NPTEL
NPTEL ONLINE COURSE
INTRODUCTION TO ABSTRACT GROUP THEORY
Module 07
Lecture 36 – "Counting Formula"
PROF. KRISHNA HANUMANTHU
CHENNAI MATHEMATICAL INSTITUTE

Now let us now come to how these two are related.
(Refer Slide Time: 00:28)

This is an important theorem. So let us say G is a group, always this is our set-up in these videos, G is a group and S is a set, G acts on S, okay. So, then in this situation there exist a bijective function φ: G mod the stabilizer to, okay, fix, let a small element s be taken in capital S, okay let me repeat the theorem. G is an arbitrary group acting on an arbitrary set S and let us fix an element of the set, small s, so s is an element of S, then there exists a bijective function between orbit of s and G mod Gs, and what is G mod Gs, G is a group, Gs is a subgroup, so G mod Gs is simply the set of left cosets of Gs in G. I must remark here that this is not a group because Gs is not necessarily a normal subgroup okay, so this is just a warning to you that, when I write G mod Gs, typically used only when you have a normal subgroup, and you consider the quotient group, but here I am using the notation for convenience, to denote the left cosets of this subgroup in this group, so in this theorem, you only think of G mod Gs as a set of left cosets. So the proof is not difficult at all.

Okay, with all the set-up that we have so far, so G mod Gs, there is a bijective map from G mod Gs to Os, so, and actually define, this should also be part of the theorem, define φ of, what is a left coset, it is of the form gGs, G mod Gs is the set of left cosets, so it is g times Gs, define this to be gs, this is of course in the orbit. So what is the function? It is taking a left coset which by definition is o f the form gGs and I will map it to the element gs which is in the orbit.

So we have to check first of all that it is a well defined map, because a left coset can have several representations with a different g here, okay, so φ first we must check is well defined. φ is well defined, so why is that? Suppose gGs = hGs, we must ensure that φ(g) = φ(h), that is, we need to check gs = hs, this obviously needs to be checked, because we are trying to define that image of gGs is gs, but it can very well happen that gGs=hGs, but g and h are different because several cosets will coincide right.

But then if gGs is equal to hGs, but gs is different from hs, then there is a problem, the function is not well defined, so we need to check this.
(Refer Slide Time: 5:52)

But this is not difficult at all, if you start working this out, it will be clear, so if gGs is equal to hGs then what do we have, this implies that g = hg prime, for some g prime in Gs, right this is clear to you right, if you have left cosets are equal, then I am going to quickly work this out, so in general if you have G is a group H a subgroup, if you have g1(H) equals g2(H), remember g1 belongs to g1(H) because g1(H) is the set of g1 times every element of capital H.

So, in particular g1 times identity will be one of the elements of g1(H), which I am assuming is equal to g2(H) so g1 belongs to g2(H), so g1= g2 times h for some h in H.

I am using the same idea here, so gGs=hGs, so g must be something h times some in Gs, right. Now this implies, if I do gs, now let's apply, bring in the set here, the element s here, gs equals h(g prime)s, because g is equal to h(g prime), but the group action property says that h(g prime)s is equal to h(g prime s), but g prime remember, where is g prime? g prime is in the stabilizer.

Since g prime is in the stabilizer, what is the stabilizer means, that is all elements in G that fix s, so g prime is an element of the stabilizer means g prime fixes s, so g prime s = s, so h(g prime s) is just hs. So we have concluded that g s equal to h s as required, so if two left cosets gs and hs as required, so there will be no problem you can choose one representative and I can choose another representative, and we apply both the function φ, we both get the same answer. So gs = hs, so that is good. So φ is well-defined.

(Refer Slide Time: 8:09)

Now we are trying to say that φ is a bijection, so φ is well-defined is all well and good, but we want to check that it is 1-1 and onto. Why is it 1-1? φ is 1-1, let's check that. What does it mean?

1-1 means if φ(g Gs) = φ(h Gs), suppose this happens we want to conclude that g Gs = h Gs. Let us work it out, φ(g Gs) = φ(h Gs), I am taking two elements to the left hand side, domain, which is G mod Gs, so I am taking two elements g Gs and h Gs, suppose, φ of these two elements are equal then that means gs = hs because φ(gGs) = gs, but this means if you now say, h inverse g is this, okay, this is something you have done before, we multiply by h inverse on both sides on the left hand side, so h inverse gs is equal to hs, h inverse h s which is s. h inverse g applied to s is s.

Two three steps are missing here, I am not writing all the steps because we have done these things before, but this means h inverse g fixes s, so it is in the stabilizer of s, so h inverse g is on the stabilizer of s, but h inverse g is in Gs, so is (h inverse g) times Gs equals Gs, remember that if you have an element in the group, the left coset determined by that element is the identity left coset, so (h inverse g)Gs is equal to Gs, but this means gGs=hGs, right.

So we have a function from G mod Gs to orbit of s, if two things map to the same thing, we are saying that they are equal, so this is 1-1, if g(Gs) and h(Gs) map to the same element, namely φ(g

Gs) = φ(h Gs), we concluded that gGs=hGs, so φ is 1-1, this completes that proof.

Finally, is φ onto? What is an element in orbit of s? It is of the form, a typical element, it is simply of the form gs, then we have, you take the same g, φ(gGs) = gs, so onto-ness is very clear here, because elements of the orbit of s are by definition of the form gs, now for the same g, g(Gs) maps the gs, so φ is onto and this completes the proof that φ is a bijective map.

Right, so this is how we relate the stabilizer and the orbit, there is a set-theoretic bijection, let me emphasise that, because Os is just a set, G mod Gs in general just a set, so there is just a bijective map from G mod Gs to Os, namely given by a coset gGs maps to gs, right this is the important definition of the function, and once you have the function defined like that it is is relatively easy to check that is is well-defined, it is 1-1 and it is onto.

So now let us see, what are the applications of this theorem. So the theorem says that, I called it a theorem I guess, it implies the cardinality, so now I am going to use this symbol, it denotes the number of elements, and okay we have used that to denote the order of a group, let's just extend it to denote the order of any set, the cardinality of any set.

(Refer Slide Time 13:00)

So the number of elements of a set is denoted by vertical bars, so if two sets are in bijection then the number of elements in those two sets are equal. This will be most useful when the group and the set are finite so, let us assume that, G is finite. So we need only G is finite, orbit will be fine, S may not be finite, it doesn't matter. So I am going to assume G is finite.

Recall the counting formula, what was the counting formula that we proved when we talked about cosets of a subgroup in a group, if G is group, H is a subgroup, we said that the number of left cosets is equal to the order of the group divided by the order of the subgroup. So G/Gs, which was denoted in our earlier videos by this, the index of, this is the index of Gs in G, this is equal to order of G divided by order of H, right. So let us, written differently, we have order of H, sorry H is Gs here, so Gs times the index of Gs in G is order of G, right. So I am just rewriting the counting formula.
(Refer Slide Time 15:22)

In our case, in our situation the index of Gs in G, is by the theorem that we just proved, remember this is all relative to all of this is relative to the fixed element s in capital S. So every time you see small s here I am referring to that fixed small s, so in our situation the index of Gs in G is the orbit size.

So we have the order of the stabilizer times the size of the orbit is equal to the order of the group, okay. This is a very important application of the theorem that we proved and the counting formula.

This is also called a counting formula, this is in fact very similar to the counting formula that we had earlier, namely G the index of a subgroup in a group G is the ratio of the orders of the two, subgroup, group divided by subgroup, applied to this particular of the case of the group action on a set we have cardinality of the stabilizer times cardinality of the order is equal to the cardinality of the group. This is very important and has many applications, we will see these in later videos, let me only say at this point that, for example, we can immediately conclude that the size of an orbit, let me say that the number elements in an orbit must divide the order of the group.

This is not really clear, right, in general. Why would, so if a group G acts on a set S, you took an orbit which is a subset of this set S, why should the size of that orbit be related to order of the group? It is not clear, right. Group is here acting on a set S, orbit is inside the set, why should the size of the orbit be related to the order of the group? And this is a consequence of the counting formula. It is not only related, it is related in a very precise way: size of the orbit must divide the cardinality of the group, the size of the group.

So this is a very useful observation which tells us that orbits, the sizes of orbits are not arbitrary, right, they have to satisfy the property that they divide the order of the group. So this reduces the choices and helps us compute the orbits in many situations, this is the counting formula.
(Refer Slide Time 19:14)

So I wanted to do one more application of orbits partition the set S, right. So let us apply this orbits partition the set S, so assume now that S is finite. Everything that we have said until this point the set S need not be finite, because even in the counting formula the size of S is irrelevant only the size of orbit is relevant. So in particular I should say that the counting formula says that if G is a finite group acting on an infinite set S, the orbits are still finite, so that is a consequence, orbits cannot be infinite because orbit size must divide the orbit, the group size. The set S may be infinite but the orbits must be finite.

But now I am going to assume that set is also finite. Then we have S must be a disjoint union of orbits because orbits are equivalence classes under the equivalence relation that I defined at the beginning of this video. So they are of the form Os1 union Os2 and the symbol for disjoint union is this, denotes. Okay, this symbol simply means you are taking the union but in addition it says that the sets involved are disjoint, right.

Because S is a finite set, obviously there are only finitely many orbits and if you take the distinct ones among them they are all disjoint and they cover S. So in particular we have the order of the set S is equal to order of the orbit S1, orbit S2, orbit Sk, this is another important counting formula, this is also related to the counting formula. It says that if S is a finite set, then S can be written as sum of orbits.

The cardinality of S, number of elements of S, can be written as sum of some orbits and because of the counting formula that I did in the previous slide, each of the numbers here is a divisor of the cardinality of the group.

So we have a very strong restriction here, so the size of the set S is the sum of some numbers. But each of those numbers divides the order of the group. So we are going to exploit in later videos this is very important observation that we made.

So let me recall, we have made two observations in this video. One is that if G is a finite group acting on a set S, and we fix an element small (s) of capital (S), that is very important. You fix, this is for a fixed element small (s) in capital (S), the stabilizer order times the orbit order is equal to the, product of the stabilizer and orbit is equal to, the cardinality of the group itself. This in particular says, as one consequence, that the number of elements in an orbit must divide the order of the group.

And another way of using the partition of S into orbits is that if S is a finite set the number of elements of S is equal to the sum of number of elements in orbits and each orbit size divides the orbit of the group.

Let me stop the video here. In subsequent videos we are going to exploit these counting formulas that we proved in this video, thank you.