MAS400: Solutions 3

Throughout this sheet F will denote an arbitrary field unless otherwise stated.

1. Perform multivariate division in $F[x, y]$ for the following cases. For critical cases, one may assume that $F = \mathbb{Q}$. Do them also with f_1 and f_2 interchanged, and for the monomial orders $\leqslant_{\text{lex}}$ and $\leqslant_{\text{grlex}}$ in which $x > y$. (You can also see what happens if $x < y$ if you like.)

   (a) $f = xy^3 - xy^2$, $f_1 = xy - x$, $f_2 = y^3$.

   (b) $f = x^2 + xy^3$, $f_1 = xy + 1$, $f_2 = y^2$.

   This working shows what you should have at each stage of the algorithm. Note that just one of q_1, q_2, r changes at each step, and then only by a term; p also changes at each step, but more then one term may be altered. The final line of table gives the output. In this working (but not in the question) all polynomials have been arranged so that the orders of their terms respect the monomial order in force, with the largest term being first. The leading coefficients of f_1 and f_2 are always 1, so this working applies in all fields.

   Mv-Div: $\leqslant_{\text{lex}}$, $\leqslant_{\text{grlex}}$ $(x > y)$; $f = xy^3 - xy^2$, $f_1 = xy - x$, $f_2 = y^3$.

Step	p	q_1	q_2	r
0 (initial)	$xy^3 - xy^2$	0	0	0
1 (final)	0	y^2	0	0

   Mv-Div: $\leqslant_{\text{lex}}$, $\leqslant_{\text{grlex}}$ $(x > y)$; $f = xy^3 - xy^2$, $f_1 = y^3$, $f_2 = xy - x$.

Step	p	q_1	q_2	r
0 (initial)	$xy^3 - xy^2$	0	0	0
1	$-xy^2$	x	0	0
2	$-xy$	x	$-y$	0
3	$-x$	x	$-y-1$	0
4 (final)	0	x	$-y-1$	$-x$

   Mv-Div: $\leqslant_{\text{lex}}$ $(x > y)$; $f = x^2 + xy^3$, $f_1 = xy + 1$, $f_2 = y^2$.

Step	p	q_1	q_2	r
0 (initial)	$x^2 + xy^3$	0	0	0
1	xy^3	0	0	x^2
2	$-y^2$	y^2	0	x^2
3 (final)	0	y^2	-1	x^2

Mv-Div: $\leqslant_{\text{lex}}$ $(x > y)$; $f = x^2 + xy^3$, $f_1 = y^2$, $f_2 = xy + 1$.

Step	p	q_1	q_2	r
0 (initial)	$x^2 + xy^3$	0	0	0
1	xy^3	0	0	x^2
2 (final)	0	xy	0	x^2

Mv-Div: $\leqslant_{\text{grlex}}$ $(x > y)$; $f = xy^3 + x^2$, $f_1 = xy + 1$, $f_2 = y^2$.

Step	p	q_1	q_2	r
0 (initial)	$xy^3 + x^2$	0	0	0
1	$x^2 - y^2$	y^2	0	0
2	x^2	y^2	-1	0
3 (final)	0	y^2	-1	x^2

Mv-Div: $\leqslant_{\text{grlex}}$ $(x > y)$; $f = xy^3 + x^2$, $f_1 = y^2$, $f_2 = xy + 1$.

Step	p	q_1	q_2	r
0 (initial)	$xy^3 + x^2$	0	0	0
1	x^2	xy	0	0
2 (final)	0	xy	0	x^2

2. Perform multivariate division in $F[x]$ when $f \in \{x^4, x^4 - 1\}$, $f_1 = x^3 + 1$, $f_2 = x^2 + 1$, and also with f_1 and f_2 interchanged. Note that there is a unique monomial order in this case. Although $F[x]$ is univariate, we cannot use univariate division as we are trying to simultaneously divide by two polynomials. What is the ideal $I = \langle f_1, f_2 \rangle$ anyway?

   The multivariate division proceeds in the same manner, regardless of field. We shall let $f = x^4 + \lambda$, where λ is an arbitrary element of F.
   Mv-Div: $f = x^4 + \lambda$, $f_1 = x^3 + 1$, $f_2 = x^2 + 1$.

Step	p	q_1	q_2	r
0 (initial)	$x^4 + \lambda$	0	0	0
1	$-x + \lambda$	x	0	0
2	λ	x	0	$-x$
3 (final)	0	x	0	$-x + \lambda$

Mv-Div: $f = x^4 + \lambda$, $f_1 = x^2 + 1$, $f_2 = x^3 + 1$.

Step	p	q_1	q_2	r
0 (initial)	$x^4 + \lambda$	0	0	0
1	$-x^2 + \lambda$	x^2	0	0
2	$1 + \lambda$	$x^2 - 1$	0	0
3 (final)	0	$x^2 - 1$	0	$1 + \lambda$

If $2 \neq 0$ (the general case) then $1 = \frac{x+1}{2} f_1 + \frac{-x^2-x+1}{2} f_2 \in I$, and so $I = F[x]$. If $\operatorname{char} F = 2$ (that is $2 = 0$), for example when $F = \mathbb{F}_2$, then $x+1 \mid f_1$ and $x+1 \mid f_2$ giving $I \leqslant \langle x+1 \rangle$. On the other hand we have $x - 1 = x + 1 = f_1 + x f_2 \in I$ so that $I = \langle x+1 \rangle$. One obtains the ideal generators using the Euclidean Algorithm. In this case multivariate division is useless for membership testing in I.

3. Let $I = \langle \underline{x}^{\alpha_1}, \underline{x}^{\alpha_2}, \ldots, \underline{x}^{\alpha_s} \rangle$ be a (finitely generated) monomial ideal of $F[x_1, \ldots, x_n]$, and $f \in F[x_1, \ldots, x_n]$. Show that if we apply multivariate division to divide f by $(\underline{x}^{\alpha_1}, \underline{x}^{\alpha_2}, \ldots, \underline{x}^{\alpha_s})$ then we get remainder $r = 0$ if and only if $f \in I$ (regardless of the fixed monomial order used).

Let $f = \sum_{\alpha \in A} a_\alpha \underline{x}^\alpha$, where $a_\alpha \in F \setminus \{0\}$ for all $\alpha \in A$. Suppose that $f \in I$. By Lemma E of notes $a_\alpha \underline{x}^\alpha \in I$ for all $\alpha \in A$, and by Lemma D of notes get, for all $\alpha \in A$, $\underline{x}^{\alpha_i} \mid \underline{x}^\alpha$ for some $i = i(\alpha)$ depending on α. (This implication obviously reverses.)

Now if $f \notin I$ then multivariate division by the $f_i = \underline{x}^{\alpha_i}$ gives a nonzero remainder, so we now consider what happens when $f \in I$. Referring to notation from `MultivariateDivision` throughout we claim that the terms of p are always a subset of the terms of f (this would not be true in general). Also, the else part of while-loop is never invoked; therefore r remains 0 throughout. Certainly these are both true on entry to the while-loop, so suppose they both hold before an application of the loop (note that we would apply the loop again only when $p \neq 0$). Let $a_\alpha \underline{x}^\alpha = \operatorname{lt}(p)$. Since $a_\alpha \underline{x}^\alpha$ is a term of f there exists i such that $f_i = \underline{x}^{\alpha_i} \mid a_\alpha \underline{x}^\alpha$. Now when $t = \operatorname{lt}(p)/\operatorname{lt}(f_i)$ (as per algorithm) we obtain $t f_i = t \operatorname{lt}(f_i) = \operatorname{lt}(p)$, so the new p is a sum of terms of f (with one fewer terms than the old p). The else part of the while-loop was not invoked so r remains 0. Therefore $r = 0$ on exiting the while-loop, and we are done.