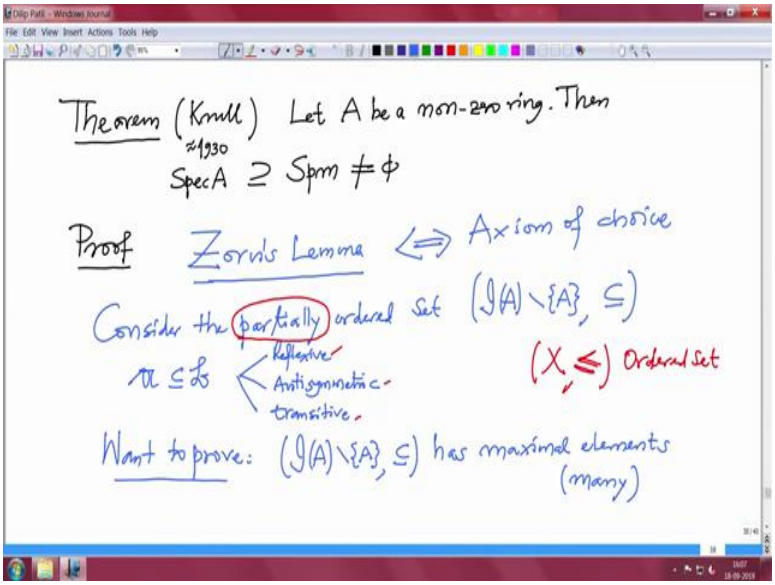
Introduction to Algebraic Geometry and Commutative Algebra
Professor Dr. Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru
Lecture 06
Krull's Theorem and consequences.

So, in the last half we have seen definition and some examples of Prime Ideals and Maximal Ideals and also we have a criterion. How to test some ideal is maximal or prime and they are just going modulo, then and then the new ring weather it is an integral domain or is it a field. This thing will test us weather the ideal is prime or maximal. But now, the original question what I was asking today, that weather is there a prime ideal at all or is there a maximal ideal at all and that is answered by the following theorem.

(Refer Slide Time: 01:21)



So, this is very important theorem and as you will see the proof is very easy, this theorem is called Krull's Theorem. Krull has put this in the beginning of twentieth century that is 1930s. So, I will just here, 1930s approximately. So, he says let A be a non-zero ring, then Spm is non empty that means there at least one maximal ideal there and once this maximal ideal this spectrum is a bigger set. So, if the subset is nonempty, then the bigger set is also non empty. So, that answers our question and let us prove this.

Proof, so the proof uses what is called Zorn's lemma, I will state it and as you might be aware that this Zorn's lemma one cannot prove it. We can only prove it, it is equivalent to what is known as axiom of choice and I will not go into much of this because that is really a topic of set theory and in mathematics Zorn's lemma is very well known and taken it, the statement is

true, but true means what? It is equivalent to some other axiom of set theory. So, it is really an axiom.

So, what is that we want to prove? We want to prove that there are maximal elements where we are considering these order set, these partially ordered set. Consider, the partially ordered set, which set? I A, ideals in A and remove this unit ideal and this is ordered by a natural inclusion. So, you see A contained in the ideal B, this is a relation on this set and it satisfy which properties? I am just recalling what is a partially ordered set.

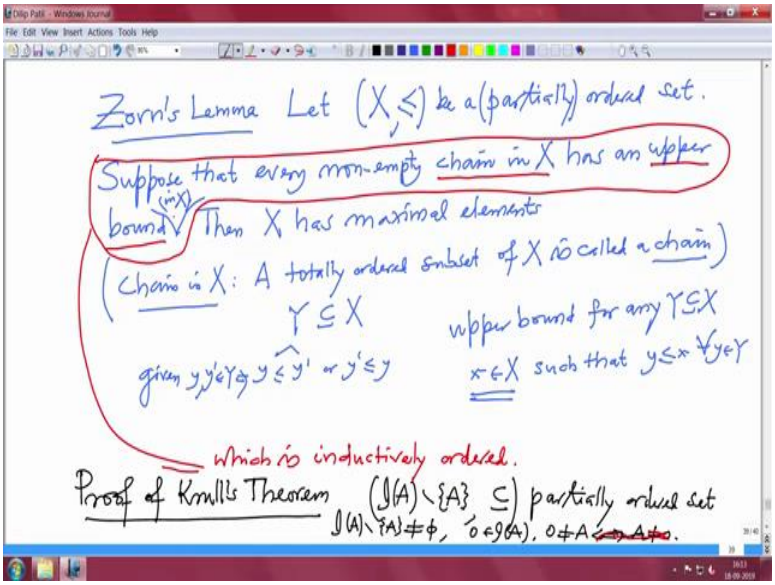
It should be reflexive, it should be transitive and it should also be it is also antisymmetric in this. So, because A is contained in A, if A is contained in B, B is contained in A, then A equal to B and if A is contained in B, B is contained in C. Then A is contained in C.

So, this is reflexive antisymmetric and transitive, actually if this, I just wanted to make this comment also some time that this is, if you see older books this word is not there, it is an ordered set. So, an ordered set is a set, X with a relation on that which is denoted by this is less equal to, with that relation it should satisfy this three properties then you call it an ordered set.

But somehow in the literature this is called a partially ordered set. Maybe mainly because of computer science people. So, we want to prove what? We are considering this ordered set, and what is to be proved? We want to prove this set, this partially ordered set has maximal elements. That maximal element will give you the maximal ideal, that is by definition of the maximal ideal and as you see there could be more, many more maximal ideals in a partially ordered set. Because it may not be, it is not totally ordered. So, any two elements are not comparable.

So, once you start doing some chain will end here and some chain will end somewhere else. So, these two definitely both of them will be maximal elements but they may not be equal. So, there may be many maximal elements. So, I just note here many may be, may not be unique. So, we need a statement how do you test a given partially ordered set as a maximal element, what condition do you need to put? So, that is precisely answered by Zorn’s lemma.

(Refer Slide Time: 07:25)



So, let me state that Zorn's lemma now. So, this is Zorn's lemma, let I will write here X less equal to be a partially ordered set. I would like not to write like this, but just in order not to get confused with the later books I am writing it. If or suppose that, every non empty chain in X has an upper bound. Then X has maximal elements. This is everything with respect to this relation.

So, let me explain what are the terms in this statement. So, the first one is chain in X. So, what is the chain in X? So, I am writing it here, chain in X means, a totally ordered sub set of X is called a chain that is a chain that means Y is a subset of X and any two elements of Y, y and y prime they are comparable, either this or y prime is less equal to this. So, given y and y prime in Y you have either this or this that means you can compare them with respect to this given order that is a chain and what is an upper bound for a subset, an upper bound for a subset?

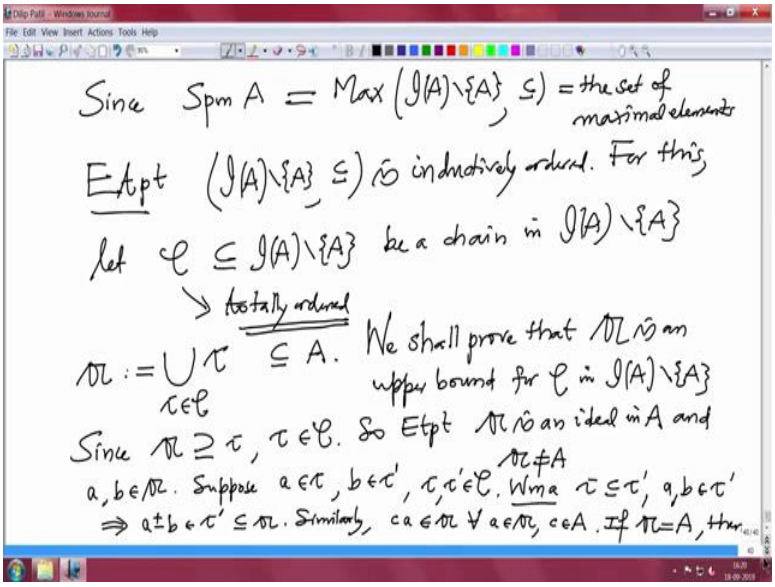
Upper bound for any subset Y of X this is an element X in X, such that y is less equal to x for every y in Y and this X may belong to Y or may not belong to Y. So, strictly (())(10:36) one should write here upper bound in X let us just to be precise. So, that explain this term upper bound and X as a maximal element is also clear both these whole statement from here to here that every non-empty chain has an upper bound in X this is also abbreviated as partially ordered set which is inductively ordered.

That is the meaning of this is this sentence, every chain in X has an upper bound in X. So, let us come back to our proof of Zorn's lemma, no not Zorn's lemma, sorry theorem of Krull. So, what do you want to prove? We want to prove. So, already we have noted that, this does

not allow me to go. So, proof of Krull's theorem, we are considering I A minus this unit ideal (())(12:11). This is partially ordered set we already noted and we definitely know this is non empty, this set is non empty I A minus this A, this is a non-empty set because 0 belong there, zero belongs to I A and 0 is not A this is the condition because 1 is here and 1 cannot be 0.

So, this is equivalent to saying the ring is non-zero. Already this says that it is non zero. I do not have to right this part that is given to us. So, therefore, given assumption says that this is a nonempty set. Now, I want to conclude that this set as a maximum elements. So, I have to prove this set is inductively ordered that means if I have taken chain in X it should have an upper bound in X.

(Refer Slide Time: 13:29)



So, since Spm of A is by definition max IA minus unit ideal (())(13:50) this is the set of maximal elements. Enough to prove that this set IA minus this with respect to this is inductively ordered, for this let C contained in this be a chain in this set that means it is a subset and it is totally ordered. Which are the upper bound also we are assuming.

So, what is this C? C is come set of ideals. C is a set of ideals, non-unit ideals and we want to produce a upper bound for this. So, let us consider union c this is ideal c in the chain in this subset C. I am considering this union, this is a union which is contained in the ring A and I want to claim that this is an upper bound for C. So, we shall prove that, let us give some name to this. So, let us call this as a, a is an upper bound for C in this and then we are done. If you prove this we are done.

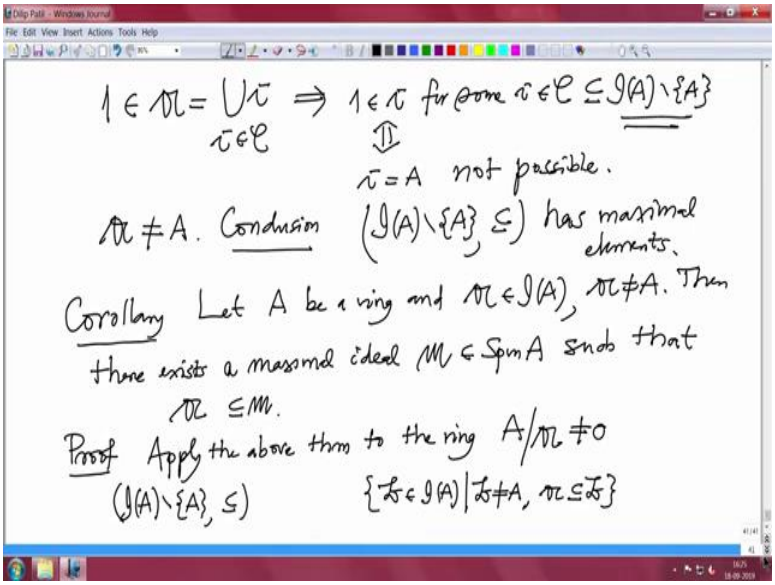
So, it is clearly an upper bound because this a, this subset a is bigger than every c in ideal. So, since a contains every ideal c. The real problem to prove that it is actually an ideal. So, enough to prove that a is an ideal in A and a should not be this, a is not equal to A, it is a proper ideal. Then it will be an element here and therefore it will be done. So, let us prove this A is an ideal.

So, what do I have to prove? That means you have to prove that it is a sub group and it is close under arbitrary scalar multiplication by of a capital A. That is where we will use the fact that this C totally ordered. So, take any element in the union a is in the union a and b both are in this a that means this a and b are in the union. So, therefore, this a will belong to one of them b will also belong to one of them. So, suppose a belongs to some c and b belongs to some c not this c. a belong to some c this, this is a gothic c and this is a script C and B belong to some c prime.

But then this c and c prime they are elements in the chain, so because of the total order, we can assume, we may assume c is contained in c prime then a is there and b is also be there. Then a and b both will belong to this c prime. But c prime is an ideal, so that will imply that a minus b will belong to c prime and c prime is contained in this a. Therefore, this is a group abelian group and now we have to check that arbitrary but that is same. So, similarly, c times a belongs to the ideal a for every a in this a and c is in the ring a.

Same thing again look at a and a will belong to some ideal c and this c is in a. So, c times a will belong to that particular c because there is an ideal and therefore this is more easier than the plus minus, this is we should write this. So, what did we check? We check that, this union is an ideal now we have to check it is a proper ideal but that is also very simple, if it is not a proper ideal, if a is equal to capital A, then.

(Refer Slide Time: 20:14)



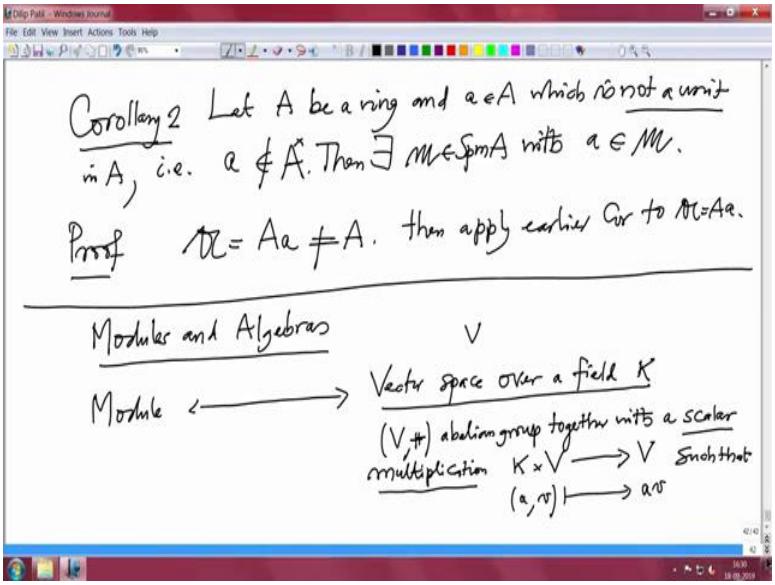
Then, what will happen? 1 will belong to the union, 1 belongs to the a that is the union c, c in C. Therefore, 1 belongs to one of them, so 1 will belong to 1c for some c in C but this was a subset of IA minus A. So, if 1 belongs here but that is equivalent to saying c will be the ideal A and it is not possible. Because this is contained not possible. So, that proves that, this A is a proper ideal and therefore we have proved every chain has an upper bound and therefore conclusion this set is partially ordered set has maximal elements, which are precisely the maximal ideals.

So, that proves that given any nonzero ring it has some maximal ideals. So, sometimes it may be unique, only 1, sometimes it may be finitely many, sometimes it can be infinitely many and so on. One corollary we can mention whatever we did above that we can do it little bit finer. So, let A be a ring and A, ideal A which is a proper ideal then there exists a maximal ideal m in A. So, that is m belongs to Spm A. Such that A given ideal a, this is a proper ideal contained in m.

Proof, now what do you consider? Again we apply the Zorn's lemma or we can apply the above theorem to the ring A modulo this a and because A is a proper ideal, this ring is nonzero. So, we can apply and we can take it a maximal ideal here. So, there is a maximal ideal here. But that maximal ideal will come from the maximal ideal of A, you do either this or when you consider that this set. We have consider this set in the Zorn's lemma now in above theorem we have considered this set, this partially ordered set and then proved that this has maximal ideal.

Now, instead of this you can consider not all ideals but ideals b, such that, first of all b is proper ideal b is not a, and a is contained in b. So, consider this set and then apply the similar thing that means it will have maximal elements that will obviously contain a by definition. So, more than this we will also prove little bit better connection the same thing again we will prove, later with better notation.

(Refer Slide Time: 24:46)



But also one more corollary I want to note, corollary 2, let A be a ring and an element a in A, which is not a unit. That is this a is not in A cross this is set of all units. You should use the notation again, more often so that you will get used to the definition this is A units. Proof, let A be the ideal generated by the small a. Then because A is not a unit this ideal is proper ideal and then apply only a corollary. I have not completed the statements, then there exists a maximal ideal in A with a belonging to m. Then apply earlier corollary to the ideal A which is the principle ideal.

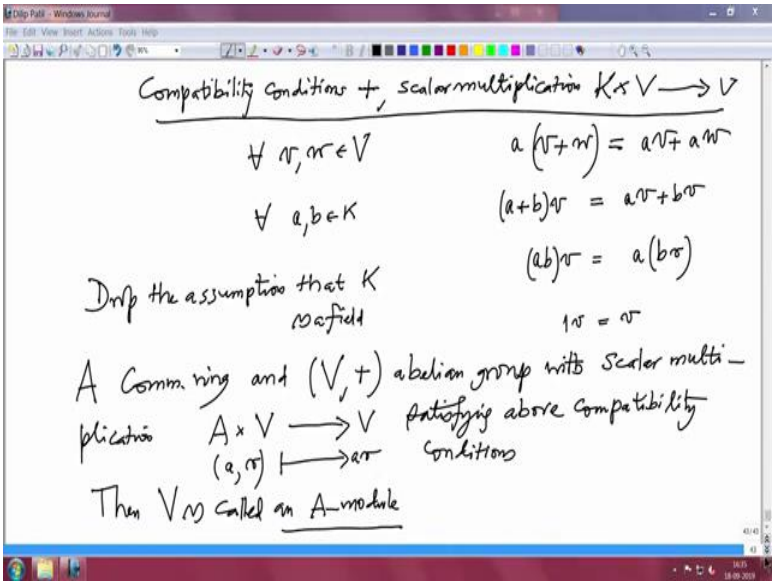
So, this is also handy sometimes because when you want to prove some element in a given ring as a unit. Then you should prove that this A does not belong any maximal ideal. Now, for some more examples I need the concept of modules and algebras. So, I think I will start today slowly. So, I will write here Modules and Algebras.

So, this will give us more, algebras are very important you have studied probably in linear algebra, algebra, one fixed algebra is studied there and it is very important to be very precise. So, let us recall a module is an analog, so module this word is an analog for a vector space. So, for a vector space you need a base field. So, this is usually written as vector space over a field K.

So, what does it recall in a minute? So, the usually the notation use for vector space is V. So, what is a vector space over a field? So, field is given to you, so vector space is an abelian group V plus, this is an abelian group, together with a scalar multiplication and what is a scalar multiplication? Scalar multiplication is a map from A cross V to V and this map the image of pairs a, comma v is denoted by a times v that is just, so this A is K.

So, that is a scalar multiplication, scalar multiplication one should think a map from K cross V to V, if you have a pair of an element in K and V an element in V. Then there image is written as this and this scalar multiplication and this Abelian group addition that should be compatible with each other. So, there are obvious conditions, such that so since there is no place I have to go to the next page.

(Refer Slide Time: 29:50)



So, what does it satisfy, it is very important to, these I call it a compatibility conditions between the Abelian group plus and scalar multiplication this K cross V to V. So, what are that, now here will one has to be little careful because there is a plus in K also and we are denoting by the same symbol so it should be clear from the way of writing. So, scalars usually denoted by a b c and vectors elements of V are denoted by V W etc.

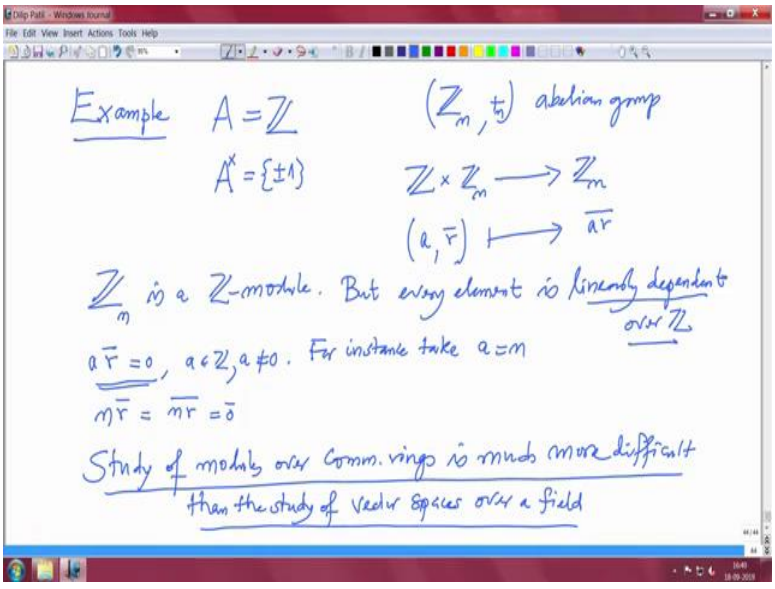
So, if I have two elements v and w than what can I do? I can add 2 in v and w in V and then multiply by a, multiply by a means scalar multiply. But on the other hand I can scalar multiply a by v, v by a and v by w, not v by w, a by w, a w and add them in V this should by same result. Similarly, if we have two scalars a and b and I can add scalars in the field and multiply by this v, multiply means scalar multiply this should be same as a v plus b v this addition is obviously in v, this addition is in K.

Similarly, for the multiplication in K, so that is a b this is multiplied in K and now scalar multiplication this should be equal to b v and then a and then obviously one of them is 1 multiplied by V is V and this are true for all v w in v all a b in K then you call it a vector space over the field K.

Now, in this definition if I remove the fact that this K is a field then and also demand its compatibility condition then I will have an Abelian group. So, now K may not be a field, so K is drop the assumption that K is a field that means what? That we are considering A commutative ring and I will use the same notation V and an Abelian group V plus with scalar multiplication from A cross V to V again denoted by same everything same satisfying above compatibility conditions is called an A module.

So, such a thing is called, then V is called an A module. Now, one might ask what is the difference then why do you need to study module you already studied Vector spaces but there is a big difference because when you drop this assumption that K is a field then you know you have a ring which is not a field then it may not have every non zero element may not be inevitable and that will, that will not give us the same result in fact one has to be little little more careful with this.

(Refer Slide Time: 35:17)



For example, so let us see, I just want to see some example, see remember in a linear algebra first theorem proves every vector space has a basis, basis means linearly independent subset which is also generating set. I will repeat this definition but just to show you that there is big difference to study modules is much more difficult than studying vector spaces because the very basic result that every vector space has basis will fail in case of modules.

So, for that I want to give you examples so now let us take given ring A equals to Z. Now, you see the only unit in these are plus minus 1 and let us take the Abelian group Z mod n plus dot modulo n. So, this is an Abelian group, this is a finite group and this clearly has a scalar multiplication of Z.

So, what is the scalar multiplication we need such a map but you have integer a and residue class r bar then where do you map it? You multiply as usual a r and take the bar of that taking bar means divide by n and taking a residue. So, this is clearly compatible with these so natural this is a natural map and it is compatible therefore with this this Z mod n is a Z modulo.

But in this Z module every element is linearly dependent over Z. What should I produce for this? That means what am I checking if I take any element here r bar this if I multiply by suitable a it should become 0. So, this is dependence relation it will become if a is non zero. For instance, you can take a equal to n. Then n times, n times r bar is by definition n r bar but it is already divisible by n. So, the remainder is 0.

So, therefore, what we checked in this example is every element is linearly independent. So, leave alone you cannot find any linearly independent subset in this. So, there will not be any basis and once there is no basis many things will fail, study of linear maps will become more complicated. So, therefore, I will just mention here modules, study of modules over commutative rings is much more difficult than the study of vector spaces over a field.

This is certain and as time goes on, I will tell you the examples which will not, which will differ from examples of vector spaces. So, we have to study these, so large these modules will also be very important in the study of commutative algebra and they are also used in while studying the geometry. So, this algebra set up is big for the studying algebraic geometry that is one of the reason why these algebraic geometric type courses are not offered in under graduate level. So, with this I will stop this lecture and we will continue in the next lecture, thank you.