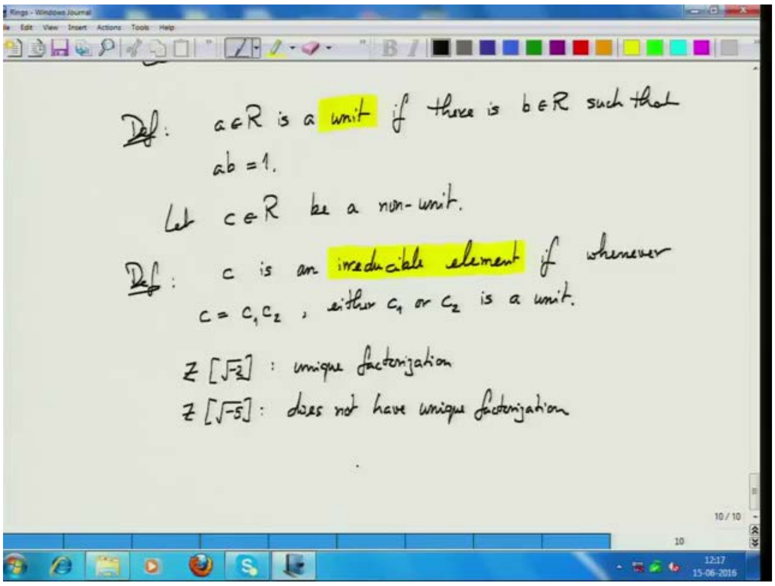
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 09
Rings: Birth of Ideals

So, today we will learn from the examples of last time and try to develop a theory which will allow us to understand how things actually factorize in rings and to set it up formally, I will go to the more general settings and then, define various quantities of interest that we have.

(Refer Slide Time: 00:53)



Def: $a \in R$ is a unit if there is $b \in R$ such that $ab = 1$.

Let $c \in R$ be a non-unit.

Def: c is an irreducible element if whenever $c = c_1 c_2$, either c_1 or c_2 is a unit.

$\mathbb{Z}[\sqrt{-2}]$: unique factorization

$\mathbb{Z}[\sqrt{-5}]$: does not have unique factorization

So, let us start with a general ring and I have said that we will be focusing only on commutative rings. So, this is what we have. The first thing when since we are interested in division that what are the elements that are divisible by, what other elements that essentially that the sense of prime factor addition of any number and that is what we want to see happening in this ring.

First thing we need to understand is what the elements that is divisible by something else. Now, one type of elements divide just about everything for example, if your ring r is a set of real numbers, in that case every number divides every other number. So, derivative there is very general and therefore, there is no concept of prime numbers there and so on. You had seen earlier as well. So, it is important to understand first that what are elements that are now that have an inverse present in the ring because if an element has an inverse present in the ring, in that case that element would divide every other element. So, let us formalize that.

So, we say that an element in the ring is a unit. If there is another element b in the ring, so that a b is 1 which is another way saying that b is the inverse of a. Now, if an element is a unit, then that element likes as a good divide every other element. We want to see c divide b is or c divided by a is same as c times b. So, if there is division available, so it is only with respect to non-unit elements that we can talk about factorizing them. So, let us c v and r be a non-unit ac.

I want to see if I can factorize c into c1, c2. There is c whether c equals c 1 c 2, there would be cs which I can factorize, there would be c which cannot factorize and that in for the case of integers that is the difference between a prime and compulsion components. So, let us give a definition to may a distinction of these two types of non-units. So, this non unit c we call an irreducible element if whenever we can write c as c 1 times c2 1 of c 1 is a unit.

Now, that is two things which are different in terms of if analogy with integers an integers. When we define a prime number, we say that whenever you see the prime whenever I write c as c 1 c 2, then c 1 or c 2 is 1 here. We are not insisting that c 1 c 2 be 1. We are saying that it should be a unit. Do you see a reason for that? There is a very simple reason that if you say c, if is try to mimic that definition, that is c 1 or c 2 is 1.

So, basically if there are see if ring has only one as unit or rather in integer scales, there are two units; 1 and minus 1. If the ring has no other unit, then this definition is the same. They call it unit or call it 1 or minus 1 is same, but if the ring has units other than 1 and minus 1, then we must use this definition otherwise I can always take any c. I can always write it as c times a b variant a is a unit because a b is 1.

So, c is c times a b and c times a b is equal to c a times b. So, I have managed to write c as product of two elements c, a and b neither of them is 1 or minus 1. So, that definition will completely fail to make any useful contribution. So, we must have a more general definition and this is the right one.

The second difference is I am not calling c a prime element. I am calling it an irreducible element and there is reason for it even though which is that prime numbers, I would keep associated with that unique factorization situation as prime number. We understand that in every number can be uniquely factored a product or prime numbers. So, I want to keep the main prime to be reserved for such structure.

In general that structure may not exist and that unique factorization we have seen. So, instead of calling such element c in this definition, prime element we will call it a irreducible element and once we have this unique factorization, then whatever terms, whatever numbers we have which admits such unique factorization or whatever irreducible elements which give rise to unique factorization will call them primes.

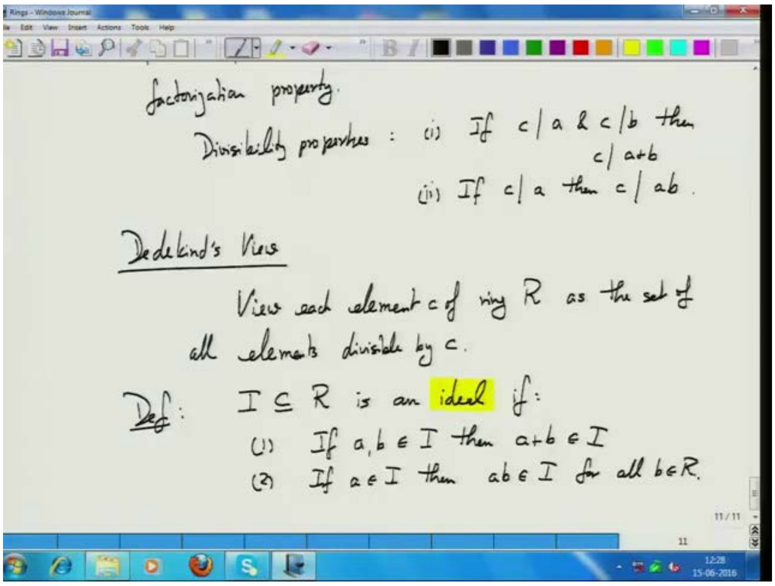
Now, we know that certain rings have unique factorization property which means do not and typical examples are living a side integer. We have z square root of minus 2. This has unique factorization and z square root of minus 5 does not have and the target remains the same. How do we restore or bring in that unique factorization property in all of these rings and more at just these rings.

So, this like a describe last time, this problem allows initially people thought that all such rings have unique factorization which came up with the problem in terms for prove Fermat's last theorem. So, then such rings were relooked at, some rings had unique factorization, some did not and there is a mathematician I mentioned last time Kummer who was the first one to address this issue and he wanted to see how can we restore unique factorization.

So, what he said was that for example in square root minus 5. We have two times 3 equals i plus square root of minus 5 times i minus square root of minus 5 and these happened to be irreducible elements. Now, I will use the terminology ad justified 231 plus square root of minus 5, 1 minus square root of minus 5 are irreducible elements in this ring. So, it cannot be factored further. What Kummer said was that is because there are some other numbers into which these number factor, but those numbers have not present in this ring z square root of minus 5.

So, he postulated these additional numbers and said that these numbers all they are irreducible in this ring. They do factor in terms of these other numbers and then, the unique factorization property occurs. So, he developed that theory and gave this mysterious other numbers.

(Refer Slide Time: 12:43)



factorization property.

Divisibility properties : (i) If $c | a$ & $c | b$ then $c | a+b$

(ii) If $c | a$ then $c | ab$.

Dedekind's View

View each element c of ring R as the set of all elements divisible by c.

Def: $I \subseteq R$ is an ideal if:

(1) If $a, b \in I$ then $a+b \in I$

(2) If $a \in I$ then $ab \in I$ for all $b \in R$.

The name ideal numbers, but what are these ideal numbers have in it? Where are they? They are nothing, but this ring z square root of minus 5. So, one has to bring them in from outside. What are their properties? All these sorts of question arise. What Kummer said was that look at these numbers are number that divide 2, 3, 1 plus square root of minus 5, 1 minus square root of minus 5.

For example, these numbers are of the kind where they satisfy the typical divisibility properties. What are typical divisibility properties? If a number divides the two primarily properties, first one that if c divides a and c divides b, then c divides a plus b and second if c divides a, then c divides a b. So, he said that these are the ideal numbers which divide the real numbers.

The numbers we are start with and they divide the division for these properties and then is were developed this theory to show that the unique factorization property would hold when you include such ideal numbers, but the whole thing was kind of unsatisfactory where examiner you can always has where exactly are these ideal numbers coming from, what really is there connection with the actual numbers. We start with since to be little you know it seems as if it is been pushed. These are concepts as in pushed to just fix this unique factorization property. Therefore, it was not very satisfactory.

Now, after Kummer another mathematician also very famous Dedekind, actually we have heard of his name Dedekind made a simple change of prospective and with that simple change of prospective, he could very nicely set the whole thing up. He could reconcile what really means by ideal numbers and what are the actual numbers, how do they interact with each other, how are they related to each other, exactly how are they coming, everything very nicely explained and this all followed by a very simple general prospective which was following what Dedekind said which I will call Dedekind's view and since we are interested in divisibility primarily. So, his view was treat each number not as a number percent. Of course, it is number, but I will adopt different view which is to view each number has a collection of numbers which are multiples of this.

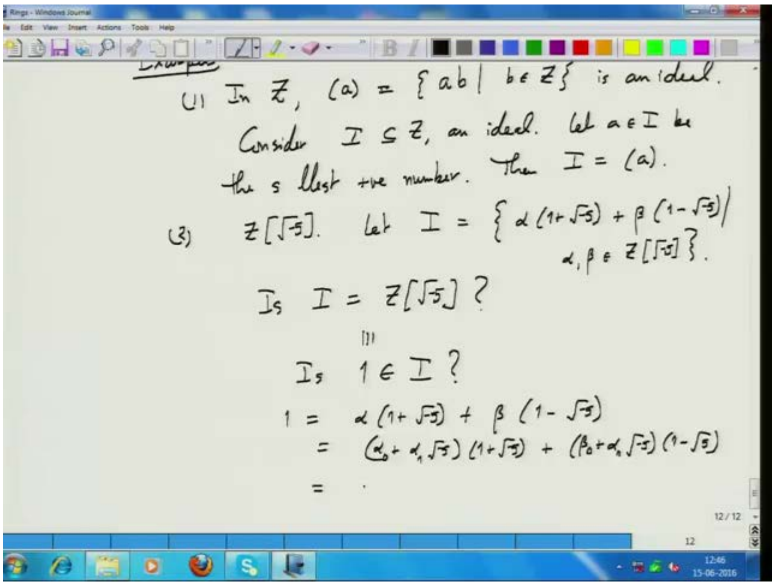
For example, take the number two in integers over integer, let us just I can view it just as a number two alternately. That is a Dedekind's view that represent number two as a set of all even numbers thus because that set is precisely set of all numbers which are divisible by 2. Similarly number 3 is viewed as set of all number which are multiples of 3, 4 with the set of all numbers which are multiples of 4.

So, it seems like a very unnecessarily complicated way viewing a number which it is in case of integers, but this view helps resolve this mystery of ideal numbers very nicely. So, at the cast of introducing this additional complexity, we are able to gain something. So, let us adopt that view and we give a name to not this is just to one element view, but I will generalize now this definition length in step to a very nice generalization which is the form we call a set i which is a subset of elements of the ring r.

If it satisfies these two properties that if two elements a b are in i, then there is some a plus b. If an element is i, then a times b for any b in r is i. So, this set i actually if you just cope to that divisibility properties precisely captures that. So, this set i, therefore is representing some number. It is representing a set of numbers which have let us say in some nice way it is divisible by one, may be more than one numbers that is something that we will see later on, but if you just compare the divisibility property with i that is precise and the advantage here is that we then in definition of i, we do not have to say there all the elements are multiples of some c.

If all the elements are multiples of say c, then certainly it satisfies these two properties, but this is more general and in fact that difference is very important in our calculations later on. So, what are ideals of a ring see some examples.

(Refer Slide Time: 22:10)



Examples

(1) In $\mathbb{Z}$, $(a) = \{ab \mid b \in \mathbb{Z}\}$ is an ideal.

Consider $I \subseteq \mathbb{Z}$, an ideal. Let $a \in I$ be the s llest +ve number. Then $I = (a)$.

(2) $\mathbb{Z}[\sqrt{-5}]$. Let $I = \{\alpha(1+\sqrt{-5}) + \beta(1-\sqrt{-5}) \mid \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$.

Is $I = \mathbb{Z}[\sqrt{-5}]$?

$\Updownarrow$

Is $1 \in I$?

$$1 = \alpha(1+\sqrt{-5}) + \beta(1-\sqrt{-5})$$
$$= (\alpha_0 + \alpha_1\sqrt{-5})(1+\sqrt{-5}) + (\beta_0 + \alpha_1\sqrt{-5})(1-\sqrt{5})$$
$$=$$

In z the ring of integers, all multiples of a number are ideals. So, I will denote this notation a with in a bracket to represent the set of all multiples of a and this notation I will use in general for general rings, not only for z are there ideals in z. The answer is no these are the only ideals in z and the proof is also straight forward. In z there is a smallest number in this ideal, I consider the smallest number let i be the smallest. Let say positive number i claim that this ideal is simply all multiples of a.

Suppose there is a number which is not multiple of a and in that case you can write g c d of let us say that number will b which is not a multiple of a, take the g c d of a m b, that is a number smaller than a. The g c d by extended Euclidean algorithm if you remember can be written as a times alpha plus b times beta. Now, since a and b are both in the ideal a times alpha is in the ideal b times beta is in the ideal and there sum is also in the ideal. So, means a g c d of a and b is also in the ideal i which is number smaller than a. That is not possible. So, it follows that the ideal is simply all multiples.

So, in integers the ideals are exactly i just changing the view there exactly numbers the Dedekind's know. In Dedekind's view we are identifying number with all the multiples of that number which is ideal and in integers the ideals are in one to one correspondence with numbers. Let us go to a more interesting case. How about z square root of minus 5 say let us look at these number as say 1 plus square root of minus 5, 1 minus square root of minus 5. Let me consider the following case. Let us define an ideal i that is the slightly complex definition.

Student: One of.

One is in this one is not in this two is in this. So, it contains all even numbers. Surely it contains all multiples or even multiple of square root of minus 5. That is also true. So, we can write it, but that is nice observation. We can write it as also as alpha 2 alpha plus to beta, beta square root of minus 5 for alpha beta and z. Why? It is because 2 alpha is in this. So, we want to show that any element in this set is in this set and element in this set is in this set that you can derive very easily, but one thing I need to explain now to be that this further I can simplify it even more. It is 2 alpha plus 2 beta square root of minus 5, where alpha-beta are simply integers.

So, this is a more presumably restricted set than this alpha and beta can be any numbers and z square root of minus 5 here alpha beta are only integers, but it follows pretty simply by the fact no matter what alpha beta are in z square root of minus 5, you substitute that in here multiply it out, collect the coefficient of square root of minus 5. One side coefficient of let us say just an integral part on the other side.

Both these numbers would be even why because everything here is even you start with there is a multiple to multiplier of 2 here. There is a multiplier of 2 here. So, it is two times alpha plus beta as square root of minus 5, two times alpha plus beta was square root of minus 5, where alpha beta are also in z square root of minus 5. Any arbitrary element you can get by this fact of z square root of minus 5, but since there is a multiplier 2 sitting outside that make every component and even integer. This is not clear where this out. I will leave this as a very simple exercise. What is important right now to observe is that this ideal, this is an ideal first we have not even show this an ideal lecture.

Student: (Refer Time: 29:50)

Two numbers of this form when you add; they still remain in this form. So, this is an idea and we can simplify this ideal to this expression now. So, this is an ideal of z square root of minus 5. The next question I am going to ask is, is there a number in z square root of minus 5, is this ideal expressible as all multiples of some number of a?

Student: t d plus square root of minus one, that is.

T3 plus square root of minus 5, not in this.

Student: Second information is 2 alpha plus 2 beta minus 5. All 5 equal to 3. Alpha should be 3 by 2.

Yeah, that is not allowed.

Student: (Refer Time: 31:22)

So, 3 plus square root of minus 5, not in this ideal, so are you saying that these two equalities do not told?

Student: Two elements (Refer Time: 31:33) minus 3.

1 plus square root of minus 5, so what I have done is wrong, sorry. So, let me erase all of these. I had something else in mind that I wanted to show here. Sorry good that you pointed out. So, let us get back to this idea. Let just try to understand this first question does this ideal contain all elements of this ring.

This question is same showing or is answering the question is one in the ideal i because if ideal contains the entire ring, then of course one is in the ideal. If one is in the ideal, then all multiples are in the ideal and all multiples of one are (Refer Time: 32:36). So, is one in this ideal i? If 1 is in the ideal i, then we will have 1 equal to some alpha, 1 plus square root of minus 5 plus beta 1 minus square root of minus 5 which is alpha plus beta plus alpha minus beta square root of minus 5, right. So, this may alpha must be equal to beta.

Student: Alpha, alpha and beta is.

(Refer Time: 33:20) square to minus 5, yeah I am treating them as integer which is wrong. So, we will have to express alpha itself as an element of z square root of minus 5 which is alpha 0 plus let us say alpha 1 square root of minus 5 and this I can write as I just collect the coefficients together alpha 0 plus beta 0 minus 5 alpha 1 should beta 1 plus 5 beta 1 and then, plus alpha 0 plus alpha 1 plus beta 0 minus beta 1, right. So, what we thus this have a solution four integers? No, first look at this; this must be equal to 1. How can this be equal to 1? This is a multiple of 5 alpha 1 plus beta one times 5 and this is alpha 0 plus beta 0.

Student: Sir. So, beta equal to alpha.

Beta 1 equal to this.

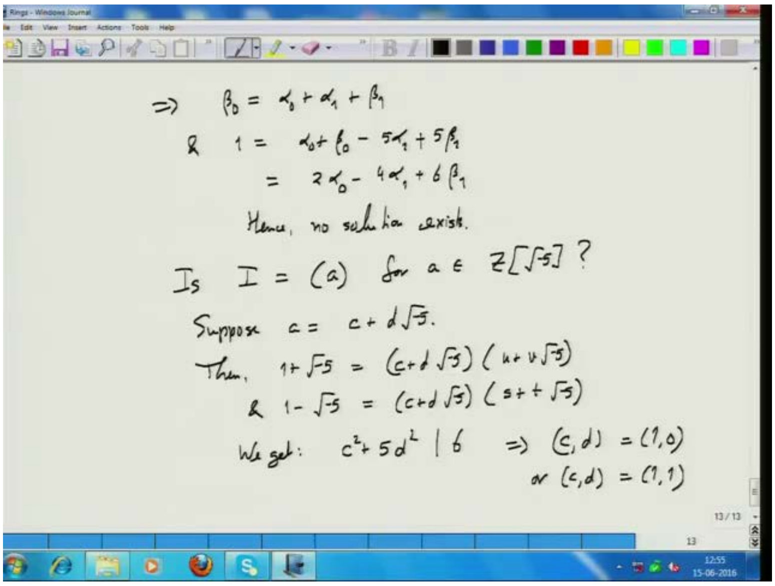
Student: Yeah.

OK.

Student: Then the (Refer Time: 35:26).

Let us do that. It is a good point, so not this.

(Refer Slide Time: 35:35)



$$\Rightarrow \quad \beta_0 = \alpha_0 + \alpha_1 + \beta_1$$

$$\& \quad 1 = \alpha_0 + \beta_0 - 5\alpha_1 + 5\beta_1$$

$$= 2\alpha_0 - 4\alpha_1 + 6\beta_1$$

Hence, no solution exist.

Is $I = (a)$ for $a \in \mathbb{Z}[\sqrt{-5}]$?

Suppose $a = c + d\sqrt{-5}$.

Then, $1 + \sqrt{-5} = (c + d\sqrt{-5})(u + v\sqrt{-5})$

& $1 - \sqrt{-5} = (c + d\sqrt{-5})(s + t\sqrt{-5})$

We get: $c^2 + 5d^2 \mid 6 \quad \Rightarrow (c, d) = (1, 0)$

or $(c, d) = (1, 1)$

So, the conclusion is that beta 1 equals alpha 0 plus alpha 1 plus beta 0 and1 equals alpha 0 plus beta 0 minus 5 alpha 1 minus 5 beta 1, alpha 0 plus beta 0 minus 5 alpha 0 minus 5 alpha 1 minus 5 beta 0 and that equals.

Student: (Refer Time: 36:14)

Sorry.

Student: (Refer Time: 36:18)

The something.

Student: Minus beta 0 to.

This one.

Student: (Refer Time: 36:24)

Said again this would be plus.

Student: (Refer Time: 36:30)

This one, you cannot see? There now you cannot see there. So, which are you talking about? So, just read out the law.

Student: Minus 5.

The part, yeah, alpha 0 plus alpha 1.

Student: (Refer Time: 36:50)

Plus beta 0, yes correct, and minus beta 1.

Student: (Refer Time: 36:57)

Minus beta 0, why would that be 1? Thus should be minus.

Student: Beta.

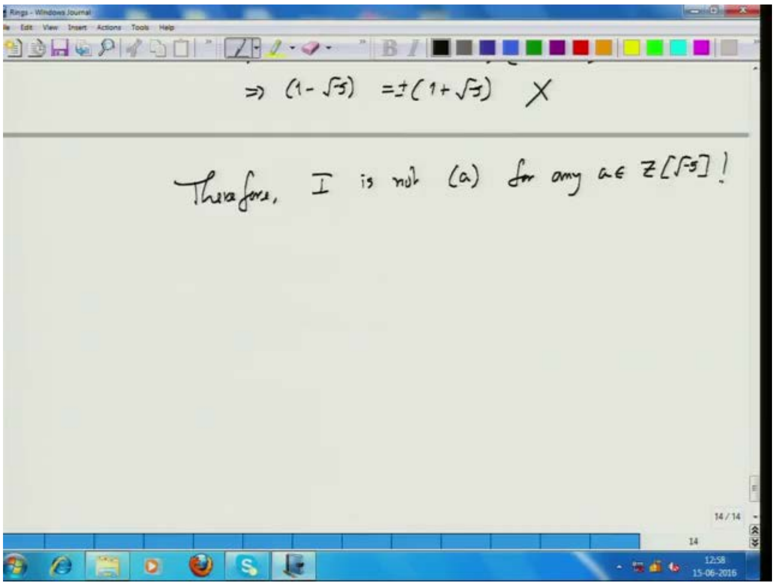
Beta 1 would be plus minus beta 0 plus beta 1, you are right. So, beta 1 therefore is or it is a beta 0 or is changes to beta 0 to be equal to beta 1 and 1 equals alpha 0 and this is clear. Then, this replaces this is this and that is not possible. There is no solution possible because this right hand side and even left hand side. So, surely this ideal contains elements does not contain 1.

Now, the next question which is through what I am leading is can this be express as multiple of some let us assume that let us try to work this out. Suppose, a equals c plus d square root of minus 5, then 1 plus square root of minus 5 is c plus d square root of minus 5 times something else, right. Let us say yes both 1 plus square root of minus 5 and 1 minus square root of minus 5 are multiples of c plus d square root of minus 5, right.

Now, let us see what the best going this if you take the norms, the norm on this side would be 6. So, c the norm of this must divide 6 and since this is 6 norms of these two are the same norm of this must divide 6. So, let just see what is now this is c square plus 5 d square this divide 6. So, what are the possibilities and where very few it could be d could be 0 and then, see must be 1, then it is fine or up d could be 1 in that case c must be also 1.

So, if c d is 0, then this is just 1 and a is 1 which is certainly not the case. There is this ring i or ideal i is not or multiples of one which does not true. We have already seen it 1 means it is this number itself 1 square root of minus 5. So, 1 plus square root of minus 5, sure I can write it as 1 plus square root of minus 5 times this and we are saying that ideal i is simply all the elements generated by 1 plus square root of minus 5.

(Refer Slide Time: 42:28)



$\Rightarrow (1-\sqrt{-5}) = \pm(1+\sqrt{-5})$ X

Therefore, I is not (a) for any $a \in \mathbb{Z}[\sqrt{-5}]$!

Then, we come to this point, however this 1 minus square root of minus 5 is it can it be written as 1 plus square root minus 5 times s plus t square root of minus 5. Why is this possible? Again if you go back take the norm, this is 6. So, this norm should be 1 which was s square plus 5 t square must be 1 which means t must be 0 which mean s must be 12 plus minus 1. So, this is just plus minus 1. This is certainly not true. That is false and therefore, we can conclude.

So, here is an ideal which is slightly funny one. It does not quite correspond if you look at the Dedekind's view. This ideal does not correspond to any number in the ring because numbers correspond to the ideal which has collection of all multiple of that number. Here is an ideal. It is an ideal in that ring, but does not correspond to any number. So, what is this and it turns out this is what in the Dedekind's view this is what Kummer ideal numbers where there is those ideal number that we brought in from outside with certain property.

It will restore the unique factorization property. Once you to adopt the Dedekind's view, those ideal numbers are ideal of this kind which is not multiples of a single number and with the help, now it can keep with the Dedekind's view, we can write any number. Now, a number in the Dedekind's view is an ideal of certain kind which is (Refer Time: 45:33).

So, any number slash ideal has a product in the unique way of certain type of number slash ideals through I need to define the product of ideals and this is just an essentially translate the arithmetic of numbers. However, numbers to arithmetic over these ideal which is Dedekind’s view that I will do next time and then, we can see that everything will focus particularly on this example of that square root of minus 5 because we know that unique factorization does not hold here. You know that 2 times 3 is equal to 6. Factorization in two different ways, so will see how using these ideals we can restore the unique factorization property.

Once we define the arithmetic over ideals and once we understand that, then we will get it. I will just take the more general structured theorems for enlarge class of rings which are called in to honor the work of Dedekind’s. They are called Dedekind rings. Those are rings which precisely admit that this unique factorization in terms of ideals.

So, that is the plan for the next class.