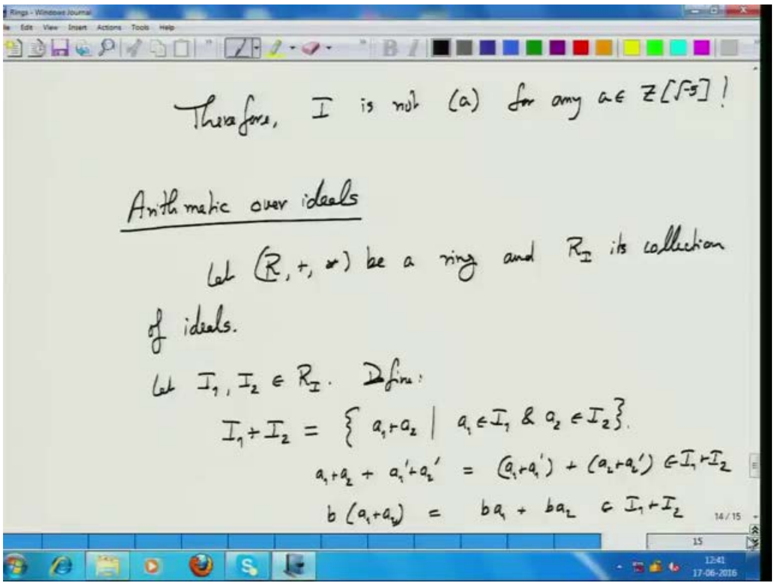
Modern Algebra
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture – 10
Rings: Ideal Arithmetic

Let us continue from the last lecture where I left of by our highlighting or some questions that we need to resolve about ideals before we can start doing arithmetic in terms of ideals completely instead of doing it in terms for numbers. In order to do arithmetic over ideals we have to define arithmetic over ideals, will let us do that first.

(Refer Slide Time: 00:45)



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

Anthmatic over ideals

Let $(R, +, *)$ be a ring and R_I its collection of ideals.

Let $I_1, I_2 \in R_I$. Define:

$$I_1 + I_2 = \{ a_1 + a_2 \mid a_1 \in I_1 \ \& \ a_2 \in I_2 \}.$$

$$a_1 + a_2 + a_1' + a_2' = (a_1 + a_1') + (a_2 + a_2') \in I_1 + I_2$$

$$b\,(a_1 + a_2) = ba_1 + ba_2 \in I_1 + I_2$$

As usual we start with a commutative ring and let us collect all the ideals of this ring in the set R sub I. Now we are treating each ideal as an element, and now you like to do arithmetic exactly as we do over ring. We again have to go through the properties of the ring and see those properties hold here. It must be commutative group under edition that is the first thing we need ensure. So, the first step is to define edition of ideals.

Let us say you have two ideals n R I. And the definition is as you would expect in the most natural way, that edition of the two ideals is simply edition of elements of ideal I 1 plus I 2 is contains all the elements of the form a 1 plus a 2, where a 1 is an I 1 and a 2 is an I 2. Now the result must be an ideal of the ring that is very important. So the question is, is this set an ideal of the ring. Think about it, answer is straight forward. It is deed an ideal of the ring, why? For ideal property we have to satisfy two conditions, there if you have two elements from I 1 plus I 2 there is some must also be in the same idea. If a 1 plus a 2 plus a 1 prime plus a 2 prime these individually are elements of this ideal then there is some is I can write as a 1 plus a 1 prime plus a 2 plus a 2 prime, a 1 plus a 2 prime is in I 1 a 2 plus a 2 prime is in I 2 and so there is some is in I 1 plus I 2.

The second property is that, you multiply any element b from the ring to an element a 1 plus a 2 of this set the result must be any how I 1 plus I 2. And this also seen very easily b times a 1 plus a 2 by distributive property of multiplication is b a 1 plus b a 2. Now since a 1 is an I 1 b a 1 also an I 1, similarly b a 2 is an I 2, I 1, I 2 being ideals. So this is an I 1 plus I 2. We have defined edition of ideals very simple.

So, this not only defines the edition also shows the closure property of edition. Now we have to verify other properties commutative is straight forward, is just because ring edition itself is commutative so I 1 plus I 2 is same as I 2 plus I 1. Then identity, what is the identity here that is important. What is the identity? Identity must be an ideal, the additive identity was 0. So, what should that ideal be?

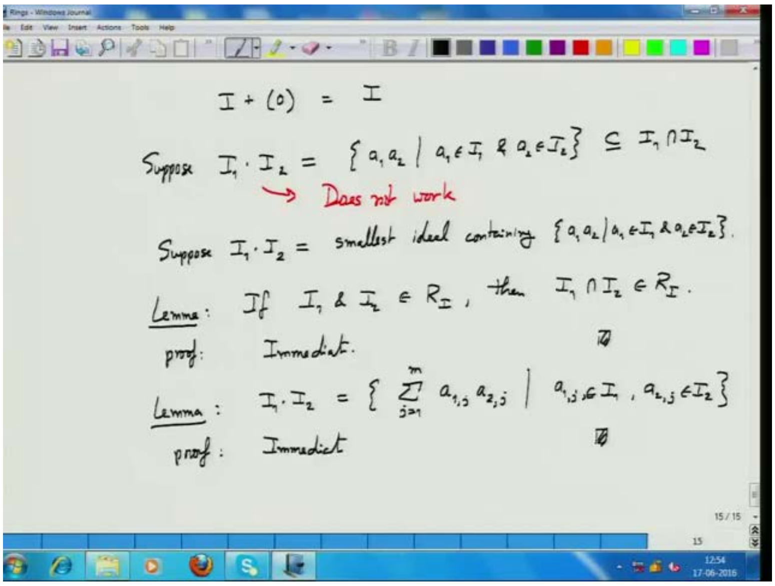
Student: Ideal of 0.

Ideal of 0; what is ideal of 0? Yes. What does it contains.

Student: Singleton set.

Single Singleton just a 0, absolutely.

(Refer Slide Time: 05:51)



$$I + (0) = I$$

Suppose $I_1 \cdot I_2 = \{ a_1 a_2 \mid a_1 \in I_1 \ \& \ a_2 \in I_2 \} \subseteq I_1 \cap I_2$

→ Does not work

Suppose $I_1 \cdot I_2 =$ smallest ideal containing $\{ a_1 a_2 \mid a_1 \in I_1 \ \& \ a_2 \in I_2 \}$.

<u>Lemma</u>: If I_1 & $I_2 \in R_I$, then $I_1 \cap I_2 \in R_I$.

proof: Immediat. ☒

<u>Lemma</u>: $I_1 \cdot I_2 = \{ \sum_{j=1}^{m} a_{1,j} a_{2,j} \mid a_{1,j} \in I_1 , a_{2,j} \in I_2 \}$

proof: Immediat ☒

So I plus 0, this is the ideal of 0 this is the 10 notation I defined earlier. This is I because you are just adding 0 to every element of I which is I, that is done. So, identity is defined, now how about the additive inverse; inverse of?

Student: I (Refer Time: 06:25).

I is inverse which are.

Student: (Refer Time: 06:29) element (Refer Time: 06:38).

Yes.

Student: (Refer Time: 06:40).

Why?

Student: Since that I 1 plus I 2 contains I 1.

I 1 plus I 2 contains I 1.

Student: Because 0.

Because 0 is belongs to any ideal, is that correct.

Student: but then it inverse if we want if you want to find (Refer Time: 07:17).

Now there is a problem with inverse, 0 does belongs to every ideal. You see 0 times and element is 0 and that must belong to the ideal. Similarly your minus same has to also belong to the ideal, because you are multiply with minus 1 every element that should belong to ideal so a belong to ideal minus a also belong to the ideal. Then I is I inverse there is I plus I is 0, it is not.

Student: (Refer Time: 07:58).

I plus i (Refer Time: 08:00) it will contain 0 is not 0. We have a problem that this is not really a group under edition, it has closure, it has commutativity, associativity also pretty much follows, it has an identity, but it does not have any inverse. So, that is something we lose already.

Fortunately it is not a big loss, because you see why we are interested in looking at the ideals, to get the uni factorization. The situation here in terms for ideals is same as the situation of positive integers, sort of positive integers or non negativity integers as I should say they also do not have inverse, but the prime factorization does hold over the set up non negative integers. So, we do not really need the additive inverse for the carrying out the prime factorization kind of operation. We do not worry about it we have require (Refer Time: 09:43) property that we need. So, that is what the edition word says.

Now multiplication of ideals, how about that? How do we define multiplication of ideals? If you try to define let us say I 1 times I 2 is in the exactly the same way a 1 a 2, where a 1 is an I 1 and a 2 is an I 2 and let us ask the question is this an ideal.

Student: (Refer Time: 10:31) I 1 is (Refer Time: 10:34).

I one is (Refer Time: 10:37) by multiplication. So this is contained in I 1 surely, it is also contained in I 2 that is very correct. This is contained in I 1 intersection I 2. That is the good observation, but is it an ideal.

Student: the form I 1 is the minimum element is within the ideal (Refer Time: 11:01) into the minimum element is within the ideal (Refer Time: 11:06) multiplication of that (Refer Time: 11:08).

If there is a minimal layer element representing here, but we have seen last time that is not true for all ideals.

Student: (Refer Time: 11:19).

Exactly, that is the problem. You multiply any element of the ring to this you stay within this that is not a problem, but if we add two element of this a 1 a 2 plus a 1 prime a 2 prime is not clear if it is I 1 in this set. This definition does not quite work. So, how do we define the product of two ideals? Suppose we define it in this way, this is cheating actually. This is forcing the product to be an ideal just by saying look at, I would like in I 1 times I 2 this ideal to contain all products a 1 of the form a 1 a 2. But that set may not be ideals, so let us pick up the smallest ideal that contains this set and define that to be I 1 dot I 2.

Question is, is this definition sensible, is there really any smallest ideal or are there multiple ideals containing this in the set which are not really comparable to each other. Fortunately, we have a lemma which says that if I 1 and I 2 are in R I and their intersection is also an ideal. Why? Again proof is very simple.

Student: If 2 element (Refer Time: 14:12).

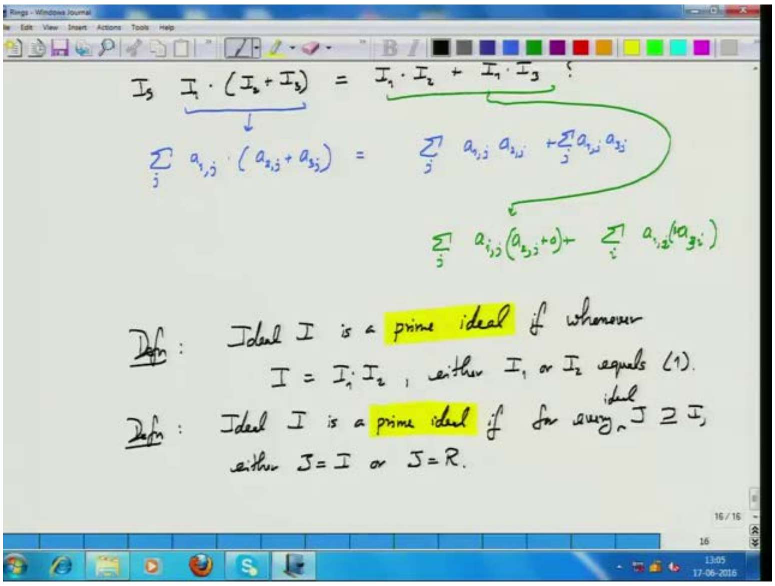
If two elements are in the intersection I going to say to there sum is also in the intersection, because they these two elements are in I 1 as well as in I 2 so there is sum should be in I 1 as well as in I 2. Similarly, take any element of the ring b and multiplied within element of a I 1 intersection I 2, since it is an I 1 so the product will be an I 1, since it is an I 2 the product will be an I 2. Therefore, it is in both I 1 and I 2. The proof is immediate. And this lemma ensures that there is indeed smallest ideal that contains this set, because there are more than one ideal containing the set their intersection will also contain the set and that is also an ideal which is the smaller ideal than these two individual. So, you can keep taking intersections, essentially take all ideals that contain the set take their intersection that is an ideal which is (Refer Time: 15:23) the smallest ideal containing.

There is another very nice characterization of this ideal I 1 dot I 2. It is the elements of the following form which are finite sum of product of a elements of I 1 I 2. And now you can directly verify that it is an ideal. Take two elements of this form add them that will also be elements of this form multiply any outer element of the ring to an element of this form that will be an element of this form. It certainly is an ideal. It certainly contain the set and is the smallest set containing this, because if this is contained in any ideal all finite sums of element of this form must also be contain in that ideal. Because that ideal must be closed under edition, so certainly this is also contained in that ideal. Now this proof is also immediate. So, that is multiplication of ideals.

Student: (Refer Time: 17:29).

That is a good question. Not always, this is always contained in I 1 intersection I 2. Why? Because this is contained in I 1 intersection I 2, I 1 intersection I 2 is an ideal and this is the smallest containing the set, therefore this ideal is containing I 1 intersection I 2. But, it may be equal to I 1 intersection I 2 it may not be equal to. So we have now the definition of multiplication of ideals. Now again we need to verify the properties of a multiplication and see for multiplication what is the closure is already defined, commutativity is clear, associativity is clear, how about the identity, what is the identity here?

(Refer Slide Time: 18:45)



$$I_s \quad \underbrace{I_1 \cdot (I_2 + I_3)}_{\downarrow} = \underbrace{I_1 \cdot I_2 + I_1 \cdot I_3}\ ?$$

$$\sum_j a_{1,j} \cdot (a_{2,j} + a_{3j}) = \sum_j a_{1,j}\, a_{2,j} + \sum_j a_{1,j}\, a_{3j}$$

$$\sum_j a_{i,j}(a_{2,j} + 0) + \sum_i a_{1,2}(1a_{3i})$$

Defn : Ideal I is a prime ideal if whenever $I = I_1 \cdot I_2$, either I_1 or I_2 equals (1).

Defn : Ideal I is a prime ideal if for every ideal $J \supseteq I$, either $J = I$ or $J = R$.

The whole ring yes, actually I one multiplied with 1 is I. This ideal is equal to the whole ring. Whenever, 1 is in an ideal then that ideal equals a whole ring because then you multiply every element of the ring you get those elements. So, this is the unit of multiplication. And for multiplication we any way do not need an inverse so we have quite fine with that. The final property is a distributivity of multiplication over edition. We have to see that I 1 times I 2 plus I 3, what this; is this property hold.

Student: (Refer Time: 19:46).

Yes. Let us just write down what is the general element of this. General element of this would be a 1 or sigma yes j a 1 j times.

Student: a 2 j.

A 2 j plus a 3 j correct. This is just multiply out and you get sigma over j a 1 j times a 2 j plus a 1 j a 3 j. This is an element of I 1 I 2 this is an element of I 1 I 3, so all the elements of this are contain in this. How about the other way round, same way? So let us take a general element here, let us use a different colored pen. This is sigma over j, a 1 j, a 2 j plus sigma over i a 1 i, a 2 i sorry a 3 i. Can I write it in this form? No, cannot write. Why not?

Student: Answer is one element (Refer Time: 21:48) is not necessary (Refer Time: 21:50)

That derivative is common here and here, but that is the simple trick to around this. Just write this as plus 0, 0 plus, and then add combined these two sums. This is an element of I 2 plus I 3, this is also an element of I 2 plus I 3, and then you are multiplying elements of I 1 and summing up there is a finite sum. Let us just say very trivial way of ensuring and this is a point. So that establishes this distributivity property and that is very crucial, because when you factoring out that is there is something (Refer Time: 22:50).

Good, so we have now established arithmetic over ideals. And since we have established arithmetic over ideals we can talk about given an ideal writing it as a product of other ideals. We in order to complete the picture we also would need to define the notion of prime ideals. That is what we would want that prime ideals should be one which are cannot be factored into smaller ideals. So, what is should that definition be? Make a guess.

Student: (Refer Time: 24:06).

Yeah, whenever.

Student: (Refer Time: 24:25) I 1 I 2 is a ideal of 1.

(Refer Time: 24:030) I 1 and I 2 that are good guess. Does this make sense? Let us mimics the property of prime numbers. There is another way of defining prime ideals, which is I is a prime ideal if every ideal ideal I which contains I either J is equal to I or J equals the (Refer Time: 26:02). This is somewhat not so intuitive definition of a prime ideal. What is the relationship if any between these two, can you think about it.

Student: when we saying I equal to I 1 plus I 2 then I 1 and I 2 are superscript of (Refer Time: 26:27).

I one and I 2 are.

Student: I mean I 1 and I 2 are (Refer Time: 26:35).

I 1 times I 2.

Student: (Refer Time: 26:40) if I is equal to j k then (Refer Time: 26:46) j equal to i (Refer Time: 26:49).

If I is equal to j k then.

Student: j is equal to I or R.

Yes.

Student: (Refer Time: 26:57).

Yes.

Student: (Refer Time: 27:01)

I will give this as a small exercise for you to work on. In the next class we will come back to this, because I want you to think a bit about these types of reasonings and see what you come up with.

Student: when I 1 and I 2 contain from the previous definition I 1 and I 2 is the subset of I 1 (Refer Time: 27:34).

I 1, I 2 is both subset of I as well I 1 as well as I 2.

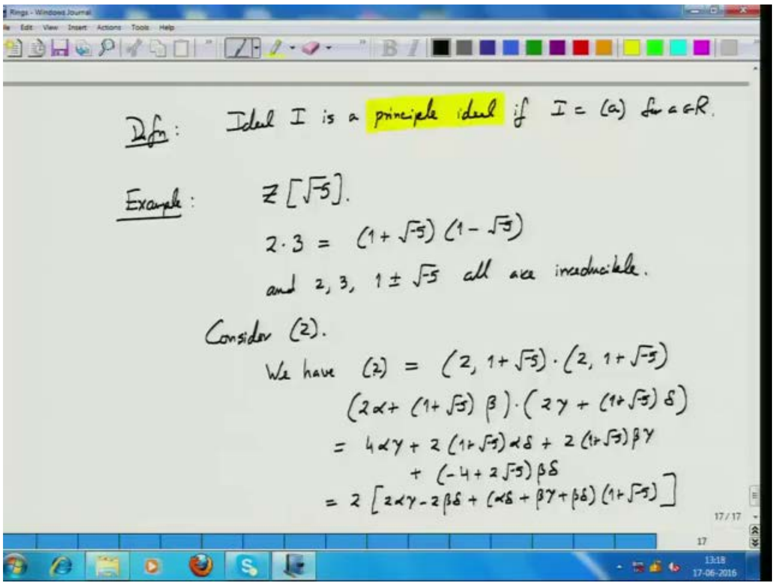
Student: I 2.

Yes

Student: So we can say that it is either subset of I or subset of I and subset of R

Work it out. Think about it at leisure, we are meeting tomorrow again so we will continue with this tomorrow morning. In either case we have defined the notion of prime ideals, and now we post the same question. In terms of ideals, what does the question translate to with respect to the factoring we are expressing an element of the ring in terms of as a unique product of prime elements, that we cannot do that is why we move to the ideals. An element of the ring in terms of ideal corresponds to and there I should define ideal is.

(Refer Slide Time: 28:48)



Dfn: Ideal I is a principle ideal if $I = (a)$ for $a \in R$.

Example: $\mathbb{Z}[\sqrt{-5}]$.

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

and $2, 3, 1 \pm \sqrt{-5}$ all are irreducible.

Consider (2).

We have $(2) = (2, 1+\sqrt{-5}) \cdot (2, 1+\sqrt{-5})$

$$(2\alpha + (1+\sqrt{-5})\beta) \cdot (2\gamma + (1+\sqrt{-5})\delta)$$

$$= 4\alpha\gamma + 2(1+\sqrt{-5})\alpha\delta + 2(1+\sqrt{-5})\beta\gamma + (-4+2\sqrt{-5})\beta\delta$$

$$= 2\left[2\alpha\gamma - 2\beta\delta + (\alpha\delta + \beta\gamma + \beta\delta)(1+\sqrt{-5})\right]$$

I have been holding on to that definition for a while. So, I found a name to this special kind of ideal which are generated by single element R I. These are called Principle Ideals.

And, now the question of uniquely factoring an element of the ring in terms of prime elements translates to uniquely factoring a principle ideal which corresponds to the element as a product of prime ideals. And that I have been saying can be shown in that for certain kind of ring which called Dedekind domains. Not only principle ideal, every ideal can be uniquely express as a product of prime ideals. That is a theorem I will not prove, so just stated it I will write it down also but let us more interestingly look an example.

The one we got stuck with and that is where the whole discussion started from, the ring z square root of minus 5. In this ring we had 2 times 3 equals 1 plus square root of minus 5 times 1 minus square root of minus 5 and 2, 3, 1 plus minus square root of minus 5 all are irreducible, we have seen this. I think I am not given a proof that these are irreducible element but I did ask you to work this out. And using the notion of norms you can very easily show that all of these elements are irreducible. So, these are irreducible elements. There is a unique factorization property break downs in this ring. And now let us look at the corresponding ideals and see what we can say.

So, first let us look at the ideal of 2. Ask the question, is this a prime idea? Answer is no. The I principle ideal 2 factors has the ideal 2 1 plus square root of minus 5 times this ideal itself, so it is a square of an ideal let us see this. What are the elements of this product ideal? All finite editions of products of this kind what is the general element of this ideal; 2 alpha plus 1 plus square root of minus 5 times beta, you multiply this with another element from this that is the same ideal here so let us say 2 gamma plus 1 plus square root of minus 5 times delta, what is this equal to, is this. Just multiplying out everything and you see this.

Now notice that every term here is an even multiple, that is I can write this as 2 times 2 alpha gamma minus 2 beta delta plus alpha delta plus beta gamma plus beta delta 1 plus square root of minus 5. Now inside this square brackets we have an element of the ring, sorry not the ring but it is actually an element of this ideal. This part is even, so that is a 2 times of something and this is just a multiple of 1 plus square root of minus 5. This is an element of these ideal and so actually it does not have to be intersection. This is enough that it is a event of the ring, because if there is a multiplied to outside which puts it inside this ideal.

Now any finite sums of this form will also be even multiples and therefore that will also be an element of the principle ideal generated by 2. So this shows that all elements of this product ideal are contained in this ideal. How about the converse? That is converse is trivial. Why?

Student: (Refer Time: 36:04).

Any element, no or the converse I have to show that every even number that is this principle ideal is contained in this ideal. In particular let us try to show that 2 is contained in this ideal. If I show that 2 are contained in this ideal then I am done. So, why is 2 contained in this ideal?

Student: take beta gamma delta (Refer Time: 36:38).

Take beta gamma delta to be 0 and this is 0.

Student: Actually that 2 is contained in this we will take already here (Refer Time: 36:54) we require 2 gamma alpha gamma (Refer Time: 36:58) beta should equal to 1.

That should equal to 1.

Student: If we take 2 common then that (Refer Time: 37:04) should be equal to 1, no that should be equal to 1 by 2.

Yes right. That is not possible, actually that is true. So, my claim is wrong that means, let us I have missed out something let us see in this calculations. One show is that the principle ideal of 4 is contained in this, but that is contained in this but that is not equal to that any way. So, what is going wrong here?

So let us stop here and I will leave this also as a bit of an exercise for you and tomorrow when we meet we will fix this and we will also discuss those two alternative definitions of prime ideals.