MODULES: FINITELY GENERATED MODULES

R. VIRK

1. Finitely generated modules

1.1. Let M be an A-module and $x \in M$. The set of all multiples ax, $a \in A$, is a submodule of M, denoted by Ax. If $M = \sum_{i \in I} Ax_i$, then the x_i are said to be a *set of generators* of M. This means that every element of M can be expressed (not necessarily uniquely) as a finite linear combination of x_i with coefficients in A. The module M is said to be *finitely generated* if it has a finite set of generators.

1.2. *Example.* A is a finitely generated A-module.

1.3. **Proposition.** *M is a finitely generated A-module if and only if it is isomorphic to a quotient of $A^{\oplus n}$ for some integer $n > 0$.*

Proof. Suppose M is finitely generated. Let $x_1, \dots, x_n \in M$ generate M. Define a morphism $f\colon A^{\oplus n} \to M, (a_1, \dots, a_n) \mapsto a_1x_1 + \cdots + a_nx_n$. Then f is an A-module homomorphism and $\mathrm{im}(f) = M$. Hence, $M \simeq A^{\oplus n}/\ker(f)$. Conversely, suppose $M \simeq A^{\oplus n}/K$ for some submodule $K \subseteq A^{\oplus n}$. Then the image of any set of generators of $A^{\oplus n}$ in M generates M. $\square$

1.4. A set of generators of M is *minimal* if no proper subset of it generates M. Two minimal sets of generators need not have the same number of elements:

1.5. *Example.* Let $A = \mathbf{C}[x]$, then $\{1\}$ and $\{x, 1+x\}$ are minimal sets of generators for the A-module A.

1.6. A set of elements $\{x_1, \dots, x_n\}$ of M is *independent* if no non-trivial linear combination of them is zero. That is, if the following condition holds: if $a_1x_1 + \cdots + a_nx_n = 0$, with $a_i \in A$, then $a_i = 0$ for all i. The set is a *basis* if it is both independent and a generating set. A basis is necessarily a minimal set of generators.

2. Nakayama's lemma

The following inoccuous looking result is often extremely useful.

2.1. **Lemma** (Nakayama's lemma)**.** *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A such that $\mathfrak{a}M = M$. Then there exists an $a \in \mathfrak{a}$ such that $(1-a)M = 0$.*

Proof. Let $e_1, \dots, e_n$ be a set of generators for M. As $\mathfrak{a}M = M$, we obtain a system of equations

$$\begin{aligned} e_1 &= a_{11}e_1 + \cdots + a_{1n}e_n, \\ &\vdots \qquad\qquad \vdots \\ e_n &= a_{n1}e_1 + \cdots + a_{nn}e_n, \end{aligned}$$

for some $a_{ij} \in \mathfrak{a}$. Let T be the matrix (a_{ij}). Then the system of equations above is equivalent to

$$(T - \mathbf{1}_n) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0,$$

where $\mathbf{1}_n$ is the $n \times n$ matrix with 1s on the diagonal and 0s elsewhere. Multiplying by the adjoint (sometimes also called the adjugate) matrix of $(T - \mathbf{1}_n)$ we obtain

$$\det(T - \mathbf{1}_n)\mathbf{1}_n \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0,$$

where $\det(T - \mathbf{1}_n)$ denotes the determinant of $T - \mathbf{1}_n$. Thus, $\det(T - \mathbf{1}_n)M = 0$. Expanding $\det(T - \mathbf{1}_n)$, we see that it gives an element of the required form. □

2.2. The following application of Nakayama's lemma shows that at least in one sense finitely generated modules behave like finite dimensional vector spaces:

2.3. **Proposition.** *Let M be a finitely generated A-module, $f\colon M \to M$ a morphism. If f is surjective then it is an isomorphism.*

Proof. We consider M as an $A[t]$-module via $tx = f(x)$, $x \in M$. It is clear that M is a finitely generated $A[t]$-module. As f is surjective, $tM = M$. So by Nakayama's lemma there exists some polynomial $p(t) \in A[t]$ such that $(1 - tp(t))M = 0$. Hence, if $x \in \ker(f)$, then $0 = (1 - tp(t))x = x$. □

3. Presentations

3.1. Just as for vector spaces we can represent an element of $A^{\oplus n}$ by an $n \times 1$ 'column vector' with entries in A. Namely, the 'column vector' $(a_{i1})_{1 \le i \le n}$ is just new notation for the element $(a_{11}, \dots, a_{n1})$. In exactly the same way as for vector spaces, any A-module homomorphism $A^{\oplus m} \to A^{\oplus n}$ can be represented by an $n \times m$ matrix with entries in A. Composition of such morphisms corresponds to multiplication of matrices. Conversely, *any* $n \times m$ matrix with entries in A gives an A-module homomorphism $A^{\oplus m} \to A^{\oplus n}$. More formally, let $\mathrm{Mat}_{n\times m}(A)$ be the set of $n \times m$ matrices with entries in A. This is an A-module in the obvious way and we have just given an A-module isomorphism $\mathrm{Hom}_A(A^{\oplus m}, A^{\oplus n}) \xrightarrow{\sim} \mathrm{Mat}_{n\times m}(A)$. This point of view will allow us to reduce several questions about modules to manipulations with matrices.

3.2. Let M be an A-module. An exact sequence of the form $M'' \to M' \to M \to 0$ with M'' and M' free is called a *presentation* of M. We will be mainly interested in presentations in which M'' and M' are of finite rank: a *finite presentation* of M is an exact sequence

$$A^{\oplus m} \to A^{\oplus n} \to M \to 0$$

with m, n positive integers.

3.3. I will now try to give a more down to earth description of a presentation for a module. Let M be an A-module. An expression of the form

$$a_1x_1 + \cdots + a_nx_n = 0, \quad a_i \in A, x_i \in M$$

is called a *relation* amongst the elements $x_1, \dots, x_n$. I claim that to give the module M is the same as giving the data of a set of generators for M and all relations amongst these generators. Before making this precise let me illustrate with some examples.

3.4. *Example.* The A-module A is the same as giving a generator e and no relations.

3.5. *Example.* Let $A = \mathbf{C}[x]$ and let $\mathfrak{a}$ be the ideal generated by x. Then the module $\mathfrak{a}$ is equivalent to the data of a generator e (corresponding to the element x) and no relations. Note that $\mathfrak{a}$ and A are isomorphic as A-modules. Now consider the module $A/\mathfrak{a}$. This module is equivalent to the data of a generator e and relations $f(x)e = 0$ for every polynomial $f(x) \in \mathbf{C}[x]$ with zero constant term. A 'finite' way of giving the relations is to just say that $xe = 0$, the module structure then forces all the other relations.

3.6. Now let's make all of this precise, or rather let me explain how the definition of presentations in terms of exact sequences makes this precise. Assume M is finitely generated. Then this is the same as saying that there is an exact sequence $A^{\oplus n} \to M \to 0$. The image of your favorite set of generators in $A^{\oplus n}$ gives a set of generators in M. The relations amongst these generators are precisely the kernel of the morphism $A^{\oplus n} \to M$. If we get lucky then this kernel is also finitely generated. That is, we get an exact sequence

$$A^{\oplus m} \to A^{\oplus n} \to M \to 0.$$

Thus, giving a presentation is the same as writing down a set of generators and the relations amongst these generators. Note that the module M can be recovered from the morphism $A^{\oplus m} \to A^{\oplus n}$, indeed M is the cokernel of this morphism. This is just a fancy way of saying that giving generators and relations completely describes the module. You should also note that the map $A^{\oplus m} \to A^{\oplus n}$ can be described by an $n \times m$ matrix. This matrix is often called the *presentation matrix*. Thus, all the information contained in the module M is completely described by its presentation matrix.

3.7. *Example.* Let $A = \mathbf{C}[x]$ and let $\mathfrak{a}$ be the ideal generated by x. Then left multiplication by x gives an A-module homomorphism $A \xrightarrow{x\cdot} \mathfrak{a}$ that is surjective. The kernel of this map is trivial. Hence, $0 \to A \xrightarrow{x\cdot} \mathfrak{a}$ is a presentation of $\mathfrak{a}$.

3.8. *Example.* Let $A = \mathbf{Z}$ and let M be the A-module with generators x, y and relations $2x - y = 0$. The morphism $A^{\oplus 2} \to M, (a, b) \mapsto ax + by$ is clearly surjective. Its kernel is generated by $2(1, 0) - (0, 1)$. Hence,

$$\mathbf{Z} \xrightarrow{\binom{2}{-1}} \mathbf{Z}^{\oplus 2} \xrightarrow{(a,b) \mapsto ax+by} M \to 0$$

is a presentation of M. Can you spot a simpler presentation of M?

3.9. A presentation is by no means unique. In fact, one could reasonably argue that the whole point behind the notion of modules is to give a systematic way of talking about when two presentations describe the same object/module.

3.10. *Example.* Let M be the zero module, in other words M is generated by e and relations $e = 0$. Let N be the $\mathbf{Z}$-module with generators x, y, z and relations

$$\begin{aligned} 2x + 3y + 5z &= 0, \\ 5x + 7y + 12z &= 0, \\ 11x - 8y + 3z &= 0, \\ 31x - 12y - 99z &= 0. \end{aligned}$$

Then $N \simeq M$ (solve the equations!).

3.11. I hope that I have convinced you by now that if we want to analyze modules, then a reasonable place to start is with finitely presented modules. Analyzing such modules is equivalent to dealing with finitely many equations in finitely many variables. Equivalently, we want to understand matrices. These are things that we have been doing since middle school. Before beginning our analysis it would certainly be nice to have an easy way of detecting modules that have finite presentations! Recall that a ring A is called *Noetherian* if every proper ideal of A is finitely generated. This is equivalent (via a standard Zorn's lemma argument) to requiring that every ascending chain of ideals in A stabilize at some point.

3.12. **Proposition.** *Let A be a Noetherian ring. Then every submodule of a finitely generated A-module is finitely generated.*

Proof. Exercise! Hint: a standard way of doing this is via induction on the number of generators. □

3.13. **Corollary.** *Let A be a Noetherian ring. Then every finitely generated A-module is finitely presented.*

Proof. Let M be a finitely generated A-module. Then we have an exact sequence $A^{\oplus n} \to M \to 0$ with n a positive integer. By Prop. 3.12 the kernel of this morphism is also finitely generated. This gives an exact sequence $A^{\oplus m} \to A^{\oplus n} \to M \to 0$. □

4. Smith normal form

4.1. Let us now begin our analysis of $m \times n$ matrices with entries in a ring A. Since we are after finitely presented modules, it makes sense (at least for now) to restrict to Noetherian rings (see Cor. 3.13). Alas, at the moment this is still too general a setting for us to be able to say anything meaningful. However, we can make a nice statement if our ring is a *principal ideal domain* or *PID* for short. Recall that this is an integral domain in which each ideal can be generated by a single element. A PID is Noetherian.

4.2. **Proposition** (Smith normal form)**.** *Let T be a $m \times n$ matrix with entries in a principal ideal domain A. Then there exist invertible matrices P and Q (with entries in A) such that PTQ^{-1} is diagonal:*

$$\begin{pmatrix} d_1 & 0 & \cdots & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & \cdots & 0 & d_m \end{pmatrix}$$

where each diagonal entry d_i divides the next d_{i+1} (i.e., the ideal generated by d_{i+1} is contained in the ideal generated by d_i). (A matrix of this form is said to be in Smith normal form*).*

4.3. *Remark.* Before giving the proof I want to make a few comments. Artin's book contains the proof for the special case $A = \mathbf{Z}$. Some very minor modifications to his proof gives a proof for Euclidean domains (= integral domains with a division algorithm). I am going to assume that you are familiar with his proof (= if I were to wake you up at 3AM and ask you to put a 3×4 integer matrix into Smith normal form you should be able to do it). The proof for general PIDs wont make much sense otherwise. The basic idea is the same, we use row and column operations (which correspond to multiplication by invertible matrices). However, in general these aren't enough (see Step 1 below).

Proof. Let a_{ij} denote the entry in the i'th row and j'th column of T. Certainly we may assume that $T \neq 0$. Proceeding by induction, we only need to show that we can replace all the entries, except a_{11}, in the first row and first column by 0, and further have a_{11} divide all the other entries in T.

Step 0: If $a_{11} = 0$, swap it with a non-zero entry.

Step 1: Choose a non-zero entry a_{i1} in the first column. If a_{11} divides a_{i1}, then certainly we can replace a_{i1} by 0 without changing any of the other entries in the first column. Suppose a_{11} does not divide a_{i1}. By swapping rows, if necessary, we may assume that $i = 2$. Let r be a generator for the ideal generated by a_{11} and a_{21}. Then $r = xa_{11} + ya_{21}$ for some $x, y \in A$. Further, $a_{11} = x'r$ and $a_{21} = y'r$ for some $x', y' \in A$. So $(xx' + yy' - 1)r = 0$. As A is an integral domain, we infer that $xx' + yy' = 1$. Consequently, the $m \times m$ matrix

$$\begin{pmatrix} x & y & 0 & \cdots & \cdots & 0 \\ -y' & x' & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \vdots & \\ 0 & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$$

is invertible. Multiplying on the left with this matrix replaces a_{11} with r and replaces a_{21} with an element divisible by r and leaves all other entries in the first column unaffected. We may now replace a_{21} by 0 without changing any of the other entries in the first column.

Step 2: Run the obvious analogue of Step 1 for entries in the first row. Of course, at some iteration this may produce a non-zero entry in the first column. Whenever this happens go back to running Step 1 for column entries. Note that the entry a_{11} is producing an ascending chain of ideals. As our ring is a PID and hence Noetherian, this chain must stabilize at some point. By construction, this chain can only stabilize when all the entries, except a_{11}, in the first row and first column are zero.

Step 3: At this point all the entries in the first row/column except a_{11} are 0. However, a_{11} may not divide all the other entries of T. Let a_{ij} be such an entry. Add the j'th column to the first column and go back to Step 1. Once more, note that the iteration of Steps 1-3 produces an ascending chain of ideals via the entry a_{11}. This chain must stabilize and by construction this can only happen when a_{11} divides all the other entries in T. $\square$

4.4. *Example.* Let $A = \mathbf{Z}$ and let $T = \left(\begin{smallmatrix} 2 & 1 \\ 4 & 5 \end{smallmatrix}\right)$. Step 1 subtracts 2 times the first row from the second to give $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 3 \end{smallmatrix}\right)$. Step 2 now multiplies this matrix on the right by $\left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$ to give $\left(\begin{smallmatrix} -1 & 0 \\ -3 & 6 \end{smallmatrix}\right)$. This sends us back to Step 1 which adds 3 times the first row to the second to give $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 9 \end{smallmatrix}\right)$, and we are done! In terms of multiplying with matrices this is the sequence

$$\left(\begin{smallmatrix} 2 & 1 \\ 4 & 5 \end{smallmatrix}\right) \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right)\cdot} \left(\begin{smallmatrix} 2 & 1 \\ 0 & 3 \end{smallmatrix}\right) \xrightarrow{\cdot\left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)} \left(\begin{smallmatrix} 1 & 0 \\ -3 & 6 \end{smallmatrix}\right) \xrightarrow{\left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)\cdot} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 9 \end{smallmatrix}\right)$$

Department of Mathematics, University of California, Davis, CA 95616
E-mail address: virk@math.ucdavis.edu