Chapter 2 §3. A Division Algorithm in $k[x_1, \ldots, x_n]$. Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$ and let $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. *Dividing f by $(f_1, \ldots, f_s)$ with respect to $>$ produces an expression*

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r, \quad \text{where } a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n] \tag{2.3.0.1}$$

It is also true that no term in the remainder r is a multiple of the leading term in f_i for some i, $1 \leq i \leq s$. Here is an outline of the division algorithm: There are $s+2$ registers. These $s+2$ registers contain (i) the dividend, D, (ii) the remainder, r, and the s quotient registers, $a_1, \ldots, a_s$. Each of the dividend, remainder, and quotient registers holds an element of $k[x_1, \ldots, x_n]$ written as a sum of monomials written in descending monomial order.

Initial Settings. To start with the dividend is f, and the remainder and each of the quotient registers is set to zero.

The Step.

Part I: Check whether the dividend is zero. If so STOP! Otherwise go on to Part II.

Part II: Find the smallest value of i, $1 \leq i \leq s$ (if any) for which the leading term of the dividend D is a monomial multiple λx^α of the leading term of the divisor f_i, then (a) replace D by $D - \lambda x^\alpha \cdot f_i$, and (b) add λx^α to quotient register a_i. If there is no such i, subtract the leading term of the dividend from the dividend and add it to the remainder.

The division algorithm then is

Put initial settings in registers
Repeat the step until dividend = zero.

The algorithm will terminate because a monomial order on $k[x_1, \ldots, x_n]$ is a well ordering, and when it terminates (2.3.0.1) will hold. Furthermore, it is never true that a term in the remainder r is a multiple of the leading term of one of the divisors, because only when it is not a multiple of the leading term of one of the divisors is a dividend term placed in the remainder.

Some Remarks: Dividing f by $(f_1, \ldots, f_s)$ with respect to the monomial order $>$ yields a unique expression of the form

$$f = a_1 f_1 + \cdots + a_s f_s + r, \qquad \text{where multidegree}(r) < \text{multidegree}(f_i),\ 1 \leq i \leq s,$$

but the quotients a_i and the remainder r will in general depend on the order of the divisors to say nothing of depending on the monomial order $>$. For example, let $f = xy^2 - x$, $f_1 = xy + 1$ and $f_2 = y^2 - 1$. Using lex order, dividing f by (f_1, f_2) yields

$$xy^2 - x = y(xy + 1) + (-x - y),$$

while dividing f by (f_2, f_1) yields

$$xy^2 - x = x(y^2 - 1) + 0.$$

The fact that the remainder vanishes is sufficient but not necessary to insure that f is in the ideal$\langle f_1, f_2 \rangle$. We must look for a better "basis" to describe this ideal if we want the division algorithm to yield a solution to ideal membership.

---

§2.3.1.

Compute the remainder on division of the given polynomial f by the order set F (by hand). Use the grlex order, then the lex order in each case.

(a) $f = x^7y^2 + x^3y^2 - y + 1$, $F = (xy^2 - x, x - y^3)$.

We will do this in the form of a table keeping track of the dividend during the course of the division. There will be columns for the successive contributions to each quotient, headed by the associated divisor, a column for the successive dividends and a column for the successive contributions to the remainder.

First using grlex order,

$xy^2 - x$	$-y^3 + x$	$x^7y^2 + x^3y^2 - y + 1$	remainder
x^6		$x^7 + x^3y^2 - y + 1$	
		$x^3y^2 - y + 1$	x^7
x^2		$x^3 - y + 1$	
		$-y + 1$	x^3
		$+1$	$-y$
			$+1$

gives

$$x^7y^2 + x^3y^2 - y + 1 = (x^6 + x^2)(xy^2 - x) + (x^7 + x^3 - y + 1)$$

Mathematica 3.01. The command

PolynomialReduce[xˆ7*yˆ2+xˆ3*yˆ2-y+1, {x*yˆ2-x,y-yˆ3},{x,y},
MonomialOrder->DegreeLexicographic]

Produces the output

$$\text{Out[1]} = \{\{x^2 + x^6,\, 0\},\, 1 + x^3 + x^7 - y\}$$

Then using lex order,

$xy^2 - x$	$x - y^3$	$x^7y^2 + x^3y^2 - y + 1$	remainder
x^6		$x^7 + x^3y^2 - y + 1$	
	x^6	$+x^6y^3 + x^3y^2 - y + 1$	
x^5y		$+x^6y + x^3y^2 - y + 1$	
	x^5y	$+x^5y^4 + x^3y^2 - y + 1$	
x^4y^2		$+x^5y^2 + x^3y^2 - y + 1$	
x^4		$x^5 + x^3y^2 - y + 1$	
	x^4	$x^4y^3 + x^3y^2 - y + 1$	
x^3y		$+x^4y + x^3y^2 - y + 1$	
	x^3y	$+x^3y^4 + x^3y^2 - y + 1$	
x^2y^2		$+2x^3y^2 - y + 1$	
$2x^2$		$+2x^3 - y + 1$	
	$2x^2$	$+2x^2y^3 - y + 1$	
$2xy$		$2x^2y - y + 1$	
	$2xy$	$2xy^4 - y + 1$	
$2y^2$		$2xy^2 - y + 1$	
2		$2x - y + 1$	
	2	$2y^3 - y + 1$	

gives

$$\begin{aligned} x^7y^2 + x^3y^2 - y + 1 = {} & (x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + 2)(xy^2 - x) \\ & + (x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2)(x - y^3) + (2y^3 - y + 1) \end{aligned}$$

which is correct.

Mathematica 3.01. The command

PolynomialReduce[x^7*y^2+x^3*y^2-y+1, {x*y^2-x,y-y^3},{x,y},
MonomialOrder->Lexicographic]

Produces the output

$$\begin{aligned}\text{Out[1]} = \{\{&2 + 2x^2 + x^4 + x^6 + 2xy + x^3y + x^5y + 2y^2 + x^2y^2 + x^4y^2,\\ &2 + 2x^2 + x^4 + x^6 + 2xy + x^3y + x^5y\},\ 1 - y + 2y^3\}\end{aligned}$$

Maple 4.0. Maple 4.0 will do something here too. Consider

```
> with(grobner);
```
$$[finduni, finite, gbasis, gsolve, leadmon, normalf, solvable, spoly]$$
```
> normalf(x^7*y^2+x^3*y^2-y+1, [x*y^2-x,y-y^3],[x,y],plex);
```
$$1 - y + y^{11} + y^{21}$$

Maple 4.0 is supposed to handle the lex order with plex. It doesn't handle the grlex order. The question arises: What is going on here? I suspect that the polynomial basis for the ideal has to be a Gröbner basis and that $xy^2 - x, x - y^3$ is not a Gröbner basis. To check this out use the Maple 4.0 command

```
> gbasis([x*y^2-x,x-y^3],[x,y],plex);
```
$$[x - y^3,\ y^5 - y^3]$$

Next let's use Mathematica 3.0.1 to see what the division algorithm would yield with $x - y^3, y^5 - y^3$ as the set of divisors. Answer: It yields $1 - y + 2y^3$ as remainder.

Finally, I ran the Maple 4.0 sequence

```
> with(grobner);
```
$$[finduni, finite, gbasis, gsolve, leadmon, normalf, solvable, spoly]$$
```
> normalf(x^7*y^2+x^3*y^2-y+1, [x-y^3,y^5-y^3],[x,y],plex);
```
$$1 - y + 2y^3$$

Thus it seems that Maple's normalf command can be relied upon only when the set of would be divisors is a Gröbner basis. To insure this it seems that the appropriate Maple 4.0 command is (after executing the with(grobner) command of course)

```
> normalf(x^7*y^2+x^3*y^2-y+1,gbasis([x-y^3,y^5-y^3],[x,y],plex),[x,y],plex);
```
$$1 - y + 2y^3$$

(b) (Part (b) of exercise 2.3.1.) Repeat part (a) with the order of the pair F reversed.

Solution. For the grlex order the mathematica output is

$$\{\{0, x^2 + x^6\}, 1 + x^3 + x^7 - y\};$$

so there is no change. For the lex order the mathematica output is

$$\{\{x^2\,y^2 + x^6\,y^2 + x\,y^5 + x^5\,y^5 + y^8 + x^4\,y^8 + x^3\,y^{11} + x^2\,y^{14} + x\,y^{17} + y^{20}, 0\}, 1 - y + y^{11} + y^{23}\}$$

which represents quite a change.

---

§**2.3.2.**

Compute the remainder on division:

(a.1) $g = x^2y^2z^2 + xy - yz \qquad F = (x - y^2, y - z^3, z^2 - 1).$

(a.2) $f = xy^2z^2 + xy - yz \qquad F = (x - y^2, y - z^3, z^2 - 1).$

(b) Repeat part (a) with the order of the set F permuted cyclically

Solution. Using Mathematica 3.0.1, the results for $(x^2y^2z^2 + xy - yz)/F$ for various F's and using grlex order are:

$$\{\{-\left(x^2\,z^2\right), 0, x^3\}, x^3 + x\,y - y\,z\} \qquad F = (x - y^2, y - z^3, z^2 - 1).$$
$$\{\{0, x^2\,y^2, -x^2\}, x^3 + x\,y - y\,z\} \qquad F = (y - z^3, z^2 - 1, x - y^2).$$
$$\{\{x^2\,y^2, -x^2, 0\}, x^3 + x\,y - y\,z\} \qquad F = (z^2 - 1, x - y^2, y - z^3).$$

Using the lex order the corresponding $(x^2y^2z^2 + xy - yz)/F$'s are:

$$\{\{y + x\,y^2\,z^2 + y^4\,z^2,$$
$$y^2 - z + y^5\,z^2 + y\,z^3 + y^4\,z^5 + z^6 + y^3\,z^8 + y^2\,z^{11} + y\,z^{14} + z^{17},$$
$$z + z^3 + z^4 + z^5 + z^6 + z^7 + z^8 + z^{10} + z^{12} + z^{14} + z^{16} + z^{18}\}, z\} \qquad F = (x - y^2, y - z^3, z^2 - 1).$$

$$\{\{x + y + x\,y - z + y\,z + x^2\,y\,z^2 + z^3 + x\,z^3 + z^4 + x^2\,z^5,$$
$$x + x^2 + z + x\,z + x\,z^2 + x^2\,z^2 + z^3 + z^4 + x\,z^4 + x^2\,z^4 + z^5 + x^2\,z^6,$$
$$1 + x + z\}, z\} \qquad F = (y - z^3, z^2 - 1, x - y^2).$$

$$\{\{y + y^2 + x^2\,y^2 + y^4 + z + y\,z + y^2\,z + y^3\,z + y^5\,z + y\,z^2 + y^2\,z^2 + y^4\,z^2,$$
$$y + x\,y^2 + y^4,$$
$$1 + y + y^2 + y^3 + y^5 + y\,z + y^2\,z + y^4\,z\}, z\} \qquad F = (z^2 - 1, x - y^2, y - z^3).$$

Using Mathematica 3.0.1, the results for $(xy^2z^2 + xy - yz)/F$ for various F's and using grlex order are:

$$\{\{-\left(x\,z^2\right), 0, x^2\}, x^2 + x\,y - y\,z\} \qquad F = (x - y^2, y - z^3, z^2 - 1).$$
$$\{\{0, x\,y^2, -x\}, x^2 + x\,y - y\,z\} \qquad F = (y - z^3, z^2 - 1, x - y^2).$$
$$\{\{x\,y^2, -x, 0\}, x^2 + x\,y - y\,z\} \qquad F = (z^2 - 1, x - y^2, y - z^3).$$

Using the lex order the corresponding $(xy^2z^2 + xy - yz)/F$'s are:

$$\{\{y + y^2\,z^2, y^2 - z + y^3\,z^2 + y\,z^3 + y^2\,z^5 + z^6 + y\,z^8 + z^{11},$$
$$z + z^3 + z^4 + z^5 + z^6 + z^7 + z^8 + z^{10} + z^{12}\}, z\} \qquad F = (x - y^2, y - z^3, z^2 - 1).$$

$$\{\{x + y - z + y\,z + x\,y\,z^2 + z^3 + z^4 + x\,z^5, x + z + x\,z + x\,z^2$$
$$+ z^3 + z^4 + x\,z^4 + z^5 + x\,z^6, 1 + z\}, z\} \qquad F = (y - z^3, z^2 - 1, x - y^2).$$

$$\{\{y + y^2 + x\,y^2 + z + y\,z + y^2\,z + y^3\,z + y\,z^2 + y^2\,z^2, y + y^2,$$
$$1 + y + y^2 + y^3 + y\,z + y^2\,z\}, z\} \qquad F = (z^2 - 1, x - y^2, y - z^3).$$

---

§**2.3.3.**

Using a computer algebra system, check your work from Exercises 1 and 2. (You may need to consult documentation to learn whether the system you are using has an explicit polynomial division command or you will need to perform the individual steps of the algorithm yourself.)

Solution. This was completed along with the exercises above.

---

§2.3.4.

If $f = a_1 f_1 + \cdots + a_s f_s + r$ is the output of the division algorithm, complete the proof begun in the text that multideg$(f) \geq$multideg$(a_i f_i)$ when $a_i f_i \neq 0$.

Solution. During the execution of the algorithm, it is only in Case I of "The Step" that any changes are made to the quotients. Namely, there λx^α is added to a_i provided that $\lambda x^\alpha \cdot f_i$ matches the leading term of the dividend D. Since it is always true that multideg$(D) \leq$multideg(f) this guarantees that the sum of the terms $\lambda x^\alpha \cdot f_i$ for i fixed can never have a multidegree greater than that of f.

---

§2.3.5.

We shall study the division of $f = x^3 - x^2y - x^2z + x$ by $f_1 = x^2y - z$ and $f_2 = xy - 1$. (a) Compute using grlex order:

$$\begin{aligned} r_1 &= \text{ remainder of } f \text{ on division by } (f_1, f_2). \\ r_2 &= \text{ remainder of } f \text{ on division by } (f_2, f_1). \end{aligned}$$

Your results should be *different*. Where in the division algorithm did the difference occur? (You may need to do a few steps by hand here.)

Solution.

$x^2y - z$	$xy - 1$	$x^3 - x^2y - x^2z + x$	remainder
		$-x^2y - x^2z + x$	x^3
-1		$-x^2z + x - z$	
		$+x - z$	$-x^2z$
		$-z$	$+x$
			$-z$

So

$$r_1 = x^3 - x^2z + x - z$$

and

$$x^3 - x^2y - x^2z + x = (-1)(x^2y - z) + r_1. \tag{2.3.5.1}$$

Changing the position of the divisors

$xy - 1$	$x^2y - z$	$x^3 - x^2y - x^2z + x$	remainder
		$-x^2y - x^2z + x$	x^3
$-x$		$-x^2z$	
			$-x^2z$

So

$$r_2 = x^3 - x^2z$$

and

$$x^3 - x^2y - x^2z + x = (-x)(xy - 1) + r_2. \tag{2.3.5.2}$$

I'm not sure what to answer here, but the first actual subtraction from the dividend removed two terms in the (f_2, f_1) order of divisors.

(b) Is $r = r_1 - r_2$ in the ideal $\langle f_1, f_2\rangle$? If so find an explicit expression $r = Af_1 + Bf_2$. If not, say why not.

Solution. Yes! $r = r_1 - r_2$ is in $\langle f_1, f_2\rangle$ in general. Subtracting (2.3.5.2) from (2.3.5.1) yields

$$0 = (-1)(x^2y - z) + x(xy - 1) + r_1 - r_2$$

or

$$r_1 - r_2 = x - z = (x^2y - z) - x(xy - 1).$$

This will work in general. If f divided by $F = (f_1, \ldots, f_s)$ gives remainder r_1 and f divided by $G = (f_{i_1}, \ldots, f_{i_s})$ yields remainder r_2 where $(i_1, \ldots, i_s)$ is a permutation of $(1, 2, \ldots, s)$, it is always true that $r_1 - r_2 \in \langle f_1, \ldots, f_s\rangle$.

(c) Compute the remainder of $r = x - z$ on division by (f_1, f_2). Why could you have predicted your answer before doing the division?

Solution. Since no term in r_i is a multiple of the leading term of f_1 or f_2, it follows that the remainder of r_i on division by (f_1, f_2) is r_i itself. The same holds for $r = r_1 - r_2$: Its remainder on division by (f_1, f_2) is, accordingly, r.

(d) Find another polynomial $g \in \langle f_1, f_2\rangle$ such that the remainder on division of g by (f_1, f_2) is nonzero. Hint: $(xy + 1) \cdot f_2 = x^2y^2 - 1$, whereas $y \cdot f_1 = x^2y^2 - yz$.

Solution. It follows from the hint that

$$yz - 1 = (-y) \cdot f_1 + (xy + 1) \cdot f_2 \in \langle f_1, f_2\rangle.$$

Since the leading term of $yz - 1$ is not a multiple of the leading term of either f_1 or f_2, when $g = yz - 1$ is divided by (f_1, f_2) the remainder is g itself or $yz - 1$ which is $\neq 0$.

Another Solution. We know that $r = x - z \in \langle f_1, f_2\rangle$. Multiplying this by y gives $xy - yz \in \langle f_1, f_2\rangle$. Dividing $xy - yz$ by (f_2, f_1) yields

$xy - 1$	$x^2y - z$	$xy - yz$	remainder
1		$-yz + 1$	
		1	$-yz$
			1

the remainder $-yz + 1$ which lies in $\langle f_1, f_2\rangle$ because of the relation

$$xy - yz = 1(xy - 1) + 0(x^2y - z) + (-yz + 1)$$

and the fact that $xy - yz \in \langle f_1, f_2\rangle$. (Of course $xy - yz = (xy - 1) + (-yz + 1)$ shows this last fact directly.)

(e) Does the division algorithm give us a solution for the ideal membership problem for the ideal $\langle f_1, f_2\rangle$? Explain your answer.

Solution. I beg off here for the moment! One thing that can be said:

$$\begin{aligned} x - z &= -x(xy - 1) + (x^2y - z); \\ yz - 1 &= (xy + 1)(xy - 1) - y(x^2y - z); \\ xy - 1 &= y(x - z) + (yz - 1); \\ x^2y - z &= (xy + 1)(x - z) + x(yz - 1). \end{aligned}$$

So $\langle x - z, yz - 1\rangle = \langle x^2y - z, xy - 1\rangle$ and the question arises: Can any element $(x - z) \cdot h_1 + (yz - 1) \cdot h_2 \in \langle x - z, yz - 1\rangle$ have a nonzero remainder when it is divided by $(x - z, yz - 1)$? I claim the answer is: No! The reason is that any such remainder must also have the form $(x - z) \cdot h_1 + (yz - 1) \cdot h_2$, but its leading term must have x degree zero; so h_1 is zero. Furthermore, its leading term cannot be a λx^α multiple of yz which implies that h_2 is also zero. We have a test for ideal membership: Divide f by $(x - z, yz - 1)$. If the remainder is zero $f \in \langle f_1, f_2\rangle$, if not, $f \notin \langle f_1, f_2\rangle$.

§**2.3.6.**

Using the grlex order, find an element g of $\langle f_1, f_2\rangle = \langle 2xy^2 - x, 3x^2y - y - 1\rangle \subset \mathbf{R}[x, y]$ whose remainder on division by (f_1, f_2) is non zero. Hint: You can find such a g where the remainder is g itself.

Solution. Use the technique of Exercise 2.5.ab. For example, take $f = 6x^2y^2$ and divide by (f_1, f_2) to get $r_1 = 3x^2$, viz.

$2xy^2 - x$	$3x^2y - y - 1$	$6x^2y^2$	remainder
$3x$		$3x^2$	
		1	$3x^2$

Then divide f by (f_2, f_1) to get remainder $r_2 = 2y^2 + 2y$, viz.

$3x^2y - y - 1$	$2xy^2 - x$	$6x^2y^2$	remainder
$2y$		$2y^2 + 2y$	
		1	$2y^2 + 2y$

The difference $r = r_1 - r_2 = 3x^2 - 2y^2 - 2y \in \langle f_1, f_2\rangle$; so the trick is to choose f so that this difference is not zero.

Alternatively, find an element g of $\langle f_1, f_2\rangle$ none of whose terms are "divisible" by the leading terms of f_1 or f_2. Viz.

$$3x^2 - 2y^2 - 2y = (-3x)(2xy^2 - x) + (2y)(3x^2y - y - 1) = -3x \cdot f_1 + 2y \cdot f_2.$$

This g will do the trick!

---

§**2.3.7.**

Answer the question of Exercise 6 for

$$\langle f_1, f_2, f_3\rangle = \langle x^4y^2 - z,\ x^3y^3 - 1,\ x^2y^4 - 2z\rangle \subset \mathbf{R}[x, y, z].$$

Find two polynomials g (not constant multiples of each other).

Solution. Take with $f_1 = x^4y^2 - z$, $f_2 = x^3y^3 - 1$, and $f_3 = x^2y^4 - 2z$,

$$g_1 = y \cdot f_1 - x \cdot f_2 = -yz + x;$$
$$g_2 = y \cdot f_2 - x \cdot f_3 = -y + 2xz.$$

---

§**2.3.8.**

Try to formulate a general pattern that fits the examples in Exercises 2.3.5cd, 2.3.6, and 2.3.7. What condition on the leading term of the polynomial $g = A_1f_1 + \cdots + A_sf_s$ would guarantee that there was a nonzero remainder on division by $(f_1, \ldots, f_s)$? What does your condition imply about the ideal membership problem?

Solution. If no term in g is a λx^α multiple of one of the leading terms $\mathrm{LT}(f_i)$, for some i, $1 \le i \le s$, then (i) g is in the ideal $\langle f_1, \ldots, f_s\rangle$ and (ii) when g is divided by $(f_1, \ldots, f_s)$ the remainder is g itself.

Requiring a little less, if the leading term in g is not a λx^α multiple of one of the leading terms $\mathrm{LT}(f_i)$, for some i, $1 \le i \le s$, then when g is divided by $(f_1, \ldots, f_s)$ the remainder is nonzero.

I'm still don't know what to say about the ideal membership problem. Clearly $f \in \langle f_1, \ldots, f_s\rangle$ if and only if the remainder when f is divided by $(f_1, \ldots, f_s)$ is $\in \langle f_1, \ldots, f_s\rangle$.

§**2.3.9.**

In the discussion around 1.4.2 it is shown that every polynomial $f \in \mathbf{R}[x, y, z]$ can be written as

$$f = h_1(y - x^2) + h_2(z - x^3) + r, \qquad h_1, h_2 \in \mathbf{R}[x, y, z],\ r \in \mathbf{R}[x].$$

The variety $\mathbf{V}(y - x^2, z - x^3)$ is the twisted cubic curve in $\mathbf{R}^3$.

(a) Give a proof of this fact using the division algorithm. Hint: You need to specify carefully the monomial ordering to be used.

Solution. If we divide f by $(y - x^2, z - x^3)$ using the lex order with $y > z > x$ we get an expression of the form

$$f = h_1(y - x^2) + h_2(z - x^3) + r, \text{ where } h_1, h_2, r \in \mathbf{R}[x, y, z]$$

and, in addition, the leading terms of $y - x^2$ and $z - x^3$ do not divide the leading term of r. This means r is not divisible by y or by z; so $r \in \mathbf{R}[x]$.

Remark. It seems that $\mathbf{R}$ could be any field here.

(b) Use the parametrization of the twisted cubic to show that $z^2 - x^4y$ vanishes at every point of the twisted cubic.

Solution. This parametrization is $t \mapsto (t, t^2, t^3)$; so we must check whether the point with these coordinates is a zero of the polynomial $z^2 - x^4y$. Substituting coordinates gives $(t^3)^2 - t^4 \cdot t^2$ which is always zero. The twisted cubic, $\mathbf{V}(y - x^2, z - x^3)$ lies on the (surface) variety $\mathbf{V}(z^2 - x^4y)$,

(c) Find an explicit representation

$$z^2 - x^4y = h_1(y - x^2) + h_2(z - x^3)$$

using the division algorithm.

Solution. Carrying out the division of $z^2 - x^4y$ by $(y - x^2, z - x^3)$ using lex order with $y > z > x$ we get

$y - x^2$	$z - x^3$	$-yx^4 + z^2$	remainder
$-x^4$		$z^2 - x^6$	
	z	$zx^3 - x^6$	
	x^3	0	

This gives

$$z^2 - x^4y = (-x^4)(y - x^2) + (z + z^3)(z - x^3).$$

---

§**2.3.10.**

Let $V \subset \mathbf{R}^3$ be the curve parametrized by (t, t^m, t^n), with $n, m \geq 2$.

(a) Show that V is an affine variety.

Solution. This means: Show that V is the set of zeros for some set of polynomials in $\mathbf{R}[x, y, z]$. Consider the set $(y - x^m, z - x^n)$. There is clearly a one-one correspondence between the zeros of $(y - x^m, z - x^n)$ and the points (t, t^m, t^n), $t \in \mathbf{R}$.

Remark: For this part of the exercise we could have n or m equal to 1.

(b) Adapt the ideas in Exercise 9 to determine $\mathbf{I}(V)$.

Solution. Suppose $f \in \mathbf{R}[x,y,z]$ vanishes on V, i.e. $f \in \mathbf{I}(V)$. Divide f by $(y-x^m, z-x^n)$ using lex order with $y > z > x$ to get

$$(*) \qquad f = h_1(y-x^m) + h_2(z-x^n) + r, \qquad h_1, h_2, r \in \mathbf{R}[x,y,z],$$

and where the leading term of r is not a λx^α multiple of either of the divisors. This means that $r \in \mathbf{R}[x]$ is a function of x alone. Supstituting the coordinates (t, t^m, t^n) into (*) gives $r(t) = 0$ for every choice of t. That is, r is zero. We have shown

$$\mathbf{I}(V) \subset \langle y-x^m, z-x^n \rangle.$$

The other inclusion is trivially true: Every $f = h_1(y-x^m) + h_2(z-x^n)$ vanishes on V, i.e. on the points (t, t^m, t^n).

Question: I still don't see why m and/or n can't be 1.

---

§2.3.11.

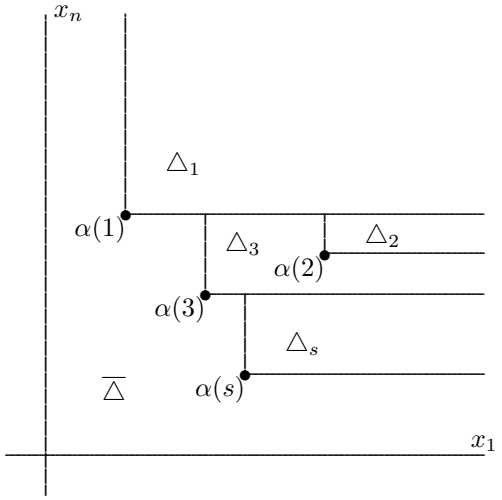
In this exercise, we will characterize completely the expression

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

that is produced by the division algorithm (among all the possible expressions for f of this form). Let $\mathrm{LM}(f_i) = x^{\alpha(i)}$ and define

$$\begin{aligned}
\triangle_1 &= \alpha(1) + \mathbf{Z}^n_{\geq 0}, \\
\triangle_2 &= [\alpha(2) + \mathbf{Z}^n_{\geq 0}] - \triangle_1, \\
&\vdots \\
\triangle_s &= [\alpha(s) + \mathbf{Z}^n_{\geq 0}] - \left(\bigcup_{i=1}^{s-1} \triangle_i \right), \\
\overline{\triangle} &= \mathbf{Z}^n_{\geq 0} - \left(\bigcup_{i=1}^{s} \triangle_i \right).
\end{aligned}$$

(Note that $\mathbf{Z}^n_{\geq 0}$ is the disjoint union of the $\triangle_i$ and $\overline{\triangle}$.)
The following diagram is an attempt to depict these regions:



(a) Show that $\beta \in \triangle_i$ if and only if $x^{\alpha(i)}$ divides x^β, but no $x^{\alpha(j)}$ with $j < i$ divides x^β.

Solution. The condition that $\beta \in \alpha(m) + \mathbf{Z}^n_{\geq 0}$ is precisely that $x^{\alpha(i)}$ divides x^β. The condition that $\beta \in \left(\bigcup_{m=1}^i \triangle_m\right)$ is thus that for some $j \leq i$, $x^{\alpha(j)}$ divides x^β. Using these interpretations it is easy to see that (a) is true.

(b) Show that $\gamma \in \overline{\triangle}$ if and only if no $x^{\alpha(j)}$ divides x^γ

Solution. Again this is clear from the interpretation of $\beta \in \alpha(m) + \mathbf{Z}^n_{\geq 0}$ given in the argument for part (a) above.

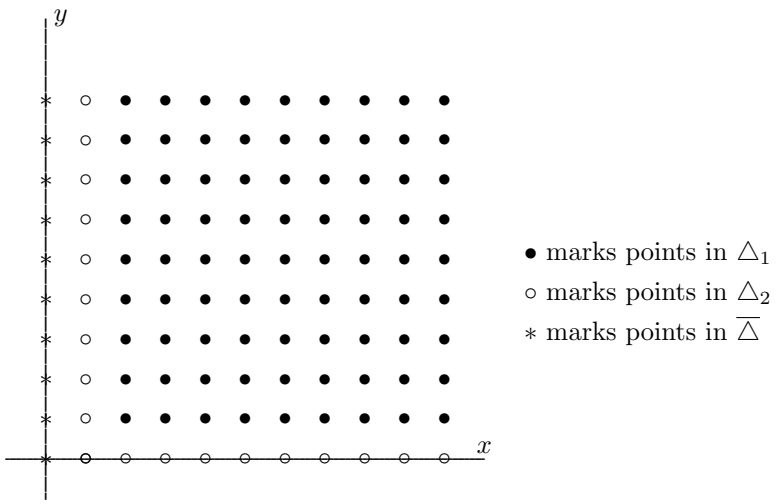
(c) Show that in the expression $f = a_1 f_1 + \cdots + a_s f_s + r$ computed by the division algorithm, for every i, every monomial x^β in a_i satisfies $\beta + \alpha(i) \in \triangle_i$, and every monomial x^γ in r satisfies $\gamma \in \overline{\triangle}$.

Solution. In order for a scalar multiple of x^β to appear in a_i it must be that some scalar multiple of $x^{\beta+\alpha(i)}$ is in the changing dividend, where $\beta + \alpha(i) \in \triangle_i$. In order for λx^γ to be a term in r for some $\lambda \in k$, it is necessary that $\gamma \in \overline{\triangle}$, because only then will λx^γ not be divisible by some leading monomial $x^{\alpha(i)}$.

(d) Show that there is exactly one expression $f = a_1 f_1 + \cdots + a_s f_s + r$ satisfying the properties given in (c).

Solution. Before we give the argument in general we illustrate a special case. Take $f_1 = x^2y - x$ and $f_2 = x - y^3$ and use lex order. Here $\alpha(1) = (2, 1)$ and $\alpha(2) = (1, 0)$.

This situation is illustrated below. $F = (x^2y - x, x - y^3)$ with lex order and $x > y > z$.



If there are two expressions $f = a_1 f_1 + a_2 f_2 + r$ matching the criteria in (d), we subtract one from the other getting an expression of the form

$$0 = A_1(x^2y - x) + A_2(x - y^3) + R, \tag{2.3.11.d}$$

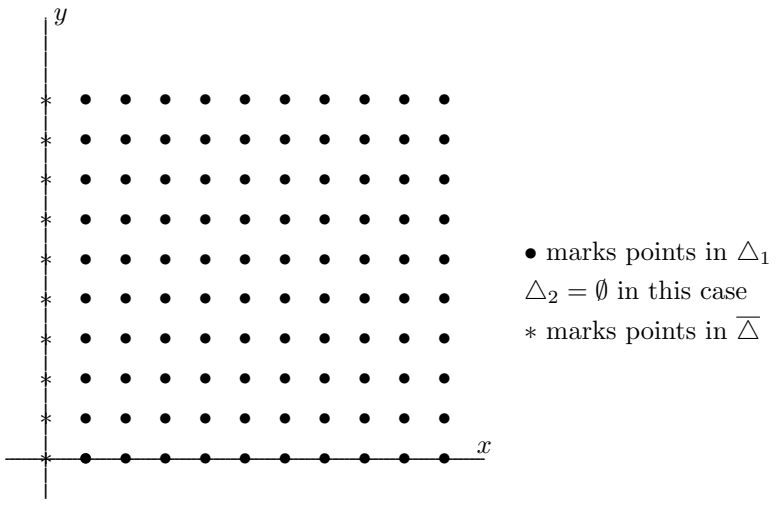
where (i) A_1 is a sum of terms $\lambda x^a y^b$ with $(2 + a, 1 + b) \in (2, 1) + \mathbf{Z}^2_{\geq 0}$ meaning in effect that a and b are non negative; (ii) A_2 is a sum of terms $\lambda x^c y^d$ with $(1 + c, d) \in \triangle_2$ which says that either $c = 0$ or $d = 0$; (iii) R is a sum of terms $\lambda x^g y^h$ with $(g, h) \in \overline{\triangle}$ meaning in effect that $g = 0$.

Claim: $A_1 = 0$. Suppose $\lambda x^a y^b$ is a term in A_1. Then $A_1(x^2y - x)$ contains the term $\lambda x^{2+a} y^{1+b}$ which falls in the $\triangle_1$ or • region in the above diagram. No term from R will ever cancel $\lambda x^{2+a} y^{1+b}$; so cancellation must come from a term in $A_2(x - y^3)$, but this too is impossible because no term in A_2 is a nonzero multiple of xy. The only possibility is that $\lambda = 0$ and by extension that A_1 is zero. Once we know that $A_1 = 0$ it is easy to see that $A_2 = 0$ (because R doesn't contain any terms in x) and then that $R = 0$.

Conclusion: Any relation of the form $f = a_1 f_1 + a_2 f_2 + r$ is necessarily unique. That at least one such equation exists follows from the division algorithm, since this algorithm produces such an equation.

It is interesting to see what happens when the order of the divisors is reversed. Take $f_1 = x - y^3$ and $f_2 = x^2 y - x$ and use lex order. Here $\alpha(1) = (1, 0)$ and $\alpha(2) = (2, 1)$.

This situation is different. $F = (x - y^3, x^2 y - x)$ with lex order and $x > y > z$.



As before if there are two expressions $f = a_1 f_1 + a_2 f_2 + r$ matching the criteria in (d), we subtract one from the other getting an expression of the form

(2.3.11.dd) $$0 = A_1(x - y^3) + A_2(x^2 y - x) + R,$$

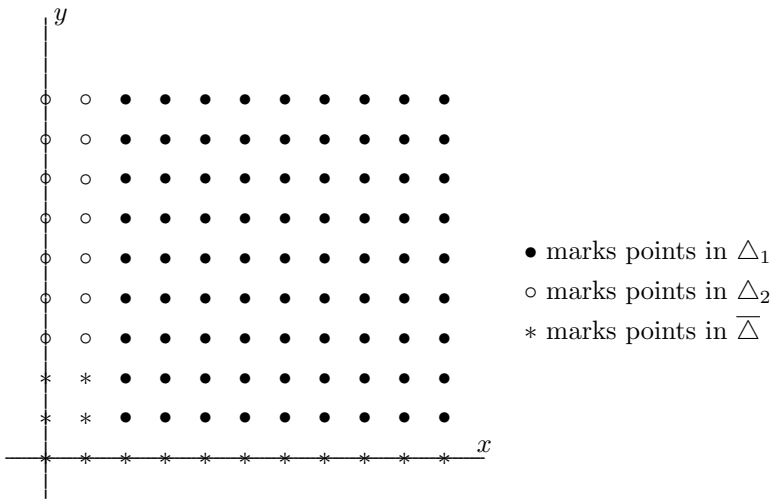
where this time (i) A_1 is a sum of terms $\lambda x^a y^b$ with $(1 + a, 0 + b) \in (1, 0) + \mathbf{Z}^2_{\geq 0}$ meaning in effect that a and b are non negative; (ii) A_2 is a sum of terms $\lambda x^c y^d$ with $(1 + c, d) \in \triangle_2 = \emptyset$ which says that $A_2 = 0$; (iii) R is a sum of terms $\lambda x^g y^h$ with $(g, h) \in \overline{\triangle}$, meaning in effect that $R \in \mathbf{R}[y]$.

In this case it is even easier to see that $A_1 = 0$ because otherwise the righthand side of (2.3.11.dd) would contain a term involving the variable x. $R = 0$ follows immediately and uniqueness is established.

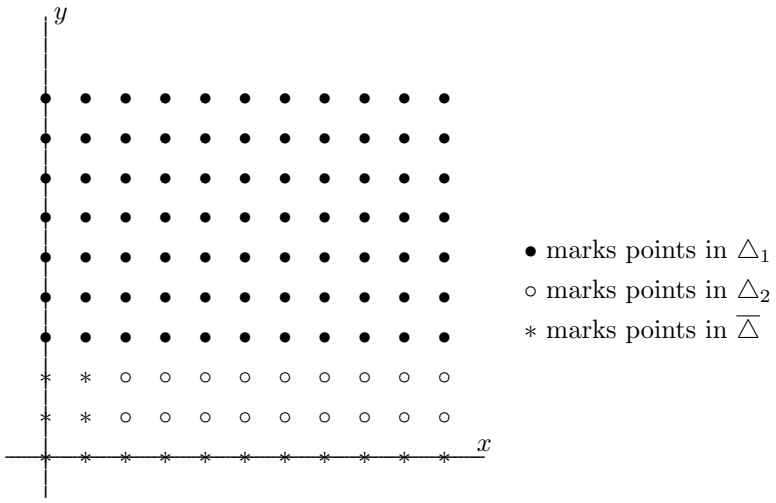
Remark. It is shown here and obvious on reflection that the second divisor will never play any role when the divisors are written in this order and division carried out using lex order with $x > y > z$, because the leading term of the first divisor divides the leading term of the second divisor.

Before leaving this example I'm curious what happens if the grlex order is used.

$F = (x^2y - x, -y^3 + x)$ with grlex order and $x > y > z$ leads to the following.



$F = (-y^3 + x, x^2y - x)$ with grlex order and $x > y > z$ leads to



Returning to the solution of (2.3.10) (d) in the general case, the argument is an extension of the one given above with no new features. If there are two expressions $f = a_1f_1 + a_2f_2 + \cdots + a_sf_s + r$ we subtract them to get

(2.3.11.d2) $$0 = A_1f_1 + A_2f_2 + \cdots + A_sf_s + r$$

with the terms λx^β which occur in A_m meeting the requirement that $\alpha(m) + \beta \in \triangle_m$ for $1 \leq m \leq s$, and the terms λx^γ which occur in r meeting the requirement that $\gamma \in \overline{\triangle}$. Suppose for some m that $A_1 = A_2 = \cdots = A_{m-1} = 0$. Let λx^β be a term of A_m, then $\beta + \alpha(m) \in \triangle_m$ and there is a term of the form $\mu x^{\beta+\alpha(m)}$ in the product A_mf_m. Now the terms in A_kf_k, $m < k \leq s$ have exponents in $\triangle_k$, and the terms in r have exponents in $\overline{\triangle}$. Since $\triangle_m$ is disjoint from the $\triangle_k$, $m < k \leq s$, and from $\overline{\triangle}$ there is no way to cancel this $\mu x^{\beta+\alpha(m)}$ and it must be that $\mu = 0$ and by extension that $A_m = 0$. By finite induction all the A_j's are zero, and then $r = 0$ too. This finishes the solution to part (d).

§**2.3.12.**

Show that the operation of computing remainders on division by $F = (f_1, \ldots, f_s)$ is linear over k. That is, if the remainder on division of g_i by F is r_i, $i = 1, 2$, then, for any $c_1, c_2 \in k$ the remainder on division of $c_1 g_1 + c_2 g_2$ is $c_1 r_1 + c_2 r_2$. Hint: Use Exercise 11.

Solution. More is true than is stated here. For example, if

$$f = a_1 f_1 + \cdots + a_s f_s + r_f,$$
$$g = b_1 f_1 + \cdots + b_s f_s + r_g,$$

Then

$$\lambda f + \mu g = (\lambda a_1 + \mu b_1) f_1 + \cdots + (\lambda a_s + \mu b_s) f_s + (\lambda r_f + \mu r_g).$$

Now the fact (2.3.11.d) that there is exactly one such expression shows not only that the operation of computing remainders is linear, but the operations of computing quotients are linear too.