

Computational Commutative Algebra
Prof. Manoj Kummini
Department of Mathematics
Chennai Mathematical Institute

Lecture – 03
Quotient Rings

(Refer Slide Time: 00:17)

Computational commutative algebra
Lecture 3.



Welcome to the 3rd lecture in Computation Commutative Algebra. We continue our study about ideals, define prime and maximal ideals and then we look at some operations on ideals.

(Refer Slide Time: 00:31)

Defn: Let R be a ring and I an ideal.
 I is said to be a **prime ideal** if
 $\forall r, s \in R, \quad r \cdot s \in I \Rightarrow r \in I \text{ or } s \in I.$



eg: $2\mathbb{Z}$ is a prime ideal of \mathbb{Z} .
 \forall nonzero $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a prime ideal
iff n is a prime number.
 0 is a prime ideal of \mathbb{Z} .




Definition: let R be a ring and I an ideal. I is said to be a prime ideal, if for all $r, s \in R$, $rs \in I$ implies that, $r \in I$ or $s \in I$. So, for example, $2\mathbb{Z}$ is a prime ideal of \mathbb{Z} . In fact, for all non-zero $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a prime ideal, if and only if n is a prime number.

One has to for the statement to be true one has to put non-zero n , because if we take n to be 0, then the 0 ideal is a prime ideal, but 0 is not a prime number. So, the statement will not be correct as it is written. So, here we only look at I mean. So, maybe one should just say that, 0 is a prime ideal of \mathbb{Z} .

(Refer Slide Time: 03:10)

Defn. R is an integral domain (or a domain) if $\forall r, s \in R \setminus \{0\}$, $rs \neq 0$.

Exercise: R is a domain $\Leftrightarrow 0$ is a prime ideal




Definition: A ring R is an integral domain, and often it is just we just say, a domain. We will drop the word integral some, because it is some very unlikely to cause confusion. If for all non-zero elements $r, s \in R$, $rs \neq 0$. And then, proposition: which is an exercise. R is a domain, if and only if 0 is a prime ideal. We said last time that in one of the earlier lectures at 0 is always an ideal in any ring. Here R is a domain, if and only if 0 is a prime ideal.

(Refer Slide Time: 04:31)

Defn. An ideal I of R is **maximal** if it is a proper ideal and \nexists an ideal J st $I \subsetneq J \subsetneq R$



Exercise: (1) R is a fld $\Leftrightarrow 0$ is a **maximal** ideal.
Every **maximal** ideal is **prime**

(2) Give an example of a **prime** ideal that is not **maximal**



Now, we look at another kind of ideals. An ideal I of R is maximal if it is a proper ideal and there does not exist an ideal J , such that I is properly contained inside J , which is also a proper ideal. In other words, I is maximal among the proper ideals of R .

So, one can show the exercises to show the following:

1. R is a field, if and only if 0 is a maximal ideal. If R is a field, then that it has only two ideals, 0 and the full ring. So, then this is clearly maximal and one has to show the other way round, that if 0 is a maximal ideal then every non-zero element is invertible.

And another exercise 2. Every maximal ideal is prime, but the converse is not true. So, give an example of a prime ideal that is not maximal. So, give example of a ring and a prime ideal in it. In fact, you have already seen it. But I would not tell you what it is.

(Refer Slide Time: 07:04)

Defn: Let $I \subseteq R$ be an ideal.
The group $(R/I, +)$
can be given a ring structure by
setting $(r+I)(s+I) = rs+I$
 $\forall r, s \in R$.
(additive identity: $0+I$
mult. identity: $1+I$)



So, here is an important property about rings. Sorry before we put another definition. Let $I \subseteq R$ be an ideal. Then we can give a ring structure. So, we know that I is a subgroup of R under the additive operation.

So, we can talk about the quotient group that is also has an induced action. The group can be given a ring structure, meaning given a multiplication on top of this. So, to do we have to say what is multiplication? What is additive identity? And then one has to check that these properties satisfies the definition of a ring, but please do that ring structure by setting.

So, elements of this set $\frac{R}{I}$ are cosets; which we write $r+I$, and then some $s+I$. So, these are cosets and we define the product. So, this is the definition: $(r+I)(s+I) = (rs+I)$, for all $r, s \in R$. So, then let us just observe that the additive identity is the 0 of this group is this the 0 of the group which is a coset of 0, $0+I$ and multiplicative identity is the coset of 1 and it is $1+I$.

(Refer Slide Time: 09:36)

This is called the quotient ring of R by I
denoted by R/I

Prop. \exists a bijective correspondence is a surjective map.

$$\begin{aligned} R &\xrightarrow{\pi} R/I \\ r &\mapsto r+I \end{aligned}$$

$$\begin{aligned} \{ \text{Ideals of } R \text{ containing } I \} &\longleftrightarrow \{ \text{Ideals of } R/I \} \\ J &\longmapsto J/I := \{ r+I \mid r \in J \} \\ \pi^{-1}(K) &\longleftarrow K \end{aligned}$$

So, this is called the quotient of R by I and it is again denoted by $\frac{R}{I}$. So, rarely there will be a confusion whether one is referring to the quotient group or the quotient ring, but we will make it clear a few things. So, this is what it is. So, now, let us look at an example on how this is done in Macaulay.

(Refer Slide Time: 10:18)

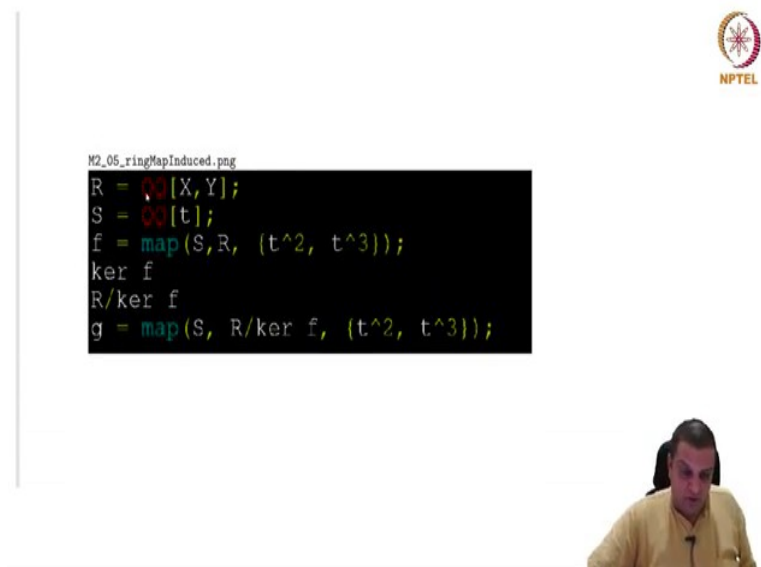
```

M2,04_ZZ17.png
i15 : ZZ/17
      ZZ
o15 = --
      17
o15 : QuotientRing

```

So, this is an example that we saw in the first lecture. We asked Macaulay ZZ/17 and it understands it correctly and this is what it said, it is a quotient ring. So, now, let us look at more one more example on finding the kernel.

(Refer Slide Time: 10:40)



So, this goes back to the example that we saw. The first example, that we saw of a ring map. Polynomial ring in two variables mapping to polynomial ring in one variable. X goes to t^2 , Y goes to t^3 and we asked for its kernel.

Then we ask for the quotient during R modulo the kernel and then we define a map. So, this will be part of the exercises that, if there is a map from R to S then, there is a ring map from the quotient ring $\frac{R}{\text{Ker } f}$ to S . So, existence of this; you will verify in the exercises and then there is an induced map and you should run these lines of code in Macaulay2 and understand what the output says.

So, I will not show you the output. This is part of the exercises that you should do with Macaulay. So, here is the important property which relates. There exists a bijective correspondence, between two sets. Ideals of R containing I and the other set that we considering is, ideals of $\frac{R}{I}$.

Now, what is the correspondence, if you have an ideal J here which contains I , that goes to the residue of I and what exactly do we mean? This we mean $r+I, r \in J$. So, we just look at the cosets of elements inside J . So, it is just J/I . So, what? And from this side R/I . For if you take an ideal of R/I . So, maybe I should have said something before this. Let me add a line here.

What is that? The map from $R \rightarrow R/I, r \mapsto r+I$. Let us call this map π . Like this is a line that I wanted to add is a ring map is a surjective ring homomorphism. So, one needs to observe that thing. And if you have an ideal K here, then send that to the inverse image of K .

So, there is a bijective correspondence. So, there are some things to be checked. That if you have an ideal containing I , then if you take on this side, it is an ideal of R/I and if you have an ideal of R/I call it K , then its inverse image under the map is. So, this is a surjective map.

So, you can just. We can just anyway talk about its inverse image. It is an ideal containing I . So, there is a bijective correspondence like this. Sorry we are. The proposition is not done yet.

(Refer Slide Time: 14:30)



Under this correspondence

$$\{\text{prime ideals of } R \text{ containing } I\} \leftrightarrow \{\text{prime ideals of } R/I\}$$

$$\{\text{maximal ideals of } R \text{ containing } I\} \leftrightarrow \{\text{maximal ideals of } R/I\}$$

Proof: Check that the two functions are inverses of each other.

Let $P \supseteq I$ be a prime ideal. WTS P/I is a prime ideal of R/I .

Under this correspondence prime ideals, prime ideals of R containing I . So, if you consider this set, this is a subset of the other one. This corresponds to prime ideals of $\frac{R}{I}$.

Similarly, you can replace prime by maximal here, and here also maximal. So, from what we have said earlier, this is a subset of that, this is a subset of this and both of these are I mean subsets of this. So, there is a bijective correspondence here, which restricts to a bijective correspondence on these subsets. And what is a. what do we mean by bijective correspondence?

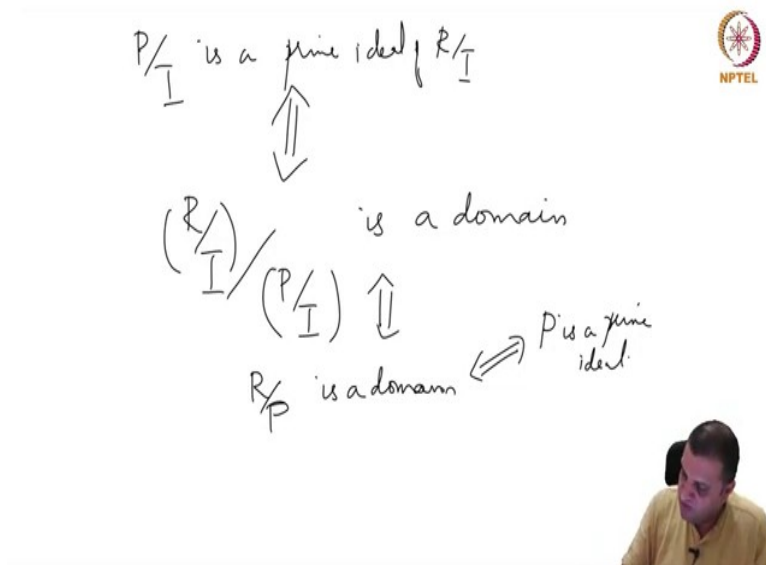
So, in this particular situation, we have defined a function from the left side to the right, here we have defined a function from the right side to the left and both these functions are identity maps. So, if you start from a J here, go there and apply this map you will get J . Start from a K here, go here and then take its inverse image and then apply this operation we will just get K .

So, these are that is why these are bijective correspondence. And under this thing this is there is this map and proof. So, whatever I just said is the proof that bijective correspondence. So, now, I will just sketch . So, proof. So, the first part is check that, the two functions are inverses of each other. That is straightforward.

Now, the question is, if you have a prime ideal here. So, I will just prove the first thing I will just prove I will just prove this. So, let P containing I be a prime ideal. We want to show that

$\frac{P}{I}$ is a prime ideal of $\frac{R}{I}$.

(Refer Slide Time: 17:48)

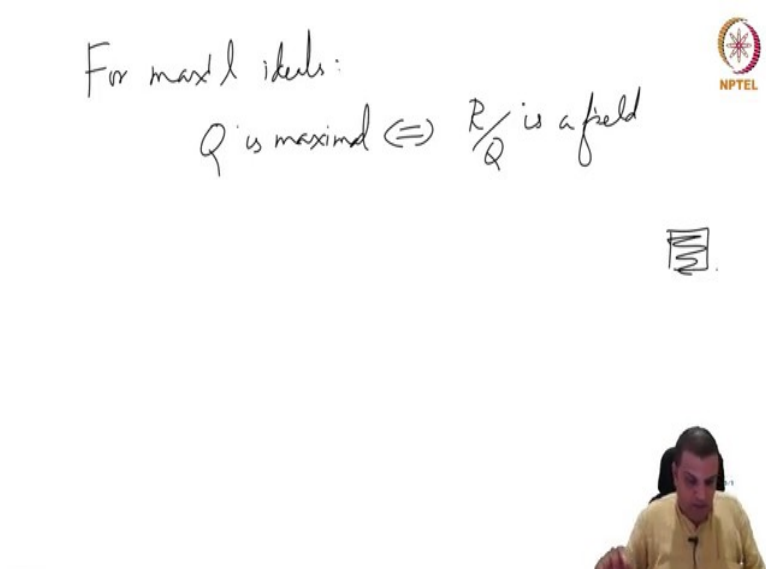


P/I is a prime ideal of R/I
 \Updownarrow
 $(R/I)/(P/I)$ is a domain
 \Updownarrow
 R/P is a domain $\Leftrightarrow P$ is a prime ideal

So, one can check that as follows. So, P/I is a prime ideal of R/I if and only if $\frac{R/I}{P/I}$ is a domain,

but what is this? This is just $\frac{R}{P}$ which is a domain. And that is actually the condition that P is a prime ideal.

(Refer Slide Time: 18:39)



For maximal ideals:
 Q is maximal $\Leftrightarrow R/Q$ is a field

So, now what about the maximal ideals? Use the fact that, Q is maximal if and only if, $\frac{R}{Q}$ is a field. Use this and then apply the same argument as one did what one did for prime ideals and similar argument. So, now let us look at couple of examples in Macaulay.

(Refer Slide Time: 19:31)



So, there is a simple command. So, here we take the ring $R=QQ[X,Y]$, then we take the ideal generated by the product XY and then we ask, is it Prime? So, there is a command called `isPrime`, this is a capital P, `isPrime ideal this?` And it says its false and that is, because in X is not there in this ideal, Y is not there in this ideal, but the product XY is there.

So, it is not a prime ideal. But of course, when you use commands like this, one should be a little careful. So, let us try in a very similar example.

(Refer Slide Time: 20:06)



So, now we look at the same thing. I mean similar thing. R is a polynomial ring in one variable over the integers, then we ask, isPrime ideal (X) ? Which it is, because polynomial ring in one variable modulo (X) would just be integer which is a domain.



So, this we know that this is a prime ideal, but if you ask Macaulay that question it says, expected base field to be QQ and actually few more. When I took screenshot I chopped the lines, but this is an error that is, because the thing has not been programmed to handle even cases like this.

So, before we use this commands one should be one should verify the context in which it would correctly solve. So, it is just a minor warning when one tries to use these things. So, now, we look at some operations on ideals .

(Refer Slide Time: 21:02)

Operations on ideals

Extension: $f: R \rightarrow S$ ring map
 $I \subseteq R$ ideal.
 $f(I)$ ~ not an ideal in general.
 $2\mathbb{Z}$ is an ideal of \mathbb{Z} . $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$
 $f(2\mathbb{Z}) = \text{set of even integers}$
NOT an ideal of \mathbb{Q}



The first thing is called Extension. So, $f: R \rightarrow S$ is a ring map. I is an ideal of R . Now, we can just look at $f(I)$. Is this an ideal? This is not an ideal, in general. In fact, one does not have to go very far to find an example. $2\mathbb{Z}$ is an ideal of \mathbb{Z} . Take f to be the natural map from \mathbb{Z} to \mathbb{Q} which is the inclusion map. Integer sitting as rational numbers with denominator 1 and $f(2\mathbb{Z}) = 2\mathbb{Z}$. $2\mathbb{Z}$ is the set of even integers.

This is not an ideal of rationals and that is because rational the set of rationals is a field. There are only two ideals, 0 or the whole ring and this is just it is neither 0 nor the whole ring. So, it is not very difficult to see this thing.

(Refer Slide Time: 22:49)

Defn. The ideal of S generated by $f(I)$ is called the extension of I to S .
(or extended ideal)
notation: $I \cdot S$



But definition: The ideal of S generated by $f(I)$ is called the extension of I to S . It is sometimes called extended ideal or the extended ideal. And notation often is just IS .

Quite often the map is clear from the context. In any case, this notation means ideal generated by the image of I under f inside S . f is defined to be this map from R to S , X goes to t^2 and Y goes to t^3 . So, we ask $f(X)$ it is a t^2 .

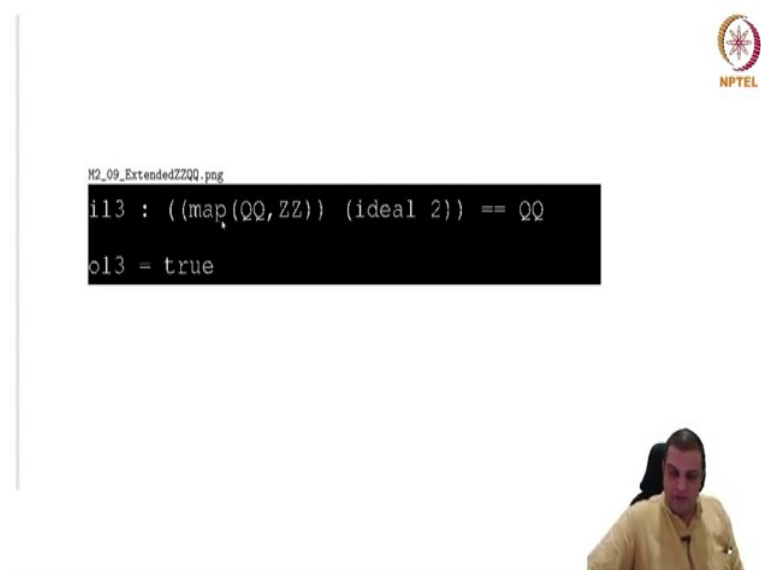
(Refer Slide Time: 24:14)

```
M2_08_ExtendedIdeal.png
i11 : R X
o11 = t^2
o11 : S
i12 : f ideal (X^2, Y)
o12 = ideal (t^4, t^3)
o12 : Ideal of S
```



Now, we ask f of ideal generated by X^2, Y and Macaulay has been programmed to realize that f just taking the set theoretic image is not going to give an ideal. So, just take the ideal generated by it. So, Macaulay already outputs ideal generated by it and X^2 goes to t^4 and Y goes to t^3 and f of the ideal (X^2, Y) is the ideal generated by these. One more example, so this is the example in which we asked.

(Refer Slide Time: 24:48)



So, let us unravel this thing. So, the point of this example is to we do not need to label all these things all the time. So, here we take the map from $\mathbb{Z}\mathbb{Z}$ to $\mathbb{Q}\mathbb{Q}$ and Macaulay knows what that map is. So, that is between this bracket and this bracket. Apply to the ideal generate by 2 that is $2\mathbb{Z}$. So, this is going to be an ideal of \mathbb{Z} . You are applying this map to this ideal and then we ask is it equal to rationales?

So, this equal to the set of rationales and it says it is true. And the point first point it is already mentioned it is not necessary to label all these things, one can just compute it like this. And the brackets here that I have used are to demark it mark the expression here. So, Macaulay to understands what we wanted to understand.

So, you should do an exercise in which you remove various pairs of brackets here and see which ones work and which one is do not.

(Refer Slide Time: 25:59)

Contraction of ideals, $f: R \rightarrow S$ ring map
 $J \subseteq S$ ideal.
 $f^{-1}(J)$ is an ideal of R .
Contracted ideal.



One more definition: contraction of ideals. So, again $f: R \rightarrow S$ be a ring map. This time J is an ideal of S . And we ask. So, what do what can we check? $f^{-1}(J)$ is already an ideal of R . And $f^{-1}(J)$ called the contracted ideal.

(Refer Slide Time: 26:52)

M2_10_preimageIn.png

```
R = QQ[X]; S = QQ[Y]; J1 = ideal (Y);  
J2 = ideal (Y^3); f = map(S,R, {Y^2});  
preimage (f, J1)  
preimage (f, J2)
```

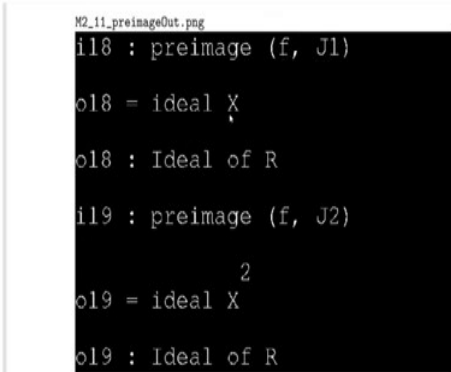


So, now let us look at. So, here we look at R , which is polynomial ring in one variable over the rationals. Take $R = \mathbb{Q}[X]$ and $S = \mathbb{Q}[Y]$. I defined an ideal like this $J_1 = (Y)$, $J_2 = (Y^3)$. So, just note that the semicolon suppress the output and we do not need to see. If we put this

command we know what it is going, what it does, we do not need to see the output specifically.

So, we can put a semicolon. And if you put a semicolon, you can give multiple commands in the same line itself. So, I just put three of them in one line, two of them in the next line. So, this is just f . So, what does this say? This says X the under this map X goes to Y^2 . Then we ask. So, the command in Macaulay is $\text{preimage}(f, J_1)$. So, this is just $f^{-1}(J_1)$ and here is a $f^{-1}(J_2)$.

(Refer Slide Time: 27:46)



```
M2_11_preimageOut.png
i18 : preimage (f, J1)
o18 = ideal X
o18 : Ideal of R
i19 : preimage (f, J2)
o19 = ideal X2
o19 : Ideal of R
```

And here so, I just show you the relevant output $\text{preimage}(f, J_1)$, this is $f^{-1}(J_1)$. It is the ideal generated by X . Preimage of J_2 under f is the ideal generated by X^2 and this is an ideal of R . So, you should verify these calculations by hand. So, now we continue little bit more of these things.

(Refer Slide Time: 28:28)

Defn: The radical of I is the set
$$\sqrt{I} := \{r \in R \mid \exists m \geq 1 \text{ such that } r^m \in I\}.$$

• $I \subseteq \sqrt{I}$
• \sqrt{I} is an ideal. (Exercise).



So, next is radical. The radical of an ideal I is the set, which we denote by the radical symbol \sqrt{I} and $\sqrt{I} = \{r \in R \mid \exists m \geq 1 \text{ such that } r^m \in I\}$.

The radical ; so, the first point that we would like to make notice that the ideal I itself is in the radical of I , that is $I \subseteq \sqrt{I}$. Because you can just take for an element of I . We can just take m to be 1. So, I here sorry that is the definition here we are liking some properties. Another property is that, radical of I is an ideal.

So, this I will sketch the argument in the exercises. And, few more properties that again, you will work out in the exercises.

(Refer Slide Time: 29:50)

Defn. Say that I is a *radical ideal* if $\sqrt{I} = I$.



Exercise. (1) prime ideals are radical.
 (2) $I_\lambda, \lambda \in \Lambda$ radical ideals $\Rightarrow \bigcap_{\lambda \in \Lambda} I_\lambda$ is a radical ideal



So, before that we just say definition: say that I is a radical ideal if $\sqrt{I} = I$. So, some exercises.

Exercise 1. Prime ideals are radical.

2. Let us say that, if we have a family of radical ideals, $\{I_\lambda\}$, λ in some index set Λ . Then the intersection $\bigcap_{\lambda \in \Lambda} I_\lambda$ is radical.

(Refer Slide Time: 31:02)

Defn. The *nil radical* of R is $\sqrt{0}$.



Exn. $\sqrt{I} = \text{preimage of the nil radical of } R/I$
 $\varphi_{R/I} \quad (R \rightarrow R/I)$



A definition: The nilradical of R , it is the radical of the 0 ideal. In other words, elements for whom some positive power is 0 . And an exercise, radical of I is the pre-image of the nilradical of $\frac{R}{I}$ for the natural surjective map $R \rightarrow \frac{R}{I}$.