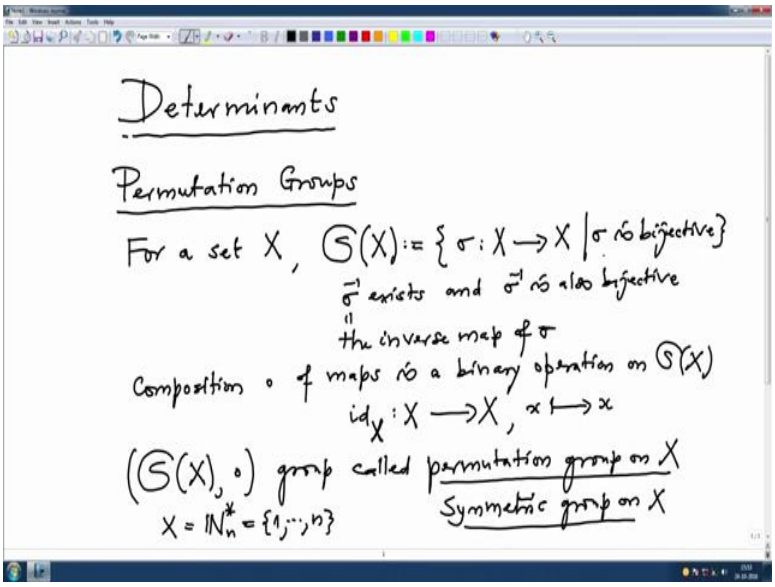
Linear Algebra
Prof. Dilip P Patil
Department of Mathematics
Indian Institute of Science, Bangalore

Lecture – 48
Permutation groups

Today in this lecture, we are going to start a new topic very important for computational purposes so called determinants.

(Refer Slide Time: 00:29)



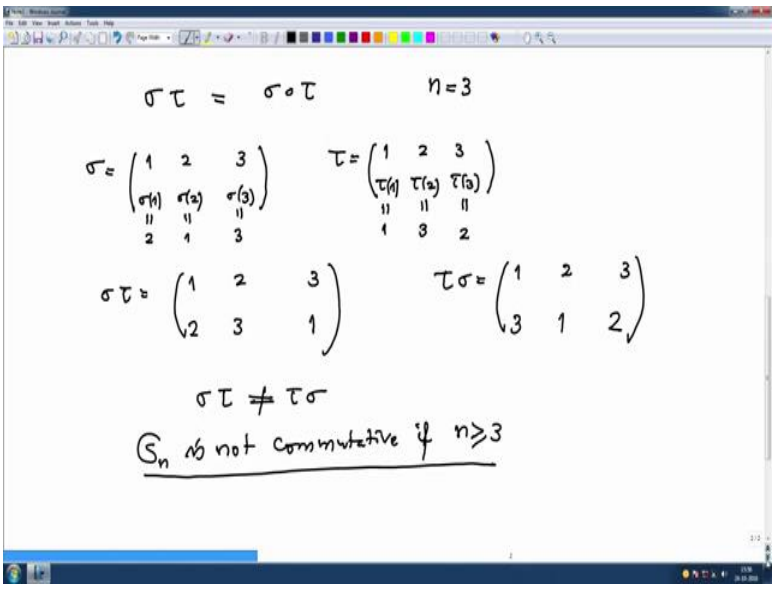
This will have several sections and for the sake of completeness I want to first discuss about permutations or rather I want to discuss permutation very important class of groups when one want to study finite group theory and we have to use this permutations especially some invariant attached to permutations in the theory of determinants that is a reason I want to do this topic more thoroughly.

So, let us introduce a notation in the beginning for a set X let us denote S X all bjective maps on X to X sigma is bijective, note that in sigma is bijective then sigma inverse exists sigma inverse exist and sigma inverse is also bijective sigma inverse is a inverse map of inverse map of sigma therefore, the set S X is close under inverses also it has a natural binary operation of composition of maps this of maps is a binary operation on S X and as we have seen several time that composition is such a natural operation that is

associative it has identity element namely the identity of the identity map of X this is the map X to X which map X to X every X to itself.

So, therefore, this S X under composition is a group this group called is called permutation group of X group on X also, it is called a symmetric group on X and we will be mainly interested in when X is a finite set namely. In fact, we will in a theory of determinants we will use this for X equal to n star n which is the set 1 to n and note the in the case of finite set X to check sigma is bijective you either have to check sigma is injective or surjective one of the checking is enough because of the pigeonhole principle once it is injective it will be bijective map from same set to say over this is only true for finite sets if it is not finite then there are bijective there are injective maps which are not bijective and so on that we will mainly concentrate on this. So, let me word about this notations.

(Refer Slide Time: 04:57)



For example very important thing which I want to bring it to your notice that I will simple write sigma tau for sigma composed tau and we will apply tau portion then sigma this is on this side which is again (Refer Time: 05:09) writing.

So, for example, if I have a permutation when n equal to 3 and if I have a permutation, I will write below one image of one that is sigma 1, this is sigma 2, this is sigma 3, this is a permutation sigma suppose I have another one which is I will call it tau which is 1, 2, 3, this is tau 1 tau 2 tau 3 I want to remove should how does one compose. So, let us take

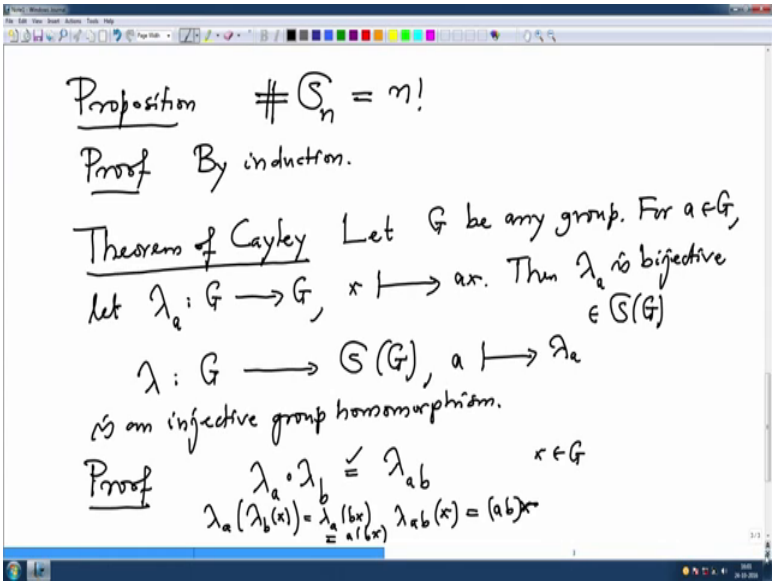
this is 2 1 and 3. So, note that when you want to control somebody's bijective or not you just have to look at the image row of sigma and take that all the entrees there are different.

So, this is 1 3 2; that means, under sigma 1 goes to 2, 2 goes to 1, 3 goes to 3 under tau 1 goes to 1 tau, 2 goes to 3, 3 goes to 2 and composition then sigma tau will be first you write down the first row that is 1 2 3 and start reading from tau one goes to 1 and then look at 1 goes to 2. So, 1 will go to 2 under composition 2 goes to 3, 3 goes to 3. So, 2 will go to 3 and we do not have to read, you do not have to check that you can check 2 goes to 3 goes to 2 and 3 goes to no 3 goes to 2 and 2 goes to 1. So, this is correct that is how one writes a composition.

Let us compute the other way also sigma tau; tau sigma so again 1 2 3. So, where do 1 go first you have to apply sigma now 1 goes to 2, 2 goes to 3. So, 1 goes to 3, 2 goes to 1, 1 goes to 1. So, 2 goes to 1, 3 goes to 3, 3 goes to 2. So, this is; and note that these 2 permutations are different because image of 1 is 2 image of 1 is 3 here. So, which obvious that sigma tau is not tau sigma.

So, from this, it is clear that the group S n is not a commutative if n is at least 3. So, so it is not commutative group. So, one as to be little careful with the group, so because they are Ablian in general another thing which I will note, but I will not prove it which is which is very well known so, but I would have written the proof in the notes.

(Refer Slide Time: 08:19)



So, let me write as a proposition cardinality of S n the group S n is n factorial proof I will just say that by induction I will not do the proof today, but ok.

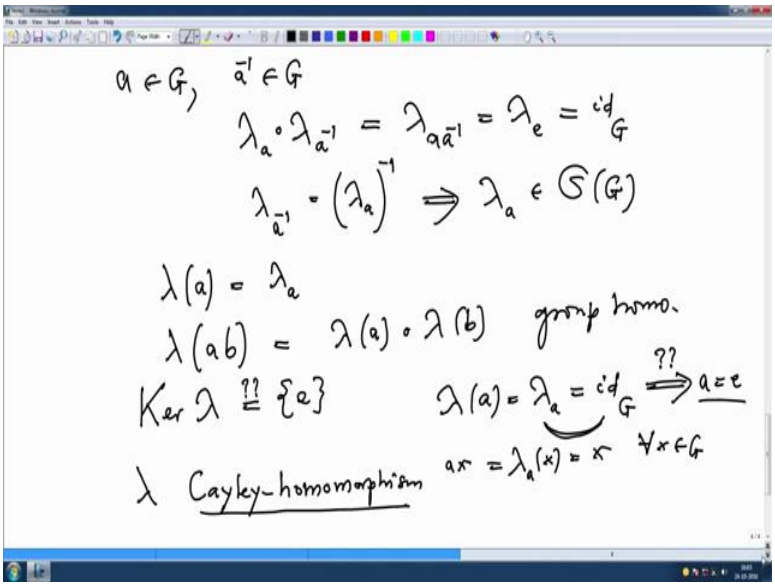
So, the most important consequence of this permutation group or definition is the theorem of Cayley that say the following let G be a group G be any group for any a in G let us let lambda a denote the multiplication on left by a; that means, any elements X in G goes to a X this is not a group of isomorphism, but it is definitely a bijective map then lambda a is actually is bijective so; that means, this lambda a actually is an elements of S of G permutations of G and then think of this lambda is a map from G to S of G.

So, this is a group under composition and this is a given group. So, this map a goes to lambda; a is an injective group in homomorphism. So, this is very important because suppose for a movement G or a finite group; that means, we have given a isomorphism of G on to its image in the permutation group. So, if one want to study anything about group finite group we might has we will study the permutation group. So, and all information about permutation groups what are the sub groups what are the orders of elements and so on.

So, the finite group theory will therefore, get reduce to study permutation groups. So, now, let us proof this, this is very easy to proof, first of all I have to proof that lambda a is bijective, but note if I take lambda a compose with lambda b this is nothing, but lambda suffix a b this is obvious because to check this equality I just try to evaluate on arbitrary elements of X both are maps on G to g. So, if I take any X in G and evaluate both the sides this is lambda a b on X which is a b X that multiplication by a b and this one is first lambda a of lambda b of x, but this is first inside things. So, that is lambda a of b X and this is a b x.

But you see it is a associative property of the group operation G therefore, this 2 maps are equal therefore, we have checked that this compose composition of lambda a and lambda b is lambda suffix a b.

(Refer Slide Time: 12:28)



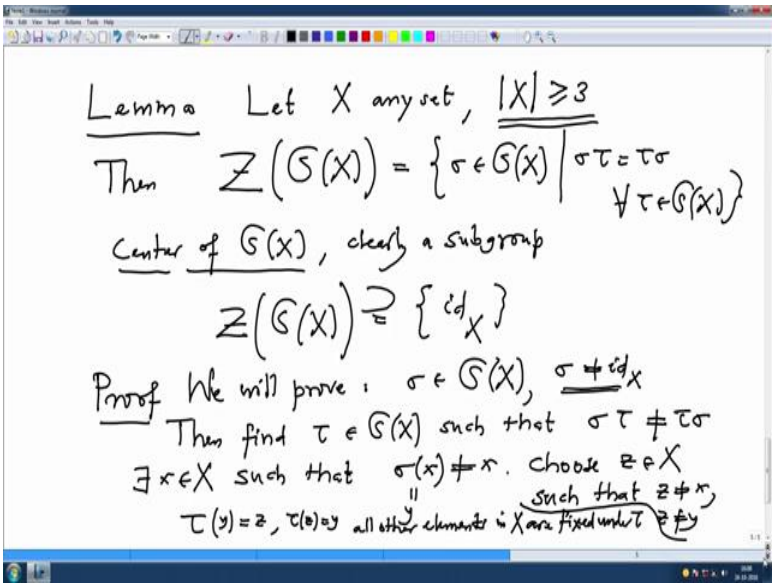
So, in particular in particular if I given any a in G we know that a inverse exist in G because it is a group. So, lambda a compose lambda a inverse this is nothing, but lambda a, a inverse which is lambda E, but lambda e is clearly identity map of G because e times suffix X or E every X. So, therefore, this lambda suffix a inverse is nothing, but lambda a inverse of the lambda a map.

So, that sure in particular that this lambda a map is a permutation now we have to check is a group homomorphism to check either a group homomorphism. So, we have this lambda of a it could be lambda suffix a. So, we have to check that lambda a b is same thing as lambda a compose lambda b, but this is what I have checked earlier so; that means, it is a group homomorphism this is a group homomorphism.

Now, I want to check it is injective. So, to check the map \ group homomorphism from a group one group to the other group to check it is injective we only have to check that kernel of that map is trivial you have to check this; that means, if lambda a which is lambda suffix a if this is identity map of G then from here I want to conclude that a is nothing, but the identity element, but that is this is equality. So, for every X it is equal so; that means, lambda a X equal to X for every X in g, but this is by definition a X this is to for every X. So, I can cancel X. So, I conclude a equal to identity cancellation is allowed because we are in a group.

So, that shows that this Cayley map; this lambda is also called Cayley homomorphism, Cayley was a English group theorist very important the same Cayley; Cayley Hamiltonian theorem in the same Cayley.

(Refer Slide Time: 15:19)



Now, the next one I want to check actually that the center of this group is this is the lemma, lemma is not using determinant, but those who want to do group theory finite group theory especially it will be very important for them. So, let X be any set group at least 3 elements cardinality X is at least 3 may not finite, but it should have at least 3 elements then the center of the group S X is what is the center by definition center by definition is all those permutations which commute with any other permutation sigma tau equal to tau sigma for all tau in S X.

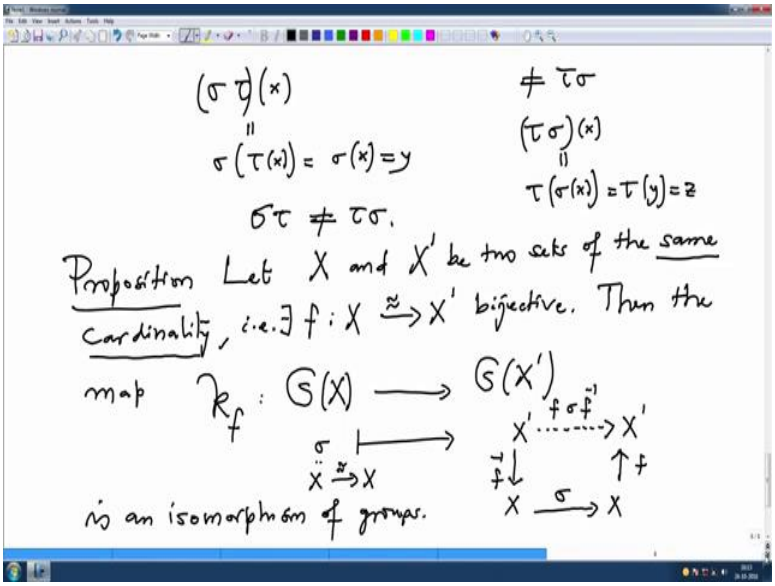
So, this is called a center of center of S X, it is clearly a sub group; a sub group because if sigma is there if sigma commutative to every tau. So, if you multiple this equation from the set by sigma inverse and that side by sigma; sigma inverse will also could commute and so on. So, it is a subgroup and the center I want to proof we want to proof that Z of S X is the trivial group; that means, the only element in the center is identity map identity map is; obviously, there is a inclusion is obvious. Now I will prove it you that if any other permutation belong to the center then it must be the identity. So, on or I will prove that. So, proof we will prove if sigma is in S X and sigma is not identity then I

will find then we will find an permutation tau such that sigma tau and tau sigma are different that will mean that sigma cannot belong to this center.

So, for that I will have to use cardinality the at least 3. So, sigma is not identity. So, therefore, we can find there exist X in X such that sigma of x is not X because it is not identity manner. So, at least at o next it will not be the same and let me call this sigma X as y and I have these 2 elements X and y in X, but X is at least cardinality 3. So, I will choice the third one. So, choose z in X such that z is different from X and z is also different from y then I will take tau to be I am looking for tau. So, I will tau to be equal to a permutation which maps y and z interchange. So, y goes to z and tau of z is y and every other all other elements are fixed all other elements in X are fixed under tau.

So, we get a permutation tau and now we just simple have to check that sigma tau is not tau sigma. So, let us check that.

(Refer Slide Time: 19:38)



So, I want to check that the sigma tau is not equal to tau sigma. So, let us evaluate these on X this is equal to sigma of tau X, but X is different from y and z. So, tau X is X. So, this is sigma of X which is y this is this slide lets us compute this slide that is tau sigma 1 X this is tau of sigma x, but that is tau of y, but tau of y is z. So, this side evaluated at X is answer is z this side evaluated at X answer is y and y is different from z.

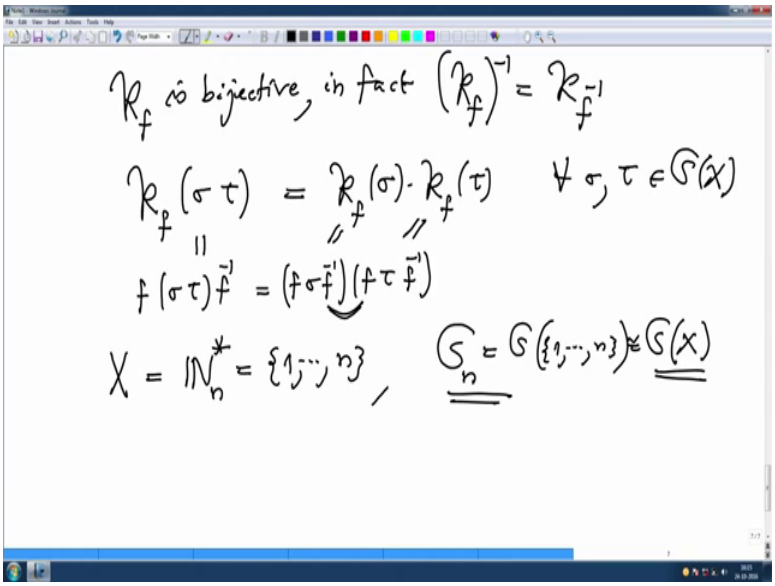
So, that shows that sigma tau is not tau sigma. So, we have group that the center of a permutation group is a trivial sub group now the next preposition shows that this permutation group does not depend on the set X it depends only on the cardinality x. So, let me write other preposition. So, suppose let X and X prime be 2 sets of the same cardinality may be finite may not be finite, but once when one says there. So, it have the same cardinality; that means, there exist a bijective map from one to the other bijective there exist f which is bijective and I will denote bijective map like this that is a meaning when we say 2 sides have the same cardinality then the map kappa f kappa f I am defining a map from the permutation group S X to the permutation group on X prime what is this map.

So, I have to map permutation straightaway go under this map. So, sigma this is a map from X t o X bijective map from X to X and I want to map it to a bijective map from X prime to X prime this is what I am looking for, but I know there is a f here which is bijective and then the inverse of f will be in the other direction f inverse and I have given this map this and I am looking for this. So, what do I do I wrote the other direction. So, let me correct here. So, this is from here I want to take f inverse followed by sigma and then follow back by f this is f is the other direction.

So, this is the map we were looking for let me draw it a dotted thing this is the map we were looking this is the map is this. So, first f inverse then sigma then f, so, this map is f inverse sigma f which is indeed a map from X prime to X prime, this is bijective this is bijective also this is bijective. So, composition of bijective is bijective . So, therefore, we indeed have a map from this S X to S X prime and this is a group isomorphism then the map is an isomorphism of groups. So, as are the groups structure is concerned the group structure does not depend on the set X it depends only on the cardinality X.

So, and this is just near checking. So, I will leave it to just check that it is a group homomorphism and check that it is bijective. So, bijective is also clear because I can actually gives the inverse map the; or let me say few words.

(Refer Slide Time: 24:31)



So, first of all kappa f is bijective. In fact, inverse of kappa f, I can we can write directly this is kappa suffix f inverse and also we have to check that kappa f of sigma tau equal to kappa f sigma times kappa f tau this is what you have to check for a every sigma tau in S X that will check that into the group homomorphism.

But see this is equal to what? By definition it is f sigma tau f inverse, but composition I can rearrange the bracket. So, this is same as sigma f sigma and I will write f inverse here and kill that by adding a f here, this is identity. So, it does not make and this one is this and this one is this. So, therefore, it respect the structure (Refer Time: 25:48), it is a group homomorphism its bijective already.

So, it is a group isomorphism. So, if one want to study these group the permutation group of X, it is enough that we can choose a set of that cardinality and that set X, I will choose n star n and we are our problem is to check study finite and in this case we will set to the notation S n equal to S of 1 to n which is S of isomorphism to S of X. So, if I want to study this I will study this now I want to study what are the what are the elements what are their orders what how do find their inverses and so on. So, this we will do it after the break.