Chapter 1, Geometry, Algebra, and Algorithms

§4. Ideals.

To set the notation: k is a field; $f_1, \dots, f_s \in k[x_1, \dots, x_n]$; $\mathbf{V}(f_1, \dots, f_s)$ denotes the set of common zeros of $f_1, \dots, f_s$ in k^n, and $\langle f_1, \dots, f_s \rangle$ denotes the ideal in $k[x_1, \dots, x_n]$ generated by the polynomials $f_1, \dots, f_s$. If $A \subset k^n$, then $\mathbf{I}(A)$ is the set of polynomials in $k[x_1, \dots, x_n]$ which vanish on A. $\mathbf{I}(A)$ is an ideal in $k[x_1, \dots, x_n]$. It is always true that

$$\langle f_1, \dots, f_s \rangle \subset \mathbf{I}\big(\mathbf{V}(f_1, \dots, f_s)\big), \tag{1.4.1}$$

but equality in (1.4.1) need not occur. For example, $\langle x^2, y^2 \rangle \subsetneq \mathbf{I}\big(\mathbf{V}(x^2, y^2)\big)$ as we will now show. If $(a_1, a_2) \in \mathbf{V}(x^2, y^2)$, then $x^2(a_1, a_2) = a_1^2 = 0$ and $y^2(a_1, a_2) = a_2^2 = 0$; so $a_1 = a_2 = 0$. The variety $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$. The set of polynomials which vanish at $(0, 0)$ is easily seen to be the ideal $\langle x, y \rangle$ of polynomials whose constant term is zero, but we won't actually use this fact. What we will show is that $x \in \mathbf{I}\big(\{(0, 0)\}\big)$ but $x \notin \langle x^2, y^2 \rangle$. In fact each polynomial f in $\langle x^2, y^2 \rangle$ has the form $f = h(x, y)x^2 + g(x, y)y^2$, $h, g \in k[x, y]$. As such each monomial in f has total degree at least 2 and this rules out x.

Although in general $\mathbf{I}\big(\mathbf{V}(f_1, \dots, f_s)\big) \supsetneq \langle f_1, \dots, f_s \rangle$ the ideal of a variety always contains enough information to determine the variety uniquely.

Proposition 1.4.8. Let V and W be affine varieties in k^n. Then
(i) $V \subset W$ if and only if $\mathbf{I}(W) \subset \mathbf{I}(V)$.
(ii) $V = W$ if and only if $\mathbf{I}(W) = \mathbf{I}(V)$.

Proof. (ii) is an easy consequence of (i); so we will just prove (i).

($V \subset W \Rightarrow \mathbf{I}(W) \subset \mathbf{I}(V)$): Suppose $V \subset W$ and $f \in \mathbf{I}(W)$. Then $f(W) = 0$; so $f(V) = 0$ and $f \in \mathbf{I}(V)$.

($\mathbf{I}(W) \subset \mathbf{I}(V) \Rightarrow V \subset W$): Suppose $\mathbf{I}(W) \subset \mathbf{I}(V)$ and $\mathbf{p} \notin W$. It suffices to show that $\mathbf{p} \notin V$. Since W is a variety there are polynomials $h_1, \dots, h_t$ such that $W = \mathbf{V}(h_1, \dots, h_t)$ If $\mathbf{p} \notin W$ it must be that $h_i(\mathbf{p}) \neq 0$ for some $1 \leq i \leq t$. Without loss of generality suppose $h_1(\mathbf{p}) \neq 0$. h_1 vanishes on W; so $h_1 \in \mathbf{I}(W) \subset \mathbf{I}(V)$. But every polynomial in $\mathbf{I}(V)$ vanishes at every point of V. Since $h_1(\mathbf{p}) \neq 0$ and $h_1 \in \mathbf{I}(V)$, it must be that $\mathbf{p} \notin V$. ∎

Here are some questions to consider:

- (Ideal Description) Can every ideal $I \subset k[x_1, \dots, x_n]$ be written as $\langle f_1, \dots, f_s \rangle$ for some $f_1, \dots, f_s \in k[x_1, \dots, x_n]$?
- (Ideal Membership) If $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, is there an algorithm to decide whether a given $f \in k[x_1, \dots, x_n]$ lies in $\langle f_1, \dots, f_s \rangle$?
- (Nullstellensatz) Given $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, what is the exact relation between $\langle f_1, \dots, f_s \rangle$ and $\mathbf{I}\big(\mathbf{V}(f_1, \dots, f_s)\big)$?

---

§1.4.1.

Consider the equations

$$x^2 + y^2 - 1 = 0,$$
$$xy - 1 = 0$$

which describe the intersection of a circle and a hyperbola.

(a) Use algebra to eliminate y from the above equations.

Solution. Multiply $x^2 + y^2 - 1 = 0$ to get $x^3 + (xy)y - x = 0$. Replace xy by 1 and multiply by x again to get $x^4 + 1 - x^2 = 0$ which is the desired result.

(b) Show how the polynomial found in part (a) lies in $\langle x^2 + y^2 - 1, xy - 1 \rangle$.

Solution.

$$x^4 - x^2 + 1 = x^2(x^2 + y^2 - 1) - (xy + 1)(xy - 1).$$

---

§1.4.2.

Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Prove the following statements are equivalent:

(i) $f_1, \ldots, f_s \in I$.

(ii) $\langle f_1, \ldots, f_s \rangle \subset I$.

Solution. ((i) $\Rightarrow$ (ii)): If $f_1, \ldots, f_s \in I$, since I is an ideal the smallest ideal containing $\{f_1, \ldots, f_s\}$, namely $\langle f_1, \ldots, f_s \rangle$ is a subset of I.

((ii) $\Rightarrow$ (i)): For each t, $1 \leq t \leq s$, $f_t \in \langle f_1, \ldots, f_s \rangle \subset I$; so $f_t \in I$.

---

§1.4.3.

Use Exercise 1.4.2 to prove the following equalities of ideals in $k[x, y]$.

(a) $\langle x + y,\, x - y \rangle = \langle x,\, y \rangle$.

Solution. $x = \frac{1}{2}(x + y) + \frac{1}{2}(x - y) \in \langle x + y, x - y \rangle$. $y = \frac{1}{2}(x + y) - \frac{1}{2}(x - y) \in \langle x + y,\, x - y \rangle$. So from Exercise 1.4.2 it follows that $\langle x,\, y \rangle \subset \langle x + y,\, x - y \rangle$. The other inclusion is even more trivial.

(b) $\langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle = \langle x,\, y \rangle$.

Solution.

$$\begin{aligned}
x - y &= (x + xy) - (y + xy) && \text{is in } \langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle;\\
(x - y)^2 &= x^2 - 2xy + y^2 && \text{is in } \langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle;\\
x + y &= (x + xy) + (y + xy) - (x - y)^2 && \text{is in } \langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle;\\
x &= \frac{1}{2}(x - y) + \frac{1}{2}(x + y) && \text{is in } \langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle.
\end{aligned}$$

Switching x and y in the preceding relations gives y is in $\langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle$. We have shown $\langle x,\, y \rangle \subset \langle x + xy,\, y + xy,\, x^2,\, y^2 \rangle$. The other inclusion is trivial.

(c) $\langle 2x^2 + 3y^2 - 11,\, x^2 - y^2 - 3 \rangle = \langle x^2 - 4,\, y^2 - 1 \rangle$.

Solution. The equality of these ideals follows from the relations

$$\begin{aligned}
2x^2 + 3y^2 - 11 &= 2(x^2 - 4) + 3(y^2 - 1),\\
x^2 - y^2 - 3 &= (x^2 - 4) - (y^2 - 1),\\
5(x^2 - 4) &= (2x^2 + 3y^2 - 11) + 3(x^2 - y^2 - 3),\\
5(y^2 - 1) &= (2x^2 + 3y^2 - 11) - 2(x^2 - y^2 - 3).
\end{aligned}$$

---

§1.4.4.

Prove: If $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ then $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.

Proof. If $\mathbf{p} \in \mathbf{V}(f_1, \ldots, f_s)$ then $f_i(\mathbf{p}) = 0$, $1 \leq i \leq s$. By hypothesis each $g_j \in \langle f_1, \ldots, f_s \rangle$; so $g_j = h_{j1}f_1 + \cdots + h_{js}f_s$, for some choice of $h_{ji} \in k[x_1, \ldots, x_n]$. But then for each j, $1 \leq j \leq t$, $g_j(\mathbf{p}) = \sum_{i=1}^{s} h_{ji}(\mathbf{p})f_i(\mathbf{p}) = 0$ which means that $\mathbf{p} \in \mathbf{V}(g_1, \ldots, g_t)$. We have shown that $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(g_1, \ldots, g_t)$. The other inclusion follows from the symmetry of the hypothesis.

---

§1.4.5.

Show that $\mathbf{V}(x + xy,\, y + xy,\, x^2,\, y^2) = \mathbf{V}(x,\, y)$.

Solution. We already know from Exercise 1.4.3.b that $\langle x+xy,\, y+xy,\, x^2,\, y^2\rangle = \langle x,\, y\rangle$. An application of Exercise 1.4.4 then gives the conclusion $\mathbf{V}(x+xy,\, y+xy,\, x^2,\, y^2) = \mathbf{V}(x,\, y)$.

---

§1.4.6.

The word "basis" is used in various ways in mathematics. In this exercise, we will see that "a basis of an ideal", as defined in this section, is quite different from "a basis of a subspace" as studied in linear algebra. Before beginning we make the remark that a basis is a subset, but in keeping with common usage we will not always distinguish between $\{f_1, \ldots, f_s\}$ and $f_1, \ldots, f_s$, leaving the reader to supply the braces which delimit the list of elements in a set.

(a) First, consider the ideal $I = \langle x\rangle \subset k[x]$. As an ideal I has a basis consisting of the single element x. But I can also be regarded as a linear subspace of $k[x]$, which is a vectorspace over k.Prove that any vector space basis of I over k is infinite.

Solution. The elements $x,\, x^2,\, \ldots,\, x^{n+1}$ of I are linearly independent over k; so any basis of I over k has to have at least n elements. Since the positive integer n is arbitrary here, it follows that any basis of I over k coontains an infinite number of elements.

(b) In linear algebra, a basis must span and be linearly independent over k, whereas for an ideal, a basisis concerned only with spanning - there is no mention of any sort of independence. The reason is that once we all polynomial coefficients, no independence is possible. To see this, consider the ideal $\langle x,\, y\rangle \subset k[x, y]$. Show that zero can be written as a linear combination of y and x with nonzero polynomial coefficients.

Solution. $0 = y(x) - x(y)$.

(c) More generally, suppose that $f_1, \ldots, f_s$ is a basis for the ideal $I \subset k[x_1, \ldots, x_n]$. If $s \geq 2$ and $f_i \neq 0$ for each i, then show that for any i and j, zero can be written as a linear combination of f_i and f_j with nonzero polynomial coefficients.

Solution. $f_j(f_i) - f_i(f_j) = 0$.

(d) A consequence of the lack of independence is that when we write an element $f \in \langle f_1, \ldots, f_s\rangle$ as $f = \sum_{i=1}^{s} h_i f_i$, the coefficients h_j are not unique. As an example, consider $f = x^2 + xy + y^2 \in \langle x,\, y\rangle$. Express f as a linear combination of x and y in two different ways.

Solution. $f = (x+y)x + y \cdot y = x \cdot x + (x+1)y$. **Note:** Even though the h_i's are not uniqe, one can measure their lack of uniqueness. This leads to the interesting topic of *syzygies*.

(e) A basis $f_1, \ldots, f_s$ of the ideal I is said to be *minimal* if no proper subset of $\{f_1, \ldots, f_s\}$ is a basis for I. For example, $\{x,\, x^2\}$ is a basis of an ideal, but not a minimal basis since x generates the same ideal. Unfortunately, an ideal can have minimal bases consisting of different numbers of elements. To see this, show that $\{x\}$ and $\{x+x^2,\, x^2\}$ are minimal bases of the same ideal of $k[x]$. Explain how this contrasts with the situation in linear algebra.

Solution. $x \in \langle x+x^2,\, x^2\rangle$ but $x \notin \langle x+x^2\rangle$ every element of which is divisible by $x+x^2$ and $x \notin \langle x^2\rangle$ because every element of $\langle x^2\rangle$ is divisible by x^2. It follows that the basis $\{x+x^2,\, x^2\}$ cannot be reduced. The same is true for the bases $\{x+xy,\, y+xy,\, x^2,\, y^2\}$ and $\{x,\, y\}$. They are both minimal bases for the same ideal. In linear algebra the number of elements in a basis is fixed. It is the dimension of the subspace spanned by the basis. Thus in linear algebra every basis is minimal in the above sense.

---

§1.4.7.

Show that $\mathbf{I}\big(\mathbf{V}(x^n,\, y^m)\big) = \langle x,\, y\rangle$ for any positive integers n and m.

Solution. ($\supset$): $\mathbf{I}\big(\mathbf{V}(x^n,\, y^m)\big)$ consists of all those polynomials which vanish at $(0,0) \in k^2$. Thus $x, y \in \mathbf{I}\big(\mathbf{V}(x^n,\, y^m)\big)$.

($\subset$): Any polynomial f in $\mathbf{I}\big(\mathbf{V}(x^n,\, y^m)\big)$ vanishes at $(0,0)$ and so has a zero constant term. But then $f \in \langle x,\, y\rangle$.

---

§1.4.8.

The ideal $\mathbf{I}(V)$ of a variety has a special property not shared by all ideals. Specifically, we define an ideal I to be *radical* if whenever a power f^m of a polynomial f is in I, then f itself is in I. More succinctly, I is radical when $f \in I \Leftrightarrow f^m \in I$ for some positive integer m.

(a) Prove that $\mathbf{I}(V)$ is always a radical ideal.

Solution. $f^m \in \mathbf{I}(V)$ means $[f(\mathbf{p})]^m = 0$ for all $\mathbf{p} \in V$. This in turn is equivalent to $f(\mathbf{p}) = 0$ for all $\mathbf{p} \in V$ or to $f \in \mathbf{I}(V)$.

(b) Prove that $\langle x^2, y^2\rangle$ is not a radical ideal. This implies that $\langle x^2, y^2\rangle \neq \mathbf{I}(V)$ for any variety $V \subset k^2$. (Indeed, for any subset $V \subset k^2$.)

Solution. If $\langle x^2, y^2\rangle$ were a radical ideal, $f \in \langle x^2, y^2\rangle$ would be equivalent to $f^2 \in \langle x^2, y^2\rangle$. We know, however, that $x^2 \in \langle x^2, y^2\rangle$ but $x \notin \langle x^2, y^2\rangle$; so $\langle x^2, y^2\rangle$ cannot be a radical ideal.

---

§1.4.9.

Let $V = \mathbf{V}(y-x^2, z-x^3)$ be the twisted cubic. Suppose $f \in k[x,y,z]$ is in $\mathbf{I}\big(\mathbf{V}(y-x^2, z-x^3)\big) = \mathbf{I}(V)$.

Theorem 1.4.9.1. If the field k is infinite, $\langle y-x^2, z-x^3\rangle = \mathbf{I}\big(\mathbf{V}(y-x^2, z-x^3)\big)$.

Proof. ($\subset$): Suppose $h \in \langle y-x^2, z-x^3\rangle$. Then $h = A(y-x^2) + B(z-x^3)$ for some $A, B \in k[x,y,z]$. If $\mathbf{p} \in \mathbf{V}(y-x^2, z-x^3)$ it follows that $h(\mathbf{p}) = A(\mathbf{p})\cdot(y-x^2)(\mathbf{p}) + B(\mathbf{p})\cdot(z-x^3)(\mathbf{p}) = A(\mathbf{p})\cdot 0 + B(\mathbf{p})\cdot 0 = 0$ and hence that $h(\mathbf{p}) = 0$; so $h \in \mathbf{I}\big(\mathbf{V}(y-x^2, z-x^3)\big)$.

($\supset$): Expand the expression $x^a y^b z^c = x^a\left(x^2 - [y-x^2]\right)^b\left(x^3 - [z-x^3]\right)^c$ keeping the bracketed terms intact to get an equation of the form $x^a y^b z^c = A(x,y,z)[y-x^2] + B(x,y,z)[z-x^3] + R(x)$, where $A, B \in k[x,y,z]$ and $R(x) \in k[x]$. (**Note.** There are many ways to group these terms; so A and B are not necessarily unique, but $R(x) = x^{a+2b+3c}$ is unique.) By doing this for each monomial in a polynomial f it follows that any $f \in k[x,y,z]$ can be written in the form $f = A(x,y,z)[y-x^2] + B(x,y,z)[z-x^3] + R(x)$, where $A, B \in k[x,y,z]$ and $R(x) \in k[x]$. Now suppose $f \in \mathbf{I}\big(\mathbf{V}(y-x^2, z-x^3)\big)$. As such f vanishes on any point of the form $\mathbf{p} = (t, t^2, t^3)$. But $f(\mathbf{p}) = R(t)$; so $R(t) = 0$ for all $t \in k$. A nonzero polynomial can have at most a finite number of roots; so if k is infinite it must be that $R(x)$ is the zero polynomial. But then $f = A[y-x^2] + B[z-x^3] \in \langle y-x^2, z-x^3\rangle$. ∎

(a) Use the parametrization of the twisted cubic to show that $y^2 - xz \in \mathbf{I}(V)$.

Solution. If $\mathbf{p} = (t, t^2, t^3)$, then $(y^2-xz)(\mathbf{p}) = \left(t^2\right)^2 - t(t^3) = 0$. This says that $y^2 - xz \in \mathbf{I}(V)$.

(b) Use the argument given in the text to express $y^2 - xz$ as a combination of $y - x^2$ and $z - x^3$.

Solution.

$$\begin{aligned} y^2 &= (x^2 + [y-x^2])^2 = x^4 + (2x^2 + [y-x^2])[y-x^2];\\ xz &= x(x^3 + [z-x^3]) = x^4 + x[z-x^3];\\ y^2 - xz &= (x^2+y)[y-x^2] - x[z-x^3]. \end{aligned}$$

---

§1.4.10.

Use the argument given for theorem 1.4.9.1 to show that $\mathbf{I}(\mathbf{V}(x-y)) = \langle x-y\rangle$.

Solution. ($\supset$): If $h \in \langle x-y\rangle$, then $h(x,y) = g(x,y)(x-y)$ for some $g \in k[x,y]$. If $\mathbf{p} \in \mathbf{V}(x-y)$, then $h(\mathbf{p}) = g(\mathbf{p})\cdot(x-y)(\mathbf{p}) = g(\mathbf{p})\cdot 0 = 0$. This means that $h \in \mathbf{I}(\mathbf{V}(x-y))$.

($\subset$): By taking a suitable linear combination of the monomial expressions $x^a y^b = (y + [x-y])^a y^b = y^{a+b} + g(x,y)[x-y]$ we get immediately that any $h(x,y) \in k[x,y]$ can be written in the form $h(x,y) = A(y) + B(x,y)[x-y]$, where $A(y) \in k[y]$ and $B(x,y) \in k[x,y]$. If $h \in \mathbf{I}(\mathbf{V}(x-y))$, h must vanish on all of the points of the form $\mathbf{p} = (t,t)$. But then substituting this in the above expression for h gives $0 = h(\mathbf{p}) = A(t) + B(t,t)(t-t)$ or $A(t) = 0$ for all $t \in k$. If k is an infinite field the only polynomial A for which $A(k) = \{0\}$ is the zero polynomial. This means A is the zero polynomial and $h(x,y) = B(x,y)[x-y] \in \langle x-y\rangle$.

§1.4.11.

Let $V \subset \mathbb{R}^3$ be the curve parametrized by (t, t^3, t^4).

(a) Prove that V is an affine variety.

Solution. $V = \mathbf{V}(y-x^3,\, z-x^4)$. ($\subset$): Every point of the form (t, t^3, t^4) is a zero of $y-x^3$ and of $z-x^4$. ($\supset$): If $\mathbf{p} \in \mathbf{V}(y-x^3,\, z-x^4)$, then $\mathbf{p} = (p_1, p_2, p_3)$, where $0 = (y-x^3)(\mathbf{p}) = p_2 - p_1^3$ and $0 = (z-x^4)(\mathbf{p}) = p_3 - p_1^4$. That is, $\mathbf{p} = (p_1, p_1^3, p_1^4)$ has the form (t, t^3, t^4) for some choice of $t \in k$.

(b) Adapt the method used for the twisted cubic above to determine $\mathbf{I}(V)$. If $h \in k[x, y, z]$ then $h = A(x, y, z)[y-x^3] + B(x, y, z)[z-x^4] + F(x)$ for some $F(x) \in k[x]$. (The proof of this is virtually identical to that given above in the argument for theorem 1.4.9.1.) If h vanishes at $\mathbf{p} = (t, t^3, t^4)$, then $0 = F(t)$, $t \in k$. So if k is infinite F is the zero polynomial and $h \in \langle y - x^3,\, z - x^4\rangle$. Thus $\langle y - x^3,\, z - x^4\rangle \subset \mathbf{I}(V)$. The other inclusion is trivial. So $\langle y - x^3,\, z - x^4\rangle = \mathbf{I}(V)$.

---

§1.4.12.

Let $V \subset \mathbb{R}^3$ be the curve parametrized by (t^2, t^3, t^4).

(a) Prove that V is an affine variety.

Solution. We will show that $V = \mathbf{V}(z - x^2,\, y^2 - xz)$. ($\subset$): If $\mathbf{p} = (t^2, t^3, t^4)$, then $(z - x^2)(\mathbf{p}) = 0$ and $(y^2 - xz)(\mathbf{p}) = 0$; so $\mathbf{p} \in \mathbf{V}(z - x^2,\, y^2 - xz)$.

($\supset$): Suppose $\mathbf{p} = (p_1, p_2, p_3) \in \mathbf{V}(z - x^2,\, y^2 - xz)$. Then $p_3 = p_1^2$ and $p_2^2 = p_1 p_3 = p_1^3$. Since we are working over the field $\mathbb{R}$ of real numbers, $p_2 = \operatorname{sign}(p_2)\sqrt{p_1^3}$. Now $p_1^3 \geq 0$; so $p_1 \geq 0$ and there is a (unique) $u = \operatorname{sign}(p_2) \cdot p_1^{\frac{1}{2}}$. It is easy to check that $u^2 = p_1$, $u^3 = \operatorname{sign}(p_2) p_1^{\frac{3}{2}} = p_2$, and $u^4 = p_1^2 = p_3$. Thus $\mathbf{p} = (u^2, u^3, u^4) \in V$.

(b) Determine $\mathbf{I}(V)$. We will show that $\mathbf{I}(V) = \langle z - x^2,\, y^2 - xz\rangle$.

($\supset$): It is clear that every polynomial of the form $A(x, y, z)(z - x^2) + B(x, y, z)(y^2 - xz)$ vanishes on V and so is in $\mathbf{I}(V)$.

($\subset$): Using the fact that $y^2 \in xz + \langle z - x^2,\, y^2 - xz\rangle$ and $z \in x^2 + \langle z - x^2,\, y^2 - xz\rangle$ we can deduce in the standard manner that any polynomial $h(x, y, z) \in yh_1(x) + h_2(x) + \langle z - x^2,\, y^2 - xz\rangle$ for a suitable choice of h_1, $h_2 \in k[x]$. If $h \in \mathbf{I}(V)$; so $h(\mathbf{p}) = 0$ for each $\mathbf{p} = (t^2, t^3, t^4)$, then substituting these values in h gives $0 = t^3 h_1(t^2) + h_2(t^2)$ for every $t \in k$. If k is an infinite field, $(t^3 h_1(t) + h_2(t)$ must be the zero polynomial. This means that $t^3 h_1(t^2) \equiv 0$ because these are just the terms of $(t^3 h_1(t) + h_2(t)$ involving odd powers of t. Similarly, $h_2(t) \equiv 0$. This shows that for such an h we have $h \in \langle z - x^2,\, y^2 - xz\rangle$ showing $\mathbf{I}(V) \subset \langle z - x^2,\, y^2 - xz\rangle$. The other inclusion is trivial and completes the argument.

---

§1.4.13.

In Exercise 1.1.2 it was shown that $x^2y + y^2x$ vanishes at all points of $\mathbb{Z}_2 \times \mathbb{Z}_2$. More generally, let $I \subset Z_2[x, y]$ be the ideal of all polynomials that vanish at all points of $\mathbb{Z}_2 \times \mathbb{Z}_2$. The goal of this exercise is to show that $I = \langle x^2 - x,\, y^2 - y\rangle$.

(a) Show that $\langle x^2 - x,\, y^2 - y\rangle \subset I$. **Solution.** This is simply a matter of substituting the coordinates of the four points in $\mathbb{Z}_2 \times \mathbb{Z}_2$ in these generating polynomials. Since $x^2 - x$ and $y^2 - y$ vanish on $\mathbb{Z}_2 \times \mathbb{Z}_2$ we have $\langle x^2 - x,\, y^2 - y\rangle \subset I$.

(b) Show that every $f \in \mathbb{Z}_2[x, y]$ can be written in the form $f = A[x^2 - x] + B[y^2 - y] + axy + bx + cy + d$, where $A, B \in \mathbb{Z}_2[x, y]$ and $a, b, c, d \in \mathbb{Z}_2$.

Proof. This is a direct consequence of the fact that powers of x and y greater than one can always be reduced modulo $\langle x^2 - x,\, y^2 - y\rangle$, since

$$x^{2k} = (x + [x^2 - x])^k = x^k \mod \langle x^2 - x,\, y^2 - y\rangle,$$
$$y^{2m} = (y + [y^2 - y])^m = y^m \mod \langle x^2 - x,\, y^2 - y\rangle.$$

For example, modulo $\langle x^2 - x,\, y^2 - y\rangle$ we have $x^7 y^5 = x^6 \cdot x \cdot y^4 \cdot y = x^3 \cdot x \cdot y^2 \cdot y = x^2 \cdot y^2 = xy$.

(c) Show that $axy + bx + cy + d \in I$ if and only if $a = b = c = d = 0$.

Solution. Suppose $(axy + bx + cy + d)(\mathbf{p}) = 0$ for $\mathbf{p} \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Using $\mathbf{p} = (0, 0)$ gives $d = 0$. Building on this, using $\mathbf{p} = (1, 0)$ gives $b = 0$. Then using $\mathbf{p} = (0, 1)$ gives $c = 0$. Finally, the choice $\mathbf{p} = (1, 1)$ yields $a = 0$. The converse is trivial.

(d) Complete the proof that $I = \langle x^2 - x,\, y^2 - y\rangle$.

Solution. ($\subset$): If h vanishes on $\mathbb{Z}_2 \times \mathbb{Z}_2$ then (b) and (c) show that $h \in \langle x^2 - x,\, y^2 - y\rangle$. ($\supset$): Each $f \in \langle x^2 - x,\, y^2 - y\rangle$ vanishes on $\mathbf{Z}_2 \times \mathbb{Z}_2$ according to (a).

(e) Express $x^2y + y^2x$ as an element of $\langle x^2 - x,\, y^2 - y\rangle$.

Solution. $x^2y + y^2x = y(x^2 - x) + xy + x(y^2 - y) + xy = y(x^2 - x) + x(y^2 - y)$ since $xy + xy = 2xy = 0$ because $2 = 0$ in $\mathbb{Z}_2$.

---

§1.4.14.

This exercise was to prove Proposition 1.4.8. Since we have already done this in the exposition before these exercises we consider it done.

---

§1.4.15.

Define

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] \colon f(a_1, \ldots, a_n) = 0 \text{ for each } (a_1, \ldots, a_n) \in S\}.$$

(a) Prove $\mathbf{I}(S)$ is an ideal.

Solution. This is straightforward and left as an observation.

(b) Let $X = \{(a, a) \in \mathbb{R}^2 \colon a \neq 1\}$. By Exercise 1.2.8 we know that X is not an affine variety. Determine $\mathbf{I}(X)$.

Solution. According to Exercise 1.4.10, any polynomial $h \in k[x, y]$ can be written in the form $h(x, y) = A(y) + B(x, y)[x - y]$ where $A(y) \in k[y]$ and $B(x, y) \in k[x, y]$. If a polynomial $h(x, y) \in \mathbf{I}(X)$ then $h(\mathbf{p}) = 0$ for any $\mathbf{p} = (a, a)$ with $a \neq 1$. This means that $A(a) = 0$ for any $0 \neq a \in \mathbf{R}$. But then $A(y)$ is the zero polynomial. It follows that such an $h(x, y) \in \langle x - y\rangle$. So $\mathbf{I}(X) \subset \langle x - y\rangle$. The other inclusion is trivial. This gives $\mathbf{I}(X) \subset \langle x - y\rangle$.

(c) Let $\mathbb{Z}^n$ be the points of $\mathbb{C}^n$ with integer coordinates. Determine $\mathbf{I}(\mathbb{Z}^n)$.

Solution. Exercise 1.1.6 shows that if $f(\mathbb{Z}^n) = 0$, then f is the zero polynomial; so $\mathbf{I}(\mathbb{Z}^n) = \{0\}$, the zero ideal of $\mathbb{R}[x_1, \ldots, x_n]$.