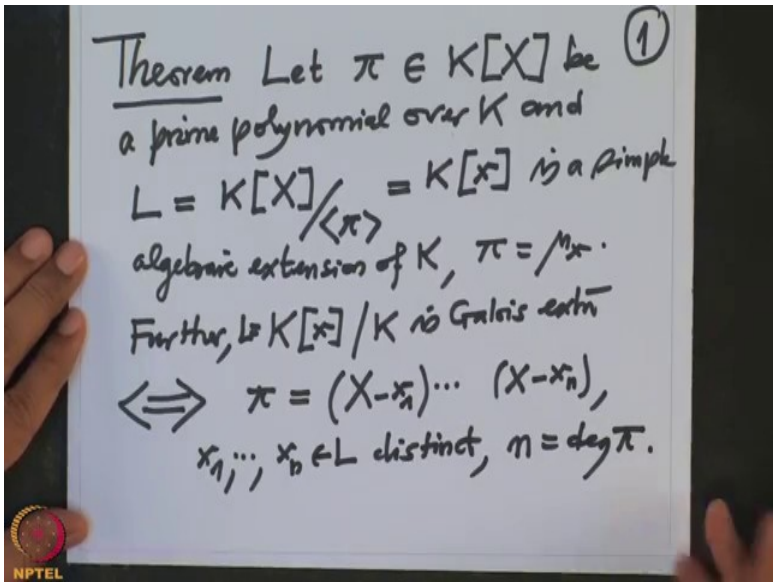
Galois' Theory
Professor Dilip P. Patil
Department of Mathematics,
Indian Institute of Science, Bangalore.
Lecture No. 27
Examples of Galois extension

In the last lecture, we have seen when can a simple field extension of a field which is algebraic is Galois, that is, if and only if the minimal polynomial of a generator splits into linear factors over L and simple linear factors.

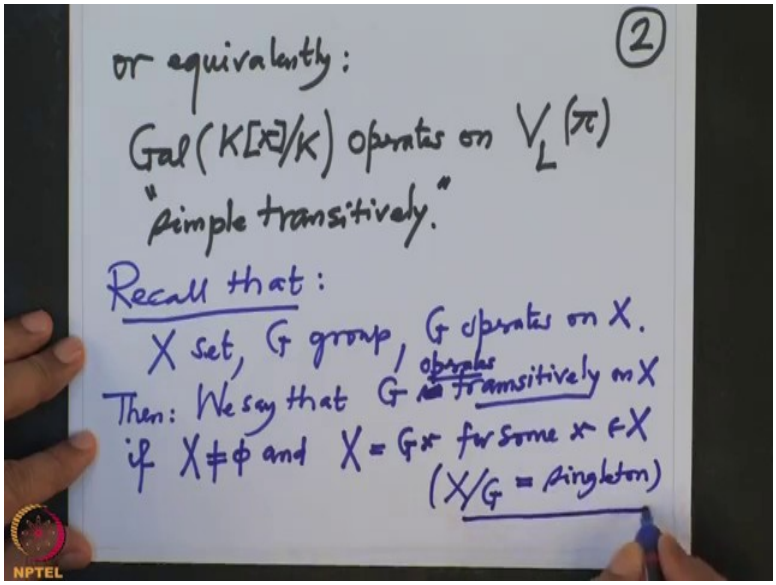
(Refer Slide Time: 0:52)



So let me record this in the form of theorem for the future use also this is very important observation, so I would write it as a theorem, so let pi be a prime polynomial over a field, be a prime polynomial over K and L equal to K X mod ideal generated by pi, then we know this is nothing but it is K x, where x is a image of the capital X and this is a simple algebraic extension of K, this pi is nothing but the minimal polynomial of x.

Further K x, K small x, which is L over K is Galois extension, if and only if, pi splits into linear factors and all this x1 to x n are elements in L distinct and this is n has to be the degree of pi, then only it can be Galois extension.

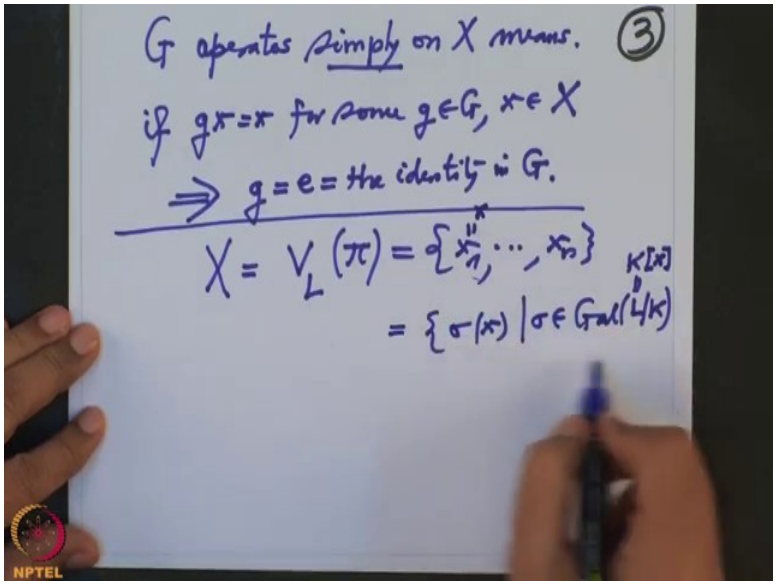
(Refer Slide Time: 3:03)



Okay, so this means what, this I want to rewrite in term of the group action, this means or equivalently the Galois group of K x over K operates on the zero set of pi in L, simply, “simple transitively” so these are the new words which we have to define for the group action, simple means, ohh first of all transitive mean there is only one orbit and simple means it is a free action that means there is no fixed, there is no isotropy.

So let us recall in general, so recall that, so in general, so X is a set, G is a group and supposed G operates on X. Okay, then we say that G is transitive or G operates transitively on X, if X is nonempty and exactly one orbit that means X, whole X is orbit of some element x for some X, once it is a orbit of one element, then it will be orbit of every element, so in other words the quotient space, so quotient space X mod G will be single term, so this also I should explain little bit more, but I will explain it after the definition of simple.

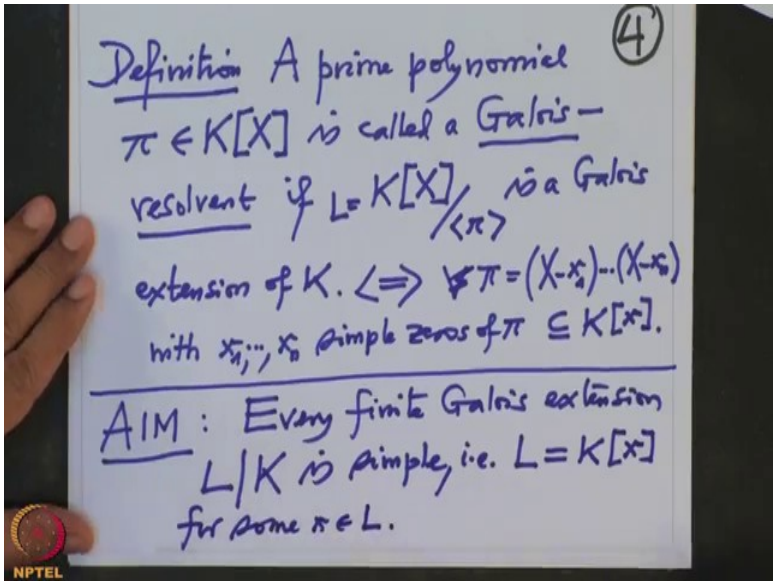
(Refer Slide Time: 5:46)



Simple means, so the transitive is defined, now we see that G operates, G acts, G operates simple, simply on X means if gx equal to x for some g in G, x in X, then this should imply g is identity e, the identity in G, so the set that G is operating in our case that X is our zero set V L of pi, this is x1 to Xn and then everytime, first of all the elements are related to each other by some G because it is transitive and then it is unique, so therefore as sigma varies, so this is same as sigma of x as sigma varies in the Galois group L over K, L is, remember L is a simple extension in K x and these x1 is x, so if I know x, I know the next one, I know the next one and all of them I know the sigma and they all are distinct, so therefore the order of this cardinality of this set will be cardinality of the Galois group.

So and which is the degree, therefore that is Galois extension, so that is, remember punchline to remember is the simple extension is Galois, if the Galois group operates on the zero set of the minimal polynomial of that generator in a simple transitive way.

(Refer Slide Time: 8:00)

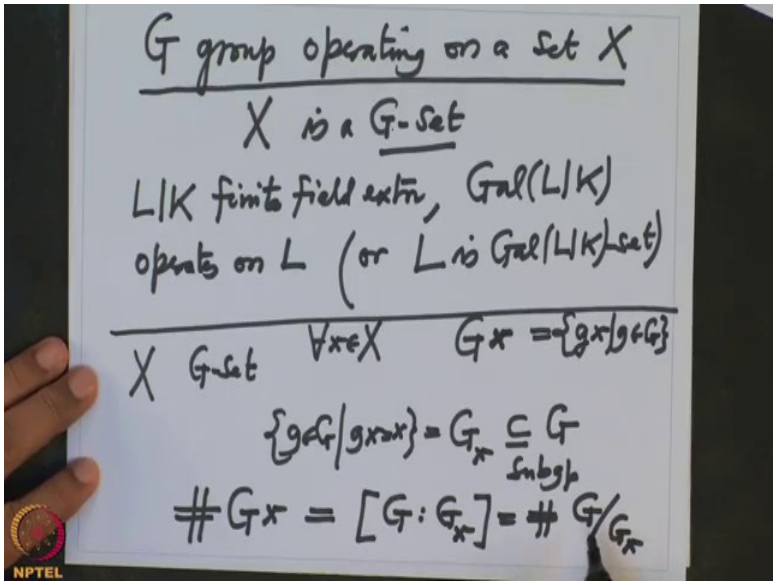


Okay, this also gives us another definition, it is a very important definition. Definition, okay, now this definition about the polynomial. A prime polynomial pi x, pi in K X is called a Galois resolvent, if K X modulo over ideal generated by pi, which is a field, is a Galois extension of K, no this is equivalent to saying that the Galois group of this operates simple transitively on pi, that means the zeros of pi are all here in this field L and they are different, and there are as many as the degree of pi, so that polynomial is called a Galois resolvent.

So Galois resolvent will give you Galois extensions and for example in a characteristic zero field, if you take any prime polynomial that always have different zeros because there is no repetition but this again I will repeat it, so we have lots of polynomials which has zero, which has simple zeros, so this is, let me write, this is equivalent to saying V, no this pi is the product of X1 minus x1, X minus xn, where with simple roots x1 to xn, simple roots, simple zeros of pi and all of them are contained in K small X, so that is the Galois resolvent.

So now I want to ultimately I will, we will prove that every, so this our gay, aim to prove. What is the next aim to prove? This is our next aim to prove that, every finite Galois extension L over K is simple, that is L is of the form K x for some x and then we will know how to test whether this is Galois or not because we just have to test on that minimal polynomial of X, whether it has a simple zeros and all zeros lies in L or not.

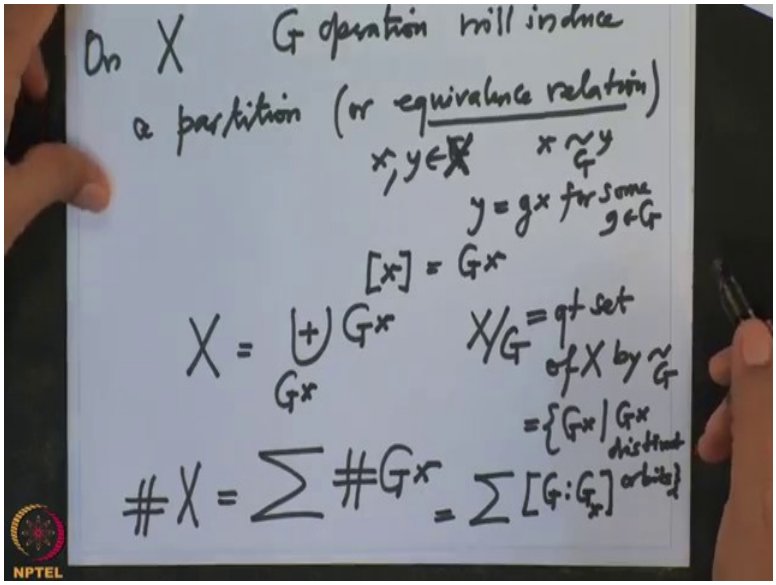
(Refer Slide Time: 11:37)



So the checking becomes simpler, whenever I have a group G operating on the set X, so first of all to write neatly, I want to introduce a notation, instead of writing such a long sentence, I will simply say X is a G set, that means X is some set, G is some group, and there is a operation of G on X, then I will call X to be a G set and we have seen our main example to study is whenever I have given a finite extension, finite field extension, then Gal L over K, this operates on L or in the newly introduced notation L is a Gal L over K set and then we have seen in general, this is what we want to study, this action.

So now just recall that whenever X is a G set, what all data we have attached to that for any x in x, we have the orbit, there all G multiples of x and we have the stabilisers, this is a subgroup of G, the one which do not move x, so these are all g in G, such that g x is x and these are all G multiples of X and we have also seen that the cardinality of the orbit equal to the index of the stabiliser, index is by definition, cardinality of the co sets of G x in G and we do not have to specify left or right because the number of left co sets is equal to number of right co sets, so this is very important orbit stabiliser theorem.

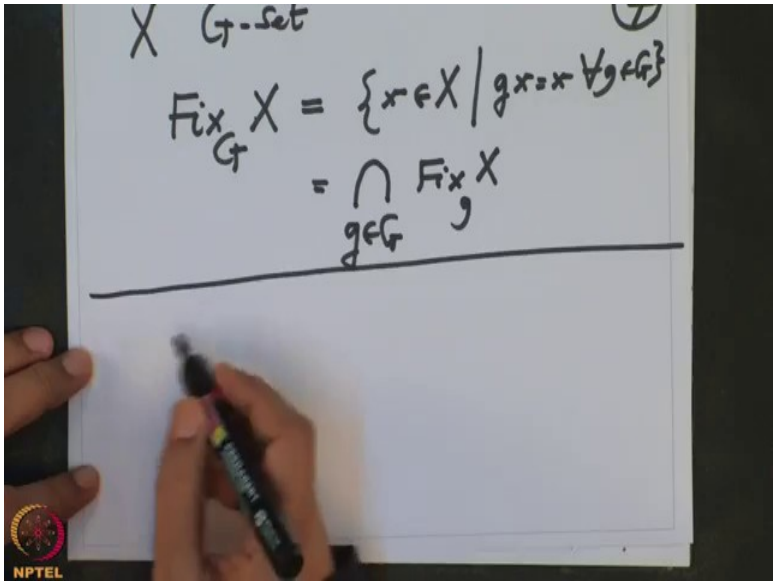
(Refer Slide Time: 14:15)



Okay, and remember also that this X is now, on X, these G operation will give a, will induce a partition or an equivalence relation, two elements of X, you call x and y, two elements of X, they say they are related by the action of G, if y equal to g x for some x, y equal to g of x, for some G, that means the equivalence class of x is nothing but the orbit of x and then, this will give you a partition of the set x and therefore X, we can write it as a Disjoint unions of the orbits, distinct orbits, so this orbits, we know because of the equivalence relation two orbits either they are equal or they are disjoint union and therefore here we are only taking those orbits which are distinct orbits, do not repeat here.

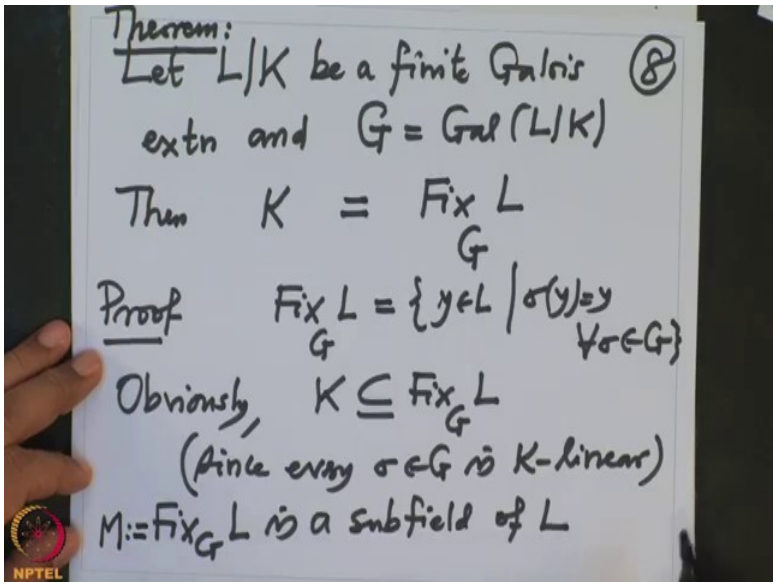
Another we have to say that, this orbit you take element, this union is running over the number of orbits, that is the quotient set, that is X mod G, this is the quotient set, quotient set of X by this relation, this equivalence relation we call it delta G, so this elements are orbits, distinct orbits G, X, distinct orbits, that is the thing, so then when you want to compute the cardinality effects, is therefore summation of the cardinality is of the orbits and this is running over only the quotient set and this orbits, you can also replace it by the indices of the isotropy, this is also the same things as summation G, Gx and only the distinct, only the elements x which is running in the set of orbits, so that is how the group operation, now if one wants to separate out the orbits which are singleton and which are non-singleton.

(Refer Slide Time: 17:23)



So but I do not need it now, but I definitely need the another invariant of the group action that is called, so suppose X is a G set, then I want to write what is fix elements of X under G, these are all elements of G, these are all elements of X, x in X such that X is fixed under every element of G, g x equal to x for every g in G, so in a notation wise if you want, this is intersection, intersection learning over in g in G, fix g X, these are all elements of X which are fix under these G and intersection means, so for all, so this is the fixed points of X under the G action on X.

(Refer Slide Time: 18:42)



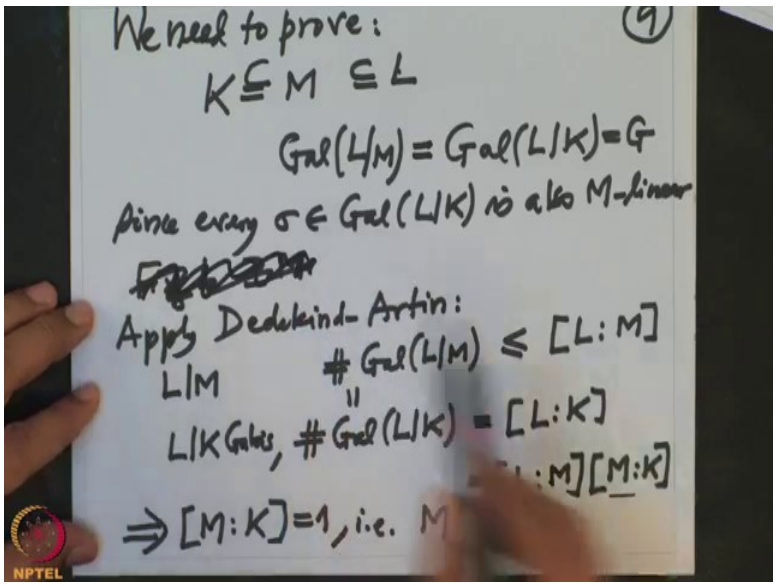
Okay, now first in our case, this is a first observation I want to now note is, so maybe I write on the next page, so I want to computer the fixed points of the Galois group action on the

bigger field N, so let L over K be a finite Galois extension and let us put G equal to Gal L over K, then K equal to, if I take the fixed points of L, G action on L, the fixed points are precisely the elements of K. Obviously, so let me write this as a theorem, this is a theorem, because we want to use it again and again.

So proof, so let us note down what is this fix G, L? These are all elements of L, all those y in L such that sigma y equal to y for all sigma in G that is the definition for the fix. So what are the sigma? Sigma is in G, sigmas are K linear maps, so sigma fixes every element of K, so obviously, K is contained in fix G L, this is obvious, since if you want, since every sigma in G is K linear, next thing note that, this fix G, L, this is a subfield of L, that is also clear because all that we have to check that is, if there are two elements, it is close under addition, subtraction, scalar multiplication, scalar multiplication you do not have to check, addition, subtraction and multiplication and the inverse.

But that is clear evident from the definition of the fix field because if y is fix, then y inverses also fix, you simply apply, take the inverses and because sigmas are the K algebra homomorphism, they will also preserve the inverses and so on, so this is also clear that, it is a subfield of L, let us call this subfield to be M and what is our problem? Our problem is to prove M equal to K.

(Refer Slide Time: 21:40)



So we need to prove K equal to M, alright this inclusion is obvious we have to check, now I want to prove these are equal, so let us look at the Galois group of, G wale Galois group of L over K, this is our G and what is relation between these Galois group and the Galois group of

L over M, this is contained in M, L, therefore, I can also consider the Galois group of L over these field M, so that is this, but if you will see somebody is M linear, then it is K linear also, so obviously this is contained here, but if somebody is K linear, that is also M linear because we know all elements of these are already fixes M, so therefore it is equality here, so since every sigma in Gal L over K is also M linear because it fix sigma L, this contains M or fix, so it is clear I do not write more, it is M linear because every element of Galois group fixes M, because that is a definition of the fix points of G action of L, G action on L, therefore it is, this equality is clear.

Now I want to apply Artin, Dedekind Artin, apply Dedekind Artin to this field extension L over M and what do I get, the cardinality of Gal L over M is smaller equal to degree L over M, but this cardinality is also same as, because there equality that cardinality of Gal L over K, but this again by Dedekind Artin to L over K, actually we know this is equality because we are assuming our extension is Galois extension, this is L over K, because this is Galois, therefore this equality, so this, but on other hand, M is a field in between, so this is also same thing as L over M times M over K, because the tower extension degrees are the product, so we have this equality is less equal to this, but it is already factor here, so that implies, this has to be one, so that implies M over K has to be one, it is one dimensional, M is one dimensional over K, but that means M equal to K.

So what do we have proved, we have proved that if you have a Galois extension and you take the fix points of that, then you do not get a bigger field than the base field that we started with, this is very important, this is infact one alternative definition of Galois extension, so then will later on we will collect what are the equivalent conditions for a field extension to be Galois extension, then this will be one of them and this also is one way to get rid of finite extension, because we have said that a finite extension is Galois.

If some equality holds but if you are extension is not finite and you still want to define it is a Galois extension, then you have no numbers, non integers involved with that, but we have fix field and a fix field should be a ground field and that could be one alternative definition but will have to prove the converses also true, so this is what we will do in due course and we will continue this next time, I will prove that every Galois extension is simple, therefore it will have primitive element and so on, so thank you we will continue next time.