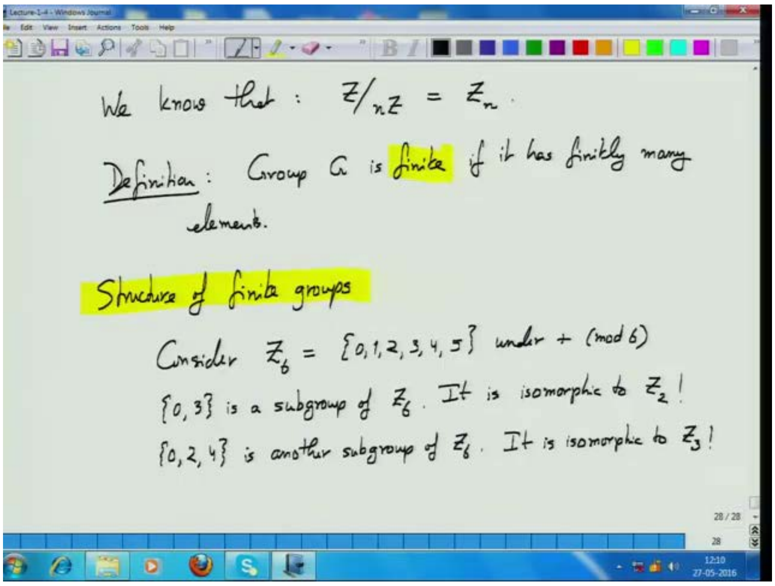
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 05
Groups: Structure Theorem

So, today we continue our discussion forward. Last time we saw this correspondence between homomorphism between two groups and the quotienting operation on groups and the (Refer Time: 00:33).

(Refer Slide Time: 01:03)



We know that : $\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n$.

Definition: Group G is finite if it has finitly many element.

Structure of finite groups

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under + (mod 6)

$\{0, 3\}$ is a subgroup of $\mathbb{Z}_6$. It is isomorphic to $\mathbb{Z}_2$!

$\{0, 2, 4\}$ is another subgroup of $\mathbb{Z}_6$. It is isomorphic to $\mathbb{Z}_3$!

Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help
28 / 28
28
12:10
27-05-2016

And as one of the examples we had seen, that when you quotient, say, set of group of integers with multiples of number n, then you get a new group, which you were calling Z's of n, right. This is a group of numbers between 0 to n minus 1 under addition (Refer Time: 01:14). Now, this is a group and rather, this is the type of groups we will now focus on.

This particular group or this is actually a collection of groups, different for varying values of n. This is what is called a finite group. I think I have defined it earlier also, does not matter, it is the repetition and this is unlike the typical groups. We have encountered group of integers or rational numbers, real numbers or matrices and so on. The only example of a finite group we saw earlier was the group of permutations over 1 to n, that is also a finite group, but this is another example of a finite group.

And if you recall one more thing in this structured theorem for finitely generated groups, what I showed was, that it any such group can be written as a product of Z’s infinitely, many Z’s times one finite group and that finite group I had left undescribed and without giving further details. So, now we will focus on finite groups and see what is their structure and how do we further use them in some of the applications. So, first let us talk about the structure of finite groups and again, here a useful example to keep in mind, mind would be Z n. Although we are talking about general finite group, this Z n is a canonical example of a finite group.

So, we can pose the same question as we had for infinite, in fact, that question is for general group. Then, a group is written as a product of two sub-groups and in case of finite group, question is, can we do that. So, let us take an example. Consider, let us say, Z 6, can I write it as a product of two subgroups. Firstly, does it have subgroups? If it does not have subgroups, then you, of course, you cannot write as a product of two subgroups, sorry.

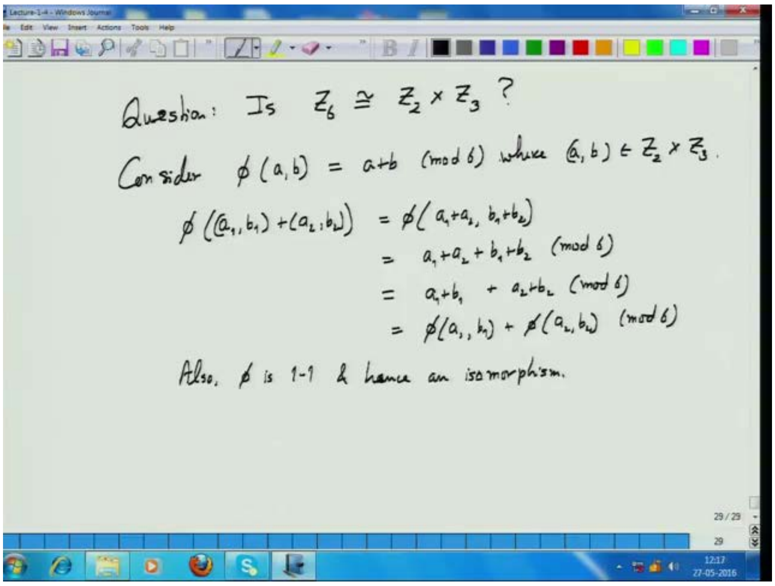
Student: (Refer Time: 05:14)

What are the subgroups? 0 and 3 is a subgroup, wonderful; yes, 0, 3 is a subgroup of Z 6. Easy to verify, 3 plus 3 is 6, which is 0 modulo 6 and these are the only two elements. Now, do you notice something interesting about this subgroup? Can you relate it to one of the groups we have already encountered? Is isomorphic to Z 2, exactly the same structure is Z 2 except that it has 0, 3 with always Z 2 having 0, 1 or and just say, naming convention is really the, 3 in this subgroup plays exactly the same role as 1 in Z. And, so I can write, it is isomorphic to. So, we have found is Z 2 sitting inside Z 6.

Student: 0, 2, 4.

0, 2, 4, wonderful, that is another example; yes, 0, 2, 4 is another subgroup. Now, can you make a similar statement at a 0, 3 is, it is, right, right it is isomorphic to Z 3. So, we got two subgroups in it. So, certainly it is at least possible, that Z 6 can be written as a product of two subgroups. Well, here are two subgroups. Can we write Z 6 as the product of, let us say, these two subgroups? What would it entail? Let us consider the following question.

(Refer Slide Time: 07:33)



Question: Is $Z_6 \cong Z_2 \times Z_3$?

Consider $\phi(a, b) = a+b \pmod 6$ where $(a, b) \in Z_2 \times Z_3$.

$$\begin{aligned}\phi((a_1, b_1) + (a_2, b_2)) &= \phi(a_1+a_2, b_1+b_2) \\ &= a_1+a_2+b_1+b_2 \pmod 6 \\ &= a_1+b_1 + a_2+b_2 \pmod 6 \\ &= \phi(a_1, b_1) + \phi(a_2, b_2) \pmod 6\end{aligned}$$

Also, ϕ is 1-1 & hence an isomorphism.

Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help
29 / 29
29
12:17
27-05-2016

One simple sanity check we can do when we want to address a question like this for finite groups is to at least count the number of elements on the two groups. If the counts are unequal, certainly they are not isomorphic. Z 6 has 6 elements, Z 2 has 2, Z 3 has 3. How about the product Z 2 cross Z 3?

Student: 6.

6, 2 times 3, because every element in Z 2, every element in Z 3 together forms one element of Z 2 cross Z 3, that is by definition. So, it has also 6 elements. So, at least the numbers do match, but that is not sufficient. We have to actually establish an isomorphism between Z 6 and Z 2 cross Z 3. The answer to this question is, yes, we can establish an isomorphism between Z 6 and Z 2 cross Z 3.

Can you make a guess of what that mapping should be?

Student: (Refer Time: 08:54)

Addition, addition of the pairs that will not be isomorphic if you look at.

Student: (Refer Time: 09:09)

Yes, yes, 3 plus 4 will become 1, no, 3 plus 4 will become 1, you are right. 3 plus 2 will become 5; 3 plus 0 will become 3; 0 plus 0 is 0; 0 plus 2 is 2; 0 plus 4 is 4. So, one is missing.

Student: 3 plus 4 (Refer Time: 09:30).

Oh, 3 plus 4 mod 6, I am sorry, that is the one is there. Let us consider, it is a good idea to investigate this, this map, phi (a, b) a plus b mod 6 when (a, b) is in Z 2 cross Z 3. Now, the question is, is this an isomorphism? So, firstly we want to check if this is a homomorphism and then want to check if it is one, one on two. So, to check if it is a homomorphism, we would want to see if.

What is this equal to? This is equal to phi of a 1 plus a 2, b 1 plus b 2. This is the definition of addition for the product group Z 2 cross Z 3. Here, again I am writing the group operation as a plus because that is a more natural representation. Typically, I am your writing in multiplicatively, but here it is clearly makes more sense to write it as an addition operation. So, the group operation on the product is simply the component wise addition here. So, which is what we get here; and by definition of phi this is equal to a 1 plus a 2 plus b 1 plus b 2 mod 6 and this is same as a 1 plus b 1 a 2 plus b 2 mod 6 that it is pretty straight forward and. So, we do get the fact that phi is a homomorphism.

Now, to check if it is an isomorphism we just need to show that it is 1, 1 on 2. Since it maps 6 elements to 6 elements, as long as we show that, it is 1 to 1 is obviously, on 2.

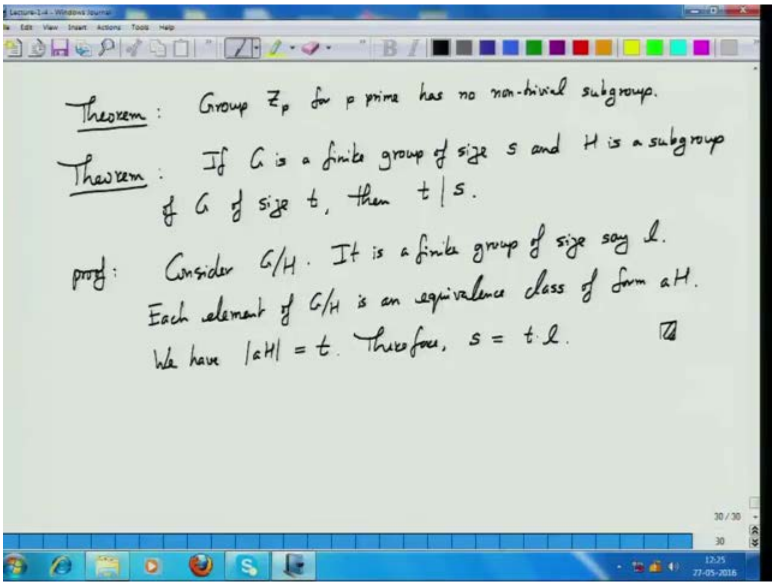
So, is this 1 to 1, we can we have just verified that it is. So, there we are. We can indeed write Z 6 as a product of two smaller segments. Fine, that is a good start.

How about Z 3or Z 2? Can we further split it?

Student: (Refer Time: 13:05).

This is the only subgroup of Z 2 or Z 3 is just the 0, which is a trivial one with that is something we are not interested in at all. So, there is no further splitting of Z 2 or Z 3. So, in that sense, Z 6 is a different, is a different structure than Z 2 or Z 3.

(Refer Slide Time: 14:08)



Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help

Theorem: Group Z_p for p prime has no non-trivial subgroup.

Theorem: If G is a finite group of size s and H is a subgroup of G of size t, then $t \mid s$.

proof: Consider G/H. It is a finite group of size say l. Each element of G/H is an equivalence class of form aH. We have $|aH| = t$. Therefore, $s = t \cdot l$. ☑

30 / 30
30
12:25
27-05-2016

How about Z 5? Can we split Z 5 into smaller subgroups? Can we find a subgroup of Z 5 that is the first question? In fact, if you just think about it for a moment you will realize that you can generalize this observation into the following theorem, that for any prime p the group Z p does not have any nontrivial subgroup. I will prove this theorem, but as a corollary of an even more general theorem.

So, let us suspend this discussion or this theorem for a bit and let us move on to the structure of subgroups of a finite group. So, if you have a finite group, it may or may not have subgroups. You have seen examples of both. If it has a subgroup, what should be the size of that subgroup? Finite group has a size, what would be the size of subgroup?

And the theorem states: if g is a finite group, if g is a finite group of size S and H is a subgroup of G, let us say its size is t, then the number t divides the number S. And the proof is almost immediate based on what we learnt last time. H is a subgroup of G, quotient G with H, this is a group, what are the elements of this group equivalence classes induced by H in G. So, G quotiented H is also a finite group. Since G is finite, it also is a finite group. It is a finite group of size, say l; that means there are l equivalence classes in G quotiented H.

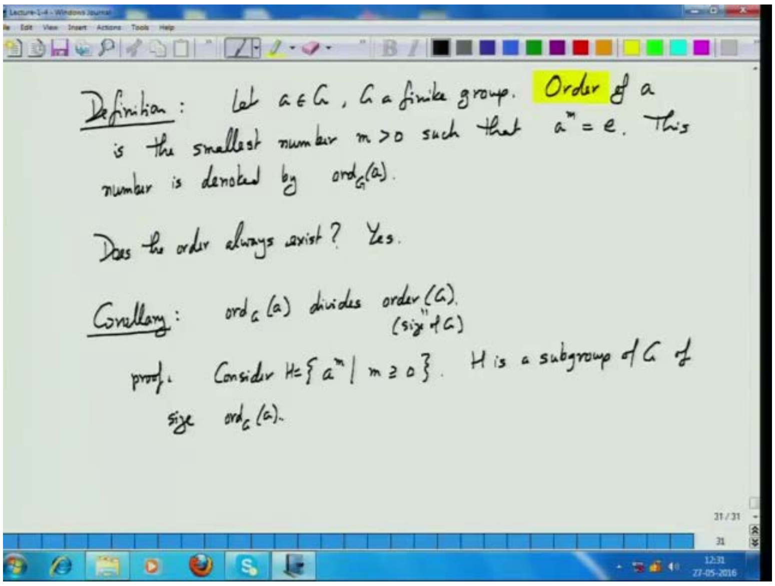
What is the size of an equivalence class? Each equivalence class is of the form a times H. How many elements are there in this equivalence class?

Student: (Refer Time: 18:12).

Size of H because if the elements of this have the form, take any element of H, multiply it with a, that is it. Two such elements cannot be equal if a 1 H is equal to a 2 H. then, you can this cancel H on both sides and get a 1 equals a 2, right. So, these are all distinct elements. Size of a H is exactly t and what is G? G consists of l distinct equivalence classes each of size t; therefore S is t times l, that is it. That established the theorem.

And now, from this theorem the previous theorem follows as a corollary because if we have a group Z p, its size is p, any subgroup will have a size that will divide p. Now, since p is prime, the only numbers that can divide p are 1 and p itself. So, a subgroup of Z p is either z p itself or the trivial group. So, it has no nontrivial subgroup.

(Refer Slide Time: 19:58)



Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help
31 / 31
31
12:31
27-05-2016

Definition : Let $a \in G$, G a finite group. Order of a is the smallest number $m > 0$ such that $a^m = e$. This number is denoted by $\mathrm{ord}_G(a)$.

Does the order always exist? Yes.

Corollary : $\mathrm{ord}_G(a)$ divides order (G).
("size of G")

proof. Consider $H = \{ a^m \mid m \geq 0 \}$. H is a subgroup of G of size $\mathrm{ord}_G(a)$.

We can now look further into this and exploit finiteness to define. Take an element of a finite group, let us call it a. We can associate a number with a, which is called the order of a. It is the smallest number m greater than 0 such that a to the m is identity. Here, I am writing the group operation as a multiplication. This number is written as, in fact, to be more specific it is ordered subscript G or a. So, this represents a fact where it is the group G respect to which you are looking a.

For a finite group b, does the order of an element always exist? That is the first question one must ask. The answer is yes and it is simple to see, just.

Student: (Refer Time: 22:11).

Sorry, pigeon hole principle, yes, you consider, so let us say, size of G is s. So, consider s plus 1 powers of a. a, a square a cube, up to a to the s plus 1, all are elements of the group G. So, two of them must be equal by pigeon hole principle and then, you know, that means, you just do the cancellation and you get a to the some power is identity. So, the answer is yes. So, it makes sense to talk about order of any element for a finite group.

What, can we establish a relationship between the order of a group, order of an element and the size of the group? Again, the answer is yes. So, in fact, it follows from a as a corollary of the previous theorem that order of a divides the order of G. here, I am using order bracket g. So, represent the order of this or the size of the group g. The proof is straight forward. Consider the set a to the m, m greater than equal to 0. So, all powers of a, this is a subgroup of G and what is the size of this subgroup? Order a, that is, it is order a is the, smallest number for which a to the m is identity. So, all smaller powers of a, a to the 1, 2 up to m minus 1, they are all distinct elements of the group and a to the m is the identity. So, there are exactly m elements or the order many elements in the group, subgroup H and that is it.

Now, you apply the previous here, okay, this is corollary. So, we have in the finite group several interesting facts. Every subgroup will divide the order of size of the group size of a subgroup. Moreover, every element has an order which is naturally associated with a subgroup of the group and follows, that the order of every element also divides the size of the subgroup.

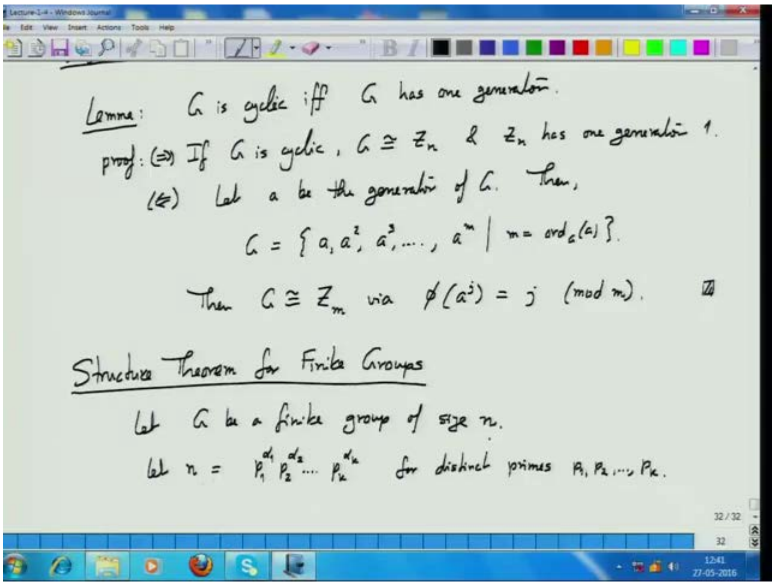
Now, we can come to some more definition, at least one more definition and then, I will define the structure or will give this structure theorem for finite groups. What is the simplest form of a finite group? Just like the simplest form of an infinite group was Z, why, because it had one generator and that generator produced all elements of that group. So, that in essence is the simplest structure in a group.

So, when we talk about the finite group, we can again look at the simplest groups or simplest finite groups being the ones, that had, that have just one generator. And do you know examples of these groups?

Student: Z n.

Z n is one typical example for any n; actually Z n is a group with just one generator. And since these are finite groups and this fact is very useful in case of a finite group, we have a special (Refer Time: 27:05) for this.

(Refer Slide Time: 27:08)



Lemma: G is cyclic iff G has one generator.

proof: ($\Rightarrow$) If G is cyclic, $G \cong Z_n$ & Z_n has one generator 1.

($\Leftarrow$) Let a be the generator of G. Then,

$$G = \{a, a^2, a^3, \ldots, a^m \mid m = ord_G(a)\}.$$

Then $G \cong Z_m$ via $\phi(a^j) = j \pmod m$. ☒

Structure Theorem for Finite Groups

Let G be a finite group of size n.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ for distinct primes $p_1, p_2, \ldots, p_k$.

Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help
32 / 32
32
12:41
27-05-2016

So, we call a finite group cyclic group if it is isomorphic to Z n. And equivalently, cyclic groups are precisely the groups with exactly one generator and that is a lemma, simple lemma. To prove, one way is straight forward. If G is cyclic, it is isomorphic to Z n and Z n has exactly one generator, therefor G has one generator. So, that direction is very straight forward, which is 1. So, that establishes if G is cyclic. So, that is a forward direction.

What about the reverse direction, which is Z? Suppose G has one generator, then you want to show that it is cyclic. So, let us say, let a be the generator of G, then by definition of generator what can we write G as? And by definition of generator, since a is generator, different powers generate all of G and since G is finite, a has an order, let us say, order of a is m, then these m powers of a, a square up to a to the m, generate precisely the G (Refer Time: 30:28). These are these powers constitute the entire G.

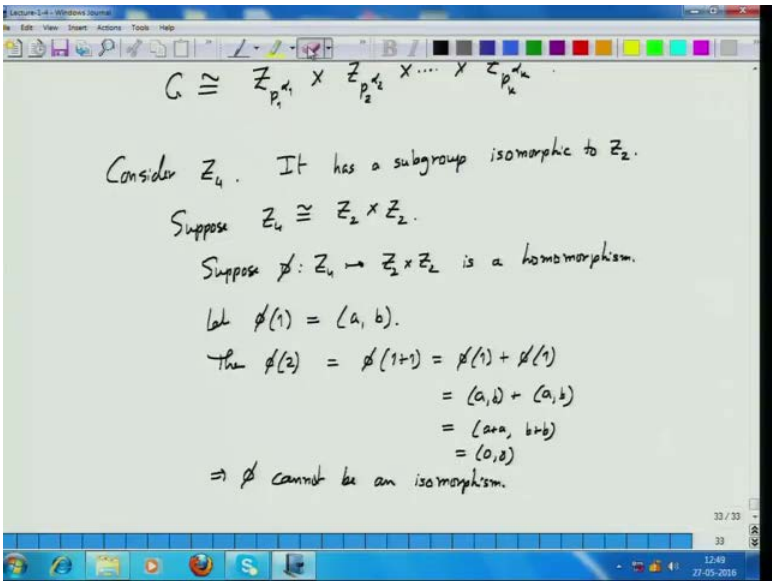
And now, we want to show, that such a G is isomorphic to Z n for some n. Do you see that isomorphism? Write G is then isomorphic to Z m, what is that isomorphism? phi of a to the j is mapped to j equals modulo m. It is easy to say, that it is homomorphism and it is say, one to one mapped and therefore, an isomorphism. So, these are in a sense, the simplest form of finite groups, cyclic groups. Note, that we have already seen, since Z n, all, for all n is cyclic group, there are still distinctions within these. Some of, say at Z p's have no subgroups, whereas Z n for a composite n does have subgroups.

Now, let me give you the structure theorem for finite groups. Let G be any finite group of size n and again, I emphasize, that I am talking about commutative group set, not a general group. And let n, which is a size of this group G p written as in its prime decomposition, p 1 to the alpha 1 p 2 to the alpha 2 up to p k to the alpha k; p 1 to p k are distinct prime numbers. Then, g is isomorphic to this product, Z p 1 to the alpha 1 cross Z p 2 to the alpha 2 to z p k to the alpha k. Each one of them is a cyclic group and therefore, all is the simplest form of a finite group and the group G itself can be written as a finitely many products of such groups. So, this completely describes the structure of a commutative finite group.

Again, I am not going to prove this theorem, you can look it up. The proof is not very difficult, just follows the concepts I have introduced, (Refer Time: 34:54) certainly little involved. Any questions so far?

So, now, you can go back and describe the structure of finitely generated groups even better, that is, contains finitely many copies of Z and then, finitely many copies of cyclic groups. This subsumes our earlier discussion about Z 6. Z 6 we wrote as Z 2 cross Z 3, that follows from this theorem because 6 is 2 times 3 and therefore, you write it as a product.

(Refer Slide Time: 35:37)



$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Consider $\mathbb{Z}_4$. It has a subgroup isomorphic to $\mathbb{Z}_2$.

Suppose $\mathbb{Z}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Suppose $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ is a homomorphism.

Let $\phi(1) = (a, b)$.

Then $\phi(2) = \phi(1+1) = \phi(1) + \phi(1)$

$= (a,b) + (a,b)$

$= (a+a, b+b)$

$= (0,0)$

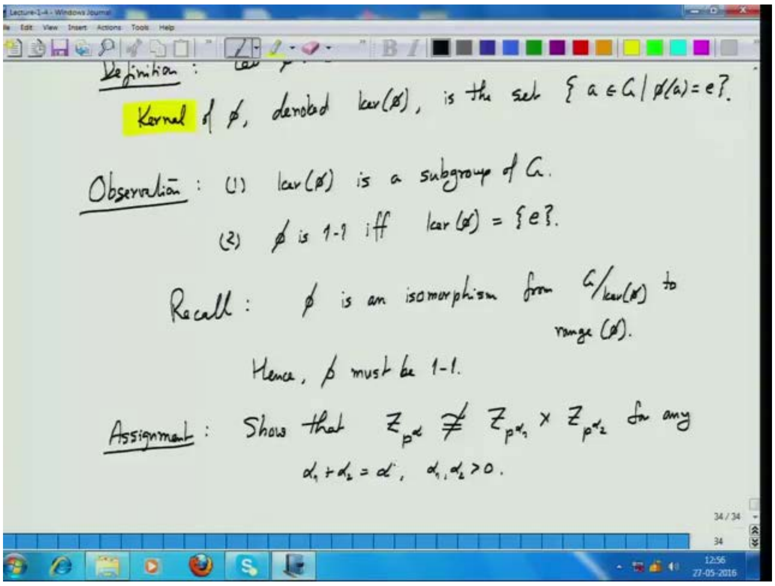
$\Rightarrow \phi$ cannot be an isomorphism.

Another interesting observation here is that we cannot further subdivide Z p 1 to the alpha 1 and to see this as an example, consider Z 4. It is 0, 1, 2 and 3. Does it have a subgroup? What is the subgroup? 0, 2 is a subgroup, that is, Z 2. So, the, if Z 4 splits as a product of two smaller groups, since the sizes have to match, it has to be two times two groups, two groups of size two each and Z 2 is one of them. So, it has, it appears, that it should be something like bring isomorphic to Z 2 cross Z 2, that by the structure theorem it goes further. This is the only way you can split Z 4.

But is it true, is Z 4 isomorphic to Z 2 cross Z 2? If it were, we should be able to establish an isomorphism between Z 4 and Z 2 cross Z 2. Now, suppose phi sending Z 4 to Z 2 cross Z 2 is a homomorphism. So, let phi of one be (a, b), then what is phi of 2? This is phi of 1 plus 1 is phi by homomorphism property. It is phi 1 plus phi 1, which is (a, b) plus (a, b), which is a plus a comma b plus b and what is a plus a in Z 2? So, (0, 0), so phi 2 is mapped to 0 by any homomorphism phi, sorry, 2 is mapped to 0 by phi, which is any arbitrary homomorphism from Z 4 to Z 2 cross Z 2, which means, this mapping, this phi sends is not one to one. It is sending 0 to 0 comma 0 as well as 2 to 0 comma 0. So, it is a homomorphism, but it has, it is not 1 to 1; this implies that phi cannot be.

So, this is the very useful tool. This homomorphism is a very useful tool to establish, just like we did, if a mapping is one to one or not and if all we need to do is to see what are the elements being mapped to the identity.

(Refer Slide Time: 40:08)



Lecture-1-4 - Windows Journal
File Edit View Insert Actions Tools Help

Definition :

Kernel of ϕ, denoted $\ker(\phi)$, is the set $\{a \in G \mid \phi(a) = e\}$.

Observation : (1) $\ker(\phi)$ is a subgroup of G.

(2) ϕ is 1-1 iff $\ker(\phi) = \{e\}$.

Recall : ϕ is an isomorphism from $G/\ker(\phi)$ to range (ϕ).

Hence, ϕ must be 1-1.

Assignment : Show that $Z_{p^{\alpha}} \not\cong Z_{p^{\alpha_1}} \times Z_{p^{\alpha_2}}$ for any $\alpha_1 + \alpha_2 = \alpha$, $\alpha_1, \alpha_2 > 0$.

34 / 34
34
12:56
27-05-2016

In fact, let me now describe another definition which is kind of familiar. We are just giving a name to something we already know. So, we already have come across this set, set of elements of G, that are mapped to identity by the homomorphism phi.

We, I am just giving a name to it, kernel, and denoting it by ker of phi. So, this set is called the kernel of the map and the observation are that first, of course, this we have already seen, kernel is a subgroup of G. Two, phi is one to one if and only if kernel phi is just one element. And this is again easy to see. If phi is one to one, surely kernel of phi will be identity because it says, if it is one to one it cannot map two elements to identity.

The interesting one direction is the other way, if kernel of phi is identity, then phi is one to one. Why? See, you recall the result we proved last time for phi being a homomorphism that induces a subgroup which is the kernel is what we are calling it today. In fact, let me just recall phi is an isomorphism from G slash kernel of phi to range of phi. We saw this last time, kernel of phi is this set and it is like this map. phi is essentially like quotienting G with the kernel of phi and which gives us equivalence classes and then, we have an isomorphism between this group and the range of phi, which is a group in, a subgroup of H.

Now, if kernel phi is identity what does it imply? G slash kernel of phi is just G and we establish phi, establish an isomorphism between G and range of phi. Clearly, one of the simpler consequences of this is that phi is one to one. Since there is an isomorphism from G, phi is an isomorphism from G to range of phi. So, it is, it is an isomorphism. So, it has to be one to one.

And this is the tool we just used to show, that there is no isomorphism between Z 4 and Z 2 cross Z 2 and that is an example of Z p power alpha, which is not, which cannot be split further. In fact, this I will give you as an exercise. Let me give that as an assignment problem also.

Prove, that Z p to the alpha, which is a cyclic group, cannot be written as a product of Z p to the alpha 1 and Z p to the alpha 2 for any alpha 1 alpha 2. They have to be nontrivial, that is, at least one. And the proof follows along the similar lines as I just described for Z 4, that is why you cannot split in the structure theorem anything (Refer Time: 46:50).

So, we will meet again tomorrow.