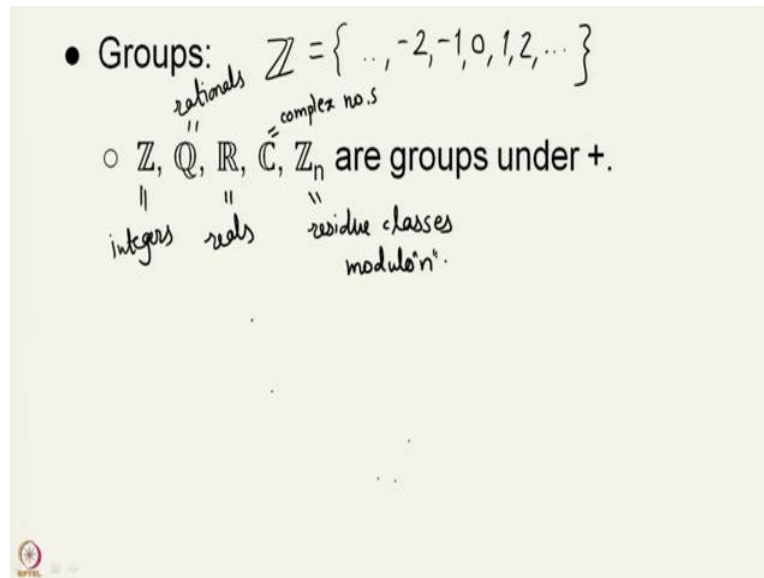


A Basic Course in Number Theory
Professor. Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 25
Primitive roots - I

In the last lecture, we saw the structure of groups, here we will see some examples.

(Refer Slide Time 00:27)



So, there are, these are some of the examples, we have the integers, the set of all integers, so remember, this denotes the set of all integers minus 1, 0, 1, 2, and so on. So, these are the integers, these are the rationals, you may call them rational numbers, these are the reals, real numbers, these are the complex numbers, and these are our residue classes modulo n all these form groups under addition. And this is something that we have seen already, or if you have not seen then maybe you should go back and see these things, these are all groups under addition, there are also groups under multiplication.

(Refer Slide Time 01:33)

- Groups:
 - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ are groups under +.
 - $\mathbb{Z}^\times, \mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, \mathbb{Z}_n^\times$ are groups under \times .
{i: (i,n)=1}
{±1} non-zero elements

So, these are the group. In general, what we have for all this is that this is the set plus minus 1, these three these are all the non zero elements in the corresponding sets. And remember, these are all the elements i where the GCD of i and n is 1. So, these are all invertible elements with respect to the product in the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ which we have seen earlier which are groups under addition.

And here we have that these corresponding invertible elements form a group under multiplication, which also tells you that the elements which we have seen earlier, the examples also have 1 more structure than addition, and that is the structure of multiplication and this is what takes us to our next concept of a ring.

(Refer Slide Time 02:34)

- Groups:
 - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ are groups under +.
 - $\mathbb{Z}^\times, \mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, \mathbb{Z}_n^\times$ are groups under \times .
- Rings: *every non-zero element is invertible.*
 - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ are rings under + and \times .
If n is composite then we get non zero elements which are not invertible.

So, we have seen the definition of group in the last lecture, perhaps in a hurried manner but we are not going to be able to spend more time on these things. A ring is something which is equipped with two binary operation and traditionally, one of them is denoted by plus and the other is denoted by product.

What we require is that the ring or the set R be a group with respect to plus. And there should be some more properties with respect to the product. The properties with respect to product are, first of all that the set be closed undertaking product, the closure property. We also demand that our rings often be associative, there are of course examples of non associative rings that people study, but we are going to look at only associativity. We do not ask for the identity element to be there and of course, we do not ask for inverse of every element.

As you see the set of Z does not have the inverse property, the multiplicative inverse of two is not there in Z . So, identity element may be there and in that case, we say that our rings are rings with identity, identity element may not be there. So, we have two structures plus and product, with respect to plus we have that it should be a group, with respect to product we demand that there be two properties, closure and associativity. But we are not going to put these two structures in isolation, we are going to have a condition which will tell you how these two structures can be combined.

Whenever you have a set and you are putting some structures randomly, you would demand that the different structures have something to do with the first structure, only then there is some meaning to the whole structure. So, here we demand that the product and addition be tied up with a rule which is called distributivity, which says that a into b plus c should be ab plus ac .

So, you have b and c , these are the two elements of the set R ; b plus c is yet another element of the set R , and you are multiplying to the b plus c by a . So, whether you take the addition first and then multiply by a or you take the multiplications first, which is ab and ac , and then add, you should get the same answer. This is called the first Distributivity law.

The second law of distributivity is that, you have a plus b into c should be equal to ac plus bc . So, there is a multiplication on the left hand side and there is a multiplication on the right hand side also. So, a dot b plus c , this is the multiplication on the left hand side, a plus b dot c or a plus b multiplied to c is the multiplication on the right hand side.

These give you two distributivity laws, this all constitutes a ring. Once again, with respect to plus it should be a group, there is one more important condition that it should be an abelian group, which is to say that $a + b$ is always equal to $b + a$. So, with respect to plus it should be an abelian group, with respect to product there should be two properties, closure and associativity and product should distribute over the sum, both on the left hand side as well as on the right hand side.

And the examples that we see here are the examples of commutative rings with identity. If you see very carefully, the examples \mathbb{Q} , \mathbb{R} , and \mathbb{C} have the property that every non zero element is invertible. Whereas, in \mathbb{Z} we have the element 2 here, which is not invertible although it is non zero. And here if n is composite, then we get non zero elements which are not invertible.

Composite just means that it is not a prime, whenever we have a prime p dividing n , and p is less than n , then p itself is an element in your ring. So, p for instance will give you such an example. So for us, what we are going to do is to consider only the groups or rings which are finite, we have been looking at these things so far in our lectures and this is what we are going to study, so we are going to be dealing with finite groups, finite rings.

Moreover, we are going to look at commutative rings where the product is also commutative. We demand that under addition, there the group should be abelian but here we demand that, here we have that the product is also abelian, that is one plus thing. And we also have that, all these rings have identity in them. So, what we are looking at are finite commutative rings with identity. We are going to require some more concepts of group theory and ring theory.

(Refer Slide Time 09:01)

The groups \mathbb{Z}_n^\times are called the unit groups of \mathbb{Z}_n , they are denoted by U_n .

We want to find the exact structure of these groups.

For that, it would be useful if you brushed up with your knowledge of basic group theory.

Concepts like subgroups, cyclic groups, direct products will be useful to know.

So, we are going to study these groups called the unit groups of \mathbb{Z}_n , these are denoted by \mathbb{Z}_n^\times , we put this cross on the head to signify that we are going to look at elements which are invertible with respect to the multiplication. These are the groups, unit groups that we are going to study, they are going to be called U_n , where U stands for units. We have already seen what the cardinality of these groups are going to be. But, after that we want to find the exact structure of these groups. So, we want to see how they behave, if you are looking at the group structure of these, this will help us in distinguishing various U_n .

Later on, we will see examples of these U_n and you will see what I mean by distinguishing the U_n by the group structure that we put on them. So, once again, I think it would be good if you brushed up with your knowledge of basic group theory. And the concepts that you should look for are subgroups, cyclic groups and direct product.

If this seems to be too much for you, then what I suggest is the following. While we go on proving the later results, we are going to use some particular concepts in groups. And I will of course, have to mention that while I give you the proofs, so when I mention that you note all these concepts down and go back and check the definitions; that will help you understand these groups in a better way.

If, of course, there are ways to do these proofs without using the group theory, which is to say that we will do the same operations but in more detail, and we will not use the word group, cyclic group, direct product or so on, but then our proofs will become very lengthy and such proofs are not inspiring. What happens is that there are same methods applied in many proofs

and therefore, you combine these methods and give them some name. So, the group theory is one such method which we are going to use in number theory.

(Refer Slide Time 11:32)

We start with understanding the structure of \mathbb{Z}_p^* or U_p .

We will prove that this group is cyclic.

An element $a \in U_n$ is called a primitive root, modulo n , if the order of $a \in U_n$ is equal to $\varphi(n)$.

$$a^{\varphi(n)} = 1 \quad \text{and} \quad a^m \neq 1 \quad \text{for any } m < \varphi(n).$$

$$\# U_n = \varphi(n)$$

It has been our experience that, the primes are well behaved whenever we study any structure associated with a general integer n . So, we start by looking at the group of units modulo a prime p , we call this to be U_p . Of course, the \mathbb{Z}_n^* is U_n , so whenever your n is the prime number p we will call them U_p . What we are going to prove first is that all these groups are cyclic, this is to say that there is an element in \mathbb{Z}_p^* whose powers will give you all elements. So, there is an element a in \mathbb{Z}_p^* such that a , a^2 , a^3 , a^4 , \dots will list all the elements in U_p , this is what we want to prove.

Perhaps, the result is true in more generality, so we make one definition here. An element a in general U_n , where n need not be a prime, an element a in U_n is called a primitive root, modulo n . So, we will work with the concept primitive root, but it is understood that whenever we are talking about primitive root there is an n which is there in the background, so we call this element a to be a primitive root if the order of a is equal to $\varphi(n)$.

What it means to say is that, a power $\varphi(n)$ is equal to 1 in U_n and a power m is not 1 for any m strictly less than $\varphi(n)$. So, when you list all these elements, a , a^2 , a^3 , and so on, you do not hit 1, once you hit 1 after taking power for some times, the next number that you will take will again be equal to a .

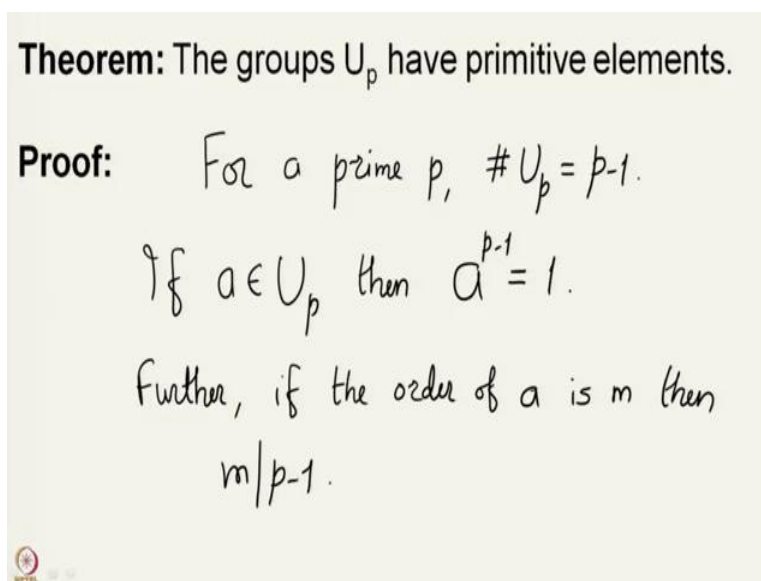
If you have that a power 10 is 1, then a power 11 which is a power 10 into a and if a power 10 is 1, then a power 11 is going to be a . So, you have a , a^2 , a^3 up to a power 9 and

a power 10 which is 1, then a power 11 will be a and you are going to get the same loop again. So, here what we demand is that of course, we are asking for the order to be $\phi(n)$, but not smaller than $\phi(n)$.

Therefore, the distinct elements that you get are $\phi(n)$ in number and we also know that cardinality of U_n is equal to the Euler phi function $\phi(n)$. So, whenever you have a primitive root modulo a number n , you have that the corresponding group is a cyclic group, U_n will then be a cyclic group.

So, we are going to be studying these structures of these U_n , trying to see whether they are cyclic or not by trying to verify whether there exists a primitive element modulo that n or not. So to begin with, where we want to prove that our group U_p is cyclic, this is to say that each U_p has a primitive element, this is what we will have to prove.

(Refer Slide Time 15:23)



Theorem: The groups U_p have primitive elements.

Proof: For a prime p , $\#U_p = p-1$.

If $a \in U_p$ then $a^{p-1} = 1$.

Further, if the order of a is m then $m|p-1$.

So, the theorem says that the groups U_p have primitive elements. So, we observe first of all that for a prime p , the cardinality of U_p is $p-1$. And we already know that, U_p being \mathbb{Z}_p^\times is a group under multiplication and if you take any element then, the $p-1$ power will always give you 1. The question is, to find an element a for which no smaller power gives you 1, this is what we want to show. Furthermore, using group theory, if a , if the order, so this is where I am now going to use some concept from group theory which is to talk about order of a .

Furthermore, if the order of a is m , then we also know that m has to divide p minus 1. So, if you take all the elements in the group U_p and separate them out by their orders, then they would be in the sets which are indexed by divisors of p minus 1.

(Refer Slide Time 17:20)

Theorem: The groups U_p have primitive elements.

Proof (contd.): Thus we have $A_m = \{a \in U_p : o(a) = m\}$

give $\coprod_{m|p-1} A_m = U_p$. $A_1 = \{1\}$.

Then $\sum_{m|p-1} \#A_m = p-1$.

Note that each $\#A_m \geq \varphi(m)$ whenever $A_m \neq \emptyset$.

So thus, we have A_m , which are elements a in U_p with the property that the order is m , give disjoint union of A_m , where you have m dividing p minus 1 is your U_p . The disjoint union of all these A_m , A_m cannot have any intersection with a different A_l because in A_m the order of the element is m , in A_l the order of the element is going to be l . And if you have any element in common, it will say that the order of the element is both m and l . But that cannot happen if m is not equal to l . So, this is a disjoint union and what we have observed before is that, these summation of their cardinalities will give you p minus 1, this is something that is quite nice.

So, what does it tell you, it tells you that when you take the summation of the cardinalities of A_n . So, for instance here you should check that A_1 is only the element 1, just to give you an example of 1 A_m , this is the only element whose order is 1, there is no other element, which to the first power is equal to 1, so 1 is the only element of order 1.

Then you will look at other divisors of p minus 1 and find the sets A_m , it may happen that some particular A_m are empty, it may happen that you are looking that say it 3 is a divisor of p minus 1, but there is no element of order 3. So, in that case A_3 will be empty, and then the cardinality of A_3 will be 0, that is quite okay. But what we certainly have is that every element in U_p has to have some order dividing p minus 1 therefore, every element of U_p is in sum A_n , and clearly A_m are subsets of U_p .

So, you have the equality that the disjoint union of A_m is U_p , which when you take the cardinalities gives you that the summation of cardinalities $|A_m|$ for m dividing $p-1$ is $p-1$. Now, what we have further is the following thing. So, each note that each A_m cardinality is bigger than or equal to $\phi(m)$.

Why do I say this, this is because when you take a particular M and you take an element of order m we are looking at, so this is true whenever A_m is non empty. So, start with an element a of order m , we are assuming that A_m is non empty, so there is an element A of order m . Then look at this cyclic subgroup generated by A , so this will be the element a , a^2 , a^3 , so on all the way up to a^{m-1} and then a^m gives you 1.

So, this is the cyclic subgroup of order m of the group U_p . Now, we want to know how many generators are there of this cyclic subgroup. So, A is 1 generator but there could be some more generators and the basic fact in cyclic groups tells you, that A^i is a generator of this cyclic group generated by A , precisely when i is co prime to m .

So, the group generated by A has $\phi(m)$ generators, these are all distinct elements. So, whenever you have an element of order m , you are going to take one of them, it will have $\phi(m)$ generators, since they generate the same subgroup, they will also be of order m . Therefore, once you have 1 element of order m , you have at least $\phi(m)$ elements of order m .

So, we have two equations here, our equation number 1 tells you that these cardinalities give you $p-1$, but then whenever this is non empty, each such cardinality is bigger than or equal to $\phi(m)$.

(Refer Slide Time 22:55)

Theorem: The groups U_p have primitive elements.

Proof (contd.): Then

$$p-1 = \sum_{m|p-1} \#A_m = \sum_{\substack{m|p-1 \\ A_m \neq \emptyset}} \#A_m \geq \sum_{\substack{m|p-1 \\ A_m \neq \emptyset}} \varphi(m)$$

$$\sum_{m|p-1} \varphi(m) \geq \sum_{\substack{m|p-1 \\ A_m \neq \emptyset}} \varphi(m)$$

Let us put these together to get the following nice result. Then, $p-1$ which is summation of cardinality A_m , where we have that m divides $p-1$, this is also clearly summation of the cardinalities A_m , where you have that m divides $p-1$ and A_m is non empty. The only difference between these two sums, the only difference between this and this is that here you are taking all the m 's dividing $p-1$, whether the A_m is empty or not.

And here taking, you are taking all those m 's dividing $p-1$, where A_m is non empty. So, the only difference between these two is the cardinality of A_m which are empty but those are anyway 0. So, these two equalities are the same, that tells us that we have this equality and this is now bigger than or equal to m dividing $p-1$ $\varphi(m)$ of course, with the condition that A_m is non empty.

But if I have my A_m to be non empty and I take the summation over m dividing $p-1$, I get φ , φ of summation of $\varphi(m)$ where m dividing $p-1$. Whereas on this side, I also have summation over $\varphi(m)$, where m divides $p-1$, this is something that we have proved after studying the Euler φ function, that summation $\varphi(d)$ where d divides n has to be n . So, what we now have is summation $\varphi(m)$, m dividing $p-1$ is of course bigger than or equal to summation $\varphi(m)$, where m divides $p-1$ and A_m is non empty.

We want to say that, these two equations are the same and therefore, we want to say that whenever A_m is non empty, we should get $\varphi(m)$ and nothing more than that. So, here we have, when we have this inequality and if you are not getting all $\varphi(m)$, then $\sum \varphi(m)$ should come with more multiplicity.

(Refer Slide Time 25:51)

Theorem: The groups U_p have primitive elements.

Proof (contd.): Further, note that each $a \in A_m$ gives a cyclic subgroup of order m , in particular, we get roots of $x^m - 1$ in \mathbb{Z}_p .

$\#A_m \leq \varphi(m)$ $\#A_m = \varphi(m)$

$\sum_{m|p-1} \varphi(m) = p-1 = \sum_{\substack{m|p-1 \\ A_m \neq \emptyset}} \varphi(m) \Rightarrow A_m \neq \emptyset \forall m|p-1.$

Further, note that each a in A_m gives a cyclic subgroup of order m , in particular we get roots of $x^m - 1$ in \mathbb{Z}_p . But once we have roots of this polynomial, it should immediately strike to you that a polynomial of degree m cannot have more than m roots. So, what we get is that the cardinality of A_m is also less than or equal to $\varphi(m)$. This is because once you have 1 element generating a cyclic group of order m in that cyclic subgroup, you will have $\varphi(m)$ elements of order m .

If you have any more elements of order m , it should give you at least 1 more element outside this cyclic group and then the polynomial $x^m - 1$ will have more than m solutions, this is something which cannot happen. So, whenever we have that the cardinality of A_m is nonzero, you will actually have that the cardinality of A_m is exactly equal to $\varphi(m)$.

And now, we go back to the previous slide which tells us that $\sum_{m|p-1} \varphi(m) = p-1$, which is also $\sum_{\substack{m|p-1 \\ A_m \neq \emptyset}} \varphi(m)$, but here the condition is that A_m is non empty. Since, these two terms are equal you should have that A_m is non empty for every m dividing $p-1$. Which tells you that, for every m for every divisor of $p-1$, there is an element of order m . And therefore, we get that in particular U_p has primitive root.

So, we have proved that the group of units modulo p is a cyclic group of order $p-1$. Go through this proof, it uses some concepts from basic group theory which are not very difficult and you will get familiar with these when you study these things more. In the next lecture, we

are going to look at structure of U_n in general and see whether they are cyclic and if they are not cyclic, then we would like to find the exact structure of these unit groups U_n . Thank you.