Eberhard-Karls-Universität Tübingen
Prof. Hannah Markwig
Alheydis Geiger

Wintersemester 2020/2021
23. December 2020

Introduction to Commutative Algebra and Algebraic Geometry
Solution to Exercise Sheet 7

Exercise 1.
Let $R = \mathbb{Q}[x, y, z]$. Compute a Groebner basis of $I = \langle xy - y, 2x^2 + yz, y - z\rangle \subset R$ with respect to the monomial order $>_{lp}$ with $x > z > y$.

Solution: We apply the Groebner basis algorithm (2.3.8):
Set $S_0 = \{xy - y, 2x^2 + yz, y - z\}$. We write $f_1 = xy - y,\ f_2 = 2x^2 + yz,\ f_3 = y - z$.
We have $P = \{(xy - y, 2x^2 + yz), (xy - y, y - z), (2x^2 + yz, y - z)\}$. Before we start with the algorithm we consider the set of pairs P. During the algorithm we will have to compute the spolys of the pairs and the remainder of an indeterminate division of the spolys with S. Only those pairs with remainder not zero will be relevant for the algorithm. By applying the product criterion we can delete those pairs (f, g) in P for which $\gcd(\mathrm{LM}(f), \mathrm{LM}(g)) = 1$.
This happens for the pairs (f_1, f_3) and (f_2, f_3), since $\mathrm{LM}(f_1) = xy$, $\mathrm{LM}(f_3) = z$ so $\gcd(xy, z) = 1$ and $\mathrm{LM}(f_2) = x^2$, $\mathrm{LM}(f_3) = z$ so $\gcd(x^2, z) = 1$.
So we can start the algorithm with $\tilde{P} = \{(xy - y, 2x^2 + yz)\}$ instead of P.

1. Step: We compute $\mathrm{spoly}(f_1, f_2)$

$$\begin{aligned}\mathrm{spoly}(xy - y, 2x^2 + yz) &= \frac{2x^2}{x} \cdot (xy - y) - \frac{xy}{x} \cdot (2x^2 + yz)\\ &= 2x \cdot (xy - y) - y \cdot (2x^2 + yz)\\ &= -2xy - y^2 z\end{aligned}$$

Now we compute the remainder of indeterminate division of $-2xy-y^2z$ with f_1, f_2, f_3. We have $\mathrm{LM}(-2xy-y^2z) = xy$, $\mathrm{LM}(f_1) = xy$, $\mathrm{LM}(f_2) = x^2$, $\mathrm{LM}(f_3) = z$. So we start with $\mathrm{LM}(f_1)|\mathrm{LM}(-2xy - y^2z)$. (Buchberger ID)

Set $q_1 = -2$ and

$$r = -2xy - y^2z - (-2)(xy - y) = -y^2z - 2y$$

The leading monomial of the new r is y^2z, which can be divided by $\mathrm{LM}(f_3) = z$.

Set $q_3 = -y^2$ and

$$r = -y^2z - 2y - (y^2)(y - z) = -2y - y^3$$

Now $\mathrm{LM}(r) = y^3$ which does not get divided by any of the leading monomials of the f_i. Since $r \neq 0$ we add $r = -2y - y^3$ to S_0 and obtain $S_1 = \{xy - y, 2x^2 + yz, y - z, -2y - y^3\}$.

2. Step: Compute the set of pairs. We now need only consider those pairs containing $f_4 = -2y - y^3$. So we have $P_1 = \{(xy-y, -2y-y^3), (2x^2+yz, -2y-y^3), (y-z, -2y-y^3)\}$. Again applying the product criterion we see that we can delete the pairs $(2x^2+yz, -2y-y^3), (y-z, -2y-y^3)$ from P_1. (The gcd of $\mathrm{LM}(2x^2+yz) = x^2$, $\mathrm{LM}(-2y-y^3) = y^3$ is one, as well as the gcd of $\mathrm{LM}(y - z) = z$, $\mathrm{LM}(-2y - y^3) = y^3$.) So we have $\tilde{P_1} = \{(xy - y, -2y - y^3)\}$

Now we compute $\mathrm{spoly}(f_1, f_4)$.

$$\begin{aligned}\mathrm{spoly}(xy - y, -y^3 - 2y) &= \frac{-y^3}{y} \cdot (xy - y) - \frac{xy}{y} \cdot (-y^3 - 2y)\\ &= -y^2 \cdot (xy - y) - x \cdot (-y^3 - 2y)\\ &= y^3 + 2xy\end{aligned}$$

We need to compute the remainder of of indeterminate division of y^3+2xy with f_1, f_2, f_3, f_4. (Buchberger ID) We have $\mathrm{LM}(y^3+2xy) = xy$, $\mathrm{LM}(f_1) = xy$, $\mathrm{LM}(f_2) = x^2$, $\mathrm{LM}(f_3) = z$, $\mathrm{LM}(f_4) = y^3$. So we start with $\mathrm{LM}(f_1)|\mathrm{LM}(y^3+2xy)$.

Introduction to Commutative Algebra and Algebraic Geometry
Solution to Exercise Sheet 7

Set $q_1 = 2$ and

$$r = y^3 + 2xy - 2(xy - y) = y^3 + 2y$$

We see immediately that $r = -f_4$ so

$$y^3 + 2xy = 2f_1 - f_4 + r_2 \text{ where } r_2 = 0.$$

Since we have checked all remaining pairs from $\tilde{P}_1$, the algorithm terminates and $S_1 = \{xy-y, 2x^2+yz, y-z, -2y-y^3\}$ is a Groebner basis of I with respect to the monomial order $>_{lp}$ with $x > z > y$. $\square$.

Exercise 2.
Let $I \subset K[\underline{x}]$ be an ideal, $>$ a global monomial ordering and $B = \mathsf{Mon}(\underline{x}) \cap (K[\underline{x}] \setminus L(I))$ the set of monomials which are not in $L(I)$ the leading ideal of I. Show that $\overline{B}$ is a K-vector space basis of $K[\underline{x}]/I$.

Proof: By Corollary 2.3.3. there exists a Groebner basis $G = (f_1, \ldots, f_k)$ of I with respect to $>$. We want to show $\overline{B}$ is a K-basis of $K[\underline{x}]/I$.
Let $g \in K[\underline{x}]$. It follows with Buchberger RedID that there exist $q_1, \ldots, q_k, r \in K[\underline{x}]$ such that $g = \sum_{i=1}^{k} q_i f_i + r$ and this satisfies ID1 and DD2.
So in particular no term or r is in $\langle \mathsf{LM}(f_i) \rangle = L(I)$. It follows that $r \in \langle B \rangle_K$. Since $\overline{g} = \overline{r} \in \langle \overline{B} \rangle_K$, $\overline{B}$ generates $K[\underline{x}]/I$ as a K-vector space.
It remains to show that $\overline{B}$ is linearly independent. Let $\sum_{b \in B} a_b \overline{b} = \overline{0}$ with $a_b \in K$ for all $b \in B$. Then $\sum_{b \in B} a_b b \in I$, so $\mathsf{LM}(\sum_{b \in B} a_b b) \in L(I)$.
As $B \cap L(I) = \emptyset$ we have $\sum_{b \in B} a_b b = 0$, so $\forall b : a_b = 0$. $\square$

Exercise 3.
Show that the Groebner basis algorithm (2.3.8.) coincides with

a) the *Euclidean algorithm* when applied to two polynomials in $K[t]$ with $>$ being the unique well-ordering on $K[t]$;

b) the *Gaussian algorithm* when applied to any finite list of linear polynomials in $K[x_1, \ldots, x_n]$ with $>$ being the degree lexicographic ordering.

   Recall: The degree lexicographical ordering $>_{Dp}$ on Mon$_n$ is defined by

$$\underline{x}^\alpha >_{Dp} \underline{x}^\beta :\Leftrightarrow |\alpha| > |\beta| \text{ or } (|\alpha| = |\beta| \text{ and } \exists k : \alpha_1 = \beta_1, \ldots, \alpha_{k-1} = \beta_{k-1}, \alpha_k > \beta_k).$$

Proof:

a) Let $f, g \in K[t]$ be two polynomials. Note that the Euclidean algorithm gives us $\mathsf{gcd}(f, g)$, but the gcd is unique up to units. So we should also think "modulo units" when we apply the Groebner basis algorithm.
Assume $\mathsf{deg}(f) \leq \mathsf{deg}(g)$. The Euclidean algorithm applied to the pair (f, g) gives us $g = q_1 f + r_1$ for some $q_1, r_1 \in K[t]$.
With the Groebner basis algorithm we start with $S = \{f, g\}$ and compute $\mathsf{spoly}(f, g)$, where we know

$$\mathsf{lcm}(\mathsf{LM}(f), \mathsf{LM}(g)) = \mathsf{LM}(g)$$

since $\mathsf{deg}(f) \leq \mathsf{deg}(g)$. We have

$$\mathsf{spoly}(f, g) = \frac{\mathsf{LT}(g)}{\mathsf{LM}(f)} f - \mathsf{LC}(f) g$$
$$\Rightarrow \mathsf{LC}(f) g = \frac{\mathsf{LT}(g)}{\mathsf{LM}(f)} f - \mathsf{spoly}(f, g)$$

Introduction to Commutative Algebra and Algebraic Geometry Solution to Exercise Sheet 7

Notice that a division of spoly(f, g) w.r.t. f, g is of the form $\tilde{q}f + \tilde{r}$ since in spoly(f, g) the leading term gets cancelled and $\deg(g) \geq \deg(f)$.

$$\begin{aligned}\Rightarrow \mathsf{LC}(f)g &= \frac{\mathsf{LT}(g)}{\mathsf{LM}(f)}f - (\tilde{q}f + \tilde{r}) \\ &= (\frac{\mathsf{LT}(g)}{\mathsf{LM}(f)} - \tilde{q})f + \tilde{r}\end{aligned}$$

This representation satisfies DD1 and DD2, since we have a global monomial ordering and we only have one variable and only one $f_i = f$. By the uniqueness of determinate division, the remainder $\tilde{r}$ of this division is $\tilde{r} = r_1\mathsf{LC}(f)$, where $\mathsf{LC}(f)$ is a unit in $K[t]$. So the remainders $\tilde{r}$ and r_1 coincide up to a unit. So now we add r_1 to S. There are two steps when we continue:

1. Continue with spoly(f, r_1). Since deg$(r_1) < \deg(f)$ the argument from above applies and we obtain the remainder r_2 (up to units) that occurs in the euclidean algorithm: $f = q_2r_1 + r_2$. Add r_2 to S.
2. Continue with spoly(g, r_1). Again this gives us the same remainder (up to units) that occurs when we perform the second step of the euclidean algorithm with the "wrong pair" namely (g, r_1). We already have the remainder of the division with remainder of (f, r_1), also we can express g via f and r_1 (from above), and have (in the first step) added r_2 to S, this new step with (g, r_1) will not give us a new element for S. We repeat this procedure until the Groebner basis algorithm terminates. Since the polynomial we add to S in each step is (up to units) one of the remainders form the euclidean algorithm, both algorithms will terminate at the same time. $\square$

b) W.l.og. all linear polynomials $f_1, \ldots, f_k$ have a non-zero coefficient at x_1. (We can assume this, since by renumbering we can assume that f_1 has a nonzero coefficient at x_1 and adding f_1 to all other f_i does not change the ideal we are considering to obtain the Groebner basis, nor does adding the first row of the matrix to all other rows change the outcome for the Gaussian algorithm.)
For all elements in the set of pairs (f_i, f_j) we have that spoly(f_i, f_j) is not divisible by $\mathsf{LM}(f_i) = x_1 = \mathsf{LM}(f_j)$ since spoly cancelled the leading term, i.e. spoly starts with x_a, $a > 1$. By Knowing that the f_i all have the same leading monomial we know that all the spoly(f_i, f_j) are linear.
Now for the first pair we pick in the set of pairs, the indeterminate division of spoly(f_i, f_j) with $S = \{f_1, \ldots, f_k\}$ will have remainder spoly(f_i, f_j), since the leading monomial for all $f_i \in S$ at this point is x_1 while spoly starts with x_a, $a > 1$. So we add this (w.l.o.g. spoly(f_1, f_2)) to S. Considering the coefficient to x_j in f_i as the (i, j)-th entry of the matrix, this means in terms of the Gauss algorithm that we add the coefficients to spoly(f_1, f_2) into an additional $k + 1$-th row.
While we continue to follow the algorithm, it is important to notice, that because we use the degree lexicographic ordering, the remainder of the ID(spoly(f_i, f_j), S) in every step (so even when i or $j \notin \{1, ..., k\}$) is linear!
All in all, adding the remainders by ID to S means adding a row which consists of "i-th row - $\frac{\mathsf{LC}(f_i)}{\mathsf{LC}(f_j)} \cdot$ j-th row" as we would expect from Gauss.
In the end we obtain a much too large matrix which (after possibly renumbering the rows) is in row echelon form. The rows consist of $f_1, \ldots, f_k$ and all the added remainders which start with x_a, $a > 1$ and by the renumbering of the row, we ordered these polynomials in sets which start with a pivot at the same entry, i.e., have the the same leading monomial.
We can now reduce our Groebner basis, by keeping one polynomial per leading monomial and deleting the others from S. This corresponds to keeping one row for each pivot-column-entry and deleting those with the pivot at the same column position. The next step of the reduced Groebner basis algorithm is to apply Buchberger RedID which corresponds in the Gaussian algorithm to ensure that in each pivot-column the entries above the pivot are zero. The last step of the reduced Groebner basis algorithm is to standardise the leading coefficients of the polynomials in S to 1, which is the same as multiplying the matrix with a diagonal matrix to ensure that all pivot entries are 1. $\square$