UFRJ

Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra - Some Solutions

Kevin Alves Vasconcellos

These notes contain solutions of some exercises of the book: **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra - Some Solutions**, by David A. Cox, John Little and Donal O'shea.

Kevin Alves Vasconcellos[1]

[1]M.Sc in Mathematics // E-mail: kevin.vasconcellos@ufrj.br // Webpage: www.im.ufrj.br/alunos/kevinvasconcellos

Contents

Chapter 1

Geometry, Algebra, and Algorithms

1.1 Polynomials and Affine Space

Question 1.1.2: Consider the field $\mathbb{F}_2$.

(i) Consider the polynomial $g(x, y) = x^2y + y^2x \in \mathbb{F}_2[x, y]$. Show that $g(x, y) = 0$ for all $(x, y) \in \mathbb{F}_2^2$. Explain why this fact does not contradict the Proposition 5.

(ii) Find a nonzero polynomial in $\mathbb{F}_2[x, y, z]$ which vanishes at every point of $\mathbb{F}_2^3$.

(iii) Find a nonzero polynomial in $\mathbb{F}_2[x_1, x_2, \dots, x_n]$ which vanishes at every point of $\mathbb{F}_2^n$.

Solution: **(i)** In fact

$$g(0,0) = 0 + 0 = 0;$$
$$g(0,1) = 0 + 0 = 0;$$
$$g(1,0) = 0 + 0 = 0;$$
$$g(1,1) = 1 + 1 = 0.$$

This fact does not contradict the Proposition 5, because $\mathbb{F}_2$ is a finite field, while the Proposition 5 requires that the ground field be infinite.

(ii) Consider the polynomial

$$f_3(x, y, z) = xyz(x-1)(y-1)(z-1).$$

Clearly we have that f_3 is a nonzero polynomial and that $f_3(a, b, c) = 0$ for all $(a, b, c) \in \mathbb{F}_2^3$.

(iii) Consider the polynomial

$$f_n(x_1, \ldots, x_n) = \prod_{k=1}^{n} x_k \prod_{k=1}^{n} (x_k - 1)$$

Clearly we have that f_n is a nonzero polynomial and that $f_n(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$. $\square$

Question 1.1.6: Denote $\mathbb{Z}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \ ; \ x_i \in \mathbb{Z} \, \forall \, i = 1, \ldots, n\}$.

(i) Prove that if $f \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at every point of $\mathbb{Z}^n$, then f is the zero polynomial.

(ii) Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and M the largest power of any variable that appears in f. Define

$$\mathbb{Z}_{M+1}^n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \ ; \ x_i \in \{1, \ldots, M+1\} \, \forall \, i = 1, \ldots, n\}.$$

Prove that if f vanishes at all points of $\mathbb{Z}_{M+1}^n$, then f is the zero polynomial.

Solution: **(i)** We will proceed by induction on the number of variables. Consider $n = 1$. Since $\mathbb{Z}$ is infinite, it is clear that if $f \in \mathbb{C}[x]$ has vanishes at every point of $\mathbb{Z}$, then $f = 0$. Suppose this fact holds for polynomials in $n-1$ variables and let $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{Z}^n$.

Note that we can rewrite f as

$$f(x_1, \ldots, x_n) = \sum_{k=0}^{t} g_k(x_1, \ldots, x_{n-1}) x_n^k,$$

where each $g_i \in \mathbb{C}[x_1, \ldots, x_{n-1}]$. Thus f is the zero polynomial if and only if each g_k is the zero polynomial. We will show this! Let $z = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{Z}^{n-1}$ and consider the polynomial

$$h_z(x_n) = \sum_{k=0}^{t} g_k(z) x_n^k \in \mathbb{C}[x_n]$$

Since $h_z(x_n) = 0$ for all $x_n \in \mathbb{Z}$, we conclude that $g_0(z) = \cdots = g_t(z) = 0$. Finally since z was chosen arbitrarily in $\mathbb{Z}^{n-1}$, the induction hypothesis tell us that $g_0 = \cdots = g_t = 0$ and so $f = 0$.

(ii): Again we will proceed by induction on the number of variables. Consider $n = 1$ and let $f \in \mathbb{C}[x_1]$. In this case M is exactly the degree of f. If f were nonzero, the Algebra Fundamental Theorem would say us that f has at most M distinct roots. Since f vanishes at $1, \ldots, M, M+1$ by hypothesis, then necessarily we get that $f = 0$. Suppose this fact holds for polynomials in $n-1$ variables and let $f \in \mathbb{C}[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{Z}_M^n$. Suppose that the largest power M appears on x_i

Note that we can rewrite f as

$$f(x_1,\ldots,x_n)=\sum_{k=0}^{M} g_k(x_1,\ldots,\hat{x_i},\ldots,x_{n-1})x_i^k,$$

where each $g_k\in\mathbb{C}[x_1,\ldots,\hat{x_i},\ldots,x_n]$. Thus f is the zero polynomial if and only if each g_k is the zero polynomial. We will show this! Let $z=(a_1,\ldots,\hat{a_i},\ldots,a_n)\in\mathbb{Z}^{n-1}$ and consider the polynomial

$$h_z(x_i)=\sum_{k=0}^{M} g_k(z)x_i^k\in\mathbb{C}[x_i].$$

Again $h_z(x_i)$ has at most M distinct roots. Since h_z vanishes at $1,\ldots,M,M+1$, we conclude that $h_z=0$ and so $g_0(z)=\cdots=g_M(z)=0$.

Here we have to note important point: For each $k=0,1,\ldots,M$, the largest power which appears on $g_k(x_1,\ldots,\hat{x_i},\ldots,x_n)$ is less or equal to M, which allows us to apply induction hypothesis. Thus since z was chosen arbitrarily in $\mathbb{Z}_M^{n-1}$, the induction hypothesis tell us that $g_0=\cdots=g_t=0$ and so $f=0$. $\square$

1.2 Affine Varieties

Question 1.2.5: Sketch

$$\mathrm{V}((x-2)(x^2-y),y(x^2-y),(z+1)(x^2-y))\subseteq\mathbb{R}^3$$

Solution: Note that

$$\mathrm{V}((x-2)(x^2-y),y(x^2-y),(z+1)(x^2-y))=\mathrm{V}(x^2-y)\cup\mathrm{V}(x-2,y,z+1).$$

Now it is easy to plot. $\square$

Question 1.2.6: Let k be an arbitrary field.

(i) Prove that a single point $\{(a_1,\ldots,a_n)\}\in k^n$ is an affine variety.

(ii) Prove that every finite subset of k^n is an affine variety.

Solution: **(i):** Note that

$$\{(a_1,\ldots,a_n)\}=\mathrm{V}(x_1-a_1,\ldots,x_n-a_n),$$

thus $\{(a_1,\ldots,a_n)\}$ is an affine variety.

(ii): Let $Z = \{P_1, \ldots, P_m\} \subseteq k^n$. Note that $Z = \bigcup_{i=1}^{m} \{P_i\}$. Since $\{P_i\}$ is an affine variety for each $i = 1, \ldots, n$ and finite union of affine varieties is an affine variety, Z is an affine variety. $\square$

Question 1.2.8: Prove that

$$X = \{(x, x) \in \mathbb{R}^2 \ ; \ x \neq 1\} \subseteq \mathbb{R}^2$$

is not an affine variety.

Solution: Suppose by contradiction that X is an affine variety, that is, $X = \mathrm{V}(f_1, \ldots, f_m)$. Thus $f_i(z) = 0$ for all $z \in X$ and there exists $j \in \{1, \ldots, m\}$ such that $f_j(1,1) \neq 0$. Considering the standard topology of $\mathbb{R}^2$, we have that $(1,1)$ is an accumulation point of X. Since the two-variable polynomials are continuous functions on $\mathbb{R}^2$ and that $f_j(z) = 0$ for all $z \in X$, by continuity, we conclude that $f_j(1,1) = 0$, which is a contradiction. $\square$

Question 1.2.9: Prove that

$$R = \{(x, y) \in \mathbb{R}^2 \ ; \ y > 0\} \subseteq \mathbb{R}^2$$

is not an affine variety.

Solution: Suppose by contradiction that R is an affine variety. Thus $R = \mathrm{V}(f_1, \ldots, f_m)$ for some polynomials $f_1, \ldots, f_m \in \mathbb{R}[x, y]$. Note there is $j \in \{1, \ldots, m\}$ such that $f_j(0, t) = 0$ for all $t > 0$ and $f_j(0,0) \neq 0$. Using the standard topology of $\mathbb{R}^2$ again, the fact that f_j is a continuous function and that

$$(0,0) = \lim_{t \to 0^+} (0, t),$$

we have that

$$f(0,0) = \lim_{t \to 0^+} f(0,t) = 0,$$

which gives us a contradiction. $\square$

Question 1.2.10: Prove that $\mathbb{Z}^n \subseteq \mathbb{C}^n$ is not an affine variety.

Solution: We saw that if $f \in \mathbb{C}[x_1, \ldots, x_n]$ is a polynomial which vanishes on $\mathbb{Z}^n$, then f vanishes everywhere. Thus, if $V(f_1, \ldots, f_m)$ is an affine variety which contains $\mathbb{Z}^n$, then

$$V(f_1, \ldots, f_m) = \bigcap_{i=1}^{m} \mathrm{V}(f_i) = \bigcap_{i=1}^{m} \mathbb{C}^n = \mathbb{C}^n \neq \mathbb{Z}^n.$$

Thus $\mathbb{Z}^n$ is not an affine variety. $\square$

Question 1.2.15: Let k be an arbitrary field.

(i) Prove that finite unions and intersection of affine varieties are again affine varieties.

(ii) Give an example to show that finite union of affine varieties need not be to be an affine variety.

(iii) Give an example to show that the set-theoretic difference $V \setminus W$ of two affine varieties need not be an affine variety.

(iv) Let $V \subseteq k^n$ and $W \subseteq k^m$ be affine varieties, and let

$$V \times W = \{(x_1, \dots, x_n, y_1, \dots, y_m) \in k^{n+m} \ ; \ (x_1, \dots, x_n) \in V, \ (y_1, \dots, y_m) \in W\}$$

be the Cartesian product. Prove that $V \times W$ is an affine variety in k^{n+m}.

Solution: **(i)** We will proceed by induction on m that the union and intersection of m affine varieties are again affine varieties. For $m = 1$, we are done. It has already proved for $m = 2$. Suppose that this fact holds for $m \in \mathbb{N}$ and let $V_1, \dots, V_m, V_{m+1}$ be $m+1$ affine varieties. Note that

$$\bigcup_{k=1}^{m+1} V_k = \left(\bigcup_{k=1}^{m} V_k\right) \cup V_{m+1} \qquad \text{and} \qquad \bigcap_{k=1}^{m+1} V_k = \left(\bigcap_{k=1}^{m} V_k\right) \cap V_{m+1}.$$

By induction hypothesis $\bigcup_{k=1}^m V_k$ and $\bigcap_{k=1}^m V_k$ are affine varieties, so, returning to the case $m = 2$, we conclude that these union and intersection are affine varieties.

(ii): If the arbitrary union of affine varieties was an affine variety, then

$$R = \bigcup_{x \in \mathbb{R}^*} \{(x, x)\} = \Delta \setminus \{(0, 0)\} \subseteq \mathbb{R}^2$$

would be an affine variety. However we already proved that R is not an affine variety.

(iii): Consider $V = \Delta = \mathrm{V}(x - y) \subseteq \mathbb{R}^2$ and $W = \{(0, 0)\} = \mathrm{V}(x, y) \subseteq \mathbb{R}^2$. We already proved that $V \setminus W$ is not an affine variety.

(iv): Indeed denote $V = \mathrm{V}(f_1, \dots, f_r) \subseteq k^n$ with $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ and $W = \mathrm{V}(g_1, \dots, g_s) \subseteq k^m$ with $g_1, \dots, g_s \in k[y_1, \dots, y_m]$. Firstly observe that we can naturally inject $k[x_1, \dots, x_n]$ and $k[y_1, \dots, y_m]$ in $k[x_1, \dots, x_n, y_1 \dots, y_m]$, thus we can consider $f_1, \dots, f_r, g_1, \dots, g_s$ as polynomials in $k[x_1, \dots, x_n, y_1 \dots, y_m]$. Now it is easy to see that

$$V \times W = \mathrm{V}(f_1, \dots, f_r, g_1, \dots, g_s) \subseteq k^{n+m},$$

so $V \times W$ is an affine variety. $\square$

1.3 Parametrizations of Affine Varieties

Question 1.3.2: Show that the curve

$$\gamma : \mathbb{R} \longrightarrow \mathbb{R}^2$$

$$t \longmapsto (\cos(t), \cos(2t))$$

parametrizes a portion of a parabola. Indicate exactly what portion of the parabola is covered.

Solution: We know that $\cos(2t) = \cos^2(t) - \sin^2(t)$. Thus calling

$$\begin{cases} y = y(t) = \cos(2t); \\ x = x(t) = \cos(t). \end{cases}$$

we obtain that

$$y = \cos^2(t) - \sin^2(t) = 2\cos^2(t) - 1 = 2x^2 - 1.$$

So γ parametrizes part of parabola the $\mathrm{V}(y - 2x^2 + 1) \subseteq \mathbb{R}^2$. Since x ranges from -1 to 1, we conclude that γ parametrizes the portion

$$\{(x, 2x^2 - 1) \in \mathbb{R}^2 \ ; \ x \in [-1, 1]\} \subseteq \mathrm{V}(y - 2x^2 + 1).$$

Question 1.3.4 Consider the parametric representation

$$\begin{cases} x = x(t) = \frac{t}{1+t}; \\ y = y(t) = 1 - \frac{1}{t^2}. \end{cases}$$

(i) Find the equation of the affine variety determined by the above parametric equations.

(ii) Show that the above equations parametrize all points of the variety found in part (i) except for the point $(1, 1)$.

Solution: (i) Note that

$$y = \frac{t^2 - 1}{t^2} = \frac{(t+1)(t-1)}{t^2} = \left(\frac{(t+1)(t-1)}{t^2}\right)\frac{t+1}{t+1} = \left(\frac{(t+1)}{t}\right)^2\left(\frac{t-1}{t+1}\right) = \frac{1}{x^2}\frac{t-1}{t+1}.$$

Thus

$$x^2 y = \frac{t-1}{t+1} = \frac{t}{t+1} - \frac{1}{t+1} = x - \frac{1}{t+1},$$

which implies that $\frac{1}{t+1} = x - x^2y$. Multiplying by t, we obtain

$$x = \frac{t}{t+1} = (x - x^2y)t,$$

Note that $x(t)$ can not be zero for any t, thus $\frac{1}{t} = 1 - xy$. Finally

$$y = 1 - \frac{1}{t^2} = 1 - (1 - xy)^2,$$

which implies that these functions parametrizes a portion of $V = \mathrm{V}((1 - xy)^2 + y - 1)$

(ii): Firstly note that $(1, 1)$ is not at image of parametrization. In fact, if we have

$$\begin{cases} 1 = \frac{t}{1+t}; \\ 1 = 1 - \frac{1}{t^2}, \end{cases}$$

we would obtain that $1/t^2 = 0$, which is an absurd. Now suppose $(a, b) \in \mathrm{V}((1 - xy)^2 + y - 1)$ with $(a, b) \neq 1$. Take $t_a = a/(1 - a)$, then we can check that $b = y(t_a)$. $\square$

Question 1.3.7: Parametrize the sphere S in n-dimensional affine space

$$S = \{(x_1, \ldots, x_n) \in k^n \ ; \ x_1^2 + \cdots + x_n^2 = 1\}.$$

Solution: Denote $N = (0, \ldots, 0, 1)$ the North Pole of S and let $P = (x_1, \ldots, x_{n-1}, 0) \in \mathrm{V}(x_n) \subseteq k^n$. It is easy to see that

$$\begin{aligned} \sigma : k &\longrightarrow k^n \\ t &\longmapsto N + (P - N)t = (x_1 t, \ldots, x_{n-1}t, 1 - t) \end{aligned}$$

parametrizes the line passing by N and P. Observe tha $\sigma(t_0)$ intersect S if and only if

$$(x_1 t_0)^2 + \cdots + (x_{n-1}t_0)^2 + (1 - t_0)^2 = 1,$$

that is, if and only if

$$t_0 = \frac{2}{x_1^2 + \cdots + x_{n-1}^2 + 1} \qquad \text{or} \qquad t = 0.$$

Note that $\sigma(0) = N$, so considering only the case where $t_0 \neq 0$, we can construct a map $\Psi : k^{n-1} \longrightarrow S$ such that

$$\Psi(x_1, \ldots, x_{n-1}) = \left(\frac{2x_1}{x_1^2 + \cdots + x_{n-1}^2 + 1}, \ldots, \frac{2x_{n-1}}{x_1^2 + \cdots + x_{n-1}^2 + 1}, \frac{x_1^2 + \cdots + x_{n-1}^2 - 1}{x_1^2 + \cdots + x_{n-1}^2 + 1} \right).$$

Note that $\mathrm{Im}(\Psi) = S \setminus \{N\}$ $\square$

Question 1.3.8: Consider the algebraic curve $C = \mathrm{V}(x^3 - cx^2 + x^3) \subseteq \mathbb{R}^2$, where $c > 0$

(i) Show that a line meet this curve at either $0, 1, 2$, or 3 points.

(ii) Show that a nonzero line through the origin $\mathrm{V}(y - mx)$ meets this curve at exactly one other point when the $c \neq m^2$.

(iii) Show that

$$\begin{cases} x = x(t) = c - t^2; \\ y = y(t) = t(c - t^2) \end{cases}$$

parametrizes C.

Solution: **(i):** Let ℓ be a line in $\mathbb{R}^2$. If $\ell = \mathrm{V}(x - a)$, then

$$\ell \cap C = \{(a, t) \ ; \ t \in \mathbb{R} \, , \, t^2 = ca^2 - a^3\}.$$

Thus $\ell \cap C$ has at most two points. If $\ell = \mathrm{V}(y - mx - b)$, then

$$\ell \cap C = \{(t, mt + b) \ ; \ t \in \mathbb{R} \, , \, t^3 + (m^2 - c)t^2 + 2mbt + b^2 = 0\}.$$

Thus $\ell \cap C$ has at most three points.

ii: Consider ℓ_m the line $\mathrm{V}(y - mx)$, with $m^2 \neq c$. Note that

$$\ell_m \cap C = \{(0, 0), \ (0, m^2 - c)\}.$$

Thus, if $m^2 \neq c$, ℓ_m will meet C at the point $(0, m^2 - c)$ outside from origin.

(iii): Consider the line $\ell = \mathrm{V}(x = 1)$ and let $(1, t) \in \ell$. Consider now the line $\ell_t = \mathrm{V}(y - tx)$. Note that $\ell_t \cap C$ if and only if $x = 0$ or $x = c - t^2$. Thus setting $x := x(t) = c - t^2$, we obtain

$$y^2 = c(c - t^2)^2 - (c - t^2)^3 = t^2(c - t^2)^2 = t^2(c - t^2)^2,$$

which implies that $|y| = |t(c - t^2)|$. Finally note that this curve is symmetric with respect the $0X$-axis and that

$$\begin{cases} x(t) = c - t^2, \\ y(t) = |t(c - t^2)| \end{cases}$$

will parametrizes the upper portion of C. If we drop the modulus, we conclude that

$$\begin{cases} x(t) = c - t^2, \\ y(t) = t(c - t^2) \end{cases}$$

parametrizes C. $\square$

Question 1.3.8: Consider the algebraic surface $V = \mathrm{V}(x^2 - y^2z^2 + z^3)$.

(i) Show that the curve $x^2 = cz^2 - z^3$ is parametrized by

$$\begin{cases} z = c - t^2; \\ x = t(c - t^2) \end{cases}$$

(ii) From part (i), prove that

$$\begin{cases} x = t(u^2 - t^2); \\ y = u; \\ z = u^2 - t^2 \end{cases}$$

parametrizes $x^2 - y^2z^2 + z^3 = 0$.

(iii) Prove that this parametrization covers the entire surface V.

Solution: **(i):** Observe that $x^2 = (y^2)z^2 - z^3$. Calling $y^2 = c$, we have that $x^2 = cz^2 - z^3$. So, using the Question 1.3.8, we get that

$$\begin{cases} z = c - t^2; \\ x = t(c - t^2) \end{cases}$$

parametrizes $C_c = \mathrm{V}(x^2 - cz^2 + z^3)$.

(ii): As $u := c$ ranges over $\mathbb{R}$, the family of curves $\{C_u\}_{u\in\mathbb{R}}$ generates the surface V, so

$$\begin{cases} x = t(u^2 - t^2); \\ y = u; \\ z = u^2 - t^2 \end{cases}$$

parametrizes V. However there is a delicate case when $u = 0$: the parametrization constructed on Question 1.3.8 considered only the case when $c \neq 0$. $\square$

1.4 Ideals

Question 1.4.9: Let $V = \mathrm{V}(y-x^2, z-x^3)$ be the twisted cubic. Consider that $\mathrm{I}(V) = \langle y-x^2, z-x^3\rangle$.

(i) Show that $y^2 - xz \in \mathrm{V}(V)$;

(ii) Express $y^2 - xz$ as polynomial combination of $y - x^2$ and $z - x^3$.

Solution: **(i):** Note that

$$\begin{cases} x = t \\ y = t^2 \\ z = t^3 \end{cases}$$

is a parametrization of V. Thus, since

$$(t^2)^2 - (t)t^3 = 0$$

for all $t \in k$, we conclude that $y^2 - xz \in \mathrm{I}(V)$.

(ii): Using the division algorithm with lexicographic order $z > y > x$, we get that

$$y^2 - xz = (y + x^2)(y - x^2) - x(z - x^3) \in \mathrm{I}(V).$$

$\square$

Question 1.4.11: Let $V \subseteq \mathbb{R}^3$ be the curve parametrized by (t, t^3, t^4)

(i) Prove that V is an affine variety.

(ii) Determine $\mathrm{I}(V)$.

Solution: **(i):** I claim that $V = \mathrm{V}(y - x^3, z - x^4)$. In fact, we easily can check that

$$\{(t, t^3, t^4) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\} \subseteq V.$$

Now let $(a, b, c) \in \mathrm{V}(y - x^3, z - x^4)$, then

$$\begin{cases} b = a^3 \\ c = a^4 \end{cases}$$

So, taking $t_0 = a$, we have $(a, b, c) = (t_0, t_0^3, t_0^4) \in \{(t, t^3, t^4) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\}$, which implies that

$$\{(t, t^3, t^4) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\} = V.$$

Thus V is an affine variety.

(ii): Note that $\langle y - x^3, z - x^4 \rangle \subseteq \mathrm{I}(\mathrm{V}(y - x^3, z - x^4))$. I claim that the equality holds. Consider the lexicographic monomial order $z > y > x$ and let $f \in \mathrm{I}(\mathrm{V}(y - x^3, z - x^4))$. By division algorithm, there are h_1, h_2 and r in $k[x, y, z]$ such that

$$f = h_1(y - x^3) + h_2(y - x^4) + h_4,$$

where or $r = 0$ or no term of r is divisible by y and z. Thus, if $r \neq 0$, r is a polynomial in $k[x]$ and so has finitely many roots. However, since

$$0 = f(t, t^3, t^4) = h_1(t, t^3, t^4)(t^3 - t^3) + h_2(t, t^3, t^4)(t^4 - t^4) + r(t)$$

for all $t \in \mathbb{R}$, we get a contradiction. □

Question 1.4.12: Let $V \subseteq \mathbb{R}^3$ be the curve parametrized by (t^2, t^3, t^4)

(i) Prove that V is an affine variety.

(ii) Determine $\mathrm{I}(V)$.

Solution: **(i):** I claim that $V = \mathrm{V}(y^2 - x^3, z - x^2)$. In fact, we easily can check that

$$\{(t^2, t^3, t^4) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\} \subseteq V.$$

Now let $(a, b, c) \in \mathrm{V}(y^2 - x^3, z - x^2)$, then

$$\begin{cases} b^2 = a^3 \\ c = a^2 \end{cases}$$

In particular, $c \geq 0$, so there is $t_0 \in \mathbb{R}$ such that $c = t_0^4$ and $a = \sqrt{t_0^4} = t_0^2$. Since $b^2 = a^3$, we conclude that $b = t_0^3$, so

$$(a, b, c) = (t_0^2, t_0^3, t_0^4) \in \{(t^2, t^3, t^4) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\}.$$

□

Question 1.4.14: Let V and W be affine varieties in k^n.

(i) Prove that $V \subseteq W$ if and only if $\mathrm{I}(V) \supseteq \mathrm{I}(W)$.

(ii) Prove that $V = W$ if and only if $\mathrm{I}(V) = \mathrm{I}(W)$.

(iii) Conclude that $V \subsetneq W$ if and only if $\mathrm{I}(V) \supsetneq \mathrm{I}(W)$.

Solution: **(i):** Suppose that $V \subseteq W$. Let $f \in \mathrm{I}(W)$, then $f(x) = 0$ for all $x \in W$. Since $V \subseteq W$, in particular, we have that $f(x) = 0$ for all $x \in V$, thus $f \in \mathrm{I}(V)$, which implies that $\mathrm{I}(V) \supseteq \mathrm{I}(W)$. Now suppose that $\mathrm{I}(V) \supseteq \mathrm{I}(W)$. Since V and W are affine varieties, then there are $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ such that

$$W = \mathrm{V}(g_1, \ldots, g_s).$$

Let $x \in V$. Given $1 \leq i \leq s$, we have that $g_i \in \mathrm{I}(W) \subseteq \mathrm{I}(V)$, thus $g_i(x) = 0$ for all $1 \leq i \leq s$. This implies that $x \in \mathrm{V}(g_1, \ldots, g_s) = W$, so $V \subseteq W$.

(ii): Applying the part (i), we obtain

$$\begin{aligned} V = W \quad &\iff \quad V \subseteq W \text{ and } W \subseteq V \quad \iff \quad \mathrm{I}(V) \supseteq \mathrm{I}(W) \text{ and } \mathrm{I}(W) \supseteq \mathrm{I}(V) \\ &\iff \quad \mathrm{I}(V) = \mathrm{I}(W) \end{aligned}$$

(iii): Suppose that $V \subsetneq W$. So $V \subseteq W$ and $V \neq W$. Applying the parts (i) and (ii), we conclude that $\mathrm{I}(V) \supseteq \mathrm{I}(W)$ and $\mathrm{I}(V) \neq \mathrm{I}(W)$, so $\mathrm{I}(V) \supsetneq \mathrm{I}(W)$. Similarly, suppose that $\mathrm{I}(V) \supsetneq \mathrm{I}(W)$. So $\mathrm{I}(V) \supseteq \mathrm{I}(W)$ and $\mathrm{I}(V) \neq \mathrm{I}(W)$. Applying the parts (i) and (ii), we conclude that $V \subseteq W$ and $V \neq W$, so $V \subsetneq W$. □

Question 1.4.15: We can generalize the ideal operator $\mathrm{I}(\_)$ as following: If $S \subseteq k^n$ is any subset, then we set

$$\mathrm{I}(S) = \{f \in k[x_1, \ldots, x_n] \ ; \ f(x) = 0 \text{ for all } x \in S\}.$$

(i) Prove that $\mathrm{I}(S)$ is an ideal of $k[x_1, \ldots, x_n]$.

(ii) Let $X = \{(x, x) \in \mathbb{R}^2 \ ; \ x \neq 1\}$. Determine $\mathrm{I}(X)$.

(iii) Let $\mathbb{Z}^n = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \ ; \ x_1, \ldots, x_n \in \mathbb{Z}\}$. Determine $\mathrm{I}(\mathbb{Z}^n)$.

Solution: **(i):** Note that $\mathrm{I}(S) \neq \emptyset$, because $0 \in \mathrm{I}(S)$. Given $f, g \in \mathrm{I}(S)$, then

$$(f+g)(x) = f(x) + g(x) = 0 + 0 = 0$$
$$(-f)(x) = -f(x) = 0$$

for all $x \in S$, thus $f+g, -f \in \mathrm{I}(S)$, thus $(\mathrm{I}(S), +)$ is an abelian group. Finally, given $f \in \mathrm{I}(S)$ and $g \in k[x_1, \dots, x_n]$, then $(gf)(x) = g(x)f(x) = g(x) \cdot 0 = 0$ for all $x \in S$, which implies that $gf \in \mathrm{I}(S)$. Then $\mathrm{I}(S)$ is an ideal of $k[x_1, \dots, x_n]$.

(ii): Observe that $\langle x - y\rangle \subseteq \mathrm{I}(X)$. We will show that the equality holds. Consider the lexicographic monomial order $x > y$ and let $f \in \mathrm{I}(X)$. By Division algorithm, there are g and r in $k[x, y]$ such that

$$f(x, y) = g(x, y)(x - y) + r(x, y),$$

where $r = 0$ or r is a polynomial only in y, that is, $r(y) = r(x, y)$ for all $(x, y) \in k^2$. Suppose that $r \neq 0$, so r admits only finitely many roots, however

$$0 = f(a, a) = g(a, a)(a - a) + r(a) = r(a)$$

for all $a \in \mathbb{R} \smallsetminus \{1\}$, which is a contradiction. Thus $r = 0$ and so $f \in \langle x - y\rangle$ Then

$$\mathrm{I}(X) = \langle x - y\rangle.$$

(iii): We already show that, if $f(x) = 0$ for all $x \in \mathbb{Z}^n$, then $f = 0$, thus

$$\mathrm{I}(\mathbb{Z}^n) = \langle 0\rangle.$$

□

Question 1.4.16: Let I be an ideal of $k[x_1, \dots, x_n]$

(i) Prove that $1 \in I$ if and only if $I = k[x_1, \dots, x_n]$.

(ii) More generally, prove that I contains a nonzero constant polynomial if and only if $I = k[x_1, \dots, x_n]$.

(iii) Suppose that $f,\ g \in k[x_1, \dots, x_n]$ satisfy $f^2,\ g^2 \in I$. Prove that $(f + g)^3 \in I$.

(iv) Suppose that $f,\ g \in k[x_1, \dots, x_n]$ satisfy $f^r,\ g^s \in I$. Prove that $(f + g)^{r+s-1} \in I$.

Solution: **(i):** Suppose that $1 \in I$. Given $f \in k[x_1, \dots, x_n]$, then $f = f \cdot 1 \in I$, thus

$$k[x_1, \dots x_n] \subseteq I \subseteq k[x_1, \dots, x_n],$$

which implies that $I = k[x_1, \dots, x_n]$. Conversely, if $I = k[x_1, \dots, x_n]$, it is clear that $1 \in I$.

(ii): If I contains a nonzero constant polynominal $p(x) = c \neq 0$, then

$$1 = \frac{1}{c} c \in I,$$

then $I = k[x_1, \ldots, x_n]$. Conversely, if $I = k[x_1, \ldots, x_n]$, then $1 \in I$ is a nonzero constant polynomial.

(iii): Just note that

$$(f+g)^3 = f^3 + 3f^2 g + 3fg^2 + g^3 = f(f^2) + 3g(f^2) + 3f(g^2) + g(g^2) \in I.$$

(iv): Just note that $(f+g)^{r+s-1} =$

$$\sum_{k=0}^{r+s-1} \binom{r+s-1}{k} f^k g^{r+s-1-k} = \sum_{k=0}^{r-1} \binom{r+s-1}{k} f^k g^{r+s-1-k} + \sum_{k=r}^{r+s-1} \binom{r+s-1}{k} f^k g^{r+s-1-k}$$

$$= g^s \sum_{k=0}^{r-1} \binom{r+s-1}{k} f^k g^{r-1-k} + f^r \sum_{k=0}^{s-1} \binom{s-1}{k} f^k g^{s-1-k} \in I$$

$\square$

Question 1.4.17:

(i) Prove that $xy \notin I := \langle x^2, y^2 \rangle$

(ii) Prove that $1, x, y, xy$ are the only monomials not contained in $\langle x^2, y^2 \rangle$.

Solution: **(i):** Considering the lexicographic monomial order with $x > y$, note that

$$S(x^2, y^2) = \frac{x^2 y^2}{x^2} x^2 - \frac{x^2 y^2}{y^2} y^2 = x^2 y^2 - x^2 y^2 = 0$$

Thus, by Buchberger criterion's, $G := \{x^2, y^2\}$ is a Gröbner basis for I. Since

$$\overline{xy}^G = xy \neq 0,$$

we conclude that $xy \notin I$.

(ii): It is obvious that $1 \notin I$. Moreover, since $\overline{x}^G = x \neq 0$ and $\overline{y}^G = y \neq 0$, then x and y are not in I. On the other hand, given $x^r y^s$ with $r \geq 2$ or $s \geq 2$, then

$$\begin{cases} x^r y^s = (x^{r-2} y^s) x^2 \in I, & \text{if } r \geq 2 \\ x^r y^s = (x^r y^{s-2}) y^2 \in I, & \text{if } y \geq 2 \end{cases}$$

This proves the part (ii). $\square$

Chapter 2

Gröbner Bases

2.1 Introduction

There were not suggested questions.

2.2 Orderings on monomials of $k[x_1, \ldots, x_n]$

Question 2.2.6: Another order is the inverse lexicographic or invlex order defined by the following: For $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha >_{invlex} \beta$ if and only if the rightmost nonzero entry of $\alpha - \beta$ is positive. Show that the invlex is equivalent to lex order with the variables permuted in certain way.

Solution: I claim that invlex is equivalent lex order with the variables permuted as following permutation on S_n

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & & 2 & 1 \end{bmatrix}.$$

Indeed, setting $y_i := x_{\sigma(i)}$, it is enough to show that

$$y_1^{a_1} y_2^{a_2} \ldots y_n^{a_n} >_{lex} y_1^{b_1} y_2^{b_2} \ldots y_n^{b_n} \quad \text{if and only if} \quad x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} >_{invlex} x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}.$$

If $y_1^{a_1} y_2^{a_2} \ldots y_n^{a_n} >_{lex} y_1^{b_1} y_2^{b_2} \ldots y_n^{b_n}$, then the leftmost nonzero entry of $\alpha - \beta$ is positive. On the variables $x_1, \ldots, x_n$, the leftmost entries of $\alpha - \beta$ become the rightmost entries of $\alpha - \beta$, so $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} >_{invlex} x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$. The converse is proved in similar way. $\square$

Question 2.2.9: Let $>_{invlex}$ the reverse lexicographic monomial order and define $>_{rinvlex}$ to be the reversal of this ordering, i.e., for α and $\beta \in \mathbb{Z}^n_{\geq 0}$

$$\alpha >_{rinvlex} \beta \iff \beta >_{invlex} \alpha.$$

(i) Show that $\alpha >_{grevlex} \beta$ if and only if $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and $\alpha >_{rinvlex} \beta$.

(ii) Is rinvlex a monomial ordering according the definition of the book?

Solution: **(i):** Note that $\alpha >_{grevlex} \beta$ if and only if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\beta >_{invlex} \alpha$. On the other hand, $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\beta >_{invlex} \alpha$ if and only if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\alpha >_{rinvlex} \beta$.

(ii): Considering $n = 2$ and $R = k[x, y]$, we have that

$$xy <_{invlex} xy^2 <_{invlex} xy^3 <_{invlex} \cdots <_{invlex} xy^n <_{invlex} \cdots$$

This ascending chain of monomials gives us the following descending chain of monomials

$$xy >_{rinvlex} xy^2 >_{rinvlex} xy^3 >_{rinvlex} \cdots >_{rinvlex} xy^n >_{rinvlex} \cdots$$

Thus we conclude that $<_{rinvlex}$ is not a well-ordering order relation on $\mathbb{Z}^2_{\geq 0}$. $\square$

Question 2.2.10: In $\mathbb{Z}_{\geq 0}$ with the usual ordering, between any two integers, there are only a finite number of other integers. Is this necessarily true in $\mathbb{Z}^n_{\geq 0}$ for a monomial order? Is it true for the grlex order?

Solution: No. Consider $\mathbb{Z}^n_{\geq 0}$ equipped with lexicographic order. Let $\alpha = (2, 0, 0, \ldots, 0)$ and $\beta = (1, 1, 0, \ldots, 0)$. Observe that $\alpha >_{lex} \beta$ and for all $k > 1$, we have

$$(2, 0, 0, \ldots, 0) >_{lex} (1, k, 0, \ldots, 0) >_{lex} (1, 1, 0, \ldots, 0).$$

It is true for graded lexicographic order. In fact, let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ in $\mathbb{Z}^n_{\geq 0}$. Suppose without lost of generality that

$$|\alpha| := \sum_{i=1}^{n} a_i \leq \sum_{i=1}^{n} b_i := |\beta|$$

Note that $S = \{k \in \mathbb{Z} \ ; \ |\alpha| \leq k \leq |\beta|\}$ is finite. Moreover, for each $k \in S$, the set

$$S_k = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} \ ; \ |(a_1, \ldots, a_n)| = k\}$$

is finite containing $\binom{k+n-1}{n-1}$ elements. Since the set of elements between α and β is contained in $\bigcup_{k \in S} S_k$, we conclude that between any two elements of $(\mathbb{Z}^n_{\geq 0}, <_{grlex})$, there are only a finite number of elements. $\square$

2.3 Monomial Ideals and Dickson's Lemma

Question 2.4.1: Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal with the property that for every $f = \sum_\alpha c_\alpha x^\alpha$, every monomial x^α appearing in f is also in I. Show that I is a monomial ideal.

Solution: Let $A = \{x^\alpha \ ; \ x^\alpha \in I\}$. I claim that $I = \langle A \rangle$. Since $A \subseteq I$, it is clear that $\langle A \rangle \subseteq I$. Now let $f = \sum_{\alpha \in L} c_\alpha x^\alpha \in I$. By hypothesis, we have $x^\alpha \in I$ for all $\alpha \in L$, so $x^\alpha \in A$ for all $\alpha \in L$ and so $f \in \langle A \rangle$. Thus $I = \langle A \rangle$ is a monomial ideal. $\square$

Question 2.4.5: Suppose that $I = \langle \{x^\alpha \ ; \ \alpha \in A \rangle$ is a monomial ideal, and let S be the set of all exponents that occur as monomials of I. For any monomial order $>$, prove that the smallest element of S with respect to $>$ must lie in A.

Solution: In fact, let α_0 be the smallest element of S with respect to $>$, α_0 exists because $>$ is well-ordered. By Dickson's lemma, we know that there are $\alpha_1, \dots, \alpha_m \in A$ such that $I = (x^{\alpha_1}, \dots, x^{\alpha_m})$. In particular, we have that $\alpha_0 \leq \alpha_i$ for all $i = 1, \dots, m$. On the other hand, since $x^{\alpha_0} \in I$, we have that x^{α_0} is divisible by some x^{α_i} and so $\alpha_i \leq \alpha_0$. Thus $\alpha_i = \alpha_0$. We proved an even stronger result: Every monomial basis for I will necessarily contain x^{α_0}. $\square$

Question 2.4.7: Prove that the Dickson's Lemma is equivalent to the following statement: Given a non-empty subset $A \subseteq \mathbb{Z}^n_{\geq 0}$, there are finitely many elements $\alpha_1, \dots, \alpha_m \in A$ such that for every $\alpha \in A$, there exist some $i \in \{1, \dots, m\}$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha = \alpha_i + \gamma$.

Solution: Let $A \subseteq \mathbb{Z}^n_{\geq 0}$ be a non-empty subset. Consider $I = \langle \{x^\alpha \ ; \ \alpha \in A\} \rangle \subseteq k[x_1, \dots, x_n]$ be the monomial ideal generated by A. By Dickson's Lemma, there exist $\alpha_1, \dots, \alpha_m \in A$ such that

$$I = \langle \{x^\alpha \ ; \ \alpha \in A\} \rangle = (x^{\alpha_1}, \dots, x^{\alpha_m}).$$

Let $\alpha \in A \subseteq I$, then $x^\alpha \in (x^{\alpha_1}, \dots, x^{\alpha_m})$, thus we conclude that $x\alpha$ is divisible for some x^{α_i}. Thus, there exists a monomial x^γ in $k[x_1, \dots, x_n]$ such that $x^\alpha = x^{\alpha_i} x^\gamma$, that is, $\alpha = \alpha_i + \gamma$ for some $i \in \{1, \dots, m\}$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$.

Conversely suppose that this statement holds. Let $I = \langle \{x^\alpha \ ; \ \alpha \in A\} \rangle \subseteq k[x_1, \dots, x_n]$ be a monomial ideal ideal by a non-empty subset $A \subseteq \mathbb{Z}^n_{\geq 0}$. Note that we can suppose that A is the set of all monomial in I. Let $\alpha_1, \dots, \alpha_m$ be such elements of A which satisfies the condition of the statement. I claim that $I = (x^{\alpha_1}, \dots, x^{\alpha_m})$. Let $f \in I$. Since I is a monomial ideal, we can assume that f is a monomial x^α. By hypothesis, there exist some $i \in \{1, \dots, m\}$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha = \alpha_i + \gamma$. Thus $x^\alpha = x^{\alpha_i} x^\gamma \in (x^{\alpha_1}, \dots, x^{\alpha_m})$, which implies that $I \subseteq (x^{\alpha_1}, \dots, x^{\alpha_m})$.

The other inclusion is clear. $\square$

Question 2.4.10: Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$. We say that $\mathbf{u}$ is a independent weight vector if $u_i > 0$ for all $i = 1, \ldots, n$ and $u_1, \ldots, u_n$ are linearly independent over $\mathbb{Q}$. Given $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we say that $\alpha >_{\mathbf{u}} \beta$ if $\langle \alpha, \mathbf{u} \rangle > \langle \beta, \mathbf{u} \rangle$

(i) Prove that $>_{\mathbf{u}}$ is a monomial order.

(ii) Show that $(1, \sqrt{2})$ is an independent weight vector, so that $>_{\mathbf{u}}$ is a weight order in $\mathbb{Z}^2_{\geq 0}$.

(iii) Show that $(1, \sqrt{2}, \sqrt{3})$ is an independent weight vector, so that $>_{\mathbf{u}}$ is a weight order in $\mathbb{Z}^3_{\geq 0}$

Solution: **(i):** Firstly we will prove that $>_{\mathbf{u}}$ is a total order relation. In fact, let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{Z}_{\geq 0}$. If

$$\langle \alpha, \mathbf{u} \rangle = \sum_{k=1}^{n} \alpha_k u_k > \sum_{k=1}^{n} \beta_k u_k = \langle \beta, \mathbf{u} \rangle,$$

then $\alpha >_{\mathbf{u}} \beta$. If

$$\langle \beta, \mathbf{u} \rangle = \sum_{k=1}^{n} \beta_k u_k > \sum_{k=1}^{n} \alpha_k u_k = \langle \alpha, \mathbf{u} \rangle,$$

then $\beta >_{\mathbf{u}} \alpha$. If

$$\langle \beta, \mathbf{u} \rangle = \sum_{k=1}^{n} \beta_k u_k = \sum_{k=1}^{n} \alpha_k u_k = \langle \alpha, \mathbf{u} \rangle,$$

then $\sum_{k=1}^{n} (\alpha_k - \beta_k) u_k = 0$. Since $\alpha_k - \beta_k \in \mathbb{Z} \subseteq \mathbb{Q}$ and $u_1, \ldots, u_n$ are L.I. over $\mathbb{Q}$, we conclude that $\alpha = \beta$. Now let α, β and $\gamma \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha >_{\mathbf{u}} \beta$ and $\beta >_{\mathbf{u}} \gamma$. Then

$$\langle \alpha - \beta, u \rangle = \sum_{k=1}^{n} (\alpha_k - \beta_k) u_k > 0 \qquad \text{and} \qquad \langle \beta - \gamma, u \rangle = \sum_{k=1}^{n} (\beta_k - \gamma_k) u_k > 0,$$

so $\langle \alpha - \gamma, u \rangle = \langle \alpha - \beta, u \rangle + \langle \beta - \gamma, u \rangle > 0$, which implies that $\alpha >_{\mathbf{u}} \gamma$. Thus $>_{\mathbf{u}}$ is a total order.

Furthermore let α, $\beta \in \mathbb{Z}^n_{\geq 0}$ such that $\alpha >_{\mathbf{u}} \beta$ and let $\gamma \in \mathbb{Z}^n_{\geq 0}$. Thus

$$\langle \alpha + \gamma, \mathbf{u} \rangle = \sum_{k=1}^{n} (\alpha_k + \gamma_k) u_k = \sum_{k=1}^{n} \alpha_k u_k + \sum_{k=1}^{n} \gamma_k u_k > \sum_{k=1}^{n} \beta_k u_k + \sum_{k=1}^{n} \gamma_k u_k = \sum_{k=1}^{n} (\beta_k + \gamma_k) u_k$$
$$= \langle \beta + \gamma, \mathbf{u} \rangle.$$

so $\alpha + \gamma >_{\mathbf{u}} \beta + \gamma$.

Finally, let $\alpha \in \mathbb{Z}^n_{\geq 0}$. Since $u_i, \ldots, u_n > 0$, we have that

$$\langle \alpha, \mathbf{u} \rangle = \sum_{k=1}^{n} \alpha_k u_k \geq 0 = \langle 0, u \rangle,$$

which implies that $\alpha \geq_{\mathbf{u}} 0$. Thus $>_{\mathbf{u}}$ is a monomial order in $\mathbb{Z}^n_{\geq 0}$.

(ii): In fact, 1 and $\sqrt{2}$ are positive numbers. Moreover, let $c_1,\ c_2 \in \mathbb{Q}$ such that

$$c_1 + c_2\sqrt{2} = 0.$$

If $c_1 \neq 0$, then we would conclude that $\sqrt{2}$ is rational, which is an absurd. Then $c_1 = 0$ and this fact implies that $c_2 = 0$. So $\mathbf{u} = (1, \sqrt{2})$ is an independent weight vector.

(iii): In fact 1, $\sqrt{2}$ and $\sqrt{3}$ are positive numbers. Moreover, let $c_1,\ c_2,\ c_3 \in \mathbb{Q}$ such that

$$c_1 + c_2\sqrt{2} + c_3\sqrt{3} = 0.$$

thus $c_1 + c_2\sqrt{2} = -c_3\sqrt{3}$. This fact implies that

$$\begin{cases} c_1^2 + 2c_2^2 - 3c_3^2 = 0; \\ c_1c_2 = 0. \end{cases}$$

It is easy to see that the unique solution in $\mathbb{Q}^3$ of this equations system is $(0,0,0)$, so $\mathbf{u} = (1, \sqrt{2}, \sqrt{3})$ is an independent weight vector. $\square$

Question 2.4.11: Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$, and fix a monomial order $>_\sigma$ on $\mathbf{Z}^n_{\geq 0}$. Given $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we say that $\alpha >_{\mathbf{u},\sigma} \beta$ if

$$\langle \alpha, \mathbf{u} \rangle > \langle \beta, \mathbf{u} \rangle \qquad \text{or} \qquad \langle \alpha, \mathbf{u} \rangle = \langle \beta, \mathbf{u} \rangle \quad \text{and} \quad \alpha >_\sigma \beta.$$

(i) Prove that $>_{\mathbf{u},\sigma}$ is a monomial order.

(ii) Find $u \in \mathbb{Z}^n_{\geq 0}$ such that $>_{\mathbf{u},\sigma}$ is the grlex order.

(iii) Prove that, given $u \in \mathbb{Z}^n_{\geq 0}$, there are $\alpha \neq \beta \in \mathbb{Z}^n_{\geq 0}$ such that $\langle \alpha, \mathbf{u} \rangle = \langle \beta, \mathbf{u} \rangle$.

Solution: **(i):** Similar to 2.4.10 (i).

(ii): Consider $\mathbf{u} = (1, 1, \ldots, 1) \in \mathbb{Z}^n_{\geq 0}$. Note that $\alpha := (\alpha_1, \ldots, \alpha_n) >_{\mathbf{u},lex} \beta := (\beta_1, \ldots, \beta_n)$ if

$$\sum_{k=1}^{n} \alpha_k = \langle \alpha, \mathbf{u} \rangle > \langle \beta, \mathbf{u} \rangle = \sum_{k=1}^{n} \beta_k$$

or if

$$\sum_{k=1}^{n} \alpha_k = \sum_{k=1}^{n} \beta_k \qquad \text{and} \qquad \alpha >_{lex} \beta.$$

Thus the induced order is the graded lexicographic one.

(iii): Let $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n_{\geq 0}$. Suppose that there are $i < j$ such that $u_i \neq u_j$. Let $m := (u_i, u_j)$, then, setting

$$\alpha := (0, \ldots, m/u_i, \ldots, 0, \ldots, 0) \qquad \text{and} \qquad \beta := (0, \ldots, 0, \ldots, m/u_j, \ldots, 0),$$

we get that $\langle \alpha, \mathbf{u} \rangle = \langle \beta, \mathbf{u} \rangle$. On the other hand, we have $u = (u, u, \ldots, u)$ for some positive integer u. Thus, since $n \geq 2$, it is enough to consider

$$\alpha := (1, 0, \ldots, 0) \qquad \text{and} \qquad \beta := (0, \ldots, 0, 1).$$

2.4 Hilbert Basis Theorem and Gröbner Bases

Question 2.5.3: Let $I = (f_1, \ldots, f_s) \subseteq k[x_1, \ldots, x_n]$ be an ideal such that $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ is strictly contained in $\langle \mathrm{LT}(I) \rangle$. Prove that there is $f \in I$ whose remainder on division by $f_1, \ldots, f_s$ is nonzero.

Solution: Let $f \in I$ such that $f \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. We can assume without lost of generality that the leader term of f does not lie in $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Thus, it is easy to see that the leader term of f is one of terms of remainder of division by $f_1, \ldots, f_s$, thus the remainder of division is nonzero. $\square$

Question 2.5.4: If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, prove that

$$\langle \{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\} \rangle = \langle \{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\} \rangle.$$

Solution: It is enough to show the two following inclusions

$$\{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\} \subseteq \langle \{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\} \rangle$$
$$\{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\} \subseteq \langle \{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\} \rangle$$

Let $c_\alpha x^\alpha \in \{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\}$, then there is $g \in I$ such that $\mathrm{LT}(g) = c_\alpha x^\alpha$. Thus

$$c_\alpha x^\alpha = c_\alpha \,\mathrm{LM}(g) \in \{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\} \rangle,$$

which implies that $\{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\} \subseteq \langle \{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\} \rangle$.

Conversely, if $x^\alpha \in \{\mathrm{LM}(g) \ ; \ g \in I \setminus \{0\}\}$, then there exists $g \in I$ such that $x^\alpha = \mathrm{LM}(g)$. Thus, since $\mathrm{LC}(g)^{-1} g \in I$, we conclude that

$$x^\alpha = \mathrm{LT}\left(\mathrm{LC}(g)^{-1} g\right) \in \{\mathrm{LT}(g) \ ; \ g \in I \setminus \{0\}\},$$

which implies that $\{\mathrm{LM}(g)\ ;\ g \in I \smallsetminus \{0\}\} \subseteq \langle\{\mathrm{LT}(g)\ ;\ g \in I \smallsetminus \{0\}\}\rangle$. $\square$

Question 2.5.7: Considering the graded lexicographic order, is $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ a Gröbner basis for the ideal generated by these polynomials? Justify.

Solution: No, it is not a Gröbner basis for $I := \langle\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}\rangle$. Indeed note that

$$2xz - y = y(x^3y^3 - 1) - x(x^2y^4 - 2z) \in I$$

and so $xz \in \langle \mathrm{LT}(I)\rangle$. On the other hand, it is clear that

$$xz \notin (x^4y^2, x^3y^3, x^2y^4) = \big(\mathrm{LT}(x^4y^2 - z^5), \mathrm{LT}(x^3y^3 - 1), \mathrm{LT}(x^2y^4 - 2z)\big).$$

$\square$

Question 2.5.11: Let $f \in k[x_1, \ldots, x_n]$. If $f \notin \langle x_1, \ldots, x_n\rangle$, then show that

$$\langle x_1, \ldots, x_n, f\rangle = k[x_1, \ldots, x_n].$$

Solution: It is easy to see that

$$\mathfrak{m} := \langle x_1, \ldots, x_n\rangle = \{g \in k[x_1, \ldots, x_n]\ ;\ g(0, \ldots, 0) = 0\}.$$

Since $f \notin \mathfrak{m}$, we have that $f(0, \ldots, 0) \neq 0$. Now note that $f := f - f(0, \ldots, 0) \in \langle \mathfrak{m}, f\rangle$ and so does $f(0, \ldots, 0) = f - (f - f(0, \ldots, 0))$. Since

$$1 = f(0, \ldots, 0)^{-1} \cdot f(0, \ldots, 0) \in \langle \mathfrak{m}, f\rangle,$$

we conclude that $\langle x_1, \ldots, x_n, f\rangle = \langle \mathfrak{m}, f\rangle = k[x_1, \ldots, x_n]$. $\square$

Question 2.5.13: Let

$$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_n \supseteq \cdots$$

be a descending chain of affine varieties. Show that there is $N \geq 1$ such that $V_N = V_{N+1} = \cdots$

Solution: Applying the operator $\mathrm{I}(\_)$ on this chain, we obtain the following ascending chain of ideals of $k[x_1, \ldots, x_n]$

$$\mathrm{I}(V_1) \subseteq \mathrm{I}(V_2) \subseteq \cdots \subseteq \mathrm{I}(V_n) \subseteq \cdots$$

Since $k[x_1, \ldots, x_n]$ is a Noetherian ring, there is $N \geq 1$ such that $\mathrm{I}(V_N) = \mathrm{I}(V_{N+1}) = \cdots$. Finally, applying the Proposition 8 of Section 1.4, we conclude that $V_N = V_{N+1} = \cdots$. $\square$

2.5 Properties of Gröbner Bases

Question 2.6.1: Fix a monomial ordering and let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Suppose that $f \in k[x_1, \ldots, x_n]$

(i) Show that f can be written in the form $f = g + r$, where $g \in I$ and no term of r is divisible by any element of $\mathrm{LT}(I)$.

(ii) Given two expressions $f = g + r = g' + r'$ as in part (i), prove that $r = r'$.

Solution: **(i):** Denote $G = \{f_1, \ldots, f_t\}$ a Gröbner basis for I. By division algorithm, there are $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$ such that

$$f = \sum_{k=1}^{t} f_k h_k + r$$

no term of r is divisible by any $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t)$. Since $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle = \langle \mathrm{LT}(I) \rangle$, if one term of r was divisible by some term of $\langle \mathrm{LT}(I) \rangle$, then we would conclude that this term is divisible by some $\mathrm{LT}(f_i)$, which is a contradiction.

(ii): Suppose that $f = g + r = g' + r'$, where $g,\ g' \in I$ and no term of r and r' are divisible by any element of $\mathrm{LT}(I)$. Thus $r' - r = g - g' \in I$. If $r' - r \neq 0$, then $\mathrm{LT}(r - r')$ is divisible by $\mathrm{LT}(f_i) \in \langle \mathrm{LT}(I) \rangle$ for some i, however this is impossible, because no term of r and r' is divisible by some element of $\langle \mathrm{LT}(I) \rangle$. $\square$

Question 2.6.3: Show that, if G is a basis for I with the property that $\overline{f}^G$ for all $f \in I$, then G is a Gröbner Basis for I.

Solution: Let $G = \{f_1, \ldots, f_t\}$ be a basis for I. Since $S(f_i, f_j) \in I$ for all $1 \leq i, j \leq t$ and, by hypothesis, we have that $\overline{S(f_i, f_j)}^G = 0$, by Buchberger's criterion, we conclude that G is a Gröbner basis. $\square$

Question 2.6.4: Let $G = \{g_1, \ldots, g_t\}$ and $G' = \{g'_1, \ldots, g'_s\}$ be Gröbner Bases for an ideal I with respect to the same monomial order in $k[x_1, \ldots, x_n]$. Show that $\overline{f}^G = \overline{f}^{G'}$ for all $f \in k[x_1, \ldots, x_n]$. Hence, the remainder on division by a Gröbner basis is even independent of which Gröbner basis we use, as long we use one particular monomial order.

Solution: Denote $r = \overline{f}^G$ and $r' = \overline{f}^{G'}$. By Question 2.6.1, there are $g,\ g' \in I$ and $r,\ r' \in k[x_1, \ldots, x_n]$ such that $g + r = f = g' + r'$ and no term of r and r' is divisible by any term of

$\langle \mathrm{LT}(I) \rangle$. Suppose that $r - r' \neq 0$. Since $r' - r = g - g' \in I$, we have

$$\mathrm{LT}(r' - r) \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle,$$

which implies that $\mathrm{LT}(r' - r)$ is divisible by some $\mathrm{LT}(g_i) \in \langle \mathrm{LT}(I) \rangle$. However it is impossible because no term of r and r' is divisible by any element of $\langle \mathrm{LT}(I) \rangle$. Thus $r' = r$ and we get the invariance of remainder under changing the Gröbner basis $\square$

Question 2.6.9: Show that $G = \{y - x^2, z - x^3\}$ is not a Gröbner Basis with respect the lexicographic order $x > y > z$.

Solution: Note that $xy - z \in I := \langle y - x^2, z - x^3 \rangle$, because

$$xy - z = x(y - x^2) + (-1)(z - x^3).$$

Since the remainder of the division of $xy - z$ by G is nonzero, we conclude that G is not a Gröbner basis of I. $\square$

Question 2.6.11: Let f, $g \in k[x_1, \ldots, x_n]$ be polynomials such that $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are relatively prime and $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$. Assume that f or g has at least two terms.

(i) Show that $S(f, g) = -(g - \mathrm{LT}(g))f + (f - \mathrm{LT}(f))g$.

(ii) Deduce that $S(f, g) \neq 0$ and that the leading monomial of $S(f, g)$ is a multiple of either $\mathrm{LM}(f)$ or $\mathrm{LM}(g)$ in this case.

Solution: **(i)**: Since $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$ are relatively prime and $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$, denoting by $\gamma = \mathrm{lcm}(\deg(\mathrm{LT}(f)), \deg(\mathrm{LT}(g)))$, we get that

$$\begin{aligned} S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g &= \mathrm{LT}(g) f - \mathrm{LT}(f) g = \mathrm{LT}(g) f - \mathrm{LT}(f) g + fg - fg \\ &= -(g - \mathrm{LT}(g)) f - (f - \mathrm{LT}(f)) g. \end{aligned}$$

(ii): Suppose by contradiction that $S(f, g) = 0$. Thus $(g - \mathrm{LT}(g))f = (f - \mathrm{LT}(f))g$, which implies that

$$\mathrm{LT}(g - \mathrm{LT}(g))\,\mathrm{LT}(f) = \mathrm{LT}\left((g - \mathrm{LT}(g))f\right) = \mathrm{LT}\left((f - \mathrm{LT}(f))g\right) = \mathrm{LT}(f - \mathrm{LT}(f))\,\mathrm{LT}(g).$$

This implies that $\mathrm{LT}(f)$ divides $\mathrm{LT}(f - \mathrm{LT}(f))\,\mathrm{LT}(g)$. However, since $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$ are relatively prime, this fact implies that $\mathrm{LT}(f)$ divides $\mathrm{LT}(f - \mathrm{LT}(f))$, which is impossible.

Furthermore we know that

$$\mathrm{LM}(S(f,g)) = \mathrm{LM}(\ -(g-\mathrm{LT}(g))f-(f-\mathrm{LT}(f))g.\ ) = x^{\delta},$$

where

$$\delta = \deg(-(g-\mathrm{LT}(g))f) = \deg(f)+\deg(g-\mathrm{LT}(g))$$

or

$$\delta = \deg((f-\mathrm{LT}(f))g) = \deg(g)+\deg(f-\mathrm{LT}(f))$$

implying that $\mathrm{LM}(S(f,g))$ is a multiple of $\mathrm{LM}(f)$ or $\mathrm{LM}(g)$. $\square$

Question 2.6.13: Let $I \subseteq k[x_1,\dots,x_n]$ be an ideal, and let $G=\{f_1,\dots,f_t\}$ be a Gröbner basis of I.

(i) Show that $\overline{f}^G = \overline{g}^G$ if and only if $f-g \in I$.

(ii) Show that $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.

Solution: **(i):** By Proposition 1, there are $h,\ h' \in I$ such that

$$f = h + \overline{f}^G,$$
$$g = h' + \overline{g}^G.$$

Thus $f-g = h-h' + (\overline{f}^G - \overline{g}^G)$. Since $h-h' \in I$, If $\overline{f}^G = \overline{g}^G$, then $f-g\in I$.

On the other hand, if $f-g \in I$, then $\overline{f}^G - \overline{g}^G \in I$. If $\overline{f}^G \neq \overline{g}^G$, then

$$\mathrm{LT}(\overline{f}^G - \overline{g}^G) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(f_1),\dots,\mathrm{LT}(f_t)\rangle,$$

which implies that $\mathrm{LT}(\overline{f}^G - \overline{g}^G)$ is divisible by some $\mathrm{LT}(f_i)$. However this is impossible, because no term of $\overline{f}^G$ and $\overline{g}^G$ is divisible by $\mathrm{LT}(f_i)$.

(ii): Using the notation of part (i), we have that $f+g = (h+h') + (\overline{f}^G + \overline{g}^G)$. Since no term of $\overline{f}^G$ and $\overline{g}^G$ is divisible by any element of $\mathrm{LT}(I)$, so no term of $\overline{f}^G + \overline{g}^G$ is divisible by any element of $\mathrm{LT}(I)$. By uniqueness of remainder of division, we conclude that

$$\overline{f+g}^G = \overline{f}^G + \overline{g}^G.$$

$\square$

2.6 Buchberger's Algorithm

Question 2.7.7: Fix a monomial order, and let G and $\widetilde{G}$ be minimal Gröbner bases for the ideal I.

(i) Prove that $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$.

(ii) Conclude that G and $\widetilde{G}$ have the same number of elements

Solution: **(i):** By definition of minimal Gröbner basis, all leading coefficients of its elements are 1. Thus, since

$$\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(\widetilde{G})\rangle$$

and G and $\widetilde{G}$ are minimal Gröbner bases for I, we conclude that $\mathrm{LT}(G)$ and $\mathrm{LT}(\widetilde{G})$ are minimal bases for the monomial ideal $\langle \mathrm{LT}(I)\rangle$. By uniqueness of minimal monomial bases, we get that $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$.

(ii): Consider $G = \{f_1, \ldots, f_r\}$ and $\widetilde{G} = \{g_1, \ldots, g_s\}$. By definition of minimal Gröbner basis, we have that $\mathrm{LT}(f_i) = \mathrm{LT}(f_j)$ if and only if $i = j$ and the same holds for the elements of $\widetilde{G}$. Now, by item (i), given $1 \leq i \leq r$, there exists $1 \leq j \leq s$ such that $\mathrm{LT}(f_i) = \mathrm{LT}(g_j)$, so

$$\mathrm{card}(G) \leq \mathrm{card}(\widetilde{G}).$$

Switching G by $\widetilde{G}$, the same argument tells us that $\mathrm{card}(\widetilde{G}) \leq \mathrm{card}(G)$. Thus

$$\mathrm{card}(G) = \mathrm{card}(\widetilde{G}).$$

□

Question 2.7.10: Let $A = [a_ij]$ be an $n \times m$ matrix with entries in k and let $f_i = \sum_{k=1}^{m} a_{ik}x_k$ be the linear polynomials in $k[x_1, \ldots, x_m]$. Then we get the ideal $I = \langle f_1, \ldots, f_n\rangle$. Consider the lex order with $x_1 > x_2 > \cdots > x_m$. Now let $B = [b_{ij}]$ be the reduced row echelon matrix of A and let $g_1, \ldots, g_t$ be the linear polynomials coming from nonzero rows of B $(t \leq n)$.

(i) Show that $I = \langle g_1, \ldots, g_t\rangle$.

(ii) Show that $G := \{g_1, \ldots, g_t\}$ is a Gröbner basis of I.

(iii) Explain why $G := \{g_1, \ldots, g_t\}$ form the reduced Gröbner basis for I.

Solution: **(i):** From basic linear algebra, we know that B is obtained from A through a finite and successive application of elementary operations on rows, which can be

(a) Multiplication a row by a nonzero constant;

(b) Switching two rows;

(c) Sum a constant multiple of a row in another row;

If we interpret each row

$$\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{i(m-1)} & a_{im} \end{bmatrix}$$

as the polynomial $f_i = \sum_{k=1}^{m} a_{ik}x_k$, then, denoting I' the ideal obtained from I after the application of an elementary operation, we conclude that

(a) If the elementary operation is multiplication of the i-th row by $\lambda \neq 0$, then

$$I' = \langle f_1, \ldots, f_{i-1}, \lambda f_i, f_{i+1}, \ldots, f_n \rangle = \langle f_1, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_n \rangle = I.$$

(b) If the elementary operation is the switching the i-th row with the j-th one, then

$$I' = \langle f_1, \ldots, f_j, \ldots, f_i, \ldots, f_n \rangle = \langle f_1, \ldots, f_i, \ldots, f_j, \ldots, f_n \rangle = I.$$

(c) If the elementary operation is the sum of λ times the i-th row with th j-th row, then

$$I' = \langle f_1, \ldots, f_i, \ldots, f_j + \lambda f_i, \ldots, f_n \rangle = \langle f_1, \ldots, f_i, \ldots, f_j, \ldots, f_n \rangle = I.$$

So, if $E_1, \ldots, E_r$ are the elementary operations applied and I^k is the ideal obtained after the application of the k-th operation, then

$$I = I^1 = I^2 = \cdots = \cdots = I^r = \langle g_1, \ldots, g_t \rangle.$$

(ii): In order to prove that $G = \{g_1, \ldots, g_t\}$ is a Gröbner basis for I, we will use the Buchberger's criterion. Given $1 \leq i \leq t$, let $s_i = \min\left\{j \in \{1, \ldots, m\} \ ; \ b_{ij \neq 0}\right\}$. Thus

$$g_i = x_{s_i} + C_i,$$

where $C_i \in k[x_1, \ldots, x_m]$ is a linear polynomial involving none of variables x_{s_j} for all $j = 1, \ldots, t$. Now note that

$$S(g_i, g_j) = \frac{x_{s_i}x_{s_j}}{x_{s_i}} g_i - \frac{x_{s_i}x_{s_j}}{x_{s_j}} g_j = x_{s_j}C_i - x_{s_i}C_j.$$

Note that, when we divide $S(g_i, g_j)$ by G, we only will use g_i and g_j and

$$S(g_i, g_j) = x_{s_j}C_i - x_{s_i}C_j = x_{s_j}g_i + (-x_{s_i})g_j,$$

which implies that $\overline{S(g_i, g_j)}^G = 0$ and so G is a Gröbner basis for I.

(iii): Evident. $\square$

Question 2.7.14: Suppose that we have n points $\mathrm{V} = \{(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)\} \subseteq k^2$, where $a_1, \ldots, a_n$ are distinct. Remember that the Lagrange interpolation polynomial of is defined by

$$h(x) = \sum_{k=1}^{n} \left(b_k \prod_{j=1, j\neq k}^{n} \frac{x - a_j}{a_k - a_j} \right) \in k[x]$$

(i) Show that $h(a_i) = b_i$ for all $i = 1, \ldots, n$ and explain why $\deg(h) \leq n - 1$.

(ii) Prove that h is the unique polynomial with degree $\leq n - 1$ satisfying $h(a_i) = b_i$ for $i = 1, \ldots, n$.

(iii) Prove that $\mathrm{I(V)} = \langle f(x), y - h(x) \rangle$, where $f(x) = \prod_{k=1}^{n} (x - a_i)$.

(iv) Prove that $G = \{f(x), y - h(x)\}$ is the Gröbner basis for $\mathrm{I(V)} \subseteq k[x, y]$ for lex order with $y > x$.

Solution: **(i):** Given $1 \leq i \leq n$, note that

$$h(x) = b_i \prod_{k=1, k\neq i}^{n} \frac{x - a_k}{a_i - a_k} + \sum_{k=1, k\neq i}^{n} \left(b_k \prod_{j=1, j\neq k}^{n} \frac{x - a_j}{a_k - a_j} \right)$$

Thus

$$h(a_i) = b_i \prod_{k=1, k\neq i}^{n} \frac{a_i - a_k}{a_i - a_k} + \sum_{k=1, k\neq i}^{n} \left(b_k \prod_{j=1, j\neq k}^{n} \frac{a_i - a_j}{a_k - a_j} \right) = b_i \cdot 1 + \sum_{k=1, k\neq i} b_k \cdot 0 = b_i.$$

Furthermore, since each product $\prod_{j=1, j\neq k}^{n} \frac{x - a_j}{a_k - a_j}$ has degree $n - 1$, then

$$h(x) = \sum_{k=1}^{n} \left(b_k \prod_{j=1, j\neq k}^{n} \frac{x - a_j}{a_k - a_j} \right)$$

has degree less or equal to $n - 1$.

(ii): Let $g(x) \in k[x]$ be another polynomial with $\deg(g) \leq n - 1$ and $g(a_i) = b_i$ for each $i = 1, \ldots, n$. Define $f := h - g \in k[x]$. So $\deg(f) \leq n - 1$ and f has n distinct roots. This implies that $f = 0$, then $g = h$.

(iii): Firstly note that $\langle f(x), y - h(x) \rangle \subseteq \mathrm{I(V)}$. Indeed, given $(x, y) \in \mathrm{V}$, then $x = a_i$ for some

$1 \leq i \leq n$, then $f(x) = f(x, y) = 0$, so $f \in \mathrm{I(V)}$. Similarly, given $(x, y) \in \mathrm{V}$, then $(x, y) = (a_i, b_i)$ for some $1 \leq i \leq n$, thus $y - h(x) = b_i - h(x_i) = b_i - b_i = 0$. Thus we conclude that

$$\langle f(x), y - h(x) \rangle \subseteq \mathrm{I(V)}.$$

Now let $g \in \mathrm{I(V)}$. Using the lex order with $y > x$, by division algorithm, there are polynomials $h_1(x, y)$, $h_2(x, y)$ and $r(x, y) \in k[x, y]$ such that

$$g(x, y) = h_1(x, y)(f(x)) + h_2(x, y)(y - h(x)) + r(x, y),$$

where no term of r is divisible by $\mathrm{LT}(y - h(x)) = y$ and $\mathrm{LT}(f(x)) = x^n$. This restriction about the remainder tells us that r is polynomial in $k[x]$ of degree less to n. So, since

$$0 = g(a_i, b_i) = h_1(a_i, b_i)(f(a_i)) + h_2(a_i, b_i)(b_i - h(a_i)) + r(a_i, b_i) = r(a_i)$$

for all $1 \leq i \leq n$, we conclude that $r = 0$. Then

$$g(x, y) = h_1(x, y)(f(x)) + h_2(x, y)(y - h(x)) \in \langle f(x), y - h(x) \rangle.$$

(iv): Note that

$$S(f(x), y - h(x)) = \frac{yx^n}{x^n} f(x) - \frac{yx^n}{y}(y - h(x)) = yf(x) - x^n(y - h(x)).$$

Applying the division algorithm, we obtain polynomials $h_1(x, y)$, $h_2(x, y)$ and $r(x, y) \in k[x, y]$ such that

$$yf(x) - x^n(y - h(x)) = h_1(x, y)(f(x)) + h_2(x, y)(y - h(x)) + r(x, y),$$

where no term of r is divisible by $\mathrm{LT}(y - h(x)) = y$ and $\mathrm{LT}(f(x)) = x^n$. Again we conclude that $r \in k[x]$ has degree less than n. Since

$$0 = b_i f(a_i) + a_i^n(b_i - h(a_i)) = h_1(a_i, b_i)(f(a_i)) + h_2(a_i, b_i)(b_i - h(a_i)) + r(a_i, b_i) = r(a_i)$$

for all $1 \leq i \leq n$, we conclude that $r = 0$. Thus $\overline{S(f(x), y - h(x))}^G = 0$, so, by Buchberger's criterion, we conclude that G is a Gröbner basis for $\mathrm{I(V)}$. $\square$

2.7 First Applications of Gröbner Bases

Question 2.8.1: Determine whether $f(x, y, z) = xy^3 - z^2 + y^5 - z^3$ is in the ideal

$$I = \langle -x^3 + y, x^2y - z \rangle.$$

Solution: Yes. Calculating the Gröbner basis of I, we obtain

$$I = \langle y^2 - xz, x^2y - z, x^3 - y\rangle.$$

Using the division algotithm, we conclude that

$$f(x,y,z) = (xy + y^3 + yxz)(y^2 - xz) + (z + z^2)(x^2y - z) + 0(x^3 - y).$$

Thus $f \in I$.

Question 2.8.11: Suppose we have numbers a, b, c which satisfies the equations

$$\begin{cases} a+b+c = 3 \\ a^2+b^2+c^2 = 5 \\ a^3+b^3+c^3 = 7 \end{cases}$$

(i) Prove that $a^4 + b^4 + c^4 = 9$.

(ii) Show that $a^5 + b^5 + c^5 \neq 11$.

(iii) Calcule $a^5 + b^5 + c^5$ and $a^6 + b^6 + c^6$

Solution: **(i):** In fact, consider the polynomial ring $R = \mathbb{C}[x, y, z]$ and the ideal

$$I = \langle x + y + z - 3, x^2 + y^2 + z^2 - 5, x^3 + y^3 + z^3 - 7\rangle$$

Calculating the Gröbner basis of I, we obtain

$$I = \langle 3z^3 - 9z^2 + 6z + 2, y^2 + yz - 3y + z^2, x + y + z - 3\rangle$$

Using Macaulay2, we conclude that $f(x,y,z) = x^4+y^4+z^4-9 \in I$, that is, there are polynomials $f_1, f_2, f_3 \in \mathbb{C}[x, y, z]$ such that

$$f(x,y,z) = f_1(x,y,z)(x+y+z-3) + f_2(x,y,z)(x^2+y^2+z^2-5) + f_3(x,y,z)(x^3+y^3+z^3-7),$$

Thus, setting $x = a$, $y = b$ and $z = c$, we conclude

$$a^4 + b^4 + c^4 - 9 = f(a,b,c) = f_1(a,b,c)0 + f_2(a,b,c)0 + f_3(a,b,c)0 = 0,$$

which implies that $a^4 + b^4 + c^4 = 9$.

(ii):

Chapter 3

Elimination Theory

3.1 The Elimination and Extension Theorems

Question 3.1.2: Consider the system of equations

$$\begin{cases} x^2 + 2y^2 = 3 \\ x^2 + xy + y^2 = 3 \end{cases}$$

(i) If I is the ideal generated by these equations, find bases of $I \cap k[x]$ and $I \cap k[y]$

(ii) Find all solutions of the equations

(iii) Which of these solutions are rationals?

(iv) What is the smallest field k containing $\mathbb{Q}$ such that all solutions lie k^2

*Solution:***(i):** Calculating the Gröbner basis of I with respect the Lexicographic order $x > y$, we obtain that

$$I = \langle y^3 - y, xy - y^2, x^2 + 2y^2 - 3 \rangle$$

Thus, denoting the Gröbner Basis of $I \cap k[y]$ by G_1, we obtain

$$G_1 = k[y] \cap \{y^3 - y, xy - y^2, x^2 + 2y^2 - 3\} = \{y^3 - y\}.$$

Hence $I \cap k[y] = \langle y^3 - y \rangle$. Similarly calculating the Gröbner basis of I with respect the Lexicographic order $y > x$, we obtain that

$$I = \langle x^4 - 4x^2 + 3, 2y + x^3 - 3x \rangle$$

Thus, denoting the Gröbner Basis of $I \cap k[x]$ by G_x, we obtain

$$G_x = k[x] \cap \{x^4 - 4x^2 + 3, 2y + x^3 - 3x\} = \{x^4 - 4x^2 + 3\}.$$

Hence $I \cap k[x] = \langle x^4 - 4x^2 + 3\rangle$.

(ii): Since

$$\begin{aligned} \mathrm{V}(\langle x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3\rangle) &= \mathrm{V}(\langle y^3 - y, xy - y^2, x^2 + 2y^2 - 3\rangle) \\ &= \mathrm{V}(\langle x^4 - 4x^2 + 3, 2y + x^3 - 3x\rangle) \end{aligned}$$

Solving the original system is equivalent to solve

$$\begin{cases} x^2 + 2y^2 = 3 \\ xy - y^2 = 0 \\ y^3 - y = 0 \end{cases}$$

Solving this system of polynomials, we find

$$\mathrm{V}(\langle x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3\rangle) = \{(\sqrt{3}, 0), (-\sqrt{3}, 0), (1, 1), (-1, -1)\}.$$

(iii): $(1, 1)$ and $(-1, -1)$.

(iv): $k = \mathbb{Q}(\sqrt{3})$. □

Question 3.1.4: Find bases for the elimination ideals I_1 and I_2 for the ideal I determined by the equations:

$$\begin{cases} x^2 + y^2 + z^2 = 4 \\ x^2 + 2y^2 = 5 \\ xz = 1 \end{cases}$$

How many rational solutions are there?

Solution: Calculating the Gröbner basis of I with respect the lexicographic order $x > y > z$, we get

$$I = \langle 2z^4 - 3z^2 + 1, y^2 - z^2 - 1, x + 2z^3 - 3z\rangle$$

Thus solving the desired equations system is equivalent to solve

$$\begin{cases} x + 2z^3 - 3z = 0 \\ y^2 - z^2 = 1 \\ 2z^4 - 3z^2 + 1 = 0 \end{cases}$$

Thus

$$\begin{aligned} \mathrm{V}(x^2+y^2+z^2-4, x^2+2y^2-5, xz-1) = \{&(1,\sqrt{2},1),(1,-\sqrt{2},1),(-1,-\sqrt{2},-1),(-1,-\sqrt{2},-1), \\ &(\sqrt{2},\sqrt{6}/2,\sqrt{2}/2),(-\sqrt{2},\sqrt{6}/2,-\sqrt{2}/2),(\sqrt{2},-\sqrt{6}/2,\sqrt{2}/2),(-\sqrt{2},-\sqrt{6}/2,-\sqrt{2}/2)\}. \end{aligned}$$

There is no rational solution. $\square$

Question 3.1.5: Fix an integer $1 \leq l \leq n$. We say that a monomial order $>$ on $k[x_1, \ldots, x_n]$ is of *l-elimination type* provided that any monomial involving one $x_1, \ldots, x_l$ is greater than all monomials in $k[x_{l+1}, \ldots, x_n]$. Prove the following Generalized Elimination Theorem: If I is an ideal of $k[x_1, \ldots, x_n]$ and G is a Gröbner basis of I with respect to a monomial order of l-elimination type, then $G \cap k[x_{l+1}, \ldots, x_n]$ is a Gröbner basis of the l-th elimination ideal $G_l = G \cap k[x_{l+1}, \ldots, x_n]$.

Solution: $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of I with respect such monomial order. Since $G_l \subseteq I_l$, by definition of Gröbner basis, it is enough to show that

$$\langle \mathrm{LT}(G_l) \rangle = \langle \mathrm{LT}(I_l) \rangle$$

It is clear that $\langle \mathrm{LT}(G_l) \rangle \subseteq \langle \mathrm{LT}(I_l) \rangle$, because, if $g \in G_l$, then $g \in I \cap k[x_{l+1}, \ldots, x_n] = I_l$, so $\mathrm{LT}(g) \in \mathrm{LT}(I_l) \subseteq \langle \mathrm{LT}(I_l) \rangle$.

Now let $f \in I_l \subseteq I$, so $\mathrm{LT}(f) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. This fact implies that $\mathrm{LT}(f)$ is divisible by some $\mathrm{LT}(g_i)$, which implies that $LT(g_i) \in k[x_{l+1}, \ldots, x_n]$ Since this monomial order is of l-elimination property, every term of g_i is on $k[x_{l+1}, \ldots, x_n]$, which allows us to conclude that $g_i \in G_l$. Hence

$$\langle \mathrm{LT}(I_l) \rangle \subseteq \langle \mathrm{LT}(G_l) \rangle.$$

Thus G_l is a Gröbner basis of I_l with respect this monomial order. $\square$

Question 3.1.6: Let's explore some interesting examples of monomial order of l-elimination type.

(i) Fix an integer $1 \leq l \leq n$, and define $>_l$ as follows: if $\alpha,\ \beta \in \mathbb{Z}^n_{\geq 0}$, then $\alpha >_l \beta$ if

$$\alpha_1 + \cdots + \alpha_l > \beta_1 + \cdots + \beta_l \quad \text{or} \quad \alpha_1 + \cdots + \alpha_l = \beta_1 + \cdots + \beta_l \text{ and } \alpha >_{grevlex} \beta.$$

Prove that $>_l$ is a monomial order of l-elimination type.

(ii) Construct a product order that induces grevlex on $k[x_1, \ldots, x_l]$ and $k[k_{l+1}, \ldots, x_n]$ and show that this order is of l-elimination type.

Solution: **(i):** It is straightforward to show that $<_l$ is an order relation. Let $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Since $(\mathbb{R}, \leq)$ is linearly ordered, then

$$\sum_{k=1}^{l} \alpha_k > \sum_{k=1}^{l} \beta_k \quad \text{or} \quad \sum_{k=1}^{l} \alpha_k < \sum_{k=1}^{l} \beta_k \quad \text{or} \quad \sum_{k=1}^{l} \alpha_k = \sum_{k=1}^{l} \beta_k.$$

- If $\sum_{k=1}^{l} \alpha_k > \sum_{k=1}^{l} \beta_k$, then $\alpha >_l \beta$;
- If $\sum_{k=1}^{l} \alpha_k < \sum_{k=1}^{l} \beta_k$, then $\alpha <_l \beta$;
- If $\sum_{k=1}^{l} \alpha_k = \sum_{k=1}^{l} \beta_k$, then we have two possibilities
  - If $\alpha \leq_{grevlex} \beta$, then $\alpha \leq_l \beta$;
  - If $\beta \leq_{grevlex} \alpha$, then $\beta \leq_l \alpha$.

So $<_l$ is a linear order relation. Now suppose that $\alpha <_l \beta$ and let $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n_{\geq 0}$

- If $\sum_{k=1}^{l} \alpha_k < \sum_{k=1}^{l} \beta_k$, then

  $$\sum_{k=1}^{l} (\alpha_k + \gamma_k) = \sum_{k=1}^{l} \alpha_k + \sum_{k=1}^{l} \gamma_k < \sum_{k=1}^{l} \beta_k + \sum_{k=1}^{l} \gamma_k = \sum_{k=1}^{l} (\beta_k + \gamma_k),$$

  thus $\alpha + \gamma <_l \beta + \gamma$.

- If $\sum_{k=1}^{l} \alpha_k = \sum_{k=1}^{l} \beta_k$, then $\alpha <_{grevlex} \beta$. However, since

  $$\sum_{k=1}^{l} (\alpha_k + \gamma_k) = \sum_{k=1}^{l} \alpha_k + \sum_{k=1}^{l} \gamma_k = \sum_{k=1}^{l} \beta_k + \sum_{k=1}^{l} \gamma_k = \sum_{k=1}^{l} (\beta_k + \gamma_k)$$

  and $\alpha + \gamma <_{grevlex} \beta + \gamma$, then $\alpha + \gamma <_l \beta + \gamma$. Finally note that, given $\alpha \in \mathbb{Z}^n_{\geq 0}$, then

  $$\sum_{k=1}^{l} \alpha_k > 0 \quad \text{or} \quad \sum_{k=1}^{l} \alpha_k = 0.$$

  If $\sum_{k=1}^{l} \alpha_k > 0$, then $\alpha >_l (0, \ldots, 0)$. On other hand, if $\sum_{k=1}^{l} \alpha_k = 0$, since $\alpha \geq_{grevlex} (0, \ldots, 0)$ always holds, we conclude that $\alpha \geq_l (0, \ldots, 0)$.

This order is of l-elimination type, because, if $\mathbf{x}^\alpha$ is monomial with $\alpha_i > 0$ for some $i = 1, \dots, l$ and $\mathbf{x}^\beta$ is monomial with $\beta_i = 0$ for all $i = 1, \dots, l$, then

$$\sum_{k=1}^{l} \alpha_k \geq \alpha_i > 0 = \sum_{k=1}^{l} \beta_k.$$

(ii): Define the following monomial order: Given $(\alpha, \beta),\ (\gamma, \lambda) \in \mathbb{Z}^l_{\geq 0} \times \mathbb{Z}^{n-l}_{\geq 0}$, then

$$(\alpha, \beta) < (\gamma, \lambda) \qquad \Longleftrightarrow \qquad \alpha <_{grevlex} \gamma \qquad \text{or} \qquad \alpha = \gamma \qquad \text{and} \qquad \beta <_{grevlex} \lambda$$

Note that $(\alpha, \beta) > (0, \lambda)$ if $\alpha \neq 0$, thus $<$ is an order of l-elimination type. $\square$

Question 3.1.9: Consider the system of equations given by

$$x^5 + \frac{1}{x^5} = y,$$
$$x + \frac{1}{x} = z.$$

Let I be the ideal in $\mathbb{C}[x, y, z]$ determined by these equations.

(i) Find a basis for $I \subseteq \mathbb{C}[y, z]$ and show that $I_2 = \{0\}$.

(ii) Use the Extension Theorem to prove that each partial solution $c \in \mathrm{V}(I_2) = \mathbb{C}$ extends to a solution in $\mathrm{V}(I) \subseteq \mathbb{C}^3$.

(iii) Which partial solutions $(b, c) \in \mathrm{V}(I_1) \subseteq \mathbb{R}^2$ extend to solutions in $\mathrm{V}(I) \subseteq \mathbb{R}^3$?

(iv) Regarding z as a parameter, solve for x and y as algebraic functions on z to obtain a "parametrization" of $\mathrm{V}(I)$.

Solution: **(i):** Using Macaulay2, we obtain that the Gröbner basis of $I = (x^10 - x^5y + 1, x^2 - xz + 1)$ with respect the lexicographic order $x > y > z$ is

$$G = \{y - z^5 + 4z^3 - 5z, x^2 - xz + 1\}$$

Thus $I_1 = I \cap \mathbb{C}[y, z] = \langle G \cap \mathbb{C}[y, z] \rangle = \langle y - z^5 + 4z^3 - 5z \rangle$.. Similarly $I_2 = I \cap \mathbb{C}[z] = \langle G \cap \mathbb{C}[z] \rangle = 0$.

(ii): Note that $\mathrm{V}(I_2) = \mathbb{C}$. Since $I_1 = \langle y - z^5 + 4z^3 - 5z \rangle$ and $c \notin \mathrm{V}(1)$ for all $c \in \mathbb{C}$, then each $c \in \mathbb{C} = \mathrm{V}(I_2)$ extends to a solution in $\mathrm{V}(I_1)$. Similarly, since $\mathrm{V}(1, 0) = \emptyset$, each $(b, c) \in V(I_1)$ extends to $(a, b, c) \in \mathrm{V}(I)$. Hence each $c \in \mathbb{C}$ extends to a solution in $\mathrm{V}(I) \subseteq \mathbb{C}^3$.

(iii): Note that, if $c \in \mathbb{R}$ is such that c extends a solution $(a, b, c) \in V(I) \cap \mathbb{R}$, then we have that

$a^2 - ac + 1 = 0$. Since $a \in \mathbb{R}$, by quadratic formula, we get $|c| \geq 2$. Hence the partial solutions $(b, c) \in V(I_1)$ which extend to a solution (a, b, c) are of form

$$\{(c^5 - 4c^3 + 5c, c)\ ;\ c \in \mathbb{R}\} \subseteq V(I_1).$$

(iv): Note that (a, b, c) is solution of the original system if and only if (a, b, c) is solution of system

$$y - z^5 + 4z^3 - 5z = 0;$$
$$x^2 - xz + 1 = 0.$$

Thus

$$\begin{aligned}\phi_1 : \mathbb{C} &\longrightarrow \mathbb{C}^3 \\ z &\longmapsto (\tfrac{z+\sqrt{z^2-4}}{2}, z^5 - 4z^3 + 5z, z)\end{aligned} \quad \text{and} \quad \begin{aligned}\phi_2 : \mathbb{C} &\longrightarrow \mathbb{C}^3 \\ z &\longmapsto (\tfrac{z-\sqrt{z^2-4}}{2}, z^5 - 4z^3 + 5z, z)\end{aligned}$$

parametrize $\mathrm{V}(I)$. $\square$

3.2 The Geometry of Elimination

Question 3.2.3: Consider the ideal $I = (yx^3 + x^2, y^3x^2 + y^2, yx^4 + x^2 + y^2) \subseteq k[x, y]$.

(i) Find a Gröbner basis for I and show that $I_1 = \langle y^2 \rangle$.

(ii) Let c_i be the coefficient of the highest power of x in f_i. Then explain why $W = \mathrm{V}(c_1, c_2, c_3) \cap \mathrm{V}(I_1)$ does not satisfies the part (ii) of Theorem 3.

(iii) Let $\widetilde{I} = \langle f_1, f_2, f_3, c_1, c_2, c_3 \rangle$. Show that $\mathrm{V}(I) = \mathrm{V}(\widetilde{I})$ and $\mathrm{V}(I_1) = \mathrm{V}(\widetilde{I}_1)$.

(iv) Let x^{N_i} be the highest power of x appearing in f_i and set $\widetilde{f}_i = f_i - c_i x^{N_i}$. Show that $\widetilde{I} = \langle \widetilde{f}_1, \widetilde{f}_2, \widetilde{f}_3, c_1, c_2, c_3 \rangle$.

(v) Repeat the part (ii) for $\widetilde{I}$ using the generators from part (iv) to find $\widetilde{W} \subsetneq \mathrm{V}(I_1)$ that satisfies part (ii) of Theorem 3.

Solution: **(i):** Using Macaulay2, we obtain that a Grobner basis for the ideal I with respect the lexicographic order $x > y$ is

$$G = \{x^2, y^2\}$$

Thus $I_1 = I \cap k[y] = \langle G \cap k[y] \rangle = \langle y^2 \rangle$.

(ii): Note that $c_1 = y$, $c_2 = y^3$, $c_3 = y$ and

$$W = \mathrm{V}(c_1, c_2, c_3) \cap \mathrm{V}(I_1) = \mathrm{V}(y, y^3) \cap \mathrm{V}(y) = \{0\}.$$

W does not satisfies part (ii) of Theorem 3, because W is not strict subset of $\mathrm{V}(I_1)$.

(iii): Note that $I \subseteq \widetilde{I}$, thus $\mathrm{V}(\widetilde{I}) \subseteq \mathrm{V}(I)$ and $\mathrm{V}(\widetilde{I_1}) \subseteq \mathrm{V}(I_1)$. Since $\mathrm{V}(I) = \{(0,0)\}$, $\mathrm{V}(I_1) = \{0\}$, $(0,0) \in \mathrm{V}(\widetilde{I})$ and $0 \in \mathrm{V}(\widetilde{I_1})$, then we get the desired equalities.

(iv): Evident.

(v): $d_1 = c_1$, $d_2 = c_2$, $d_3 = c_3$, $d_4 = 1$, $d_5 = 1$, $d_6 = 1$. We have that $\widetilde{W} = \mathrm{V}(d_1, \ldots, d_6) = \emptyset$, $\widetilde{W} \subsetneq \mathrm{V}(I_1)$ and

$$\mathrm{V}(I_1) \smallsetminus \widetilde{W} = \{0\} \smallsetminus \emptyset \subseteq= \{0\} = \pi_1(\{(0,0)\}) = \pi_1(V).$$

$\square$

Question 3.2.4: Consider the ideal

$$I = \langle x^2 + y^2 + z^2 + 2, 3x^2 + 4y^2 + 4z^2 + 5 \rangle$$

Let $V = \mathrm{V}(I)$ and $\pi_1 : k^3 \longleftarrow k^2$ be the projection on the two last coordinates.

(i) Working on $\mathbb{C}$, prove that $\mathrm{V}(I_1) = \pi_1(V)$.

(ii) Working on $\mathbb{R}$, prove that $V \neq \emptyset$ and that $\mathrm{V}(I_1)$ is infinite. Thus $\mathrm{V}(I_1)$ may be much larger than the smallest variety containing $\pi(V)$ when the field is not algebraically closed.

Solution: **(i):** Using Macaulay2, we obtain that a Grobner basis for the ideal I with respect the lexicographic order $x > y > z$ is

$$G = \{y^2 + z^2 - 1, x^2 + 3\}.$$

Thus $I_1 = \langle G \cap \mathbb{C}[y, z] \rangle = \langle y^2 + z^2 - 1 \rangle$ and $\mathrm{V}(I_1) = \{(y, z) \in \mathbb{C}^2 \ ; \ y^2 + z^2 = 1\}$. Note that every partial solution of $\mathrm{V}(I_1)$ can be extended to partial solution of V. Thus every element of $\mathrm{V}(I_1)$ is projection of some element of V, which implies $\mathrm{V}(I_1) \subseteq \pi_1(V)$. Since the other inclusion always holds, the equality follows.

(ii): Working in $\mathbb{R}$, we have that

$$x^2 + y^2 + z^2 + 2 \geq 2 > 0,$$
$$3x^2 + 4y^2 + 4z^2 + 5 \geq 5 > 0$$

for all $(x, y, z) \in \mathbb{R}^3$, thus $\mathrm{V}(I) = \emptyset$ and so $\pi_1(V) = \emptyset$. However $\mathrm{V}(I_1) = \{(y, z) \in \mathbb{C}^2 ; y^2 + z^2 = 1\}$ is infinite, thus

$$\overline{\pi_1(V)} = \emptyset \neq V(I_1).$$

□

Question 3.2.5: Suppose that $I \subseteq \mathbb{C}[x, y]$ is an ideal such that $I_1 \neq \{0\}$. Prove that $\mathrm{V}(I_1) = \pi_1(V)$, where $V = \mathrm{V}(I)$ and π_1 is the projection on y-axis.

Solution: We already know that $\pi_1(V) \subseteq \mathrm{V}(I_1)$. Since $I_1 \subseteq k[y]$ is a nonzero ideal, we know that $V(I_1)$ is finite and non-empty. Thus $\pi_1(V)$ is finite, and so closed on Zariski topology, which implies that

$$\mathrm{V}(I_1) = \overline{\pi_1(V)} = \pi_1(V).$$

□

3.3 Implicitization

There were not exercises at this section.

3.4 Singular Points and Envelopes

Question 3.4.1: Let C be the curve in k^2 defined by $\mathrm{V}(x^3 - xy + y^2 - 1)$ and note that $(1, 1) \in C$. Consider the straight line parametrized by

$$x = 1 + ct,$$

$$y = 1 + dt.$$

Compute the multiplicity of this line when it meets C at $(1, 1)$. What does this tell you about the tangent line?

Solution: Consider the polynomial

$$\begin{aligned} g(t) = (1 + ct)^3 - (1 + ct)(1 + dt) + (1 + dt)^2 - 1 &= c^3t^3 + (3c^2 - cd + d^2)t^2 + (2c + d)t \\ &= t(c^3t^2 + (3c^2 - cd + d^2)t + (2c + d)). \end{aligned}$$

Now we have two cases

- $d \neq -2c$: In this case L will meet C at $(1,1)$ with multiplicity 3

- $d = -2c$: In this case, one gets $g(t) = t^2(c^3t + (3c^2 - cd + d^2)) = t^2(c^3t + 9c^2)$, so L will meet C at $(1,1)$ with multiplicity 3 if $\mathrm{char}(k) = 3$, and with multiplicity 2 if $\mathrm{char}(k) \neq 5$. In particular, the multiplicity of intersection of the tangent line with the curve depends on the characteristic of field.

$\square$

Question 3.4.2: We need to show that the the notion of multiplicity is independent of how the line is parametrized.

(i) Show that two parametrizations

$$\gamma(t) = \begin{cases} x = a + ct \\ y = b + dt \end{cases} \qquad \lambda(t) = \begin{cases} x = a + c't \\ y = b + d't \end{cases}$$

correspond to the same line if and only if there is a nonzero $\lambda \in k$ such that $(c,d) = \lambda(c',d')$.

(ii) Suppose that the two parametrizations of part (i) correspond to the same line L that meet $V(f)$ at (a,b). Prove that the polinomials

$$g(t) = f(a + ct, b + dt)$$
$$g'(t) = f(a + c't, b + d't)$$

have the same multiplicity at $t = 0$.

Solution: **(i):** Since the lines λ and γ pass by the same point (a,b), they will be are the same line if and only if they have the same inclination. Since the inclinations of γ and λ are d/c and d'/c', respectively, then γ and λ will parametrize the same line if and only if

$$\frac{d}{d'} = \frac{c}{c'}.$$

Calling by κ is quotient, we have that $d = \kappa d'$ and $c = \kappa c'$, so

$$(d,c) = \kappa(d',c')$$

(ii): Note that

$$g'(\kappa t) = f(a + c'(\kappa t), b + d'(\kappa t)) = f(a + (c'\kappa)t, b + (d'\kappa)t) = f(a + ct, b + dt) = g(t),$$

which implies that $g^{(m)}(t) = \kappa^m g'^{(m)}(t)$. Now, since a polynomial $p(t)$ has multiplicity m in $t = 0$ if and only if $p^{(k)}(0) = 0$ for $k = 0, \ldots, m-1$ and $p^{(m)}(0) \neq 0$, the result follows. $\square$

Question 3.4.3: Consider the straight lines

$$x = t$$
$$y = b + t$$

For which values of b is the line tangent to the circle $x^2 + y^2 = 2$.

Solution: Considering $g(t) = f(t, b+t) = 2t^2 + 2bt + b^2 - 2$, we observe that such lines are tangent if and only if 0 is a root of g with multiplicity greater than 1, and it is possible if and only if the discriminant of quadratic equation $2t^2 + 2bt + b^2 - 2 = 0$ is 0. Calculating the discriminant, we obtain

$$\Delta = 4b^2 - 4 \cdot 2 \cdot (b^2 - 2) = -4b^2 + 16$$

Thus $\Delta = 0$ if and only if $b = -2$ or $b = 2$ $\square$

Question 3.4.4: If $(a, b) \in \mathrm{V}(f)$ and $\nabla f(a, b) \neq (0, 0)$, prove that the tangent line of $\mathrm{V}(f)$ at (a, b) is defined by the equation

$$\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b) = 0.$$

Solution: Let

$$\gamma(t) = \begin{cases} x(t) = a + ct \\ y(t) = b + dt \end{cases}$$

be a parametrization of the tangent line of L of $\mathrm{V}(f)$ at (a, b). Considering the polynomial $g(t) = f(\gamma(t))$, since L is the tangent line of $\mathrm{V}(f)$ at (a, b), we have that

$$0 = g'(0) = \frac{\partial f}{\partial x}(a, b)c + \frac{\partial f}{\partial y}(a, b)d$$

However, since $(x(t) - a, y(t) - b) = t(c, d)$ for all $t \in k$, multiplying the equation above by t and switching tc, td by $x(t) - a$, $y(t) - b$, respectively, we get

$$\frac{\partial f}{\partial x}(a, b)(x(t) - a) + \frac{\partial f}{\partial y}(a, b)(y(t) - b) = 0.$$

$\square$

Question 3.4.5: Let $g \in k[t]$ be a polynomial such that $g(0) = 0$. Assume that $\mathbb{Q} \subseteq k$.

(i) Prove that $t = 0$ is a root of multiplicity ≥ 2 of g if and only if $g'(0) = 0$.

(ii) More generally, prove that $t = 0$ is a root of multiplicity $\geq m$ of g if and only if $g^{(1)}(0) = \cdots = g^{(m-1)}(0) = 0$

Solution: **(i):** Suppose that $t = 0$ is a root of multiplicity ≥ 2 of g. Thus $g(t) = t^2 h(t)$ for some $h(t) \in k[t]$. Since $g'(t) = 2th(t) + t^2 h'(t)$, then $g'(0) = 0$. Conversely suppose that $g'(0) = 0$. Since $t = 0$ is a root of g, there is $h(t) \in k[t]$ such that $g(t) = th(t)$. However, since $g'(t) = h(t) + th'(t)$, we conclude that $h(0) = 0$, thus there is a polynimial $j(t) \in k[t]$ such that $h(t) = tj(t)$, which implies that $g(t) = t^2 j(t)$ and so $t = 0$ is a root of multiplicity ≥ 2 of g.

(ii): We will proceed by induction on m. For $m = 1$, the result holds trivially. Suppose that the result holds for $m = n$. Let $g(t)$ be a polynomial such that $t = 0$ is a root with multiplicity $\geq n + 1$. Thus

$$g(t) = th(t)$$

for some $h(t) \in k[t]$ with root of multiplicity $\geq n$ in $t = 0$. Now note that

$$g'(t) = h(t) + th'(t)$$

By induction hypothesis, $h'(0) = (h')^{(1)} = \cdots = (h')^{(n-2)} = 0$, so 0 is root of multiplicity $\geq n-1$ of $h'(t)$, so $h'(t) = t^{n-1}k(t)$ and

$$g'(t) = t^n \widetilde{h}(t) + t^{n-1}k(t) = t^{(n-1)}(t\widetilde{h}(t) + k(t)).$$

That is, $t = 0$ is a root with multiplicity $\geq n - 1$ of $g'(t)$. By induction hypothesis, we conclude that

$$g(0) = g^{(1)}(0) = \cdots = g^{(n)}(0) = 0.$$

Now suppose let $g(t)$ be a polynomial such that $g(0) = g^{(1)}(0) = \cdots = g^{(n)}(0) = 0$. Thus

$$(g')^{(0)}(0) = \cdots = (g')^{(n-1)}(0) = 0,$$

By induction hypothesis, we get that $t = 0$ is a root with multiplicity $\geq n$ of $g'(t)$, that is, $g'(t) = t^n h(t)$. Moreover, since $g(0) = g^{(1)}(0) = \cdots = g^{(n-1)}(0) = 0$, we also have that $g(t) = t^n k(t)$. Thus

$$t^n h(t) = g'(t) = nt^{k-1}k(t) + t^n k'(t)$$

So $t(h(t) - k'(t)) = nk(t)$. Since $\mathrm{char}(k) = 0$, we conclude that $k(t)$ is of form $tf(t)$ for some $f(t) \in k[t]$, so

$$g(t) = t^{n+1} f(t).$$

$\square$

Question 3.4.6: Let L be the line parametrized by

$$\begin{cases} x(t) = a + ct \\ y(t) = b + dt \end{cases},$$

where $(a, b) \in \mathrm{V}(f)$. Also let $g(t) := f(a + ct, b + dt)$. Prove that L meets $\mathrm{V}(f)$ with multiplicity m if and only if $g(0) = g^{(1)}(0) = \cdots = g^{(m-1)}(0) = 0$ and $g^{(m)}(0) \neq 0$.

Solution: Suppose that L meets $\mathrm{V}(f)$ with multiplicity m, then there exists $h(t) \in k[t]$ such that $g(t) = t^m h(t)$ and $h(0) \neq 0$. Applying the Leibniz rule of derivative, we have

$$g^{(k)}(t) = \sum_{j=0}^{k} \binom{k}{j} \frac{m!}{j!} t^{m-j} h^{(k-j)}(t)$$

Thus $g^{(k)}(0) = 0$ for all $k = 0, \ldots, m-1$ and

$$g^{(m)}(0) = \sum_{j=0}^{m} \binom{m}{j} \frac{m!}{j!} 0^{m-j} h^{(m-j)}(0) = h(0) \neq 0.$$

Conversely suppose that $g(0) = g^{(1)}(0) = \cdots = g^{(m-1)}(0) = 0$ and $g^{(m)}(0) \neq 0$. Using the Question 3.4.5, we know that L meet $\mathrm{V}(f)$ with multiplicity $\geq m$, however, since $g^{(m)}(0) \neq 0$, L does not meet $\mathrm{V}(f)$ with multiplicity $\geq m + 1$, so the result follows. $\square$

Question 3.4.7: Let $C = \mathrm{V}(y - f(x)) \subseteq k[x, y]$. Thus C is the graph of $f \in k[x]$.

(i) Give an algebraic proof that the tangent line L to C at $(a, f(a))$ is parametrized by

$$x = a + t$$
$$y = f(a) + f'(a)t.$$

(ii) Show that the tangent line at $(a, f(a))$ meets the curve with multiplicity ≥ 3 if and only if $f''(a) = 0$.

(iii) Show that the multiplicity is exactly 3 if and only if $f''(a) = 0$, but $f'''(a) \neq 0$.

(iv) Over $\mathbb{R}$, a point of inflection is defined to be the point where $f''(x)$ changes of signal. Prove that if the multiplicity is 3, then $(a, f(a))$ is a point of inflection.

Solution: **(i):** Consider the polynomial $g(t) = f(a) + f'(a)t - f(a+t) \in k[t]$. Note that $g(0) = 0$. In order to show that L is the tangent line to C at $(a, f(a))$, it is enough to show that $g'(0) = 0$. However it is easy, because

$$g'(t) = f'(a) - f'(a+t)$$

and so $g'(0) = 0$.

(ii): Note that the tangent line at $(a, f(a))$ meets the curve with multiplicity ≥ 3 if and only if $g''(0) = 0$. However, since

$$g''(t) = -f''(a+t),$$

this happens if and only if $f''(a) = g''(0) = 0$.

(iii): Note that the multiplicity is exactly 3 if and only if $g''(0) = 0$ and $g'''(0) \neq 0$. However, since

$$g'''(t) = -f'''(a+t),$$

this happens if and only if $f''(a) = -g''(0) = 0$ and $f'''(a) = -g'''(0) \neq 0$.

(iv): If the multiplicity is 3, we have that $f''(a) = 0$, but $f'''(a) \neq 0$. Suppose without lost of generality that $f'''(a) > 0$. By continuity, there is a neighborhood U of a such that $(f'')'(x) = f'''(x) > 0$ for all $x \in U$, which implies that there is $\epsilon > 0$ such that, for all $x \in (a - \epsilon, a)$, $f''(x) < 0$ and, for all $x \in (a, a + \epsilon)$, $f''(x) > 0$. Thus $f''(t)$ changes of sign in $t = a$. $\square$

Question 3.4.8: We will compute some singular points.

(i) Show that $(0, 0)$ is the unique singular point of $\mathrm{V}(y^2 - x^3)$.

(ii) Find every singular points of the curve $\mathrm{V}(y^2 - cx^2 + x^3)$.

(iii) Show that the circle $\mathrm{V}(x^2 + y^2 - a) \subseteq \mathbb{R}^2$ has no singular points when $a > 0$.

Solution: **(i):** Consider the following system of equations

$$\begin{cases} 2y = 0 \\ -3x^2 = 0 \\ y^2 - x^3 = 0 \end{cases}$$

It is clear that the unique solution of this system is $(0,0)$

(ii): Consider the following system of equations

$$\begin{cases} 2y = 0 \\ -2cx + 3x^2 = 0 \\ y^2 - cx^2 + x^3 = 0 \end{cases}$$

Note that the unique solution of this system is $(0,0)$. In fact, the curve self-intersects in $(0,0)$.

(iii): Consider the following system of equations

$$\begin{cases} 2x = 0 \\ 2y = 0 \\ x^2 + y^2 - a = 0 \end{cases}$$

The unique point (a,b) such that $\nabla f(a,b) = 0$ is the origin. However this point does not belong to the circle if $a > 0$. Thus the non-degenerated circle has no singular point.

Question 3.4.9: One use of multiplicities is to show that one singularity is "worse" than another.

(i) For the curve $\mathrm{V}(y^2 - x^3)$, show that most lines through the origin meet the curve with multiplicity exactly 2.

(ii) For the curve $\mathrm{V}(x^4 + 2xy^2 + y^3)$, show that all lines through the origin meet the curve with multiplicity ≥ 3.

Solution: (i): Let L be a line parametrized by

$$\gamma(t) = \begin{cases} x(t) = ct \\ y(t) = dt \end{cases}.$$

Considering $f(x,y) = y^2 - x^3$, then

$$g(t) = f(\gamma(t)) = d^2t^2 - c^3t^3 = t^2(d^2 - c^3t).$$

Thus, except the horizontal line, all other lines meet $\mathrm{V}(f)$ at $(0,0)$ with multiplicity exactly 2.

(ii): Let L be a line parametrized by

$$\gamma(t) = \begin{cases} x(t) = ct \\ y(t) = dt \end{cases}.$$

Considering $f(x,y) = x^4 + 2xy^2 + y^3$, then

$$g(t) = f(\gamma(t)) = c^4t^4 + 2cd^2t^3 + d^3t^3 = t^3(c^4t + 2cd^2 + d^3).$$

Thus all lines through the origin meet the curve with multiplicity ≥ 3. □

Question 3.4.10: We know that $(0,0)$ is a singular point of the curve $C = \mathrm{V}(y^2 - x^2 - x^3)$. But in the picture of C, it looks likes there are two "tangent" lines through the origin. Can we use multiplicities to pick these out?

(i) Show that with two exceptions, all lines through the origin meet C with multiplicity exactly 2. What are the lines that have multiplicity 3?

(ii) Explain how your your answer to part (i) relates to the picture in the text. Why should the "tangent" have the higher multiplicity.

Solution: **(i):** Let L be a line parametrized by

$$\gamma(t) = \begin{cases} x(t) = ct \\ y(t) = dt \end{cases}.$$

Considering $f(x,y) = y^2 - x^2 - x^3$, then

$$g(t) = f(\gamma(t)) = d^2t^2 - c^2t^2 - c^3t^3 = t^2(d^2 - c^2 - c^3t).$$

Thus, except when $c = \pm d$, all lines through the origin meet C with multiplicity exactly 2. The lines with multiplicity 3 are

$$\gamma_1(t) = \begin{cases} x(t) = t \\ y(t) = t \end{cases} \qquad \gamma_2(t) = \begin{cases} x(t) = t \\ y(t) = -t \end{cases}.$$

(ii): We observe that lines that have higher multiplicities are the "tangent" lines. □

Question 3.4.11: The four-leaved rose is defined by the equation $\mathrm{V}((x^2 + y^2)^3 - 4x^2y^2)$.

(i) Show that most lines through origin meet the rose with multiplicity 4 at the origin.

(ii) Find the lines through the origin that meet with multiplicity > 4.

Solution: **(i):** Let L be a line parametrized by

$$\gamma(t) = \begin{cases} x(t) = ct \\ y(t) = dt \end{cases}$$

and let $g(t) = f(\gamma(t)) = (c^2+d^2)^3t^6 - 4c^2d^2t^4 = t^4((c^2+d^2)^3t^2 - 4c^2d^2)$. Except the vertical and the horizontal lines, that is, when $c = 0$ or $d = 0$, all other lines meet $\mathrm{V}(f)$ in $(0,0)$ with multiplicity 4 considering $\mathrm{char}(k) \neq 2$.

(ii): The unique lines that meet $\mathrm{V}(f)$ at $(0,0)$ with multiplicity > 4 are the horizontal and vertical lines. They meet $\mathrm{V}(f)$ with multiplicity 6. $\square$

Question 3.4.12: Consider the surface $\mathrm{V}(f) \subseteq k^3$ defined by $f \in k[x,y,z]$.

(i) Define what it means for $(a,b,c) \in \mathrm{V}(f)$ to be a singular point.

(ii) Determine all singular points of the sphere $\mathrm{V}(x^2+y^2+z^2-1)$. Does your answer make sense?

(iii) Determine all singular points on the surface $\mathrm{V}(x^2 - y^2z^2 + z^3)$.

Solution: **(i):** A point (a,b,c) in $\mathrm{V}(f)$ is said singular if $\nabla f(a,b,c) = (0,0,0)$, where

$$\nabla f(a,b,c) = \left(\frac{\partial f}{\partial x}(a,b,c),\ \frac{\partial f}{\partial y}(a,b,c),\ \frac{\partial f}{\partial z}(a,b,c)\right).$$

A point $P \in \mathrm{V}(f)$ is said regular if P is non-singular.

(ii): Considering $f(x,y,z) = x^2+y^2+z^2-1$, we have that

$$\nabla f(x,y,z) = (2x, 2y, 2z)$$

Thus $\nabla f(x,y,z) = 0$ if and only if $(x,y,z) = (0,0,0)$. However, $(0,0,0) \notin \mathrm{V}(f)$, thus the sphere $\mathrm{V}(f)$ does not contain singular points.

(iii): Considering $f(x,y,z) = x^2 - y^2z^2 + z^3$, we have that

$$\nabla f(x,y,z) = (2x,\ 2z^2y,\ 2zy^2 + 3z^2).$$

Thus $\nabla f(x,y,z) = 0$ if and only if $(x,y,z) = (0,\lambda,0)$, where $\lambda \in k$. Since $(0,\lambda,0) \in \mathrm{V}(f)$ for all $\lambda \in k$, we conclude that

$$\mathrm{Sing}(f) = \{(0,\lambda,0) \in k^3 \ ;\ \lambda \in k\}.$$

Analyzing the plot of this surface, we observe that occurs self-intersection exactly at the singular points of $\mathrm{V}(f)$. $\square$

Chapter 4

The Algebra-Geometry Dictionary

4.1 Hilbert's Nullstellensatz

Question 4.1.1: Recall that $\mathrm{V}(y-x^2, z-x^3)$ is the twisted cubic in $\mathbb{R}^3$.

(i) Show that $\mathrm{V}((y-x^2)^2+(z-x^3)^2)$ is also the twisted cubic.

(ii) Show that any variety in $\mathrm{V}(I) \subseteq \mathbb{R}^n$, $I \subseteq \mathbb{R}[x_1, \dots, x_n]$, can be defined by a single polynomial equation (and hence by a principal ideal).

Solution: **(i):** Suppose that $(x_0, y_0, z_0) \in \mathrm{V}(y-x^2, z-x^3)$, so

$$\begin{cases} y_0 - x_0^2 = 0 \\ z_0 - x_0^3 = 0 \end{cases}$$

Hence $(y_0-x_0^2)^2+(z_0-x_0^3)^2 = 0^2+0^3 = 0$, which implies that $(x_0, y_0, z_0) \in \mathrm{V}((y-x^2)^2+(z-x^3)^2)$ and $\mathrm{V}(y-x^2, z-x^3) \subseteq \mathrm{V}((y-x^2)^2+(z-x^3)^2)$.

Conversely if $(x_0, y_0, z_0) \in \mathrm{V}((y-x^2)^2+(z-x^3)^2)$, then $(y_0-x_0^2)^2+(z_0-x_0^3)^2 = 0$. Since $\mathbb{R}$ is an ordered field, one has that $y_0 - x_0^2 = 0$ and $z_0 - x_0^3 = 0$, which implies that $(x_0, y_0, z_0) \in \mathrm{V}(y-x^2, z-x^3)$ and $\mathrm{V}((y-x^2)^2+(z-x^3)^2) \subseteq \mathrm{V}(y-x^2, z-x^3)$.

(ii): Let $I \subseteq \mathbb{R}[x_1, \dots, x_n]$. As this polynomial ring is Noetherian, $I = \langle f_1, \dots, f_m \rangle$ is a finitely generated ideal. By field ordering of $\mathbb{R}$, we have

$$\begin{cases} f_1(a) = 0 \\ \quad\vdots \\ f_m(a) = 0 \end{cases} \qquad \Longleftrightarrow \qquad \sum_{k=1}^{m} f_k^2(a) = 0.$$

Thus, considering $F = \sum_{k=1}^{m} f_k^2$, one has $\mathrm{V}(f_1, \ldots, f_m) = \mathrm{V}(F)$. $\square$

Question 4.1.2: Let k be an arbitrary field and $J = \langle x^2 + y^2 - 1, y - 1\rangle \subseteq k[x, y]$ an ideal. Find $f \in \mathrm{I}(\mathrm{V}(J))$ such that $f \notin J$.

Solution: Consider the polynomial $f(x, y) = x$. Observe that $f \notin J$. Indeed, calculating the Gröbner basis for J, we obtain $J = \langle x^2, y - 1\rangle$. Thus, by division algorithm, one concludes that $f \notin J$. However $f^2(x, y) = x^2 \in \mathrm{I}(\mathrm{V}(J))$, because

$$f^2 = 1 \cdot (x^2 + y^2 - 1) - (y + 1)(y - 1)$$

and so f^2 vanishes at every point where the elements of J vanish. Finally, as $\mathrm{I}(\mathrm{V}(J))$ is a radical ideal, one concludes that $f \in \mathrm{I}(\mathrm{V}(J))$. $\square$

Question 4.1.8: The purpose of this exercise is to show that if k is not an algebraically closed field, then any variety $V \subseteq k^n$ can be defined by a single equation.

(i) If $g = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ is a polynomial of degree n in x, define the homogenization g^h of g with respect the variable y to be the polynomial $g^h = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$. Show that g has a root in k if and only if there is $(a, b) \in k^2$ such that $(a, b) \neq (0, 0)$ and $g^h(a, b) = 0$.

(ii) If k is not an algebraically closed field, prove that there is $f \in k[x, y]$ such that the variety $\mathrm{V}(f) \subseteq k^2$ consist if just the origin $(0, 0) \in k^2$.

(iii) If k is not an algebraically closed field, prove that for each integer $l > 0$, there is a polynomial $f \in k[x_1, \ldots, x_l]$ such that the only solution $f = 0$ is the origin $(0, \ldots, 0) \in k^l$.

(iv) If $W = \mathrm{V}(g_1, \ldots, g_s)$ is any variety in k^n, where k is not an algebraically closed field, then show that W can be defined by a single equation.

Solution: **(i):** Suppose that g admits a root and let $x = a$ be a root of g. Note that

$$\begin{aligned} g^h(a, 1) = a_0a^n + a_1a^{n-1} \cdot 1 + \cdots + a_{n-1}a \cdot 1^{n-1} + a_n \cdot 1^n &= a_0a^n + a_1a^{n-1} + \cdots + a_{n-1}a + a_n \\ &= g(a) = 0. \end{aligned}$$

Thus $(a,1) \neq (0,0)$ and $g^h(a,1) = 0$.

Conversely suppose that there is $(a,b) \in k^2$ such that $(a,b) \neq (0,0)$ and $g^h(a,b) = 0$. Thus

$$a_0a^n + a_1a^{n-1}b + \cdots + a_{n-1}ab^{n-1} + a_nb^n = 0$$

Firstly observe that b is necessarily non-zero. Indeed if $b = 0$, so $a \neq 0$, thus we have $g^h(a,b) = g^h(a,0) = a_0a^n = 0$, which implies that $a_0 = 0$, which is a contradiction, because a_0 is the leader coefficient. Hence suppose $b \neq 0$. Multiplying the equation above by $1/b^n$, one obtains

$$g(a/b) = a_0\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{a}{b}\right) + a_n = 0.$$

and so $x = a/b$ is root of g.

(ii): Since k is not an algebraically closed field, let $f(x) \in k[x]$ be an irreducible polynomial with $\deg(f) > 1$. As $f(x)$ is irreducible, $f(x)$ does not admits roots in k. Considering $n = \deg(f)$, define

$$g(x,y) = y^n f\left(\frac{x}{y}\right) \in k[x,y].$$

Note that $g(0,0) = 0$ and, by item (i), g does not admits root different from $(0,0)$, so $(0,0)$ is the unique root of g.

(iii): We will proceed by induction on the number of variables l. If $l = 1$, the polynomial $f_1(x) = x \in k[x]$ vanishes only in 0. Suppose that this fact holds for polynomials in $l = n$ variables. Let $h(y,z) \in k[y,z]$ be a polynomial such that $\mathrm{V}(h) = \{(0,0)\}$ and, applying the induction hypothesis, let $f(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$ be a polynomial such that $\mathrm{V}(f) = \{(0,\ldots,0)\} \subseteq k^n$. Define

$$g(x_1,\ldots,x_n,x_{n+1}) := h(f(x_1,\ldots,x_n),x_{n+1}).$$

It is easy to see that $\mathrm{V}(g) = \{(0,\ldots,0)\} \subseteq k^{n+1}$.

(iv): Let $V = \mathrm{V}(g_1,\ldots,g_s) \subseteq k^n$ be a variety. Since k is not algebraically closed, let $f(y_1,\ldots,y_s) \in k[y_1,\ldots,y_s]$ such that $\mathrm{V}(f) = \{(0,\cdots,0)\} \subseteq k^s$ and define the polynomial $G(x_1,\ldots,x_n) = f(g_1,\ldots,g_s)(x_1,\ldots,x_n) \in k[x_1,\ldots,x_n]$. I claim that

$$\mathrm{V}(G) = \mathrm{V}(g_1,\ldots,g_s).$$

Indeed, if $(a_1,\ldots,a_n) \in \mathrm{V}(G)$, thus

$$f(g_1(a_1,\ldots,a_n),\ldots,g_s(a_1,\ldots,a_n)) = f(g_1,\ldots,g_s)(a_1,\ldots,a_n) = G(a_1,\ldots,a_n) = 0,$$

which implies that $g_1(a_1,\dots,a_n)=\cdots=g_s(a_1,\dots,a_n)=0$ by property of f and so $(a_1,\dots,a_n)\in \mathrm{V}(g_1,\dots,g_s)$.

Conversely, given $(a_1,\dots,a_n)\in \mathrm{V}(g_1,\dots,g_s)$, then

$$G(a_1,\dots,a_n)=f(g_1,\dots,g_s)(a_1,\dots,a_n)=f(g_1(a_1,\dots,a_n),\dots,g_s(a_1,\dots,a_n))=f(0,\dots,0)=0$$

and so $(a_1,\dots,a_n)\in \mathrm{V}(G)$. $\square$

Question 4.1.9: Let k be an arbitrary field and S be the subset of all polynomials in $k[x_1,\dots,x_n]$ that have no zeros in k^n. If I is an ideal in $k[x_1,\dots,x_n]$ such that $I\cap S=\emptyset$, then show that $\mathrm{V}(I)\neq\emptyset$.

Solution: Firstly suppose that k is an algebraically closed field. Suppose by contradiction that $\mathrm{V}(I)=\emptyset$, so, applying the Hilbert's Nullstellensatz, we obtain

$$\sqrt{I}=\mathrm{I}(\mathrm{V}(I))=\mathrm{I}(\emptyset)=k[x_1,\dots,x_n],$$

which means that $1\in I$, generating a contradiction, because $1\in S$.

Now suppose that k is not an algebraically closed field. By Question 4.1.8, there is $g\in k[x_1,\dots,x_n]$ such that $\mathrm{V}(I)=\mathrm{V}(g)$. Furthermore, looking carefully the solution of Question 4.1.8, we realize that g belongs to I and, since $I\cap S=\emptyset$, we conclude that $\mathrm{V}(I)=\mathrm{V}(g)\neq\emptyset$. $\square$

4.2 Radical Ideals and Ideal-Variety Correspondence

Question 4.2.11: Find a basis for the ideal

$$\sqrt{\langle x^5-2x^4+2x^2-x,\, x^5-x^4-2x^3+2x^2+x-1\rangle}.$$

Solution: Observe that $x^5-2x^4+2x^2-x=x(x-1)^3(x+1)$ and $x^5-x^4-2x^3+2x^2+x-1=(x-1)^3(x+1)^2$. Then

$$\begin{aligned} J &:= \langle x^5-2x^4+2x^2-x,\, x^5-x^4-2x^3+2x^2+x-1\rangle \\ &= \langle \gcd\{x(x-1)^3(x+1),(x-1)^3(x+1)^2\}\rangle=\langle (x-1)^3(x+1)\rangle. \end{aligned}$$

Hence $\sqrt{J}=\langle (x-1)(x+1)\rangle$. $\square$

Question 4.2.12: Let $f(x,y)=x^5+3x^4y+3x^3y^2-2x^4y^2+x^2y^3-6x^3y^3-6x^2y^4+x^3y^4-2xy^5+3x^2y^5+3xy^6+y^7\in\mathbb{Q}[x,y]$. Compute $\sqrt{\langle f\rangle}$.

Solution: Observing that $\sqrt{\langle f\rangle}=\langle f_{red}\rangle$, apply the Proposition 4.2.12 [1] $\square$

[1] Proved in Question 4.2.13 (ii) in this article.

Question 4.2.13: A field k has characteristic 0 if it contains a field isomorphic to the field $\mathbb{Q}$ of rational numbers; Otherwise, k has positive characteristic.

(i): Let k be a field of characteristic 0 and let $f \in k[x_1, \ldots, x_n]$ be a nonconstant polynomial. If the variable x_j appears in f, prove that $\partial f/\partial x_j \neq 0$.

(ii): Let k be a field of characteristic 0 and let $I = \langle f \rangle$ be a principal ideal in $k[x_1, \ldots, x_n]$. Prove that $\sqrt{\langle f \rangle} = \langle f_{red} \rangle$, where

$$f_{red} = \frac{f}{\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)}.$$

(iii): Prove that the part (ii) may fail if $\mathrm{char}(k) \neq 0$.

Solution: **(i):** Let f be a nonconstant polynomial and suppose that the variable x_j appears in f. Observe that we can write f as

$$f(x_1, \ldots, x_n) = \sum_{k=0}^{m} p_k(x_1, \ldots, \widehat{x_j}, \ldots, x_n) x_j^k,$$

where $p_m(x_1, \ldots, \widehat{x_j}, \ldots, x_n) \neq 0$ and $m \geq 1$ by hypothesis that the variable x_j appears in f. Deriving with respect x_j, we obtain

$$\frac{\partial f}{\partial x_j}(x_1, \ldots, x_n) = \sum_{k=0}^{m} k p_k(x_1, \ldots, \widehat{x_j}, \ldots, x_n) x_j^{k-1} = \sum_{k=0}^{m-1} (k+1) p_{k+1}(x_1, \ldots, \widehat{x_j}, \ldots, x_n) x_j^k$$

Note that $\partial f/\partial x_j \neq 0$, because $m p_m(x_1, \ldots, \widehat{x_j}, \ldots, x_n) x_j^{m-1} \neq 0$ and this term can not be annihilate by the others ones.

(ii): Since $k[x_1, \ldots, x_n]$ is an UFD, we can factor $f(x_1, \ldots, x_n) = f_1^{a_1} \cdots f_m^{a_m}$, where f_i is an irreducible polynomial and $a_i \geq 0$ for all $1 \leq i \leq m$. Note that

$$\sqrt{\langle f \rangle} = \sqrt{\langle f_1^{a_1} \cdots f_m^{a_m} \rangle} = \langle f_1 \cdots f_m \rangle.$$

Thus in order to prove the desired formula, it is enough to show that

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1 - 1} \cdots f_m^{a_m - 1}.$$

Note that

$$\frac{\partial f}{\partial x_i} = \sum_{k=1}^{m} \left(a_k f_1^{a_1} \cdots f_{k-1}^{a_{k-1}} f_k^{a_k - 1} f_{k+1}^{a_{k+1}} \cdots f_m^{a_m} \frac{\partial f_k}{\partial x_i} \right)$$
$$= f_1^{a_1 - 1} \cdots f_m^{a_m - 1} \sum_{k=1}^{m} \left(a_k f_1 \cdots f_{k-1} \widehat{f_k} f_{k+1} \cdots f_m \frac{\partial f_k}{\partial x_i} \right)$$

This gives us that $f_1^{a_1-1}\cdots f_m^{a_m-1}$ divides $\gcd\{f, \partial f/\partial x_1, \ldots, \partial f/\partial x_n\}$. Finally we just need to prove that, for each i, there is some $\partial f/\partial x_j$ such that it is not divisible by $f_i^{a_i}$. Write $f = f_i^{a_i} g$, where f_i does not divide g. Since f is not constant, some variable x_j must appear in f_i. The product rules gives us

$$\frac{\partial f}{\partial x_j} = a_i f_i^{a_i-1}\frac{\partial f_i}{\partial x_j} g + f_i^{a_i}\frac{\partial h}{\partial x_j} = f_i^{a_i-1}\left(a_i g\frac{\partial f_i}{\partial x_j} + f_i\frac{\partial h}{\partial x_j}\right).$$

If $\partial f/\partial x_j$ is divisible by $f_i^{a_i}$, then f_i must divide $h \cdot (\partial f_i/\partial x_j)$. Observe that this product is non-zero, because the variable x_j appears in f_i.

Since f_i is irreducible, then either f_i divides $\partial f_i/\partial x_j$ or f_i divides h. But the first option is not possible, because $\partial f_i/\partial x_j$ has total degree less than the the total degree of f_i. This implies that f_i divides h, which is a contradiction. Hence

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1}\cdots f_m^{a_m-1}.$$

(iii): Let $f(x_1, \ldots, x_n) = x_1^p + \cdots + x_n^p \in \mathbb{F}_p[x_1, \ldots, x_n]$. Note that

$$\frac{\partial f}{\partial x_i}(x_1, \ldots, x_n) = p x_i^{p-1} = 0$$

for all $i = 1, \ldots, n$. So

$$\frac{f}{\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)} = \frac{f}{f} = 1.$$

However clearly we have that $\sqrt{\langle f\rangle} \neq \langle 1\rangle$. $\square$

Question 4.2.15: Prove that the ideal $I = \langle xy, xz, yz\rangle$ is radical. *Solution:* Indeed calculating the Gröbner Basis for I with respect the lexicographic order $x > y > z$, we obtain $G = \{xy, xz, yz\}$. Since the monomials

$$\begin{cases} \mathrm{LT}(xy) = xy, \\ \mathrm{LT}(xz) = xz, \\ \mathrm{LT}(yz) = yz. \end{cases}$$

are square-free, by Question 4.2.16 (ii), we conclude that I is a radical ideal. $\square$

Question 4.2.16: Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Assume that I has Gröbner basis $G = \{g_1, \ldots, g_t\}$ such that for all i, $\mathrm{LT}(g_i)$ is square-free.

(i): If $f \in \sqrt{I}$, then $\mathrm{LT}(f)$ is divisible by $\mathrm{LT}(g_i)$ for some i.

(ii): Prove that I is radical.

Solution: **(i):** Let $f \in \sqrt{I}$ and $m \in \mathbb{N}$ such that $f^m \in I$. Since $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$ is a monomial ideal, we have that $\mathrm{LT}(f^m)$ is divisible by $\mathrm{LT}(g_i)$ for some i. However, since $\mathrm{LT}(f^m) = \mathrm{LT}(f)^m$ and $\mathrm{LT}(g_i)$ is square-free, then $\mathrm{LT}(f)$ is certainly divisible by $\mathrm{LT}(g_i)$.

(ii): By item (i) we conclude that $\langle \mathrm{LT}(\sqrt{I})\rangle \subseteq \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$. The other inclusion is trivial, because $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle \subseteq \langle \mathrm{LT}(I)\rangle \subseteq \langle \mathrm{LT}(\sqrt{I})\rangle$. Thus

$$\langle \mathrm{LT}(\sqrt{I})\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle,$$

with $g_1, \ldots, g_t \in I \subseteq \sqrt{I}$, which implies that G is a Gröbner basis for $\sqrt{I}$. But, since $G = \{g_1, \ldots, g_t\}$ also is Gröbner basis for I, then

$$I = \langle g_1, \ldots, g_t\rangle = \sqrt{I},$$

which implies that I is a radical ideal. $\square$

Question 4.2.17:

(i) Prove that a monomial ideal in $k[x_1, \ldots, x_n]$ is radical if and only if its minimal generators are square free.

(ii) Given an ideal $I \subseteq k[x_1, \ldots, x_n]$, prove that if $\langle \mathrm{LT}(I)\rangle$ is radical, then I is radical.

(iii) Give an example to show that the converse of part (ii) can fail.

Solution: **(i):** Let I be a monomial ideal and let $\{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_m}\}$ be a minimal basis for I. Suppose that one of its minimal generators $\mathbf{x}^{\alpha_i}$, with $\alpha_i = (a_1, \ldots, a_n)$ is not square-free. It means that there is $1 \leq j \leq n$ such that $a_j \geq 2$. Consider the monomial

$$f(x_1, \ldots, x_n) = x_1^{\min\{1,a_1\}} x_2^{\min\{1,a_2\}} \cdots x_n^{\min\{1,a_n\}}$$

Observe that $f(x_1, \ldots, x_n) \notin I$, because, if f is divisible by some $\mathbf{x}^{\alpha_k}$, $k \neq i$, then $\alpha_k \leq (\min\{1, a_1\}, \cdots, \min\{1, a_n\})$. It would imply that $\alpha_k \leq \alpha_i$, which is impossible. Moreover f is not divisible by $\mathbf{x}^{\alpha_i}$, because $(\min\{1, a_1\}, \cdots, \min\{1, a_n\}) < (a_1, \ldots, a_n)$. On the other hand $f^{a_1+\cdots+a_n}$ is divisible by $\mathbf{x}^{\alpha_i}$ and so $f^{a_1+\cdots+a_n} \in I$. Thus I is not radical.

Now suppose that all minimal generators of I are square free. Let $\mathbf{x}^\alpha \in \sqrt{I}$ and suppose that $(\mathbf{x}^\alpha)^r = \mathbf{x}^{r\alpha} \in I$. Since I is monomial, then there is $1 \leq j \leq m$ such that $\alpha_j \leq r\alpha$. As the entries of α_j are either 0 or 1 because x^{α_j} is square free, then $\alpha_j \leq \alpha$, which implies that $\mathbf{x}^\alpha \in I$, so I is radical.

(ii): Let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis for I. Then $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle$. Since $\langle \mathrm{LT}(I) \rangle$ is radical, then each generator of $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle$ is square-free. By Question 4.2.16, we conclude that I is a radical ideal.

(iii) Consider the radical ideal $I = \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$. However note that the initial ideal $\langle \mathrm{LT}(I) \rangle = \langle x^2 \rangle$ clearly is not radical. $\square$

4.3 Sums, Products, and Intersections of Ideals

Question 4.3.11: Two ideals I and J of $k[x_1, \ldots, x_n]$ are said comaximal if and only if $I + J = k[x_1, \ldots, x_n]$.

(i) Show that if $k = \mathbb{C}$, then I and J are comaximal if and only if $\mathrm{V}(I) \cap \mathrm{V}(J) =$. Give a example that it is false in general.

(ii) Show that if I and J are comaximal ideals, then $IJ = I \cap J$.

(iii) Is the converse of (ii) true?

(iv) If I and J are comaximal ideals, prove that I^r and J^s are comaximal idelas for all positive integers r and s.

(v) Let $I_1, \ldots, I_r$ be idals in $k[x_1 \ldots, x_n]$ and suppose that I_i and $J_i := \bigcap_{j \neq i} I_j$ are comaximal ideals for all i. Show that

$$I_1^m \cap \cdots \cap I_r^m = (I_1 \cdots I_r)^m = (I_1 \cap \cdots \cap I_r)^m$$

for all integers m.

Solution: **(i):** Suppose that I and J are comaximal ideals, then

$$\mathrm{V}(I) \cap \mathrm{V}(J) = \mathrm{V}(I + J) = \mathrm{V}(k[x_1, \ldots, x_n]) = \emptyset.$$

Conversely suppose that $\mathrm{V}(I) \cap \mathrm{V}(J) = \emptyset$, thus, by Hilbert's Nullstellensatz, we obtain

$$\sqrt{I + J} = \mathrm{I}(\mathrm{V}(I + J)) = \mathrm{I}(\mathrm{V}(I) \cap \mathrm{V}(J)) = \mathrm{I}(\emptyset) = k[x_1, \ldots, x_n],$$

which implies that $I + J = k[x_1, \ldots, x_n]$. Consider $k = \mathbb{R}$ and $I = \langle x^2 + y^2 + 1 \rangle$, $J = \langle yx \rangle$. Observe that $\mathrm{V}(I) \cap \mathrm{V}(J) = \emptyset$, but $I + J = \langle x^2 + y^2 + 1, xy \rangle \neq k[x_1, \ldots, x_n]$.

(ii): As $IJ \subseteq I \cap J$ always holds, it is sufficient to prove the reverse inclusion. Let $g \in I$ and $h \in J$ such that $g + h = 1$. Given $f \in I \cap J$, then $f = fg + fh$. Observe that

$$\begin{aligned} fg \in IJ, &\text{ because } g \in I \text{ and } f \in J, \\ fh \in IJ, &\text{ because } f \in I \text{ and } h \in J. \end{aligned}$$

Thus $f = fg + fh \in IJ$ and $I \cap J \subseteq IJ$.

(iii): The converse is false. Indeed consider $I = \langle x^2 + y^2 + 1 \rangle$ and $J = \langle x^2 + 1 \rangle$. Note that $IJ = I \cap J$, but $I + J \neq k[x_1, \ldots, x_n]$.

(iv): Firtly we will prove that I and J^s are comaximal ideals. Indeed, as I and J are comaximal, there are $f \in I$ and $g \in J$ such that $f + g = 1$, thus

$$1 = (f+g)^s = \sum_{k=0}^{s} \binom{s}{k} f^k g^{s-k} = g^s + \sum_{k=1}^{s} \binom{s}{k} f^k g^{s-k} = g^s + f \left(\sum_{k=1}^{s} \binom{s}{k} f^{k-1} g^{s-k} \right) \in J^s + I,$$

so J^s and I are comaximal ideals, because $1 \in J^s + I$. Now, since I and J^s are comaximal, switching I by J^s, J by I and applying the same proceeding above for $s = r$, one concludes that I^r and J^s are comaximal ideals.

(v): We will proceed by induction on r. If $r = 1$, the statement holds trivially. For $r = 2$, hypothesis reduces to say that I_1 and I_2 are comaximals. Since we already proved that I_1^m and I_2^m are comaximal, so $(I_1 I_2)^m = I_1^m I_2^m = I_1^m \cap I_2^m$. Moreover, as $I_1 \cap I_2 = I_1 I_2$, so $(I_1 \cap I_2)^m = (I_1 I_2)^m$. Hence

$$I_1^m \cap I_2^m = (I_1 I_2)^m = (I_1 \cap I_2)^m.$$

Suppose that the statement holds for $r = n$ and let $I_1, \ldots, I_n, I_{n+1}$ ideals such that I_i and $J_i := \bigcap_{j \neq i} I_j$ are comaximal ideals for all $i = 1, \ldots, n+1$. By hypothesis, we have that

$$I_{n+1} + \bigcap_{k=1}^{n} I_k = k[x_1, \ldots, x_n],$$

so

$$I_{n+1}^m \cap \left(\bigcap_{k=1}^{n} I_k \right)^m = I_{n+1}^m \left(\bigcap_{k=1}^{n} I_k \right)^m$$

Since I_i and $K'_j := \bigcap_{j\neq i}^n$ also are comaximal ideals for all $i = 1, \ldots, n$, we can apply the induction hypothesis and conclude that

$$\begin{aligned}\big(I_1 \cdots I_n \cdot I_{n+1}\big)^m = \big(I_1^m \cdots I_n^m\big) I_{n+1}^m = \left(\bigcap_{k=1}^n I_k\right)^m I_{n+1}^m = \left(\bigcap_{k=1}^n I_k\right)^m \cap I_{n+1}^m = \left(\bigcap_{k=1}^n I_k^m\right) \cap I_{n+1}^m \\ = \bigcap_{k=1}^{n+1} I_k^m.\end{aligned}$$

Furthermore, as I_i and $J_{n+1} := \bigcap_{j=1}^n I_j$ are comaximal ideals, applying the induction hypotesis again, we obtain

$$\left(\bigcap_{k=1}^{n+1} I_k\right)^m = \left(\left(\bigcap_{k=1}^n I_k\right) \cap I_{n+1}\right)^m = \left(\bigcap_{k=1}^n I_k\right)^m \cap I_{n+1}^m = \left(\bigcap_{k=1}^n I_k^m\right) \cap I_{n+1}^m = \bigcap_{k=1}^{n+1} I_k^m,$$

which proves the statement. $\square$

Question 4.3.13: Let A be an $m \times n$ constant matrix and suppose that $x = (x_1, \ldots, x_m) = A \cdot (y_1, \ldots, y_n) = A \cdot y$, where we are think $x \in k^m$ and $y \in k^n$ as columns vectors of variables. Define the map

$$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n]$$

by sending $f \in k[x_1, \ldots, x_m]$ to $\alpha_A(f) \in k[y_1, \ldots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.

(i): Show that α_A is k-linear homomorphism of k-modules.

(ii): Show that α_A is ring homomorphism.

(iii): Show that $\ker(\alpha_A) = \{f \in k[x_1, \ldots, x_m] \ ; \ \alpha_A(f) = 0\}$ is an ideal of $k[x_1, \ldots, x_m]$.

(iv): Given I an ideal of $k[x_1, \ldots, x_m]$, prove that $\alpha_A(I) = \{\alpha_A(f) \ ; \ f \in I\}$ is not necessarily an ideal of $k[y_1, \ldots, y_n]$. We denote $\langle \alpha_A(I) \rangle$ the ideal generated by $\alpha_A(I)$ and it is called the extension of I to $k[y_1, \ldots, y_n]$ under A.

(v): If I' is an ideal of $k[y_1, \ldots, y_n]$, show that $\alpha_A^{-1}(I') = \{f \in k[x_1, \ldots, x_m] \ ; \ \alpha_A(f) \in I'\}$ is an ideal of $k[x_1, \ldots, x_m]$. This ideal is called the contraction of I' in $k[x_1, \ldots, x_m]$ under A.

Solution: **(i):** Denoting $A = [a_{ij}]$, then

$$\alpha_A(f)(y_1, \ldots, y_n) = f\left(\sum_{k=1}^n a_{1k} y_k, \ldots, \sum_{k=1}^n a_{mk} y_k\right)$$

for any $f \in k[x_1, \ldots, m]$. Thus, given $f, g \in k[x_1, \ldots, x_m]$ and $\lambda \in k$, we have

$$\alpha_A(f + \lambda g)(y_1, \ldots, y_n) = (f + \lambda g)\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right) = f\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right) +$$
$$\lambda g\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right) = \alpha_A(f)(y_1, \ldots, y_n) + \lambda\alpha_A(g)(y_1, \ldots, y_n)$$
$$= (\alpha_A(f) + \lambda\alpha_A(g))(y_1, \ldots, y_n),$$

which implies that $\alpha_A(f + \lambda g) = \alpha_A(f) + \lambda\alpha_A(g)$ and so α_A is k-linear.

(ii): Given f, $g \in k[x_1, \ldots, x_m]$, we have

$$\alpha_A(f \cdot g)(y_1, \ldots, y_n) = (f \cdot g)\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right)$$
$$= f\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right) \cdot g\left(\sum_{k=1}^{n} a_{1k}y_k, \ldots, \sum_{k=1}^{n} a_{mk}y_k\right)$$
$$= \alpha_A(f)(y_1, \ldots, y_n) \cdot \alpha_A(g)(y_1, \ldots, y_n) = \big(\alpha_A(f) \cdot \alpha_A(g)\big)(y_1, \ldots, y_n),$$

so $\alpha_A(f \cdot g) = \alpha_A(f) \cdot \alpha_A(g)$. Since $\alpha_A(1)(y_1, \ldots, y_n) = 1$, one concludes that α_A is a ring homomorphism.

(iii): Since α_A is a ring homomorphism, $\ker(\alpha_A)$ is an ideal of $k[x_1, \ldots, x_m]$.

(iv): The image of an ideal under α_A will be an ideal of $k[y_1, \ldots, y_n]$ if and only if α_A is surjective. If A is the zero matrix, then α_A is the evaluation at $(0, \ldots, 0) \in k^m$, so $\alpha_A(k[x_1, \ldots, x_m]) = k \subsetneq k[y_1, \ldots, y_n]$, so $\alpha_A(k[x_1, \ldots, x_m])$ is not ideal.

(v):[2] Let $I' \subseteq k[y_1, \ldots, y_n]$ be an ideal. Note that $0 \in \alpha_A^{-1}(I')$, because $\alpha_A(0) = 0 \in I'$. Given f and g in $\alpha_A^{-1}(I')$, we have that $\alpha_A(f) \in I'$ and $\alpha_A(g) \in I'$, thus

$$\alpha_A(f + g) = \alpha_A(f) + \alpha_A(g) \in I',$$

so $f + g \in \alpha_A^{-1}(I')$. Finally let $f \in \alpha_A^{-1}(I')$ and $g \in k[x_1, \ldots, x_m]$. Since

$$\alpha_A(g \cdot f) = \alpha_A(g) \cdot \alpha_A(f) \in I',$$

one concludes that $g \cdot f \in \alpha_A^{-1}(I')$ and so $\alpha_A^{-1}(I')$ is an ideal of $k[x_1, \ldots, x_m]$. $\square$

Question 4.3.14: Let A and α_A be as in Question 4.1.13 and let $K = \ker(\alpha_A)$. Let I and J be ideals of $k[x_1, \ldots, x_m]$. Show that

[2] A simpler solution: The contraction of ideals always is an ideal, because α_A is a ring homomorphism.

(i): If $I \subseteq J$, then $\langle \alpha_A(I) \rangle \subseteq \langle \alpha_A(J) \rangle$.

(ii): $\langle \alpha_A(I+J) \rangle = \langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle$.

(iii): $\langle \alpha_A(I \cdot J) \rangle = \langle \alpha_A(I) \rangle \cdot \langle \alpha_A(J) \rangle$.

(iv): $\langle \alpha_A(I \cap J) \rangle \subseteq \langle \alpha_A(I) \rangle \cap \langle \alpha_A(J) \rangle$, with equality if $K \subseteq I$ or $K \subseteq J$ and α_A is onto.

(v): $\langle \alpha_A(\sqrt{I}) \rangle \subseteq \sqrt{\langle \alpha_A(I) \rangle}$, with equality if $K \subseteq I$ and α_A is onto.

Solution: **(i):** Note that, since $I \subseteq J$, we have

$$\{\alpha_A(f) \ ; \ f \in I\} \subseteq \{\alpha_A(f) \ ; \ f \in J\}.$$

Hence

$$\langle \alpha_A(I) \rangle = \langle \{\alpha_A(f) \ ; \ f \in I\} \rangle = \langle \{\alpha_A(f) \ ; \ f \in J\} \rangle = \langle \alpha_A(J) \rangle.$$

(ii): Let $L \in \langle \alpha_A(I+J) \rangle$, then there are $h_1, \ldots, h_r \in k[y_1, \ldots, y_n]$, $f_1, \ldots, f_r \in I$ and $g_1, \ldots, g_r \in J$ such that $L = \sum_{k=1}^r h_k \alpha_A(f_k + g_k)$. As

$$L = \sum_{k=1}^r h_k \alpha_A(f_k + g_k) = \sum_{k=1}^r h_k \alpha_A(f_k) + \sum_{k=1}^r h_k \alpha_A(g_k) \in \langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle,$$

then $\langle \alpha_A(I+J) \rangle \subseteq \langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle$.

Conversely observe that $\langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle$ is generated by $\{\alpha_A(f) \ ; \ f \in I\} \cup \{\alpha_A(g) \ ; \ g \in J\}$ and

$$\{\alpha_A(f) \ ; \ f \in I\} \cup \{\alpha_A(g) \ ; \ g \in J\} \subseteq \{\alpha_A(f+g) \ ; \ f \in I, \, g \in J\},$$

where the last set is set of generators of $\langle \alpha_A(I+J) \rangle$, so $\langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle \subseteq \langle \alpha_A(I+J) \rangle$.

(iii): Note that

$$\begin{aligned} \langle \alpha_A(I \cdot J) \rangle = \langle \{\alpha_A(f \cdot g) \ ; \ f \in I, \, g \in J\} \rangle &= \langle \{\alpha_A(f) \cdot \alpha_A(g) \ ; \ f \in I, \, g \in J\} \\ &= \langle \alpha_A(I) \rangle \cdot \langle \alpha_A(J) \rangle. \end{aligned}$$

(iv): Since $I \cap J \subseteq I$ and $J \subseteq I \cap J$, the part (i) says that $\langle \alpha_A(I \cap J) \rangle \subseteq \langle \alpha_A(I) \rangle$ and $\langle \alpha_A(I \cap J) \rangle \subseteq \langle \alpha_A(J) \rangle$. Thus

$$\langle \alpha_A(I \cap J) \rangle \subseteq \langle \alpha_A(I) \rangle \cap \langle \alpha_A(J) \rangle.$$

Suppose that α_A is onto and $K \subseteq I$. The main point here is that, when α_A is onto, we have $\langle \alpha_A(J) \rangle = \alpha_A(J)$ for any ideal $J \subseteq k[x_1, \ldots, x_m]$. Let $f \in \alpha_A(I) \cap \alpha_A(J)$, thus there exist $g \in I$ and $h \in J$ such that $\alpha_A(g) = f = \alpha_A(h)$. As

$$\alpha_A(g - h) = \alpha_A(g) - \alpha_A(h) = f - f = 0,$$

we have that $g - h \in K \subseteq I$. Hence $h \in I \cap J$ and $f = \alpha_A(h) \in \alpha_A(I \cap J) = \langle \alpha_A(I \cap J) \rangle$.

(v): Let $h \in \langle \alpha_A(\sqrt{I}) \rangle$, there are $h_1, \ldots, h_r \in k[y_1, \ldots, y_n]$ and $f_1, \ldots, f_r \in \sqrt{I}$ such that

$$L = \sum_{k=1}^{r} g_k \alpha_A(f_k)$$

As $f_1, \ldots, f_r \in \sqrt{I}$, we can suppose without lost of generality that there is $N \in \mathbb{N}$ such that $f_1^N, \ldots, f_r^N \in I$, so $L^{rN} =$

$$\sum_{t_1+\cdots+t_r=rN} c_{t_1,\ldots t_r} \alpha_A(f_1)^{t_1} \alpha_A(f_2)^{t_2} \cdots \alpha_A(f_r)^{t_r} = \sum_{t_1+\cdots+t_r=rN} c_{t_1,\ldots t_r} \alpha_A(f_1^{t_1}) \alpha_A(f_2^{t_2}) \cdots \alpha_A(f_r^{t_r})$$

Since $t_1 + \cdots + t_r = rN$, each term of this sum is such that there is $1 \leq i \leq r$ such that $t_i \geq N$, which implies that each $c_{t_1,\ldots t_r} \alpha_A(f_1^{t_1}) \alpha_A(f_2^{t_2}) \cdots \alpha_A(f_r^{t_r})$ belongs to $\langle \alpha_A(I) \rangle$, so $L^{rN} \in \langle \alpha_A(I) \rangle$ and $L \in \sqrt{\langle \alpha_A(I) \rangle}$.

Let $f \in \sqrt{\langle \alpha_A(I) \rangle}$, so there is $r \in \mathbb{N}$ such that $f^r \in \langle \alpha_A(I) \rangle = \alpha_A(I)$, which implies that $g \in I$ such that $\alpha_A(g) = f^r$. On the other hand, as α_A is onto, there is $h \in k[x_1, \ldots, x_m]$ such that $\alpha_A(h) = f$. As

$$\alpha_A(g - h^r) = \alpha_A(g) - \alpha_A(h)^r = f^r - f^r = 0,$$

then $g - h^r \in K \subseteq I$ and so $h^r \in I$. Finally, since $h \in \sqrt{I}$ and $\alpha_A(h) = f$, we conclude that $f \in \alpha_A(\sqrt{I})$ and we obtain the desired equality. $\square$

Question 4.3.15: Let A and α_A be as in Question 4.1.13 and let $K = \ker(\alpha_A)$. Let I' and J' be ideals of $k[y_1, \ldots, y_n]$. Show that

(i): If $I' \subseteq J'$, then $\alpha_A^{-1}(I') \subseteq \alpha_A^{-1}(J')$.

(ii): $\alpha_A^{-1}(I' + J') \supseteq \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$, with equality if α_A is onto.

(iii): $\alpha_A^{-1}(I' \cdot J') \supseteq \alpha_A^{-1}(I') \cdot \alpha_A^{-1}(J')$, with equality if α_A is onto and the right-hand side contains K.

(iv): $\alpha_A^{-1}(I' \cap J') = \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$.

(v): $\alpha_A^{-1}(\sqrt{I'}) = \sqrt{\alpha_A^{-1}(I')}$.

Solution: **(i):** Let $f \in \alpha_A^{-1}(I')$, so $\alpha_A(f) \in I' \subseteq J'$, which implies that $f \in \alpha_A^{-1}(J')$ and so $\alpha_A^{-1}(I') \subseteq \alpha_A^{-1}(J')$.

(ii): Let $f + g \in \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$, where $f \in \alpha_A^{-1}(I')$ and $g \in \alpha_A^{-1}(J')$. Then $\alpha_A(f) \in I'$ and $\alpha_A(g) \in J'$, which implies that

$$\alpha_A(f + g) = \alpha_A(f) + \alpha_A(g) \in I' + J',$$

which implies that $f + g \in \alpha_A^{-1}(I' + J')$ and so $\alpha_A^{-1}(I' + J') \supseteq \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$.

Now suppose that α_A is onto and let $f \in \alpha_A^{-1}(I' + J')$, then $\alpha_A(f) \in I' + J'$. Let $g' \in I'$ and $h' \in J'$ such that $\alpha_A(f) = g' + h'$. As α_A is onto, there are $g,\ h \in k[x_1, \dots, x_m]$ such that $g' = \alpha_A(g)$ and $h' = \alpha_A(h)$, thus

$$\alpha_A(f - (g + h)) = \alpha_A(f) - \alpha_A(g) - \alpha_A(h) = \alpha_A(f) - g' - h' = 0,$$

which implies that $f - (g + h) = k \in K$. Thus $f = (g + k) + h$. Since $g + k \in \alpha_A^{-1}(I')$ and $h \in \alpha_A^{-1}(J')$, we conclude that $f \in \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$ and so $\alpha_A^{-1}(I' + J') = \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$.

(iii): Let $f \in \alpha_A^{-1}(I') \cdot \alpha_A^{-1}(J')$, then there are $s \in \mathbb{N}$, $g_1, \dots, g_s \in \alpha_A^{-1}(I')$ and $h_1, \dots, h_s \in \alpha_A^{-1}(J')$ such that

$$f = \sum_{k=1}^{s} g_k h_k,$$

so

$$\alpha_A(f) = \alpha_A\left(\sum_{k=1}^{s} g_k h_k\right) = \sum_{k=1}^{s} \alpha_A(g_k h_k) = \sum_{k=1}^{s} \alpha_A(g_k)\alpha_A(h_k) \in I'J',$$

which implies that $f \in \alpha_A^{-1}(I'J')$ and $\alpha_A^{-1}(I'J') \supseteq \alpha_A^{-1}(I') \cdot \alpha_A^{-1}(J')$.

Suppose that α_A is onto and the right-hand side contains K. Let $f \in \alpha_A^{-1}(I'J')$, so there are $s \in \mathbb{N}$, $g'_1, \dots, g'_s \in I'$ and $h'_1, \dots, h'_s \in J'$ such that

$$\alpha_A(f) = \sum_{k=1}^{s} g'_k h'_k.$$

As α_A is onto, there are $g_1, \dots, g_s, h_1, \dots, h_s \in k[x_1, \dots, x_m]$ such that $\alpha_A(g_i) = g'_i$ and $\alpha_A(h_i) = h'_i$ for all $1 \le i \le s$. Thus

$$\alpha_A\left(f - \sum_{k=1}^{s} g_k h_k\right) = \alpha_A(f) - \sum_{k=1}^{s} \alpha_A(g_k)\alpha_A(h_k) = \alpha_A(f) - \sum_{k=1}^{s} g'_k h'_k = 0,$$

so $f = \sum_{k=1}^{s} g_k h_k + z$, where $z \in K$. Finally, since $g_k \in \alpha_A^{-1}(I')$, $h_k \in \alpha_A^{-1}(J')$ for all $1 \le k \le s$ and $k \in K \subseteq \alpha_A^{-1}(I') \cdot \alpha_A^{-1}(J')$, one concludes that $f \in \alpha_A^{-1}(I') \cdot \alpha_A^{-1}(J')$.

(iv): Note that, since $I \cap J \subseteq I$ and $I \cap J \subseteq J$, then $\alpha_A^{-1}(I' \cap J') \subseteq \alpha_A^{-1}(I')$ and $\alpha_A^{-1}(I' \cap J') \subseteq \alpha_A^{-1}(J')$, so $\alpha_A^{-1}(I' \cap J') \subseteq \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$.

On the other hand, given $f \in \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$, then $\alpha_A(f) \in I'$ and $\alpha_A(f) \in J'$, which implies that $\alpha_A(f) \in I' \cap J'$ and so $f \in \alpha_A^{-1}(I \cap J)$.

(v): Let $f \in \alpha_A^{-1}(\sqrt{I'})$, then there are $s \in \mathbb{N}$ such that $\alpha_A(f)^s \in I'$. So $f^s \in \alpha_A^{-1}(I')$ and $f \in \sqrt{\alpha_A^{-1}(I')}$, which implies that $\alpha_A^{-1}(\sqrt{I'}) \subseteq \sqrt{\alpha_A^{-1}(I')}$.

On the other hand, given $f \in \sqrt{\alpha_A^{-1}(I')}$, then $f^s \in \alpha_A^{-1}(I')$ for some $s \in \mathbb{N}$, which implies that $\alpha_A(f^s) = \alpha_A(f)^s \in I'$ and $\alpha_A(f) \in \sqrt{I'}$. Thus $f \in \alpha_A^{-1}(\sqrt{I'})$ and $\sqrt{\alpha_A^{-1}(I')} \subseteq \alpha_A^{-1}(\sqrt{I'})$. $\square$

4.4 Zariski Closures, Ideals Quotients, and Saturations

Question 4.4.4: Let I and J be ideals of $R = k[x_1, \ldots, x_n]$. Suppose that I is a radical ideal. Then

(i): Prove that $I :_R J$ is an radical ideal.

(ii): Prove that $I :_R J = I :_R \sqrt{J} = I :_R J^\infty$.

Solution: **(i):** Let $x \in \sqrt{I :_R J}$, thus there is $m \in \mathbb{N}$ such that $x^m J \subseteq I$. Given $y \in J$, note that $(xy)^m = x^m y^m \in I$. As I is a radical ideal, one has that $xy \in I$. Finally, since $y \in J$ was chosen arbitrarily, we conclude that $x \in I :_R J$ and so $\sqrt{I :_R J} \subseteq I :_R J$. As the other inclusion always holds, the statement follows.

(ii): As $J \subseteq \sqrt{J}$, the inclusion $I :_R \sqrt{J} \subseteq I :_R J$ is clear. Let $x \in I :_R J$ and $y \in \sqrt{J}$. Thus there is $m \in \mathbb{N}$ such that $(xy)^m = x^{m-1}(xy^m) \in I$. As I is a radical ideal, we conclude that $xy \in I$ and, since $y \in \sqrt{J}$ was chosen arbitrarily, one concludes that $x \in I :_R \sqrt{J}$ and $I :_R J \subseteq I :_R \sqrt{J}$.

Next observe that $I :_R J \subseteq I :_R J^\infty$ always holds by definition. Let $x \in I :_R J^\infty$ and $y \in J$. By definition there exists $m \in \mathbb{N}$ such that $y \in I :_R J^m$ and so $(xy)^m = x^{m-1}(xy^m) \in I$. As I is a radical ideal, we conclude that $xy \in I$ and, since $y \in J$ was chosen arbitrarily, one concludes that $x \in I :_R J$ and $I :_R J^\infty \subseteq I :_R J$. $\square$

Question 4.4.8: Let V, $W \subseteq k^n$ be varieties. Prove that $\mathrm{I}(V) :_R \mathrm{I}(W) = \mathrm{I}(V \setminus W)$.

Solution: Let $f \in \mathrm{I}(V \setminus W)$ and $g \in \mathrm{I}(W)$. We have to prove that $fg \in \mathrm{I}(V)$. Indeed let

$x \in V$. If $x \in W$, then $(fg)(x) = f(x)g(x) = f(x) \cdot 0 = 0$. Otherwise $x \in V \smallsetminus W$ and so $(fg)(x) = f(x)g(x) = 0 \cdot g(x) = 0$. Thus $fg \in \mathrm{I}(V)$ and, as $g \in \mathrm{I}(W)$ was chosen arbitrarily, we conclude that $f \in \mathrm{I}(V) :_R \mathrm{I}(W)$.

Conversely, given $f \in \mathrm{I}(V) :_R \mathrm{I}(W)$, we have to prove that $f(x) = 0$ for all $x \in V \smallsetminus W$. Let $x \in V \smallsetminus W$. As $W = \mathrm{V}(g_1, \ldots, g_m)$ is a variety and $x \notin W$, there is $1 \leq i = i(x) \leq m$ such that $g_i(x) \neq 0$. Note that $g_i \in \mathrm{I}(W)$, thus, as $fg_i \in \mathrm{I}(V)$, $(fg_i)(x) = f(x)g_i(x) = 0$ and we conclude that $f(x) = 0$. Since $x \in V \smallsetminus W$ was chosen arbitrarily, we prove that $f \in \mathrm{I}(V \smallsetminus W)$ and so $\mathrm{I}(V) :_R \mathrm{I}(W) \subseteq \mathrm{I}(V \smallsetminus W)$. $\square$

Question 4.4.14: Let I, J be ideals of $k[x_1, \ldots, x_r]$. Prove that $I :_R J^\infty = I :_R J^N$ if and only if $I :_R J^N = I :_R J^{N+1}$. Then use this to describe an algorithm for computing the saturation $I :_R J^\infty$ based on the algorithm for computing ideal quotients.

Solution: Remember that $I :_R J^\infty = \bigcup_{k=1}^\infty I :_R J$ and that

$$I :_R J \subseteq I :_R J^2 \subseteq I :_R J^3 \subseteq \cdots \subseteq I :_R J^N \subseteq I :_R J^{N+1} \subseteq \cdots .$$

Thus if $I :_R J^\infty = I :_R J^N$, one has

$$I :_R J^N \subseteq I :_R J^{N+1} \subseteq I :_R J^\infty = I :_R J^N,$$

so $I :_R J^N = I :_R J^{N+1}$.

Conversely suppose that $I :_R J^\infty = I :_R J^N$, in order to prove that $I :_R J^\infty = I :_R J^N$, it is enough to prove that $I :_R J^N = I :_R J^{N+n}$ for all $n \in \mathbb{N}$. We will proceed by induction on n. For $n = 1$, the equality holds by hypothesis. Suppose that the equality holds for $n = m$, that is, $I :_R J^N = I :_R J^{N+m}$. By Question 4.4.16 (*ii*), one has that

$$I :_R J^{N+(m+1)} = I :_R (J^{N+m}J) = (I :_R J^{N+m}) :_R J = (I :_R J^N) :_R J = I :_R J^{N+1} = I :_R J^N.$$

By Induction principle, we have that $I :_R J^N = I :_R J^{N+n}$ for all $n \in \mathbb{N}$, so

$$I :_R J^\infty = \bigcup_{k=1}^{\infty} (I :_R J^k) = \bigcup_{k=N}^{\infty} (I :_R J^k) = \bigcup_{k=N}^{\infty} (I :_R J^N) = I :_R J^N.$$

Finally consider $J = \langle f_1, \ldots, f_r \rangle$. We know that $I :_R J^\infty = \bigcap_{k=1}^r (I :_R (f_k)^\infty)$. Let $m_k = m(k)$ be the first integer $I :_R (f_k)^{m_k} = I :_R (f_k)^{m_k+1}$ for all $k = 1, \ldots, r$. We just proved that $I :_R (f_k)^\infty = I :_R (f_k)^{m_k}$. Thus, setting $m := \max\{m_1, \ldots, m_r\}$, we still have that $I :_R (f_k)^\infty = I :_R (f_k)^m$ for all $k = 1, \ldots, r$, hence

$$I :_R J^\infty = \bigcap_{k=1}^{r} (I :_R (f_k)^\infty) = \bigcap_{k=1}^{r} (I :_R (f_k)^m) = I :_R J^m.$$

$\square$

Question 4.4.15: Show that N can be arbitrarily large in $J :_R I^\infty = J :_R I^N$.

Solution: Consider the ideals $I = \langle x^N \rangle$ and $J = \langle x \rangle$ of $R := k[x]$. Note that

$$I :_R J^i = \langle x^N \rangle :_R \langle x^i \rangle = \langle x^{N-i} \rangle$$

for all $1 \leq i \leq N-1$, thus

$$I :_R J \subsetneq I :_R J^2 \subsetneq I :_R J^2 \subsetneq \cdots \subsetneq I :_R J^{N-1} \subsetneq I :_R J^N = I :_R J^{N+1} = k[x].$$

$\square$

Question 4.4.16: Let I, J and K be ideals of $R = k[x_1, \ldots, x_n]$. Prove the following

(i): $IJ \subseteq K$ if and only if $I \subseteq K :_R J$;

(ii): $(I :_R J) :_K = I :_R JK$.

Solution: **(i):** Suppose that $IJ \subseteq K$. Given $x \in I$, we have $xJ \subseteq IJ \subseteq K$, so $x \in K :_R J$ and $I \subseteq K :_R J$. Conversely suppose that $I \subseteq K :_R J$. Let $z \in IJ$, so there are $m \in \mathbb{N}$, $a_1, \ldots, a_m \in I$ and $b_1, \ldots, b_m \in J$ such that

$$z = \sum_{k=1}^{m} a_k b_k.$$

As $I \subseteq K :_R J$, then $a_k b_k \in K$ for all $1 \leq k \leq m$, thus $z \in K$ and $IJ \subseteq K$.

(ii): Let $x \in (I :_R J) :_R K$. Observe that $xK \subseteq I :_R J$, which implies that $x(JK) = (xK)J \subseteq I$ by part (i). Thus $x \in I :_R JK$ and $(I :_R J) :_K \subseteq I :_R JK$.

Conversely let $x \in I :_R JK$. By definition, $(xK)J = x(JK) \subseteq I$, which implies that $xK \subseteq I :_R J$. Invoking the part (i) again, one concludes that $x \in (I :_R J) :_R K$ and so $I :_R JK \subseteq (I :_R J) :_R K$. $\square$

Question 4.4.17: Consider the ideals $I_1, \ldots, I_r, J \subseteq R = k[x_1, \ldots, x_n]$.

(i) Prove that

$$\left(\bigcap_{k=1}^{r} I_k \right) :_R J = \bigcap_{k=1}^{r} (I_k :_R J).$$

(ii) Prove that

$$\left(\bigcap_{k=1}^{r} I_k \right) :_R J^\infty = \bigcap_{k=1}^{r} (I_k :_R J^\infty).$$

Solution: **(i):** Let $f \in \left(\bigcap_{k=1}^{r} I_k\right) :_R J$, then $fJ \subseteq \bigcap_{k=1}^{r} I_k \subseteq I_i$ for all $i = 1, \dots, r$, which implies that $f \in I_i : J$ for all $i = 1, \dots, r$ and so

$$f \in \bigcap_{k=1}^{r} (I_k :_R J).$$

Conversely let $f \in \bigcap_{k=1}^{r} (I_k :_R J)$, thus $f \in I_k :_R J$ for all $k = 1, \dots, r$. This means that $fJ \subseteq I_K$ for all $k = 1, \dots, r$, which implies that $fJ \subseteq \left(\bigcap_{k=1}^{r} I_k\right)$ and so

$$f \in \left(\bigcap_{k=1}^{r} I_k\right) :_R J.$$

(ii): Let $f \in \left(\bigcap_{k=1}^{r} I_k\right) :_R J^\infty$, so there is $N \in \mathbb{N}$ such that $fJ^N \subseteq \bigcap_{k=1}^{r} I_k \subseteq I_k$ for all $k = 1, \dots, r$. This implies that $f \in I_k :_R J^N \subseteq I_k :_R J^\infty$ for all $k = 1, \dots, r$ and so

$$f \in \bigcap_{k=1}^{r} (I_k :_R J^\infty).$$

Conversely let $f \in \bigcap_{k=1}^{r} (I_k :_R J^\infty)$. Thus $f \in I_k :_R J^\infty$ for all $k = 1, \dots, r$ and so there are $m_k = m(k) \in \mathbb{N}$ such that $fJ^{m_k} \subseteq I_k$ for $k = 1, \dots, r$. Taking $m := \max\{m_1, \dots, m_r\}$, one obtains

$$fJ^m \subseteq fJ^{m_k} \subseteq I_k$$

for all $k = 1, \dots, r$, which implies that

$$f \in \left(\bigcap_{k=1}^{r} I_k\right) :_R J^m \subseteq \left(\bigcap_{k=1}^{r} I_k\right) :_R J^\infty.$$

$\square$

Question 4.4.18: Let A be an $m \times n$ constant matrix and suppose that $x = (x_1, \dots, x_m) = A \cdot (y_1, \dots, y_n) = A \cdot y$, where we are think $x \in k^m$ and $y \in k^n$ as columns vectors of variables. Define the map

$$\alpha_A : k[x_1, \dots, x_m] \longrightarrow k[y_1, \dots, y_n]$$

by sending $f \in k[x_1, \dots, x_m]$ to $\alpha_A(f) \in k[y_1, \dots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.

(i): Given ideals $I,\ J \subseteq k[x_1, \dots, x_m]$, prove that $\langle \alpha_A(I :_R J) \rangle \subseteq \langle \alpha_A(I) \rangle :_R \langle \alpha_A(J) \rangle$ with equality if $I \supseteq K := \ker(\alpha_A)$ and α_A is onto.

(ii): Given ideals $I',\ J' \subseteq k[y_1,\dots,y_n]$, how that $\alpha_A^{-1}(I' :_R J') = \alpha_A^{-1}(I') :_R \alpha_A^{-1}(J')$ when α_A is onto.

Solution: **(i):** It is enough to show that if $f \in \alpha_A(I :_R J)$, then $f \in \langle \alpha_A(I)\rangle :_R \langle \alpha_A(J)\rangle$. Given $f \in \alpha_A(I :_R J)$, then $f = \alpha_A(g)$ for some $g \in I :_R J$. Let $h \in \langle \alpha_A(J)\rangle$, then there are $r \in \mathbb{N}$, $g_1,\dots,g_r \in k[y_1,\dots,y_n]$ and $f_1,\dots,f_r \in J$ such that

$$h = \sum_{k=1}^{r} g_k \alpha_A(f_k)$$

Thus

$$f \cdot h = \alpha_A(g)\left(\sum_{k=1}^{r} g_k \alpha_A(f_k)\right) = \sum_{k=1}^{r} g_k \alpha_A(g)\alpha_A(f_k) = \sum_{k=1}^{r} g_k \alpha_A(g f_k)$$

Since $\alpha_A(gf_k) \in \alpha_A(I)$ for all $k = 1,\dots,r$, then $fh \in \alpha_A(I)$ and so $f \in \langle \alpha_A(I)\rangle :_R \langle \alpha_A(J)\rangle$ and $\langle \alpha_A(I :_R J)\rangle \subseteq \langle \alpha_A(I)\rangle :_R \langle \alpha_A(J)\rangle$.

Next suppose that $I \supseteq K := \ker(\alpha_A)$ and α_A is onto. Let $f \in \langle \alpha_A(I)\rangle :_R \langle \alpha_A(J)\rangle = \alpha_A(I) :_R \alpha_A(J)$. We will prove that $f \in \alpha_A(I :_R J)$. As α_A is onto, there is $g \in k[x_1,\dots,x_m]$ such that $\alpha_A(g) = f$. Now it is enough to show that $g \in I :_R J$. Indeed, given $h \in J$, note that

$$\alpha_A(gh) = \alpha_A(g)\alpha_A(h) = f\alpha_A(h) \in \alpha_A(I).$$

Thus there is $p \in I$ such that $\alpha_A(gh - p) = 0$. As $I \supseteq K$, we have that $gh - p \in I$ and so $gh \in I$. Since $h \in J$ was chosen arbitrarily, we conclude that $g \in I :_R J$.

(ii): Let $f \in \alpha_A^{-1}(I' :_R J')$ and $g \in \alpha_A^{-1}(J')$. Note that $\alpha_A(f) \in I' :_R J'$ and $\alpha_A(g) \in J'$. Since

$$\alpha_A(fg) = \alpha_A(f)\alpha_A(g) \in I',$$

we get that $fg \in \alpha_A^{-1}(I')$. As $g \in \alpha_A^{-1}(J')$ was chosen arbitrarily, we conclude that $f \in \alpha_A^{-1}(I') :_R \alpha_A^{-1}(J')$ and $\alpha_A^{-1}(I' :_R J') \subseteq \alpha_A^{-1}(I') :_R \alpha_A^{-1}(J')$.

Conversely let $f \in \alpha_A^{-1}(I') :_R \alpha_A^{-1}(J')$. In order to prove the other inclusion, it is enough to show that $\alpha_A(f) \in I' :_R J'$. Given $h \in J'$, there is $g \in k[x_1,\dots,x_m]$ such that $\alpha_A(g) = h$ because α_A is onto. In particular $g \in \alpha_A^{-1}(J')$, so $fg \in \alpha_A^{-1}(I')$ and

$$\alpha_A(f)h = \alpha_A(f)\alpha_A(g) = \alpha_A(fg) \in I'.$$

Since $h \in J'$ was chosen arbitrarily, we conclude that $\alpha_A(f) \in I' :_R J'$ and so $\alpha_A^{-1}(I') :_R \alpha_A^{-1}(J') \subseteq \alpha_A^{-1}(I' :_R J')$. $\square$

4.5 Irreducible Varieties and Prime Ideals

Question 4.5.6: Let k be a infinite field.

(i) Prove that any straight line in k^n is irreducible.

(ii) Prove that any linear subspace of k^n is irreducible.

Solution: **(i):** Let $\mathcal{L} \subseteq \mathbb{A}^n$ be a straight line. Then $\mathcal{L}$ can be defined parametrically by $\phi : k \longrightarrow \mathcal{L}$ such that

$$\phi(t) = \begin{cases} x_1(t) = b_1 + c_1 t, \\ x_2(t) = b_2 + c_2 t, \\ \qquad \vdots \\ x_n(t) = b_n + c_n t. \end{cases}$$

As the field is infinite, we conclude that $\mathcal{L}$ is an irreducible variety.

(ii): Let $W \subseteq k^n$ be a linear subspace of k^n and let $\{w_1, \dots, w_m\}$ be a basis for W, where $m \leq n$. Consider the linear operator $T : k^n \longrightarrow k^n$ such that

$$T(e_i) = \begin{cases} w_i, & \text{if } 1 \leq i \leq m, \\ 0, & \text{otherwise.} \end{cases}$$

Now define $\phi : k^m \longrightarrow k^n$ such that $\phi(x_1, \dots, x_m) = T(x_1, \dots, x_m, 0, \dots, 0)$. Observe that $\operatorname{Im}(\phi) = W$, because

$$\phi(x_1, \dots, x_m) = T(x_1, \dots, x_m, 0, \dots, 0) = \sum_{k=1}^{m} x_k T(e_k) = \sum_{k=1}^{m} x_k w_k,$$

and, denoting $w_i = (a_{1i}, a_{2i}, \dots, a_{ni})$, then

$$(y_1, \dots, y_n) = \phi(x_1, \dots, x_m) = \begin{cases} y_1(t) = \sum_{k=1}^{m} x_k a_{1k}, \\ y_2(t) = \sum_{k=1}^{m} x_k a_{2k}, \\ \qquad \vdots \\ y_n(t) = \sum_{k=1}^{m} x_k a_{nk}. \end{cases}$$

Since k is an infinite field and W is a variety defined parametrically, we conclude that W is an irreducible variety. $\square$

Question 4.5.7: Show that

$$\mathrm{I}(\{(a_1,\dots,a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n\rangle.$$

Solution: It is clear that the ideal $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ is contained in $\mathrm{I}(\{(a_1,\dots,a_n)\})$. Now let $f \in \mathrm{I}(\{(a_1,\dots,a_n)\})$. Doing the division of f by $\{x_1 - a_1, \dots, x_n - a_n\}$ using the Lexicographic order $x_1 > \cdots > x_n$, the division algorithm tells us that there exist $h_1, h_2, \dots, h_n \in k[x_1,\dots,x_n]$ and $r \in k$ such that

$$f(x) = h_1(x)(x_1 - a_1) + \cdots + h_n(x)(x_n - a_n) + r.$$

As $f \in \mathrm{I}(\{(a_1,\dots,a_n)\})$, then

$$0 = f(a_1,\dots,a_n) = \sum_{k=1}^{n} h_k(a_1,\dots,a_n)(a_k - a_k) + r = \sum_{k=1}^{n} h_k(a_1,\dots,a_n)\cdot 0 + r = r,$$

which implies that

$$f(x) = h_1(x)(x_1 - a_1) + \cdots + h_n(x)(x_n - a_n) \in \langle x_1 - a_1, \dots, x_n - a_n\rangle.$$

Hence $\mathrm{I}(\{(a_1,\dots,a_n)\}) \subseteq \langle x_1 - a_1, \dots, x_n - a_n\rangle$. $\square$

Question 4.5.9: Suppose that k is a field which is not algebraically closed.

(i) Show that if $I \subseteq k[x_1,\dots,x_n]$ is maximal, then $V(I)$ is empty or a point in k^n

(ii) Show that there exists a maximal ideal $I \subseteq k[x_1,\dots,x_n]$ for which $V(I) = \emptyset$.

(iii) Conclude that if k is not algebraically closed, there is always a maximal ideal of $k[x_1,\dots,x_n]$ which is not of form $\langle x_1 - a_1, \dots, x_n - a_n\rangle$.

Solution: **(i):** Suppose that $\mathrm{V}(I) \neq \emptyset$ and let $(a_1,\dots,a_n) \in \mathrm{V}(I)$. Thus

$$\{(a_1,\dots,a_n)\} \subseteq \mathrm{V}(I).$$

Applying the I( ) operator, we obtain

$$I \subseteq \sqrt{I} \subseteq \mathrm{I}(\mathrm{V}(I)) \subseteq \mathrm{I}(\{(a_1,\dots,a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n\rangle.$$

Since I is a maximal ideal and $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ is proper, we conclude that $I = \langle x_1 - a_1, \dots, x_n - a_n\rangle$, which implies that

$$\mathrm{V}(I) = \mathrm{V}(\langle x_1 - a_1, \dots, x_n - a_n\rangle) = \{(a_1,\dots,a_n)\}.$$

(ii): Since k is not an algebraically closed field, there is a non-constant polynomial $f_1(x_1) \in k[x_1]$ which does not admits roots in $k[x]$. Define the ideal $I = \langle f_1(x_1), x_2, \ldots, x_n \rangle \subseteq k[x_1, \ldots, x_n]$. Note that I is a maximal ideal, because

$$\frac{k[x_1, \ldots, x_n]}{I} \cong \frac{k[x_1]}{\langle f_1(x_1) \rangle}$$

and the last ring trivially is a field. Finally it is easy to see that $\mathrm{V}(I) = \emptyset$, Indeed, if else, given $(a_1, \ldots, a_n) \in \mathrm{V}(I)$, we would have that $f_1(a_1) = 0$, which is not possible because f_1 was chosen such that it does not admits roots in k.

(iii): Since there is always a maximal ideal I such that $\mathrm{V}(I) = \emptyset$ when k is not algebraically closed and $\mathrm{V}(J)$ always is non-empty when J is of form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, we conclude that, when k is not algebraically closed, there is always a maximal ideal $\mathfrak{m}$ which is not of form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

Question 4.5.11: If $f \in \mathbb{C}[x_1, \ldots, x_n]$ is irreducible, prove that $\mathrm{V}(f)$ is irreducible.

Proof: In fact, it is enough to show that $\mathrm{I}(\mathrm{V}(f))$ is a prime ideal. By Hilbert's Nullstellensatz, we have that

$$\mathrm{I}(\mathrm{V}(f)) = \sqrt{\langle f \rangle} = \langle f \rangle.$$

Since $k[x_1, \ldots, x_n]$ is an Unique Factorization Domain, f is a prime element, thus $\langle f \rangle$ is a prime ideal, which implies that $\mathrm{V}(f)$ is an irreducible variety. $\square$

Question 4.5.12: Prove that if I is any proper ideal of $\mathbb{C}[x_1, \ldots, x_n]$, then $\sqrt{I}$ is the intersection of maximal ideals containing I.

Proof: By Hilbert's Nullstellensatz, we have that

$$\sqrt{I} = \mathrm{I}(\mathrm{V}(I)) = \mathrm{I}\left(\bigcup_{z \in \mathrm{V}(I)} \{z\} \right) = \bigcap_{z \in \mathrm{V}(I)} \mathrm{I}(\{z\}) = \bigcap_{z \in \mathrm{V}(I)} \mathfrak{m}_z,$$

where $\mathfrak{m}_z$ is the maximal ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, with $z = (a_1, \ldots, a_n) \in \mathrm{V}(I)$. Now it remains to prove that every maximal ideal containing I is of form $\mathfrak{m}_z$ for some $z \in \mathrm{V}(I)$.

This fact is trivial. Since the field is algebraically closed, if $\mathfrak{m}$ is a maximal ideal, then $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $z = (a_1, \ldots, a_n) \in \mathbb{C}^n$, and, as $I \subseteq \mathfrak{m}$, then

$$\{(a_1, \ldots, a_n)\} = \mathrm{V}(\mathfrak{m}) \subseteq \mathrm{V}(I),$$

which proves the last statement. $\square$

Question 4.5.13: Let $f_1, \ldots, f_n \in k[x_1]$ be polynomials of one variable and consider the ideal

$$I = \langle f_1(x_1), x_2 - f_2(x_1), \ldots, x_n - f_n(x_1) \rangle \subseteq k[x_1, \ldots, x_n].$$

Assume that $\deg(f_1) = m > 0$.

(i): Show that every $f \in k[x_1, \ldots, x_n]$ can be written uniquely as $f = q + r$, where $q \in I$ and $r \in k[x_1]$ with $r = 0$ or $\deg(r) < m$.

(ii): Let $f \in k[x_1]$. Show that $f \in I$ if and only if f is divisible by f_1 in $k[x_1]$.

(iii): Prove that I is prime if and only if $f_1 \in k[x_1]$ is irreducible.

(iv): Prove that I is radical if and only if $f_1 \in k[x_1]$ is square-free.

(v): Prove that $\sqrt{I} = \langle (f_1)_{red} \rangle + \mathrm{I}$.

Solution: **(i):** Considering the lexicographic monomial order $x_n > x_{n-1} > \cdots > x_1$, we obtain that $G = \{f_1(x_1), x_2 - f_2(x_1), \ldots, x_n - f_n(x_1)\}$ is a Gröbner basis for I. Thus, given $f \in k[x_1, \ldots, x_n]$, there are unique g, $r \in k[x_1, \ldots, x_n]$ such that $f = g + h$. Moreover, as $\mathrm{LM}(x_i - f_1(x_1)) = x_i$ for all $2 \leq i \leq n$ and $\mathrm{LM}(f_1(x_1)) = x^m$, r actually is a polynomial in $k[x_1]$ with degree at most $m - 1$.

(ii): Suppose that $f(x_1)$ is divisible by $f(x_1)$ in $k[x_1]$, so there is $h(x_1) \in k[x_1]$ such that $f(x_1) = h(x_1) f_1(x_1)$ and so

$$f(x_1) = h(x_1) f_1(x_1) + \sum_{k=2}^{n} (x_k - f_1(x_1)) \cdot 0 \in I.$$

Conversely suppose that $f(x_1) \in I$, so there are $h_1, \ldots, h_n \in k[x_1, \ldots, x_n]$ such that

$$f(x_1) = f_1(x_1) h_1 + \sum_{k=2}^{n} (x_k - f_1(x_1)) h_k.$$

Applying the division algorithm, we actually conclude that $f(x_1) = f_1(x_1) h_1$ and, since $f_1(x_1)$ is just a polynomial in x_1, we get that $h_1 \in k[x_1]$. Thus $f(x_1)$ is divisible by $f_1(x_1)$.

(iii): Observe that

$$\frac{k[x_1, \ldots, x_n]}{I} \cong \frac{k[x_1, f_1(x) \ldots, f(x_1)]}{\langle f_1(x_1) \rangle} = \frac{k[x_1]}{\langle f_1(x_1) \rangle}.$$

Thus I is prime if and only if $k[x_1]/\langle f_1(x_1) \rangle$ is an integral domain. Thus I is a prime ideal if and only if $f_1(x_1)$ is a prime element of $k[x_1]$. Since every prime element is irreducible, the statement follows.

(iv:) Similarly I is radical if and only if $k[x_1, x_1, \dots, x_n]/I$ is a reduced ring. Since

$$\frac{k[x_1, \dots, x_n]}{I} \cong \frac{k[x_1]}{\langle f_1(x_1)\rangle}.$$

Then I is radical if and only if $\langle f_1(x_1)\rangle$ is a radical ideal of $k[x_1]$. However it is clear that, in an unique factorization domain, a principal ideal is radical if and only if its generator is square-free.

(v): By definition, one has that $I \subseteq \sqrt{I}$. Moreover $\langle (f_1(x_1))_{red}\rangle \subseteq \sqrt{I}$, because, given $h \in \langle (f_1(x_1))_{red}\rangle$, then there is $g \in k[x_1, \dots, x_n]$ such that $h = (f_1)_{red} g$. Since $(f_1)_{red}^m$ is multiple of f_1 for some $m \in \mathbb{N}$, we conclude that

$$h^m = (f_1)_{red}^m g^m \in \langle f_1(x_1)\rangle \subseteq I$$

and so $\langle (f_1(x_1))_{red}\rangle \subseteq \sqrt{I}$, thus $\langle (f_1(x_1))_{red}\rangle + I \subseteq \sqrt{I}$.

Conversely let $f \in \sqrt{I}$. By definition there is $m \in \mathbb{N}$ such that $f^m \in I$. If $f \in k[x_1]$, by part (ii), f^m is divisible by $f_1(x_1)$ in $k[x_1]$ and so $f \in \langle (f_1)_{red}\rangle$. Otherwise, as $x_2 - f_2(x_1), \dots, x_n - f_n(x_1)$ are irreducible polynomials, we conclude that, if $f^m \in I$, then $f \in I$, so $\sqrt{I} \subseteq \langle (f_1(x_1))_{red}\rangle + I$. $\square$

4.6 Decomposition of a variety into irreducibles

Question 4.7.1: Show that the intersection of any collection of prime ideals is radical.

Solution: Let $\mathcal{C} = \{\mathfrak{p}_i\}_{i \in L}$ be a collection of prime ideals of R and define

$$I = \bigcap_{i \in L} \mathfrak{p}_i$$

I claim that I is radical. Indeed let $x \in \sqrt{I}$, so there is $n \in \mathbb{N}$ such that $x^n \in I$. Thus $x^n \in \mathfrak{p}_i$ for all $i \in L$. Since each $\mathfrak{p}_i$ is a prime ideal, then $x \in \mathfrak{p}_i$ for all $i \in L$, which implies that $x \in \bigcap_{i \in L} \mathfrak{p}_i = I$. Hence $I = \sqrt{I}$ and so I is a radical ideal. $\square$

Question 4.7.2: Show that an irredundant intersection of prime ideals never is prime

Solution: Indeed let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals such that $\mathfrak{p} \cap \mathfrak{q} \subsetneq \mathfrak{p}$ and $\mathfrak{p} \cap \mathfrak{q} \subsetneq \mathfrak{q}$. By hypothesis, there are $x \in \mathfrak{p} \setminus \mathfrak{q}$ and $y \in \mathfrak{q} \setminus \mathfrak{p}$. Observe that neither $x \in \mathfrak{p} \cap \mathfrak{q}$ nor $y \in \mathfrak{p} \cap \mathfrak{q}$, however $xy \in \mathfrak{p}\mathfrak{q} \subseteq \mathfrak{p} \cap \mathfrak{q}$, which implies that $\mathfrak{p} \cap \mathfrak{q}$ is not prime. $\square$

Question 4.7.4: Consider the ideal $I = \langle xz - y^2, x^3 - yz\rangle \subseteq R = k[x, y, z]$

(i): Show that $I :_R \langle x^2y - z^2\rangle = \langle x, y\rangle$;

(ii): Show that $I :_R \langle x^2y - z^2\rangle$ is prime.

(iii): Show that $I = \langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle$.

Solution: **(i):** Observe that

$$x \cdot (x^2y - z^2) = x^3y - xz^2 = z(xz - y^2) + y(x^3 - yz).$$
$$y \cdot (x^2y - z^2) = x^2y^2 - yz^2 = (-x^2)(xz - y^2) + z(x^3 - yz).$$

Hence $\langle x, y\rangle \subseteq I :_R \langle x^2y - z^2\rangle$. Observe that $I :_R \langle x^2y - z^2\rangle \subsetneq \langle x, y, z\rangle$. Indeed if $g(x, y, z) \in I :_R \langle x^2y - z^2\rangle$ is such that $g(0, 0, 0) \neq 0$, then I must contain a polynomial whose one of terms is only z^2, however clearly we can see that I does not satisfy this property. Next if

$$\langle x, y\rangle \subsetneq I :_R \langle x^2y - z^2\rangle \subseteq \langle x, y, z\rangle,$$

then $I :_R \langle x^2y - z^2\rangle$ contains a polynomial whose one of terms only contains the variable z. Thus, since $\langle x, y, \rangle \subseteq I :_R \langle x^2y - z^2\rangle$, then actually we can find a non-zero polynomial $p(z)$ just in variable z in $I :_R \langle x^2y - z^2\rangle$. Observe that $p(z)(x^2y - z^2) \in I$ and contains a term which only contains z as variable, however it is impossible, because no non-zero polynomial in I contains a term just having z as variable. Thus

$$I :_R \langle x^2y - z^2\rangle = \langle x, y\rangle.$$

(ii): Since $I :_R \langle x^2y - z^2\rangle = \langle x, y\rangle$ and

$$\frac{R}{I :_R \langle x^2y - z^2\rangle} = \frac{k[x, y, z]}{\langle x, y\rangle} \cong k[z]$$

then $I :_R \langle x^2y - z^2\rangle$ is a prime ideal.

(iii): Call $\mathfrak{a} = \langle x, y\rangle$, $\mathfrak{b} = \langle xz - y^2, x^3 - yz\rangle = I$ and $\mathfrak{c} = \langle z^2 - x^2y\rangle$. Using these definitions, we have

$$\langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle = \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$$

Since $\mathfrak{b} \subseteq \mathfrak{a}$, by the modular law, we have

$$\langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle = \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}.$$

Since $\mathfrak{a} \cap \mathfrak{c} = 0$, then

$$\langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{b} = I.$$

$\square$

4.7 Proof of Closure Theorem

There were not exercises at this section.

4.8 Primary decomposition of ideals

Question 4.8.4: We showed that every irreducible ideal is primary. Surprisingly the converse is false. Let $I = \langle x^2, xy, y^2\rangle \subseteq k[x, y]$

(i): Show that I is primary.

(ii): Show that $I = \langle x^2, y\rangle \cap \langle x, y^2\rangle$

(i): Let $f,\ g \in k[x, y]$ such that $f(x, y)g(x, y) \in I$. Suppose that $f(x, y) \notin I$, then $f(x, y)$ contains one of the following terms: λ or λx or λy, where λ is a non-zero element of k. Since $fg \in I$, then the constant term of g is necessarily zero, which implies that $g^2 \in I$ and so $g \in \sqrt{I}$. Thus I is a primary ideal.

(ii): Observe that $I \subsetneq \langle x^2, y\rangle$ and $I \subsetneq \langle x, y^2\rangle$, so $I \subseteq \langle x^2, y\rangle \cap \langle x, y^2\rangle$. Now, given $f(x, y) \in \langle x^2, y\rangle \cap \langle x, y^2\rangle$, we have that

- The coefficient of x is 0, because the polynomials of $\langle x^2, y\rangle$ have no terms λx
- The coefficient of y is 0, because the polynomials of $\langle y^2, x\rangle$ have no terms λy
- The term constant is 0, because the polynomials of $\langle x^2, y\rangle$ (or $\langle y^2, x\rangle$) has have no constant terms.

Then $f \in \langle x^2, y\rangle \cap \langle x, y^2\rangle$, which implies that $I = \langle x^2, y\rangle \cap \langle x, y^2\rangle$ and so I is a reducible ideal. □

Question 4.8.6: Let I be the ideal $\langle x^2, xy\rangle \subseteq \mathbb{Q}[x, y]$.

(i): Prove that

$$I = \langle x\rangle \cap \langle x^2, xy, y^2\rangle = \langle x\rangle \cap \langle x^2, y\rangle$$

(ii): Prove that for any $a \in \mathbb{Q}$

$$I = \langle x\rangle \cap \langle x^2, y - ax\rangle$$

is minimal primary decomposition of I. Thus I has infinitely many distinct minimal primary decompositions.

Solution: **(i):** Observe that, as $I \subseteq \langle x^2, xy, y^2 \rangle$ and $I \subseteq \langle x \rangle$, then $I \subseteq \langle x^2, xy, y^2 \rangle \cap \langle x \rangle$. Now let $f \in \langle x^2, xy, y^2 \rangle \cap \langle x \rangle$. Observe that f does not contains polynomial in y. Moreover f does not contain the term λx because no polynomial in $\langle x^2, xy, y^2 \rangle$ has the term λx. Thus $f \in I$, which implies that

$$I = \langle x^2, xy, y^2 \rangle \cap \langle x \rangle.$$

Since both ideals $\langle x^2, y^2, xy \rangle$ and $\langle x \rangle$ are primary and they mutually irredundant, we conclude $I = \langle x^2, xy, y^2 \rangle \cap \langle x \rangle$ is a minimal primary decomposition of I.

Similarly observe that $I \subseteq \langle x \rangle$ and $I \subseteq \langle x^2, y \rangle$, so we have that $I \subseteq \langle x \rangle \cap \langle x^2, y \rangle$. Now let $f \in \langle x \rangle \cap \langle x^2, y \rangle$. Since $f \in \langle x \rangle$, every term of f contains x as variable, f has no term of form λy and every polynomial of f has the constant term equal to 0. Finally, as $f \in \langle x^2, y \rangle$, f has no term of form λx. Thus $f \in \langle x^2, xy \rangle = I$, which implies that

$$I = \langle x \rangle \cap \langle x^2, y \rangle.$$

Since $\sqrt{\langle x^2, y \rangle}$ is maximal, then $\langle x^2, y \rangle$ is primary. Moreover, since they are mutually irredundant, then $I = \langle x \rangle \cap \langle x^2, y \rangle$ is minimal primary decomposition of I.

(ii): Let $\mathfrak{a} = \langle x \rangle$, $\mathfrak{b} = \langle x^2 \rangle$ and $\mathfrak{c} = \langle y - ax \rangle$. Since $\mathfrak{b} \subseteq \mathfrak{a}$, by modular law, we have

$$\langle x \rangle \cap \langle x^2, y - ax \rangle = \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c} = \langle x^2 \rangle + \langle x \rangle \cap \langle y - ax \rangle = \langle x^2, xy \rangle = I$$

Since the ideal $\sqrt{\langle y - ax, x^2 \rangle} = \langle x, y \rangle$ is maximal, then $\langle y - ax, x^2 \rangle$ is primary. Furthermore, since $\langle x \rangle$ and $\langle y - ax \rangle$ are mutually irredundant, then

$$I = \langle x \rangle \cap \langle x^2, y - ax \rangle$$

is minimal primary decomposition of I for each $a \in \mathbb{Q}$. In particular, the decomposition primary is not unique and an ideal can admits infinitely many minimal primary decompositions. $\square$

Chapter 5

Polynomial and Rational Functions on a Variety

5.1 Polynomial Functions

Question 5.1.1: Let V be the twisted cubic in $\mathbb{R}^3$ and $W = \mathrm{V}(v - u - u^2)$ in $\mathbb{R}^2$. Show that

$$\phi : V \longrightarrow W$$

$$(x, y, z) \longmapsto (xy, z + x^2y^2)$$

defines a polynomial mapping from V to W

Solution: Considering $\pi_1 : \mathbb{R}^2 \longrightarrow \mathbb{R}$ and $\pi_2 : \mathbb{R}^2 \longrightarrow \mathbb{R}$ the natural natural projections, observe that $\pi_1 \circ \phi \in \mathbb{R}[x, y, z]$ and $\pi_2 \circ \phi \in \mathbb{R}[x, y, z]$. Thus ϕ is a polynomial mapping. It remains to check now that ϕ is well-defined, that is, we have to check that $\big(\pi_1 \circ \phi(x, y, z), \pi_2 \circ \phi(x, y, z)\big) \in W$ for all $(x, y, z) \in V$. Note that, given $(x, y, z) \in V$, we have that

$$(\pi_2 \circ \phi)(x, y, z) - (\pi_1 \circ \phi)(x, y, z) - (\pi_1 \circ \phi)(x, y, z)^2 = (z + x^2y^2) - (xy) - (xy)^2 = z - xy = 0$$

because $z - xy = 1 \cdot (z - x^3) + (-x)(y - x^2)$. This fact implies $\mathrm{Im}(\phi) \subseteq W$ and so ϕ is well-defined. $\square$

Question 5.1.2: Let $V = \mathrm{V}(y - x) \subseteq \mathbb{R}^2$ and $\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$ be a polynomial mapping represented by

$$\phi(x, y) = (x^2 - y, y^2, x - 3y^2).$$

The image of V under ϕ is a variety in $\mathbb{R}^3$. Find the system of equations defining the image of ϕ.

Solution: Indeed note that

$$\mathrm{Im}(\phi) = \{(x^2 - y, y^2, x - 3y^2) \in \mathbb{R}^3 \ ; \ (x, y) \in \mathrm{V}(x - y)\} = \{(x^2 - y, y^2, x - 3y^2) \in \mathbb{R}^3 \ ; \ x = y\}$$

Set

$$\begin{cases} u = x^2 - y = x^2 - x \\ v = y^2 = x^2 \\ w = x - 3y^2 \end{cases}$$

Considering the ideal $I = \langle u - x^2 + x, v - x^2, w - x + 3y^2 \rangle \subseteq \mathbb{R}[x, u, v, w]$ and the Lexicographic order $x > u > v > w$, then, the first elimination suggests us that

$$\mathrm{Im}(\phi) = \mathrm{V}(9v^2 + 6vw - v + w^2, u + 2v + w)$$

Note that if $(a, b, c) \in \mathrm{V}(9v^2 + 6vw - v + w^2, u + 2v + w)$, then

$$\begin{cases} 9b^2 + 6bc - b + c^2 = 0, \\ a + 2b + c = 0 \end{cases}$$

and so Moreover, we have that $b \geq 0$, because

$$(3b + c)^2 - b = 9b^2 + 6bc - b + c^2 = 0,$$

which implies that $b = (3b + c)^2 \geq 0$. From relations above, we conclude that

$$\begin{cases} a = -2b - c = b - \sqrt{b}; \\ c = -3b + \sqrt{b}. \end{cases}$$

Hence, setting $(\sqrt{b}, \sqrt{b}) \in V$ and using the relations above, we conclude that $\phi(\sqrt{b}, \sqrt{b}) = (a, b, c)$. $\square$

Question 5.1.5: Show that $\phi_1(x, y, z) = (2x^2 + y^2, z^2 - y^3 + 3xz)$ and $\phi_2(x, y, z) = (2y + xz, 3y^2)$ represent the same polynomial mapping from the twisted cubic in $\mathbb{R}^3$ to $\mathbb{R}^2$.

Solution: Indeed, denoting the twisted cubic by $V = \mathrm{V}(y - x^2, z - x^3) \subseteq \mathbb{R}^3$, it is enough to show that

$$\begin{cases} 2x^2 + y^2 - 2y - xz \in \mathrm{I}(V), \\ z^2 - y^3 + 3xz - 3y^2 \in \mathrm{I}(V). \end{cases}$$

Since

$$2x^2 + y^2 - 2y - xz = (-x)(z - x^3) + (y + x^2 - 2)(y - x^2),$$
$$z^2 - y^3 + 3xz - 3y^2 = (z + x^3 + 3x)(z - x^3) + (-y^2 - yx^2 - 3y - x^4 - 3x^2)(y - x^2),$$

we conclude that $\phi_1(x, y, z) = \phi_2(x, y, z)$ for all $(x, y, z) \in V$, so $\phi_1 = \phi_2$. □

Question 5.1.6: Consider the mapping $\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^5$ defined by

$$\phi(u, v) = (u, v, u^2, uv, v^2).$$

(i): The image of ϕ is variety S known as an Affine Veronese surface. Find its implicit representation

(ii): Show that the projection $\pi : S \longrightarrow \mathbb{R}^2$ defined by $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2)$ is the inverse mapping of $\phi : \mathbb{R}^2 \longrightarrow S$. What does this imply about S and $\mathbb{R}^2$.

Solution: **(i):** I claim that

$$S = \mathrm{V}(x_1^2 - x_3, x_2^2 - x_5, x_1x_2 - x_4)$$

In fact it is clear that $S := \mathrm{Im}(\phi) \subseteq \mathrm{V}(x_1^2 - x_3, x_2^2 - x_5, x_1x_2 - x_4)$. Now let $(a, b, c, d, e) \in \mathrm{V}(x_1^2 - x_3, x_2^2 - x_5, x_1x_2 - x_4)$. Observe that

$$c = a^2, \qquad d = ab, \qquad e = b^2.$$

Thus $\phi(a, b) = (a, b, a^2, ab, b^2) = (a, b, c, d, e)$, which implies that $\mathrm{V}(x_1^2 - x_3, x_2^2 - x_5, x_1x_2 - x_4) \subseteq S$. Hence

$$S = \mathrm{V}(x_1^2 - x_3, x_2^2 - x_5, x_1x_2 - x_4).$$

(ii): Note that $(\pi \circ \phi)(u, v) = \pi(u, v, u^2, uv, v^2) = (u, v)$ for all $(u, v) \in \mathbb{R}^2$, which implies that $\pi \circ \phi = 1_{\mathbb{R}^2}$. Now let $(x_1, x_2, x_3, x_4, x_5) \in S$, then there exists $(u, v) \in \mathbb{R}^2$ such that

$$(x_1, x_2, x_3, x_4, x_5) = (u, v, u^2, uv, v^2)$$

Hence $x_3 = u^2 = x_1^2$, $x_4 = uv = x_1x_2$ and $x_5 = v^2 = x_2^2$, so

$$(\phi \circ \pi)(x_1, x_2, x_3, x_4, x_5) = \phi(x_1, x_2) = (x_1, x_2, x_1^2, x_1x_2, x_2^2) = (x_1, x_2, x_3, x_4, x_5).$$

Thus $\phi \circ \pi = 1_S$ and so the Affine Veronese Surface is isomorphic to the two-dimensional affine space $\mathbb{A}^2_{\mathbb{R}}$. □

Question 5.1.8: Let $V = \mathrm{V}(xy, xz) \subseteq \mathbb{R}^3$.

(i): Show that neither of the polynomial functions $f = y^2 + z^2$ and $g = x^2 - x$ is identically zero on V, but that their product is identically zero on V.

(ii): Find $V_1 = V \cap \mathrm{V}(f)$ and $V_2 = V \cap \mathrm{V}(g)$ and show that $V = V_1 \cup V_2$.

Solution: **(i):** In fact, considering $z_1 = (0, 1, 0) \in V$ and $z_2 = (2, 0, 0) \in V$, we observe that $f(z_1) = 1 \neq 0$ and $g(z_2) = 2 \neq 0$. Hence $f, g \neq 0$ in V. However

$$fg = y^2x^2 - y^2x + z^2x^2 - z^2x = (xy)^2 - y(xy)^2 + (xz)^2 - z(xz).$$

Since $xy = xz = 0$ for all $(x, y, z) \in V$, we conclude that $fg = 0$ em V.

(ii): Observe that

$$V_1 = \mathrm{V}(xy, xz, y^2 + z^2) = \{(t, 0, 0) \in \mathbb{R}^3 \ ; \ t \in \mathbb{R}\} = \mathrm{V}(y, z).$$

$$V_2 = \mathrm{V}(xy, xz, x^2 - x) = \mathrm{V}(x) \cup \mathrm{V}(y, z, x - 1) = \{(0, u, v) \in \mathbb{R}^3 \ , \ u, v \in \mathbb{R}\} \cup \{(0, 0, 1)\}.$$

By definition, $V_1 \subseteq V$ and $V_2 \subseteq V$, so $V_1 \cup V_2 \subseteq V$. On the other hand let $w = (x, y, z) \in V$. If $x = 0$, then $w \in V_2$. If $x \neq 0$, then $y = z = 0$, which implies that $w \in V_1$. Thus $V \subseteq V_1 \cup V_2$ and so

$$V = V_1 \cup V_2.$$

□

Question 5.1.10: In this problem, we will show that there are no nonconstant polynomial mappings from $V = \mathbb{R}$ and $W = \mathrm{V}(y^2 - x^3 + x) \subseteq \mathbb{R}^2$. Thus, these varieties are not isomorphic.

(i): Suppose that $\phi : \mathbb{R} \longrightarrow W$ is a polynomial mapping represented by $\phi(t) = (a(t), b(t))$, where $a(t), b(t) \in \mathbb{R}[t]$. Explain why it must be true that $b(t)^2 = a(t)(a(t)^2 - 1)$.

(ii): Explain why the two factors on the right side of the equation in part (i) must be relatively prime in $\mathbb{R}[t]$.

(iii): Using the unique factorizations of a and b into powers of irreducible polynomials, show that $b^2 = ac^2$ for some polynomial $c \in \mathbb{R}[t]$.

(iv): From part (iii) it follows that $c^2 = a^2 - 1$. Deduce from this equations that c, a and, hence, b must be constant polynomials.

Solution: **(i):** Indeed, since $\phi(t) = (a(t), b(t)) \in W$ for all $t \in \mathbb{R}$, we have $b(t)^2 - a(t)^3 + a(t) = 0$, which implies that

$$b(t)^2 = a(t)(a(t)^2 - 1).$$

(ii): Let $m(t) = \gcd(a(t), a(t)^2 - 1)$ the greatest common divisor between $a(t)$ and $a(t)^2 - 1$. Note that $m(t)$ divides $a(t)$ and, hence, $a(t)^2$. Since $m(t)$ also divides $a(t)^2 - 1$, we have that $m(t)$ divides

$$1 = a(t)^2 + (1 - a(t)^2)$$

which implies that $m(t)$ is unity in $\mathbb{R}[t]$ and so $a(t), a(t)^2 - 1$ are relatively prime polynomials.

(iii): Let $b(t) = up_1(t)^{a_1} \cdots p_n(t)^{a_n}$, $a(t) = vq_1(t)^{b_1} \cdots q_m(t)^{b_m}$ and $a(t)^2 - 1 = wg_1(t)^{c_1} \cdots g_r(t)^{c_r}$ be the factorization of $b(t)$, $a(t)$ and $a(t)^2 - 1$ in monic irreducible polynomials, respectively. Thus

$$u^2 p_1(t)^{2a_1} \cdots p_n(t)^{2a_n} = vq_1(t)^{b_1} \cdots q_m(t)^{b_m} \cdot wg_1(t)^{c_1} \cdots g_r(t)^{c_r}.$$

Since $a(t), a(t)^2 - 1$ are relatively prime polynomials, $q_i \neq g_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq r$. By Unique factorization property of $\mathbb{R}[t]$, we conclude that $c_1, \ldots, c_r$ are even integers, which implies that $a(t)^2 - 1 = c^2(t)$ for some $c(t) \in \mathbb{R}[t]$. Hence $b^2(t) = a(t)c^2(t)$.

(iv): From (iii), we conclude that that $a(t)^2 - 1 = c(t)^2$ for some $c(t) \in \mathbb{R}[t]$. Thus

$$\big(a(t) - c(t)\big)\big(a(t) + b(t)\big) = a(t)^2 - c(t)^2 = 1$$

Thus $a(t)$ and $c(t)$ are constant polynomials. Since $b(t)^2 = a(t)c(t)^2$ is a constant polynomial, we also conclude that $b(t)$ is constant. From this question, we conclude that there are no non-constant polynomial mappings between $\mathbb{R}$ and $\mathrm{V}(y^2 - x^3 - x) \subseteq \mathbb{R}^2$.

Chapter 6

Projective Algebraic Geometry

6.1 The Projective Plane

Question 8.1.11: The projective line in $\mathbb{P}^2(k)$ is defined by

$$L_{(A,B,C)} = \{(x:y:z) \in \mathbb{P}^2(k) \ ; \ Ax + By + Cz = 0\},$$

where (A,B,C) is a nonzero point of k^3.

(i): Why do we need to make the restriction $(A,B,C) \neq (0,0,0)$?

(ii): Show that (A,B,C) and (A',B',C') define the same projective line if and only if $(A,B,C) = \lambda(A',B',C')$ for some nonzero real number λ.

(iii): Conclude that the set of projective lines in $\mathbb{P}^2(k)$ can be identified with the set

$$\{(A,B,C) \in k^3 \ ; \ (A,B,C) \neq (0,0,0)\}/\sim .$$

This set is called the dual projective plane and is denoted by $\mathbb{P}^2(k)^\vee$.

(iv): Describe the subset of $\mathbb{P}^2(k)^\vee$ corresponding to affine lines.

(v): Given the point $p \in \mathbb{P}^2(k)$, consider the set $\tilde{p}$ of all projective lines containing p. We can regard $\tilde{p}$ as a subset of $\mathbb{P}^2(k)^\vee$. Show that $\tilde{p}$ is a projective line in $\mathbb{P}^2(k)^\vee$. We call $\tilde{p}$ the pencil of lines through p.

(vi): The cartesian product $\mathbb{P}^2(k) \times \mathbb{P}^2(k)^\vee$ has the natural subset

$$I = \{(P,L) \in \mathbb{P}^2(k) \times \mathbb{P}^2(k)^\vee \ ; \ p \in L\}.$$

Show that I is described by equation $Ax + By + Cz = 0$, where $(x : y : z) \in \mathbb{P}^2(k)$ and $(A : B : C) \in \mathbb{P}^2(k)^\vee$.

Proof: **(i):** If $(A, B, C) = (0, 0, 0)$, then $L_{(A,B,C)}$ would be the whole projective plane $\mathbb{P}^2(k)$.

(ii): Observe that $L_{(A,B,C)}$ can be view as the homogeneous coordinates of elements of $\ker(\phi_{(A,B,C)}) \setminus \{(0, 0, 0)\}$, where

$$\begin{aligned} \phi_{(A,B,C)} : k^3 &\longrightarrow k \\ (x, y, z) &\longmapsto Ax + By + Cz. \end{aligned}$$

Thus let (A, B, C), $(A', B', C') \in k^3$ be nonzero points and suppose that $L_{(A,B,C)} = L_{(A',B',C')}$. Define the linear mapping

$$\begin{aligned} \phi : k^3 &\longrightarrow k^2 \\ (x, y, z) &\longmapsto (Ax + By + Cz, A'x + B'y + C'z) \end{aligned}$$

The hypothesis $L_{(A,B,C)} = L_{(A',B',C')}$ implies that

$$\dim(\ker(\phi)) = \dim(\ker(\phi_{(A,B,C)})) = \dim(\ker(\phi_{(A',B',C')})) = 2,$$

which implies that $\operatorname{rank}(\phi) = 1$ and so the the 2×2 minors of

$$\begin{bmatrix} A & B & C \\ A' & B' & C' \end{bmatrix}$$

are zero. So

$$\begin{cases} AB' = BA' \\ AC' = CA' \\ BC' = CB' \end{cases}$$

Supposing, without lost of generality that A, $B' \neq 0$, then

$$\frac{A}{A'} = \frac{B}{B'} = \frac{C}{C'}.$$

$\square$

(iii): Define the mapping

$$\eta : \{(A, B, C) \in k^3 \ ; \ (A, B, C) \neq (0, 0, 0)\}/\sim \longrightarrow \mathbb{P}^2(k)^\vee$$

such that $\eta([(A,B,C)]) = L_{(A,B,C)}$. Clearly η is surjective. Moreover, by item (ii), η is well-defined and is injective.

(iv): Let L be an affine line in k^3 parametrized by

$$\gamma(t) = (a_0 + at, b_0 + bt, c_0 + ct).$$

Suppose that L does not pass by the origin and let $\Gamma(t) = (a_0 + at : b_0 + bt : c_0 + ct)$ be the homogeneous coordinates in the projective plane. The corresponding points in dual projective space are the lines $Ax + By + Cz = 0$ such that

$$A(a_0 + at) + B(b_0 + bt) + C(c_0 + ct) = 0$$

Thus for all $t \in k$, we have

$$Aa_0 + Bb_0 + Cc_0 = -t(Aa + Bb + Cc)$$

This is just possible if

$$\begin{cases} Aa_0 + Bb_0 + Cc_0 = 0 \\ Aa + Bb + Cc = 0 \end{cases}$$

Thus $(A : B : C) = (bc_0 - cb_0 : ca_0 - ac_0 : ab_0 - ba_0)$.

On other hand, if L passes by the origin, the corresponding points in the dual projective space are the the lines $Ax + By + Cz = 0$ such that $(A,B,C) \in \langle (a,b,c) \rangle^{\perp} \smallsetminus \{0\} \subseteq k^3$.

(vi): Suppose that $(p, L) \in I$, where $p = (x_0 : y_0 : z_0)$ and $L = \mathrm{V}(A_0x + B_0x + C_0x)$, then $p \in L$ and so $Ax + By + Cz = 0$, which implies that

$$(p, L) \in \{\big((x : y : z), \mathrm{V}(Ax + Bx + Cx)\big) \in \mathbb{P}^2(k) \times \mathbb{P}^2(k)^{\vee}\ ;\ Ax + By + Cz = 0\}.$$

Now let $(x_0 : y_0 : z_0) \in \mathbb{P}^2(k)$ and $(A_0 : B_0 : C_0) \in \mathbb{P}^2(k)^{\vee}$ such that $A_0x_0 + B_0y_0 + C_0z_0 = 0$, thus, considering $p = (x_0 : y_0 : z_0)$ and $L = \mathrm{V}(A_0x + B_0y + C_0z)$, we have that $(p, L) \in I$. $\square$

6.2 Projective Space and Projective Varieties

Question 8.2.9: Let $V = \mathrm{V}(f_1, \ldots, f_s)$ be a projective variety defined by homogeneous polynomials $f_i \in k[x_0, \ldots, x_n]$. Show that $W = V \cap U_i$ can be identified with the affine variety $\mathrm{V}(g_1, \ldots, g_s) \subseteq k^n$ define by the dehomogenized polynomials

$$g_j(x_1, \ldots, x_i, x_{i+1}, \ldots, x_n) = f_j(x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n), \quad j = 1, \ldots, s.$$

Solution: Using the identification $\phi_i : U_i \longrightarrow k^n$ such that

$$\phi_i(x_0, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) = (x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i)$$

Note that

$$\begin{aligned}
V \cap U_i &= \{(x_0 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots : x_n) \in \mathbb{P}^n(k) \ ; \ f_j(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) = 0\} \\
&= \{(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in k^n \ ; \ f_j(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n) = 0\} \\
&= \{(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in k^n \ ; \ g_j(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = 0\} = \mathrm{V}(g_1, \dots, g_s).
\end{aligned}$$

□

Question 8.2.11: Let $f \in k[x_1, \dots, x_n]$. If $F \in k[x_0, x_1, \dots, x_n]$ is any homogeneous polynomial satisfying $F(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$, then $F = x_0^e f^h$ for some $e \geq 0$.

Proof: By hypothesis, we have that $F^{dh} = f$. By Proposition 7 (e), we conclude that there is $e \geq 0$ such that $F = x_0^e f^h$. □

Question 8.2.13: Consider the variety $W' = \mathrm{V}(z^2 - x^3 + xz^2) \subseteq k^2$. Show that $(x, z) = (0, 0)$ is a singular point of W'.

Proof: Consider the parametrized line

$$\begin{aligned}
\sigma : k &\longrightarrow k^2 \\
t &\longmapsto (at, bt)
\end{aligned}$$

Considering the polynomial

$$g(t) := f \circ \sigma(t) = (bt)^2 - (at)^3 + (at)(bt)^2 = t^2(b^2 + t(ab^2 - a^3)),$$

then any line passing through $(0, 0)$ has multiplicity ≥ 2, so $(0, 0)$ is a singular point of W'. □

Question 8.2.14: For each of following affine varieties, apply the homogeneization process in order to write W as $V \cap U_0$, where V is projective variety and U_0 is the open affine $\mathbb{P}^2 \setminus \mathrm{V}(x_0)$. In each case, identify $V \setminus W = V \cap H$, where H is the hyperplane at infinity.

(i): $W = \mathrm{V}(y^2 - x^3 - ax - b) \subseteq \mathbb{R}^2$, $a, b \in \mathbb{R}$. Is the point $V \cap H$ singular here?

(ii): $W = \mathrm{V}(x_1 x_3 - x_2^2, x_1^2 - x_2) \subseteq \mathbb{R}^3$. Is there a extra component at infinity here?

(iii): $W = \mathrm{V}(x_3^2 - x_1^2 - x_2^2)$.

Proof: **(i):** Observe that $W = V \cap U_z$, where $V = \mathrm{V}(y^2z - x^3 - axz^2 - bz^3)$. Note the points of $V \cap H$ satisfies the system

$$\begin{cases} y^2z - x^3 - axz^2 - bz^3 = 0 \\ z = 0 \end{cases}$$

Thus $V \cap H = \{(0 : 1 : 0)\}$. Since $V \cap H \subseteq V \cap U_y$, doing the dehomogenization of V with respect the variable y, we obtain that $V \cap U_y = \mathrm{V}(z - x^3 - axz^2 - bz^3)$. Considering $g(x, z) := z - x^3 - axz^2 - bz^3$, observe that

$$\nabla g(0,0) = (-3x^2 - az^2, 1 - 2axz - 3bz^2)\big|_{(0,0)} = (0,1) \neq (0,0).$$

Thus $(0 : 1 : 0)$ is a regular point of V.

(ii): Observe that $W = V \cap U_0$, where $V = \mathrm{V}(x_1x_3 - x_2^2, x_1^2 - x_2x_0)$. The points of $V \cap H$ satisfies the system

$$\begin{cases} x_1x_3 - x_2^2 = 0 \\ x_1^2 - x_2x_0 = 0 \\ x_0 = 0 \end{cases}$$

Thus $V \cap H = \{(0 : 0 : 0 : 1)\}$, so V admits extra component at infinity.

(iii): Consider $g(x_0, x_1, x_2, x_3) = x_3^2 - x_1^2 - x_2^2 \in k[x_0, x_1, x_2, x_3]$. Note that $W = U_0 \cap \mathrm{V}(g)$. The points of $V \cap H$ satisfies the system

$$\begin{cases} x_3^2 - x_1^2 - x_2^2 = 0 \\ x_0 = 0 \end{cases}$$

Thus

$$V \cap H = \{(0 : a : b : c) \in \mathbb{P}^4 \;\; ; \;\; (a, b, c) \in W\}.$$

$\square$

Question 8.2.16: A homogeneous polynomial $f \in k[x_0, \dots, x_n]$ can also define an affine variety $C = \mathrm{V}_a(f) \subseteq k^{n+1}$, where the subscript denotes we are working in the affine space. We call C the affine cone over the projective variety $V = \mathrm{V}(f) \subseteq \mathbb{P}^n(k)$.

(i): Show that if C contains the point $P \neq (0, \dots, 0)$, then C contains whole line through the origin in k^{n+1} spanned by P.

(ii): A point $P \in k^{n+1} \setminus \{0\}$ gives homogeneous coordinates for a point $p \in \mathbb{P}^n(k)$. Show that p is in the projective variety V if and only if the line through the origin determined by P is contained in C.

(iii): Deduce that C is the union of the collection of lines through the origin in k^{n+1} corresponding to the points in V.

Proof: **(i):** Suppose that f is an homogeneous polynomial with $\deg(f) = d$. If C contains a point $P = (a_0, \ldots, a_n) \neq 0$, then $f(a_0, \ldots, a_n) = 0$. Thus, as f is homogeneous, for all $\lambda \in k$,we have that

$$f(\lambda P) = f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n) = 0.$$

Thus the line $L_P = \{tP \ ; \ t \in k\} \subseteq C$ and so C contains whole line through the origin spanned by P.

(ii): Suppose that V contains the point $p = (x_0 : \cdots : x_n)$, so $f(tx_0, \ldots, tx_n) = 0$ for all $t \in k$. This means that the line $\{t(x_0, \ldots, x_n); t \in k\}$ through the origin determined by $P = (a_0, \ldots, a_n)$ is contained in C.

Conversely, if the line $\{t(x_0, \ldots, x_n); t \in k\}$ through the origin determined by $P = (a_0, \ldots, a_n)$ is contained in C, then $f(tx_0, \ldots, tx_n) = 0$ for all $t \in k$. This implies that f vanishes at point $p = (a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$. Thus $p \in V = \mathrm{V}(f)$.

(iii): I claim that

$$C = \bigcup_{p \in V} \{tP \ ; \ t \in k\}$$

Indeed it is easy to verify the equality when $\deg(f) = 0$, so suppose that $\deg(f) = d > 0$. It is clear that $(0, \ldots, 0)$ belongs both sides of equation. If $P = (a_0, \ldots, a_n) \in C$ with $P \neq 0$, the item (ii) says that the corresponding point $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n(k)$ belongs to V. Thus $P = 1 \cdot (a_0, \ldots, a_n) \in \bigcup_{p \in V} \{tP \ ; \ t \in k\}$.

Conversely, if $P = (a_0, \ldots, a_n) \neq 0 \in \bigcup_{p \in V} \{tP \ ; \ t \in k\}$, then $(ta_0 : \cdots : ta_n) \in V$ for some $t \neq 0$, which implies that

$$t^d f(a_0, \ldots, a_n) = f(t^d a_0 : \cdots : t^d a_n) = 0$$

and so $f(a_0, \ldots, a_n) = 0$, that is, $P = (a_0, \ldots, a_n) \in C$. $\square$

Question 8.2.17 Homogeneous polynomials satisfy an important relation known as Euler's

Formula. Let $f \in k[x_0, \ldots, x_n]$ be homogeneous of total degree d. Then Euler's Formula states that

$$\sum_{k=0}^{n} x_k \frac{\partial f}{\partial x_k} = d \cdot f$$

(i): Verify the Euler's Formula for the polynomial $f(x_0, x_1, x_2) = x_0^3 - x_1 x_2^2 + 2x_1 x_3^2$.

(ii): Prove the Euler's formula.

Proof: **(i):** Calculating the partial derivatives, we obtain

$$\begin{aligned}
\frac{\partial f}{\partial x_0}(x_0, x_1, x_2, x_3) &= 3x_0^2 \\
\frac{\partial f}{\partial x_1}(x_0, x_1, x_2, x_3) &= -x_2^2 + 2x_3^2 \\
\frac{\partial f}{\partial x_2}(x_0, x_1, x_2, x_3) &= -2x_1 x_2 \\
\frac{\partial f}{\partial x_3}(x_0, x_1, x_2, x_3) &= 4x_1 x_3
\end{aligned}$$

Thus

$$\sum_{k=0}^{3} x_k \frac{\partial f}{\partial x_k} = 3f.$$

(ii): Write f as

$$f(x_0, \ldots, x_n) = \sum_{\alpha \in I} a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n}$$

where $\alpha_0 + \cdots + \alpha_n = d$ for all $\alpha \in I$. Observe that

$$\begin{aligned}
\sum_{k=0}^{n} x_k \frac{\partial f}{\partial x_k} &= \sum_{k=0}^{n} x_k \frac{\partial}{\partial x_k}\left(\sum_{\alpha \in I} a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n}\right) = \sum_{k=0}^{n} x_k \left(\sum_{\alpha \in I} \frac{\partial}{\partial x_k} a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n}\right) \\
&= \sum_{k=0}^{n} x_k \left(\sum_{\alpha \in I} \alpha_k a_\alpha x_0^{\alpha_0} \cdots x_k^{\alpha_k - 1} \cdots x_n^{\alpha_n}\right) = \sum_{k=0}^{n} \left(\sum_{\alpha \in I} \alpha_k a_\alpha x_0^{\alpha_0} \cdots x_k^{\alpha_k} \cdots x_n^{\alpha_n}\right) \\
&= \sum_{k=0}^{n} \left(\sum_{\alpha \in I} \alpha_k a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n}\right) = \sum_{\alpha \in I} \left(\sum_{k=0}^{n} \alpha_k a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n}\right) = \sum_{\alpha \in I} d a_\alpha x_0^{\alpha_0} \cdots x_n^{\alpha_n} = df.
\end{aligned}$$

□

Question 8.2.18: In this exercise, we will consider hyperplanes in $\mathbb{P}^n(k)$ in greater details.

(i): Show that two homogeneous linear polynomials

$$\begin{cases} a_0 x_0 + \cdots + a_n x_n = 0, \\ b_0 x_0 + \cdots + b_n x_n = 0 \end{cases}$$

define the same hyperplane in $\mathbf{P}^n(k)$ if and only if there is $\lambda \neq 0$ such that $a_i = \lambda b_i$ for all $0 \leq i \leq n$.

(ii): Show that the map sending the hyperplane $\mathrm{V}(a_0x_0 + \cdots + a_nx_n)$ to the vector $(a_0, \ldots, a_n)$ gives a one-to-one correspondence

$$\phi : \{\text{hyperplanes in } \mathbb{P}^n(k)\} \longrightarrow (k^{n+1} \setminus \{0\})/\sim$$

where $\sim$ is the equivalence relation of Definition 1. The set on the left is called the dual projective space and is denoted by $\mathbb{P}^n(k)^\vee$. Geometrically, the points of $\mathbb{P}^n(k)^\vee$ are hyperplanes in $\mathbb{P}^n(k)$.

(iii): Describe the subset of $\mathbf{P}^n(k)^\vee$ corresponding to the hyperplanes containing $p = (1 : 0 : \cdots : 0)$.

Proof: **(i):** Observe that $\mathrm{V}(a_0x_0 + \cdots + a_nx_n)$ is a hyperplane if and only if $(a_0, \ldots, a_n) \neq 0$. Thus we should consider only the cases in which $(a_0, \ldots, a_n) \neq 0$. Consider the hyperplanes $V_1 = \mathrm{V}(a_0x_0 + \cdots + a_nx_n)$ and $V_2 = \mathrm{V}(b_0x_0 + \cdots + b_nx_n)$ and suppose that $V_1 = V_2$. Define the linear mapping

$$\psi : k^{n+1} \longrightarrow k^2$$

$$(x_0, \ldots, x_n) \longmapsto (\textstyle\sum_{k=0}^n a_kx_k, \sum_{k=0}^n b_kx_k)$$

Note that $V_1 = V_2$ if and only if $\dim(\ker(\psi)) = n$. By Kernel-Image theorem, we have that the matrix

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_n \end{pmatrix}$$

has rank 1, so the linear space generated by the rows are LD, so there is $\lambda \neq 0$ such that

$$(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n).$$

(ii): Note that ϕ is well defined, because if $\mathrm{V}(a_0x_0 + \cdots + a_nx_n) = \mathrm{V}(b_0x_0 + \cdots + b_nx_n)$, then $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$ for some $\lambda \neq 0$, which implies that

$$\phi(V(a_0x_0 + \cdots + a_nx_n)) = [(a_0, \ldots, a_n)] = [(b_0, \ldots, b_n)] = \phi(V(b_0x_0 + \cdots + b_nx_n))$$

Clearly ϕ is surjective. Moreover, if

$$\phi(V(a_0x_0 + \cdots + a_nx_n)) = [(a_0, \ldots, a_n)] = [(b_0, \ldots, b_n)] = \phi(V(b_0x_0 + \cdots + b_nx_n)),$$

so there is $\lambda \neq 0$ such that $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$. By item (ii), we have that

$$\mathrm{V}(a_0x_0 + \cdots + a_nx_n) = \mathrm{V}(b_0x_0 + \cdots + b_nx_n),$$

which implies that ϕ is injective.

(iii): Observe that $\mathrm{V}(a_0x_0 + \cdots + a_nx_n)$ is a hyperplane in $\mathbb{P}^n(k)$ containing the point $p = (1 : 0 : \cdots : 0)$ if and only if $a_0 = 0$. Thus

$$\{V \in \mathbb{P}^n(k)^\vee \ ; \ (1:0:\cdots:0) \in V\} = \{\mathrm{V}(a_0x_0 + \cdots + a_nx_n) \in \mathbb{P}^n(k)^\vee \ ; \ a_0 = 0\} = \mathbb{P}^{n-1}(k)^\vee.$$

□

Question 8.2.19: Let k be an algebraically closed field. Show that every homegeneous polynomial in two variables can be factored into linear homogeneous polynomials in $k[x_0, x_1]$:

$$f(x_0, x_1) = \prod_{k=1}^{d} (a_kx_0 + b_kx_1),$$

where d is the total degree of f.

Proof: Consider $g(x_1) = f^{dh}(x_1) = f(1, x_1) \in k[x_1]$. Since k is an algebraically closed field, we can factor $g(x_1)$ into linear factors

$$g(x_1) = \prod_{k=1}^{d'} (a_kx_1 + b_k),$$

where $d' \leq d$. Making the homogeneization of g with respect the variable x_0, we obtain

$$f = (f^{dh})^h = x_0^e \left[x_0^{d'} \prod_{k=1}^{d'} \left(a_k \frac{x_1}{x_0} + b_k \right) \right]$$

where e is the largest non-negative integer such that x_0^e divides f. A careful analysis shows us that $e = d - d'$, so

$$f = x_0^d \prod_{k=1}^{d'} \left(a_k \frac{x_1}{x_0} + b_k \right) = x_0^{d-d'} \prod_{k=1}^{d'} (a_kx_1 + b_kx_0) = \prod_{k=1}^{d} (a_kx_1 + b_kx_0),$$

where $b_k = 1$ for all $d' + 1 \leq k \leq d$ and $a_k = 0$ for all $d' + 1 \leq k \leq d$. □

Question 8.2.20: The pencil determined by two surfaces $V = \mathrm{V}(f) \subseteq k^n$ and $W = \mathrm{V}(g) \subseteq k^n$ is the family of hypersurfaces $\mathrm{V}(f + cg)$ for $c \in k$. Setting $c = 0$, we obtain V as an element of the pencil. However, W is not (usually) an element of the pencil when defined in this way. To include W, we must proceed as follows.

(i): Let (a, b) be homogeneous coordinates in $\mathbb{P}^1(k)$. Show that $\mathrm{V}(af + bg)$ is well-defined in the sence that all homogeneous coordinates $(a : b)$ for a given point in $\mathbb{P}^1(k)$ yield the same variety $\mathrm{V}(af + bg)$. Thus, we obtain a family of varieties parametrized by $\mathbb{P}^1(k)$, which is also called the pencil of varieties defined by V and W.

(ii): Show that both V and W are contained in the pencil $\mathrm{V}(af + bg)$.

(iii): Let $k = \mathbb{C}$. Show that every affine curve $\mathrm{V}(f) \subseteq \mathbb{C}^2$ defined by a polynomial f of total degree d is contained in a pencil of curves $\mathrm{V}(aF + bG)$ parametrized by $\mathbb{P}^1(\mathbb{C})$, where $\mathrm{V}(F)$ is union of lines and G is a polynomial of degree strictly less than d.

Proof: **(i):** In fact let $(a : b) = (c : d)$ elements of $\mathbb{P}^1(\mathbb{C})$. Thus there is $\lambda \neq 0$ such that $a = \lambda c$ and $b = \lambda d$. Hence

$$\mathrm{V}(af + bg) = \mathrm{V}(\lambda cf + \lambda dg) = \mathrm{V}(\lambda(cf + dg)) = \mathrm{V}(\lambda) \cup \mathrm{V}(cf + dg) = \emptyset \cup \mathrm{V}(cf + dg) = \mathrm{V}(cf + dg).$$

(ii): Indeed, considering $(a : b) = (1 : 0)$, we obtain $\mathrm{V}(af + bg) = \mathrm{V}(f) = V$. On the other hand, considering $(a : b) = (0 : 1)$, we obtain $\mathrm{V}(af + bg) = \mathrm{V}(g) = W$.

(iii): Decompose f as

$$f = f_0 + f_1 + \cdots + f_d$$

where f_i is the homogeneous component of f of degree i. Set $F = f_d$ and $G = f_0 + \cdots + f_{d-1}$. Thus, considering the pencil $\mathrm{V}(aF + bG)$ parametrized by $\mathbb{P}^1(\mathbb{C})$, we obtain that $\mathrm{V}(f)$ is the curve associated to parameter $(1 : 1)$. Note that G is a polynomial with total degree strictly less than d. Moreover, since the field is algebraically closed and F is homogeneous, by Question 8.2.19, we can factor F as

$$F = \prod_{k=1}^{d} (a_k x_0 + b_k x_1).$$

Thus

$$\mathrm{V}(F) = \mathrm{V}\left(\prod_{k=1}^{d} (a_k x_0 + b_k x_1)\right) = \bigcup_{k=1}^{d} \mathrm{V}(a_k x_0 + b_k x_1).$$

□

6.3 The Projective Algebra-Geometry Dictionary

Question 8.3.1: Show that a principal ideal $I = \langle f \rangle \subseteq k[x_0, \ldots, x_n]$ is homogeneous if and only if f is a homogeneous ideal.

Suppose that f is a homogeneous ideal of total degree d and denote it by f_d. Let $g \in \langle f \rangle$. If $g \in I$, there is $h \in k[x_1, \ldots, x_n]$ such that $g = fh$. Writting

$$g = g_0 + \cdots + g_r,$$
$$h = h_0 + \cdots + h_s,$$

then

$$g_0 + \cdots + g_r = fh = f_d(h_0 + \cdots + h_s) = f_d h_0 + \cdots + f_d h_s$$

Comparing the homogeneous components of g, we conclude that each g_i is of form $f_d h_j = f h_j$, where $i = d + j$. Thus $g_i \in I$ for all $1 \leq i \leq r$ and so I is homogeneous.

On the other hand suppose that I is homogeneous and $f = f_0 + \cdots + f_d$, with $f_d \neq 0$. I will prove that $f = f_d$. Since $f \in I$, by homogeneity, we have that $f_d \in I$, so there is $g \in k[x_0, \ldots, x_n]$ such that $f_d = fg$. A simple analysis of homogeneous components shows us that the total degree of g must be 0. Thus $g = \lambda$ is a non-zero constant polynomial, which implies that $f = \lambda^{-1} f_d$ and so f is homogeneous. $\square$

Question 8.3.2: This exercise will study how the algorithms of Chapter 2 interact with homogeneous polynomials.

(i): Suppose we use the division algorithm to divide a homogeneous polynomial f by homogeneous polynomial $f_1, \ldots, f_s$. This gives an expression of the form

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

Prove that the quotients $a_1, \ldots, a_s$ and the remainder r are homogeneous polynomials (possibly zero). What is the total degree of r.

(ii): If f, g are homogeneous polynomials, prove that the S-polynomial is homogeneous.

(iii): By analyzing the Buchberger algorithm, show that a homogeneous ideal has a homogeneous Gröbner Basis.

(iv): Prove the implication $(ii) \Longleftrightarrow (iii)$ of Theorem 2.

Proof: **(i):** It is enough to analyze carefully the Division Algorithm. If the remainder is not the zero polynomial, its degree coincides with the total degree of f.

(ii): Let f and g be homogeneous polynomials with total degree equal to r and s, respectively. Denote

$$\text{multideg}(f) = \alpha = (\alpha_1, \dots, \alpha_n),$$
$$\text{multideg}(g) = \beta = (\beta_1, \dots, \beta_n).$$

Observe that $\sum_{k=1}^{n} \alpha_k = d$ and $\sum_{k=1}^{n} \beta_k = d'$. Set $\gamma_i = \max\{\alpha_i, \beta_i\}$ for each $i = 1, \dots, n$ and define

$$\mathbf{x}^\gamma = x_1^{\gamma_1} \cdots x_n^{\gamma}.$$

By definition we have that

$$S(f,g) = \frac{\mathbf{x}^\gamma}{\text{LT}(f)} f - \frac{\mathbf{x}^\gamma}{\text{LT}(g)} g = \text{LC}(f)^{-1} \mathbf{x}^{\gamma-\alpha} f - \text{LC}(g)^{-1} \mathbf{x}^{\gamma-\beta} g$$

Let x^η be a monomial of f and x^ζ a monomial of g, where $\eta = (a_1, \dots, a_n)$ and $\eta = (b_1, \dots, b_n)$ with $\sum_{k=1}^{n} a_k = r$ and $\sum_{k=1}^{n} b_k = s$. It is enough to show that

$$\sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\} - \alpha_i + a_i) = \sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\} - \beta_i + b_i).$$

However, it is clear, because

$$\begin{aligned} \sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\} - \alpha_i + a_i) &= \sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\}) - r + r = \sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\}) - s + s \\ &= \sum_{i=1}^{n} (\max\{\alpha_i, \beta_i\} - \beta_i + b_i). \end{aligned}$$

(iii): Let $I = (f_1, \dots, f_n)$ be a homogeneous ideal. The Bucheberger's algorithm says us that a Gröbner basis of I consists in joint to $F = \{f_1, \dots, f_n\}$ a finite number of non-zero polynomials of form $\overline{S(f_i, f_j)}^F$. Since $S(f_i, f_j)$ are homogeneous for each $i \neq j$ by item (ii), the item (i) says that $\overline{S(f_i, f_j)}^F$ also are homogeneous for all $i \neq j$. Thus the Gröbner basis of I is constituted by homogeneous polynomials.

(iv): If I is a homogeneous ideal, the part (iii) tells us that I admits a Gröbner Basis constituted by homogeneous polynomials. In particular, I admits a reduced Gröbner basis. Conversely if I admits a Gröbner basis $G = \{g_1, \dots, g_r\}$ constituted by homogeneous polynomials, then $I = \langle g_1, \dots, g_r \rangle$ is a homogeneous ideal. □

Question 8.3.4: Suppose that $I \subseteq k[x_1, \dots, x_n]$ has a basis G consisting of homogeneous polynomials.

(i): Prove that G is a Gröbner basis for I with respect the lex order if and only if G is a Gröbner basis for I with respect the grlex one (assuming that the variables are ordered in the same way).

(ii): Conclude that, for a homogeneous ideal, the reduced Gröbner basis for lex and grlex orders are the same.

Proof: **(i):** By hypothesis I i an homogeneous ideal, because it is generated by homogeneous polynomial. Consider the $k[x_1, \ldots, x_n]$ equipped with the Lex order. By Question 8.3.3, I admits a Gröbner basis constituted by homogeneous polynomials. In order to prove that G is a Gröbner for I with respect the grlex order, it is enough to show that, if f is a homogeneous polynomial, then the leading term of f with respect the lex order coincides with the leading therm of f with respect the grlex one. But it is clear because, since f is a homogeneous polynomial, the total degrees of all monomials are the same, and so is the Lexicographic order which will be decide what monomial will be bigger than another, so G is a Gröbner basis for I with respect the grlex order. The converse is proved using absolutely the same argument.

(ii): Let G be a Gröbner basis of I with respect both orders. Dividing each polynomial by its leading coefficient, we obtain that G is a Gröbner basis of I with respect both orders constituted by monic polynomials. Eliminating all polynomials $p \in G$ such that p contains a monomial belonging in $\langle \mathrm{LT}(G \smallsetminus \{p\}) \rangle$, we obtain a Gröbner basis satisfying the axioms to be reduced. By uniqueness of reduced Gröbner basis, we conclude that reduced Gröbner bases for I with respect lex and grlex coincides. □

Question 8.3.13: In this exercise, we will show how to define the field of rational functions on an irreducible projective variety $V \subseteq \mathbb{P}^n(k)$. If we take a homogeneous polynomial $f \in k[x_0, \ldots, x_n]$, then f does give well-defined function on V. To see why, let $p = (a_0 : \cdots : a_n) \in V$. Then we also have $p = (\lambda a_0 : \cdots : \lambda a_n)$ for any $\lambda \in k \smallsetminus \{0\}$ and

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n),$$

where d is the total degree of f.

(i): Explain why the above equation makes it impossible for us to define $f(p)$ as a single-valued function in V.

(ii): If $g \in k[x_0, \ldots, x_n]$ is also homogeneous of total degree d and $g \in\notin \mathrm{I}(V)$, then show that $\phi = f/g$ is a well-defined function in a nonempty set $\mathrm{V} \smallsetminus (V \cap \mathrm{V}(g)) \subseteq V$.

(iii): We say that $\phi = f/g$ and $\phi' = f'/g'$ are equivalent on V, written $\phi \sim \phi'$, provided that there exists a proper variety $W \subseteq V$ such that ϕ and ϕ' are well-defined and coincides in $V \smallsetminus W$. Prove that $\smallsetminus$ is an equivalence relation. An equivalence class for $\sim$ of rational function on V, and the set of all equivalence classes is denoted by $k(V)$.

(iv): Show that addition and multiplication of equivalence classes is well-defined and makes $k(V)$ into a field called the field of rational functions of projective variety V.

Solution: **(i):** In fact, suppose that $f(a_0, \ldots, a_n) = t \neq 0$, thus, since $\lambda(a_0 : \cdots : a_n)$ and $(a_0 : \cdots : a_n)$ are the same point in $\mathbb{P}^n(k)$, we would have that $t = \lambda^d t$ for all λ nonzero, which is clearly impossible.

(ii): Let $p = (a_0 : \cdots : a_n) \in V \smallsetminus (V \cap \mathrm{V}(g))$. Observe that

$$\phi(\lambda p) := \frac{f(\lambda p)}{g(\lambda p)} = \frac{\lambda^d f(p)}{\lambda^d g(p)} = \frac{f(p)}{g(p)} := \phi(p).$$

Thus ϕ is well-defined.

(iii): The reflexivity and symmetry are clear. Let $\phi = f/g$, $\psi = r/s$ and $\zeta = u/v$ well-defined such that $\phi \sim \psi$ and $\psi \sim \zeta$. Thus there are nonempty open subsets $U \subseteq V$ and $W \subseteq V$ such that ϕ, ψ coincide and are well-defined on U and ψ, ζ coincide and are well-defined on W. Since V is irreducible, $U \cap W \neq \emptyset$, thus ϕ and ζ coincide and are well-defined on the nonempty subset $U \cap W \subseteq V$. Thus $\sim$ is an equivalence relation.

(iv): Let $\phi = f/g$, $\psi = r/s$ be rational functions on V. Observe $(\mathrm{V}(g) \cup \mathrm{V}(s) \cap V = \mathrm{V}(gs) \cap V$ is a proper subset of V. Indeed, since $\mathrm{V}(g) \cap V$ and $\mathrm{V}(s) \cap V$ are proper closed subsets of V and V is irreducible, then

$$\mathrm{V}(gs) \cap V = (V \cap \mathrm{V}(g)) \cup (V \cap \mathrm{V}(s))$$

is a proper closed subset of V. Since

$$\phi + \psi = \frac{fs + rg}{gs} \qquad\qquad \phi \cdot \psi = \frac{fr}{gs},$$

$\mathrm{V}(gs) \cap V$ is properly contained in V, we conclude that the addition and multiplication are well-defined operations. Now suppose that $\phi \neq 0$ and define $\zeta = g/f$. Since $\phi \neq 0$, we have that $f \notin \mathrm{I}(V)$, thus $\mathrm{V}(f) \cap V$ is a proper closed subset of V, which implies that ζ is well-defined on nonempty open set $V \smallsetminus \mathrm{V}(g)$. Since $\phi \cdot \zeta = \zeta \cdot \phi = 1$ on nonempty open subset $V \smallsetminus \mathrm{V}(fg)$, we conclude that $\zeta = \phi^{-1}$, so $k(V)$ is a field.

(v): Suppose without lost of generality that $i = 0$ and denote $V = \mathrm{V}(f_1, \ldots, f_r)$, $f_1, \ldots, f_r \in k[x_0, \ldots, x_n]$. Note that

$$V \cap U_0 = \{(1 : a_1 : \cdots : a_n) \in \mathbb{P}^n(k) \ ; \ f_1(1, a_1, \ldots, a_n) = \cdots = f_r(1, a_1, \ldots, a_n) = 0\}$$

Doing the identification U_0 with k^n with the mapping $(a_0 : a_1 : \cdots : a_n) \longrightarrow (a_1/a_0, \cdots, a_n/a_0)$, we can interpret $V \cap U_0$ as

$$V \cap U_0 = \{(a_1 : \cdots : a_n) \in k^n \ ; \ f_1(1, a_1, \ldots, a_n) = \cdots = f_r(1, a_1, \ldots, a_n) = 0\} = \mathrm{V}(f_1^{dh}, \ldots, f_r^{dh}).$$

Thus $V \cap U_0$ has structure of affine variety. Now define

$$\eta : k[x_1, \ldots, x_n] \longrightarrow k(V)$$

such that $\eta(x_i) = x_i/x_0$. It is clear that $\mathrm{I}(V \cap U_0) \subseteq k[x_1, \ldots, x_n]$ is contained in the $\ker(\eta)$, so η induces

$$\widehat{\eta} : \frac{k[x_1, \ldots, x_n]}{\mathrm{I}(V \cap U_0)} \longrightarrow k(V)$$

such that $\widehat{\eta}(\overline{x_i}) = x_i/x_0$. Since $\widehat{\eta}$ sends nonzero elements to nonzero elements, then $\widehat{\eta}$ induces

$$\phi : k(V \cap U_0) \longrightarrow k(V)$$

such that $\phi(f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)) = \widehat{\eta}(f(x_1, \ldots, x_n))\widehat{\eta}(g(x_1, \ldots, x_n))^{-1}$. As $k(V \cap U_0)$ is field, we have that ϕ is one-to-one. Finally let $\phi = f/g \in k(V)$, where f, g are homogeneous polynomials with total degree d. Since $g \notin \mathrm{I}(V \cap U_0)$, we obtain that

$$\phi(f/g) = \frac{f}{x_0^d} \cdot \frac{x_0^d}{g} = f/g = \phi,$$

thus ϕ is surjective and so a field isomorphism. $\square$