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

Wintersemester 2020/2021
16. December 2020

Introduction to Commutative Algebra and Algebraic Geometry
Solution to Exercise Sheet 6

Exercise 1 (*Product criterion*).
Let K be a field, $>$ be a monomial order, $f, g \in K[\underline{x}]$, $\gcd(\mathsf{LM}(f), \mathsf{LM}(g)) = 1$.
Show that there is a polynomials division with remainder of $\mathsf{spoly}(f, g)$ by (f, g) with remainder 0.

Hint: Show first that spoly$(f, g) = a_0 f + b_0 g$ for $a_0 = -tail(g)$ and $b_0 = tail(f)$ and then define recursively $a_i = tail(a_{i-1})$ and $b_i = tail(b_{i-1})$. Consider the maximal value N such that $u \cdot spoly(f, g) = a_N f + b_N g$ for some element $u \in K[\underline{x}]^*$ and distinguish the two cases that LT$(a_N f)$+LT$(b_N g)$ vanishes respectively does not vanish.

Proof: We want to show: $\exists u \in K[\underline{x}]^*, q_1, q_2 \in K[\underline{x}]$ such that $u\mathsf{spoly}(f, g) = q_1 f + q_2 g + 0$ satisfies ID1 ($\mathsf{LM}(\mathsf{spoly}(f, g)) \geq \mathsf{LM}(q_1 f), \mathsf{LM}(q_2 g)$) and ID2 (always satisfied for $r = 0$).
We show the statement from the hint first:

$$\begin{aligned}\mathsf{spoly}(f, g) &= \frac{\mathsf{LT}(g)}{gcd(\mathsf{LM}(f), \mathsf{LM}(g))} \cdot f - \frac{\mathsf{LT}(f)}{gcd(\mathsf{LM}(f), \mathsf{LM}(g)} \cdot g \\ &= \mathsf{LT}(g) \cdot f - \mathsf{LT}(f) \cdot g\end{aligned}$$

because $\gcd(\mathsf{LM}(f), \mathsf{LM}(g)) = 1$. It is $f = \mathsf{LT}(f) + \mathsf{tail}(f), g = \mathsf{LT}(g) + \mathsf{tail}(g)$ so we can set

$$\begin{aligned}\mathsf{spoly}(f, g) &= \mathsf{LT}(g) \cdot f - \mathsf{LT}(f) \cdot g \\ &= (g - \mathsf{tail}(g)) \cdot f - (f - \mathsf{tail}(f)) \cdot g \\ &= gf - fg + (-\mathsf{tail}(g))f + (\mathsf{tail}(f))g \\ &= (-\mathsf{tail}(g))f + (\mathsf{tail}(f))g \end{aligned} \tag{1}$$

Set $a_0 = -\mathsf{tail}(g)$, $b_0 = \mathsf{tail}(f)$. Now we define recursively $a_i = \mathsf{tail}(a_{i-1})$, $b_i = \mathsf{tail}(b_{i-1})$.
Set $N := \max\{\text{no. of terms occuring in } f, \text{ no. of terms occuring in } g\}$, then $a_N = b_N = 0$.
Choose $\nu \in \{0, \ldots, N\}$ maximal such that $\exists u \in K[\underline{x}]^* : \ u \cdot \mathsf{spoly}(f, g) = a_\nu f + b_\nu g$. Such a ν exists because of 1.
It remains to show that this satisfies ID1. We distinguish the cases that $\mathsf{LT}(a_\nu f) + \mathsf{LT}(b_\nu g)$ vanishes respectively does not vanish.
1.case: $\mathsf{LT}(a_\nu f) + \mathsf{LT}(b_\nu g) \neq 0$.
$\Rightarrow$ $\mathsf{LM}(u \cdot \mathsf{spoly}(f, g)) = \max\{\mathsf{LM}(a_\nu f), \mathsf{LM}(b_\nu g)\}$.
$\Rightarrow$ $u \cdot \mathsf{spoly}(f, g) = a_\nu f + b_\nu g$ satisfies ID1.
2.case: $\mathsf{LT}(a_\nu f) + \mathsf{LT}(b_\nu g) = 0$.
Since $\mathsf{LC}(f), \mathsf{LC}(g), \mathsf{LC}(a_\nu), \mathsf{LC}(b_\nu) \neq 0$ the above applies that

$$\mathsf{LT}(a_\nu) \cdot \mathsf{LT}(f) = -\mathsf{LT}(b_\nu) \cdot \mathsf{LT}(g)$$

Since $\gcd(\mathsf{LM}(f), \mathsf{LM}(g)) = 1$ and $\mathsf{LT}(f)$ divides the left hand side it also has to divide the right hand side, so there exists a term T such that $\mathsf{LT}(a_\nu) = T \cdot \mathsf{LT}(g)$ and $\mathsf{LT}(b_\nu) = -T \cdot \mathsf{LT}(f)$.

$$\begin{aligned}\Rightarrow\ (u - T) \cdot \mathsf{spoly}(f, g) &= a_\nu f + b_\nu g - T(\mathsf{LT}(g) \cdot f - \mathsf{LT}(f) \cdot g) \\ &= a_\nu f + b_\nu g - \mathsf{LT}(a_\nu) \cdot f - \mathsf{LT}(b_\nu) \cdot g) \\ &= a_{\nu+1} f + b_{\nu+1} g\end{aligned}$$

By the maximality of ν it follows that either $\nu = N$ or $u - T \notin K[\underline{x}]^*$.

- If $\nu = N$ it follows that: $\exists u \in K[\underline{x}]^* : u \cdot \mathsf{spoly}(f, g) = 0 \cdot f + 0 \cdot g + 0$
  $\Rightarrow$ $\mathsf{spoly}(f, g) = 0$ itself and this satisfies ID1.

- If $u - T \notin K[\underline{x}]^*$: Since $u \in K[\underline{x}]^*$ we have $T \neq 0$.
  $\Rightarrow$ $\mathsf{LT}(a_\nu) = T \cdot \mathsf{LT}(g) = \mathsf{LT}(T \cdot g)$ **Contradiction**, since $a_\nu = \mathsf{tail}(\mathsf{tail}(\ldots(\mathsf{tail}(g))))$.

Introduction to Commutative Algebra and Algebraic Geometry
Solution to Exercise Sheet 6

□

Exercise 2.
The degree lexicographical ordering $>_{Dp}$ on Mon_n is defined by

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

A polynomial $f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \underline{x}^\alpha \in K[x_1, \dots, x_n]$ is called *homogeneous* if for all α with $a_\alpha \neq 0$ the absolute value $|\alpha|$ is constant.
Show that a monomial ordering $>$ on Mon_n equals $>_{Dp}$ if and only if $>$ is a degree ordering and for any homogeneous $f \in K[\underline{x}]$ with $\mathsf{LM}(f) \in K[x_k, \dots, x_n]$ we have $f \in K[x_k, \dots x_n], k = 1, \dots, n$.

Proof: „$\Rightarrow$": Dp is a degree ordering by definition. Let $f \in K[\underline{x}]$ a homogeneous polynomial with $\mathsf{LM}(f) \in K[x_k, \dots, x_n]$ for some k.
Assume there exists a monomial $\underline{x}^\gamma$ in f such that $\underline{x}^\gamma \notin K[x_k, \dots, x_n]$. Write $\underline{x}^\alpha = \mathsf{LM}(f)$. Since f is homogeneous $\Rightarrow |\alpha| = |\gamma|$. But $\exists\, k' < k : \gamma_{k'} > (\alpha)_{k'} = 0$. This implies $\underline{x}^\gamma > \underline{x}^\alpha = \mathsf{LM}(f)$ Contradiction!
„$\Leftarrow$": Suppose for the monomial ordering $>$ satisfies $\underline{x}^\alpha > \underline{x}^\beta$ and $\underline{x}^\alpha <_{Dp} \underline{x}^\beta$ for $\underline{x}^\alpha \neq \underline{x}^\beta$.
Since both $>$ and $>_{Dp}$ are degree orderings, this implies that $|\alpha| = |\beta|$. Therefore, there exists k such that $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}, \alpha_k < \beta_k$. We can conclude that $k \neq n$ since for $k = n$ we would know that $|\alpha| = |\beta|$ and $\alpha_1 = \beta_1, \dots, \alpha_{n-1} = \beta_{n-1}$ which would also imply $\alpha_n = \beta_n$ and thus $\underline{x}^\alpha = \underline{x}^\beta$, contradiction.
Define

$$\begin{aligned}
\tilde{\alpha} &:= (0, \dots, 0, \alpha_{k+1}, \dots, \alpha_n) \\
\tilde{\beta} &:= (0, \dots, 0, \beta_k - \alpha_k, \beta_{k+1}, \dots, \beta_n) \\
\gamma &:= (\alpha_1, \dots, \alpha_k, 0, \dots, 0)
\end{aligned}$$

Then we know:

$$\underline{x}^{\tilde{\alpha}} \cdot \underline{x}^\gamma = \underline{x}^\alpha \underset{<_{Dp}}{>} \underline{x}^\beta = \underline{x}^{\tilde{\beta}} \cdot \underline{x}^\gamma \Rightarrow \underline{x}^{\tilde{\alpha}} \underset{<_{Dp}}{>} \underline{x}^{\tilde{\beta}}$$

Define now $f = \underline{x}^{\tilde{\alpha}} + \underline{x}^{\tilde{\beta}}$. Then f is homogeneous, since $|\tilde{\alpha}| = |\alpha| - |\gamma| = |\beta| - |\gamma| = |\tilde{\beta}|$. And f satisfies $\mathsf{LM}^>(f) = \underline{x}^{\tilde{\alpha}} \in K[x_{k+1}, \dots, x_n]$ but $f \notin K[x_{k+1}, \dots, x_n]$.This contradicts the prerequisite. □

Exercise 3.
Apply IDBuchberger to the following triple $(g, G, >)$:

$$g = x^4 + y^4 + z^4 + xyz,\ G = \{\partial g/\partial x, \partial g/\partial y, \partial g/\partial z\},\ >_{dp}.$$

Solution: Set $r_0 := g,\ f_1 := \partial g/\partial x = 4x^3 + yz,\ f_2 := \partial g/\partial y = 4y^3 + xz,\ f_3 := \partial g/\partial z = 4z^3 + xy.$
1. Step: $\mathsf{LM}(f_1) = x^3 | x^4 = \mathsf{LM}(r_0)$.
Set $q_1 := \frac{\mathsf{LT}(r_0)}{\mathsf{LT}(f_1)} = \frac{1}{4}x$ and

Introduction to Commutative Algebra and Algebraic Geometry
Solution to Exercise Sheet 6

$$
\begin{aligned}
r_1 &= \frac{\mathsf{spoly}(r_0, f_1)}{\mathsf{LC}(f_1)} = \frac{1}{\mathsf{LC}(f_1)} \cdot (\mathsf{LC}(f_1) \cdot \frac{lcm(\mathsf{LM}(r_0), \mathsf{LM}(f_1))}{\mathsf{LM}(r_0)} \cdot r_0 - \mathsf{LC}(r_0) \cdot \frac{lcm(\mathsf{LM}(r_0), \mathsf{LM}(f_1))}{\mathsf{LM}(f_1)} \cdot f_1) \\
&= \frac{1}{\mathsf{LC}(f_1)} \cdot (\frac{\mathsf{LT}(f_1)}{gcd(\mathsf{LM}(r_0), \mathsf{LM}(f_1))} \cdot r_0 - \frac{\mathsf{LT}(r_0)}{gcd(\mathsf{LM}(r_0), \mathsf{LM}(f_1))} \cdot f_1) \\
&= \frac{1}{4} \cdot (\frac{4x^3}{x^3} \cdot (x^4 + y^4 + z^4 + xyz) - \frac{x^4}{x^3} \cdot (4x^3 + yz) = \\
&= \frac{1}{4} \cdot (4(x^4 + y^4 + z^4 + xyz) - x \cdot (4x^3 + yz)) \\
&= \frac{1}{4} \cdot (4(y^4 + z^4 + xyz) - xyz) \\
&= y^4 + z^4 + \frac{3}{4}xyz
\end{aligned}
$$

2. Step: $\mathsf{LM}(f_2) = y^3 | y^4 = \mathsf{LM}(r_1)$.
Set $q_2 = \frac{\mathsf{LT}(r_1)}{\mathsf{LT}(f_2)} = \frac{1}{4}y$ and

$$
\begin{aligned}
r_2 &= \frac{\mathsf{spoly}(r_1, f_2)}{\mathsf{LC}(f_2)} \\
&= \frac{1}{4} \cdot (\frac{4y^3}{gcd(y^4, y^3)} \cdot r_1 - \frac{y^4}{gcd(y^4, y^3)} \cdot f_2) \\
&= r_1 - y \cdot \frac{f_2}{4} \\
&= z^4 + \frac{1}{2}xyz
\end{aligned}
$$

3. Step: $\mathsf{LM}(f_3) = z^3 | z^4 = \mathsf{LM}(r_2)$
Set $q_3 = \frac{\mathsf{LT}(r_2)}{\mathsf{LT}(f_3)} = \frac{1}{4}z$ and

$$
\begin{aligned}
r_3 &= \frac{\mathsf{spoly}(r_2, f_3)}{\mathsf{LC}(f_3)} \\
&= \frac{1}{4} \cdot (\frac{4z^3}{z^3} \cdot r_2 - \frac{z^4}{z^3} \cdot f_3) \\
&= \frac{1}{4} \cdot (4(z^4 + \frac{1}{2}xyz) - z \cdot (4z^3 + xy)) \\
&= \frac{1}{4}xyz
\end{aligned}
$$

4. Step: There remains no f_i with $\mathsf{LM}(f_i)|\mathsf{LM}(r_3)$, so the algorithm terminates and we obtain:

$$
\begin{aligned}
q_1 f_1 + q_2 f_2 + q_3 f_3 + r_3 &= \frac{1}{4}x(4x^3 + yz) + \frac{1}{4}y(4y^3 + xz) + \frac{1}{4}z(4z^3 + xy) + \frac{1}{4}xyz \\
&= x^4 + y^4 + z^4 + xyz \\
&= g
\end{aligned}
$$

□