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

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

October 27, 2011

Throughout this document any ring is a commutative ring with identity. Any time we use k it is a field.

The theory of modules over a ring is a generalization of the linear algebra, the theory of vector spaces over a field. Many of the terms and results for vector spaces extend quite easily to modules, but there are some issues that require careful formulation.

The theory of modules is also a generalization of the theory of abelian groups. In fact, every abelian group is a $\mathbb{Z}$-module (and conversely).

1 Definition and key properties of modules

Definition 1.1. A module M over a ring R is an abelian group with an R-action (aka R-multiplication). For each $r \in R$ and $m \in M$ there is a unique element $rm = mr$ of M. This R-action satisfies the following properties. For $r, r' \in R$ and $m, m' \in M$,

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

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

When there is clearly a single ring under consideration we may simply say that M is a module, with the understanding that it is over this ring.

The most fundamental examples are the following three.

Example 1.2. The Cartesian product $R \times R \times \cdots \times R$ is an abelian group using coordinate wise addition. If there are n copies of R, we will this as R^n. We make it into an R-module by introducing the R-action $r(r_1, \ldots, r_n) = (rr_1, rr_2, \ldots, rr_n)$. Check that this satisfies the properties of modules.

Example 1.3. An ideal I of R is an R-module using the multiplication in R as the R-action. Since an ideal absorbs products we have $ra \in I$. The properties that R-action must satisfy are easy to verify. They follow from the properties of multiplication in R.

Example 1.4. For I an ideal in R, the quotient ring R/I is an R- module. The R-action that we use is based is this: For $r \in R$ and $a + I \in R/I$, define $r(a + I) = ra + I$. Verify this satisfies the required properties.

Notice that the latter two examples are trivial when R is a field, since the only ideals in a field are the 0 and the whole field.

Definition 1.5. A module M is *cyclic* when it is generated by a single element. That is, $M = Ra$ for some $a \in M$.

When R is a field M is cyclic just means that M is one-dimensional.

For arbitrary R an ideal is cyclic as an R-module just means that the ideal is principal.

For arbitrary R and any ideal I in R, the quotient ring R/I is cyclic, generated by $1 + I$. Verify!

Thus, we may think of "cyclic" as a more general notion than principal; it is applicable to all modules, not just ideals.

If we have several modules, their Cartesian product has a natural module structure. The proof is routine and left to you.

Proposition 1.6. *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 over R.*

Definition 1.7. The Cartesian product with the module structure in the proposition is usually called the direct sum of the M_i and it is written $M_1 \oplus M_2 \oplus \cdots \oplus M_t$.

There are some basic properties of modules that should be checked: see Ash 4.1.2.

There are three other examples in Ash that I want to briefly mention, but we will not use them a lot.

Example 1.8. The polynomial ring $R[x]$ over R is an R-module. In fact, is said to be "free" with an infinite basis $1, x, x^2, \ldots$. Every element of $R[x]$ can be written is a unique way as a finite sum of these basis elements.

Example 1.9. Let $M_n(R)$ be the ring of $n \times n$ matrices over R. Then $M(R)$ is a free R-module when we allow R to act by multiplication on each component of the matrix. The module $M(R)$ is really just R^{n^2} with components arranged in a square, and it has a basis E_{ij} for $i, j \in \{1, \ldots, n\}$. Here E_{ij} is the matrix which is 1_R in position i, j and 0_R otherwise.

Example 1.10. If $\phi : R \longrightarrow S$ is a homomorphism of rings, then S is an R-module. The R-action is defined via ϕ, the action of r on s is defined to be $\phi(r)s$. You can check that this satisfies the required properties for S to be an R-module. When an R-module also has the structure of a ring it is called an algebra over R.

The previous two examples, $R[x]$ and $M(R)$ are actually R-algebras.

Extending this example a bit, if N is an S-module then we can treat it as an R module via ϕ. The action of $r \in R$ on $n \in N$ is $\phi(r)n$.

2 Homomorphisms

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

Definition 2.1. A function $\phi : M \to N$ is a homomorphism of R-modules when $\phi(m + m') = \phi(m) + \phi(m')$ and $\phi(rm) = r\phi(m)$ for $m, m' \in M$ and $r \in R$. The first condition says that ϕ is a homomorphism of abelian groups, and the second that ϕ respects R-action. We say ϕ is an isomorphism when it is also a bijection.

Proposition 2.2. *If $\phi : M \longrightarrow N$ is a bijective homomorphism of R-modules (that is, an isomorphism) then the inverse function ϕ^{-1} is also a homomorphism (and therefore an isomorphism).*

Proof. We need to check that $\phi^{-1}(n+n') = \phi^{-1}(n)+\phi^{-1}(n')$ for all $n, n' \in N$ and that $\phi^{-1}(rn) = r\phi^{-1}(n)$. There are unique m, m' such that $\phi(m) = n$ and $\phi(m') = n'$ Since $\phi(\phi^{-1}(n) + \phi^{-1}(n')) = \phi(m + m') = \phi(m) + \phi(m') = n + n'$ we can apply ϕ^{-1} (which is a function!) to get $\phi^{-1}(n) + \phi^{-1}(n') = \phi^{-1}(n + n')$.

Similarly, $\phi(r\phi^{-1}(n)) = r\phi(\phi^{-1}(n)) = rn$. Now apply ϕ^{-1}. □

Example 2.3. 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 2.4. If $M = \oplus_{i=1}^{n} M_i$ is the direct sum of the modules M_i then the projection $M \longrightarrow M_i$ is a module homomorphism. There is also a module homomorphism $M_i \longrightarrow M$, it takes $m_i \in M_i$ to the element of M which is m_i in the ith component and 0 elsewhere. This injection is a clear generalization of the analogous statement for vector spaces.

Notice that for two rings R, S there is generally no ring homomorphism from R to $R \times S$ since we require that a homomorphism take the multiplicative identity to the multiplicative identity.

Definition 2.5. Let M be an R-module. A submodule of M is a subset that is also a module using the R-action on M.

Equivalently, 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 $k \in K$.

The next propositions are easy generalizations of results for abelian groups. Proofs are left as exercises.

Proposition 2.6. *Let $\phi : M \longrightarrow N$ be a homomorphism of modules. Then* $\ker(\phi)$ *is a submodule of M and* $\mathrm{im}(\phi)$ *is a submodule of N.*

Example 2.7. 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.

Not all submodules of R^t are as simple as the previous example!

Proposition 2.8. *If B is a subset of M then the set of all combinations $r_1 b_1 + \ldots r_n b_n$ for $b_i \in B$ and arbitrary $n \in \mathbb{N}_0$ is a submodule of M.*

Proof. The four properties that the R-action have to satisfy are automatic, since M is already an R-module. We have closure under addition: Two arbitrary elements are $(r_1 b_1 + \ldots r_n b_n)$ and $(r'_1 b'_1 + \ldots r'_m b'_m)$ for b_i and b'_i in B. Their sum is also a finite sum of multiples of elements of B. We also have closure under multiplication by elements of R: $r(r_1 b_1 + \ldots r_n b_n) = (rr_1 + \ldots r r_n b_n)$ is also a sum of multiples of elements in B. □

The next example is a special case of the proposition.

Example 2.9. If I is an ideal in R then the module generated by am for $a \in I$ and $m \in M$ is a submodule of M. We call it IM.

Definition 2.10. Let M be an R-module and let K be a submodule of M. For any $m \in M$, the set $m + K = \{m + k : k \in K\}$ is called a coset of K.

Since M is an abelian group, the set of cosets forms an abelian group, which is written M/K. Not surprisingly M/K has an R-module structure.

Theorem 2.11. *Let M be an R-module and let K be a submodule of M. The cosets of K partition M. That is, any two cosets are either disjoint or equal.*

The set of cosets has the structure of R-module using the action $r(a + K) = ra + K$.

The fundamental theorems for group homomorphisms, and ring homomorphisms have analogues for module homomorphisms.

Theorem 2.12 (Factor)**.** *Let $\phi : M \longrightarrow M'$ be a homomorphism of modules and let K be the kernel. If N is a submodule of K then ϕ factors through $\pi : M \longrightarrow M/N$. That is, there is a uniquely defined homomorphism $\tilde{\phi} : M/N \longrightarrow M'$ such that $\phi = \tilde{\phi} \circ \pi$.*

Furthermore, $\tilde{\phi}$ is surjective iff ϕ is, and $\tilde{\phi}$ is injective iff $N = K$.

Theorem 2.13 (1st Isomorphism)**.** *If $\phi : M \longrightarrow M'$ is surjective then $M' \cong M/\ker\phi$.*

Example 2.14. 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 $\mathbb{Z}/4$.

Theorem 2.15 (Correspondence)**.** *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.*

Theorem 2.16 (3rd Isomorphism)**.** *Let K be a submodule of N and N a submodule of K. Then N/K is a submodule of M/K and*

$$\frac{M/K}{N/K} \cong \frac{M}{N}$$

3 Generating sets and free modules

The following definitions are natural extensions from the theory of vector spaces.

Definition 3.1. A subset $B = \{b_1, \ldots b_t\}$ of module M is a spanning set when every element of M can be written as a linear combination of the elements in B. The elements of B are linearly independent when $\sum r_i b_i = 0$ iff each $r_i = 0$. When B spans M and the elements of B are linearly independent, we say B is a basis for M.

A module M is *finitely generated* when it has a finite spanning set. It is *finite free* when it has a finite basis.

We will only consider finitely generated modules.

Example 3.2. The R-module $R^n = R \oplus R \oplus \cdots \oplus R$ is finite free. It has a basis $e_1, \ldots, e_n$ where e_i is 1 in the ith position and 0 elsewhere. This basis is called the standard basis. Of course, as with vector spaces, it is not the only basis.

Example 3.3. Every ideal in $\mathbb{Z}$ is principal, and therefore finitely generated. The rings $\mathbb{Z}/n$ are generated by 1, but they are not free as $\mathbb{Z}$-modules. The spanning set $\{1\}$ is not linearly independent, for the element $n \in \mathbb{Z}$ and $1 \in \mathbb{Z}/I$, $n1 = 0$ is a linear combination that gives 0, although $n \neq 0$.

Example 3.4. The Hilbert basis theorem showed that any ideal in $k[x_1, \ldots, x_n]$ is finitely generated (as an ideal, which also implies it is finitely generated as a module).

Example 3.5. Non-principal ideals in $k[x, y]$ are not free. This needs proof, but as an example I will show that the ideal $\langle x, y\rangle$ does not have x, y as a basis. There is no common divisor of x and y, so $\langle x, y\rangle$ is not cyclic (i.e. not principal). Note that $y(x) - x(y) = 0$. Think of the (x) and (y) as generators of $\langle x, y\rangle$ and the y and x as coefficients from $k[x, y]$. This shows that x and y are not linearly independent.

A vector space has a well-defined dimension; every basis has the same cardinality. The situation is more complicated for general modules, but, fortunately, it is relatively simple for free modules. Let's just prove it in the finite case.

Theorem 3.6. *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. The trick is to mod out by a maximal ideal I of R to get a vector space over the field R/I.

Let IM be the submodule of M generated by am for $a \in I$ and $m \in M$. We have shown that IM is a submodule of M. I leave it to you to show

that M/IM is a module over R/I with action $(r+I)(m+IM) = rm+IM$. Since R/I is a field, M/MI is a vector space over R/I and has a well defined dimension. We will show this dimension is equal to the number of elements in any basis for M.

Suppose $b_1, \ldots, b_t \in M$ is a basis for M. Since the b_i span M, it is clear that the $b_i + IM$ span M/IM. (Thus the dimension of M/IM is at most t.) Now suppose that some linear combination of the $b_i + M$ is $0 + IM$; $\sum_{i=1}^{t}(r_i + I)(b_i + IM) = 0 + IM$. Then

$$\begin{aligned} 0 + IM &= \sum_{i=1}^{t}(r_i + I)(b_i + IM) \\ &= \sum_{i=1}^{t}(r_i b_i + IM) \\ &= (\sum_{i=1}^{t} r_i b_i) + IM \end{aligned}$$

This shows that $\sum_{i=1}^{t} r_i b_i \in IM$. Check that any element of IM may be written as a sum $\sum_{i=1}^{t} a_i b_i$ for $a_i \in I$. Thus $\sum_{i=1}^{t} r_i b_i = \sum_{i=1}^{t} a_i b_i$ and therefore $\sum_{i=1}^{t}(r_i - a_i)b_i = 0$. Since the b_i are independent, $r_i - a_i = 0$ for all i. Going back to our original linear combination, since each $r_i = a_i \in I$ all the coefficients in $\sum_{i=1}^{t}(r_i + I)(b_i + IM) = 0 + IM$ are actually 0 in R/I. This shows that t is at most the dimension of M/IM and completes the proof that the number of elements in a basis for M is equal to the dimension of M/IM for any maximal ideal I. □

4 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

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & \ldots & m_{1,t} \\ m_{2,1} & m_{2,2} & \ldots & m_{2,t} \\ \ldots & \ldots & \ldots & \ldots \\ m_{s,1} & m_{s,2} & \ldots & m_{s,t} \end{bmatrix}$$

By the properties of R-module homomorphisms, ϕ agrees with matrix multiplication by M, $\phi(x) = xM$ for any $x \in R^s$.

Suppose that M is a finitely generated R-module, with spanning set $b_1, b_2, \ldots, b_t$. Consider the homomorphism $R^t \longrightarrow M$ taking the standard basis element e_i to b_i. The map is surjective since an arbitrary element of M, which can be written $\sum_{i=1}^{t} r_i b_i$, is the image of $(r_1, \ldots, r_t)$.

Definition 4.1. A *presentation* of M, which we may also call 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 $\ker(\phi) = \mathrm{im}(\psi)$. The image of ϕ generates M and the kernel of ϕ is the set of relations on those generators.

Polynomial rings over a field

For the remainder of these notes, we will focus on polynomial rings over a field.

Example 4.2. Consider the ideal $\langle x, y\rangle$ in $R = k[x, y]$. Then

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

is a surjective homomorphism. Recall that I'm writing elements of R^n as row vectors. So a 2×1 matrix gives a homomorphism from R^2 into R. Here $\langle x, y\rangle$ is the image.

The kernel of this map is the set of all $(f_1, f_2) \in R^2$ such that $f_1 x + f_2 y = 0$. We will prove later that a polynomial ring in n variables over a field, $k[x_1, \ldots, x_n]$, is a unique factorization domain. Writing $f_1 x = -f_2 y$ and using unique factorization, we have that $x \mid f_2$ and $y \mid f_1$, and the quotients f_2/x and $-f_1/y$ must be equal. Consequently, a presentation of $\langle x, y\rangle$ is

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

Definition 4.3. Let $F = \{f_1, \ldots, f_t\}$ be elements of R. Consider the homomorphism

$$\begin{array}{c} R^t \longrightarrow \langle F\rangle \\ e_i \longmapsto f_i \end{array}$$

The kernel of this homomorphism is called the *syzygy module* of F and is written $S(F)$.

We would like to identify generators for $S(F)$ and construct a surjective homomorphism from R^s for some s to $S(F)$. This would give a presentation of $\langle F \rangle$.

Monomial ideals

Let us first treat monomial ideals in $R = k[x_1, \ldots, x_n]$.

Consider the monomial ideal generated by

$$G = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\} \tag{1}$$

and let

$$\gamma_{ij} = \text{lcm}\{\alpha_i, \alpha_j\} \tag{2}$$

Here $\alpha_i \in \mathbb{N}_0^n$, so each α_i is a vector of length n. IVA uses $\alpha(i)$, rather than α_i, but that notation becomes unwieldy in what follows, so I've adopted α_i. Just remember that it is an element of $\mathbb{N}_0^n$. Note also that $\text{lcm}(\alpha, \beta)$ might more properly be called the least common sum, it is the smallest element $\gamma \in \mathbb{N}_0^n$ such that $\gamma - \alpha$ and $\gamma - \beta$ are both in $\mathbb{N}_0^n$.

For the presentation $R^s \longrightarrow \langle G \rangle$ taking basis vector e_i to x^{α_i} we have elements of the syzygy module

$$\bar{S}_{ij} = x^{\gamma_{ij} - \alpha_i} e_i - x^{\gamma_{ij} - \alpha_j} e_j \tag{3}$$

We will show that these generate the syzygy module.

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

We will call an element $\bar{m} = (m_1, \ldots, m_s)$ of R^s *homogenous* of degree δ (with respect to $(\alpha_1, \ldots, \alpha_s)$) when the entries of m are all monomials and $\text{LE}(m_i x_i^\alpha) = \delta$ for all nonzero m_i. We may also write this as $\text{LE}(m_i) + \alpha_i = \delta$.

Lemma 4.4. *Any element of R^s, where $R = k[x_1, \ldots, x_n]$, may be written in a unique way as a sum of homogeneous elements.*

Proof. Let $\bar{h} = (h_1, \ldots, h_s) \in R^s$. 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 $\bar{h} = \sum_{\beta \in \mathbb{N}_0^n} (h_{1,\beta} x^{\beta - \alpha_1}, \ldots, h_{s,\beta} x^{\beta - \alpha_s})$ expresses $\bar{h}$ as a sum of homogeneous terms. □

Example 4.5. Consider $k[x, y]$, (so $n = 2$) and $s = 3$. Let $h = (1 + x + y, x + 2y + 3x^2, y + 2x^2)$. If $\alpha_1 = \alpha_2 = \alpha_3 = (0, 0)$ there is no shifting and we may write h as the sum of homogeneous elements

$$\begin{aligned} &(1, 0, 0) \\ &(x, x, 0) \\ &(y, 2y, y) \\ &(0, 3x^2, 2x^2) \end{aligned}$$

If $\alpha_1 = (1, 0)$, and $\alpha_2 = (0, 1)$ and $\alpha_3 = (0, 0)$ then h is the sum of homogeneous elements

$$\begin{aligned} (1, 0, 0) &\quad \text{of multidegree } (1, 0) \\ (x, 0, 2x^2) &\quad \text{of multidegree } (2, 0) \\ (0, 0, y) &\quad \text{of multidegree } (0, 1) \\ (y, x, 0) &\quad \text{of multidegree } (1, 1) \\ (0, 3x^2, 0) &\quad \text{of multidegree } (2, 1) \\ (0, 2y, 0) &\quad \text{of multidegree } (0, 2) \end{aligned}$$

Lemma 4.6. *For G a set of monomials, any element of $S(G)$ may be written as a sum of homogeneous elements in $S(G)$.*

Proof. Let $\bar{h} = (h_1, \ldots, h_s) \in S(G)$. Write $\bar{h} = \sum_{\beta \in \mathbb{N}_0^n} (h_{1,\beta} x^{\beta - \alpha_1}, \ldots, h_{s,\beta} x^{\beta - \alpha_s})$ as a sum of homogeneous terms, as in the previous lemma. 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 $\sum_{i=1}^{s} h_{i,\beta} = 0$. Thus, each term in the homogeneous expansion of $\bar{h}$ is in $S(G)$. □

Theorem 4.7. *For a monomial generating set G, the $\bar{S}_{ij}$ in* (3) *generate $S(G)$.*

Proof. By the previous 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. Observe that 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. □

Example 4.8. Consider $k[x,y]$ and let $G = (y^2, x^2y, x^3)$. The image of the following homomorphism is $\langle G \rangle$.

$$\begin{array}{ccc} R^2 & \longrightarrow & \langle G \rangle \\ & \begin{bmatrix} y^2 \\ x^2y \\ x^3 \end{bmatrix} & \end{array}$$

A presentation of $\langle G \rangle$ is

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

In this example the exponents of the elements of G are $\alpha_1 = (0,2)$, $\alpha_2 = (2,1)$ and $\alpha_3 = (3,0)$. 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

Let us now work with a monomial ordering $<$ on $R = k[x_1, \ldots, x_n]$.

Let $G = (g_1, \ldots, g_s)$ be a Groebner basis for the ideal it generates with respect to the term order $<$. We want to relate the generators and relations representation of $\langle G \rangle$ to that for $S(G)$. Let's assume that G is a minimal Groebner basis, so no leading term divides another and the g_i are monic. Let $LE(g_i) = \alpha_i$ and let $\gamma_{ij} = \text{lcm}(\alpha_i, \alpha_j)$.

Since the g_i are all monic, 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 Groebner basis, $S(g_i, g_j) \xrightarrow{G} 0$, and this means that $S(g_i, g_j) = \sum_k a_k g_k$ where $a_k \in R$ and $\text{LE}(a_k g_k) \leq \text{LE}(S(g_i, g_j)) < \gamma_{ij}$. The latter inequality comes from the cancellation of the degree γ_{ij} terms that occurs in the computation of $S(g_i, g_j)$ and the first inequatity is from the definition of $\xrightarrow{G}$. Rewriting this we get

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

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 $S(\mathrm{LT}(G))$.

Theorem 4.9. *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 $S(G)$.*

Proof. We may write any $\bar{h} \in R^s$ as a sum of homogeneous elements relative to $(\alpha_1, \ldots, \alpha_s)$ as we did in Lemma 4.4. Thus, $\bar{h} = \sum_{\beta\in\mathbb{N}_0^n}(h_{1,\beta}x^{\beta-\alpha_1}, \ldots, h_{s,\beta}x^{\beta-\alpha_s})$.

Suppose that $\bar{h} \in S(G)$ and let $\delta = \max_i\{\mathrm{LE}(h_i) + \alpha_i\}$. Let $\bar{m}$ be the "leading term" of $\bar{h}$, that is the vector consisting of the homogeneous terms of degree δ in $\bar{h}$. Then $\bar{m} = (m_1, \ldots, m_s)$ is homogeneous and each m_i is either 0 or of degree $\delta - \alpha_i$.

We know that $\sum_{i=1}^s h_i g_i = 0$, so in particular the term in x^δ is 0. This term is $\sum_{i=1}^s m_i \,\mathrm{LM}(g_i)$, and recall $\mathrm{LM}(g_i) = x^{\alpha_i}$. Thus we have that $\bar{m} \in S(\mathrm{LT}(G))$. Since the $\bar{S}_{ij}$ generate $S(\mathrm{LT}(G))$ we have $\bar{m} = \sum_{i\neq j} n_{ij}\bar{S}_{ij}$ for monomials n_{ij}.

Now consider $\bar{h} - \sum_{i,j} n_{ij}\bar{T}_{ij}$. It is still in $S(G)$. The homogeneous part of degree δ is 0, because the leading term of h is $\bar{m}$ and the leading term of $\sum_{i\neq,j} n_{ij}\bar{T}_{ij}$ is $\sum_{i\neq j} n_{i\neq j}\bar{S}_{ij}$, which by construction is also $\bar{m}$.

Continuing this process recursively we may at each step subtract some combination of the T_{ij}, lowering the leading term at each time. This process must eventually terminate leaving us with the 0 element of $S(G)$. Thus $\bar{h}$ is a combination of the T_{ij}. □

Example 4.10. Consider $k[x, y]$ with glex and $x > y$. Let $G = (y^2 - x, x^2y - x, x^3 - y^3)$. A presentation of $\langle \mathrm{LT}(G)\rangle$ was given in Example 4.8. Let us extend this to a presentation 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 $S(G)$

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

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

5 Exercises

Please read and work Ash 4.1 #3, 4, 5, 6 and Ash 4.3 #3, 4.

Problem 1: Consider the ring $2^{-1}\mathbb{Z}$ as a module over $\mathbb{Z}$.

- **(a)** Show that $2^{-1}\mathbb{Z}$ is not finitely generated. (By contradiction.)
- **(b)** Show that any two elements of $2^{-1}\mathbb{Z}$ are linearly dependent: some combination is 0.
- **(c)** Consider the module $2^{-1}\mathbb{Z}/\mathbb{Z}$. Show that any element is a *torsion* element. This means that some nonzero multiple is 0.
- **(d)** Show that $2^{-1}\mathbb{Z}/\mathbb{Z}$ satisfies the descending chain condition but not the ascending chain condition.

Problem 2: Find a presentation for the ideal $\langle x - y^2, x^2 y - x \rangle$ in the lexicographic order for $x > y$ and in the lexicographic order for $y > x$.