Lecture Notes for Math 627B
Modern Algebra
Modules and Groebner Bases

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
wwww-rohan.sdsu.edu/ ˜ mosulliv

March 23, 2009

1 Definition and key properties of modules

Definition 1.1. A module M over a ring R is an abelian group with R-multiplication satisfing the following properties.

- $1m = m$
- $r(r'm) = (rr')m$
- $(r + r')m = rm + r'm$
- $r(m + m') = rm + rm'$

When R is a field, a module is just a vector space over R.

Example 1.2. The direct product $R \times R \times \cdots \times R$ is an abelian group. We make it into an R-module by introducing the R-multiplication $r(r_1, \ldots, r_n) = (rr_1, rr_2, \ldots, rr_n)$. Check that this satisfies the properties of modules.

If there are t copies of R, we will write R^t for this module.

Example 1.3. Ideals are modules.

Example 1.4. The quotient ring of R by an ideal is a module.

Proposition 1.5. *Let $M_1, M_2, \ldots, M_t$ be modules. Then $M_1 \times M_2 \times \cdots \times M_t$ with component-wise multiplication by R is also a module.*

Naturally, the first things we want to consider are structure preserving functions and subsets of a module which are modules themselves.

Definition 1.6. A function $\phi : M \to N$ is a homomorphism of R-modules when ϕ is a homomorphism of abelian groups and $\phi(rm) = r\phi(m)$. It is an isomorphism when it is also a bijection.

Definition 1.7. A module M is *cyclic* when it is generated by a single element. That is, $M = Ra$ for some $a \in M$.

A module M is *finite free* when it is isomorphic to R^t for some t.

The last definition makes you wonder if t is unique. Fortunately it is.

Theorem 1.8. *Let R be a finitely generated integral domain. If the R-module M is isomorphic to R^t and to R^s, then $s = t$. This number is called the rank of M.*

Proof. (sketch!) The trick is to mod out by a maximal ideal I of R. You get $(R/I)^t \cong (R/I)^s$. But R/I is a field, so $(R/I)^s$ and $(R/I)^t$ are vector spaces. We now use the fact that the dimension of a vector space is well defined. □

Example 1.9. Not all modules are free. For example the ideal $\langle x, y\rangle$ in $k[x, y]$ is not free. There is no common divisor of x and y, so $\langle x, y\rangle$ is not cyclic. Also $y(x) - x(y) = 0$.

$\mathbb{Z}/n$ is a $\mathbb{Z}$-module. It is clearly not free because $\mathbb{Z}$ is infinite and $\mathbb{Z}/n$ is finite.

Example 1.10. For I an ideal of R the inclusion map $I \longrightarrow R$ is a module homomorphism.

The quotient map $R \longrightarrow R/I$ is also a module homomorphism.

Example 1.11. A principal ideal is a cyclic module. The homomorphism $\phi_a : R \longrightarrow R$ taking 1 to a has image the ideal $\langle a\rangle$. If R is an integral domain then the map is injective, so R is isomorphic to $\mathrm{im}(\phi_a) = \langle a\rangle$.

Show that in $\mathbb{Z}/4$, the ideal $\langle 2\rangle$ is cyclic, but *not* isomorphic to $\mathbb{Z}/4$.

Definition 1.12. A submodule of M is a subgroup K of M that is closed under multiplication by elements of R, that is $rk \in K$ for all $k \in K$.

Example 1.13. An ideal I in R is a submodule of R.

Example 1.14. If I_1, I_2, …, I_t are ideals in R, then $I_1 \times I_2 \times \cdots \times I_t$ is a submodule of R^t.

Proposition 1.15. *Let $\phi : M \longrightarrow N$ be a homomorphism of modules. Then $\ker(\phi)$ is a submodule of M and $\operatorname{im}(\phi)$ is a submodule of N.*

Proposition 1.16. *If N is a submodule of M then the quotient group M/N also has the structure of an R-module.*

This leads to the isomorphism theorems:

Theorem 1.17 (First isomorphism, factor)**.** *Let $\phi : M \longrightarrow N$ be a homomorphism of R-modules, and let $K = \ker(\phi)$. There is a unique homomorphism, $\tilde{\phi} : M/K \longrightarrow N$ such that $\tilde{\phi} \circ \pi = \phi$ where π is the natural homomorphism $M \to M/K$.*

Furthermore, if ϕ is surjective then $\tilde{\phi}$ is an isomorphism.

Theorem 1.18 (Correspondence, third isomorphism)**.** *Let K be a submodule of M. There is a one-to-one correspondence between submodules of M/K and submodules of M containing K.*

If N is a submodule of N containing K then $M/N \cong M/K \Big/ N/K$ as R-modules.

2 Generators and relations for a module

We will write elements of R^s as row vectors of length s. Any homomorphism is assumed to be an R-module homomorphism.

Let M be an $s \times t$ matrix of elements of R. Then M defines an R-module homomorphism from R^s to R^t using the usual rules for matrix multiplication. Conversely, suppose ϕ is an R-module homomorphism from R^s to R^t. Let $e_1, \ldots, e_s$ be the standard basis for R^s and $f_1, \ldots, f_t$ be the standard basis for R^t. Write $\phi(e_i) = m_{i1}f_1 + m_{i2}f_2 + \cdots + m_{it}f_t$. Form the matrix $M = [m_{ij}]$. By the properties of R-module homomorphisms, ϕ is agrees with matrix multiplication by M, $\phi(x) = xM$ for any $x \in R^s$.

Definition 2.1. A *presentation* of a module M is a surjective homomorphism from a free module onto M, $\phi : R^t \longrightarrow M$.

A *generators and relations representation of M* is a sequence of two homomorphisms $R^s \xrightarrow{\psi} R^t \xrightarrow{\phi} M$ such that ϕ is surjective and $\ker(\phi) = \operatorname{im}(\psi)$. The image of ϕ generates M and the kernel of ϕ is the set of relations on those generators.

A sequence of homomorphisms $M_0 \xrightarrow{\phi_1} M_1 \xrightarrow{\phi_2} \ldots \xrightarrow{\phi_k} M_k$ is exact when $\ker(\phi_{i+1}) = \operatorname{im}(\phi_i)$ for $i = 1, \ldots, k-1$.

A generators and relations representation of M is an exact sequence of two homomorphisms.

Example 2.2. Consider the ideal $\langle x, y\rangle$ in $R = k[x, y]$. Then

$$R^2 \longrightarrow \langle x, y\rangle$$
$$\begin{bmatrix} x \\ y \end{bmatrix}$$

gives a presentation of $\langle x, y\rangle$. A generators and relations representation is

$$\begin{array}{ccccc} R^2 & \longrightarrow & R^2 & \longrightarrow & \langle x, y\rangle \\ & \begin{bmatrix} y & -x \end{bmatrix} & & \begin{bmatrix} x \\ y \end{bmatrix} & \end{array}$$

Polynomial Rings

Now $R = k[x_1, \ldots, x_n]$

Definition 2.3. Let $F = \{f_1, \ldots, f^s\}$ be elements of R. Consider the homomorphism

$$R^t \longrightarrow \langle F\rangle$$
$$e_i \longmapsto f_i$$

The kernel of this homomorphism is called the *syzygy module* of F.

For a monomial ideal $G = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$, where $\alpha_i \in \mathbb{N}_0^n$, let $\gamma_{ij} = \operatorname{lcm}\{\alpha_i, \alpha_j\}$. For the presentation $R^s \longrightarrow \langle G\rangle$ taking basis vector e_i to g_i we have elements of the syzygy module $\bar{S}_{ij} = x^{\gamma_{ij}-\alpha_i}e_i - x^{\gamma_{ij}-\alpha_j}e_j$. We will show that these generate the syzygy module.

First, note that any $h \in R$ may be written as $\sum_{\beta\in\mathbb{N}_0^n} h_\beta x^\beta$. Now for any $\alpha \in \mathbb{N}_0$ we may shift the indices by α and write h as $\sum_{\beta\in\mathbb{N}_0^n} h'_\beta x^{\beta-\alpha}$. We simply set $h'_\beta = 0$ if $\beta \not\succeq \alpha$ and $h'_\beta = h_{\alpha-\beta}$ if $\beta \succeq \alpha$. For example if $h = 1 + 2x + 3y + 5x^2 + 4y^2$ and $\alpha = (1, 0)$ then $h'_{(0,a)} = 0$ for any a and $h'_{(1,0)} = 1$, $h'_{(2,0)} = 2$, $h'_{(1,1)} = 3$, $h'_{(3,0)} = 5$, $h'_{(1,2)} = 4$.

Let us now work with a monomial ordering $<$ on R. We will call an element $\bar{m} = (m_1, \ldots, m_s)$ of R^s *homogogeneous* of degree δ (with respect to the presentation for $\langle G\rangle$) when the entries of m are all monomials and $\operatorname{LE}(m_i) + \alpha_i = \delta$ for all nonzero m_i.

Proposition 2.4. *For G a set of monomials, any element of $S(G)$ may be written as a sum of homogeneous elements.*

Proof. Let $\bar{h} = (h_1, \ldots, h_s) \in S(G)$. Expand each h_i using α_i as discussed above: $h_i = \sum_{\beta\in\mathbb{N}_0} h_{i,\beta} x^{\beta-\alpha_i}$. Then $\bar{h} = \sum_{\beta\in\mathbb{N}_0^n}(h_1 x^{\beta-\alpha_1}, \ldots, h_s x^{\beta-\alpha_s})$ expresses $\bar{h}$ as a sum of homogeneous terms. We can see from the following computation that each of the homogeneous terms is in $S(G)$.

$$\begin{aligned}
0 &= \sum_{i=1}^{s} h_i x^{\alpha_i} \\
&= \sum_{i=1}^{s} x^{\alpha_i} \sum_{\beta\in\mathbb{N}_0^n} h_{i,\beta} x^{\beta-\alpha_i} \\
&= \sum_{\beta\in\mathbb{N}_0^n} \sum_{i=1}^{s} h_{i,\beta} x^{\beta} \\
&= \sum_{\beta\in\mathbb{N}_0^n} x^{\beta} \sum_{i=1}^{s} h_{i,\beta}
\end{aligned}$$

Since a polynomial is zero only when each term in its expansion is 0, the final sum shows that each $\sum_{i=1}^{s} h_{i,\beta} = 0$. $\square$

Theorem 2.5. *For a monomial generating set G, the $\bar{S}_{ij}$ generate $S(G)$.*

Proof. By the lemma, it is enough to show that any homogeneous element may be written as a sum of the $\bar{S}_{ij}$. Let $\bar{m}$ be homogeneous of degree δ, so $\bar{m} = (c_1 x^{\delta-\alpha_1}, \ldots, c_s x^{\delta-\alpha_s})$ with $c_i \in k$. We must have $\delta \succeq \alpha_i$ for any i for which $c_i \neq 0$. We now argue that if there are two or more nonzero terms, we can subtract a multiple of some $\bar{S}_{ij}$, and get another homogeneous element of $S(G)$ which has fewer nonzero terms. By continuing this process we eventually get at most one nonzero term. But a vector with exactly one nonzero term is clearly not in $S(G)$. Thus we end with the 0 vector, and therefore $\bar{m}$ can be written as a sum of multiples of the $\bar{S}_{ij}$.

Suppose c_i and c_j are nonzero. We know $\delta \succeq \alpha_i, \alpha_j$ so $\delta \succeq \gamma_{ij}$. Now

$$\begin{aligned}
c_i x^{\delta-\gamma_{ij}} \bar{S}_{ij} &= c_i x^{\delta-\gamma_{ij}} \left(x^{\gamma_{ij}-\alpha_i} e_i - x^{\gamma_{ij}-\alpha_j} e_j \right) \\
&= c_i x^{\delta-\alpha_i} e_i - c_i x^{\delta-\alpha_j} e_j
\end{aligned}$$

Subtracting from $\bar{m}$ eliminates the ith term in $\bar{m}$ and results in a homogeneous element of $S(G)$ with one fewer nonzero term. $\square$

Example 2.6. Consider $k[x, y]$ with glex and $x > y$. Let $G = (y^2, x^2y, x^3)$. A presentation of $\langle G \rangle$ is

$$R^2 \quad \overset{\begin{bmatrix} y^2 \\ x^2y \\ x^3 \end{bmatrix}}{\longrightarrow} \quad \langle G \rangle$$

A representation of the syzygy module for $S(G)$ is

$$R^3 \quad \overset{\begin{bmatrix} x^2 & -y & 0 \\ 0 & x & -y \\ -x^3 & 0 & y^2 \end{bmatrix}}{\longrightarrow} \quad R^2 \quad \overset{\begin{bmatrix} y^2 \\ x^2y \\ x^3 \end{bmatrix}}{\longrightarrow} \quad \langle G \rangle$$

The first row of the syzygy matrix is homogeneous of degree $(2, 2)$, the second is homogeneous of degree $(3, 1)$ and the third is homogeneous of degree $(3, 2)$. Notice that we used all the syzygys, although the final one can be expressed as a combination of the first two. The kernel of the left hand homomorphism is not trivial. You can see that it is generated by $(x, y, 1)$. A more efficient representation would use just the first two syzygys.

Groebner Bases

Now consder $G = (g_1, \dots, g_s)$ a Groebner basis for the ideal it generates. We want to relate the generators and relations representation of $\langle G \rangle$ to that for $S(G)$. Let's assume the g_i are monic; let $LE(g_i) = \alpha_i$ and let $\gamma_{ij} = \text{lcm}(\alpha_i, \alpha_j)$. We may write any $\bar{h} \in R^s$ as a sum of homogeneous elements relative to $(\alpha_1, \dots, \alpha_s)$ as we did in the last section. If $\delta = \max_i\{\text{LE}(h_i) + \alpha_i\}$, then the $\text{LT}(\bar{h})$ is the vector consisting of the homogeneous terms of degree δ in $\bar{h}$.

Recall that the S-polynomial of g_i and g_j is

$$S(g_i, g_j) = x^{\gamma_{ij} - \alpha_i} g_i - x^{\gamma_{ij} - \alpha_j} g_j$$

Since G is a Groeber basis, $S(g_i, g_j) \xrightarrow{G} 0$, and this means that $S(g_i, g_j) = \sum_i a_i g_i$ with $\text{LE}(a_i g_i) \le \text{LE}(S(g_i, g_j)) < \gamma_{ij}$. The latter inequality comes from the cancellation of the degree γ_{ij} terms that occurs in the computations of $S(g_i, g_j)$ and the first inequatity is from the definition of $\xrightarrow{G}$. Rewrite this we get

$$(x^{\gamma_{ij} - \alpha_i} - a_i) g_i + (-x^{\gamma_{ij} - \alpha_j} - a_j) g_j - \sum_{k \ne i,j} a_k g_k = 0$$

so

$$\bar{T}_{ij} = (x^{\gamma_{ij}-\alpha_i} - a_i)e_i + (-x^{\gamma_{ij}-\alpha_j} - a_j)e_j - \sum_{k\neq i,j} a_k e_k$$

is an element of $S(G)$. The leading term of this element is $x^{\gamma_{ij}-\alpha_i}e_i + -x^{\gamma_{ij}-\alpha_j}e_j$: It is equal to the element $\bar{S}_{ij}$ in the presentation of $S(\mathrm{LT}(g))$.

More generally, suppose that $\bar{m} = (m_1, \ldots, m_s)$ is homogeneous of degree δ in $S(\mathrm{LT}(G))$. Consider $f = \sum m_i g_i$. This is an element of $\langle G\rangle$, so $f \xrightarrow{G} 0$. Since $\bar{m} \in S(\mathrm{LT}(G))$, the leading term of f is less than δ. Similar to the situation for the S-polynomials, $f = \sum m_i g_i = \sum_i a_i g_i$ with $\mathrm{LE}(a_i g_i) \leq \mathrm{LE}(f) < \delta$. Then $\bar{m} - \bar{a} \in S(G)$ and $\mathrm{LT}(\bar{m} - \bar{a}) = \bar{m}$.

We have essentially proven this theorem.

Theorem 2.7. *Let $G = (g_1, \ldots, g_s)$ be a Groebner basis for the ideal it generates. Let $\bar{S}_1, \ldots, \bar{S}_r$ be a homogeneous basis for $S(\mathrm{LT}(G))$. There exist $\bar{T}_1, \ldots \bar{T}_r \in S(G)$ with $\mathrm{LT}(\bar{T}_j) = \bar{S}_j$ and these T_j generate $S(G)$.*

Example 2.8. Consider $k[x, y]$ with glex and $x > y$. Let $G = (y^2 - x, x^2y - x, x^3 - y^3)$. A representation of $\langle\mathrm{LT}(G)\rangle$ was given in Example 2.6. Let us extend this to a representation of $\langle G\rangle$.

We have

$$\begin{aligned} S(g_1, g_2) &= x^2(y^2 - x) - y(x^2y - x) \\ &= -x^3 + xy \\ &= -y(y^2 - x) - (x^3 - y^3) \\ S(g_2, g_3) &= x(x^2y - x) - y(x^3 - y^3) \\ &= y^4 - x^2 \\ &= (y^2 + x)(y^2 - x) \end{aligned}$$

A similar computation for $S(g_1, g_3)$ may be done. From $S(g_1, g_2)$ we get $T_{12} = (x^2 - y, y, -1) \in S(G)$ and from $S(g_2, g_3)$ we get $T_{23} = (y^2 + x, x, -y) \in S(G)$. Notic that $\mathrm{LT}(T_{12}) = S_{12}$ and $\mathrm{LT}(T_{23}) = S_{23}$ (using the homogeneity defined by $\alpha_1 = (0, 2)$, $\alpha_2 = (2, 1)$, $\alpha_3 = (3, 0)$). We get the following representation of the syzygy module $S(G)$

$$\begin{array}{ccccc} R^3 & \longrightarrow & R^2 & \longrightarrow & \langle G\rangle \\ & \begin{bmatrix} x^2 + y & -y & 1 \\ y^2 + x & -x & y \\ -x^3 + y^3 & 0 & y^2 - x \end{bmatrix} & & \begin{bmatrix} y^2 \\ x^2y \\ x^3 \end{bmatrix} & \end{array}$$

As in the previous example, the last syzygy is redundant, a more efficient representation would use just the first two syzygys.