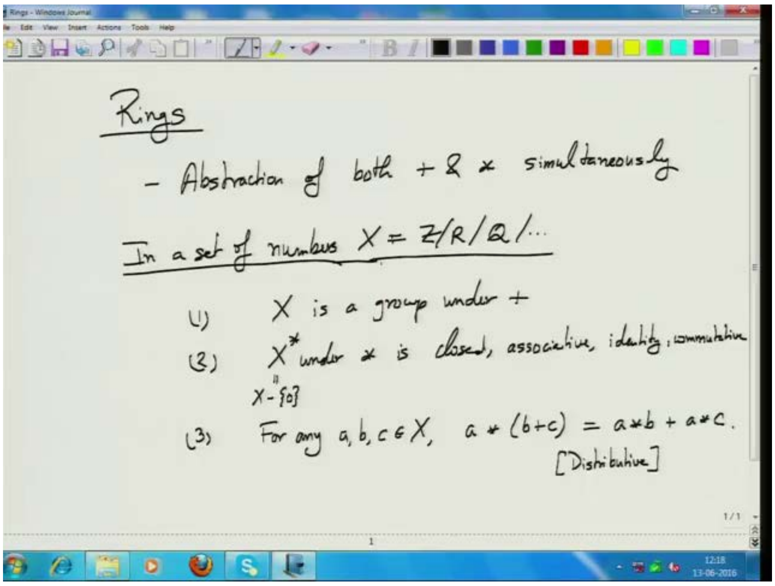
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 07
Rings: Introduction

We finished with the groups last time, and I hope I managed to convey the nice properties of the abstraction we get, starting from the simple arithmetic and coming to groups. Now, today, I will start on the next abstraction which is called rings. Rings are perhaps the single most important abstract object in whole of mathematics. It is extremely fundamental, extremely useful, and is applied in a very wide variety of domains.

And, the reason, at least one of the reasons for why it is so important is simply that, it very nicely abstracts almost the whole arithmetic. If you recall, if you go back to our motivating example of numbers, numbers, we know, admit 2 operations, addition and multiplication, and then, when we abstracted our groups from them, we said, let us just focus on one of these 2 operations. Now, in case of rings, we abstract, or try to abstract the full arithmetic, which means, simultaneously abstract out both the operations, and the way they interact with each other.

(Refer Slide Time: 01:49)



Rings

- Abstraction of both + & × simultaneously

In a set of numbers $X = \mathbb{Z}/\mathbb{R}/\mathbb{Q}/\ldots$

(1) X is a group under +

(2) $\underset{X-\{0\}}{\overset{\shortparallel}{X^*}}$ under × is closed, associative, identity, commutative

(3) For any $a, b, c \in X$, $a * (b+c) = a*b + a*c$.

[Distributive]

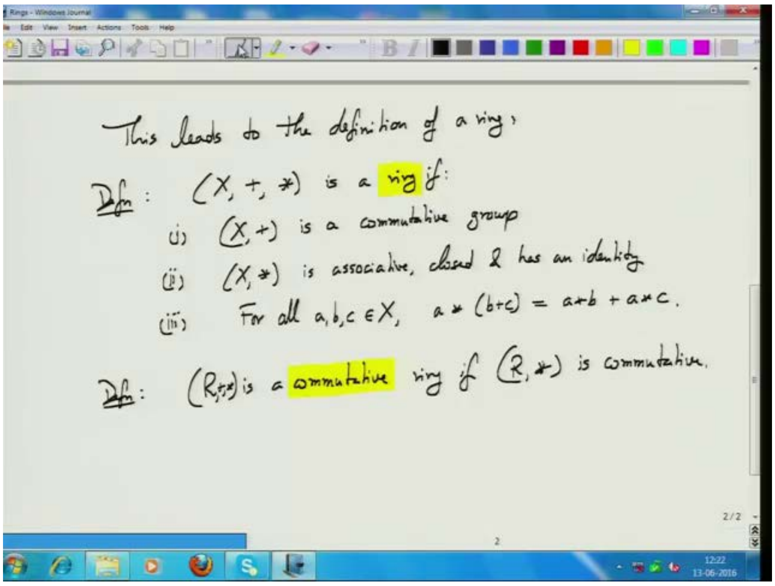
Now, if you see the set of numbers, the addition and multiplication operation satisfies certain properties and we can express those properties in terms of the abstraction we already have. For example, in a set of numbers, let us say, X, X is a group under addition, whether we start with X being a set of integers, or a set of rational numbers, or set of real numbers, etcetera, it is a group under addition. And again, when I say group, I mean a commutative group.

In fact, that is the reason why we abstracted out the group structure to begin with. Now, what can we say about the set under multiplication? For sum of this, like real numbers or rational, the non-zero numbers form a group under multiplication; we have also seen that. But, it is not true in case of integers. In case of integers, we do not get a group under multiplication. And, I will not, at this point, like to leave out integers from the picture, because, I want to abstract out this arithmetic in a most general possible way. We can do arithmetic on integers, but it is somewhat more restricted, in terms of division not being there, or only part of the division being there. We can divide 4 by 2, but we cannot divide 4 by 3.

So, in that sense, one would like to abstract out the most general arithmetic structure, and because of that, I would not say that, this set of numbers, they group under multiplication, but, it does satisfy all other group properties, namely, X star I should say; X star means X minus zero. Under multiplication, it is closed. It is associative as an identity, and it is also commutative. The only property missing is the inverse. So, that is the structure of the numbers under multiplication.

We already know the structure of the numbers under addition, but, there is one thing that is still missing, is the way addition and multiplication interact with each other, and that is captured by the next property. This is called Distributive property. This property captures the way, when we do addition and multiplication simultaneously, what happens. So, a multiplied with b plus c, this number, is same as a multiplied with b, and a multiplied with c added to it. These three are the properties we can abstract out, when working with any set of numbers, and this is what is a ring.

(Refer Slide Time: 06:49)



This leads to the definition of a ring:

Defn: $(X, +, *)$ is a ring if:

(i) $(X, +)$ is a commutative group

(ii) $(X, *)$ is associative, closed & has an identity

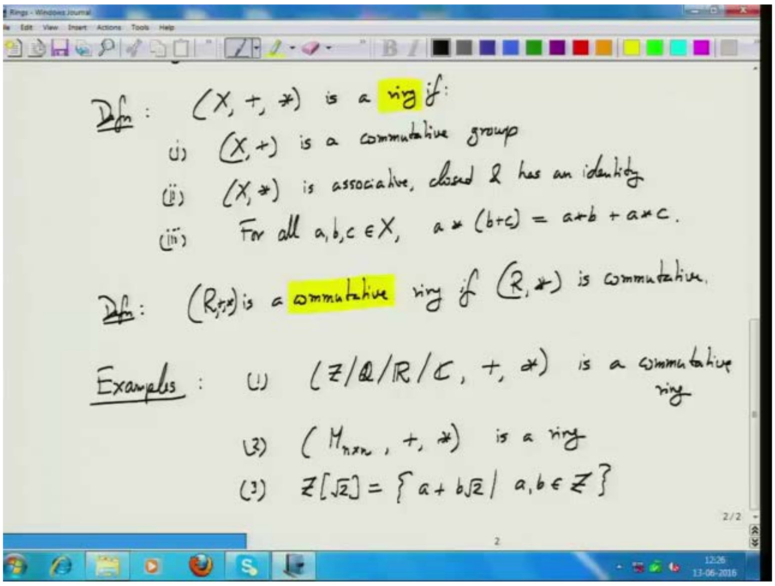
(iii) For all $a, b, c \in X$, $a * (b+c) = a*b + a*c$.

Defn: $(R, +, *)$ is a commutative ring if $(R, *)$ is commutative.

Let me say; so, almost this exactly the same set of property that I had listed earlier, with one minor difference, which is that, I have removed the commutative property for the multiplication operation. And, depending on whether multiplication is commutative or not, the ring will be a commutative ring or not. Sorry, plus star, of course. The structure R, under addition and multiplication, is a commutative ring if the multiplication operation is commutative.

Note that, addition or operation must always be commutative. We are not leaving any option for it to be not commutative. And again, for the purpose of this course, we will be interested essentially in commutative rings; not in other types of rings. So, whenever I say a ring, without meaning either commutative, or non-commutative, it will normally mean a commutative ring. So, that is the definition; very straight forward. And now, we can immediately ask examples of rings.

(Refer Slide Time: 10:26)



Dfn : $(X, +, *)$ is a ring if:

(i) $(X, +)$ is a commutative group

(ii) $(X, *)$ is associative, closed & has an identity

(iii) For all $a, b, c \in X$, $a * (b+c) = a*b + a*c$.

Dfn: $(R, +, *)$ is a commutative ring if $(R, *)$ is commutative.

Examples : (1) $(\mathbb{Z}/\mathbb{Q}/\mathbb{R}/\mathbb{C}, +, *)$ is a commutative ring

(2) $(M_{n \times n}, +, *)$ is a ring

(3) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

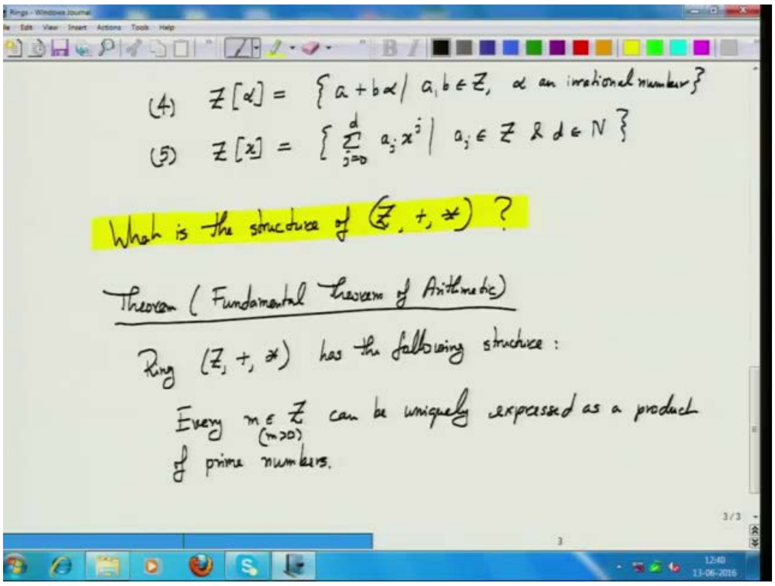
Of course, integers, rationals, reals, complex numbers, under addition and multiplication is a commutative ring. That is straight forward. That is where the definition comes from. I have got other examples; you have any other suggestions? Matrices, absolutely yes; if you look at, and there is this notation that is used here. Let us use M, n cross n to represent the set of all n cross n matrices, under addition and matrix multiplication is a ring. It is not necessarily a commutative ring. Because, under multiplication, the matrices do not, not all matrices commute; so, it is not a commutative ring. (Refer Time: 11:49)

Any other examples? That is very nice. So, what you are saying is, a plus i root 2. What is i? Square root of minus 1; so what is the set of numbers you are talking about? a is from integers, and i root 2? a plus i root 2 will not make sense. Probably, you mean a plus b root 2, where a and b are both integers.

So, that is indeed a ring. It is given a specific name Z bracket square root 2, and it is, contains numbers of the kind a plus b root 2, where a and b are integers. Why is this a ring? This requires lit bit of (Refer Time: 13:10). Firstly, it is group under addition. That is, that is clear. What is the additive identity as zero, and the inverse etcetera is (Refer Time: 13:27). Inverse of a plus b root 2 is minus a minus b root 2. So, it is clearly a group under addition. How about multiplicative property? Identity is 1, for multiplication; it is closed under multiplication. When you multiply to same number, you will get another number of the same kind. It is clearly associative just by virtue of being, these are all real numbers. And similarly, the distributive properties also hold. So, it is a ring.

In fact, instead of root 2, I can have something else also; I can have root 3.

(Refer Slide Time: 14:17)



(4) $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}, \ \alpha \text{ an irrational number}\}$

(5) $\mathbb{Z}[x] = \{\sum_{j=0}^{d} a_j x^j \mid a_j \in \mathbb{Z} \ \& \ d \in N\}$

What is the structure of $(\mathbb{Z}, +, *)$?

Theorem (Fundamental theorem of Arithmetic)

Ring $(\mathbb{Z}, +, *)$ has the following structure:

Every $\underset{(m>0)}{m \in \mathbb{Z}}$ can be uniquely expressed as a product of prime numbers.

Any irrational number, exactly; in general, I can have Z with alpha, a set of numbers a plus b alpha, a, b in Z, alpha, an irrational number. That is great. That is great progress. What about other examples? How about a set of polynomials? Let us say, polynomials in one variable. So, shall we say, Z bracket x; this is a polynomial in one variable. So, that is... where a j is in Z, and d is a positive integer. So, this is just a collection of all polynomials, with integer coefficients, in variable x. Is this a ring? Pretty obviously, yes, because, you can add polynomials; you can multiply polynomials.

Under addition, it clearly forms a group. Under multiplication, again, this expected properties of multiplication hold, and multiplication distributes over addition. That is, if you have polynomials p, q and r, then, p times q plus r, is the same as p times q, plus p times r. So, again, it is very simple, but nice example of a ring. And, the good thing is, we can already see this abstraction generalizing, and giving, spanning a number of different types of structures; polynomials, matrices, numbers, and numbers of different kind; you have this integer, rational, irrational number as well.

Student: (Refer Time: 16:49) polynomial multiplication (Refer Time: 16:51)?

Multiply two polynomials? Sorry?

Student: (Refer Time: 16:55)

Yes, yes, d is not fixed; d can be any positive integer. So, multiplying two polynomials of degree d 1 and d 2, will give us a polynomial of degree d 1 plus d 2; that is right; and, you are very right that, if you restrict, or put an upper bound on the degree, then, it ceases to be a ring; because of the same reason that, if you multiply two polynomials, their degree might exceed. So, these are some very typical examples of rings.

And, for rings, the central question again is, what is the structure of a ring? Just like, we had this, asked this central question about groups, what is the structure of a group. And then, we put in a large number of cases, explained the structure, that a group is several copies of a set. Not all groups, but like, finitely generated groups consists of several copies of the set, plus a small piece which is the finite group part; and, that also has copies of the kind Z p to the alpha, for different prime numbers.

So, in the same fashion, we can ask, what is the structure of a ring. And again, we will not be able to explain the structure of all possible rings; that can be very bizarre. But, we will be able to explain the structure of a fairly large class of rings, and the clue to that again starts from this, the real, original example of a ring, which is the ring of integers. Just like the group under addition for integers, in a sense, formed, or gave us, the canonical example of a group; and that group, we could find, or we can, we could express other groups into form of this z; several copies of z, or z quotient-ed with a subgroup. In the similar fashion, we should ask, what is the, I mean, what way is the structure of set of integers reflected, or found in other rings.

Are you following me? No? So, in case of groups, we found, after some investigation that, the group under, of integers, under addition, is perhaps the most basic type of group; the simplest type of group, with one generator. And then, we can express any finitely generated group as several copies of Z, right. So, in that sense, the group of integers was the simplest group possible, and other, more complex groups can be expressed in terms of this. So, the structure of the group of integers is found in, it is repeated, or copied, in multiple copies, in any finitely generated group.

And, we asked the same question for the ring of integers, that firstly, what is the structure of ring or integers? Structure of group of integers is pretty simple. Under addition, it is a single generator 1 that generates the entire group. So, we, now that we have two operations, we will again ask, what is the structure of the ring of integers, and then, ask the question, is this structure found in other rings as well? So, first question that we must ask is, what is the structure of the ring of integers?

Now, we have integers with both addition and multiplication operation. And, there is a very nice structure that has been found in this ring, which is called the fundamental theorem of arithmetic. This is something you have come across already that, every integer can be uniquely expressed as a product of prime numbers. So, what is the proof of this? Do any of you remember? Firstly, you, one has to define what prime numbers are; (Refer Time: 23:57) which are the numbers which have no divisors, except 1 and the number itself.

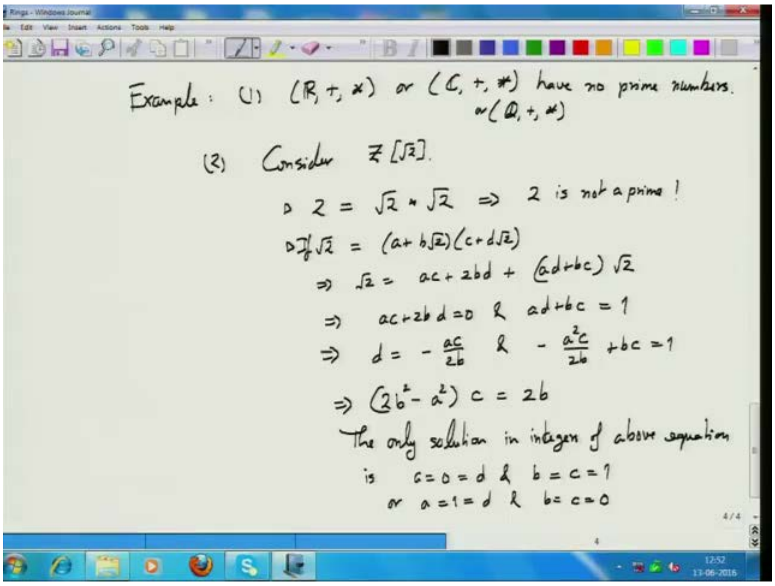
So, we are talking about the notion of division, which only exists partially, in case of integers. And, so, prime numbers are those which cannot be divided by any other number, except 1 and itself. And, you can write. Firstly, we can write every number as the product of prime numbers; that is the first step one needs to carry out to prove this. Can you do that? That should be easy; I will leave that to you. Do not have to think about it; you can, you have already done that in school, you can recall that proof.

Similarly, one can show that, if a number has more than one expression as a product of primes, these expressions, or the primes in these are the same. There cannot be two distinct ways of writing a number as a product of prime numbers. There is one thing which I forgot. Every m in Z, which is positive; a negative number, one has to multiply with minus 1, which is not exactly a prime number; and that, we have to also use in the product. So, every m in Z, m greater than 0, can be uniquely expressed as a product of prime numbers.

So, that is the basic structure of the ring of integers. And, we would like to know, if in a general ring, such a structure, or a similar structure exists. Let us take an example. Firstly, this structure will only exist in rings, where division is not fully available. If you look at a ring of rational numbers, there, there are no prime numbers. Why? Or, let us look at a ring of real numbers; I claim there are no prime numbers in it. See, the proof is very simple.

Suppose, the number a, which is a real number, is a prime, then, a by 2 is also a real number; and a is 2 times a by 2; so, it is certainly not a prime. So, there exists no real primes; or, in a ring of reals, there are no primes; in a ring of complex numbers, there are no primes; in a ring of rational numbers, there are no primes. And, the reason is the same in all three of them that, the division is available completely.

(Refer Slide Time: 29:24)



Example : (1) $(\mathbb{R}, +, *)$ or $(\mathbb{C}, +, *)$ have no prime numbers. or $(\mathbb{Q}, +, *)$

(2) Consider $\mathbb{Z}[\sqrt{2}]$.

▷ $2 = \sqrt{2} * \sqrt{2} \Rightarrow$ 2 is not a prime !

▷ If $\sqrt{2} = (a + b\sqrt{2})(c + d\sqrt{2})$

$\Rightarrow \sqrt{2} = ac + 2bd + (ad + bc)\sqrt{2}$

$\Rightarrow ac + 2bd = 0$ & $ad + bc = 1$

$\Rightarrow d = -\frac{ac}{2b}$ & $-\frac{a^2c}{2b} + bc = 1$

$\Rightarrow (2b^2 - a^2)c = 2b$

The only solution in integers of above equation is $a = 0 = d$ & $b = c = 1$ or $a = 1 = d$ & $b = c = 0$

So, you can divide any number by any other number, and get a third number. So, that is something we will not really be looking at, because, that does not quite mimic this, or cannot mimic the structure of the ring of integers. So, let us restrict the attention only to the rings, where division is not fully available. And, further, I will restrict attention to only commutative rings.

Okay, now, with this setup, let us go back to the examples we had listed. What was the example? 1 is already ruled out; 2 is not, because 2 is not commutative. What about 3? Yes, 3. Well, 3 is a subset of 4. So, 4 and 5, these are the two rings; in both these rings division is not fully available. So, let us consider Z with root 2 to begin with.

What is the structure of numbers in here? Does fundamental theorem of arithmetic hold? Well, in order to see if the fundamental theorem of arithmetic holds, we have to define the prime numbers. What are prime numbers in this ring? Is 3 a prime number in this ring? Or, let me ask you; is 2 a prime number in this ring? 2 should be a prime number in this one, why?

Student: (Refer Time: 30:41)

So, in order to show that 2 is prime, by definition, prime number is a number which cannot be divided, by any number, except 1 and itself. Now, for 2 to be a prime number, we have to prove that, in this ring, 2 cannot be divided by any other number, except 1 and 2. Is that true? It is not true. 2 is square root 2 times square root of 2; both, (Refer Time: 31:28) it is the same number squared, and square root 2 is an element, or is a number in this ring. So, 2 is not a prime in this ring. Root 2 is a prime; that is a good point. Is root 2 a prime?

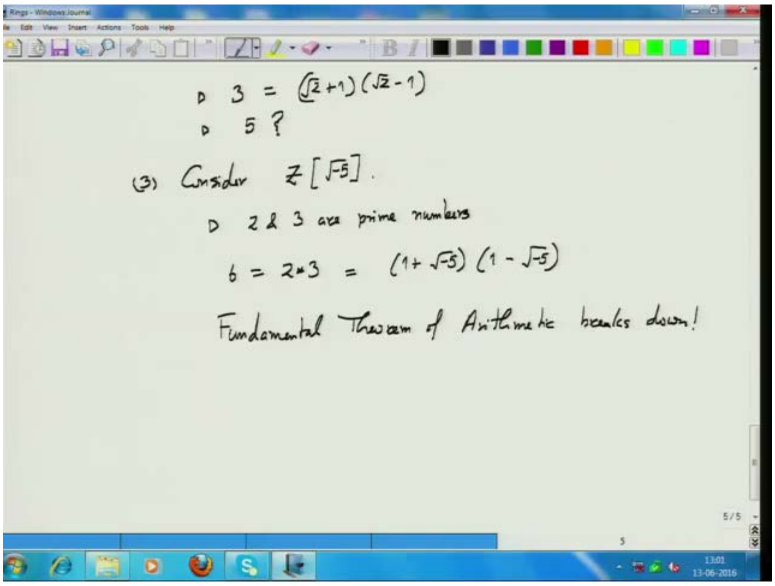
Suppose, root 2 can be written as a plus b root 2, times c plus d root 2; that is a general form of 2 numbers. And, in order to show that the number is prime or not, you have to just write it in this fashion, and see, if you can find values of a, b, c, d, that is fine. This implies that, root 2 is a c plus 2 b d, plus a d plus b c times square root 2. This implies that, a c plus 2 b d is zero, and a d plus b c is 1. So, just multiplying out the right hand side, and then, equating, this is an integer; this is also an integer times root 2.

So, if this is equal to root 2, then the integral part must be zero, and this multiplier of root 2 must be 1. So, what do we get out of this? This tells us that, d is equal to minus a c by 2 b, and here, we get, minus a square c by 2 b plus b c is 1; and, this gives us, b square, or, 2 b square minus a square times c is 2 b; and a, b, and c, all 3 of them, are integers. So, first, the right hand side is an even number. So, left hand side must also be an even number, which means a square c plus 2 b square c is an even number. So, a square c is an even number, which means either a, or c, is an even number.

So, now, we have to do some bit of slightly messy argument. If a is an even number, then, a square is a multiple of 4; correct? And, that would, that is ok, that is not a problem. b and c equal to, yes, and a and d to be 0; that will just give us that, that factorization; you are saying a and d are 0, b and c are 1; so that is square root 2 times 1; that is the solution. Sure, that is the solution. That is good to know.

Is that the only solution? That is the question. And, what I am claiming, and I will leave that to you to workout is that, the only solution in integers is a equals zero equals d, and b equals, c equals, 1. Or, the other way; or, a equals 1, equals d, and b, c are zero. And, this will show that, square root 2 is indeed a prime number. So, prime numbers do exist, but they look different; because, 2 is no longer a prime.

(Refer Slide Time: 36:42)



- $3 = (\sqrt{2}+1)(\sqrt{2}-1)$
- 5 ?

(3) Consider $\mathbb{Z}[\sqrt{-5}]$.

- 2 & 3 are prime numbers

$6 = 2*3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Fundamental Theorem of Arithmetic breaks down!

Similarly, 3 is not a prime number, because, 3, I can write as square root 2 plus 1, times square root of 2 minus 1. 4 is certainly not a prime; it is 2 times 2 (Refer Time: 36:54).

How about 5? Seems a prime? Seems a prime, yes; but, this is getting to be painful, in the sense that, we have to. Every element-wise, we, we have to go and see, and verify, if it is a prime, or not, it is going to be very difficult to really understand the structure of this. Can we come up with a more general result, saying (Refer Time: 37:46), this is a list of all primes. So, that is one question. I do not expect an answer from you immediately. But, fortunately, it is possible to list down the list of all primes in this.

And the way, again, we have to do it, listing first for Z bracket square root 2, then, for Z bracket square root 3, then, for Z bracket square root of 5. Again, that will be a painful process. Ideally, for any Z bracket square root of n, we would like to have a list of prime numbers; and, that is indeed possible. We can list down, come up with the expression for all the primes in such rings. That is, would resolve at least one question. But, the other question still remains unsolved. So, suppose we have the list of all primes. Is the fundamental theorem of arithmetic true? That is, every number can be uniquely written as a product of prime numbers; the answer is not necessary.

For example, let us consider Z and, let me give that correctly now; square root of minus 5. In this, one can show that, 2 and 3 are prime numbers. Z square root of minus 5 makes sense. It is same as Z bracket square root of 5i. So, it is a subset of complex numbers. In this ring, 2 and 3 happen to be prime numbers; and, the proof is again of the same kind; you just express it in terms of a general product, and see that the solutions are only trivial ones. But now, I can write 6 as 2 into 3. So, 6 is a product of 2 primes 2 and 3; I can also write 6 as 1 plus square root of minus 5, times 1 minus square root of minus 5. So, there is the problem.

Look, maybe, these are not prime numbers, one could say; 1 plus square root of minus5, maybe it is not prime. If it is not prime, it will factor further into prime numbers. And, this will also, may also, will also factor further into prime numbers. Eventually, all those terms, it will have at least 2 factors of primes. This will also have at least 2 factors of prime, but there is, in all, before at least four prime factors, whereas, in here, there are only 2 prime factors; but there is no way these 2 factorizations are the same. They are equal, but they are not the same.

So, the fundamental theorem of arithmetic breaks down here, and then, suddenly, there is a problem. Because, then, it is not clear, what exactly is a structure here. We have prime numbers here, but, we can write each number as multiple ways, in multiple ways as products of prime numbers; and that creates a problem. These are the questions that immediately arise. These are not, you know, very strange rings; these are simply, slight generalizations of the ring of integers. You put in one additional number, irrational number, in the ring of integers that gives you another ring, which is a slightly bigger set of numbers.

And there itself, the structure that existed in integers no longer exists. And, there is a major problem that arises, because, that structure does not exist anymore, studying rings of this kind becomes a challenge, because, we cannot have that. See, having a unique prime factorization is a very nice property. Any number, you can then write in terms of prime numbers, and study those prime numbers, prime factorizations separately. But here, there are multiple prime factorizations, and one prime factorization may give you one thing, and another prime factorization will give you another thing.

So, it is not clear what one should want. So, these are the challenges that immediately, almost immediately, came about, in, when we study the ring of integers. And, there is a very nice history, for which I have run out of time. So, I will tell you about it next time, about the, exactly, why and how these rings of integers, this additional (Refer Time: 44:06) rings of integers were discovered; and initially, actually, it was believed, without thinking much about it implicitly that, fundamental theorem of arithmetic will hold everywhere.

But, that lead to some very, like, certain consequences, which people believed to be true. And then, at some point, it was discovered that, fundamental theorem of arithmetic actually breaks down. And, if it breaks down, then all the earlier consequences were false.

So, that will form the beginning of the next lecture.