Syzygies without Tor

Dennis B. Westra

Syzygies are fascinating objects; they contain important information of modules and they have the advantage that they can be calculated. In this expository text we give a brief introduction and prove an important theorem of Hilbert.

Syzygies were introduced by David Hilbert in his seminal paper [1] already in 1890. Hilbert wanted to use his syzygies for invariant theory, but nowadays, syzygies are of general importance in algebraic geometry. Again, Hilbert was ahead of his time. The reader might then ask, "ok, nice, but what are these syzygies?" (and how do I pronounce the word?) In short, a syzygy of a module is a kernel appearing in a free resolution. (The pronunciation is `si-si-gee`.) In the text below we give a longer definition with some more preparation.

We will give a proof of Hilbert's syzygy theorem that does not use the more advanced notions as Tor and Koszul complexes. The proof is not the author's own proof, but can be found in the formidable book written by Zariski and Samuel[4]. First we give a brief introduction to free resolutions and syzygies.

1 Syzygies and free resolutions

We will assume that the reader knows what rings and modules are. For those who get frightened, we recommend to read a few section in the nicely written book by Miles Reid [2], or read some parts in the first chapters of the (almost exhaustive) book by Serge Lang [3]. Furthermore we will assume that the reader knows what a Noetherian ring is, what a finitely generated module is, what a free module is and the basic fact that any submodule of a finitely generated module of a Noetherian ring is again finitely generated. All our rings are commutative, associative and have a 1. We shortly give the definition of an exact sequence, since that will be of crucial importance: a chain of modules connected by maps $M_1 \to M_2 \to M_3 \to ...$ is called exact at M_2 if the kernel of the map $M_2 \to M_3$ is precisely the image of the map $M_1 \to M_2$. In particular, the map $M_1 \to M_3$ which is the concatenation of the maps $M_1 \to M_2$ and $M_2 \to M_3$ maps all of M_1 to zero in M_3. A sequence is called exact if it is exact at each module that has an arrow on its left and on its right (to exclude the endpoints). Some exercises to get a feeling for what happens: (i) a sequence $0 \to M_1 \to M_2$ is exact if and only if $M_1 \to M_2$ is injective, (ii) a sequence $M_1 \to M_2 \to 0$ is exact if and only of $M_1 \to M_2$ is a surjective, (iii) a sequence $0 \to M_1 \to M_2 \to 0$ is exact if and only if $M_1 \cong M_2$. (iv) For vector spaces $0 \to V_1 \to V_2 \to V_3 \to 0$ is exact if and only if $V_2 \cong V_1 \oplus V_3$.

The starting point is a Noetherian ring R. All finitely generated free modules are of the form R^q for some integer $q \geq 1$. Elements of R^q we will denote $\mathbf{r} = (r_1, \dots, r_q)$, where the r_i are elements of R. If a module M is finitely generated, then there are some generators $m_1, \dots, m_s$ in M such that each $m \in M$ can be written as $m = r_1 m_1 + \dots + r_s m_s$ for some $r_i \in R$. These r_i

might not be unique. Thus, a finitely generated module M that is generated by s generators $m_1, \ldots, m_2$, admits a surjective map $R^s \to M$, where $(r_1, \ldots, r_s)$ is mapped to $r_1 m_1 + \ldots + r_s m_s$. In terms of exact sequences, this is written as

$$R^s \longrightarrow M \longrightarrow 0\,.$$

The kernel of this map $R^s \to M$ is called a first syzygy of M. We see that a first syzygy depends on the choice of the generators, and that for a fixed choice of generators $m_1, \ldots, m_s$, the first syzygy measures how nonunique the r_i in an expansion $m = r_1 m_1 + \ldots + r_s m_s$ are.

Let us now introduce some more notation, since it will get messy: we write K_1 for the kernel of the map $R^s \to M$, and for R^s we write F_1. We thus are in the situation where there is a surjective map $\varphi_1 : F_1 \to M$, with F_1 a finitely generated free module.

Next we consider the kernel of this map $F_1 \to M$. We know that the kernel is a submodule of R^s and thus finitely generated. Hence there exists a surjective map $F_2 \to K_1$, where F_2 is a finitely generated free module. We combine this map $F_2 \to K_1$ with the inclusion of K_1 into F_1 to get $\varphi_2 : F_2 \to F_1$. The map φ_2 is neither surjective, nor injective, but the following sequence is exact

$$F_2 \longrightarrow F_1 \to M \longrightarrow 0\,.$$

The kernel K_2 of the map $F_2 \to F_1$ is called a second syzygy; since it depends on the choice of the generators of the kernel K_1. The procedure we just performed to attach F_2 to the chain can be repeated again and again: for the kernel K_2 we can attach a finitely generated free module F_3 that maps onto the generators of K_2, and we combine this with the inclusion $K_2 \to F_2$ to get a map $F_3 \to F_2$. Then the sequence

$$F_3 \longrightarrow F_2 \longrightarrow F_1 \to M \longrightarrow 0\,,$$

is exact. Proceeding in this way we obtain a so-called free resolution of M:

$$... \longrightarrow F_{i+1} \longrightarrow F_i \longrightarrow ... \longrightarrow F_1 \longrightarrow M \longrightarrow 0\,.$$

The kernel of the map $F_i \to F_{i-1}$ is called an ith syzygy of M. With a slight abuse of language one also calls the free resolution of M a syzygy.

Since both the free resolution and the precise form of the syzygies depend on choices of generators at each step of the process of adding a free module to the chain, one might wonder whether these resolutions and syzygies are of any use at all. Another question might be, whether the free resolution is finite under some circumstances. The answer to the last question is yes for local regular rings and for free polynomial rings. For this last case we give a proof below (for the other case, we refer to Zariski and Samuel [4]). To answer the first question, we actually need to require that the reader knows more. For example, free resolutions are a particular example of projective resolutions, which are needed to calculate the mysterious $\mathrm{Tor}^i(M, N)$ and which are ubiquitous in the literature (and hence important). What actually counts here is the homology of a sequence one obtains by tensoring a free resolution with N: after tensoring with N the obtained sequence might no longer be exact and the $\mathrm{Tor_i(M, N}$ measure how nonexact this sequence is, and thus how nonflat N is. A more geometric application is given by considering an algebraic variety X embedded in $\mathbb{C}^n$. When we want to know the dimension of X, we can do it by calculating the Hilbert function of the associated coordinate ring, which in practice can be a horrendous task. If we know a free resolution, life becomes easier, since we know the Hilbert functions of free polynomial rings - they are rather easy. To summarize: yes, there are case where free resolutions are useful and in fact, the information one uses is not so much in the precise form of the free modules appearing in the free resolution as well as in the chain as a whole. This information is not changed when we find another free resolution. (Note: this kind of thinking initialized the birth of triangulated categories and the general theory of derived functors, leading to complicated issues like Grothendieck duality.)

2 Equivalences of first syzygies

The presentation of Zariski and Samuel starts with an observation that is rather useful and that ends with a lemma that is of general interest.

The observation is captured in the statement:

> for two different first syzygies S and S', there exist free modules T and T' such that $S \oplus T \cong S' \oplus T'$.

To see this, we consider what happens when we choose a different set of generators for M. Suppose, we have two sets of generators $B = \{m_1, \ldots, m_s\}$ and $B' = \{n_1, \ldots, n_t\}$ giving rise to two maps: $\varphi : F \to M$ and $\varphi' : F' \to M$, where $F = R^s$, $F' = R^t$ and $\varphi : (r_1, \ldots, r_s) \mapsto m_1 r_1 + \ldots + m_s r_s$ and $\varphi'(r_1, \ldots, r_t) :\mapsto n_1 r_1 + \ldots + n_t r_t)$. Let K be the kernel of φ and K' the kernel of φ'. We then consider the map $\psi : F \oplus F' \to M$ given by $\psi(\mathbf{x}, \mathbf{y}) = \varphi(\mathbf{x}) + \varphi(\mathbf{y})$ and call L the kernel of ψ. Clearly, $K \oplus K' \subset L$. Since both B and B' are sets of generators, we have an expression of the form

$$n_i = \sum_k c_{ik} m_k \,.$$

We now define the s-vectors $\mathbf{c}_i = (c_{i1}, , \ldots, c_{is}) \in F$ and the elements $\mathbf{t_i} \in F \oplus F'$ by

$$\mathbf{t}_i = (\mathbf{c}_i, \mathbf{e}_i) \,,$$

where $\mathbf{e}_i \in F'$ is a t-vector with zeros everywhere, except at the ith entry, where there is a 1. The $\mathbf{t}_i$ generate a submodule T of L and one easily sees that T is a free module. Let now $(\mathbf{x}, \mathbf{y})$ be an element of T, then $\sum_i x_i m_i + \sum_j y_j n_j = 0$. But then

$$0 = \sum (x_i + y_j c_{ji}) m_i \,,$$

and thus $\mathbf{x} + \sum y_j \mathbf{c}_j$ lies in S. We can then write any element of L as

$$(\mathbf{x}, \mathbf{y}) = (\mathbf{x} + \sum y_j \mathbf{c}_j, 0) - \sum y_j \mathbf{t}_j \,,$$

which means that $L = T \oplus S$. Interchanging the S and S', we see that there exists a free module T' such that $L = T' \oplus S'$. We conclude that for two first syzygies S and S' there exist two finitely generated free modules T and T' such that $S \oplus T \cong S' \oplus T'$.

We now show that the observation gives rise to an equivalence relation on the class of finitely generated R-modules. We define two modules M and M' to be equivalent if there exist free modules F and F' such that $M \oplus F \cong M' \oplus F'$.

If M and M' are equivalent we write $M \sim M'$. Trivially we have $M \sim M$; just take the zero-module. Furthermore, if M and M' are isomorphic, then $M \sim M'$. By the definition of being equivalent, if $M \sim M'$ then also $M' \sim M$ - because we defined the equivalence in a symmetric way. Now let $M \sim M'$ and $M' \sim M''$, then there are free modules F, F', G' and G'' such that $M \oplus F \cong M' \oplus F'$ and $M' \oplus G' \cong M'' \oplus G''$. Hence we have

$$M \oplus F \oplus G' \cong M' \oplus F' \oplus G' \cong M'' \oplus G'' \oplus F' ,$$

and it follows that $M \sim M''$.

To prove that all further syzygies are equivalent in the sense mentioned above, it suffices to show that if two modules are equivalent then their first syzygies are also equivalent. Let therefore M and M' be equivalent modules, so that there are free modules L and L' with $M \oplus L \cong M' \oplus L'$. Let F and F' be two finitely generated free modules such that

$$0 \longrightarrow S \longrightarrow F \longrightarrow M \longrightarrow 0 , \quad 0 \longrightarrow S' \longrightarrow F' \longrightarrow M' \longrightarrow 0 ,$$

are exact. Thus S is a first syzygy of M and S' is a first syzygy of M'. Let us denote the surjective map $F \to M$ by φ and the surjective map $F' \to M'$ by φ' so that $S = \text{Ker}\varphi$ and $S' = \text{Ker}\varphi'$. It is easily verified that the map

$$F \oplus L \to M \oplus L , \quad (\mathbf{f}, \mathbf{l}) \mapsto (\varphi(\mathbf{f}), \mathbf{l}) ,$$

has kernel S and the map

$$F' \oplus L' \to M' \oplus L' , \quad (\mathbf{f}', \mathbf{l}') \mapsto (\varphi'(\mathbf{f}'), \mathbf{l}') ,$$

has kernel S'. Since $M \oplus L \cong M' \oplus L'$ the first syzygies are equivalent, hence $S \sim S'$. So we conclude that no matter how the choices are made in obtaining a free resolution of M, all the syzygies (the kernels of the maps appearing in the free resolution) are equivalent.

Now we will take a step ahead. We want to prove that for modules of nice rings, the free resolutions are finite. By finite we mean that the free resolution contains only a finite number of nonzero free modules. In order that the free resolution terminates at the $(n+1)$th step it is necessary and sufficient that the nth syzygy is a free module. To prove that the statement that the resolution terminates at the $(n+1)$th step is independent of the choices made, it is sufficient to prove that when two modules are equivalent to each other and one of them is a free module, then so is the other. Indeed, suppose that the nth syzygy K in a free resolution is free, so that the $(n+1)th$ free module is zero in the free resolution. Then in any other free resolution the nth syzygy K' is equivalent to K by the above and hence also free. Thus the other free resolution also terminates at the $(n+1)$th step. So we are set to prove the following: let M be any module such that there is a finitely generated free module F such that $M \oplus F$ is a free module, then M is free. Unfortunately, the statement does not hold for all rings. We therefore restrict from now to the case where $R = k[x_1, \ldots, x_n]$ for some n. Since R is now canonically $\mathbb{Z}$-graded, we also require that our modules are $\mathbb{Z}$-graded and that the action of R preserves the grading. The assumptions now imply that finitely generated graded modules are generated by homogeneous elements. In this case we are better off than in the general case. So, we make the milder statement:

Consider $R = k[x_1, \dots, x_n]$ as a $\mathbb{Z}$-graded ring and suppose M is a $\mathbb{Z}$-graded finitely generated R-module. Then M is free if and only if there exists a free module F so that $M \oplus F$ is free.

If M is free, then also $M \oplus R$ is free. For the converse, we note that the statement is proven if we have proven the following: M is free if and only if $M \oplus R$. Indeed, we look at the modules $M \oplus R$, $M \oplus R^2$, and so on. When we reach $M \oplus F$, we conclude that at the previous step we already had a free module, and thus at the step before that we also had a free module and so on, till we have traced back our path to M.

Assume $M \oplus R$ is generated by homogeneous generators $f_1, \dots, f_s$, so that $M \oplus R \cong R^s$. Any $m \in M$ we can inject into $M \oplus R$ and then there are r_i so that $m = \sum r_i f_i$. We decompose the f_i as $f_i = m_i + a_i e$, where the m_i are in M, the a_i are in R and e is the generator of the R-summand (so to say, the 1). Since the f_i are homogeneous and e is homogeneous, so the a_i are homogeneous. We then have for m

$$m = \sum_i r_i m_i + \Big(\sum_j r_j a_j\Big) e\,.$$

As the sum is direct, we thus have $\sum_j r_j a_j = 0$ and we conclude that the m_i generate M. As $(0, e) \in M \oplus R$ there are homogeneous $t_i \in R$ so that $e = \sum t_i f_i = \sum t_i m_i + \sum_j t_j a_j e$ from which it follows that $\sum_i t_i a_i = 1$. This equation can only be fulfilled in R if there is a t_i whose constant part is nonzero. As the t_i are homogeneous, it follows that at least one t_i must be in k, and is thus invertible. So we assume t_1 is invertible. From the equation

$$\sum_i t_i m_i = 0\,,$$

it follows that M can be generated by $m_2, \dots, m_s$. The amazing step is now that we claim that the generators $m_2, \dots, m_s$ are independent; that is, the canonical map $R^{s-1} \to M$ sending $(r_2, \dots, r_s)$ to $r_2 m_2 + \dots r_s m_s$ has zero kernel. This implies that M is a free module. So we consider any relation of the form $\sum c_i m_i = 0$ and we are interested in the existence of solutions $\mathbf{c}$ with $c_1 = 0$. We calculate

$$0 = \sum_i c_i m_i = \sum_i c_i (f_i - a_i e) = \sum_i c_i f_i - \Big(\sum_j c_j a_j\Big)\Big(\sum_i t_i f_i\Big)\,,$$

from which it follows that $c_i = t_i \sum_j c_j a_j$. But, then if $c_1 = 0$, then since t_1 is invertible, we must have $\sum_j c_j a_j = 0$ and then all c_i vanish. Hence, there is no nontrivial $\mathbf{c}$ with $c_1 = 0$ and $\sum c_i m_i = 0$. Thus the $m_2, \dots, m_s$ generate a free module and thus M is free. This concludes the proof of the statement, and we are ready to deal with the proof that all free resolutions are finite.

We remark that the above proof also works for more general $\mathbb{Z}$-graded rings and for local rings. For these cases we refer to [4].

3 Finitely many syzygies

We again make the simplifying assumption that $R = k[x_1, \dots, x_n]$. We consider the ideals $\mathfrak{m}_j = (x_1, \dots, x_j)$. The ideal

$$(\mathfrak{m}_{j-1} : \mathfrak{m}_j) = \{r \in R | r\mathfrak{m}_j \subset \mathfrak{m}_{j-1}\}$$

clearly contains $\mathfrak{m}_{j-1}$. If p is any polynomial depending nontrivially on x_j, then pq also depends nontrivially on x_j, for any nonzero q. Thus $(\mathfrak{m}_{j-1} : \mathfrak{m}_j) = \mathfrak{m}_{j-1}$. With this observation in mind, we are ready to prove the following:

> Let R be the $\mathbb{Z}$-graded ring $k[x_1, \ldots, x_n]$ and M be a finitely generated $\mathbb{Z}$-graded module of R. Then the nth syzygy is a free module.

The theorem is due to David Hilbert and is known as the Hilbert Syzygy Theorem. Actually, Hilbert proved its theorem in a slightly more general form, whose proof is virtually the same. We again refer to [4] for a more complete discussion. Below we give the proof of the statement, which will also be the end of this exposition.

We may assume that M is a submodule of a free module. Indeed, if not we can find a free module F so that $F \to M$ is surjective and the kernel S of such a map is a first syzygy and S is a submodule of a free module. A free resolution of M is then constructed by making a free resolution of S.

Given a free resolution

$$\ldots \longrightarrow F_{i+1} \longrightarrow F_i \longrightarrow \ldots \longrightarrow F_1 \longrightarrow M \longrightarrow 0\,,$$

we call φ_i the map $F_{i+1} \to F_i$ and we call S_i the kernel of φ_{i-1}. Then $S_i \subset F_i$.

Now suppose that y is an element of $S_k \cap \mathfrak{m}_1 F_k$ for $k \geq 1$. Then $y = x_1 a$ for some $a \in F_k$ and $\varphi_{k-1}(y) = 0$ so that $x_1 \varphi_{k-1}(a) = 0$. Since all the modules in the resolutions are free or submodules of a free module, this equation can only be solved if $\varphi_{k-1}(a) = 0$ and thus $y \in \mathfrak{m}_1 S_k$. It follows that $S_k \cap \mathfrak{m}_1 F_k = \mathfrak{m}_1 S_k$ for all $k \geq 1$.

In a next step we suppose that y is an element of $S_k \cap \mathfrak{m}_1 F_k$ for $k \geq 2$. Then we can write $y = x_1 a_1 + x_2 a_2$ for some $a_1, a_2 \in F_k$ and we have $x_1 \varphi_{k-1}(a_1) + x_2 \varphi_{k-1}(a_2) = 0$. It follows that

$$x_2 \varphi_{k-1}(a_2) \in \mathfrak{m}_1 F_{k-1}\,.$$

Using the preparing remark that $(\mathfrak{m}_{j-1} : \mathfrak{m}_j) = \mathfrak{m}_{j-1}$, we deduce that $\varphi_{k-1}(a_2)$ is in $\mathfrak{m}_1 F_{k-1}$. Since furthermore $\varphi_{k-1}(a_2) \in S_{k-1}$ we have $\varphi_{k-1}(a_2) \in \mathfrak{m}_1 S_{k-1}$. Since $S_{k-1} = \mathrm{Im}(\varphi_{k-1})$ there is a $b \in F_k$ with $\varphi_{k-1}(a_2) = x_1 \varphi_{k-1}(b)$. We then write

$$y = x_1(a_1 + x_2 b) + x_2(a_2 - x_1 b)\,,$$

from which we see that $y \in \mathfrak{m}_2 S_k$. Hence it follows that $S_k \cap \mathfrak{m}_2 F_k = \mathfrak{m}_2 S_k$ for all $k \geq 2$. Now the reader might already see the pattern! We will do one more step...

Suppose that

$$y = x_1 a_1 + x_2 a_2 + x_3 a_3 \; \in \mathfrak{m}_3 F_k \cap S_k$$

for $k \geq 3$. Then it follows that $x_3 \varphi_{k-1}(a_3)$ lies in $\mathfrak{m}_2 F_{k-1}$. We conclude by the preparing remark that $\varphi_{k-1}(a_3)$ lies in $\mathfrak{m}_2 F_{k-1}$. Since $\varphi_{k-1}(a_3)$ also lies in S_{k-1} we see that $\varphi_{k-1}(a_3)$ is an element of $\mathfrak{m}_2 S_{k-1} = \mathfrak{m}_2 \mathrm{Im}(\varphi_{k-1})$. We thus can write

$$\varphi_{k-1}(a_3) = x_1 \varphi_{k-1}(b_1) + x_2 \varphi_{k-1}(b_2)\,,$$

for some $b_1, b_2 \in F_k$. Expressing y as

$$y = x_1(a_1 + x_3 b_1) + x_2(a_2 + x_3 b_2) + x_3(a_3 - x_1 b_1 - x_2 b_2)\,,$$

shows that $y \in \mathfrak{m}_3 S_k$. Hence $\mathfrak{m}_3 F_k \cap S_k = \mathfrak{m}_3 S_k$ for all $k \geq 3$. We can repeat this procedure till we reach

$$\mathfrak{m}_n F_n \cap S_n = \mathfrak{m}_n S_n \,.$$

Now, let $s_1, \ldots, s_t$ be a set of homogeneous generators of S_{n-1} and assume that no s_i can be expressed in terms of the other generators. There is a surjective map $R^t = F_n \to S_{n-1}$. Suppose y is in the kernel of this map. Then there is a relation $\varphi_{n-1}(y) = \sum_i y_i s_i = 0$ for some $y_i \in R$. Since the s_i are homogeneous, all the homogeneous components of $\sum_i y_i s_i$ have to vanish. In particular this implies that all a_i have to lie in $\mathfrak{m}_n$: Assume conversely that $y_1 = \alpha(1-p)$ with $\alpha \in k$ and $p \in \mathfrak{m}_n$. We then write

$$(1-p)s_1 = -\alpha^{-1} \sum_{i>1} y_i s_i \,.$$

Looking at the left-hand side and knowing that the degrees of the homogeneous parts of ps_1 are higher than the degree of s_1, we see that s_1 can be expressed in terms of the s_i with $i > 2$, which is a contradiction to the assumption that no s_j can be expressed in terms of the others. Therefore all y_i are in $\mathfrak{m}_n$ and we have $S_n \subset \mathfrak{m}_n F_n$. Combining this with the equality $\mathfrak{m}_n F_n \cap S_n = \mathfrak{m}_n S_n$ we obtain

$$S_n = \mathfrak{m}_n S_n \,.$$

But then, S_n must be zero: Let y be a homogeneous element of lowest degree d in S_n, then $y \in \mathfrak{m}_n S_n$ and thus there must be some $x_i \in (S_n)_{d-1}$ and $r_i \in R$ so that $y = \sum_i r_i x_i$. But since by assumption $(S_n)_{d-1} = 0$, we can only have $x_i = 0$ and thus $y = 0$. Hence $S_n = 0$ and thus S_{n-1} is free, which is what we wanted to prove.

Any comments, remarks and questions can be sent to `dbwestra@gmail.com`.

References

[1] David Hilbert, Über die theorie von algebraischen formen, Math. Ann. 36 (1890).

[2] Miles Reid, Undergraduate Algebraic Geometry, London Mathematical Society Student Texts, Cambridge University Press (1995).

[3] Serge Lang, Algebra, Addison-Wesley Publishing Company (1993).

[4] O. Zariski and P. Samuel, Commutative algebra, Volume II, Graduate Texts in Mathematics, Springer Verlag (1985).