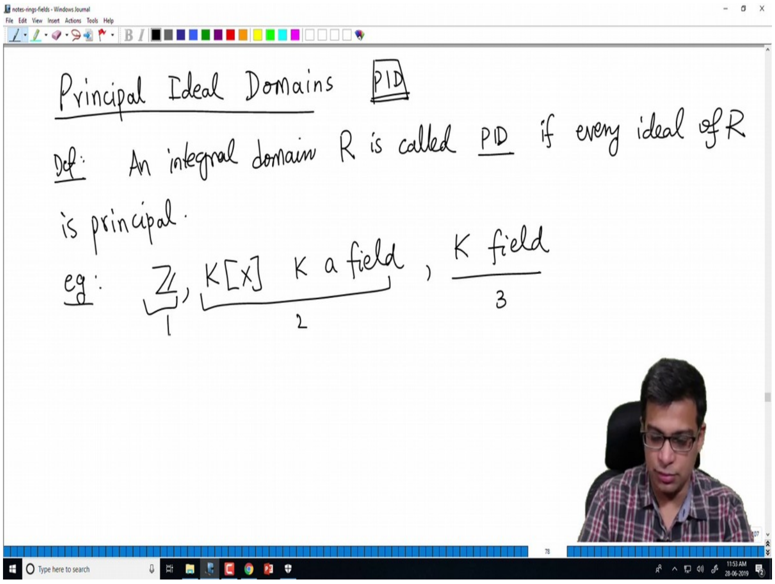
Introduction To Rings And Fields
Prof. Krishna Hanumanthu
Department of Mathematics
Chennai Mathematical Institute

Lecture - 25
Principal Ideal Domains

In the last two, three videos, we talked about the notion of irreducible elements and prime elements in an arbitrary integral domain and we also introduced the notion of greatest common divisor for a pair of elements and we saw an example where they greatest common divisor may not exist. So, the general statements we have proved; let me quickly recall without writing them. We proved that in any integral domain, a prime element is irreducible that is automatically true, but irreducible elements may not be prime.

And we saw an example of the ring Z adjoint square root of minus 5 in which case in which ring 2 is an irreducible element, but it is not a prime element. So, in the next couple of videos we are going to study two very important classes of rings in which irreducible elements are in fact, going to be prime ok.

(Refer Slide Time: 01:07)



Principal Ideal Domains $\boxed{\text{PID}}$

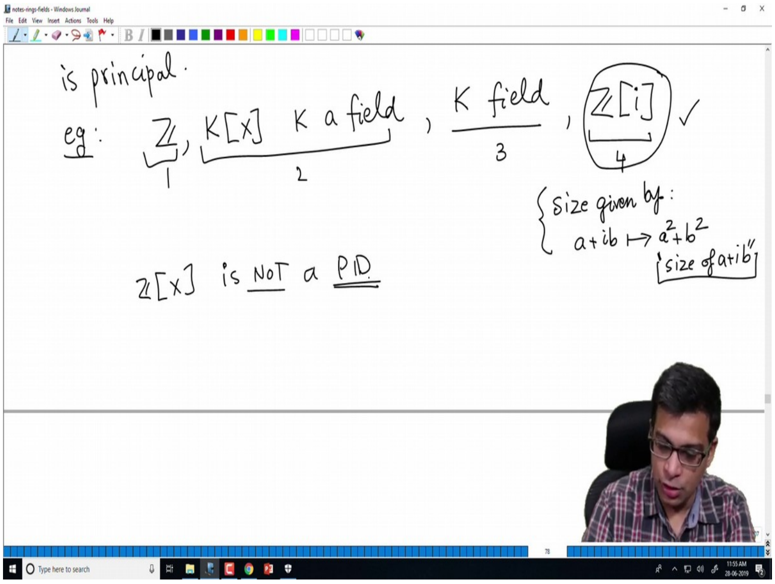
Def: An integral domain R is called PID if every ideal of R is principal.

eg: $\underbrace{\mathbb{Z}}_{1}, \underbrace{K[x] \;\; K \text{ a field}}_{2}, \underbrace{K \text{ field}}_{3}$

In the first class of examples is class of rings are called Principal Ideal Domains. So, they are referred to in short as PIDs. So, principal ideal domains are very simple. So, a ring so, this is the definition; an integral domain R is called so, I will always use the abbreviation PID for principal ideal domain. So, an integral domain is called a PID if every, as the name suggest every ideal must be principal; every ideal of R is principal. So, in other words every ideal I is in fact, generated by a single element.

So, the most important examples that we have encountered already in the course are of course, the ring of integers and the polynomial ring in one variable over a field right. So, these are some of the standard examples and of course, K a field itself. A field is definitely a PID because it is an integral domain and it has only two ideals the zero ideal and the unit ideal, both of which are principal. So, we have three examples here; this second and third are in fact, classes of examples.

(Refer Slide Time: 02:45)



is principal.

$$\underline{\text{eg}}: \underbrace{\mathbb{Z}}_{1}, \underbrace{K[x] \quad K \text{ a field}}_{2}, \underbrace{\underline{K \text{ field}}}_{3}, \boxed{\underbrace{\mathbb{Z}[i]}_{4}} \checkmark$$

$$\left\{\begin{array}{l}\text{size given by:}\\ a+ib \mapsto \underbrace{a^2+b^2}_{\text{"size of } a+ib\text{"}}\end{array}\right.$$

$\mathbb{Z}[x]$ is $\underline{\text{NOT}}$ a $\underline{\underline{\text{PID}}}$.

notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help
Type here to search

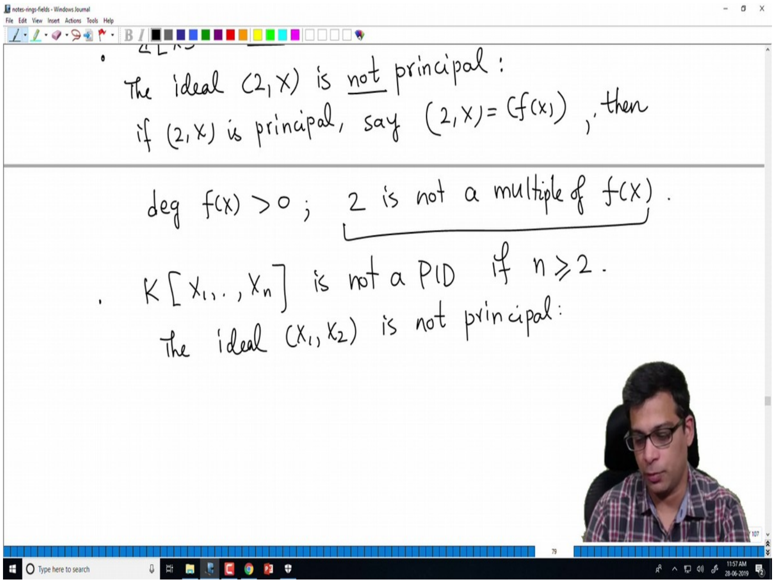
And some other rings that we have encountered before which happened to be PID is this ok. So, this I will not prove for you because that will take me away from what I want to do, but the idea is the same as the examples we have considered.

So, if we quickly recall how did we prove that every ideal in Z is principal or that every ideal in K x is principal we used essentially what is called Euclidean algorithm right; Euclidean division algorithm. We have the notion of size in these rings. Size of an integer it is just its absolute value, size of a polynomial is its degree. So, given any ideal we picked an element with a least degree in the polynomial ring and least positive number in the case of integers. Here we have a size given by the norm of an element of this.

So, as I said I will not go into details, but we can always do the following. Given an ideal we can pick the pick an element with the least possible norm or size which is the sum of squares of the real and imaginary parts. So, this is the size of a plus ib and carry out the same procedure that we used. Given any ideal if it is 0 ideal, we are done; if it is not pick an element with the smallest size, then argue that every other element is a multiple of this by sort of dividing the two elements.

So, we can carry out the division process exactly as in the case of integers or in the polynomial ring, but this is a useful example of principal ideal domain; what is not an example of principal domain principal ideal domain and it is this some familiar ring to us it is a very nice ring otherwise, but this is not a PID.

(Refer Slide Time: 04:49)



notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help

The ideal $(2, X)$ is not principal:
if $(2, X)$ is principal, say $(2, X) = (f(x))$, then

deg $f(x) > 0$; $\underbrace{2 \text{ is not a multiple of } f(x)}$.

- $K[X_1, .., X_n]$ is not a PID if $n \geq 2$.

The ideal (X_1, X_2) is not principal:

The reason is the ideal for example, 2 comma X is not principal, it is not difficult to check this explicitly right because if 2 X is principal say, what is a principal ideal it is generated by a single element. So, say it is generated by a polynomial f X, then first of all you argue that f must not be a constant polynomial. In other words degree of f must be positive why because I will just say this and I will let you work out the details.

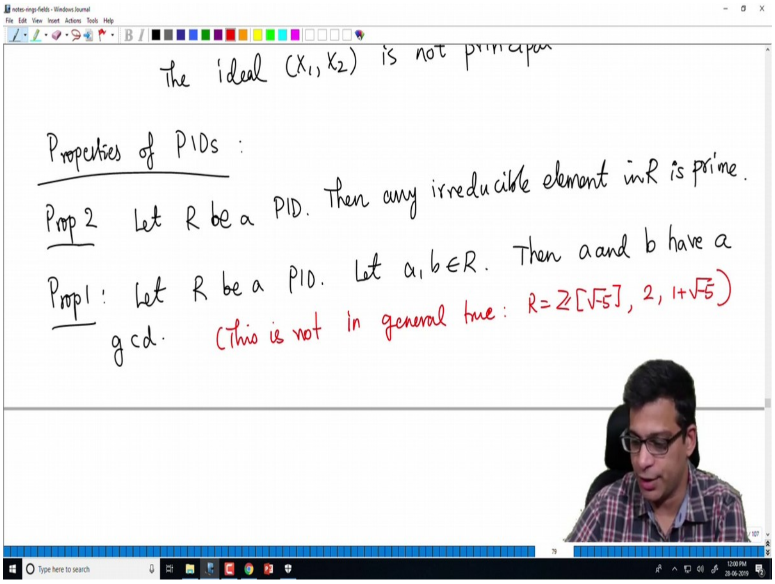
If degree f X is 0; that means, f X is actually a an integer it is a constant polynomial means it is an integer no way that it can generate X because remember if 2 comma X is equal to f X x is a multiple of f X. So, it cannot be a generator it cannot be an integer because X is never a multiple of an integer unless it is 1 of course, but if it is 1 the ideal generated by 1 is the entire ring, which 2 X is not. So, degree of f X must be positive.

And once its positive, 2 is not a multiple of because if it is a positive degree polynomial when you multiply by any other polynomial degree only increases, it may stay the same. If you multiply by constants or it will actually increase if you multiply by non constant polynomials, but it will never decrease. So, you can never obtain 2 as a multiple of this is a simple explanation for why Z X is not a PID.

Similarly, K X 1 ... X n is not a PID if n is at least 2 right; the reason is the ideal X 1 comma X 2 is not principal the same kind of reason as before. These are two independent variables. So, you cannot choose any single polynomial whose multiples are X 1 and X 2. So, this will never happen if you remember the language of irreducible elements X 1 and X 2 are irreducible elements. So, they cannot be written as products multiples of some other polynomial.

Same polynomial will not do for X 1 and X 2 X 1 of course, is a multiple of X 1 and X 2 is a multiple of X2, but there is no single polynomial whose multiples include X1 and X2. So, these are not PIDs. So, these are nice rings polynomial rings over in n variables over a field where n is at least 2 and polynomial ring in one variable over the integers are not are nice rings, but they are not PIDs ok. So, what are the some interesting properties of PIDs that I want to emphasize in this video.

(Refer Slide Time: 07:41)



The ideal (X_1, X_2) is not principal

Properties of PIDs :

Prop 2 Let R be a PID. Then any irreducible element in R is prime.

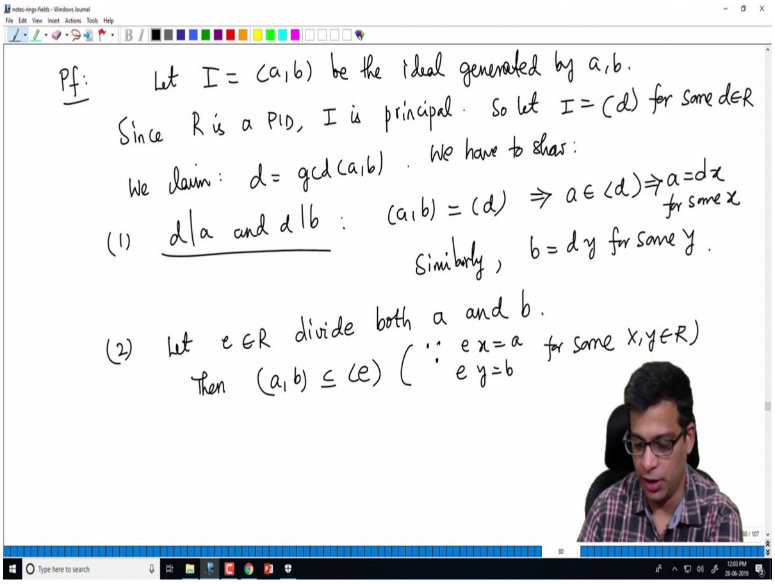
Prop 1 : Let R be a PID. Let $a, b \in R$. Then a and b have a gcd. (This is not in general true : $R = \mathbb{Z}[\sqrt{-5}]$, 2, $1+\sqrt{-5}$)

So, properties of PIDs properties of PIDs; one is that these are actually propositions, proposition. Let R be a PID, then any irreducible element in R is prime. Remember that we saw in an example that in general if you have an integral domain irreducible elements may not be prime though prime elements are always irreducible, but irreducible elements are not necessarily prime in general; however, in a PID that happens to be the case ok. So, actually I should make this proposition 2 and I will write proposition 1 for now which I will prove first and then we will do proposition 2 ok.

So, what is proposition 2? Let R proposition 1, what is proposition 1? Let R be a PID and let us take two elements then a and b have a g c d, ok. So, I am going to use this to prove the first second proposition. So, why is this? I want to say that if you have two elements, then g c d always exists as I have again indicated in the same example R equal to Z adjoined square root minus 5; this is not generally true.

So, let me recall this is not in general true as the example of edge. So, I do not remember the two examples maybe this. So, you take these two elements, they are both elements of the ring R they are not unit is and they have no greatest common divisor so; however, in the case of PID s any two elements have g c d and why is that.

(Refer Slide Time: 10:01)



Pf: Let $I = (a, b)$ be the ideal generated by a, b.

Since R is a PID, I is principal. So let $I = (d)$ for some $d \in R$

We claim: $d = \gcd(a, b)$. We have to show:

(1) $d | a$ and $d | b$: $(a, b) = (d) \Rightarrow a \in (d) \Rightarrow a = dx$ for some x

Similarly, $b = dy$ for some y.

(2) Let $e \in R$ divide both a and b.

Then $(a, b) \subseteq (e)$ ($\because$ $ex = a$, $ey = b$ for some $x, y \in R$)

So, let us consider it is very simple both propositions are in fact, very easy to prove. So, let I be the ideal generated by a, b; ideal generated by a and b; since R is a PID I is principal, every ideal is principal. So, let I be equal to some d for some it is a principal ideal.

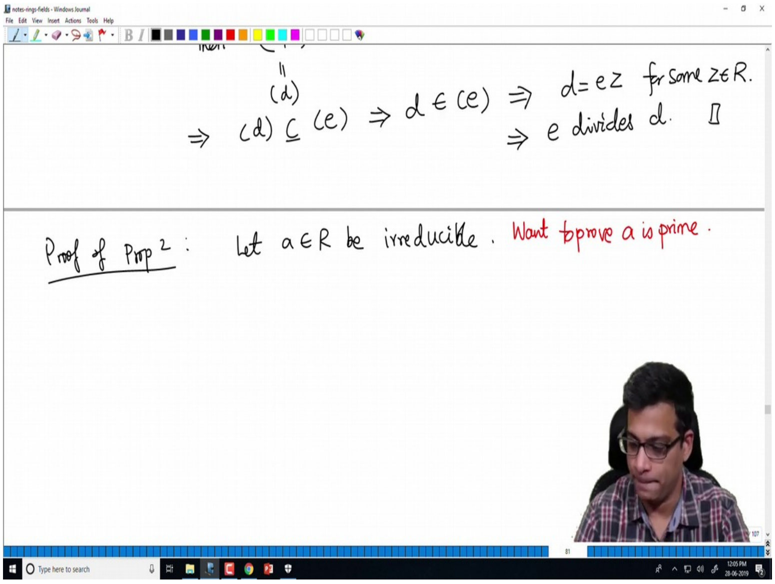
So, it is generated by a single element; let us call that d, then we claim that as you guess d is a g c d of a and b. Remember g c d there may exist several g c d s, but d is one of them. So, first of all remember what is g c d. We have to show one that d divides a and d divides b. So, let us quickly check this. Why is this true?

Remember the ideal generated by a, b is equal to the ideal generated by d, but a is an element of the ideal generated by a, b. So, a is an element of the ideal generated by d; that means, a is equal to d x for some x; similarly b is an element of a, b. So, b is an element of the ideal generated by d. So, b is d y for some y which is exactly the definition of d dividing b and d dividing a. So, d divides a and d divides b; in other words it is a common divisor.

Now, we need to show that it is a greatest common divisor. So, let us choose e an element of R divide; let e divide both a and b, right. So, let e divide both a and b; that means, then I claim that a, b the ideal is contained in e, why is this? This is because a x equal to e b y equal to e for some x and y in R by definition of e dividing both a and b; that means, a x sorry this is not correct I should write e x equal to a, e y equal to b, e divides a.

That means, e x is equal to a for some x e y is equal to b for some y; that means, a is of the form e x means a is in e x a is in the ideal generated by a e similarly, b is in the ideal generated by e. So, a, b is the entire ideal if the generators are in some ideal the entire ideal generated by a and b is in e.

(Refer Slide Time: 12:59)


notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help
Type here to search
12:05 PM
28-06-2019

then

$\|$

(d)

$$\Rightarrow (d) \subseteq (e) \Rightarrow d \in (e) \Rightarrow d = ez \text{ for some } z \in R.$$

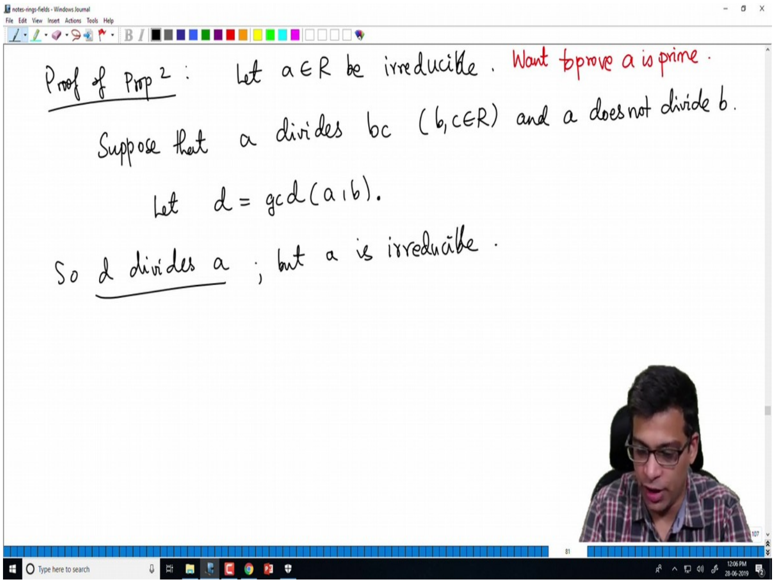
$$\Rightarrow e \text{ divides } d. \quad \square$$

Proof of Prop 2: Let $a \in R$ be irreducible. Want to prove a is prime.

But this is actually d e so; that means, the ideal generated by d is contained in the ideal generated by e; that means, the element d is in the ideal generated by e; that means, d is equal to e z for some z right d is an element of e means d is an element of the ideal generated by e means d is of the form e times some other ring element; that means, e divides d. So, this completes the proof of the proposition which said that any two elements I have g c d.

Now, I am going to prove the second proposition. So, this is proof of proposition 1, now I will do proof of proposition 2. Remember proposition 2 said in an in a PID every irreducible element is prime. So, let a in R be irreducible right. So, suppose, we want to prove that we want to prove a is prime right. I claimed that every irreducible element is prime.

(Refer Slide Time: 14:17)


notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help

Proof of Prop 2 : Let $a \in R$ be irreducible. Want to prove a is prime.

Suppose that a divides bc $(b, c \in R)$ and a does not divide b.

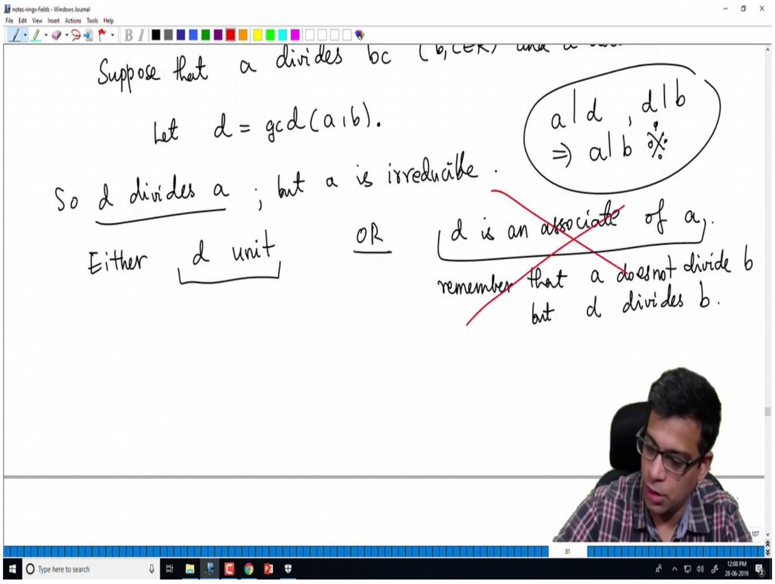
Let $d = \gcd(a, b)$.

So d divides a ; but a is irreducible.

So, we want to prove that a is prime, but if prime means so, suppose that a divides a product of two elements let us say b c, where b and c are in R. So, we want to show that a divides either b or a divides c ok. So, now, assume also that and a does not divide b. If it divides b we are done suppose it does not divide b, we are going to show that a divides c ok. So, now, not that so, by proposition one there is a g c d of b and a and b.

Remember when I write g c d of a and b it may suggest that there is a unique g c d, but I am not claiming that this is just a convenient notation for me all I am saying is that there is a g c d which I am calling d. Let us take the g c d of a and b. Now, we know that d divides by definition of g c d, d divides a. So, d divides a, but a is irreducible right by hypotheses a is irreducible. So, we have two possibilities an irreducible device; an irreducible element cannot have proper divisors.

(Refer Slide Time: 15:49)


notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help

Suppose that a divides bc (b,c∈R) and a

Let $d = \gcd(a, b)$.

So $\underline{d \text{ divides } a}$; but a is irreducible.

$a \mid d$, $d \mid b$
$\Rightarrow a \mid b$ ✗

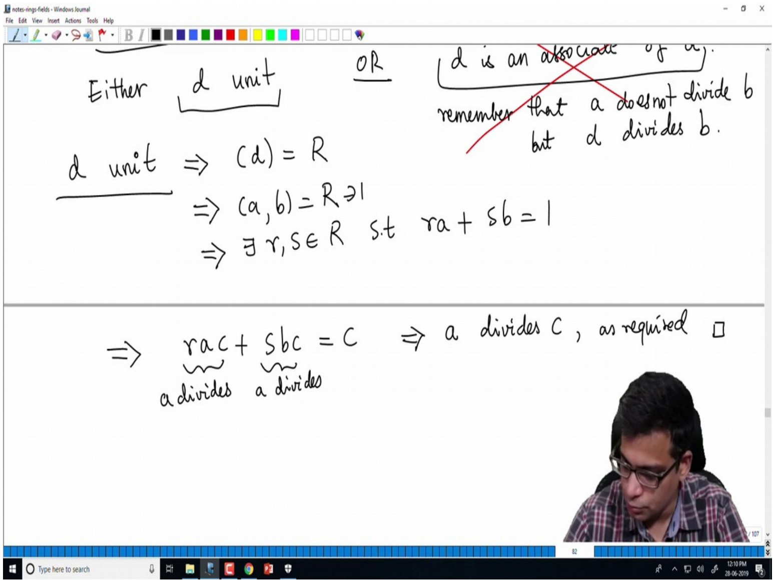
Either $\underbrace{d \text{ unit}}$ $\underline{\text{OR}}$ ~~d is an associate of a.~~

~~remember that a doesnot divide b~~
~~but d divides b.~~

So, either we have that d is a unit or d is an associate of a, right. We have that d is an associate of a or d is a unit I because a is irreducible d is not because a is irreducible a cannot have proper divisors, d is a divisor it cannot be proper. So, in other words it fails to be proper either because it is a unit or because it is an associate of a; I claimed that the second case cannot occur because if d is an remember that a does not divide b right. I am I am assuming that a does not divide b, but d divides b. So, d divides b because d is a g c d of a and b. So, definitely d divides b. So, now, d divides b a does not divide b. So, a and b cannot be associates.

Remember what is the meaning of associates they either differ by a unit or in other words d is a multiple of a and a unit or equivalently d divides a and a divides d. So, if d divides b and a divides b a does not divide b a cannot divide d because if a divides d; then if a divides d and d divides b; that means, a divides b, which cannot happen. So, in other words d and a cannot be associates. So, this case cannot occur right. I will put it like that: this case cannot occur. So, d must be a unit.

(Refer Slide Time: 17:37)



Either $\underbrace{d \text{ unit}}$ OR ~~$\underbrace{d \text{ is an associate of } a}$.~~

~~remember that a does not divide b but d divides b.~~

$\underline{d \text{ unit}} \Rightarrow (d) = R$

$\Rightarrow (a, b) = R \ni 1$

$\Rightarrow \exists\, r, s \in R$ s.t $ra + sb = 1$

$\Rightarrow \underbrace{rac}_{a \text{ divides}} + \underbrace{sbc}_{a \text{ divides}} = c \Rightarrow a$ divides c, as required □

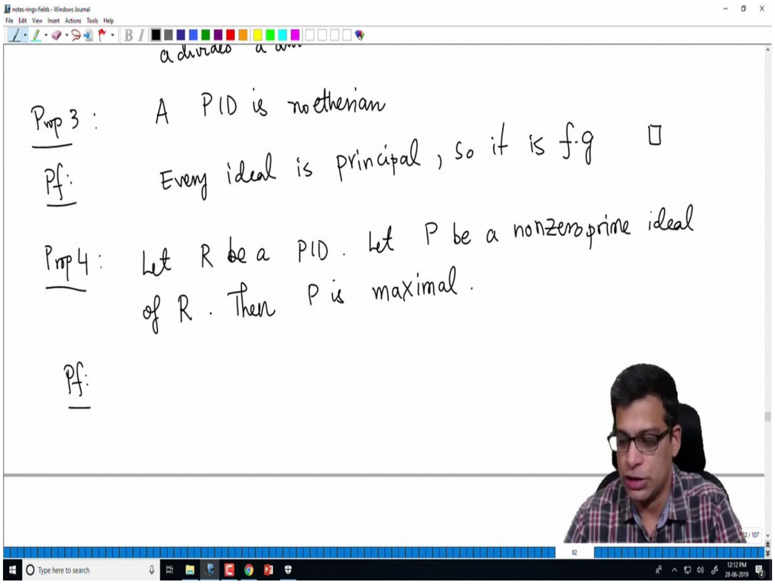
So, d is a unit, but this means the ideal generated by d is entire R, because a unit is an element which has a multiplicative inverse; that means, d times some element is one; that means, one is in the ideal generated by d. In other words it is equal to R, but, that means, the ideal generated by a and b is 1 right because d is a g c d of a and b; that means, the ideal generated by a b by previous proposition how do you get the g c d. It is the generator of the ideal generated by a and b which is R.

So, ideal generated by a and b is R; that means, there exist elements e comma s in capital R such that r s sorry r a plus s b is equal to 1 right because 1 is an element of R; 1 is an element of R. It is also simultaneously an element of the ideal generated by a and b. Any arbitrary element of the ideal generated by a and b is of the form r a plus s b where r and s are two ring elements.

But; that means, I can multiply both sides by c to get r a c plus s b c is equal to c; I am just simply multiplying this equation by c. So, r a c plus s b c is equal to c. But now note that this term a divides this term by definition right because it is a times r c. On the other hand a also divides this term this term. Why is this? Because a divides b c by hypotheses a divides b c. So, a divides s b c no matter what s is a divides s b c. This means a divides c right, because if a divides r a c a divides r s b c; that means, a divides their sum if an two numbers are two elements are divisible by a their sum is also divisible by a. So, a divides c which is what we require right.

So, this completes the proof of the proposition. The proposition claimed that any irreducible element is prime. So, if you have a PID every irreducible element is prime, I have just proved that I have started with an irreducible element which divides a product and it does not divide one of them and I have concluded that it divides the other.

(Refer Slide Time: 20:11)


notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help

a divides a

Prop 3 : A PID is noetherian

Pf: Every ideal is principal, so it is f.g □

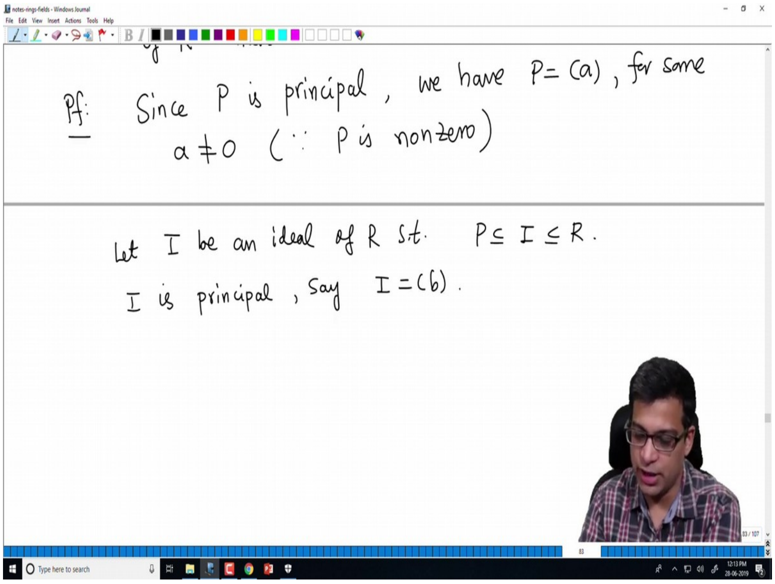
Prop 4 : Let R be a PID. Let P be a nonzero prime ideal of R. Then P is maximal.

Pf:

So, this finishes the proof of proposition 2. Some other properties of PIDs is that a PID is Noetherian. This is very easy right this is a one line proof: every ideal of a PID is principal. So, certainly it is finitely generated right it is much stronger in fact, than being finitely generated.

So, a PID is automatically Noetherian and one final do proposition. I will do just to illustrate some interesting properties of PIDs. Let R be a PID, let capital P be a non zero prime ideal of R then P is in fact, a maximal ideal; P is maximal. So, in a PID it is an interesting statement that which is in general certainly not true every non zero prime ideal is maximal. In fact, so, let us prove this.

(Refer Slide Time: 21:21)



Pf: Since P is principal, we have $P = (a)$, for some $a \neq 0$ ($\because$ P is nonzero)

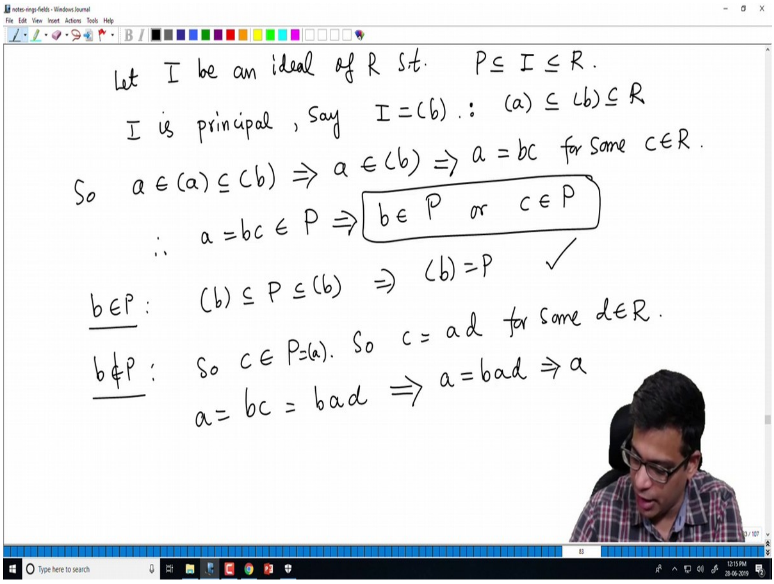
Let I be an ideal of R s.t. $P \subseteq I \subseteq R$.

I is principal, say $I = (b)$.

So, since P is principal the property of a PID that every ideal is principal is extremely powerful as this propositions are telling you. So, since P is principal, we have a generator a; let us say for some a non-zero, remember that is because P is non-zero. P is non-zero means P is not the zero ideal; that means, it has non-zero elements. So, it is generated by a non-zero element. Now I want to show that P is maximal, what is a maximal ideal? It is an ideal which is not contained in any bigger proper ideal.

So, we are going to take a bigger ideal, let I be an ideal of R such that P is contained in I and I is contained in R of course, I is contained in R, but the point is it is it contains P. So, again using the hypotheses that I is principal or P is R is PID, I is principal. So, suppose I is generated by a single element right.

(Refer Slide Time: 22:47)


notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help
Type here to search
12:15 PM
28-06-2019

Let I be an ideal of R s.t. $P \subseteq I \subseteq R$.

I is principal, say $I = (b)$. $\therefore$ $(a) \subseteq (b) \subseteq R$

So $a \in (a) \subseteq (b) \Rightarrow a \in (b) \Rightarrow a = bc$ for some $c \in R$.

$\therefore$ $a = bc \in P \Rightarrow \boxed{b \in P \text{ or } c \in P}$

$\underline{b \in P}$: $(b) \subseteq P \subseteq (b) \Rightarrow (b) = P$ ✓

$\underline{b \notin P}$: So $c \in P = (a)$. So $c = ad$ for some $d \in R$.

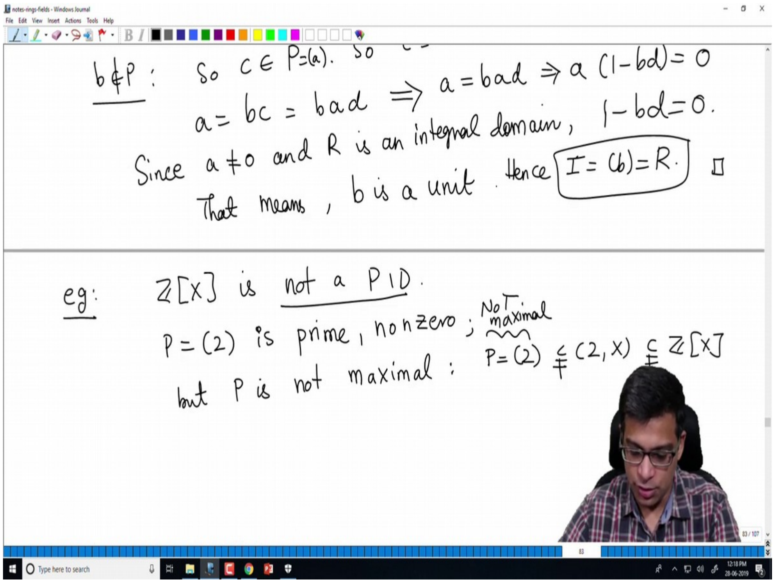
$a = bc = bad \Rightarrow a = bad \Rightarrow a$

So, what we have is, just rewriting this a is contained in ideal generated by a is contained in the ideal generated by b. So, a is an element of a which is contained in b so; that means, a is an element of the ideal generated by b; that means, a is equal to b c for some c in R by definition a is a multiple of b. So, a is equal to b c for some c in R, hence a equal to b c belongs to P and P is a prime ideal remember from a few lectures ago. What is a prime ideal?

It is an ideal such that if a product belongs to that ideal one of the elements belongs to the ideal. So, b is in P or c is in P. So, let us see both implications, both cases give us something right. So, suppose b is in P; in this case the entire ideal b is contained in P; that means, of course, we know that P is contained in b by hypotheses; that means, b is equal to P. So, this is ok. I am trying to prove that there is no bigger ideal in this case it just happens to be the same ideal.

Suppose b is not in P then what do we have here. So, c is in P right because remember either b is in P or c is in P because P is a prime ideal if b is not in P c is in P. So, and what is P? P is the ideal generated by a. So, c can be written as a d for some d in R for some d in R, but now let us start with this earlier equation a is equal to b c. So, a is equal to b c, but c we just observed is a d. So, this is b a d; that means, a is equal to b a d.

(Refer Slide Time: 24:57)



$\underline{b \notin P}$: So $c \in P = (a)$. So

$a = bc = bad \Rightarrow a = bad \Rightarrow a(1-bd) = 0$

Since $a \neq 0$ and R is an integral domain, $1 - bd = 0$.

That means, b is a unit. Hence $\boxed{I = (b) = R.}$ □

$\underline{eg:}$ $\mathbb{Z}[x]$ is $\underline{\text{not a PID}}$.

$P = (2)$ is prime, nonzero ; $\overset{\text{Not maximal}}{}$

but P is not maximal : $P = (2) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$

notes-rings-fields - Windows Journal
File Edit View Insert Actions Tools Help

That means, a times 1 minus b d is equal to 0. I am just subtracting b c d from both sides b a d from both sides and factoring a, but since b is non zero a is non zero and R is a integral domain 1 minus b d is 0 right. We have in an integral domain if two elements multiplied to 0; one of them must be 0 so; that means, b is a unit right; that means, b is a unit because b d is equal to 1. So, b has a multiplicative inverse.

So, b is a unit and hence the ideal generated by b which I called I is R ok. So, we are done because I have started with an arbitrary ideal that contains P and I have concluded it is either equal to P. It is either equal to P or it is equal to R ok. So, P must be maximal it is an interesting statement that every non zero prime is maximal. So, again we see that by in this example. So, this is not a PID as I proved earlier and in this there are the ideal P which is generated by 2 is prime non-zero, but P is not maximal right because P which is generated by 2 is contained in 2 X right. So, this is not equal to 2 and this is not equal to Z X.

So, again this is not maximal because it is contained in a proper bigger ideal. So, this again confirms that Z X is not a PID because in a PID we have shown that every non zero prime ideal is maximal ok. So, these are some of the properties of PIDs and in the future videos, we will talk more about this. So, just to recap what we have done PIDs are rings where every non-zero, every ideal is principal, the most standard examples for us are integers, polynomial rings over any field and fields. Of course, but some of the other nice rings that we have considered Z X, polynomial rings in more than two variables are not PIDs. PIDs have the nice property that any irreducible element is prime and they are Noetherian, any two elements have g c d s and every non zero prime ideal is principal.

So, let me stop this video here; in this video we have talked about principal ideal domains. In the next video, we will start learning about unique factorisation domains.

Thank you.