Ideals, Varieties, and Algorithms Problems

Last Edited on 5/17/24 at 23:31

Chapter 1

§1.6

a. We induct on the number of variables n. When $n = 1$, if $f \in \mathbb{C}[x]$ vanishes on all $\mathbb{Z}[x]$ then by the Fundamental Theorem of Algebra, $f = 0$. Now suppose that for all $k < n$ the claim holds. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanish on all of $\mathbb{Z}^n$. We may collect all the powers of x_n and obtain that for some finite N

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Fix some $(a_1, \ldots, a_{n-1}) \in \mathbb{Z}^{n-1}$. Then $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ is the zero polynomial by the case of $n = 1$. Thus, each of the g_i must vanish on all of Z^{n-1} which implies by the induction hypothesis each of the g_i are the zero polynomial. Overall we have that f is the zero polynomial in $\mathbb{C}[x_1, \ldots, x_n]$.

b. Fix M. We induct on the number of variables n. Let $f \in \mathbb{C}[x]$ be a polynomial of degree at most M that vanishes on $\mathbb{Z}_{M+1}^n$. Then since f vanishes on $M+1$ points but has degree less than or equal to M, by the Fundamental Theorem of Algebra we must have that f is the zero polynomial. Now suppose that for all $k < n$, if $f \in \mathbb{C}[x_1, \ldots, x_k]$ is a polynomial whose variables are of degree at most M vanishing on $\mathbb{Z}_{M+1}^k$, then f is the zero polynomial. Now suppose that $f \in \mathbb{C}[x_1, \ldots, x_n]$ is a polynomial whose variables are of degree at most M vanishing on $\mathbb{Z}_{M+1}^n$. We may collect all the powers of x_n and obtain that

$$f = \sum_{i=0}^{M} g_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Fix some $(a_1, \ldots, a_{n-1}) \in \mathbb{Z}_{M+1}^{n-1}$. Then $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ is the zero polynomial by the case of $n = 1$. Thus, each of the g_i must vanish on all of Z_{M+1}^{n-1} which implies by the induction hypothesis each of the g_i are the zero polynomial. Overall we have that f is the zero polynomial in $\mathbb{C}[x_1, \ldots, x_n]$.

§2.6

a. Let $(a_1, \ldots, a_n) \in k^n$. Then we have that the only set of polynomials that vanishes at this point exactly is $f_1 := x_1 - a_1, \ldots, f_n := x_n - a_n$. Thus $\mathbf{V}(f_1, \ldots, f_n) = \{(a_1, \ldots, a_n)\}$.

b. For a finite set of points in k^n, we can build a variety for each point akin to part **a**. By **Lemma 2** of **§2**, we can take a union on of these varieties and form a variety which is equal to this finite set of points.

§2.8 Let $X = \{(x, x) \mid x \in \mathbb{R},\ x \neq 1\}$. Let $f(x, y)$ be a polynomial in $\mathbb{R}[x, y]$ vanishing on X. Let $g(x) = f(x, x)$ be a polynomial in $\mathbb{R}[x]$. Then we have that since g is a nonzero polynomial, it must have finitely many roots. However, g vanishes at all $x \neq 1$ which implies that g must be the zero polynomial. In particular we must have that f vanishes at $(1, 1)$ which is a contradiction.

§2.9 Suppose $R = \{ (x,y) \in \mathbb{R}^2 \mid y > 0 \}$ was an affine variety. Then $R \cap V(x) = \{ (0,y) \in \mathbb{R}^2 \mid y > 0 \}$ is also an affine variety. Let $f = a_n(y)x^n + a_{n-1}(y)x^{n-1} + \cdots + a_0(y)$ be a polynomial in this variety. Since $f \in R \cap V(x)$, this polynomial must vanish at $x = 0$ for any $y > 0$. Since $\mathbb{R}$ is an infinite field, by Proposition 5 of **§1** we must have that $a_0(y) = 0$. Therefore, every polynomial in $R \cap V(x)$ must a polynomial in $\mathbb{R}[y][x]$ with constant term 0. Since every polynomial is of this form, then in fact the polynomial must vanish along the whole line $x = 0$, contradicting the fact that they vanish solely along the half line $\{ (0,y) \in \mathbb{R}^2 \mid y > 0 \}$. Thus R cannot be an affine variety.

§2.10 Suppose f vanishes on $\mathbb{Z}^n$. Let M be the maximal degree of any variable in f. Then in particular we have that f vanishes on $\mathbb{Z}^n_{M+1}$ which by **§1.6b** means f is the zero polynomial. Thus $\mathbb{Z}^n$ cannot be an affine variety.

§2.11

a. If n is odd, then $(x,y) = (0,1)$ and $(x,y) = (1,0)$ are trivial solutions. If n is even, then $(x,y) = (0,\pm 1)$ and $(x,y) = (\pm 1, 0)$ are trivial solutions. Clearly, these are the only trivial solutions.

b. ⟨⟨ **Kind of obvious but annoying to write out.** ⟩⟩

§2.15

a. We prove by induction on n for the case of finite union (the case for union is the same). Let k be a field. If V_1 and V_2 are an affine varities then by **Lemma 2** of **§2** we have that $V_1 \cup V_2$ is an affine variety. Now suppose that for all $k < n$, $\bigcup_{i=1}^{k} V_i$ is an affine variety where each V_i is an affine variety. Let $V_i, \ldots, V_n$ be a collection of affine varieties in k^n. We have that $\bigcup_{i=1}^{n} V_i = \left(\bigcup_{i=1}^{n-1} V_i \right) \cup V_n$. By the induction hypothesis, $\bigcup_{i=1}^{n-1} V_i$ is an affine variety. Using this and the case of $n = 2$, we have that overall $\bigcup_{i=1}^{n} V_i$ is an affine variety.

b. Consider the set $X = \{ (x,x) \mid x \in \mathbb{R},\ x \neq 1 \}$. We know by **§2.8** that X is not an affine variety. However for fixed $x \in \mathbb{R}$, we know by **§2.6 a** that singular points are affine varieties. Thus

$$X = \bigcup_{x \in \mathbb{R},\ x \neq 1} \{ (x,x) \}$$

is an infinite union of affine varieties that is not an affine variety itself.

c. We know that $\{ (1,1) \}$ is an affine variety. The affine variety $\mathbf{V}(x-y)$ is the set $\{ (x,x) \mid x \in \mathbb{R} \}$. However, we have that $\mathbf{V}(y-x) \setminus \{ (1,1) \}$ is not an affine variety.

d. Suppose $V = \mathbf{V}(f_1, \ldots, f_s)$ and $W = \mathbf{V}(g_1, \ldots, g_t)$. We claim that $V \times W$ as defined in the problem is equivalent to

$$S = \{ (x_1, \ldots, x_n, y_1, \ldots, y_m) \in k^{n+m} \mid f_1(x_1, \ldots, x_n) = \cdots f_s(x_1, \ldots, x_n) = g_1(y_1, \ldots, y_m) = g_t(y_1, \ldots, y_m) = 0 \}.$$

Suppose $(x_1, \ldots, x_n, y_1, \ldots, y_m) \in V \times W$. Then we know that for all $1 \leq i \leq s$ that $f_i(x_1, \ldots, x_n) = 0$ and for all $1 \leq j \leq t$ that $g_j(y_1, \ldots, y_m) = 0$. Thus $(x_1, \ldots, x_n) \in V$ and $(y_1, \ldots, y_m) \in W$ and thus $(x_1, \ldots, x_n, y_1, \ldots, y_m) \in S$.

Now suppose $(x_1, \ldots, x_n, y_1, \ldots, y_m) \in S$. Then $(x_1, \ldots, x_n) \in V$ since for all $1 \leq i \leq s$ we have that $f_i(x_1, \ldots, x_n) = 0$. Similarly we have that $(y_1, \ldots, y_m) \in W$ since for all $1 \leq j \leq t$ we have that $g_j(y_1, \ldots, y_m) = 0$. Thus $(x_1, \ldots, x_n, y_1, \ldots, y_m) \in V \times W$.

⟨⟨ **Maybe I should do some exercises from §3.** ⟩⟩

§4.1

a. Since $y = \frac{1}{x}$ we have that $x^2 + y^2 - 1 = x^2 + \frac{1}{x^2} - 1$ which implies that $x^4 - x^2 + 1 = 0$.

b. Using the fact that $(xy-1)(xy+1) = x^2y^2 - 1$, we have that

$$x^2(x^2+y^2-1) + (-1)(xy+1)(xy-1) = x^4 + x^2y^2 - x^2 - x^2y^2 + 1 = x^4 - x^2 + 1 \in \left\langle x^2+y^2-1, xy-1 \right\rangle.$$

§4.2 Suppose $f_1, \ldots, f_s \in I$. Then for any polynomial $h \in k[x_1, \ldots, x_n]$ we have $h \cdot f_i \in I$ for $1 \leq i \leq s$. Thus for any polynomial in $\langle f_1, \ldots, f_s \rangle$, that polynomial is in I.

Now suppose $\langle f_1, \ldots, f_s \rangle \subseteq I$. Then clearly each $f_i \in I$. Thus, the two statements are equivalent.

§4.4 This follows immediately from the fact that $V(f_1, \ldots, f_s) = V(\langle f_1, \ldots, f_s \rangle)$ but we haven't proven that at this stage.

Suppose $\overline{a} = (a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$. Then $f_1(\overline{a}) = \cdots = f_s(\overline{a}) = 0$. Since for all i, we have that $g_i \in \langle f_1, \ldots, f_s \rangle$ we have that $g_i(\overline{x}) = h_1 f_1(\overline{x}) + \cdots + h_s f_s(\overline{x})$ where $h_i \in k[\overline{x}]$. Thus $g_i(\overline{a}) = h_1 f_1(\overline{a}) + \cdots + h_n f_s(\overline{a}) = 0$ and $\overline{a} \in V(g_1, \ldots, g_t)$. The reverse inclusion is the exact same.

§4.5 This is immediate from applying **Proposition 4** of **§4** to **Exercise 3** of **§4**.

§4.6

a. Suppose there was a finite basis of polynomials $\{ p_1, \ldots, p_n \} \subseteq k[x]$. Let d be the greatest degree of these polynomials. Then $x^{d+1} \in k[x]$ but no linear combination of the p_i's can ever equal x^{d+1} which contradicts the fact that our set is indeed a basis.

b. By commutativity, we can write 0 as $xy - xy = (x)y - (y)x$.

c. Similarly if $\{ f_1, \ldots, f_s \}$ is the basis for some ideal $I \subseteq k[x_1, \ldots, x_n]$ then we have that for $i \neq j$ that $0 = (f_i)f_j - (f_j)f_i$.

d. We have that $x^2 + (x+y)y = x^2 + xy + y^2 = y^2 + (x+y)x$.

e. It is not hard to see that $\langle x \rangle$ and $\left\langle x + x^2, x^2 \right\rangle$ are both minimal bases. Clearly we have that $x + x^2 - x^2 = x$ and so $\langle x \rangle \subseteq \langle x + x^2, x^2 \rangle$. Similarly we get that $\langle x + x^2, x^2 \rangle \subseteq \langle x \rangle$. Thus, both $\{ x \}$ and $\left\{ x^2, x + x^2 \right\}$ are minimal bases of the same ideal.

This is different to linear algebra. Note that these bases have different cardinality. However, two bases of the same vector space in linear algebra must have the same cardinality.

§4.7 If we have that $x^n = y^n = 0$, then we must have that $x = y = 0$. Thus we have that $\mathbf{I}(\mathbf{V}(x^n, y^n)) = \mathbf{I}(\{ 0, 0 \})$ which we know to be equal to $\langle x, y \rangle$.

§4.8

a. Suppose $f^k \in \mathbf{I}(V)$ for some $f \in k[x_1, \ldots, x_n]$ and some $k \in \mathbb{N}$. By cancellation, f^k vanishing on V implies that f vanishes on V. Thus $f \in \mathbf{I}(V)$. Clearly if $f \in \mathbf{I}(V)$ then for all $k \in \mathbb{N}$ we have that $f^k \in \mathbf{I}(V)$.

b. We have that $x^2 \in \left\langle x^2, y^2 \right\rangle$. However, note that $x \notin \langle x^2, y^2 \rangle$. Thus $\langle x^2, y^2 \rangle$ is not radical.

§4.14

a. We have that $V = W$ if and only if $V \subseteq W$ and $W \subseteq V$. But this is equivalent to $I(V) \supseteq I(W)$ and $I(W) \supseteq I(V)$. Since this in turn is equivalent to $I(V) = I(W)$, we have that $V = W$ if and only if $I(V) = I(W)$.

b. Since $V \neq W$, we cannot have that $W \subseteq V$ meaning that $I(W) \supsetneq I(V)$. Following the above argument, the claim is immediate.

§4.15

a. Clearly $0 \in \mathbf{I}(S)$ since 0 vanishes on every point. Then suppose $f, g \in \mathbf{I}(S)$ and $h \in k[x_1, \ldots, x_n]$. Then for each $(a_1, \ldots, a_n) \in S$ we have that

$$(f + h \cdot g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + h(a_1, \ldots, a_n) \cdot g(a_1, \ldots, a_n) = 0 + 0 = 0.$$

Thus, $\mathbf{I}(S)$ is an ideal.

b. Clearly $\langle x - y \rangle \subseteq \mathbf{I}(X)$. To show the converse, let $f(x, y) \in \mathbf{I}(X)$. In **Exercise 8** of **§2** we showed that $g(t) = f(t, t) \in \mathbb{R}[t]$ must be zero. ⟨⟨ **This implies that** ⟩⟩ $x - y$ must divide $f(x, y)$ and so $\mathbf{I}(X) \subseteq \langle x - y \rangle$.

c. Suppose $f \in \mathbb{C}[x_1, \ldots, x_n]$ was in $\mathbf{I}(\mathbb{Z}^n)$. Let M be the maximal degree of any variable in f. Then in particular, f vanishes on $\mathbb{Z}^n_{M+1}$ and thus by **§1.6b** and we must have that f is the zero polynomial. Thus $\mathbf{I}(\mathbb{Z}^n) = \{0\}$.

§4.16

a. Clearly if $I = k[\overline{x}]$ then $1 \in I$. Now suppose that $1 \in I$. Clearly $I \subseteq k[\overline{x}]$. Then for all $f(\overline{x}) \in k[\overline{x}]$, $1 \cdot f(\overline{x}) = f(\overline{x}) \in I$ and so $k[\overline{x}] \subseteq I$.

b. If $\lambda \neq 0 \in I$, then $\frac{1}{\lambda} \cdot \lambda = 1 \in I$. Applying the previous exercise yields the claim.

c. We have that $(f + g)^3 = f^3 + 3f^2 g + 3f g^2 + g^3 = (f + 3g)f^2 + (g + 3f)g^2$ and so $(f + g)^3 \in I$.

d. By the binomial theorem, we have that

$$(f + g)^{r+s-1} = \sum_{i=0}^{r+s-1} \binom{r+s-1}{i} f^i g^{r+s-1-i} = \sum_{i=0}^{r-1} \binom{r+s-1}{i} f^i g^{r+s-1-i} + \sum_{i=r}^{r+s-1} \binom{r+s-1}{i} f^i g^{r+s-1-i}.$$

We have that g^s divides the first summation and f^r divides the second summation. Thus $(f + g)^{r+s-1} \in I$.

§4.17

a. We have that $xy \notin \langle x^2, y^2 \rangle$ since any polynomial of the form $f(x, y) = f_1(x, y)x^2 + f_2(x, y)y^2$ has $\deg_x(f) \geq 2$ and $\deg_y(f) \geq 2$.

b. Similar to the proof that $x \notin \langle x^2, y^2 \rangle$, we have that $1, y \notin \langle x^2, y^2 \rangle$. However, any other monomial m either has $\deg_x(m) \geq 2$ or $\deg_y(m) \geq 2$ so $m \in \langle x^2, y^2 \rangle$. Thus, all other monomials m are in $\langle x^2, y^2 \rangle$.

§4.18

a. Clearly $\langle x_1, \ldots, x_n \rangle \subseteq \mathbf{I}(\{0\})$. Now suppose that $f(\overline{x}) \in \mathbf{I}(\{0\})$. This implies that f has constant term 0. Then $f(\overline{x}) = 0 + \sum_{j=1}^n \sum_{\overline{I}, I_j > 0} a_{\overline{I}} \overline{x}^{\overline{I}} = 0 + \sum_{j=1}^n x_j \sum_{\overline{I}, I_j > 0} a_{\overline{I}} \overline{x}^{\overline{I} - (0, \ldots, 1, \ldots 0)}$. Thus $f \in \langle x_1, \ldots, x_n \rangle$.

b. This says that all polynomials with constant term 0 vanish at the origin. ⟨⟨ **Does it say anything else?** ⟩⟩

§5.4 Given polynomial $f, g \in k[x]$, let $h = \gcd(f, g)$ and let $S = \{Af + Bg \mid A, B \in k[x]\}$. This set is non-empty since it contains f and g itself. Since this set is non-empty, there exists some polynomial m of minimal degree in S. We must have that m divides every element of S. Suppose there were some $A, B \in k[x]$ such that $m \nmid Af + Bg$. Then by the Euclidian Algorithm we could find a polynomial $r = m - (Af + Bg)q$ for some $q \in k[x]$ which is of strictly smaller degree, contradicting the minimality of the degree of m. In particular now, we have that $m \mid f, g$ which implies $m \mid \gcd(a, b)$ and that $\gcd(f, g) \in S$. Thus $\gcd(f, g) = Af + Bg$ for some $A, B \in k[x]$.

§5.5 Clearly $\langle f - qg, g \rangle \subseteq \langle f, g \rangle$ since $f - qg = (f) - q(g)$ and $g = (g)$. Then since $(f - qg) + q(g) = f$ and $g = (g)$ we have the reverse inclusion as well.

§5.11

a. If $\mathbf{V}(f) = \emptyset$ then by the Fundamental Theorem of Algebra, we must have that $\deg(f) = 0$. Thus, f is a nonzero constant since if it was zero, then we would have $\mathbf{V}(f) = \mathbb{C}$. Now suppose f is a nonzero constant. Then clearly $\mathbf{V}(f) = \emptyset$.

b. Let $d = \gcd(f_1, \ldots, f_s)$. We know that $\langle d \rangle = \langle f_1, \ldots, f_s \rangle$. Using this, the fact that if two sets of polynomials generate the same ideals, then their affine varieties are the same, and **a.** we get the claim.

c. Using **b.**, we get that $\mathbf{V}(f_1, \ldots, f_s) \neq \emptyset$ if and only if $\gcd(f_1, \ldots, f_s)$ is a non-constant polynomial in $\mathbb{C}[x]$.

§5.12

a. Let $f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$. Suppose $a \in \mathbf{V}(f)$. Then we know that $f(a) = 0$ which implies that $a = a_i$ for some $1 \leq i \leq l$. Thus, $a \in \{a_1, \ldots, a_l\}$. Now suppose $a \in \{a_1, \ldots, a_l\}$. Then clearly $f(a) = 0$ which implies that $a \in \mathbf{V}(f)$.

b. Let $f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$. By **a.** we have that $\mathbf{I}(\mathbf{V}(f)) = \mathbf{I}(\{a_1, \ldots, a_l\})$. Take any polynomial g in $\mathbf{I}(\{a_1, \ldots, a_l\})$. Since $g(a_i) = 0$ for all $1 \leq i \leq l$, we have that $f_{\text{red}} | g$ and thus $g \in \langle f_{red} \rangle$. Now suppose we have some $g \cdot f_{\text{red}} \in \langle f_{\text{red}} \rangle$. Then note that since $f_{\text{red}}(a_i) = 0$ for all $1 \leq i \leq l$, we must have that $(g \cdot f_{\text{red}})(a_i) = 0$ for all $1 \leq i \leq l$. Thus $g \cdot f_{\text{red}} \in \mathbf{I}(\{a_1, \ldots, a_l\})$.

§5.14

a. We have that $f' = r(x-a)^{r-1}h + (x-a)^r h' = (x-a)^{r-1}(rh + (x-a)h')$. Note that $rh + (x-a)h'$ cannot vanish at a since if it did, we would have that $rh(a) = 0$ and since r is a nonzero constant we would contradict the fact that $h(a) \neq 0$.

b. We proceed by induction on l. If $l = 1$ then by part **a.** we know the claim holds. Suppose the claim holds for $f = c(x-a_1)^{r_1} \cdots (x-a_k)^{r_k}$ for all $1 \leq k < l$ with $a_1, \ldots, a_k \in \mathbb{C}$. Let $f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$. Then we have that $f = g \cdot c(x-a_l)^{r_l}$ where $g = (x-a_1)^{r_1} \cdots (x-a_{l-1})^{r_{l-1}}$. By our inductive hypothesis, we have that $g' = (x-a_1)^{r_1-1} \cdots (x-a_{l-1})^{r_{l-1}-1} H$ for some $H \in \mathbb{C}[x]$ which does not vanish at $\{a_1, \ldots, a_{l-1}\}$. Thus we have that

$$\begin{aligned} f' &= g' \cdot c(x-a_l)^{r_l} + g \cdot c r_l (x-a_l)^{r_l-1} \\ &= (x-a_1)^{r_1-1} \cdots (x-a_{l-1})^{r_{l-1}-1} H \cdot (x-a_l)^{r_l} + (x-a_1)^{r_1} \cdots (x-a_{l-1})^{r_{l-1}} \cdot c r_l (x-a_l)^{r_l-1} \\ &= (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1} (H(x-a_l)^{r_l} + c r_l (x-a_1) \cdots (x-a_{l-1})^{r_{l-1}}). \end{aligned}$$

Consider the polynomial $H(x-a_l)^{r_l} + c r_l (x-a_1) \cdots (x-a_{l-1})^{r_{l-1}}$. We know that H does not vanish on $\{a_1, \ldots, a_{l-1}\}$ and thus the whole polynomial does not vanish on this set. We also have that the polynomial does not vanish on a_l since each a_i is distinct by assumption and both c and r_l are nonzero. Thus the claim holds.

c. Let $f = c(x-a_1)^{r_1} \cdots (x-a_l)^{r_l}$ and thus by **b.** we have that $f' = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1} H$ where H is a polynomial in $\mathbb{C}[x]$ that does not vanish on $\{a_1, \ldots, a_l\}$. Clearly we have that $(x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}$ divides both f and f'. Suppose d divides f and f'. Then we know that since $d \in \mathbb{C}[x]$ that d factors completely. Thus, the fact that d divides f implies that the points where d vanishes at is a subset of $\{a_1, \ldots, a_l\}$. Furthermore, since d divides f' we must have that the power of each factor $(x-a_i)$ must be at most $r_i - 1$. Overall we must ave that d divides $(x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}$ and that $\gcd(f, f') = (x-a_1)^{r_1-1} \cdots (x-a_l)^{r_l-1}$.

§5.15

a. Let $f = c(x-a_1)^{r_1}\cdots(x-a_l)^{r_l}$. Then we have that $f' = (x-a_1)^{r_1-1}\cdots(x-a_l)^{r_l-1}H$, where H is a polynomial in $\mathbb{C}[x]$ that does not vanish on $\{a_1,\ldots,a_l\}$, and $f_{\text{red}} = c(x-a_1)\cdots(x-a_l)$. Then by **§5.14c.** we have that

$$\frac{f}{\gcd(f,f')} = \frac{c(x-a_1)^{r_1}\cdots(x-a_l)^{r_l}}{(x-a_1)^{r_1-1}\cdots(x-a_l)^{r_l-1}} = c(x-a_1)\cdots(x-a_l) = f_{\text{red}}.$$

b. Using the previous formula from **a.**, we may find using SageMath that the following is the square-free part of $f = x^{11}-x^{10}+2x^8-4x^7+3x^5-3x^4+x^3+3x^2-x-1$:

$$f_{\text{red}} = (x-0.341163901914010-1.16154139999725i)^2\cdot(x-0.341163901914010+1.16154139999725i)^2 \cdot(x+0.682327803828019)^2\cdot(x+1)^2\cdot(x-1)^3$$

§5.16 Suppose we are given a set of polynomial $f_1,\ldots,f_s \in \mathbb{C}[x]$. Let $d = \gcd(f_1,\ldots,f_s)$. First we know that $\langle f_1,\ldots,f_s\rangle = \langle d\rangle$. Thus, by the fact that if two sets of polynomials generate the same ideals then their varieties are the same, we know that $\mathbf{I}(\mathbf{V}(f_1,\ldots,f_s)) = \mathbf{I}(\mathbf{V}(d))$. We know by **§5.12b.** that $\mathbf{I}(\mathbf{V}(d)) = \langle d_{\text{red}}\rangle$. Then from **§5.15a.** we know that $d_{\text{red}} = \frac{d}{\gcd(d,d')}$. We can easily compute this quantity using the Euclidian Algorithm and the Division Algorithm. Thus overall we have that $\mathbf{I}(\mathbf{V}(f_1,\ldots,f_s)) = \langle d_{\text{red}}\rangle = \left\langle \frac{d}{\gcd(d,d')}\right\rangle$.

Chapter 2

§1.4

a. ⟨⟨ **Duh** ⟩⟩

b Consider any finite generating set $\langle f_1, \ldots, f_s \rangle$. For each f_i, let m_i be $\max\{ j \in \mathbb{N} \mid \deg_{x_j} f_i > 0 \}$. Each m_i is finite as polynomials have finitely many terms. Let $m = \max_i m_i$. Then $x_{m+1} \in I$ but $x_{m+1} \notin \langle f_1, \ldots, f_s \rangle$.

§2.7

a. Suppose that for some $\alpha \in \mathbb{Z}^n_{\geq 0}$ we had $\alpha < 0$. Then we know that the leftmost nonzero entry of $0 - \alpha$ exists and is positive, suppose it occurs at $0 - \alpha_i$. However if $-\alpha_i > 0$ then we must have that $\alpha_i < 0$ which is impossible. Thus all $\alpha \in \mathbb{Z}^n_{\geq 0} \geq 0$.

b. Suppose $x^\alpha \mid x^\beta$. Then for some $\gamma \in \mathbb{Z}^n_{\geq 0}$ we have that $x^\beta = x^\alpha \cdot x^\gamma$. Thus, by **a.**, we have that $\beta = \alpha + \gamma \geq \alpha$ since $\gamma \geq 0$. The converse also holds by reversing the logic with $\gamma = \beta - \alpha \geq 0$.

c. Suppose that $\alpha + \beta$ was the minimum element of $\alpha + \mathbb{Z}^n_{\geq 0}$ for some $\beta \neq 0$. Then in particular we have that $\beta > 0$. But $\alpha = \alpha + 0 \in \alpha + \mathbb{Z}^n_{\geq 0}$. Thus we have that $\alpha + \beta < \alpha + 0 \implies \beta < 0$ which we know is impossible. Thus α must be the minimum element.

§2.10 This is not necessarily true. Take lexographical order in $\mathbb{Z}^2_{\geq 0}$ for example. We know this is a monomial order. We have that for any $x \in \mathbb{Z}_{\geq 0}$ that $(3,0) >_{lex} (2,x) >_{lex} (1,0)$. However there are infinitely many such x. Thus there are infinitely many elements between $(3,0)$ and $(1,0)$.

This holds for graded lex order. As a rough heuristic we only show that for $\alpha \in \mathbb{Z}^n_{\geq 0}$ there are only finitely many elements β such that $\alpha >_{grlex} \beta >_{grlex} 0$. We know that the integer equation $x_1 + \cdots + x_n = |\alpha|$ has a finite number of solutions in $\mathbb{Z}^n_{\geq 0}$. There are also finitely many integers between $|\alpha|$ and 0 and thus overall we must have that there are only finitely many elements between α and 0.

§2.11

a. Let $m = x^\beta, f = \sum_\alpha a_\alpha x^\alpha$. Then $m \cdot f = \sum_\alpha a_\alpha x^{\alpha+\beta}$. Suppose $d = \text{multideg}(f)$. Then since $d = \max\left\{ \alpha \in \mathbb{Z}^n_{\geq 0} \;\middle|\; a_\alpha \neq 0 \right\}$, we have $d + \beta = \max\left\{ \alpha \in \mathbb{Z}^n_{\geq 0} \;\middle|\; a_\alpha \neq 0 \right\}$. Thus $\text{LM}(m \cdot f) = x^{d+\beta} = m \cdot \text{LM}(f)$.

Similarly we have that $\text{LC}(m \cdot f) = a_{\text{multideg}(m \cdot f)} = a_{\text{multideg}(f)} = \text{LC}(f)$. Thus we have that $\text{LT}(m \cdot f) = \text{LC}(m \cdot f)\,\text{LM}(m \cdot f) = \text{LC}(f) \cdot m \cdot \text{LM}(f) = m \cdot \text{LT}(f)$.

b. Since the definitions of LT, LC, and LM all depend on multideg(f), we only aim to show that multideg$(f \cdot g) =$ multideg(f)+multideg(g). This is immediate from the definitions of multideg and the fact that $\max\{ a + b \mid a \in A, b \in B \} = \max(A) + \max(B)$. ⟨⟨ **It would be nice to formally type this for completeness but I've done this multiple times before.** ⟩⟩

c. The most we can hope for is that $\text{multideg}\left(\sum_{i=1}^s f_i g_i\right) \leq \max\{ \text{multideg}(f_i g_i) \mid 1 \leq i \leq s \}$. We may not have equality due to cancellation.

§2.13 Suppose we had a monomial order such that $x^j < x^i$ for some $j > i$. Then $1 < x^{j-i}$ since this is a monomial order. However, since this is a monomial order, we must have that $1 \cdot x^i = x^i < x^{j-i} \cdot x^i = x^j$ which is a contradiction.

§3.4

a. Clearly for any polynomial we have that $\text{multideg}(f) = \text{multideg}(\text{LT}(f))$. If $q_i f_i \neq 0$ then we must have that neither q_i nor f_i are equal to 0. Let p be as in the proof of the multivariate division algorithm. We know that $q_i = {}^{\text{LT}(p)}/_{\text{LT}(f_i)}$ for some value of p as the algorithm goes on. Since $\text{multideg}(\text{LT}(p)) \leq \text{multideg}(\text{LT}(f))$ we have that $\text{multideg}(q_i) \leq \text{multideg}\left({}^{\text{LT}(f)}/_{\text{LT}(f_i)}\right) = \text{multideg}(\text{LT}(f)) - \text{multideg}(f_i)$. Thus we have that $\text{multideg}(q_i f_i) = \text{multideg}(q_i) + \text{multideg}(f_i) \leq \text{multideg}(\text{LT}(f)) = \text{multideg}(f)$.

b. We have that r does not divide into any of the $q_i f_i$ implying that $\text{multideg}(r) \leq \text{multideg}(q_i f_i)$ which implies by **a.** that $\text{multideg}(f) \geq \text{multideg}(r)$.

§4.1 Let $A = \{\, \alpha \in \mathbb{Z}^n_{\geq 0} \mid x^\alpha \in I \,\}$. With this, let $I' = \langle\, x^\alpha \mid \alpha \in A \,\rangle$. We wish to show that $I = I'$. Let $x^\alpha \in I'$. Then, by the definition of A, $x^\alpha \in I$ and we are done. Now let $f = \sum c_\alpha x^\alpha \in I$, then by the property of I we have that every $x^\alpha \in I$ and so $\alpha \in I$ meaning $x^\alpha \in I'$. Since each $x^\alpha \in I'$, we must have that $f \in I'$.

§4.2 We want to show that if $f \in I$, I a monomial ideal, then every term of f is in I. Since I is a monomial ideal, then $I = \langle\, \alpha \mid \alpha \in A \,\rangle$ for some $A \in \mathbb{Z}^n_{\geq 0}$. By the definition of a monomial ideal, f is of the form $f = \sum_{\alpha \in A} h_\alpha x^\alpha$ where $h_\alpha \in k[x_1, \ldots, x_n]$. Clearly for each α, $x^\alpha \in I$ so $h_\alpha x^\alpha \in I$ and thus every term of f is in I.

§4.3

a. The following image is the solution:

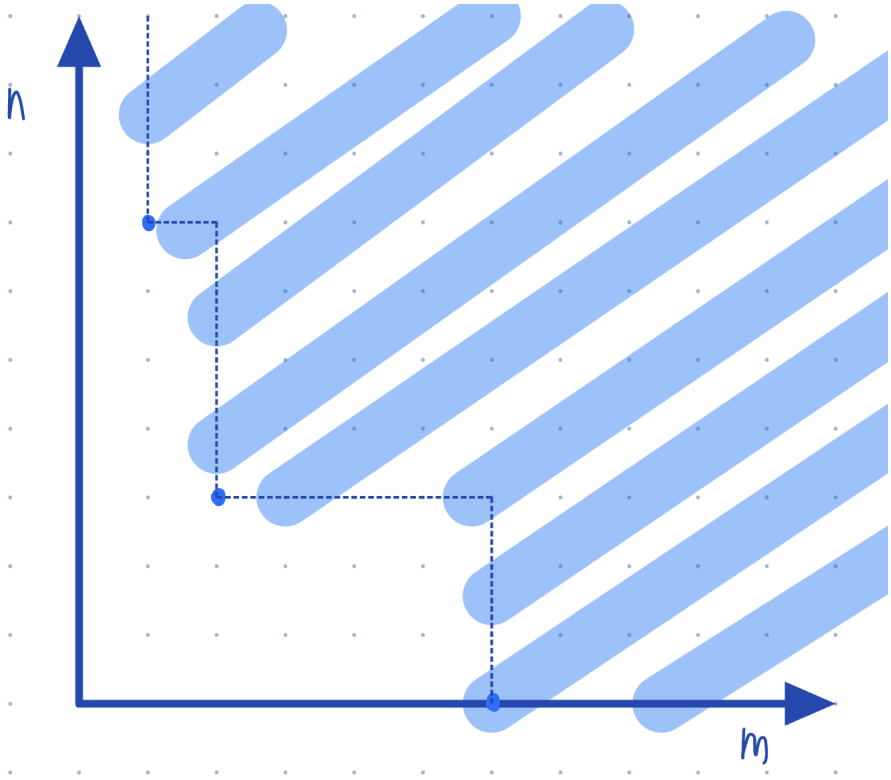

Figure 1: Shaded region represents possible $x^n y^m \in \left\langle x^6, x^2 y^3, x y^6 \right\rangle$

b. The *unshaded* region in the image represents possible remainders up to multiplication by a constant. ⟨⟨ **This would be annoying to actually describe.** ⟩⟩

§4.4

a. We have that $I = \left\langle x^3y^6, x^5y^4, x^6 \right\rangle$. We have that the "projection" $J = \left\langle x^3 \right\rangle$. Since $x^3y^6 \in I$, we have that $m = 6$. Thus we find "slices" J_ℓ for $0 \leq \ell \leq m-1 = 5$. We have that

$$J_0 = J_1 = J_2 = J_3 = \left\langle x^6 \right\rangle$$
$$J_4 = J_5 = \left\langle x^5 \right\rangle$$

Thus $I = \left\langle x^6, x^6y, x^6y^2, x^6y^3, x^5y^4, x^5y^5, x^3y^6 \right\rangle$.

b. We may take our basis from **a.** and do repeated trial division to make it minimal. Thus $I = \left\langle x^6, x^5y^4, x^3y^6 \right\rangle$

§4.5 Let μ be the minimal element of S. ⟨⟨ **Is the minimal element not 0?** ⟩⟩ We have that $A \subseteq S$ and thus for all $\alpha \in A$, $\mu \leq \alpha$ and so $x^\mu | x^\alpha$. But x^{mu} lies in I and so $x^\alpha \mid x^\mu$ for some $\alpha \in \mu$. Thus $x^\mu = x^\alpha$ and $\mu = \alpha$.

§4.7 Suppose Dickson's Lemma is true. Let A be a nonempty subset of $\mathbb{Z}^n_{\geq 0}$. Consider the monomial ideal $I = \langle x^\alpha \mid \alpha \in A \rangle$. Then we know there exists a finite basis such that $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$ Let $\alpha \in A$. Then we know that some $x^{\alpha(i)}$ divides x^α. Thus $x^\alpha = x^{\alpha(i)}x^\gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$. Thus $\alpha = \alpha(i) + \gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$.

Now suppose that for a nonempty subset $A \subseteq \mathbb{Z}^n_{\geq 0}$, we can find a finite set $\{\alpha(1), \ldots, \alpha(s)\} \subseteq A$ such that for any $a \in A$ we have that for some $1 \leq i \leq s$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$ that $\alpha = \alpha(i) + \gamma$. Let $\langle x^\alpha \mid \alpha \in A \rangle$ be a monomial ideal and let $\{\alpha(1), \ldots, \alpha(s)\} \subseteq A$ be the set as described before for A. Then we claim that $I = \langle \alpha(1), \ldots, \alpha(s) \rangle$. Suppose $f \in I$. Then we know that every term of f lies in I. Thus we only need to consider monomials $x^\alpha \in I$. We know that for some $1 \leq i \leq s$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$ that $\alpha = \alpha(i) + \gamma$. This implies that some $x^{\alpha(i)}$ divides x^α. Thus we have that $x^\alpha \in \langle \alpha(1), \ldots, \alpha(s) \rangle$. The other direction of containment is trivial due to the fact that $\langle \alpha(1), \ldots, \alpha(s) \rangle \subseteq A$. Thus we have found a finite basis for I, proving Dickson's Lemma.

§4.8 Suppose the remainder of f on division by $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ is 0. Then the polynomial division algorithm yields an expression showing that $f \in I$. Now suppose that $f \in I$. Then every term of f lies in I, let $c_\beta x^\beta$ be such a term. Then x^β lies in I which means that some $x^{\alpha(i)}$ divides x^β. We may do this for every term in f. Since ever term is divisible by $\text{LT}(x^{\alpha(i)}) = x^{\alpha(i)}$ for some i, we have that division of f by $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ has remainder 0.

§5.3

a. Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal such that $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \subsetneq \langle \text{LT}(I) \rangle$ Thus there is some $f \in I$ such that $\text{LT}(f) \notin \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. After division by $F = (f_1, \ldots, f_s)$ we have that

$$f = q_1f_1 + \cdots + q_sf_s + r$$

such that no term of r is divisible by any of the $\text{LT}(f_i)$ by definition of remainder. Then by Lemma 2 of **§4** we must have that $\text{LT}(r) \notin \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. Since $0 \in \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$, $\text{LT}(r) \neq 0$ and r is non-zero. ⟨⟨ **This feels circular** ⟩⟩

b. Gröbner bases are the best for ideal membership since if we have some Gröbner basis $\{g_1 \ldots . g_t\}$ then we can test $f \in I$ by checking if the remainder of f after division by $(g_1, \ldots, g_t)$ is zero or not.

§5.5 Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Let $G = \{ g_1, \ldots, g_t \}$ be a Gröbner basis for I. Thus we have that $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Since $\langle \text{LT}(I) \rangle$ is a monomial ideal, Lemma 2 of **§4** tells us that some $\text{LT}(g_i)$ divides $\text{LT}(f)$ for $f \in I$.

Now suppose that we have some set $\{ g_1, \ldots, g_t \}$ such that for every $f \in I$ we had that some $\text{LT}(g_i)$ divides $\text{LT}(f)$. This satisfies the definition of a Gröbner basis.

§5.10 Let $I \subseteq k[x_1, \ldots, x_n]$ be a principal ideal. Suppose $\{ g_1, \ldots, g_t \}$ be a finite subset of of I containing some g_i such that $I = \langle g_i \rangle$. Clearly we have that $\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle \subseteq \langle \text{LT}(I) \rangle$. Now suppose we have some $\text{LT}(f) \in \langle \text{LT}(I) \rangle$. Then we know by **§5.5** and the fact that $I = \langle g_i \rangle$ we have that $f = g_i h_i$ for some $h_i \in k[x_1, \ldots, x_n]$. Then in particular we have that $\text{LT}(g_i)$ divides $\text{LT}(f)$ and thus $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$.

§5.11 Clearly we have that $\langle x_1, \ldots, x_n, f \rangle \subseteq k[x_1, \ldots, x_n]$. Now let $g \in k[x_1, \ldots, x_n]$. Consider g divided by $(x_1, \ldots, x_n)$. Then, without loss of generality by combining like terms, we have that $g = q_1 x_1 + \cdots + q_n x_n + r$ where none of the monomials of r are divisible by any of the x_i. Thus r must be a constant. If $r = 0$ then we have that $g \in \langle x_1, \ldots, x_n \rangle \subseteq \langle x_1, \ldots, x_n, f \rangle$. Otherwise suppose that $r \neq 0$. Then note that $f \notin \langle x_1, \ldots, x_n \rangle$ and thus, after division by $(x_1, \ldots, x_n)$, we have that $f = p_1 x_1 + \cdots + p_n x_n + s$ where s is the remainder and importantly we have that $s \neq 0$. Thus $\langle x_1, \ldots, x_n, f \rangle$ contains every non-zero constant and we have that $r \in \langle x_1, \ldots, x_n, f \rangle$. Thus overall we have that $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$.

§5.12 Suppose that every ascending chain of ideals in $k[x_1, \ldots, x_n]$ eventually stabilizes. Suppose that some ideal I has no finite generating set. Then we may define a series of ascending ideals as follows. Let $I_1 = \langle g_1 \rangle$ for some $g_1 \in I$. Then for $n \geq 2$ we define $I_n = \langle g_1, \ldots, g_{n-1}, g_n \rangle$ where $g_n \notin \langle g_1, \ldots, g_{n-1} \rangle$. We know such g_n must exist since I has no finite generating set. Then we get the following chain of ideals:

$$I_1 \subsetneq I_2 \subsetneq \cdots$$

However, the existence of this chain contradicts the ascending chain condition. Thus such an infinite chain cannot exist. Thus and infact we must have that for some $N \in \mathbb{N}$ that $I_N = I_{N+1} = \cdots$. Thus we have a finite generating set $I = \langle g_1, \ldots, g_N \rangle$, proving the Hilbert Basis Theorem.

§5.13 Since $V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$, then we know that $\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \mathbf{I}(V_3) \subseteq \cdots$. Thus by the Ascending Chain Condition we have that for some $N \in \mathbb{N}$ that $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \mathbf{I}(V_{N+2}) = \cdots$. Thus we have $V_N = V_{N+1} = \cdots$.

§5.15 Let $V_i = \mathbf{V}(f_1, \ldots, f_i)$. Clearly $V_j \subseteq V_i$ whenever $j \geq i$. Then we have $\mathbf{I}(V_i) \subseteq \mathbf{I}(V_j)$ whenever $j \geq i$. Thus we have that

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \mathbf{I}(V_3) \cdots .$$

By the Ascending Chain Condition, this must stabilize at some $\mathbf{I}(V_N)$ and that $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots = \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots))$. Thus we have that $V_N = V_{N+1} = \cdots = \mathbf{V}(f_1, f_2, \ldots)$.

§5.16 Let $V \subseteq k^n$ be some variety. Suppose we have $(a_1, \ldots, a_n) \in V$. Then by definition of $\mathbf{I}(V)$, we have that for all $f \in \mathbf{I}(V)$ that $f(a_1, \ldots, a_n) = 0$ and thus $(a_1, \ldots, a_n) \in \mathbf{V}(\mathbf{I}(V))$.

We have that $V = \mathbf{V}(S)$ for some set of polynomials $S \subseteq k[x_1, \ldots, k_n]$. Then let I be the ideal generated by S, which by the Hilbert Basis Theorem can be finitely generated. Thus we have that $V = \mathbf{V}(f_1, \ldots, f_s)$ for some polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Thus $\mathbf{V}(\mathbf{I}(V)) = \mathbf{V}(\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)))$. We have that $\mathbf{V}(\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))) \subseteq \mathbf{V}(f_1, \ldots, f_s)$ if and only if $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ which we know is true. Thus overall we have that $\mathbf{V}(\mathbf{I}(V)) = V$.

§6.1

a. Let $G = \{ g_1, \ldots, g_t \}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$. Let $f \in k[x_1, \ldots, x_n]$. Then we have that on division of f by G that $f = q_1 g_1 + \cdots + q_n g_n + r$ such that $r, q_i \in k[x_1, \ldots, x_n]$. Furthermore, no term of r is divisible by any of the $\text{LT}(g_i)$. Since $I = \langle g_1, \ldots, g_t \rangle$ we have that $q_1 g_1 + \cdots + q_t g_t \in I$. Furthermore, since no term of r is divisible by any term of $\text{LT}(g_i)$ and $\langle \text{LT}(I) \rangle$ is a monomial ideal generated by the $\text{LT}(g_i)$'s, no term of r is divisible by any term in $\text{LT}(I)$.

b. Now suppose that $f = g + r = g' + r'$ satisfying **a.** such that $r \neq r'$. Then $g - g' \in I \implies r' - r \in I$. Thus $\text{LT}(r' - r) \in \langle \text{LT}(I) \rangle$ which implies some $\text{LT}(g_i)$ divides $r - r'$ which in turn some element in $\text{LT}(I)$ divides $r - r'$. This is impossible and thus we must have that $r = r'$.

§6.3 Suppose that $G = \langle g_1, \ldots, g_t \rangle$ is a basis with the property such that for all f in a polynomial ideal I we have that $\overline{f}^G = 0$. Note that for all $g_i, g_j \in G$, we have that $S(g_i, g_j) \in I$. Then since $\overline{G(g_i, g_j)}^G = 0$, Buchberger's Criterion, we have that G is a Gröbner basis.

§6.13

a. Suppose $\overline{f}^G = \overline{g}^G$. Then we have that $f = p + r$ and $g = q + r$ for some $p, q \in I$ and $r \in k[x_1, \ldots, x_n]$. Then we have that $f - g = p + r - q - r = p - q \in I$.

b. We have that for $f, g \in k[x_1, \ldots, x_n]$ that $f = p + r$ for $p \in I$ and r such that no term of r is divisible by any element of $\text{LT}(I)$. Similarly write g as $g = q + s$. Then we have that $\overline{f}^G + \overline{g}^G = r + s$. Clearly we can write $f + g = (p + q) + (r + s)$. Since $p, q \in I$ we have that $p + q \in I$. Then since no term of r or s is divisible by any term in $\text{LT}(I)$, we have that no term of $r + s$ is divisible by any term of $\text{LT}(I)$. Thus by **§6.1** we have that $\overline{f + g}^G = r + s = \overline{f}^G + \overline{g}^G$.

c. We can write $f = p + r$ and $g = q + s$ where $p, q \in I$ and none of the terms of r, s are divisible by any leading term of any element of I. Thus, $\overline{fg}^G = \overline{(p + r)(q + s)}^G = \overline{pq}^G + \overline{qr}^G + \overline{ps}^G + \overline{rs}^G$. Clearly $\overline{pq}^G = \overline{qr}^G = \overline{ps}^G = 0$ and so we just need to show that $\overline{\overline{f}^G \overline{g}^G}^G = \overline{rs}^G$. However since these remainders are unique, we have that $\overline{f}^G = r$ and $\overline{g}^G = s$ and the claim is proven.

§7.2

a. Lex order: $\{ x^2 - y, x^2 y - 1, y^2 - 1, x y^2 - x \}$

Grlex order: $\{ x^2 - y, x^2 y - 1, y^2 - 1, x y^2 - x \}$

b. Lex order: $\{ x^2 + y, -3, x^4 + 2x^2 y + y^2 + 3 \}$

Grlex order: $\{ x^2 + y, -3, x^4 + 2x^2 y + y^2 + 3 \}$

Since $-3 \in I$ then $1 \in I$ and thus $I = \mathbb{Q}[x, y]$ and $\mathbf{V}(I) = \emptyset$

c. Lex order: $\{ y - z^5, x - z^4 \}$

Grlex order: $\{ yz^3 - x^2, -y^2 z^2 + x^3, x^4 - y^3 z, xz - y, -z^5 + y, -z^4 + x \}$

§7.5 let I be a polynomial ideal and let G be a Gröbner basis for I with the property that $\text{LC}(g) = 1$ for all $g \in G$. Suppose G is a minimal Gröbner basis. Let $H \subsetneq G$ be a proper subset. Then there is some polynomial $p \in G$ such that $p \notin H$. Suppose that H was a Gröbner basis for I. Then we would have that $p \in \langle H \rangle$. Then in particular we would have that $\text{LT}(p) \in \langle \text{LT}(G \setminus \{ p \}) \rangle$. This contradicts the minimality of G and thus we must have that H cannot be a Gröbner basis for G.

Now suppose that no proper subset of G can be a Gröbner basis for I. Then that means for all $\text{LT}(H) \subsetneq \text{LT}(G)$ we have that $\langle \text{LT}\, H \rangle \neq \langle \text{LT}(I) \rangle$. Thus G must be a minimal Gröbner basis for I.

§7.7

a. Let I be a polynomial ideal and let $G = \langle g_1, \ldots, g_t \rangle, \tilde{G} = \langle g'_1, \ldots, g'_s \rangle$ be minimal Gröbner bases for I. Since $\tilde{G}$ is a Gröbner basis for I, we can apply this to some get $\text{LT}(g_i)$ to yield that $\text{LT}(g'_k) \mid \text{LT}(g_i)$ for some $\text{LT}(g'_k)$. Similarly, we have that some $\text{LT}(g_l) \mid \text{LT}(g'_k)$. Thus we have that $\text{LT}(g_\ell) \mid \text{LT}(g_i)$. But G is minimal and so we must have that $\ell = i$. Thus $\text{LT}(g_i) = c\,\text{LT}(g'_k)$ for some non-zero constant c. By minimality of G and $\tilde{G}$, we have that $c = 1$ and thus $\text{LT}(g_i) = \text{LT}(g'_k) \in G'$. This implies that $\text{LT}(G) \subseteq \text{LT}(\tilde{G})$. The proof for the reverse direction is symmetric and overall we have that $\text{LT}(G) = \text{LT}(\tilde{G})$.

b. Note that every element in G has a unique leading term since if two elements had the same leading term this would contradict minimality. Since $\text{LT}(G) = \text{LT}(\tilde{G})$, we can match elements by their leading term. Thus the sets have the same number of elements.

§7.8 Given an ideal I, we may compute a Gröbner basis G using Buchberger's Algorithm. Then we may turn G into a minimal basis using **Lemma 3** from **§7**. Since G is a finite set and $\langle \text{LT}(G) \rangle$ is a monomial ideal, this is a finite process. Thus we now have that G is a minimal Gröbner basis for I. Since all leading coefficients of the polynomials in G are 1, we only need to make it so that for all $p \in G$, no term of p lies in $\langle \text{LT}(G \setminus \{p\}) \rangle$. To do this, we just need to replace elements in G with fully reduced elements. We may do this using the process in the proof of **Theorem 5** in **§7**. This is a finite process since once we replace an element with a fully reduced element, that fully reduced element is fully reduced in any minimal Gröbner basis and the process in the proof retains minimality.

§7.9 **⟨⟨ Sage cannot do multivariate division and I do not want to learn Singular or Macaulay2 ⟩⟩**

§7.10

a. Suppose we replace $g_i \in G = \{g_1, \ldots, g_t\}$ with $a \cdot g_i + b \cdot g_t$, $i \neq j$, $a, b \neq 0 \in k$. Let G' be the resulting set. Then clearly $g_\ell \in \langle G' \rangle$ for $\ell \neq i$. Then note that since $j \neq i$, g_j and thus $b \cdot g_j \in \langle G' \rangle$. Thus $a \cdot g_i + b \cdot g_j - b \cdot g_j = a \cdot g_i \in \langle G' \rangle$. Then we have that $a^{-1}a \cdot g_i = g_i \in \langle G' \rangle$. Thus $\langle G' \rangle$ generates I.

b. Let g_i and g_j, $i \neq j$, be rows in B. Suppose the leading 1 in the ith row of B is in column s. Then we can write $g_i = x_s + C$ as described in the hint. Similarly, we may write $g_j = x_\ell + D$. Note that $\operatorname{lcm}(\textsc{lm}(g_i), \textsc{lm}(g_j)) = x_s x_\ell$. Thus we have that

$$\begin{aligned} S(g_i, g_j) &= \frac{x_s x_\ell}{x_s}(x_s + C) - \frac{x_s x_\ell}{x_\ell}(x_\ell + D) \\ &= x_\ell x_s + x_\ell C - x_s x_\ell - x_s D \\ &= x_\ell C - x_s D \end{aligned}$$

Carrying out the long division of $x_\ell C - x_s D$ by $\{ x_s + C, x_\ell + D \}$ yields that the remainder is zero. Thus by Buchberger's criterion, G is a Gröbner basis.

c. Let G again be the Gröbner basis defined by the rows of B. Clearly by the definition of row reduced echelon form, the leading coefficients of each polynomial in G is 1. Let $g_i = x_s + C$ as before. Consider $X = \langle \textsc{lt}(G \setminus \{ g_i \}) \rangle$. This consists of just leading terms of the rows, and thus only consists of x_ℓ corresponding to leading 1's. Thus we have that $x_s \notin X$. Furthermore, we have that none of the terms in C contain variables corresponding to leading 1's by definition and thus no terms of C are in X. Thus G is the reduced Gröbner basis.

§7.11 Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^i$ be polynomials in $k[x]$ and without loss of generality suppose $n \geq m$. Then we have that $\operatorname{lcm}(\textsc{lm}(f), \textsc{lm}(g)) = x^n$. Thus we have

$$\begin{aligned} S(f, g) &= \frac{x^n}{\textsc{lt}(f)} * f - \frac{x^n}{\textsc{lt}(g)} g \\ &= \frac{x^n}{a_n x^n} f - \frac{x^n}{b_m x^m} g \\ &= \frac{1}{a_n} f - \frac{x^n}{b_m x^m} g \\ &= \frac{1}{a_n}\left(f - \frac{a_n x^n}{b_m x^m} g \right) \\ &= \frac{1}{a_n}\left(f - \frac{\textsc{lt}(f)}{\textsc{lt}(g)} g \right). \end{aligned}$$

However, note that the first the first step of the Euclidian Algorithm is to compute $r_1 = f - \frac{\textsc{lt}(f)}{\textsc{lt}(g)} g$. So these steps are the same up to a constant.

§8.8

a. The following image is a plot of the parametric surface T:

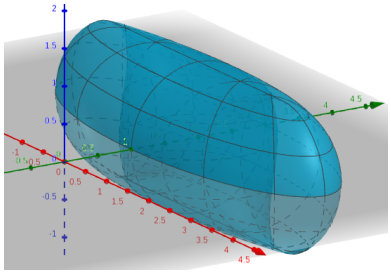

Figure 2: Plot of $((2\cos(t))\cos(u), (2+\cos(t))\sin(u), \sin(t))$ for $0 \leq t, u \leq 2\pi$.

b. Let $a = \cos(t), b = \sin(t), c = \cos(u)$ and $d = \sin(u)$. Then we have

$$\begin{aligned} x &= (2+\cos(t))\cos(u) = (2+a)c \\ y &= (2+\cos(t))\sin(u) = (2+a)d \\ z &= \sin(t) = b \end{aligned}$$

c. The following is a Gröbner basis for the ideal $\left\langle x-(2+a)c, y-(2+a)d, z-b, a^2+b^2-1, c^2+d^2-1 \right\rangle$:

$$\begin{aligned} &\{-ad-2d+y, \\ &dz^2+3d+\frac{1}{4}x^2y+\frac{1}{4}y^3+\frac{1}{4}yz^2-\frac{13}{4}y, \\ &-4cx-4dy+x^2+y^2+z^2+3, \\ &cdx+d^2y-y, \\ &-ac-2c+x, \\ &-cdz^2-3cd+4dx-xy, \\ &-a+cx+dy-2, \\ &\frac{1}{4}dx^2y+\frac{1}{4}dy^3+\frac{1}{4}dyz^2+\frac{3}{4}dy-y^2, \\ &-\frac{1}{4}x^4-\frac{1}{2}x^2y^2-\frac{1}{2}x^2z^2+\frac{5}{2}x^2-\frac{1}{4}y^4-\frac{1}{2}y^2z^2+\frac{5}{2}y^2-\frac{1}{4}z^4-\frac{3}{2}z^2-\frac{9}{4}, \\ &ax+cz^2+3c-2x, \\ &\frac{1}{4}dx^2+\frac{1}{4}dy^2+\frac{1}{4}dz^2+\frac{3}{4}d-y, \\ &c^2+d^2-1, \\ &a^2+b^2-1, \\ &cz^2+3c+\frac{1}{4}x^3+\frac{1}{4}xy^2+\frac{1}{4}xz^2-\frac{13}{4}x, \\ &-cy+dx, \\ &-b+z\} \end{aligned}$$

§8.11

a. Let $I = \left\langle a+b+c-3, a^2+b^2+c^2-5, a^3+b^3+c^3-7 \right\rangle$. We use the Ideal Membership Problem to compute if $a^4+b^4+c^4-9 \in I$ and see that this is true. Thus, $a^4+b^4+c^4 = 9$.

b. Similar to part **a.** we use the Ideal Membership Problem and see that $a^5+b^5+c^5-11 \notin I$.

c. To compute $a^5+b^5+c^5$, we divide this polynomial by a Gröbner basis for I and see that on division by this Gröbner basis, $a^5+b^5+c^5 = \frac{29}{3}$. Similarly we have that $a^6+b^6+c^6 = \frac{19}{3}$.

§9.3 Let f, g be elements of a basis for I such that the leading monomials of each element in the basis are coprime. If $\gcd(\text{LM}(f), \text{LM}(g)) = 1$ then we have that $\text{lcm}(\text{LM}(f), \text{LM}(g)) = \text{LM}(f)\,\text{LM}(g)$. Thus we have $S(f,g) = \frac{\text{LM}(f)\,\text{LM}(g)}{\text{LC}(f)\,\text{LM}(f)} f - \frac{\text{LM}(f)\,\text{LM}(g)}{\text{LC}(g)\,\text{LM}(g)} g = \frac{\text{LM}(g)}{\text{LC}(f)} f - \frac{\text{LM}(f)}{\text{LC}(g)} g$. This implies that $S(f,g) \to_G 0$ and thus by **Theorem 3** of **§9** we have that G is a Gröbner basis for I.