Introduction to Algebraic Geometry and Commutative Algebra

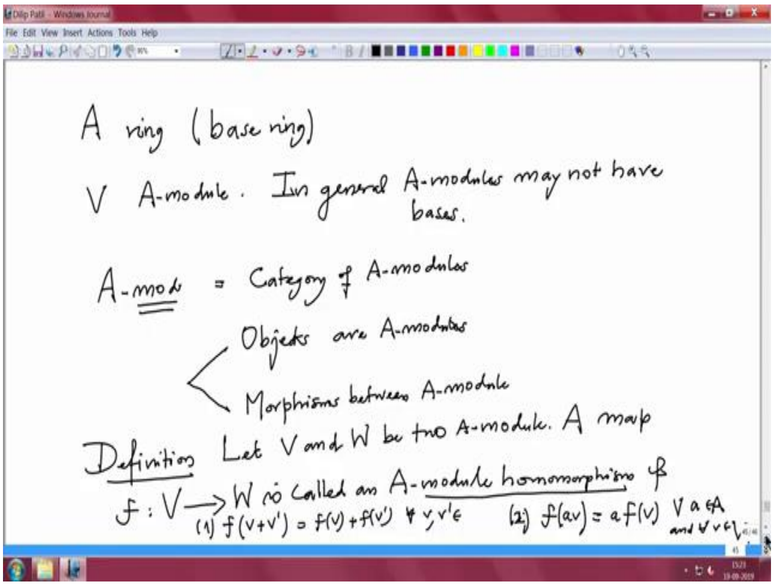
Professor Dr. Dilip P. Patil
Department of Mathematics
Indian Institute of Science, Bengaluru

Lecture 07

Module, submodules and quotient modules

Let us continue our lectures, recall from the last lecture I have defined what is a module. Which is generalization of a vector space the only different is the base is not filled anymore its commutative ring. So, let me continue that.

(Refer Slide Time: 00:55)



So, we have fix ring A, this is a ring and usually ring recall that, I mean a commutative ring and this is sometimes I will keep referring as base ring and module V is an A module. I will denote many books will write m, n, etc for the module, but I will keep the same notation from linear algebra and I will keep writing v, w, etc modules over A. And we saw that in general modules may not have bases. In general, A modules may not have bases.

But to this topic I will comeback after sometime, the reason being I want to go back to geometry and I will do with the minimal module which is needed for our purpose and then comeback to it little later. So, whenever we have like we have rings, then we have this category of rings, groups, category of groups. So, similarly, the collections of A modules, A mod this is, I want to denote this category of A modules by this.

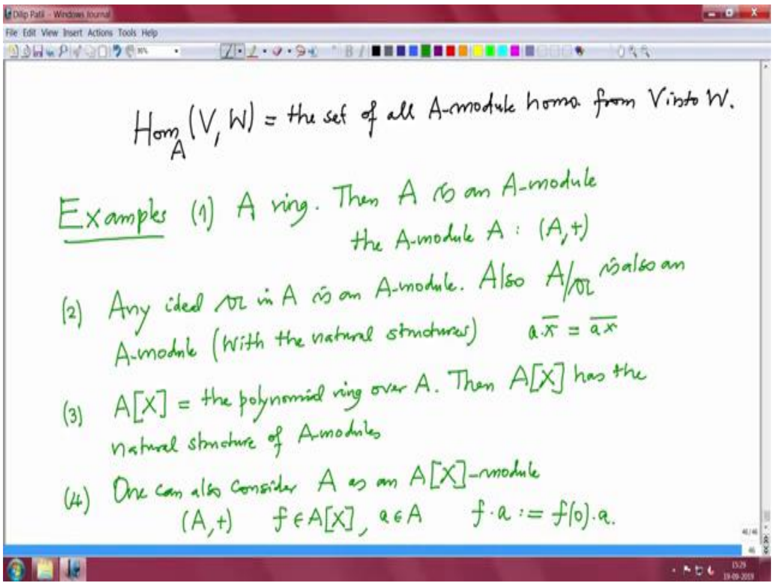
So, this is the category of A modules, once again I will recall. What I will be really still not very 100 percent precise. So, what is the category? Category has two input data, one is objects. So, what are the objects we are talking about? The objects we are talking about are the modules over this fixed ring A, fix base ring A.

So, objects are A modules and secondly morphism between the modules, morphisms between A modules. And together they should satisfy some obvious properties and with all this it is called a category of A modules like we have category of rings, we have category of groups, we have category of sets and we will keep adding some more examples and one fine day I will define more generally what do you mean by category precisely.

So, this is just a working knowledge. So, right now our problem is what are the morphism between the two modules, so that is the definition. So, let V and W be two A modules, a map f from V to W is called an A module homomorphism, A module homomorphism. If two things, see what is the module? Module has two structures, one is additive structure in which it is an Abelian group and the other is scalar multiplication map. So, this map should preserve both these structures. So, what does that mean? If 1 f is, f preserve the addition that means f of V plus V prime equal to f of V plus f of V prime for all V, V prime in V.

This means it is an Abelian group homomorphism and second one is, second one is it should preserve the scalar multiplication also that means f of a times v equal to a times f of v. This should be true for all a in A and all V in V. We should see some examples. So, an A module homomorphism is a map from the module V to module W, which preserves addition and also scalar multiplication. Sometimes A module homomorphism also shortly called A linear maps between V and W.

(Refer Slide Time: 07:31)



And the set of all A modulo homomorphism from the module V to module W is denoted by hom V, W this is the set of all A module homomorphisms from V into W. So, to see some examples first of all we need to see some examples of modules. So, let us see first examples, some examples, so A is one, A is our ring then A is an A module. What is the scalar multiplication, first of all the addition, is the addition in the ring and scalar multiplication is a multiplication in the ring. So, with this it is obvious that, A is a module over A, when I say the A module A that means the structure is the underlying addition of the ring that is this additive abelian group and scalar multiplication is the multiplication in the ring with this.

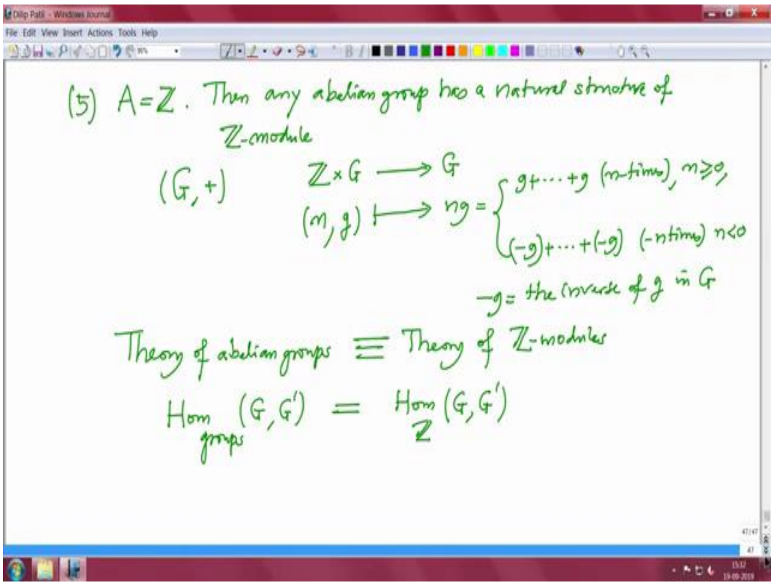
So, two, an ideal, any ideal I or let me be like earlier gothic a in A is an A module. So, this is why the second condition for the ideal that the gothic A is close under scalar multiplication of A that was that makes this as the module. Also the quotient ring A mod a is also an A module. I would just simply say with the natural structures. What do I mean by this for this by example the addition we go out from the ring to this quotient ring, that is addition in this module and scalar multiplication is just a times any x bar is equal to any a x bar. That is a scalar multiplication.

So, third one is very important remember from a ring A we have constructed the polynomial ring. Say, let us say in one variable, this is the polynomial ring over A. That means the polynomials have coefficients in A and this is a ring by usual addition of polynomials and multiplication of polynomials and this one, then A X has the natural structure of A modules where the multiplication, where the addition in the polynomial is usual polynomial addition and scalar multiplication of A on A is precisely you multiply scalar by polynomials as usual you multiply two polynomials, so this is one.

So, also fourth one, one can also consider A as an A X module. So, for this what do I have to do, I have to give you what is the scalar multiplication of the polynomial on to this given ring. So, well the additive Abelian group is Abelian group of A, the ring A. So, this is the given Abelian group and if I have a polynomial f with coefficients in A and if I have any scalar a, how do I multiply f with a?

This is by definition you can take f of 0 times a and now it is easy to check that this is a A module, a becomes an A X module. This is little bit artificial and this is not a unique way. So, you can have several A module structures, several A X module structures on the ring A. So, this is not unique and this is also not very natural.

(Refer Slide Time: 13:29)

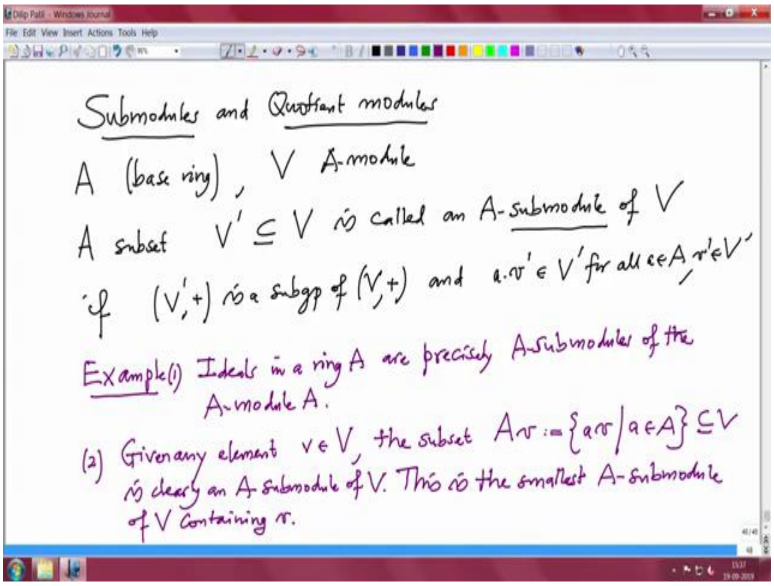


So the next one, five, now if you take the ring A to be Z then any Abelian group has a natural structure of Z module. So, if you have any abelian group G, G plus. How do you define a scalar multiplication of Z on G that is usually how you multiply, so if this is n times g. This is n, g. Now, what is n, g by definition? This is g plus g plus g n times if n is bigger equal to 0 and otherwise it is minus g plus, plus, plus, plus, plus minus g minus n times if n is negative.

Where minus g is the inverse of g in the group g. So, this is minus g equal to the inverse of g in G, because it is Abelian. So, with this, this is also natural. So, the theory of abelian groups is identical with the theory of Z modules and also the homomorphisms, hom groups G, G prime this is same as hom Z G, G prime.

So, any Abelian group homomorphism is a Z module homomorphism and in the Z module homomorphism is an Abelian homomorphism. So, if you have, you would have studied modules over arbitrary commutative ring then the study of abelian groups is included in that. So, that is one.

(Refer Slide Time: 16:15)



Now next one, now, recall very quickly sub modules like for rings we have ideals. So, for modules we have sub modules and quotient modules. Let us recall this quickly, so we have a fix ring A, base ring and V is A module. Then when do you a subset to be a sub module? So, a subset V prime of V is called an A submodule of V. Sometimes you drop this in the notation A because once you have fix ring then you do not have to write that but it is may be better.

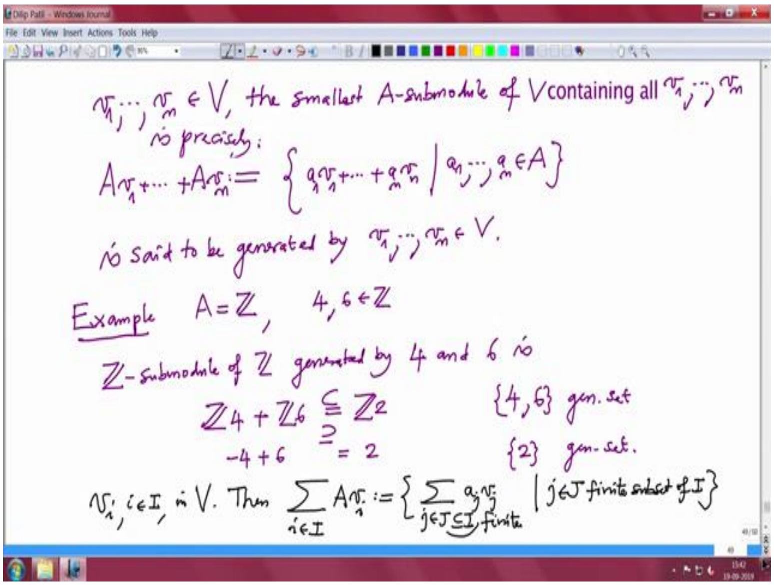
If, the same addition, so V prime with plus is a sub group of V plus and the scalar multiplication restricts to V prime and a times any V prime is belongs to V prime for all a in V, a in A and V prime in V prime. That means if I restrict the structure of V to V prime that itself becomes an A module then it is a it is called a sub module.

Now, for example, ideals in a ring A are precisely A submodules of the module A, of the A module A that is precisely. Because ideals are the subgroups and also restriction of a multiplication goes inside it induces a scalar multiplication on the ideal A. So, how do you find submodules of a module? So, this is one.

Two, given any element, v in V, how do I generate a submodule out of this V? So, I want to make submodule so you take obvious notation the subset A v, these are all A multiples of that given v. So, this is by definition as usual a times v where a is varying in A. This is a subset of V, is clearly an A submodule of V.

So, if you have two elements here you can add, you can subtract and again you will the element of the same type and also multiply by any scalar a and you will get again, element of the same type. So, it is a submodule and this is the smallest A submodule of V containing small v. So, that gives again for us to imitate what we have defined in case of a ring and ideals.

(Refer Slide Time: 21:06)



So, be very quickly, suppose I have a finitely many elements v1 to vn in a module V. Then the smallest A submodule of V is precisely this set A v 1 dot dot dot plus A vn, this is by definition. All A linear combinations of v1 to vn. So, a1v1 plus, plus, plus, plus anvn. Where a1 to an are elements in the ring A. Again it is very easy to check it is smallest it is very easy to check it is a submodule and this submodule is said to be generated by v1 to vn.

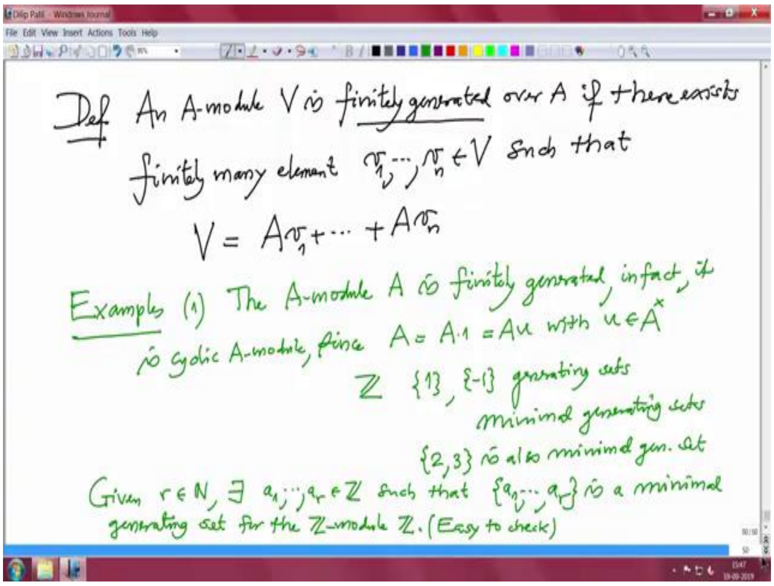
It may have different set generators also. For example, let me write one example. Example, let us take A to be the ring Z and elements 4 and 6, 4 and 6 are elements here. So, what is the submodule of Z, Z submodule of Z generated by 4 and 6 is Z 4 plus Z 6 but this is also same as Z 2. See this one is obvious 4 is a multiple of 2, 6 is also multiple of 2 therefore, all elements here are multiples of 2.

So, Z 2 is one submodule that contains both this and therefore, it contains a submodule generated by that. Conversely, 2 you can write as the combination 4 and 6. 2 equal to minus 4 plus 6. So, therefore, this containment is also clear, so therefore, it is. So, 4 and 6 is a generating set for this submodule and 2 is also generating set. So, generating set is not unique usually this is a generating set. This is also generating set, when does one call a set to be minimal generating set?

If you already know linear algebra in a good set up then you can guess most often and you can write your definitions correctly, examples correctly. So, when do you call a set of generators of a submodule to be minimal, that means you cannot drop any one of them. So, I will make that as the next definitions. So, before that let us write. So, again there is nothing special about finitely many elements.

So, if I have a family vi, i in I in V, then what should be this. This summation i in I A vi this is by definition all the finite sums among vis A linear combinations among vis. So, this is summation, summation over j, j in J and J is a finite set subset of I. This is finite and then we are taking some elements in aj, vj where j is in j and the j is finite subset of I. Obviously this is a submodule by the same checking and this is a smallest submodule which contain all the elements in vi. So, that is it.

(Refer Slide Time: 26:27)



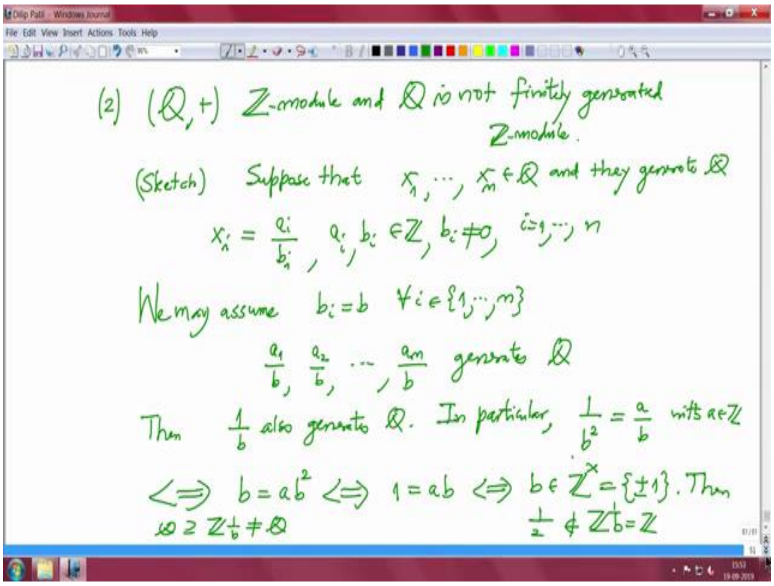
Now, when do you say a module is finitely generated? So, definition an A module V is finitely generated over A, if there exist finitely many elements v1 to vn in V. Such that V equal to A v1 plus, plus, plus, plus A vn. So, that means V is the smallest sub module of V which contain all this v1 to vn.

So, again examples the A module A is finitely generated, in fact, it is cyclic, cyclic A module. What does that mean? That means it is generated by 1 element, since A is generated by 1 or it is also generated by any unit. So, in particular Z is, 1 is also generator of Z and minus 1 is also generator of Z. These are the only two generators of the Z module Z.

These are generating sets. It has also of course there are many generating sets, but these are the smallest generating sets, these are minimal generating sets. But of course 2, 3 is also minimal generating set. Because you cannot drop 2, you cannot drop 3 also. So, it is a minimal generating set. So, among the minimal generating sets the cardinalities are not same you see this is, that was not happening in case of a vector space.

In a vector space, all minimal generating sets have the same cardinality. So, that was, this is not true for modules. In fact you can write down, given any integer r, natural number r, there exists a1 to ar in Z such that the set a1 to ar is a minimal generating set for the Z module Z. This is very easy to check, well it is not all that trivial, but it requires some work. So, things can become complicated now.

(Refer Slide Time: 31:01)



Some example of a module which is not finitely generated. So, to look at Q, Q plus rational numbers with addition. So, this is a Z module and Q is not finitely generated. Z module. Let me sketch the proof, so sketch. So, suppose there is a finite generating set. What does that mean? The generating set consists of sub rational numbers. Suppose that, x1, xn are rational numbers and they generate Q. So, these are rational numbers. So, they have numerator and a denominator.

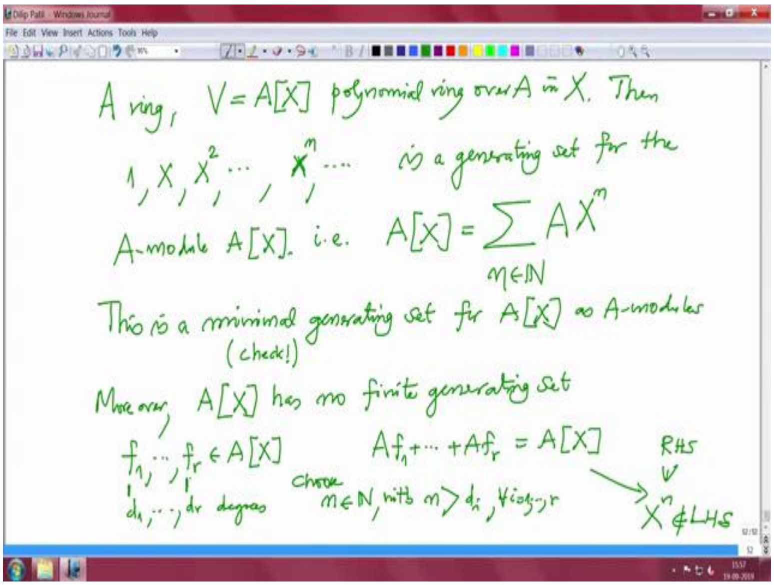
So, I can write xi equal to ai by bi, where ai, bi are integers bi nonzero, i equal to 1 to n. So, note if they generate if xi generate then these new guys a1 by b, make the same denominator I make the common denominator. So, simply I will write we may assume all bis are equal to b. Simply multiply up and down by some by take all b1 to bn and multiply up and down and then we are not changing xi. So, it will same generate the denominator is common norm.

And now, so that means what? That is we are assuming a1 by b, a2 by b, an by b this generates Q. But if they generate Q, then 1 by b also generates that is obvious, because if 1 by b there this a1 is an integer. So, a1 by b is also there, we are allowed to take Z linear combinations, so this is also generates. But then if this generate, what does that mean? That means any rational number is a multiple of Z multiple of this b.

So, in particular 1 by b square will be some a by b with a in Z, but what will this mean? This is equivalent to saying multiply cross. So, that is and cancel b, so b equal to a times b square. So, b equal to a times b square but that is if and only if b is nonzero. So, that is equal to (())(35:26) cancel one of the b, 1 equal to ab that is equivalent to saying, b is a unit in Z. But the units in Z are precisely plus minus 1. So, b is plus minus 1. So, no matter what you do you only get integers with b is in plus minus 1.

So, if you multiply any element of 1 or minus 1 by integer you will b get only integer you will never get 1 by p for example half. So, then half is not an element in the submodule generated by b, because this submodule is Z only, 1 by b this submodule is Z only and therefore, half is not there and therefore what we have approved is Z times 1 by b, these are submodule generated by 1 by b of Q. This can never be Q, if b is plus minus 1. So, that proves that Q is not finitely generated Z module.

(Refer Slide Time: 36:51)



One more very important example we will use all the time. So, now take arbitrary A, commutative always and the module V to be the polynomial ring over A in one variable, this is the polynomial ring over A in X.

We have seen that this has a natural A module structure and I want to say that first of all let us write one generating set. Then 1 X, X square and all the monomials in X X power n etc. This is a generating set for the A module A X. Because any polynomial is a linear combination of this, this is a countable set. So, therefore, in the notation, so that is A X equal to summation over n A X power n. This is the smallest submodule generated by that.

But this is a minimal generating set, this is a minimal generating set for AX as A modules. That is also clear because if you drop any one of them you can never get X power m in terms of the remaining 1, so that I will not check this, I will just say check precisely check this. So, in particular, so not in particular moreover A X has no finite generating set. Because if it has a finite generating set, let us call them f1 to fr, if these polynomials generate A X that means what? That means if I write A f1 plus, plus, plus, plus a fr this is A X and I should get a contradiction, A linear combination of this,

So, you see these guys have some degrees d1 to dr, the degrees of f1, this is degree of fr. Now, choose any n in N, choose n in N with n bigger than everybody for all i. Then X power N is an element here, but you cannot write A linear combination of f1 to fr because maximum you will get d1 to dr degrees here and these degree is n.

So, that is not possible so this is not this does not belong to LHS, this belong to RHS that is it is a polynomial of degree n but it cannot belong here. So, with this we will continue now the next half I will introduce algebras and then after that we will be ready for more geometric setup and whenever I need it again I will come back to the study of modules later. So, thank you and we will meet after the break.