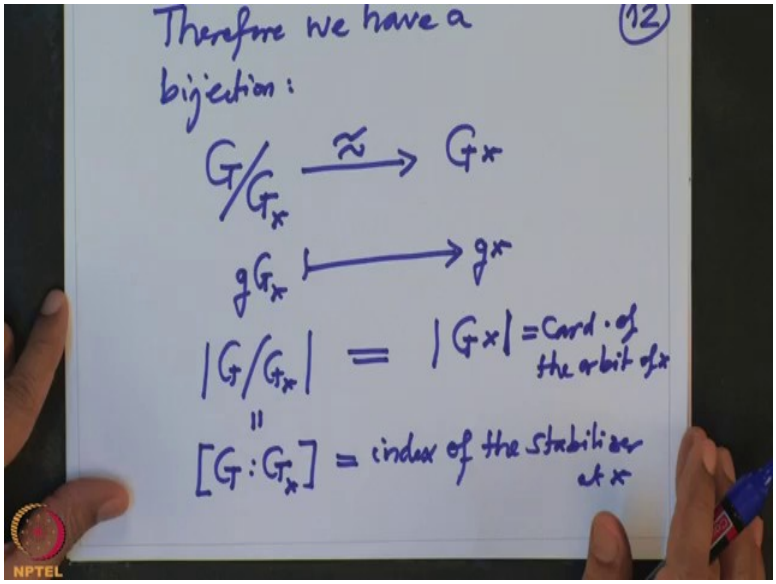


This is theorem, this is called orbit stabiliser theorem, it says that to get the map, the map G to Gx orbit, this g going to gx, this is a set map, this map is clearly surjective and what are the fibres, fibres.

So that means if I take any element here ϕ, any gx, let call is my best phi and look at any element here gx, so what is phi inverse of gx, ϕ^{-1} of gx is precisely all those h and g, such that this h also goes to gx, hx equal to gx, this is same thing as g times Gx because rewriters this, this is equivalent to saying a multiplied by h from this side.

So x equal to $h^{-1}gx$ but this is equivalent to saying h inverse g belongs to Gx but this is equivalent to saying, you multiply by h, so you will get g belong to hGx, so I will correct here, this is not g but this is, equivalent to saying is correct. the two co-sets are equal, so this is Gx, h belongs to Gx, so this is G, so this is the co-set of the isotropy at G, this is given G, so therefore when I go, when I look at, so that will induce a bijection, so this induce, so the last.

(Refer Slide Time: 31:44)



Therefore we have a bijection G co-sets Gx through orbit this, this map is a simple, take any co-set Gx and map it to g times x. This is clearly a bijection that is what we have checked, by checking the fibres, so therefore in particular the cardinality of this, cardinality of this G mod Gx is same thing as cardinality of the orbit.

But this cardinality is also denoted by the index, these are the numbers of left co-sets, so the index of the stabiliser equal to the cardinality of the orbit, this is the cardinality of the orbit of x, stabiliser at x, so that is why it is called a orbit stabiliser theorem, this was done by a Lagrange and that is why the Lagrange theorem what will in an abstract group theory, the cardinality of x, the cardinality of the subgroup divides the cardinality of the group.

That is come from this because you can take h to be equal to the co-sets and then the h is operating on that and so on, we will continue our field theory study and then, we will start using the group actions right from the beginning. Thank you.