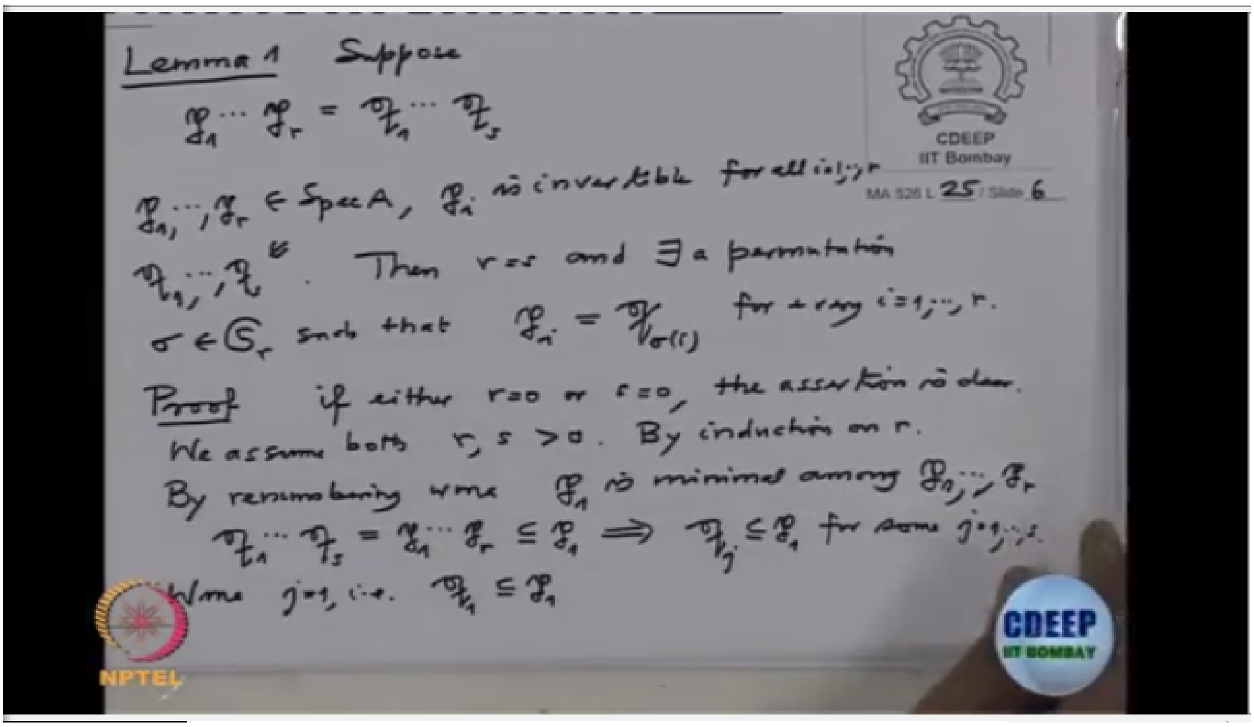
Lecture - 60

Dadekind Domains

and Prime factorization of Ideals.

Okay. Okay, the first lemma, so lemma one. Okay. So, suppose I have two decompositions. Suppose, p one to pr, these are prime ideals. And that is also equal to product q one to qs, where p one to pr are prime ideals and A is a domain always. And q one to qs are also prime ideals. Assume that, I'm only assuming that pis are invertible. Ps is invertible for all i one to r. I'm not assuming qis are invertible. Then, r equal to s, and up to permutation this r same. And there exist a permutation sigma of r letters [2:12 inaudible] sr such that pi equal to q suffix sigma i for every for every guy. This means they are unique up to permutation. So, proof. So, if r equal to zero, if either r equal to zero or s equal to zero, the assertion is clear. Right? If r equal to zero, the empty product is the whole ring. And if s equal to zero, this is the whole ring. So the assertion is clear in this case. So, I can assume both, we assume both r and s are positive. And I'm going to prove the assertion by induction on r. by induction on r. Okay. So, we have this finitely many prime ideals, all of them are invertible. And among them I will assume p one is minimal among them. So, we may assume by re-numbering, we may assume p one is minimal among p one to pr. Now look at the product q one to q s, this is same as p one to pr, and this is obviously, contain in p one. So this product of ideal is containing the prime ideal. Therefore, one of them is contain there. So qj will be contain in p one for some j in one to s. So by permuting qjs, I will assume j equal to one. So, we may assume j equal to one, that is, we are assuming q one is contain in p one.

(Refer Slide Time 5:38)



Lemma 1 Suppose

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

$\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \operatorname{Spec} A$, $\mathfrak{p}_i$ is invertible for all $i = 1, \dots, r$

$\mathfrak{q}_1, \dots, \mathfrak{q}_s \in$. Then $r = s$ and $\exists$ a permutation $\sigma \in \mathfrak{S}_r$ such that $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ for every $i = 1, \dots, r$.

Proof if either $r = 0$ or $s = 0$, the assertion is clear.

We assume both $r, s > 0$. By induction on r.

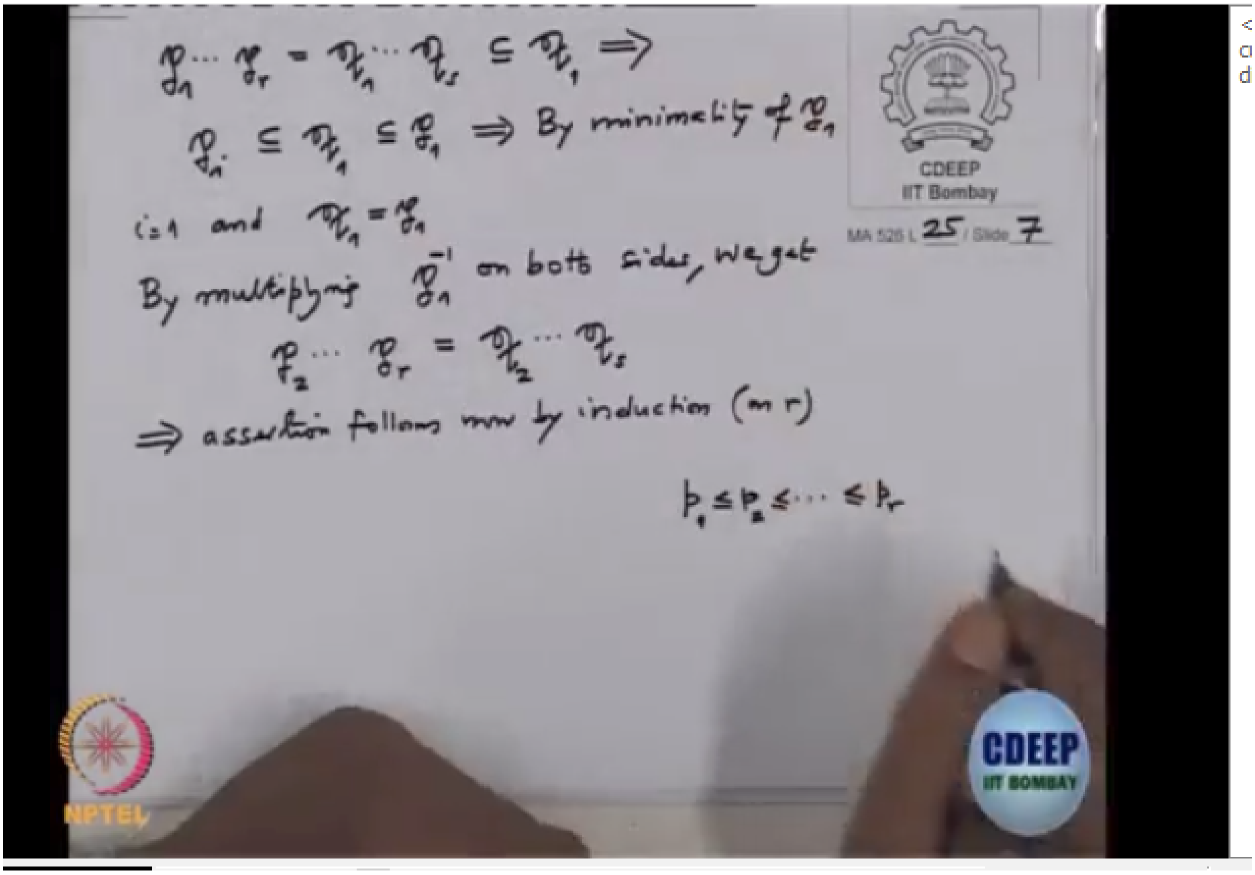
By renumbering wma $\mathfrak{p}_1$ is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_r$

$$\mathfrak{q}_1 \cdots \mathfrak{q}_s = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_1 \Rightarrow \mathfrak{q}_j \subseteq \mathfrak{p}_1 \text{ for some } j = 1, \dots, s.$$

Wma $j = 1$, i.e. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$

Now, do the other way. Now look at the product p one to pr which is q one to qs, which is contain in q one, and this q one is prime, therefore, one of them has to be contain in q one. So, there exists pi contained in q one. But this q one was contained in p one. So this qi contain in p one, therefore i has to be, by minimality i has to be one. So by minimality of p one, i is one, and then all these are equal. And q one equal to p one. So we have proved one of them equal. Now cancel, for cancellation you need inevitability. But we have given p one is invertible, and the other side is q one, which is also p one. So, it's invertible, so you can cancel it. And then, so by multiplying p one inverse on both sides, we get p two, pr equal to q two, qs. And then, by induction… So, assertion follows now by induction, that was on r. Let me remind you, this proof is very similar. You remember, when you were writing you r prime decomposition of numbers, you were writing them in this order, p one less equal to p two and so on, pr and then we were inducting on in the number of vectors. So this is the same proof.

(Refer Slide Time 8:20)



$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{q}_1 \Rightarrow$

$\mathfrak{p}_i \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1 \Rightarrow$ By minimality of $\mathfrak{p}_1$

$i=1$ and $\mathfrak{q}_1 = \mathfrak{p}_1$

By multiplying $\mathfrak{p}_1^{-1}$ on both sides, we get

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$$

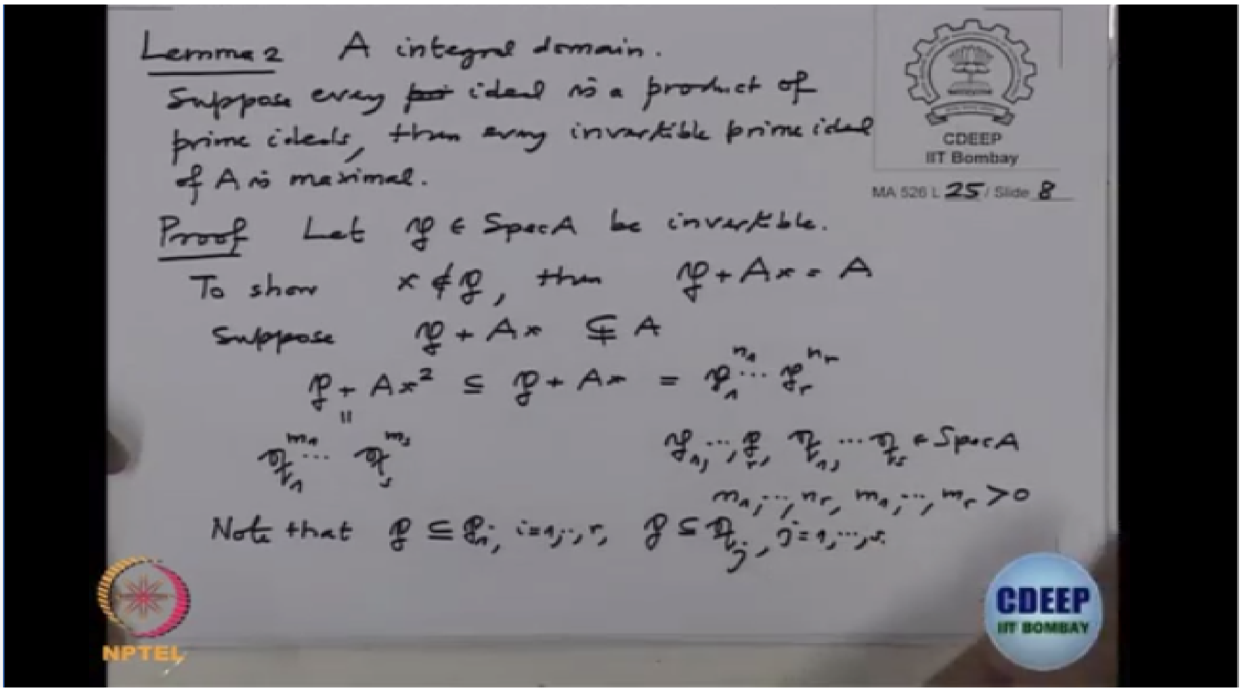
$\Rightarrow$ assertion follows now by induction (on r)

$p_1 \le p_2 \le \cdots \le p_r$

Okay. So, this was lemma one. And lemma two also, we'll need, we'll need two lemmas. They are all simple of this type. So, lemma two. Now, again, we are assuming an integral domain, A integral domain. And in the above lemma also, we didn't even assume A is [8:45 inaudible]. Suppose, every prime ideal, every ideal is a product of prime ideals. Remember, this earlier lemma is a preparation for proving it uniqueness. And this one will be preparation for proving its existence. The existence of the product. Then every invertible prime of A is maximal. So what is the lemma? Suppose, every ideal is a product of prime ideals, then every invertible prime ideal has to be maximal. Proof. So, let p be an invertible prime ideal, p in this be invertible. Remember, invertible means, a times a colon p should be equal to [10:26 inaudible] now, I want to prove p is maximal. Okay. So, p is maximal, how do you show p is maximal? So that means, to show that, if I take an element outside p, then p plus ideal generated by x, this should be the whole ring. So that will mean, p is maximal, you know, bigger ideal than p. okay. So, suppose, we want to show this. So suppose it is not true, then we should look for a contradiction. So suppose p plus ax, this is a proper ideal.

Then we should look for a contradiction. Okay. So, look at that p plus ax square, this is contain in p plus ax. So, if this is proper, these are also proper. And so both these ideals are by assumption all ideals are product of prime ideal. So, both these ideals are product of prime ideals.so, this for example, this will be, let's say this is p, p one n one, pr nr. And this one will be q one m one, qsms, where this p one to pr are prime ideals, q one to qs are also prime ideals. And this n one to nr, m one to ms, they are positive. Only those we write there. So what does this show? This shows, you see p is contained in this and p is also contained in this. So p is contain in all these guys. Note that p is contain in all pis, i is from one to r, and also p is contain in qjs, where j is one to s.

(Refer Slide Time 13:31)



Lemma 2 A integral domain.

Suppose every ~~pr~~ ideal is a product of prime ideals, then every invertible prime ideal of A is maximal.

MA 526 L 25 / Slide 8

Proof Let $\mathfrak{p} \in \mathrm{Spec} A$ be invertible.

To show $x \notin \mathfrak{p}$, then $\mathfrak{p} + Ax = A$

Suppose $\mathfrak{p} + Ax \subsetneq A$

$$\mathfrak{p} + Ax^2 \subseteq \mathfrak{p} + Ax = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$$

$$\| \quad \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$$

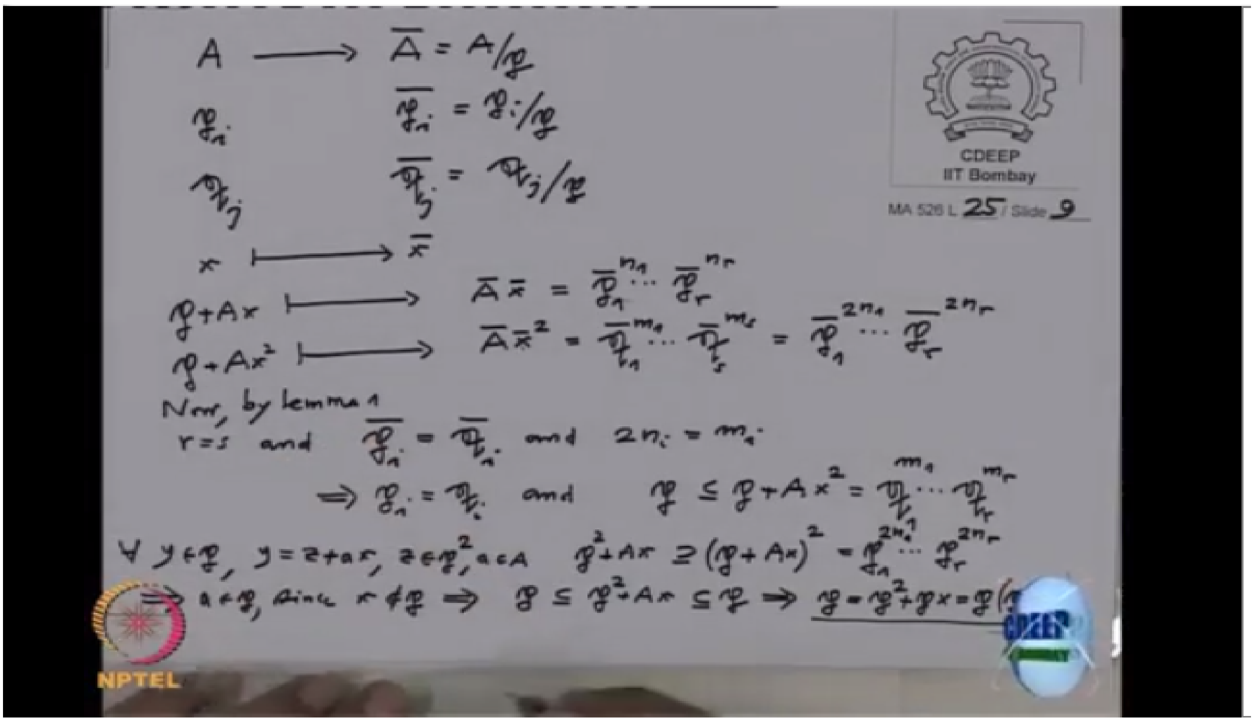
$\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots \mathfrak{q}_s \in \mathrm{Spec} A$

$m_1, \dots, n_r, m_1, \dots, m_r > 0$

Note that $\mathfrak{p} \subseteq \mathfrak{p}_i, i = 1, \dots, r$, $\mathfrak{p} \subseteq \mathfrak{q}_j, j = 1, \dots, s$.

So I want to go mod that p. So we are replacing A by A bar which is A by p, and then this pA is here, they'll get replaced by pi bar which is pi by p. And this qjs will get replaced by qj bars, which is qj by p. Alright. And element will get replaced by x bar under this map. So, therefore, the ideal p plus ax, that will get replaced by a bar x bar, because p will go to zero. Similarly, p plus ax square, that will get replaced by a bar x bar square. And then we will have equations like this, this is p one bar n one, pr bar n r. And this will be q one bar m one, qs bar ms. Alright. But why did we do this? That is because this ideal is a square of this ideal. See, that was not the case in earlier. So, therefore, from here, from this decomposition, this is a square of that ideal. So, this is same as p one bar two n one, p bar r two nr. This is what we know. Now here, what? This ideal, ax is a principle ideal in a domain, therefore, they are invertible. And if the product is invertible, factor is invertible. If a product is invertible, a factor is invertible. That's obvious. So, therefore, all these p bars are invertible. And therefore, by earlier result what we proved, if you have such a decomposition, all these guys are invertible, then up to a permutation, first of all, this number equal to this number, r equal to s. R equal to s. Now, by lemma, now by lemma one, r equal to s, pi bar equal to qi I will write, q bar i. I have sought that permuted ration in that. And also the numbers are same. And two ni equal to mi. So that, first of all, we'll say that pi equal to qi. So, this shows pi equal to qi. And what do we get? And when p, this is contain in p plus Ax square which is q one m one, qrmr, which is also same as p one two n one, pr two nr. But this one, the last one is same as, this is contained in, this is equal to first, p plus Ax square because this ps are qs. So I will replace now p one by q one, and then will be two. And then put it back here. So this is p plus Ax whole square. But that is contain in p… Oh, this is contain in p square plus Ax. So what did we achieve? So pA, this contain in p square x. So, that means any y in p, so y in p, y is here. So, it is here. That means, any y in p, we can write it as z plus Ax, where z is in p square and a is in A for any y. We can write like this. But y is in p, z is in p square, so z is in p, therefore Ax is in p. So that will imply, and x, what was x? x is not [19:30 inaudible]. Remember, x is not [19:32 inaudible] and we wanted to prove this. So, from here, we get a belong to p since x is not in p. So we got a is in p. But once we get A is in p, then what did we get? That means, any y, we can write it as somebody is in p square and somebody is in p here. So, that means, we proved that, so that implies p is contained in p square plus Ax which is contained in p because we started with this and then that coefficient is in p, therefore, this part will be in p. so, therefore, equality here, so that shows that p equal to p square plus px which is p times p plus ax. But now multiply by p inverse because we are assuming is invertible. So if you multiply by p inverse, what do we get? If you multiply this by p inverse, then this will become the ring A, this will go, and this will become the ring A.

(Refer Slide Time 21:11)



$A \longrightarrow \bar{A} = A/\mathfrak{p}$

$\mathfrak{p}_i \qquad \bar{\mathfrak{p}}_i = \mathfrak{p}_i/\mathfrak{p}$

$\mathfrak{q}_j \qquad \bar{\mathfrak{q}}_j = \mathfrak{q}_j/\mathfrak{p}$

$x \longmapsto \bar{x}$

$\mathfrak{p}+Ax \longmapsto \bar{A}\bar{x} = \bar{\mathfrak{p}}_1^{n_1}\cdots\bar{\mathfrak{p}}_r^{n_r}$

$\mathfrak{p}+Ax^2 \longmapsto \bar{A}\bar{x}^2 = \bar{\mathfrak{q}}_1^{m_1}\cdots\bar{\mathfrak{q}}_s^{m_s} = \bar{\mathfrak{p}}_1^{2n_1}\cdots\bar{\mathfrak{p}}_r^{2n_r}$

Now, by lemma 1

$r=s$ and $\bar{\mathfrak{p}}_i = \bar{\mathfrak{q}}_i$ and $2n_i = m_i$.

$\Rightarrow \mathfrak{p}_i = \mathfrak{q}_i$ and $\mathfrak{p} \subseteq \mathfrak{p}+Ax^2 = \mathfrak{q}_1^{m_1}\cdots\mathfrak{q}_r^{m_r}$

$\forall\, y\in\mathfrak{p},\ y = z+ax,\ z\in\mathfrak{p}^2, a\in A \quad \mathfrak{p}^2+Ax \supseteq (\mathfrak{p}+Ax)^2 = \mathfrak{p}_1^{2n_1}\cdots\mathfrak{p}_r^{2n_r}$

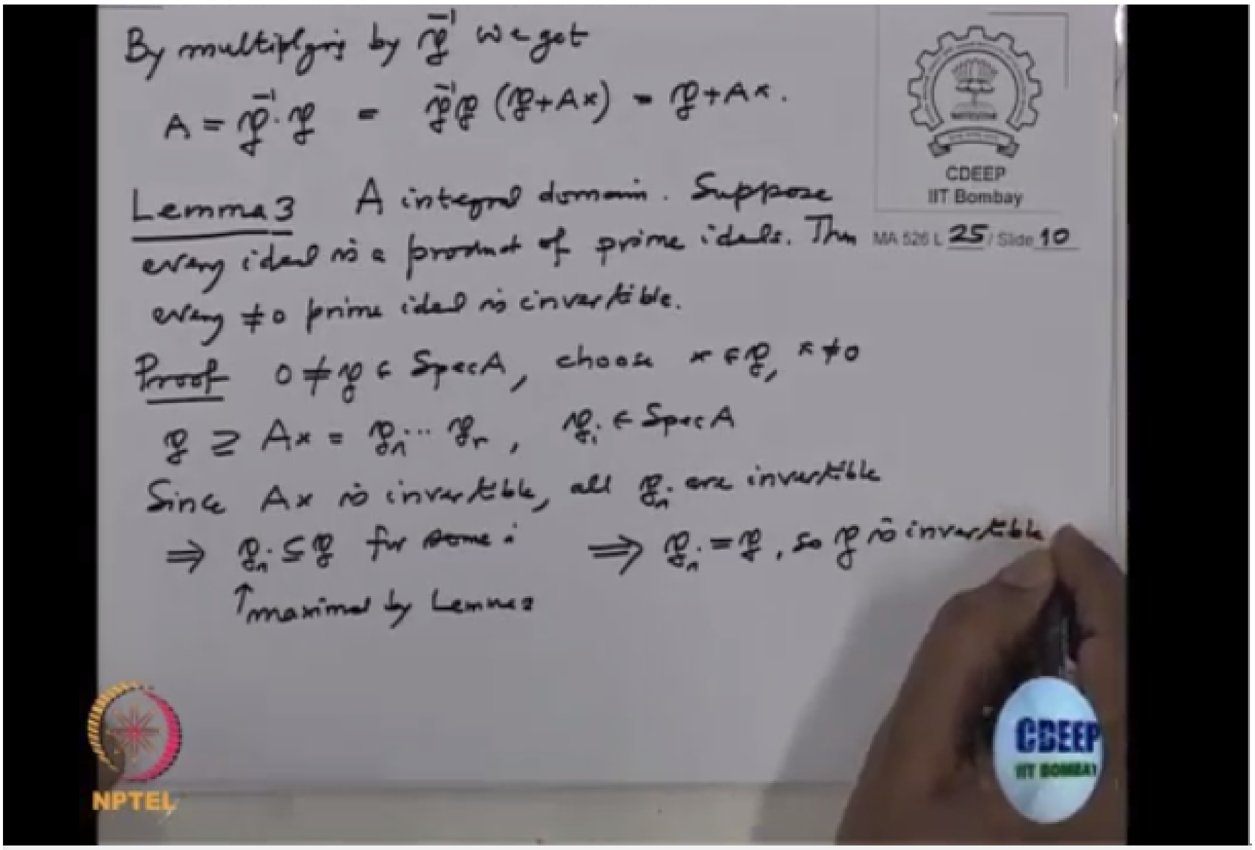
$\Rightarrow a\in\mathfrak{p}$, since $x\notin\mathfrak{p} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}^2+Ax \subseteq \mathfrak{p} \Rightarrow \underline{\mathfrak{p} = \mathfrak{p}^2+\mathfrak{p}x = \mathfrak{p}(}$

CDEEP
IIT Bombay
MA 526 L 25 / Slide 9

So, by multiplying by p inverse, we get p inverse p which is A, the other side is equal to p inverse p and in p plus Ax, so which would be p plus Ax. So that's it.

That’s what we wanted to show. Alright. So now one more only, and then we will be finish in two, three minutes. So, what did we prove here? Let us summarize. In this lemma we have proved that if every ideal is a product of prime ideals, then every invertible prime ideal is maximum, invertible prime ideal is maximum. And in the first lemma, we have proved that, if an ideal is product of prime ideals, two different decompositions in two prime ideals, and in one all prime ideals are invertible, then they are equal up to a permutation. This lemma says, assume, so A integral domain… All these proofs, even element in number theory proofs for integers. The main idea was converting product into the sum. That was the main idea. So, if A integral domain, and suppose every ideal is a product of prime ideals, then every non-zero prime ideal is invertible. Oaky. So, proof. We want to prove that every non-zero prime ideal is invertible. And we have given that every ideal is a product of prime ideal. So, start with a non-zero prime ideal. I want to produce inverse for this. And we know what should the inverse be. So, choose x in p and x non-zero prime ideal, therefore, we can choose that. And, now look at the ideal Ax, this is product of prime ideals, p one to pr, pi primes. This is a principle ideal, so all these guys are invertible. Since A principle ideals are invertible, all the factors are invertible. But the product is, this is also contain in p, because x is contain in p. Therefore, one of them has to be contain in p. so, pi has to be contain in p for some i. But pi is invertible prime ideal. So earlier, lemma says, earlier lemma, assumption of every ideal is a product of prime ideals which here also, there is an assumption. And the earlier lemma says, if some prime ideal is invertible, then it has to be maximal. So this pi is invertible prime ideal, so it’s maximal. This is maximal by lemma two. Therefore, this pi has to be p, oi is p. And therefore, p is invertible. So, p is invertible.

(Refer Slide Time 26:08)



By multiplying by $\mathfrak{p}^{-1}$ we get

$$A = \mathfrak{p}^{-1}\cdot\mathfrak{p} = \mathfrak{p}^{-1}\mathfrak{p}(\mathfrak{p}+Ax) = \mathfrak{p}+Ax.$$

Lemma 3 A integral domain. Suppose every ideal is a product of prime ideals. Then every $\neq 0$ prime ideal is invertible.

Proof $0 \neq \mathfrak{p} \in \operatorname{Spec} A$, choose $x \in \mathfrak{p}$, $x \neq 0$

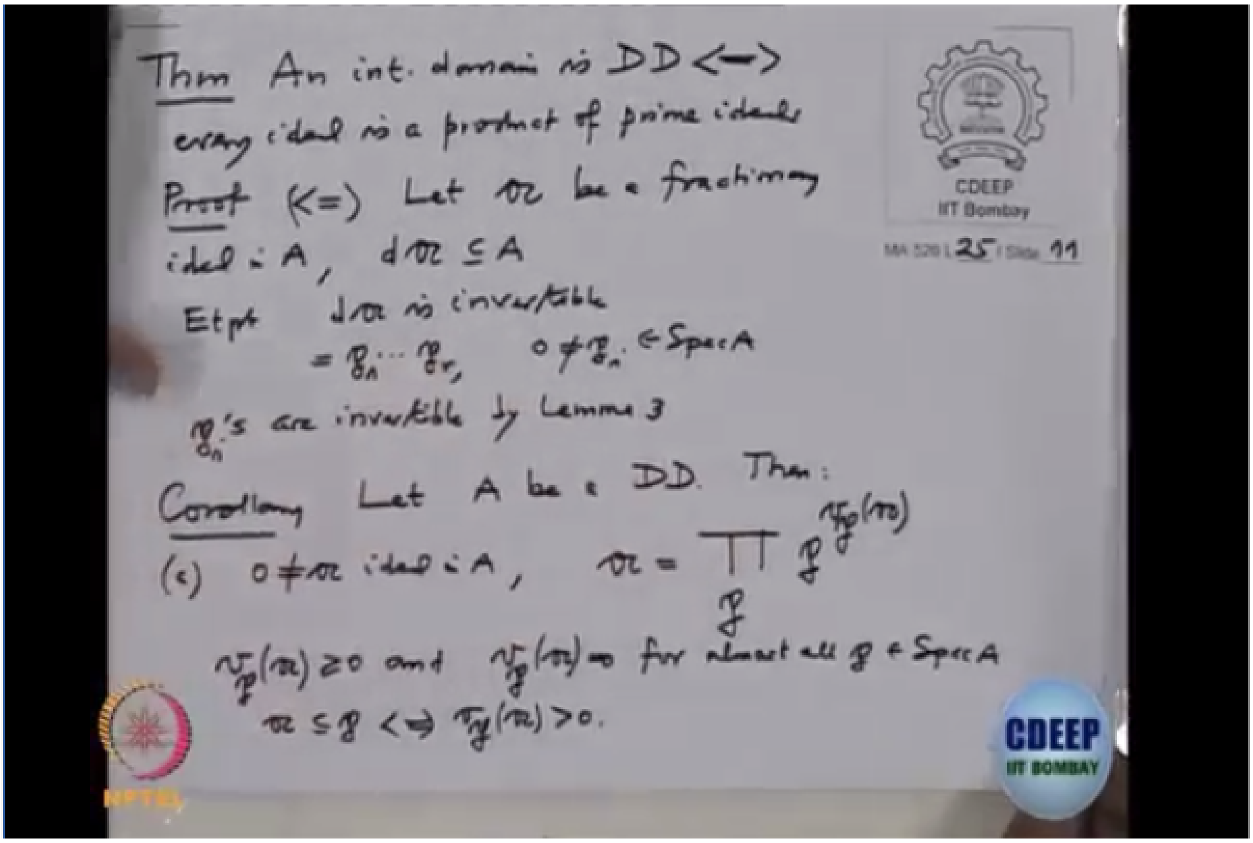
$\mathfrak{p} \supseteq Ax = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{p}_i \in \operatorname{Spec} A$

Since Ax is invertible, all $\mathfrak{p}_i$ are invertible

$\Rightarrow \underset{\uparrow \text{maximal by Lemma 2}}{\mathfrak{p}_i} \subseteq \mathfrak{p}$ for some i $\Rightarrow \mathfrak{p}_i = \mathfrak{p}$, so $\mathfrak{p}$ is invertible

Now, we are ready to prove. So what do we want to prove? So, Dadekind domain, so the theorem we wanted to prove was, an integral domain is DD if and only if every ideal is a product of prime ideals. So, proof. So, only one way we have to prove, this way, the other way we already proved, so we want to prove this way. Alright. Suppose, every ideal is a product of prime ideal, then I want to prove A is Dadekind domain. That means, I want to prove that A is noetherian of dimension less equal to one. What do we want to prove? I want to prove that normal of dimension less equal to one. Alright. So, let a be a fractioning ideal, I will prove that fractioning ideals are invertible. I will prove one of the equivalent distance of the earlier. So, every fractioning ideal is invertible. So, let d be a common denominator, d times A contain in A. so, to prove A is invertible, I will prove d is invertible. So, enough to prove d times A is invertible. But it's a integral ideal, so it's a product of prime ideals. So, this is a product of non-zero prime ideals, p one to pr, where zero is not equal to pi, all these are prime ideals. But non-zero prime ideals are invertible. That is what it shows. If every ideal is a product of prime ideals, under this assumption, lemma three says that every non-zero prime ideal is invertible. So, therefore, all these pi's are invertible by lemma three. Therefore, product is invertible. Therefore, di is invertible, therefore A is invertible. So, therefore, we are done. So let me write the corollary. So, let A be Dadekind domain, then part (a) If I have a non-zero ideal, zero not equal to a ideal in A, then we can write this as, a, we can write it as product, product is running over p, p power vpa. And this vpa is non-negative and vpa equal to zero for almost all p. So that, indeed this product is finite product, because only finitely many are non-zero. So, prime ideal p occurs in this if and only if that vp is positive. So, a contain in p if and only if vpa is positive. So that is the prime decomposition.

(Refer Slide Time 31:02)



Thm An int. domain is DD $\Longleftrightarrow$ every ideal is a product of prime ideals

Proof ($\Leftarrow$) Let $\mathfrak{a}$ be a fractionary ideal in A, $d\mathfrak{a} \subseteq A$

Etpt $d\mathfrak{a}$ is invertible

$= \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $0 \neq \mathfrak{p}_i \in \operatorname{Spec} A$

$\mathfrak{p}_i$'s are invertible by Lemma 3

Corollary Let A be a DD. Then:

(a) $0 \neq \mathfrak{a}$ ideal in A, $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$

$v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ and $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for almost all $\mathfrak{p} \in \operatorname{Spec} A$

$\mathfrak{a} \subseteq \mathfrak{p} \Longleftrightarrow v_{\mathfrak{p}}(\mathfrak{a}) > 0$.

And that is the part a. So this is a existence. Actually, this we can do it for the fractioning ideal also. So I will not write it. This we can do it for the fractioning ideals also, like you do it fir integers and for the rational numbers know where you allow this to be not only non-negative but allow them to be negative also. Okay. So, two more comments I will make here. So, here, I would like you to check that, so let me write in the exercise form. (1) So A integral domain. If A is… Assume it is VFD, integral domain VFD. Then, A is DD if and only if A is a PID. So, once you assume it is UFD, then it is PID. (2) Also, if a DD which is semi-local, semi-local means the maximal ideals, this is a finite set, only finitely many maximal ideals and Dadekind domain, then A is a PID. It is always interesting to know when Dadekind domain is a principle ideal domain because this is again, come from the fact that you want to know when the integral closure of z in a number field when it is a PID. When it is a UFD, but then it's Dadekind domain and UFD, then it's PID. So, it's always interesting to know when is the Dadekind domain PID. Okay, third one. Third one is little bit more general. This is true for any UFD[33:49 inaudible]. So, A is UFD and it has a finitely many prime elements, with p, let us denote PA, this is the set of all prime elements in A. And strictly speaking, I should write that this is the set of all representatives for prime elements up to associate. Take the relation associate, and in that set, you collect the representatives of the prime elements. So, suppose this PA is a finite set, then A is a PID. In fact, it will be dedicated, in fact an ED, more stronger. I will give a hint for this. So, they are finitely many prime elements, so they are finitely many vp's. Take vp's which p is in this p. P is in p. So, they are finitely many of this. So look at this function vp, vp, p in p, so that this is equivalent function. Where did you do that? If an ideal if invertible and it's product of prime ideal, if somebody is invertible, then all factors in that will also be invertible know. Factors. See, suppose six is invertible, then is an two invertible? Because you multiply by inverse of this and only you take the guy you wanted to be invertible and collect.