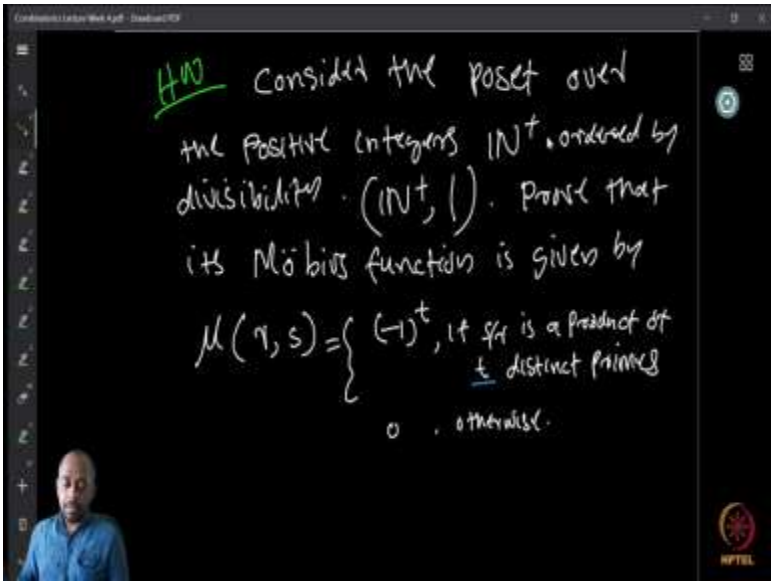
Combinatorics
Professor Doctor Narayanan N
Department of Mathematics
Indian Institute of Technology, Madras
Product Theorem and applications of Mobius Inversion

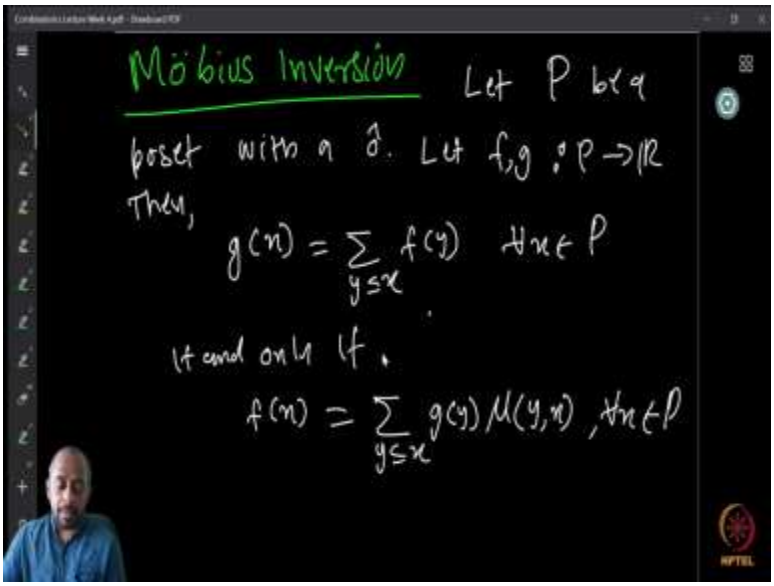
(Refer Slide Time: 00:15)



Now as a homework this is very important that you do this. Consider the poset over the positive integers $\mathbb{N}^+$ ordered by the divisibility relation $(\mathbb{N}^+, |)$. And we looked at a small subset of this earlier. Now prove that its Mobius function is given by, $\mu(r,s) = (-1)^t$, if the number $\frac{s}{r}$ is a product of t distinct primes.

So t must be precisely the product of t distinct primes, it cannot have like a prime square, for example. So in other cases $\mu(r,s) = 0$, so if $\frac{s}{r}$ is containing a prime power, for example, then this will be 0, but otherwise it is going to be $(-1)^t$, where we have exactly t distinct primes. Now, so this is your homework.

(Refer Slide Time: 01:41)

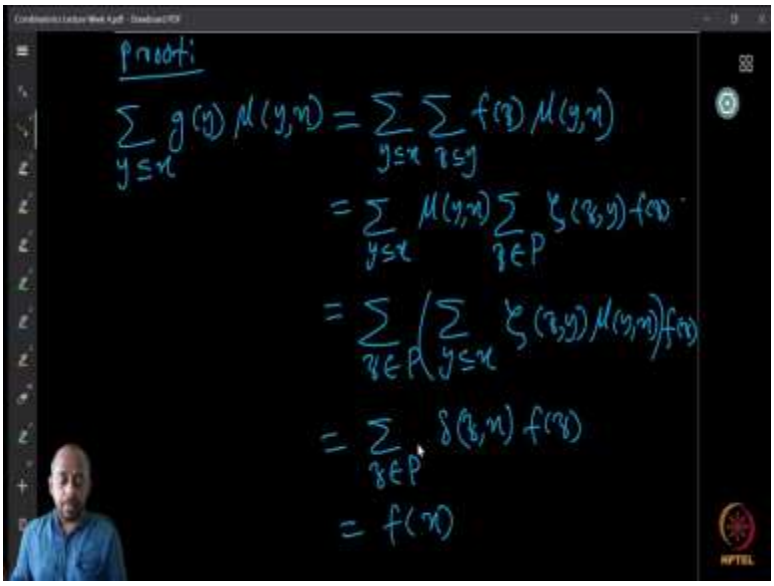


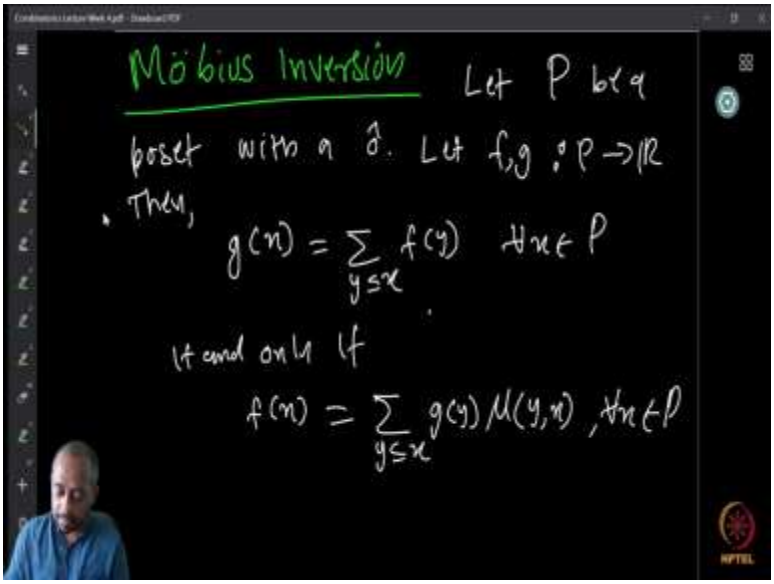
Now, we look at what we wanted to look in this section which is the Mobius inversion. So let P be a poset with a $\hat{0}$. So, if you remember $\hat{0}$ we defined in the previous lecture. So, you know, so this actually simplified a statement, in fact, one can make it little more general. So, what we really need is that the poset should have all its primary principle order ideals to be finite.

So, what is the principle order ideal? I am not going to write the definition, but to be brief, so if you take an element all elements which is less than or equal to this must be also in the ideal so that is an order ideal. And so a principal order ideal is the order ideal generated by a single element, so all its principal order ideals are finite then we can do the same proof it will work.

The main idea is that like when you telescope the sum it should stop at some, and if you are considering finite posets it is basically equivalent to the same statement because you can always add a $\hat{0}$ and then make it equivalent to this. But for our purpose this is good enough. So, now let f and g be real valued functions on P, then $g(x) = \sum_{y \le x} f(y)$, for every x in P if and only if $f(x) = \sum_{y \le x} g(y)\mu(y,x)$, for every x in P, where μ is the Mobius function of the poset P. So, this is called Mobius inversion. So, it says that this f and g are functions from P to $\mathbb{R}$ or in fact P to $\mathbb{C}$ also works well, if and only if, whenever g is expressed as a sum of f this way, f is expressed as a sum in this way. So this result is called Mobius inversion and this is quite easy to prove.

(Refer Slide Time: 04:50)





So, what we do is we just use the definition of the convolution product and then just work out the details. So just look at this, so $\sum_{y \le x} g(y)\mu(y,x)$. Now, what is that? This is, so that is what is given here. So, we want to show that this is actually $f(x)$. So g is given this way, we are going to show that this is precisely what is, so we will start with on the hand side and then work it out.

So by the definition of the product $g.\mu$ is defined as $\sum_{y \le x} \sum_{z \le y} g(y)\mu(y,x)$ because, I can write $g(x)$ in this way. Now this is basically $\sum_{y \le x} \mu(y,x) \sum_{z \in P} \zeta(z,y) f(z)$, so this is where the magic happens.

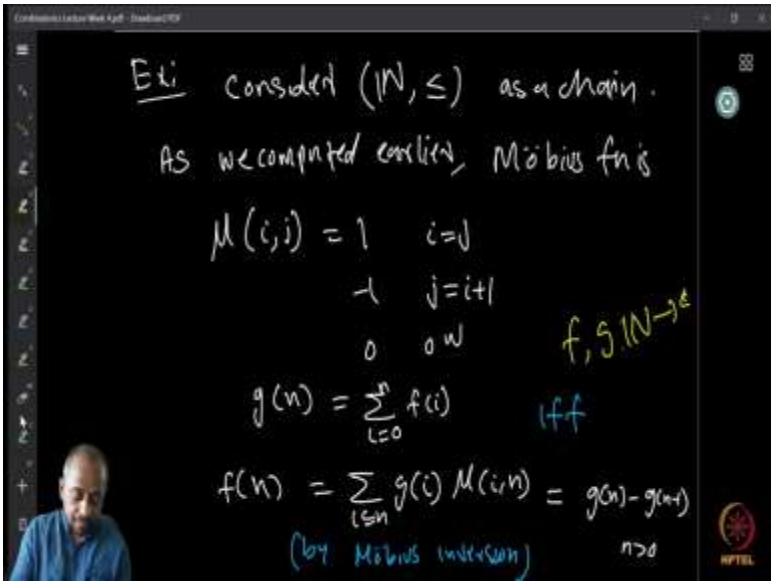
So we use the zeta function here because zeta function as we observed before is one precisely when a set is in the interval that we want otherwise it is going to be 0. So therefore, I can just add zeta here to do this. Now, I can do a reordering of the summation. So changing the order of the summation this I can write as $\sum_{z\in P}(\sum_{z\leq y}\zeta(z,y)\mu(x,y))f(z)$.

But this one is in the convolution product and zeta and mu are inverses of each other, so therefore this becomes delta. So, therefore this is basically $\delta(z,x)$. And so we get $\sum_{z\in P}\delta(z,x)f(z)$

But delta function is precisely 1 when z is equal to x and otherwise it is 0, so therefore the only one time which survives is when z is actually equal to x.

So therefore, this is actually equal to $f(x)$ and that is precisely what we wanted to prove. So, since all these steps are reversible we, so we get this identity.

(Refer Slide Time: 07:45)



So, how to use the Mobius inversion? So, here is some example. So consider the example that we looked at the natural numbers with the usual order which is a chain. Now in the previous example that we looked at for computing the Mobius function we only looked at a small subset of n, 1 to n, but one can see that because of the telescoping property that we observed it works for all the n.

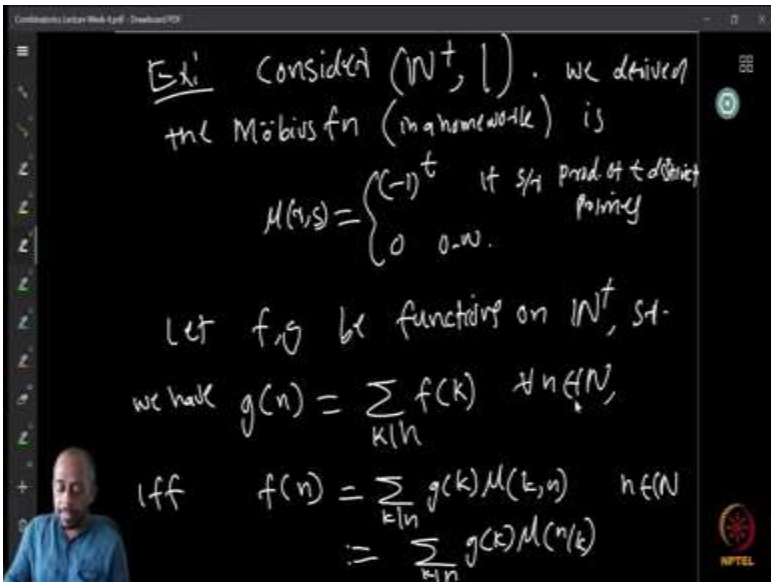
So therefore the Mobius function of this poset is also given by $\mu(i,j) = 1$ when $i = j$ and is equal to -1 when $j = i + 1$ and 0 otherwise. So once you have the Mobius function let us take two

functions, let us say g and f both from. So, whenever we are going to look at the functions it must be from poset to real numbers or like complex numbers something like that.

So, therefore we look at two such functions, so let us say that $g(n) = \sum_{i=0}^{n} f(i)$. So, this is an example that we looked at before, but now we see it in this avatar, where $g(n) = \sum_{i=0}^{n} f(i)$, f is also a function over the integers g is also function over the integers. Now this is if and only if, of course, $f(n)$ is equal to, by the Mobius inversion formula, $f(n) = \sum_{i \leq n} g(i)\mu(i, n)$

Now, what is this? $\mu(i, n)$ is precisely 1 when i equal to j and precisely minus 1 when j is equal to i plus 1 and everywhere else it is 0. So, therefore you will see that this is actually equal to $g(n) - g(n-1)$ and this explains our earlier observation of the same thing why it should be this way, so this is also because of the Mobius inversion formula.

(Refer Slide Time: 10:30)



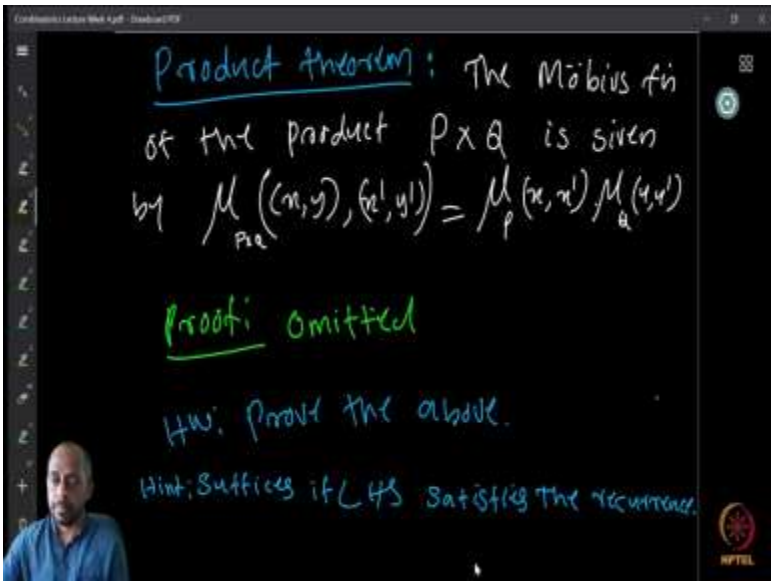
Another example, we can look at the positive natural numbers $\mathbb{N}^+$ together with the divisibility order. So again I asked you to derive the Mobius function of this, if you have done that you would have found out that $\mu(r, s)$ is equal to $(-1)^t$ if $\frac{s}{r}$ is the product of t distinct primes and otherwise it is 0.

So assuming that you have computed this we can now continue. So, now let f and g be functions defined over $\mathbb{N}^+$ such that let us say $g(n) = \sum_{k|n} f(k)$ for every n in $\mathbb{N}$. So $g(n)$ is sum overall the devisors $f(k)$. Then Mobius inversion says that f(n) is given by summation $f(n) = \sum_{k|n} g(k)\,\mu(k, n)$, that is the definition of Mobius inversion.

Now suppose, so if you look at $\mu(r, s)$, it only depend on what is s/r. So, I can instead make it a one variable function by saying that $\mu\left(\frac{s}{r}\right) = \mu(r, s)$. So the Mobius function can be written in just one variable in this case. And therefore, let me write it as $\mu(s/r)$ here, so therefore I get $\mu(n/k)$.

So, therefore I get $f(n) = \sum_{k|n} g(k)\,\mu(n/k)$. And this is precisely the classical Mobius inversion formula from number theory. In fact, this is probably the reason the name Mobius inversion stuck to this technique that is a generalization of the classical Mobius inversion.

(Refer Slide Time: 13:14)

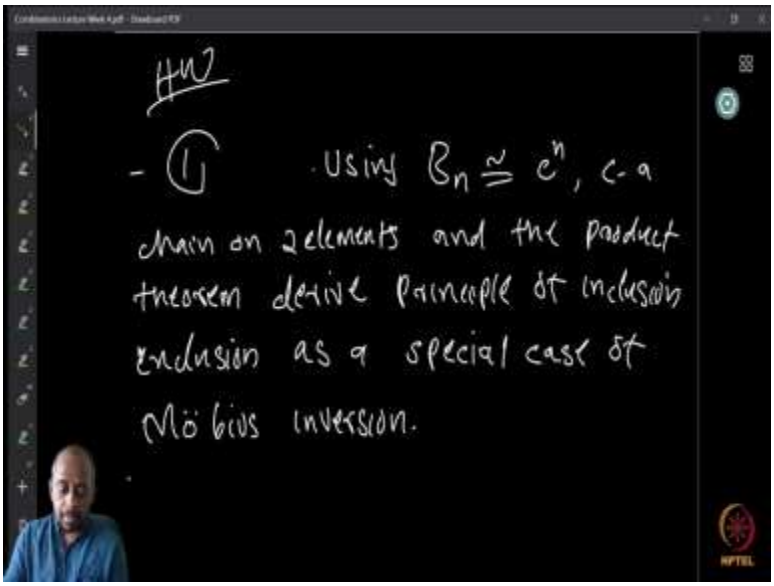


Now we look at the product theorem. So, we defined the product of two posets earlier. So consider the Cartesian product of posets P and Q. So, the product theorem says that the Mobius function of the product P × Q is given by the product of the Mobius functions. So, Mobius function of the product $\mu_{P\times Q}\big((x,y),(x',y')\big) = \mu_P(x,x')\mu_Q(y,y')$.

So, the proof, I am omitting the proof here, it is very easy actually but I can give it as a homework, so prove this above and there are several ways of proving this. So, one is by showing that, so to show that this is indeed the product, you just need to show that it satisfies the recurrence or another proof method is by expanding this we know what is this product, what is this with respect to the definition.

We know what is the definition of this and this as summation and then you take the product of this and compare the coefficients and show that they are also the same. So there are there are many ways of doing this. So I am omitting the proof but you can understand how many different proofs you can have and this is very useful .

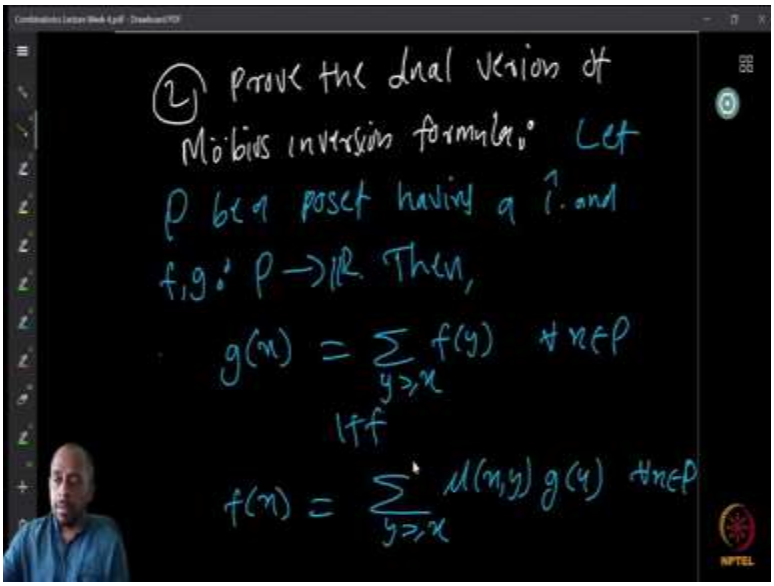
(Refer Slide Time: 15:08)



So, how to use this? Well, again I will give you this as a homework so we already asked you to prove that the Bernoulli poset Bn is isomorphic to the nth power of a chain on two elements. So where c is the chain of two elements Bn is isomorphic to the product of a chain of two elements with itself n times. Now, because of this property we can use now the product theorem.

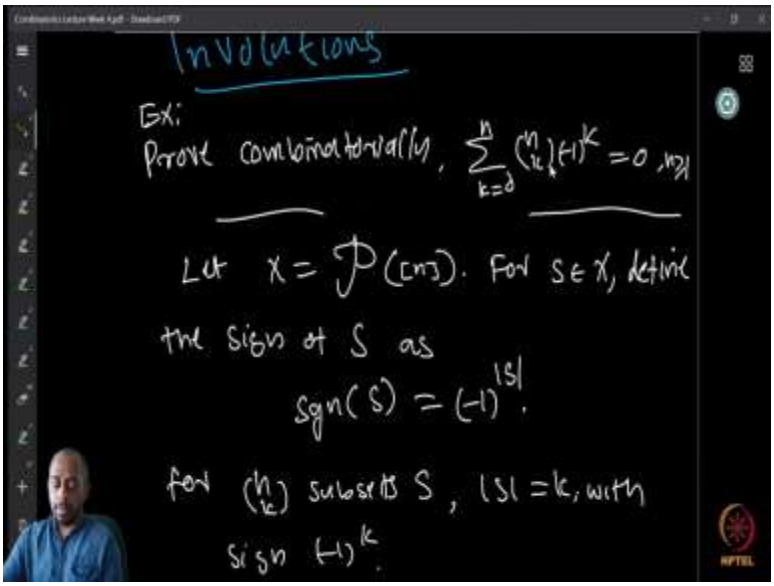
So, if you know how to compute the Mobius function of this then you can also compute the Mobius function of the Bn by the product theorem. So, now first use this to find the Mobius function of Bn, show that like it is indeed the one that we discussed and then connect it with the principle of inclusion and exclusion and derive it as a special case of Mobius inversion. So, Mobius inversion is a special case of, I mean, principle of inclusion and exclusion is a very specific case of Mobius inversion. So, you can prove this again by using this product theorem.

(Refer Slide Time: 16:35)



Another home work is to prove the dual version of Mobius inversion formula that is suppose the P is a poset having a $\hat{1}$, so in the first case we say that P has a $\hat{0}$. And then f and g are functions defined over P which are real valued functions then again $g(x) = \sum_{y \geq x} f(y)$ if and only if $f(x) = \sum_{y \geq x} \mu(x, y) g(y)$. So, just note the order and also there is a $\hat{1}$ here it is different from $\hat{0}$ and then work out the details similarly. So, this is called a dual version of the Mobius inversion formula.

(Refer Slide Time: 17:39)

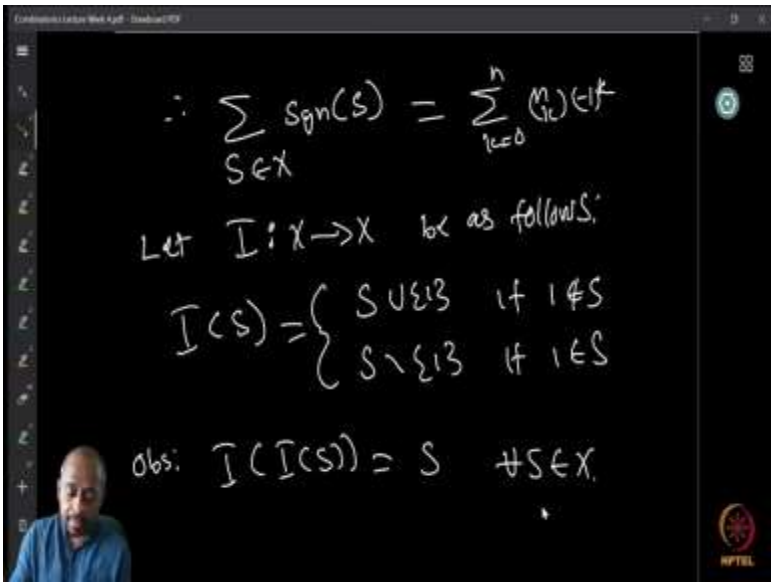


Now, I want to wind up with a slightly different topic called involutions. I will, it is a very-very brief introduction to involutions. We just look at a single example and then we formally define it and then that is it. So, let us look at an example. Suppose, you are asked to prove this something which you already done, prove combinatorially $\sum_{k=0}^{n}\binom{n}{k}(-1)^k$.

Now we already have seen a couple of proofs of this but now I want to prove this using let us say involution. So what is involution I will define soon but for the time being let us just look at the proof. So, let me denote by X the power set of the set one to n which is the base set of the Bernoulli poset. So, let us look at the set X and then you take any subset of 1 to n and then define the $sgn(S) = (-1)^{|S|}$.

So the sign of the set is minus 1 whole raised to its cardinality, so this I can define for every subset of 1 to n or every element of the power set. Now for any k, n choose k subsets S of the set 1 to n has cardinality k that is by the definition of n choose k that is what we call n choose k. And therefore, all of them has sign $(-1)^k$ because cardinality of S is k so we have n choose k subsets with the sign minus 1 raised to k.

(Refer Slide Time: 20:01)



So what I can write the sum that we are looking at as

$$\sum_{S \in X} sgn(S) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k$$

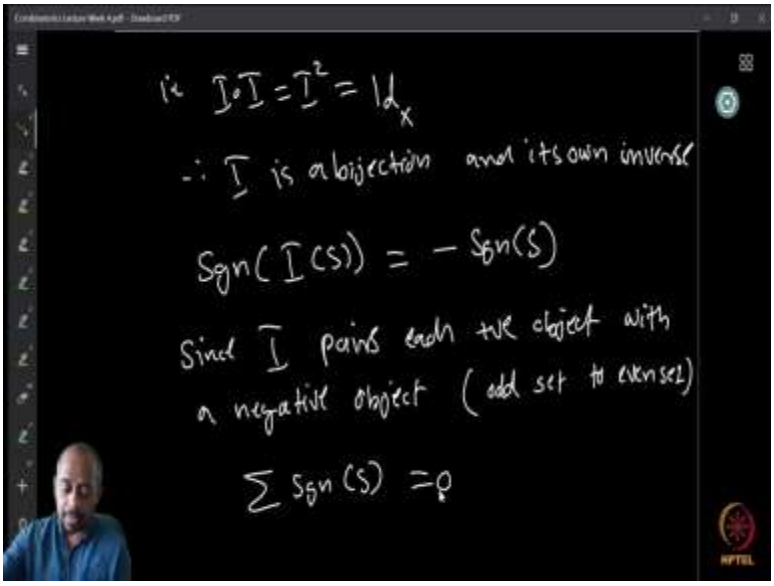
Now, let us define a function $I: X \rightarrow X$ as follows. So, the function I takes S, thus S is the subset of 1 to n.

$$I(S) = \begin{cases} S \cup \{1\}, if\ 1 \notin S \\ S - \{1\}, if\ 1 \in S \end{cases}$$

So, I of S takes the set S to S union singleton 1, if 1 is not in S. So, if the element one is not in the set S, then I add it, I just add it to S. On the other hand, suppose S contains one, then I just remove it from S, so it is S minus singleton one. So, I takes S to S union one if one is not in S and it will take S to S minus singleton 1, if one is actually in S.

So, we can observe that I is its own inverse, that is $I\big(I(S)\big) = S$. If I(S) is this form then I am going to add it back and then I know, the next step I(I(S)), if it is this form, I am going to remove it. So in whichever case I will get $I\big(I(S)\big) = S$. So therefore I is its own inverse and I square is equal to identity, that is $I.I = I^2 = I$

(Refer Slide Time: 21:52)

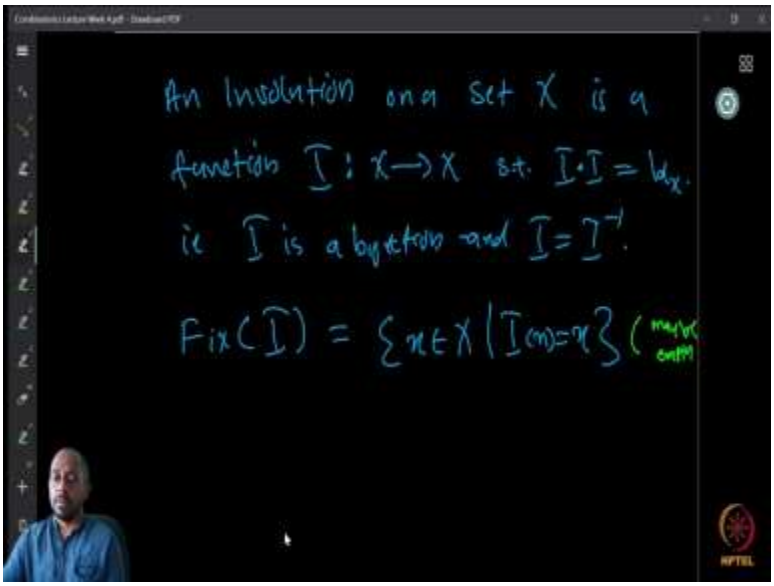


So, I·I is the identity of X. So I is a bijection because I square is identity, I is a bijection and of course again it is on inverse. Now, what is the sign of I of S? Well, because S takes elements from whatever is cardinality either its cardinality minus 1 or its cardinality plus 1. I am going to either add or subtract exactly one element.

So this will be minus sign of S because minus 1 raised to the cardinality is different and I pairs each positive object with a negative object because that is what I does. That is $sgn(I(S)) = -sgn(S)$

So if this was of sign positive then it is going to set with the negative sign because the cardinality, the parity of the cardinality changes. So therefore, $\sum sgn(S) = 0$, if you take all S in X, sign of S is equal to 0. So and that is precisely what we had here, so that is precisely this thing. So, therefore by this observation that we have shown that it is 0. So, this is a proof using the idea of involution.

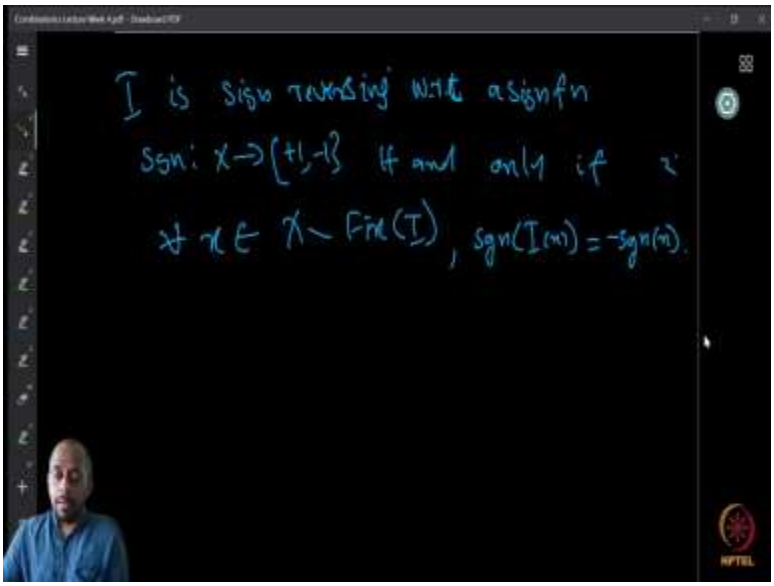
(Refer Slide Time: 23:33)



So, what is involution? So, an involution on a set X is a function that maps from X to itself such that its square is the identity which means that I is a bijection and I is its own inverse. Now, if you take an involution I call $Fix(I)$ as the set of all elements that is not unchanged under I, that is $Fix(I) = \{x \in X \mid I(x) = x\}$.

So this set may be empty, because I can change, for example, in the previous case we saw that this set is actually empty, because, we may take all the odd sets to even sets and even sets to odd sets, so therefore there is no element that is fixed. The $Fix(I)$ can be the empty set also.

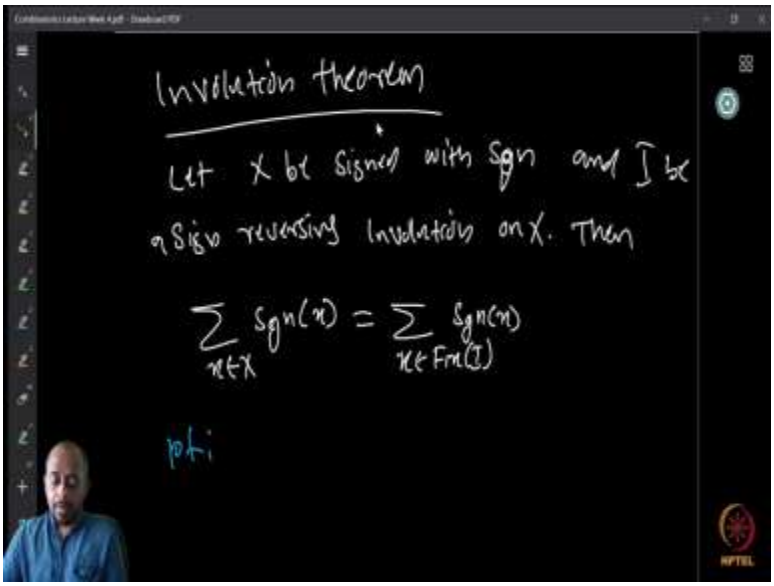
(Refer Slide Time: 24:33)



Now I is a sign reversing involution with respect to a sign function sgn, let us say that the sign function $sgn : X \to \{1, -1\}$. So I is sign reversing if and only if for all the elements that are not fixed by I, the sign actually changes. So for all $x \in X - Fix(I)$, $sgn(I(x)) = -sgn(x)$) So, of course, the fixed elements will not change the sign.

But the sign function is already fixed, we are not going to change the sign function. We are only looking at what happens to the elements after the image under the image. So if $sgn(I(x)) = -sgn(x)$) for every $x \in X - Fix(I)$, those elements that are not fixed by I, then I say I is a sign reversing involution.

(Refer Slide Time: 25:42)

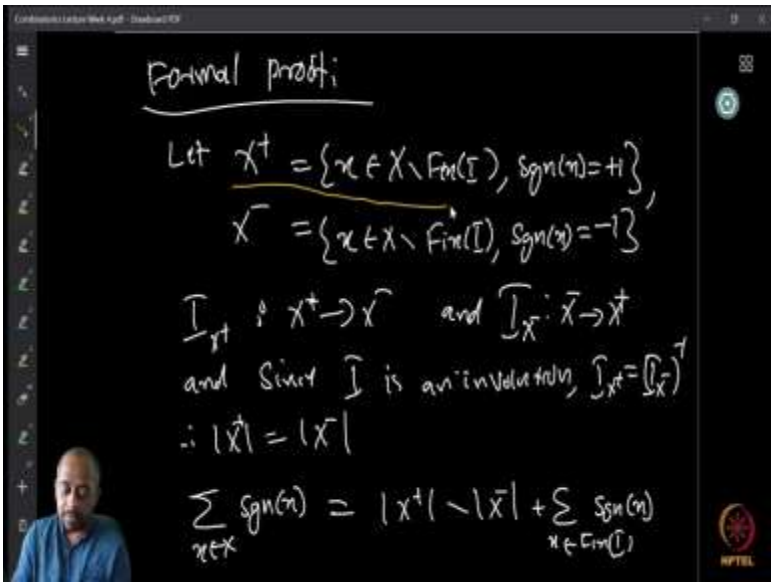


And then we have the involution theorem so what is the evolution theorem that let us say that X be a set which is signed with the function sgn and I be a sign reversing involution on X with respect to the function sgn. Then $\sum_{x \in X} sgn(x) = \sum_{x \in Fix(I)} sgn(x)$. So this is the evolution theorem.

And this is quite useful, you will see in your homeworks and the proof is almost trivial. So, just looking at it we can see that why this should be the case because if you look at all the elements that are not fixed by I. So I basically takes the elements that are not fixed and changes the sign and because the square, I applied again will get back in that it is a bijection.

So we can see that the number of elements that has the plus sign must be equal to the number of elements that has the minus sign and therefore they will cancel out and those are the guys which are outside the $Fix(I)$. So therefore, everything else will be added to 0 and therefore the remaining things will be those elements in $Fix(I)$ with its own sign, so that is the idea, so that is an informal proof. Now, if you want to formally prove this we can also do that.

(Refer Slide Time: 27:45)

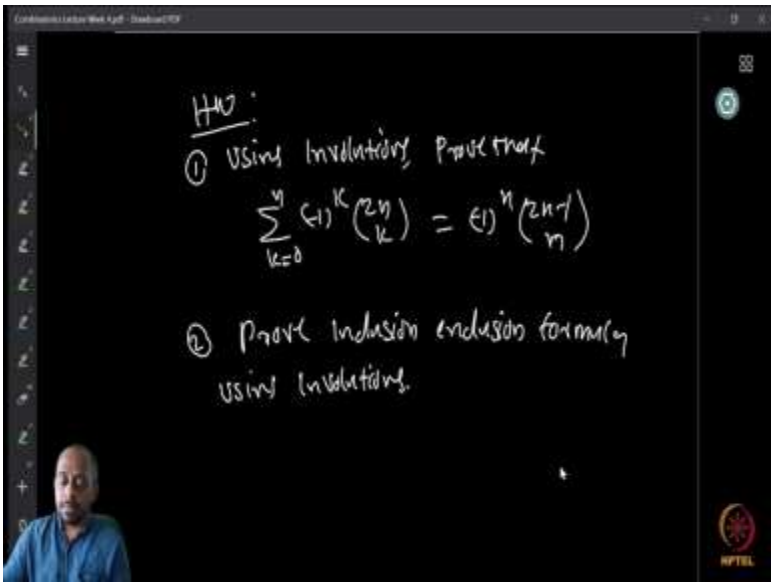


So, just by defining these things so let us say that X^+ is the set of all elements in not fixed by I whose sign is plus 1, and X^- is those elements not fixed by I whose sign is minus 1. Then the involution I restricted to X^+, I_{X^+} is something which takes X^+ to X^-. And then convolution restricted to X^-, I_{X^-} takes X^- to X^+.

Now we know that I is an involution therefore it is a bijection. So, therefore I_{X^+} must be $(I_{X^-})^{-1}$ and similarly vice versa. And therefore because this is the bijection we know that , the function going from X^+ to X^- is the bijection, their cardinalities must be the same.

And therefore $\sum_{x \in X} sgn(x) = |X^+| - |X^-| + \sum_{x \in Fix(I)} sgn(x)$

(Refer Slide Time: 29:16)



So here is a couple of home works, using involutions prove that this identity, binomial identity

$\sum_{k=0}^{n}(-1)^k\binom{2n}{k} = (-1)^n\binom{2n-1}{n}$. Again you can think of proofs using involutions you can think of proofs without using involutions combinatorial proof again.

And you can also look at algebraic proofs. So you have three different ways of proofs you can think of it. But in this homework you should do this. Then as we mentioned, no I did not mention this maybe; you can also prove inclusion explosion formula using involutions. So give a proof of inclusion explosion formula using involutions. I think with that we will stop for today and see you next week.