Solutions to Algebraic Curves - An Introduction to Algebraic Geometry - William Fulton

Samy Lahlou

January 11, 2026

Preface

The goal of this document is to share my personal solutions to the exercises in the book Algebraic Curves - An Introduction to Algebraic Geometry by William Fulton during my reading.
As a disclaimer, the solutions are not unique and there will probably be better or more optimized solutions than mine. Feel free to correct me or ask me anything about the content of this document at the following address :
samy.lahloukamal@mcgill.ca

Contents

Chapter 1

Affine Algebraic Sets

1.1 Algebraic Preliminaries

1.1. Let R be a domain. (a) If F, G are forms of degree r, s respectively in $R[X_1, ..., X_n]$, show that FG is a form of degree $r + s$. (b) Show that any factor of a form in $R[X_1, ..., X_n]$ is also a form.

Solution

(a) The form F is a sum of monomials of degree r and G is a sum of monomials of degree s. Hence, using the definition of the product of two polynomials, the polynomial FG is a sum of products ab where a is a monomial of degree r and b is a monomial of degree s. Hence, ab is a monomial of degree $r + s$ so FG is a sum of monomials of degree $r + s$. Therefore, equivalently, FG is a form of degree $r + s$.

(b) Let f be a divisor of a form F of degree N, then $F = fg$ for some polynomial g. Suppose that f is not a form, then we can write $f = f_a + f_{a+1} + \cdots + f_b$ where f_i is a form of degree i, $a < b$, and $f_a, f_b \neq 0$. Similarly, we can write $g = g_c + g_{c+1} + \cdots + g_d$ where g_i is a form of degree i, $c \leq d$, and $g_c, g_d \neq 0$. It follows that

$$F = fg = f_a g_c + [f_a g_{c+1} + f_{a+1} g_c] + \cdots + f_b g_d$$

is the decomposition of F into a sum of forms. However, $f_a g_c \neq 0$ is a form of degree $a + c$ and $f_b g_d \neq 0$ is a form of degree $b + d > a + c$. But this impossible because F is already a form so it cannot be decomposed into nonzero forms of different degree.

1.2. Let R be a UFD, K the quotient field of R. Show that every element z of K may be written $z = a/b$, where $a, b \in R$ have no common factors; this representative is unique up to units of R.

Solution Let $z \in K$ and write it as a/b with $a, b \in R$. Since R is a UFD, then we can define $d = \gcd(a, b)$, $a = a'd$ and $b = b'd$. Since d is the greatest common divisor of a and b, then a' and b' have no common divisor. Hence, $z = a/b = a'/b'$ where the numerator and the denominator have no common divisor. Next, we need

to show that this representation of z is unique up to multiplication by units. If c/d is another representation of z as a quotient of two elements in R with $\gcd(c,d) = 1$, then $a'/b' = c/d$. From this equation, we get that $a'd = b'c$. Hence, a' divides $b'c$, but $\gcd(a,b) = 1$ so a' divides c. Similarly, c divides $a'd$ but $\gcd(c,d) = 1$ so c divides a'. Thus, $c' = ua'$ where u is a unit. If we plug this into the equation $a'd = b'c$, we get that $a'd = b'ua'$, and hence, $d = ub'$. Therefore, c and d are equal to a and b, up to multiplication by a unit.

1.3. Let R be a PID, let P be a nonzero, proper, prime ideal in R. (a) Show that P is generated by an irreducible element. (b) Show that P is maximal.

Solution

(a) Since R is a PID, then $P = (p)$ where $p \in R$. Since P is nonzero, and proper, then p is not zero, nor a unit. Suppose that p is reducible, then there exist two non-units and nonzero elements $a, b \in R$ such that $p = ab$. Since P is prime, then $ab = p \in (p)$ implies that $a \in (p)$ or $b \in (p)$. If $a \in (p)$, p divides a. Since a divides p, then $ab = p = au$ where u is a unit, so $b = u$, a contradiction. Therefore, p is irreducible.

(b) Let $I = (f)$ be an ideal containing P, then $p \in (f)$ which implies that f divides p. But the only divisors of p are units and unit multiples of p. In the first case, $I = R$, in the second case, $I = P$. Therefore, P is maximal.

1.4. Let k be an infinite field, $F \in k[X_1, ..., X_n]$. Suppose $F(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Show that $F = 0$. (*Hint:* Write $F = \sum F_i X_n^i$, $F_i \in k[X_1, ..., X_{n-1}]$. Use induction on n, and the fact that $F(a_1, ..., a_{n-1}, X_n)$ has only a finite number of roots if any $F_i(a_1, ..., a_{n-1}) \neq 0$.)

Solution Let's prove this by induction on n. When F is a polynomial in $k[X]$ such that $F(a) = 0$ for all $a \in k$, then $F = 0$ because F has at most finitely many roots when it is nonzero. Next, suppose that $G \in k[X_1, ..., X_{n-1}]$ with $G(a_1, ..., a_{n-1}) = 0$ for all $(a_1, ..., a_{n-1}) \in k^{n-1}$ implies that $G = 0$, and consider a polynomial $F \in k[X_1, ..., X_n]$ with $F(a_1, ..., a_n) = 0$ for all $(a_1, ..., a_n) \in k^n$. If we view F as an elements of $k[X_1, ..., X_{n-1}][X_n]$, then we can write $F = \sum_i F_i X_n^i$ where $F_i \in k[X_1, ..., X_{n-1}]$. Fix $(a_1, ..., a_{n-1}) \in k^{n-1}$ and consider the polynomial $f(X) = F(a_1, ..., a_{n-1}, X) = \sum_i F_i(a_1, ..., a_{n-1}) X^i$, then $f(a_n) = 0$ for all a. By the case $n = 1$, we have that $f = 0$, and hence, that $\sum_i F_i(a_1, ..., a_{n-1}) X^i = 0$. By properties of polynomials, it follows that $F_i(a_1, ..., a_{n-1}) = 0$ for all i. Since it holds for all $(a_1, ..., a_{n-1}) \in k^{n-1}$, then by induction, $F_i = 0$ for all i. Hence, $F = \sum_i F_i X_n^i = 0$. Therefore, by induction, it holds for all n.

1.5. Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[X]$. (*Hint:* Suppose $F_1, ..., F_n$ were all of them, and factor $F_1 \cdots F_n + 1$ into irreducible factors.)

Solution Suppose that there are finitely many irreducible monic polynomials $F_1, ..., F_n$. Define the polynomial $F = F_1 \cdots F_n + 1$, then this polynomial must

be divisible by F_i for some i. However, F_i certainly divides $F_1 \cdots F_n$ so F_i must divide $F - F_1 \cdots F_n = 1$. But this is a contradiction since the only monic polynomial dividing 1 is 1, which is not irreducible since it is a unit. Therefore, by contradiction, there are infinitely many irreducible polynomials.

1.6. Show that any algebraically closed field is infinite. (*Hint:* The irreducible monic polynomials are $X - a$, $a \in k$.)

Solution Clearly, every polynomial of the form $X - a$ with $a \in k$ is irreducible. Moreover, since k is algebraically closed, then every polynomial can be factored into a product of linear factors so the irreducible polynomials are precisely the polyomials of the form $X - a$ with $a \in k$. It is easy to see then that there are as many irreducible polynomials as elements in k. In the previous Problem, it is shown that there are always infinitely many irreducible polynomials. Therefore, k is infinite.

1.7. Let k be a field, $F \in k[X_1, ..., X_n]$, $a_1, ..., a_n \in k$. (a) Show that

$$F = \sum \lambda_{(i)}(X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}, \quad \lambda_{(i)} \in k.$$

(b) If $F(a_1, ..., a_n) = 0$, show that $F = \sum_{i=1}^{n}(X_i - a_i)G_i$ for some (not unique) G_i in $k[X_1, ..., X_n]$.

Solution

(a) Notice that $F = F(X_1 + a_1 - a_1, ..., X_n + a_n - a_n)$. Hence, if we let $G = F(X_1 + a_1, ..., X_n + a_n) \in k[X_1, ..., X_n]$, then we can write

$$G = \sum \lambda_{(i)} X_1^{i_1} \cdots X_n^{i_n},$$

then

$$F = G(X_1 - a_1, ..., X_n - a_n) = \sum \lambda_{(i)}(X_1 - a_1)^{i_1} \cdots (X_n - a_n)^{i_n}$$

for some $\lambda_{(i)} \in k$.

(b) If $F(a_1, ..., a_n) = 0$, then $G(0, ..., 0) = 0$, so G has no constant term. Let's prove that G can be written as $\sum X_i H_i$ where $H_i \in k[X_1, ..., X_n]$. We can write G as $X_1 H_1 + H_1'$ where none of the monomials in H_1' contain a factor of X_1. Next, write H_1' as $X_2 H_2 + H_2'$ where none of the monomials in H_2' contain a factor of X_1 or X_2. If we repeat this process, we get that $G = \sum X_i H_i$. It follows that

$$F = \sum (X_i - a_i) H_i(X_1 - a_1, ..., X_n - a_n).$$

1.2 Affine Space and Algebraic Sets

1.8. Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets, together with $\mathbb{A}^1(k)$ itself.

Solution Let S be an arbitrary set polynomials in $k[x]$. If S is empty or $S = \{0\}$, then $V(S) = \mathbb{A}^1(k)$. If S contains a nonzero polynomial F, then $V(S) \subset V(F)$.

Since F is a one-variable polynomial, then it has finitely many roots, and so $V(F)$ is finite. It follows that $V(S)$ is a finite subset of $\mathbb{A}^1(k)$. Conversely, we know that any finite subsets are algebraic sets. Therefore, the algebraic subsets of $\mathbb{A}^1(k)$ are precisely the finite subsets and $\mathbb{A}^1(k)$ itself.

1.9. If k is a finite field, show that every subset of $\mathbb{A}^1(k)$ is algebraic.

Solution Let U be a subset of $\mathbb{A}^n(k)$, then U us finite and so it must be algebraic by property n°5 of the section.

1.10. Give an example of a countable collection of algebraic sets whose union is not algebraic.

Solution If we let $k = \mathbb{R}$, and $V_i = \{i\}$ for all $i \in \mathbb{Z}$, then all the V_i's are algebraic subsets of $A^1(k)$ but their union is not since it would contradict Problem 1.8.

1.11. Show that the following are algebraic sets:

(a) $\{(t, t^2, t^3) \in \mathbb{A}^3(k) | t \in k\}$;

(b) $\{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) | t \in \mathbb{R}\}$;

(c) the set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = \sin(\theta)$.

Solution

(a) Let $U = \{(t, t^2, t^3) \in \mathbb{A}^3(k) | t \in k\}$ and $V = V(x^3 - z, x^2 - y)$. Let $(x, y, z) \in U$, then there is a $t \in k$ such that $x = t$, $y = t^2$, and $z = t^3$. It follows that $x^3 - z = 0$ and $x^2 - y = 0$. Hence, $(x, y, z) \in V$. Conversely, if $(x, y, z) \in V$, and if we let $t = x$, then $y = x^2 = t^2$ and $z = x^3 = t^3$. Hence, $(x, y, z) \in U$. Therefore, $U = V$ and so U is algebraic.

(b) Since the set $U = \{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) | t \in \mathbb{R}\}$ is simply the unit circle in $\mathbb{R}^2$, then we know that we can rewrite it as $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | x^2 + y^2 = 1\}$, or simply as $V(x^2 + y^2 - 1)$. Thus, it is an algebraic set.

(c) Using the fact that $r = \sqrt{x^2 + y^2}$ and $\sin(\theta) = y/\sqrt{x^2 + y^2}$, we get that the set $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | r = \sin(\theta)\}$ is equal to

$$\{(x, y) \in \mathbb{A}^2(\mathbb{R}) | \sqrt{x^2 + y^2} = y/\sqrt{x^2 + y^2}\}.$$

Equivalently, we can rewrite it as $V(x^2 + y^2 - y)$. Hence, it is an algebraic set.

1.12. Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^2(k)$, $L \not\subset C$. Suppose $C = V(F)$, $F \in k[X, Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points. (*Hint:* Suppose $L = V(Y - (aX + b))$, and consider $F(X, aX + b) \in k[X]$.)

Solution Let $F \in k[X, Y]$ be a polynomial of degree n and suppose that $C = V(F)$. Since L is a line, then we can write $L = V(G)$ with $G = aX + bY + c$ for some

$a, b, c \in k$ where a and b cannot be both zero. Suppose without loss of generality that b is non-zero, then $(X, Y) \in L$ if and only if $Y = -\frac{a}{b}X - \frac{c}{b}$. Consider now the polynomial $F(X, -\frac{a}{b}X - \frac{c}{b}) \in k[X]$, then this is a polynomial of degree n. Let X be one of its roots, then $(X, -\frac{a}{b}X - \frac{c}{b}) \in L \cap C$. Conversely, if $(X, Y) \in L \cap C$, then $Y = -\frac{a}{b}X - \frac{c}{b}$ which implies that $F(X, Y) = 0$ and so X is a root of $F(X, -\frac{a}{b}X - \frac{c}{b})$. Therefore, the roots of X are in bijection with the elements in $L \cap C$. Since $F(X, -\frac{a}{b}X - \frac{c}{b})$ is a polynomial of degree n, then it has at most n roots, and hence, $L \cap C$ is a finite set of no more than n points.

1.13. Show that each of the following sets is not algebraic:

(a) $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin(x)\}$.

(b) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$, where $|x + iy|^2 = x^2 + y^2$ for $x, y \in \mathbb{R}$.

(c) $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) | t \in \mathbb{R}\}$;

Solution

(a) Suppose that $\{y = \sin(x)\} = V(S)$ for some $S \subset k[X, Y]$. Since $\{y = \sin(x)\} \neq \mathbb{A}^2(\mathbb{R})$, then S must contain a nonzero polynomial $F \in k[X, Y]$, of degree n. Since $F \in S$, then $F(x, \sin(x)) = 0$ for all $x \in \mathbb{R}$. Consider now the polynomial $F(0, X) \in k[X]$, then this polynomial must have at most n roots. However, there are infinitely many $x \in \mathbb{R}$ such that $\sin(x) = 0$ since F has infinitely many roots. Therefore, by contradiction, the set $\{y = \sin(x)\}$ is not algebraic.

(b) Suppose that $\{|z|^2 + |w|^2 = 1\} = V(S)$, since $\{|z|^2 + |w|^2 = 1\} \neq \mathbb{A}^2(\mathbb{C})$, then there must be a nonzero polynomial $F \in k[X, Y]$ such that $F(z, w) = 0$ for all $z, w \in \mathbb{C}$ such that $|z|^2 + |w|^2 = 1$. Let $C = V(F)$, and let $L = V(X)$ be a line. We know that $L \not\subset C$ since $(0, 2) \in L$ but $(0, 2) \notin C$. Hence, by Problem 1.12, $L \cap C$ is finite. However, for every complex number w with $|w| = 1$, we have that $(0, w) \in L \cap C$. Since there are infinitely many such complex numbers w, then $L \cap C$ is infinite, a contradiction. Therefore, $\{|z|^2 + |w|^2 = 1\}$ is not an algebraic set.

(c) Suppose that $\{(\cos(t), \sin(t), t)\}_{t \in \mathbb{R}} = V(S)$ for some $S \subset k[X, Y, Z]$. Since $\{(\cos(t), \sin(t), t)\}_{t \in \mathbb{R}} \neq \mathbb{A}^3(\mathbb{R})$, then S must contain a nonzero polynomial $F \in k[X, Y, Z]$, of degree n. Since $F \in S$, then $F(\cos(t), \sin(t), t) = 0$ for all $t \in \mathbb{R}$. Consider now the polynomial $F(1, 0, X) \in k[X]$, then this polynomial must have at most n roots. However, there are infinitely many $t \in \mathbb{R}$ such that $\cos(x) = 1$, $\sin(x) = 0$, and hence, $F(1, 0, x) = F(\cos(x), \sin(x), x) = 0$, so F has infinitely many roots. Therefore, by contradiction, the set is not algebraic.

1.14. Let F be a nonconstant polynomial in $k[X_1, \ldots, X_n]$, k is algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 1$, and $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite. (*Hint:* See Problem 1.4.)

Solution First, notice that k must be infinite since it is algebraically closed. Hence, the case $n = 1$ follows from Problem 1.8. For the case $n = 2$, suppose that there are

finitely many (x, y) such that $F(x, y) \neq 0$. Let (x_0, y_0) be such a pair, then we get that there finitely many y such that $F(x_0, y) = 0$. But since $F(x_0, y) \in k[y]$, then we get a contradiction with the case $n = 1$. Therefore, $\mathbb{A}^n(k) \setminus V(F)$ is infinite for the case $n = 2$.

Now, let $n \geq 1$, $F \in k[X_1, ..., X_n]$, and suppose that $\mathbb{A}^n(k) \setminus V(F)$ is finite. Let $(a_1, ..., a_n) \in \mathbb{A}^n(k)$ be such that $F(a_1, ..., a_n) \neq 0$, then the polynomial $F(a_1, ..., a_{n-1}, X) \in k[X]$ is such that there are finitely many $x \in k$ such that it is nonzero. But this is in contradiction with the case $n = 1$. Thus, by contradiction, the set $\mathbb{A}^n(k) \setminus V(F)$ is infinite.

1.15. Let $V \subset \mathbb{A}^n(k)$, $W \subset \mathbb{A}^m(k)$ be algebraic sets. Show that

$$V \times W = \{(a_1, ..., a_n, b_1, ..., b_m) \mid (a_1, ..., a_n) \in V, (b_1, ..., b_m) \in W\}$$

is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the *product* of V and W.

Solution For all $F \in V$ and $G \in W$, define $F^\times, G^\times \in k[X_1, ..., X_{n+m}]$ by

$$F^\times(X_1, ..., X_{n+m}) = F(X_1, ..., X_n) \text{ and } G^\times(X_1, ..., X_{n+m}) = G(X_{n+1}, ..., X_{n+m}).$$

If we consider the set $V(\{F^\times\}_{F \in V})$, we get that it is equal to the elements in $\mathbb{A}^{n+m}(k)$ where the first n entries are in V. Similarly, $V(\{G^\times\}_{G \in W})$ is equal to the elements in $\mathbb{A}^{n+m}(k)$ where the last m entries are in V. It follows that $V(\{F^\times\}_{F \in V} \cup \{G^\times\}_{G \in W}) = V \times W$. Therefore, $V \times W$ is an algebraic set.

1.3 The Ideal of a Set of Points

1.16. Let V, W be algebraic sets in $\mathbb{A}^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.

Solution If $V = W$, then $I(V) = I(W)$ trivially. Now, if $I(V) = I(W)$, then $V(I(V)) = V(I(W))$. Since V and W are algebraic sets, then $V(I(V)) = V$ and $V(I(W)) = W$. Hence, $V = W$.

1.17. (a) Let V be an algebraic set in $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ a point not in V. Show that there is a polynomial $F \in k[X_1, ..., X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$. (*Hint:* $I(V) \neq I(V \cup \{P\})$.) (b) Let $P_1, ..., P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, ..., F_r \in I(V)$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$. (*Hint:* Apply (a) to the union of V and all but one point.) (c) With $P_1, ..., P_r$ and V as in (b), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$ for all i and j. (*Hint:* Consider $\sum_j a_{ij} F_j$.)

Solution

(a) Since $P \notin V$, then $V \neq V \cup \{P\}$ and so $I(V) \neq I(V \cup \{P\})$ by Problem 1.16. Since $V \subset V \cup \{P\}$, then $I(V \cup \{P\}) \subset I(V)$ and so it must be that $I(V) \not\subset I(V \cup \{P\})$. This implies that there is a $F_0 \in I(V) \subset k[X_1, ..., X_n]$ such that $F_0 \notin I(V \cup \{P\})$. In other words, there is polynomial $F_0 \in k[X_1, ..., X_n]$ such that $F_0(Q) = 0$ for all $Q \in V$ and $F_0(P) \neq 0$. Define $F(x) = F_0(P)^{-1} F_0(x)$ for all $x \in \mathbb{A}^n(k)$, then $F(Q) = 0$ for all $Q \in V$ and $F(P) = 1$.

(b) Let $i \in [\![1, r]\!]$, since $V \cup \{P_j\}_{j \neq i}$ is an algebraic set that doesn't contain P_i, then by part (a) there is a function $F_i \in I(V)$ such that $F_i(P_j) = 0$ whenever $j \neq i$ and $F_i(P_i) = 1$.

(c) Since the set up is the same as in (b), then we already showed that, for all $i \in [\![1, r]\!]$, there exists a polynomial $F_i \in I(V)$ such that $F_i(P_j) = 0$ for all $j[\![1, r]\!] \setminus \{i\}$ and $F_i(P_i) = 1$. For all $i \in [\![1, r]\!]$, define $G_i = \sum_{k=1}^{r} a_{ik} F_k$. Since the F_i's are all in the ideal $I(V)$, then $G_i \in I(V)$. Moreover, for all $j \in [\![1, r]\!]$, we have that $G_i(P_j) = \sum_{k=1}^{r} a_{ik} F_k(P_j) = a_{ij}$.

1.18. Let I be an ideal in a ring R. If $a^n \in I$, $b^m \in I$, show that $(a+b)^{n+m} \in I$. Show that $\mathrm{Rad}(I)$ is an ideal. Show that any prime ideal is radical.

Solution By the Binomial Formula, we have that

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

When $k \in [\![0, n-1]\!]$, we have that the term of index k is in I because it can be written as $\binom{n+m}{k} a^k b^{n-k} \cdot b^m$ and b^m is in I. Similarly, if $k \in [\![n, n+m]\!]$, the term of index k can be written as $\binom{n+m}{k} a^{k-n} b^{n+m-k} \cdot a^n$, and $a^n \in I$, so it is also in I. All the terms in the sum above are in I so $(a+b)^{n+m}$ must be in I.

Since $\mathrm{Rad}(I) \supset I$ and $0 \in I$, then $0 \in \mathrm{Rad}(I)$. If $a, b \in \mathrm{Rad}(I)$, then there exist positive integers n and m such that $a^n, b^m \in I$. By the previous part, $(a+b)^{n+m} \in I$ which implies that $a + b \in \mathrm{Rad}(I)$. Thus, $\mathrm{Rad}(I)$ is closed under addition. Finally, if $a \in \mathrm{Rad}(I)$ and $r \in R$, then there is a positive integer n such that $a^n \in I$. Since $(ra)^n = r^n a^n \in I$, then $ra \in \mathrm{Rad}(I)$. Therefore, $\mathrm{Rad}(I)$ is an ideal.

Let I be a prime ideal, to prove that I is radical, it suffices to prove that $\mathrm{Rad}(I) \subset I$. Let $i \in \mathrm{Rad}(I)$, then $i^n \in I$ where $n \geq 1$ is the smallest positive integer for which $i^n \in I$. If $n = 1$, we are done. Suppose that $n > 1$, then we have that $i \cdot i^{n-1} \in I$. Since I is prime, then either i or i^{n-1} is in I. Since n is minimal, then both cases are impossible. Therefore, $\mathrm{Rad}(I) = I$ and so I is radical.

1.19. Show that $I = (X^2 + 1) \subset \mathbb{R}[X]$ is a radical (even a prime) ideal, but I is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.

Solution Suppose that $p^n \in (X^2+1)$, then $X^1 + 2 \mid p^n$. Since X^2+1 is irreducible in $\mathbb{R}[X]$, then $X^2 + 1 \mid p$ which implies that $p \in (X^2 + 1)$. Therefore, $(X^2 + 1)$ is radical. Suppose that $(X^2 + 1) = I(X)$ for some $X \subset \mathbb{A}^1(\mathbb{R})$. If $X = \varnothing$, then $(X^2 + 1) = I(\varnothing) = \mathbb{R}[X]$ which is false since $X \notin (X^2 + 1)$. Hence, there is a $x \in \mathbb{A}^1(\mathbb{R})$ such that $x \in X$. Since $X^2 + 1 \in I(X)$, then $x^2 + 1 = (X^2 + 1)(x) = 0$ which is impossible since $X^2 + 1$ has no roots in $\mathbb{R}$. Therefore, $(X^2 + 1)$ is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$.

1.20. Show that for any ideal I in $k[X_1, ..., X_n]$, $V(I) = V(\mathrm{Rad}(I))$, and $\mathrm{Rad}(I) \subset I(V(I))$.

Solution Since $I \subset \text{Rad}(I)$, then $V(\text{Rad}(I)) \subset V(I)$. Conversely, let $P \in V(I)$ and $F \in \text{Rad}(I)$, then $F^n \in I$ for some $n \geq 1$. It follows that $F^n(P) = 0$ and so $F(P)$. Thus, $P \in V(\text{Rad}(I))$. Therefore, $V(I) = V(\text{Rad}(I))$.

Now, from the fact that $S \subset I(V(S))$ for all subsets S of $k[X_1, ..., X_n]$, if we take $S = \text{Rad}(I)$, then $\text{Rad}(I) \subset I(V(\text{Rad}(I))) = I(V(I))$ by the first part of the exercise.

1.21. Show that $I = (X_1 - a_1, ..., X_n - a_n) \subset k[X_1, ..., X_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[X_1, ..., X_n]/I$ is an isomorphism.

Solution Let J be an ideal properly containing I, and let $F \in J \setminus I$. Write F as

$$F(X_1, ..., X_n) = F_k(X_1, ..., X_{n-1})X_n^k + \cdots + F_0(X_1, ..., X_{n-1}).$$

Since $F \in J$ and $F_k(X_1, ..., X_{n-1})(X_n - a_n)^k \in I \subset J$, then $F - F_k(X_1, ..., X_{n-1})(X_n - a_n)^k \in J$ where the resulting polynomial is now a polynomial in $k[X_1, ..., X_{n-1}][X_n]$ of degree $k-1$. By repeating this process, we can obtain a polynomial $G \in J$ which is a polynomial in $k[X_1, ..., X_{n-1}]$. Again, if we repeat the same procedure, we get a constant polynomial $H \in J$. This constant polynomial is nonzero because otherwise, we would get that F is the sum of all the polynomials in I that we subtracted and so F would be in I. Thus, $H \in J$ is a nonzero constant so $1 \in J$. It follows that $J = k[X_1, ..., X_n]$. Therefore, I is maximal.

Consider the natural homomorphism $\varphi : k \to k[X_1, ..., X_n]/I$ that maps each scalar to equivalence class of its respective constant polynomial. This is a well defined homomorphism because it is equal to the natural homomorphism from k to $k[X_1, ..., X_n]$ composed with the projection homomorphism from $k[X_1, ..., X_n]$ to $k[X_1, ..., X_n]/I$. This homomorphism is injective because it is a field homomorphism. This homomorphism is injective because in the first part of this exercice, we showed that every polynomial in $k[X_1, ..., X_n]$ is equivalent to a constant polynomial. Therefore, φ is an isomorphism.

1.4 The Hilbert Basis Theorem

1.22. Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism. (a) Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containg I, and for every ideal J of R containg I, $\pi(J) = J'$ is an ideal of R/I. This sets up a natural one-to-one correspondence between {ideals of R/I} and {ideals of R that contain I}. (b) Show that J' is a radical ideal if and only if J is radical. Similarly for prime and maximal ideals. (c) Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[X_1, ..., X_n]/I$ is Noetherian.

Solution

(a) Let J' be an ideal of R/I and consider the set $J = \pi^{-1}(J')$. Since $\pi(0) = I = 0 \in J'$, then $0 \in \pi^{-1}(J') = J$. Let $a, b \in J$, then $\pi(a), \pi(b) \in J'$ which implies that $\pi(a + b) = \pi(a) + \pi(b) \in J'$. It follows that $a + b \in J$. Similarly, if $a \in J$ and $r \in R$, then $\pi(a) \in J'$ which implies that $\pi(ra) = \pi(r)\pi(a) \in J'$. Hence, $ra \in J$. Thus, J is an ideal of R. Finally, for all $i \in I$, we have that $\pi(i) = 0 \in J'$ so $i \in J$. Therefore, J is an ideal of R containing I.

Next, let J be an ideal of R that contains I, and define $J' = \pi(J)$. Since $0 \in J$ and $\pi(0) = 0$, then $0 \in J'$. Let $\pi(a), \pi(b) \in J'$, then $\pi(a)+\pi(b) = \pi(a+b) \in J'$ since $a + b \in J$. If $\pi(r) \in R/I$ and $\pi(a) \in J'$, then $\pi(r)\pi(a) = \pi(ra) \in J'$ since $ra \in J$. Therefore, J' is an ideal of R/I.

(b) Suppose that J' is radical and let $j^n \in J$, then $\pi(j)^n = \pi(j^n) \in J'$. Since J' is radical, then $\pi(j) \in J' = \pi(J)$ which implies that $j \in \pi^{-1}(\pi(J))$. Therefore, J is radical. Conversely, suppose that J is radical and let $\pi(j)^n \in J'$, then $\pi(j^n) \in J' = \pi(J)$. It follows that $j^n \in J$ which implies that $j \in J$. Thus, $\pi(j) \in J'$. Therefore, J' is radical.

Suppose that J' is prime and let $ab \in J$, then $\pi(a)\pi(b) = \pi(ab) \in J'$. By the primality of J', either $\pi(a)$ or $\pi(b)$ is in J'. Without loss of generality, if $\pi(a) \in J'$ then $a \in J$. It follows that J is prime. Conversely, if J is prime and $\pi(ab) = \pi(a)\pi(b) \in J'$, then $ab \in J$ which implies that $a \in J$ (wlog). It follows that $\pi(a) \in J'$. Therefore, J is prime.

Suppose that J' is maximal and let M be an ideal properly containing J, then its image $M' = \pi(M)$ is an ideal that contains J'. Let $m \in M \setminus J$, then $\pi(m) \in M' \setminus J'$ because if $\pi(m) \in J'$, then $m \in J$. Hence, M' properly contains J'. Since J' is maximal, then $M' = R/I$. By the bijection between the ideal classes, we must have $M = R$. Therefore, J is a maximal ideal. Conversely, suppose that J is maximal and let M' be an ideal that properly contains J'. Let $M = \pi^{-1}(M')$, then M is an ideal that contains J. Since M' contains J' properly, there must be an $m \in M$ such that $\pi(m) \in M' \setminus J'$. From this, it must be that $m \in M \setminus J$ and so M contains J properly. Since J is maximal, then $M = R$ and so $M' = R/I$. Therefore, J' is maximal.

(c) Suppose that J is finitely generated, then we can write $J = (j_1, ..., j_n)$. Let $\pi(j) \in J'$, then

$$\pi(j) = \pi\left(\sum_k r_k j_k\right) = \sum_k \pi(r_k)\pi(j_k) \in (\pi(r_1), \ldots, \pi(r_n)).$$

It follows that $J' \subset (\pi(r_1), \ldots, \pi(r_n))$. On the other hand, since the $\pi(j_k)$'s are in J', then $(\pi(r_1), \ldots, \pi(r_n)) \subset J'$. Therefore, J' is finitely generated.

Now, suppose that R is Noetherian and let J' be an ideal of R/I, then $J' = \pi(J)$ where J is an ideal of R containing I. Since R is Noetherian, then J is finitely generated and so J' is also finitely generated. Therefore, R/I is Noetherian.

1.5 Irreducible Components of an Algebraic Set

1.23. Give an example of a collection $\mathscr{S}$ of ideals in a Noetherian ring such that no maximal member of $\mathscr{S}$ is a maximal ideal.

Solution Take the ring to be $\mathbb{Z}$ and take the collection $\mathscr{S} = \{(4)\}$ containing only one element. It is clear that (4) is a maximal element of $\mathscr{S}$ even though it is not a maximal ideal of $\mathbb{Z}$.

1.24. Show that every proper ideal in a Noetherian ring is contained in a maximal ideal. (*Hint:* If I is the ideal, apply the lemma to {proper ideals that contain I}.)

Solution Let I be a proper ideal and let $\mathscr{S}$ be the collection of proper ideals that contain I. By the lemma, $\mathscr{S}$ must contain a maximal element J that contain I. If J is not a maximal ideal, then it must be itself contained in a proper ideal of the ring. However, this new proper ideal would be in $\mathscr{S}$ and would contradict the maximality of J in $\mathscr{S}$. Therefore, J is a maximal ideal that contain I.

1.25. (a) Show that $V(Y - X^2) \subset \mathbb{A}^2(\mathbb{C})$ is irreducible; in fact, $I(V(Y - X^2)) = (Y - X^2)$. (b) Decompose $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ into irreducible components.

Solution

(a) Let's show that $I(V(Y - X^2))$ is a prime ideal. First, notice that $I(V(Y - X^2)) = (Y - X^2)$. Since $Y - X^2$ is irreducible in $\mathbb{C}[X, Y]$, then $(Y - X^2)$ is prime. Therefore, $V(Y - X^2)$ is irreducible.

(b) First, notice that $Y^4 - X^2 = (Y^2 - X)(Y^2 + X)$ and $Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 - X^2)(Y^2 + X) = (Y - X)(Y + X)(Y^2 + X)$. Let's prove that our algebraic set V is equal to $V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. First, if $(x, y) \in V$, then $y^4 = x^2$ and $(y - x)(y + x)(y^2 + x) = 0$. From the second equation, we have the following cases: if $y = x$, then either $x = y = 0$ or $y^4 = x^2$ implies that $y^2 = 1$, and hence, that $x = y = \pm 1$; if $y = -x$, then either $x = y =$ or the same considerations as before gives us that $y = \pm 1$, and hence, $x = \mp 1$, $y = \pm 1$; finally, if $y^2 = -x$, then $y^2 + x = 0$. The outcome of all of these cases show that $(x, y) \in V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. The converse is even easier to prove, if $y^2 + x = 0$, then (x, y) satisfy both polynomials describing V and so it is in V; if $x = 1$ and $y = \pm 1$, then it clearly satisfies both polynomials again and so it is in V. Therefore, $V = V(Y^2 + X) \cup \{(1, 1)\} \cup \{(1, -1)\}$. The three sets are clearly irreducible algebraic sets so we are done.

1.26. Show that $F = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ is an irreducible polynomial, but $V(F)$ is reducible.

Solution By contradiction, suppose that there exist two polynomials $p, q \in \mathbb{R}[X, Y]$ such that $y^2 + x^2(x - 1)^2 = p(x, y)q(x, y)$, then in particular, if we fix any $x \in \mathbb{R} \setminus \{0, 1\}$, we can view this equation as an equation where y is the only variable. But this would mean that the polynomial $y^2 + x^2(x - 1)^2$ is reducible in $\mathbb{R}[y]$ which is false. Therefore, the polynomial F is irreducible.

To show that $V(F)$ is reducible, notice that the only solutions to the equation $Y^2 + X^2(X - 1)^2 = 0$ are $(0, 0)$ and $(1, 0)$. Therefore, $V(F) = \{(0, 0)\} \cup \{(1, 0)\}$.

1.27. Let V, W be algebraic sets in $\mathbb{A}^n(k)$, with $V \subset W$. Show that each irreducible component of V is contained in some irreducible component of W.

Solution First, write $V = \bigcup_i V_i$ and $W = \bigcup_j W_j$ where the unions are finite. Since $V \subset W$, then for each i, we have $V_i = \bigcup_j (W_j \cap V_i)$. Since V_i is irreducible, then

we must have that $V_i = W_j \cap V_i \subset W_j$ for some j. Therefore, every irreducible component of V is contained in an irreducible component of W.

1.28. If $V = V_1 \cup \cdots \cup V_r$ is the decomposition of an algebraic set into irreducible components, show that $V_i \not\subset \bigcup_{i \neq j} V_j$.

Solution First, recall that $V_i \not\subset V_j$ for all $i \neq j$. Next, suppose that $V_i \subset \bigcup_{i \neq j} V_j$, then $V_i = \bigcup_{i \neq j}(V_j \cap V_i)$. But since V_i is irreducible, then $V_i = V_j \cap V_i \subset V_j$ for some $i \neq j$. This contradiction proves that the original claim holds.

1.29. Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite.

Solution Simply notice that when k is infinite, we have $I(\mathbb{A}^n(k)) = \{0\}$ and $\{0\}$ is a prime ideal. Therefore, $\mathbb{A}^n(k)$ is irreducible.

1.6 Algebraic Subsets of the Plane

1.30. Let $k = \mathbb{R}$. (a) Show that $I(V(X^2 + Y^2 + 1)) = (1)$. (b) Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

Solution

(a) Since $X^2 + Y^2 + 1$ has no roots in $\mathbb{A}^2(\mathbb{R})$, then

$$I(V(X^2 + Y^2 + 1)) = I(\varnothing) = \mathbb{A}^2(\mathbb{R}) = (1).$$

(b) Let V be an algebraic subset of $\mathbb{A}^2(\mathbb{R})$. If $V = \mathbb{A}^2(\mathbb{R})$, then $V = V(0)$; if $V = \varnothing$, then $V = V(1)$; if $V = \{(a, b)\}$, then we can write V as $V((X-a)^2+(Y-b)^2)$ because $(X-a)^2+(Y-b)^2 = 0$ if and only if $X = a$ and $Y = b$; if V is any other algebraic set, then we already know that $V = V(F)$ for some $F \in \mathbb{R}[X, Y]$ using Corollary 2.

1.31. (a) Find the irreducible components of $V(Y^2-XY-X^2Y+X^3)$ in $\mathbb{A}^2(\mathbb{R})$, and also in $\mathbb{A}^2(\mathbb{C})$. (b) Do the same for $V(Y^2-X(X-1)^2)$, and for $V(X^3+X-X^2Y-Y)$.

Solution

(a) Notice that $Y^2 - XY - X^2Y + X^3 = (Y - X^2)(Y - X)$, then $V(Y^2 - XY - X^2Y + X^3) = V(Y - X^2) \cup V(Y - X)$. This decomposition is the irreducible decomposition in $\mathbb{C}[X, Y]$ because both $Y - X^2$ and $Y - X$ are irreducible, and using Corollary 3. This is also the irreducible decomposition in $\mathbb{A}^2(\mathbb{C})$ because both $Y - X^2$ and $Y - X$ are irreducible in $\mathbb{R}[X, Y]$ and both have an infinite associated algebraic set.

(b) The first polynomial is irreducible and has infinitely many solutions in $\mathbb{A}^2(\mathbb{R})$, hence, its associated algebraic set is irreducible. The second polynomial has the same factorization into irreducible polynomials in $\mathbb{A}^2(\mathbb{R})$ and in $\mathbb{A}^2(\mathbb{C})$ so again, the factorization is the same in the two cases.

1.7 Hilbert's Nullstellensatz

1.32. Show that both theorems and all of the corollaries are false if k is not algebraically closed.

Solution For the Weak-Nullstellensatz, take $k = \mathbb{R}$, $n = 1$, $I = (X^2 + 1)$, then $V(I) = \varnothing$ since $X^2 + 1$ has no roots in $\mathbb{R}$. The same set up disproves the Hilbert's Nullstellensatz, as well as Corollary 1 and 2. For the third corollary, it suffices to look at $V(Y^2 + X^2(X-1)^2)$ in $\mathbb{R}$ and see that even though the polynomial is irreducible, the algebraic set is reducible into $\{(0,0)\}$ and $\{(1,0)\}$. Similarly, if we take $I = (X^2+Y^2) \subset \mathbb{R}[X,Y]$, then $V(I) = \{(0,0)\}$ is finite but $\mathbb{R}[X,Y]/(X^2+Y^2)$ is infinite dimensional. This last example shows that corollary 4 doesn't hold if k is not algebraically closed.

1.33. (a) Decompose $V(X^2 + Y^2 - 1, X^2 - Z^2 - 1) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components. (b) Let $V = \{(t, t^2, t^3) \in \mathbb{A}^3(\mathbb{C}) | t \in \mathbb{C}\}$. Find $I(V)$, and show that V is irreducible.

Solution

(a) First, notice that $(x^2 + y^2 - 1, x^2 - z^2 - 1) = (x^2 + y^2 - 1, (y + iz)(y - iz))$. It follows that

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

Since

$$\begin{aligned}\mathbb{C}[x,y,z]/(x^2 + y^2 - 1, y + iz) &\cong (\mathbb{C}[x,y,z]/(y + iz))/(x^2 + y^2 - 1) \\ &\cong \mathbb{C}[x,y]/(x^2 + y^2 - 1)\end{aligned}$$

is an integral domain, then the ideal $(x^2 + y^2 - 1, y + iz)$ is prime, and hence, $V(x^2 + y^2 - 1, y + iz)$ is irreducible. Similarly, the algebraic set $V(x^2 + y^2 - 1, y - iz)$ is irreducible as well. Therefore, we have found the decomposition of the algebraic set $V(x^2 + y^2 - 1, x^2 - z^2 - 1)$ into irreducible algebraic sets.

(b) First, notice that $V = V(Y - X^2, Z - X^3)$. Hence, if we let $I = (Y - X^2, Z - X^3)$ and notice that $\mathbb{C}[X,Y,Z]/I \cong \mathbb{C}[X]$ is an integral domain, then we get that I is a prime ideal, and hence, $I(V) = I(V(I)) = I = (Y - X^2, Z - X^3)$ by the Nullstellensatz.

1.34. Let R be a UFD. (a) Show that a monic polynomial of degree two or three in $R[X]$ is irreducible if and only if it has no roots in R. (b) The polynomial $X^2 - a \in R[X]$ is irreducible if and only if a is not a square in R.

Solution

(a) First, notice that if a polynomial of degree 2 or 3 is reducible, then it must be divisible by a polynomial of degree 1. Moreover, in the decomposition of the polynomial into two smaller (in the sense of the degree) polynomials, the leading coefficients of each smaller polynomial must be inverses of each other

since the original polynomial is monic. In that case, we can multiply the two polynomials by constants such that the degree one polynomial dividing the original polynomial is monic as well. It follows that a reducible, monic, degree 2 or 3 polynomial must have a root since it is divisible by a polynomial which has a root. The converse is easy.

(b) This follows from part (a) using the fact that $X^2 - a$ has a root if and only if a has a root in R.

1.35. Show that $V(Y^2 - X(X-1)(X-\lambda)) \subset \mathbb{A}^2(k)$ is an irreducible curve for any algebraically closed field k, and any $\lambda \in k$.

Solution Let's show that the polynomial $y^2 - x(x-1)(x-\lambda)$ is irreducible. By contradiction, let $p(x,y)$ and $q(x,y)$ be two nontrivial polynomials such that $p(x,y)q(x,y) = y^2 - x(x-1)(x-\lambda)$, then the highest degree of y in p_1 and p_2 must be either 0 and 2, or 1 in both. However, the first case would imply that $y^2 - x(x-1)(x-\lambda)$ is factorizable by a polynomial in x, which is not the case. Thus, we must have $p(x,y) = p_1(x)y + p_0(x)$ and $q(x,y) = q_1(x)y + q_0(x)$ for some one variable polynomials p_1, p_0, q_1, q_0. In that case,

$$\begin{aligned} &y^2 - x(x-1)(x-\lambda) \\ &\quad = p_1(x)q_1(x)y^2 + (p_1(x)q_0(x) + p_0(x)q_1(x))y + p_0(x)q_0(x) \end{aligned}$$

which implies that $p_1(x)q_1(x) = 1$, $p_1(x)q_0(x) + p_0(x)q_1(x) = 0$ and $p_0(x)q_0(x) = x(x-1)(x-\lambda)$. Since $p_1(x)q_1(x) = 1$, then $p_1(x) = q_1(x) = 1$ without loss of generality. It follows that $q_0(x) = -p_0(x)$, and hence, $-p_0(x)^2 = x(x-1)(x-\lambda)$. But $x(x-1)(x-\lambda)$ is a polynomial of degree 3 while $-p_0(x)^2$ must have an even degree. Therefore, by contradiction, $y^2 - x(x-1)(x-\lambda)$ is irreducible, implying that $V(Y^2 - X(X-1)(X-\lambda))$ is irreducible.

1.36. Let $I = (Y^2 - X^2, Y^2 + X^2) \subset \mathbb{C}[X,Y]$. Find $V(I)$ and $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/I)$.

Solution Notice that $I = (Y^2 - X^2, Y^2 + X^2) = (X^2, Y^2)$. Hence, $V(I) = V(X^2, Y^2) = \{(0,0)\}$. Since

$$\mathbb{C}[X,Y]/(X^2,Y^2) \cong \{c_0 + c_1X + c_1Y + c_2XY : c_i \in \mathbb{C}\},$$

then $\dim_{\mathbb{C}}(\mathbb{C}[X,Y]/I) = 4$.

1.37. Let k be any field, $F \in K[X]$ a polynomial of degree $n > 0$. Show that the residues of $\overline{1}, \overline{X}, ..., \overline{X}^{n-1}$ form a basis of $K[X]/(F)$ over K.

Solution First, it is clear that the elements $\overline{1}, \overline{X}, ..., \overline{X}^{n-1}$ span the elements in $K[X]/(F)$ since every polynomial in $K[X]$ is equivalent to a polynomial of degree at most $n-1$ modulo F. Next, let's show that n elements are linearly independent: let $c_0, c_1, ..., c_{n-1} \in K$ such that

$$c_0\overline{1} + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} = \overline{0},$$

in $K[X]/(F)$, then equivalently:

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1} = p(X)F(X)$$

for some polynomial $p \in K[X]$. The degree of the left hand side is necessarily less than or equal to $n-1$; however, the degree of the right hand side is either 0 or strictly greater than $n-1$. For the equality to hold, it must be that the left hand side has degree 0, and hence, that $c_i = 0$ for all i.

Therefore, the elements $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ are linearly independent, and hence, they form a basis of $K[X]/(F)$.

1.38. Let $R = k[X_1, ..., X_n]$, k algebraically closed, $V = V(I)$. Show that there is a natural one-to-one correspondence between algebraic subsets of V and radical ideals in $k[X_1, ..., X_n]/I$, and that irreducible algebraic sets (resp. points) correspond to prime ideals (resp. maximal ideals). (See Problem 1.22.)

Solution We already know that there is a one-to-one correspondence between the radical ideals of $k[X_1, ..., X_n]/I$ and the radical ideals of $k[X_1, ..., X_n]$ containing I. By Nullstellensatz, we know that there is a one-to-one correspondence between the radical ideals of $k[X_1, ..., X_n]$ and the algebraic sets. Since $V(J) \supset V(I)$ if and only if $J \subset I$, then in particular, there is a one-to-one correspondence between the radical ideals of $k[X_1, ..., X_n]$ containing I and the algebraic sets contained in $V(I)$. Therefore, there is a one-to-one correspondence between the radical ideals of $k[X_1, ..., X_n]/I$ and the algebraic sets contained in $V(I)$. Since an ideal of R/I is prime if and only if its associated ideal is prime in R, then an ideal is prime in R/I if and only if the associated algebraic set conatined in $V(I)$ is irreducible (from the equivalence between prime and irreducible set). The logic is the same for the maximal ideal case.

1.39. (a) Let R be a UFD, and let $P = (t)$ be a principal, proper, prime ideal. Show that there is no prime ideal Q such that $0 \subset Q \subset P$, $Q \neq 0$, $Q \neq P$. (b) Let $V = V(F)$ be an irreducible hypersurface in $\mathbb{A}^n$. Show that there is no irreducible algebraic set W such that $V \subset W \subset \mathbb{A}^n$, $W \neq V$, $W \neq \mathbb{A}^n$.

Solution

(a) Suppose that there is an ideal Q such that $0 \subset Q \subset P$, $Q \neq 0$, $Q \neq P$. Since Q is nonzero, then there is a nonzero element $q \in Q$. Since R is a UFD, then there is a maximal number n such that t divides q since t is irreducible. Since $Q \subset P$, then $q = k_1 t$ for some $k \in R$. But Q is prime so $k_1 t \in Q$ implies that $k_1 \in Q$ or $t \in Q$. But t cannot be in Q since otherwise, $P \subset Q$, a contradiction. Hence, $k_1 \in Q$ which implies that $k_1 = k_2 t$. Applying this argument as much as we want implies that for all i, there is an integer k_i such that $q = k_i t^i$. In particular, when $i = n+1$, we get that t^{n+1} divides q. But this contradicts the fact that n is maximal. Therefore, such a prime ideal Q cannot exist.

(b) If we consider the irreducible divisors of F, then the fact that $V(F)$ is irreducible implies that $F = F_0^n$ where F_0 is irreducible. It follows that $I(V) = (F_0)$ is principal, proper and prime. Hence, applying part (a) to $R = k[X_1, ..., X_n]$ and $t = F_0$ gives us that there is no prime ideal J such that $0 \subsetneq J \subsetneq I(V)$.

Since there is a one-to-one correspondence between prime ideals and irreducible algebraic sets, the last statement is equivalent to the fact that there is no irreducible algebraic set W such that $V \subsetneq W \subsetneq \mathbb{A}^n$.

1.40. Let $I = (X^2 - Y^3, Y^2 - Z^3) \subset k[X, Y, Z]$. Define $\alpha : k[X, Y, Z] \to k[T]$ by $\alpha(X) = T^9$, $\alpha(Y) = T^6$, $\alpha(Z) = T^4$. (a) Show that every element of $k[X, Y, Z]/I$ is the residue of an element $A + XB + YC + XYD$ for some $A, B, C, D \in k[Z]$. (b) If $F = A + XB + YC + XYD$, $A, B, C, D \in k[Z]$, and $\alpha(F) = 0$, compare like powers of T to conclude that $F = 0$. (c) Show that $\ker(\alpha) = I$, so I is prime, $V(I)$ is irreducible, and $I(V(I)) = I$.

Solution

(a) Simply notice that for polynomial F in $k[X, Y, Z]$, this polynomial is equivalent to a polynomial $PX+Q$, $P, Q \in k[Y, Z]$, modulo X^2-Y^3, and every polynomial $H \in k[Y, Z]$ is equivalent to $RY + S$, $R, S \in k[Z]$, modulo $Y^2 - Z^3$. It follows that every element in $k[X, Y, Z]$ is equivalent to a polynomial of the form $A + XB + YC + XYD$ for some polynomials $A, B, C, D \in k[Z]$ modulo I. It follows that every element in $k[X, Y, Z]/I$ is the residue of such a polynomial.

(b) If $F = A + XB + YC + XYD$ with $\alpha(F) = 0$, then

$$0 = \alpha(A) + T^9\alpha(B) + T^6\alpha(C) + T^{15}\alpha(D).$$

Since $\alpha(Z) = T^4$, then the powers of T in $\alpha(A)$ are all multiples of 4. Similarly, the powers of T in $T^9\alpha(B)$ are all of the form $4k + 1$, the powers of T in $T^6\alpha(C)$ are all of the form $4k + 2$ and the powers of T in $T^{15}\alpha(D)$ are all of the form $4k + 3$. Therefore, the only way the sum can be equal to zero is when all the coefficients of the polynomials A, B, C, D are zero, and hence, that $A = B = C = D = 0$, or finally, when $F = 0$.

(c) Since $\alpha(X^2 - Y^3) = \alpha(Y^2 - Z^3) = 0$, then $I \subset \ker(\alpha)$. Next, by part(a), we know that for an arbitrary F, we have that $F = A + XB + YC + XYD + E$ where $A, B, C, D \in k[Z]$ and $E \in I$. Hence, $\alpha(F) = 0$ implies that

$$\alpha(A + XB + YC + XYD) + \alpha(E) = 0.$$

But $I \subset \ker(\alpha)$ so $\alpha(E) = 0$. Hence,

$$\alpha(A + XB + YC + XYD) = 0$$

which implies that $A + XB + YC + XYD = 0$ by part (b). Thus, $F = E \in I$ which proves that $\ker(\alpha) \subset I$. Therefore, $\ker(\alpha) = I$.

To show that I is prime, let $AB \in I = \ker(\alpha)$ which implies that $\alpha(AB) = 0$. But $\alpha(AB) = \alpha(A)\alpha(B)$ so either $\alpha(A)$ or $\alpha(B)$ is zero. Equivalently, one of A or B must be in $\ker(\alpha) = I$. Therefore, I is prime. By the Nullstellensatz, it follows that $V(I)$ is irreducible, and $I(V(I)) = I$.

1.8 Modules; Finiteness Conditions

1.41. If S is module-finite over R, then S is ring-finite over R.

Solution If S is module-finite over R, then there are elements $s_1, ..., s_n \in S$ such that every element in S is of the form $r_1s_1 + \cdots + r_ns_n$ with $r_i \in R$. Consider now the ring $R[s_1, ..., s_n]$, the smallest ring containing R and the elements $s_1, ..., s_n$. Clearly, this ring is contained in S since S is a ring conatining R and the elements $s_1, ..., s_n$. Conversely, if $r_1s_1 + \cdots + r_ns_n \in S$, then $r_1s_1 + \cdots + r_ns_n \in R[s_1, ..., s_n]$ because $R[s_1, ..., s_n]$ is a ring, so it contains all the elements r_is_i, and also their sum. Therefore, $S = R[s_1, ..., s_n]$, so S is ring-finite over R.

1.42. Show that $S = R[X]$ (the ring of polynomials in one variable) is ring-finite over R, but not module-finite.

Solution It is clear that the ring S is ring-finte since it is equal to the smallest ring containing R and X. Next, suppose that S is module-finite, then there exist polynomials $p_1, ..., p_n$ such that every polynomial can be written as an R-linear combination of $p_1, ..., p_n$. However, if we let N be the maximal degree of the p_i's, then any linear combination of the p_i's will have a degree at most N. It follows that not all polynomials in S can be written as an R-linear combination of the p_i's. Therefore, S is not module-finite.

1.43. If L is ring-finite over K (K, L fields) then L is a finitely generated field extension of K.

Solution If L is ring-finite over K, then $L = K[v_1, ..., v_n]$ for some $v_1, ..., v_n \in L$. But since L is a field, then the quotient field of $K[v_1, ..., v_n]$ is itself, i.e., $K[v_1, ..., v_n] = K(v_1, ..., v_n)$. Therefore $L = K(v_1, ..., v_n)$, which proves that L is a finitely generated field extension of K.

1.44. Show that $L = K(X)$ (the field of rational functions in one variable) is a finitely generated field extension of K, but L is not ring-finite over K. (*Hint:* If L were ring-finite over K, a common denominator of ring generators would be an element $b \in K[X]$ such that for all $z \in L$, $b^n z \in K[X]$ for some n; but let $z = 1/c$, where c doesn't divide b (Problem 1.5).)

Solution It is clear that L is a finitely generated field extension of K since it can be written as the $K(X)$. Next, suppose that $L = K[p_1/q_1, ..., p_n/q_n]$ for some $p_i/q_i \in L$, then every rational function in one variable can be written as a polynomial in p_i/q_i. But notice that for any polynomial in p_i/q_i, there exists an integer $N \geq 1$ such that multiplying the polynomial by $(q_1 \cdots q_n)^N$ gives a polynomial in X. Now, consider the rational function $1/(q_1 \cdots q_n + 1) \in L$. For all $N \geq 1$, $(q_1 \cdots q_n)^N/(q_1 \cdots q_n + 1)$ is a not a polynomial in X because the numerator is not divisible by the denominator. Thus, by contradiction, L is not ring-finite.

1.45. Let R be a subring of S, S a subring of T.

(a) If $S = \sum Rv_i$, $T = \sum Sw_j$, show that $T = \sum Rv_iw_j$.

(b) If $S = R[v_1, ..., v_n]$, $T = S[w_1, ..., w_m]$, show that $T = R[v_1, ..., v_n, w_1, ..., w_m]$.

(c) If R, S, T are fields, and $S = R(v_1, ..., v_n)$, $T = S(w_1, ..., w_m)$, show that $T = R(v_1, ..., v_n, w_1, ..., w_m)$.

Solution

(a) Let $\sum s_j w_j$ be an arbitrary element of T, then each s_j can be written as $\sum_i r_{ij} v_i$. Hence:

$$\sum_j s_j w_j = \sum_j \left(\sum_i r_{ij} v_i \right) w_j = \sum_j \sum_i r_{ij} v_i w_j.$$

Therefore, $T = \sum R v_i w_j$ because every element in T can be written as an R-linear combination of $v_i w_j$.

(b) Let $p(w_1, ..., w_m)$ be an arbitrary element in T with $p \in S[X_1, ..., X_m]$, then $p(w_1, ..., w_m)$ is a succession of additions and multiplications of elements in S and $w_1, ..., w_m$. But since every element s in S can be written as a polynomial $p_s(v_1, ..., v_n)$ with $p_s \in R[X_1, ..., X_n]$, then $p(w_1, ..., w_m)$ is an addition and multiplication of polynomials in $v_1, ..., v_n$ and $w_1, ..., w_m$. Since additions and multiplications of polynomials in $v_1, ..., v_n, w_1, ..., w_m$ is still a polynomial in $v_1, ..., v_n, w_1, ..., w_m$, then every element of T can be written as a polynomial in $v_1, ..., v_n, w_1, ..., w_m$. Therefore, $T = R[v_1, ..., v_n, w_1, ..., w_m]$.

(c) Since T contains S and the elements $w_1, ..., w_m$, and S contains R and the elements $v_1, ..., v_n$, then T is a field containing R and the elements $v_1, ..., v_n$, $w_1, ..., w_m$. It follows that $R(v_1, ..., v_n, w_1, ..., w_m) \subseteq T$. Conversely, since $R(v_1, ..., v_n) \subseteq R(v_1, ..., v_n, w_1, ..., w_m)$, then $S \subseteq R(v_1, ..., v_n, w_1, ..., w_m)$. It follows that $T = S(w_1, ..., w_m) \subseteq R(v_1, ..., v_n, w_1, ..., w_m)$. Therefore, $T = R(v_1, ..., v_n, w_1, ..., w_m)$.

1.9 Integral Elements

1.46. Let R be a subring of S, S a subring of (a domain) T. If S is integral over R, and T is integral over S, show that T is integral over R. (*Hint:* Let $z \in T$, so we have $z^n + a_1 z^{n-1} + ... + a_n = 0$, $a_i \in S$. Then $R[a_1, ..., a_n, z]$ is module-finite over R.)

Solution Let $z \in T$, since T is integral over S, then there exists elements $a_1, ..., a_n \in S$ such that $z^n + a_1 z^{n-1} + ... + a_n = 0$. It follows that z is integral over $R[a_1, ..., a_n]$, so the ring $R[a_1, ..., a_n, z]$ is module-finite. Since $R[v]$ is a subring of $R[a_1, ..., a_n, z]$, then z is integral over R by Proposition 3. Therefore, T is integral over R.

1.47. Suppose (a domain) S is ring-finite over R. Show that S is module-finite over R if and only if S is integral over R.

Solution If S is module-finite over R, then for all $z \in S$, we have that $R[z]$ is a subring of S, which is module-finite over R, so z is integral over R. Therefore, S is integral over R.

Conversely, suppose that S is integral over R. Since S is ring-finite over R, then $S = R[v_1, ..., v_n]$ for some $v_1, ..., v_n \in S$. For all i, there exists an integer n_i such that every power v_i^m with $m > n_i$ can be written in terms of v_i, v_i^2, ..., $v_i^{n_i}$ (because v_i solves a polynomial equation). Since $S = R[v_1, ..., v_n]$, then every element in S can be written as $p(v_1, ..., v_n)$ where $p(x_1, ..., x_n)$ is a polynomial in $R[x_1, ..., x_n]$. Since every polynomial is a sum of monomials of the form $\prod_i v_i^{m_i}$, then rewriting each higher powers of v_i in terms of the lower powers gives us that $p(v_1, ..., v_n)$ is a sum of monomials of the form $\prod_i v_i^{m_i}$ with the restriction $m_i \leq n_i$. Thus, every element of S can be written as a linear combination of these monomials, which there are finitely many. Thus, S is generated as a module by these monomials. Therefore, S is module-finite.

1.48. Let L be a field, k an algebraically closed subfield of L. (a) Show that any element of L that is algebraic over k is already in k. (b) An algebraically closed field has no module-finite field extensions except itself.

Solution

(a) Let $z \in L$ be algebraic over k, then there is a (monic) polynomial $p(x) \in k[x]$ such that $p(z) = 0$. Since k is algebraically closed, then $p(x) = (x - a_1) \cdots (x - a_k)$ for some $a_1, ..., a_n \in k$. But since $(z - a_1) \cdots (z - a_k) = 0$, then $z = a_i$ for some i, and hence, $z \in k$.

(b) Let K be a module-finite extension of k and let $z \in K$, then $k[z]$ is contained in a module-finite ring over k, so z must be integral over k. Hence, z is algebraic over k, which implies that $z \in k$ by part (a). Therefore, $K = k$.

1.49. Let K be a field, $L = K(X)$ the field of rational functions in one variable over K. (a) Show that any element of L that is integral over $K[X]$ is already in $K[X]$. (*Hint:* If $z^n + a_1 z^{n-1} + \cdots = 0$, write $z = F/G$, F, G relatively prime. Then $F^n + a_1 F^{n-1} G + \cdots = 0$, so G divides F.) (b) Show that there is no nonzero element $F \in K[X]$ such that for every $z \in L$, $F^n z$ is integral over $K[X]$ for some $n > 0$. (*Hint:* See Problem 1.44.)

Solution

(a) Let $p/q \in K(X)$ be integral over $K[X]$, then there exist polynomials $a_1, ..., a_n \in K[X]$ such that

$$\frac{p^n}{q^n} + a_1 \frac{p^{n-1}}{q^{n-1}} + \cdots + a_{n-1} \frac{p}{q} + a_n = 0.$$

Multiplying both sides by q^n and isolating p^n gives us

$$p^n = -a_1 p^{n-1} q - \cdots - a_{n-1} p q^{n-1} - a_n q^n.$$

Now, let b be an irreducible divisor of q, then b divides the right hand side, and hence, the left hand side which is equal to p^n. Since b is irreducible, then

b divides p. But this shows that every irreducible factor of q divides p, which directly implies that q divides. Hence, $p/q \in K[X]$.

(b) Such an element cannot exist because it would mean that for every $p/q \in L$, there is a n such that $F^n p/q \in K[X]$. If $p = 1$ and $q = F + 1$, then $F^n/(F+1) \notin K[X]$ for all n, contradicting the existence of F.

1.50. Let K be a subfield of a field L. (a) Show that the set of elements of L that are algebraic over K is a subfield of L containing K. (*Hint:* If $v^n + a_1 v^{n-1} + \cdots + a_n = 0$, and $a_n \neq 0$, then $v(v^{n-1} + \dots) = -a_n$.) (b) Suppose L is module-finite over K, and $K \subset R \subset L$. Show that R is a field.

Solution

(a) An element of L is algebraic over K if and only if it is integral over K. Hence, the subset of elements of L algebraic over K form a subring of L. Hence, it suffices to show that if an element is algebraic over K, then its inverse is algebraic over K. Let $z \in L$ be algebraic over K, then $a_n z^n + \cdots + a_0 = 0$ for some $a_i \in K$ such that $a_0 \neq 0$. It follows that $a_0(z^{-1})^n + \cdots + a_n = 0$ which proves that z^{-1} is algebraic pver K. Therefore, the elements that are algebraic over K form a subfield of L which contains K (because every element of K is algebraic over K).

(b) There must be a mistake in the statement of this question because it is clearly false.

1.10 Field Extensions

1.51. Let K be a field $F \in K[X]$ an irreducible monic polynomial of degree $n > 0$. (a) Show that $L = K[X]/(F)$ is a field, and if x is the residue of X in L, then $F(x) = 0$. (b) Suppose L' is a field extension of K, $y \in L'$ such that $F(y) = 0$. Show that the homomorphism from $K[X]$ to L' that takes X to y induces an isomorphism of L with $K(y)$. (c) With L', y as in (b), suppose $G \in K[X]$ and $G(y) = 0$. Show that F divides G. (d) Show that $F = (X - x)F_1$, $F_1 \in L[X]$.

Solution

(a) By Problem 1.3, the ideal (F) is maximal so $K[X]/(F)$ is a field. In this field, the residue of $F(X)$ is 0. Since $F(x)$ is equal to the residue of $F(X)$, then $F(x) = 0$.

(b) The image of the homomorphism $\phi : K[X] \to L'$ mapping $p(X)$ to $p(y)$ is $K[y]$ by definition. Hence, we have the isomorphism $K[y] \cong K[X]/\ker\phi$. Since $K[X]$ is a PID, then $\ker\phi = (f)$ for some $f \in K[X]$. Since $\phi(F) = F(y) = 0$, then $F \in \ker\phi = (f)$. It follows that f divides F, and so by irreducibility of F, f is either 1 or F. If $f = 1$, then $\ker\phi = k[X]$ which is a contradiction, so $f = F$. Hence, $K[y] \cong K[X]/(F) \cong L$. Since L is a field, then $K[y] = K(y)$. Therefore, $L \cong K(y)$.

(c) If $G(y) = 0$, then $G \in \ker \phi = (F)$. It follows that F divides G.

(d) Since x is a root F, then viewing F as a polynomial in $L[X]$ gives us that $F = (X - x)F_1$ where $F_1 \in L[X]$.

1.52. Let K be a field, $F \in K[X]$. Show that there is a field L containing K such that $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$. (*Hint:* Use Problem 1.51(d) and induction on the degree.) L is called a splitting field of F.

Solution When $n = 1$, it is trivial because it suffices to take $L = K$. When $n > 1$, suppose that the statement holds for all polynomials of degree strictly smaller than n. By Problem 1.51(d), we can construct a field L_0 that contains K and where $F = (X - a_n)F_1$ where $F_1 \in L[X]$. By induction, let L be a field containing L_0 such that $F_1 = (X - a_1) \cdots (X - a_{n-1})$, then L is a field containing K such that $F = (X - a_1) \cdots (X - a_n)$.

1.53. Suppose K is a field of characteristic zero, F an irreducible monic polynomial in $K[X]$ of degree $n > 0$. Let L be a splitting field of F, so $F = \prod_{i=1}^{n}(X - x_i)$, $x_i \in L$. Show that the x_i are distinct. (*Hint:* Apply Problem 1.51(c) to $G = F_X$; if $(X - x)^2$ divides F, then $G(x) = 0$.)

Solution Let x be a root of F in L and suppose that $(X - x)^2$ divides F, then $(X - x)$ divides $F_X \in K[X]$. Hence, $G(x) = 0$, so F divides F_X. But this is impossible since F_X has a degree smaller than F. Thus, $(X - x)^2$ doesn't divide F, and so the x_i are distinct.

1.54. Let R be a domain with quotient field K, and let L be a finite algebraic extension of K. (a) For any $v \in L$, show that there is a nonzero $a \in R$ such that av is integral over R. (b) Show that there is a basis $v_1, ..., v_n$ for L over K (as a vector space) such that each v_i is integral over R.

Solution

(a) Since L is algebraic over K, there are elements $a_i, b_i \in R$ such that

$$\frac{a_n}{b_n}v^n + ... + \frac{a_1}{b_1}v + \frac{a_0}{b_0} = 0.$$

Rewriting all of the fractions such that the have the same denominator, we get

$$\frac{a'_n}{b}v^n + ... + \frac{a'_1}{b}v + \frac{a'_0}{b} = 0$$

which implies that

$$a'_n v^n + ... + a'_1 v + a'_0 = 0.$$

Finally, multiplying both sides by $a_n'^{n-1}$ gives us

$$(a'_n v)^n + \cdots + (a'_1 a_n'^{n-2})(a'_n v) + a'_0 a_n'^{n-1} = 0$$

which shows that $a'_n v$ is integral over R. Finally, a'_n is nonzero because a_n is nonzero and none of the b_i are zero.

(b) Since L is a finite extension of K, there is a basis $u_1, ..., u_n$ for L over K. By part (a), there exist nonzero elements $a_i \in R$ such that $v_i := a_i u_i$ is integral over R. Since scaling the elements in a basis don't change the fact that the elements form a basis, then $v_1, ..., v_n$ is a basis for L over K composed only of elements which are integral over K.

Chapter 2

Affine Varieties

2.1 Coordinate Rings

2.1. Show that the map that associates to each $F \in k[X_1, ..., X_n]$ a polynomial function in $\mathcal{F}(V, k)$ is a ring homomorphism whose kernel is $I(V)$.

Solution Let $\varphi : k[X_1, \ldots, X_n] \to \mathcal{F}(V, k)$ be the map that sends each polynomial to its associated function on V. Let's show that it is a ring homomorphism. It is clear that $F(\lambda) = \lambda$ for all $\lambda \in k$. Moreover, since φ is simply a restriction map, then it preserves addition and multiplication of polynomials. Thus, it is a ring homomorphism.

Next, suppose that $F \in \ker \varphi$, i.e $\varphi(F) = 0$, then it follows that $F(x) = 0$ for all $x \in V$, and hence, $F \in I(V)$. Conversely if $F \in I(V)$, then $F(x) = 0$ for all $x \in V$ so $\varphi(F) = 0$ and hence, $F \in \ker \varphi$. Therefore, $\ker \varphi = I(V)$.

2.2. Let $V \subset \mathbb{A}^n$ be a variety. A *subvariety* of V is a variety $W \subset \mathbb{A}^n$ that is contained in V. Show that there is a natural one-to-one correspondence between algebraic subsets (resp. subvarieties, resp. points) of V and radical ideals (resp. prime ideals, resp. maximal ideals) of $\Gamma(V)$. (See Problems 1.22, 1.38.)

Solution This problem is strictly the same as Problem 1.38.

2.3. Let W be a subvariety of a variety V, and let $I_V(W)$ be the ideal of $\Gamma(V)$ corresponding to W. (a) Show that every polynomial function on V restricts to a polynomial function on W. (b) Show that the map from $\Gamma(V)$ to $\Gamma(W)$ defined in part (a) is a surjective homomorphism with kernel $I_W(V)$, so that $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$.

Solution

(a) Let $f \in \mathcal{F}(V, k)$ be a polynomial function, then there is a polynomial $F \in k[X_1, ..., X_n]$ such that $F(x) = f(x)$ for all $x \in V$. Hence, the function $f|_W \in \mathcal{F}(W, k)$ is also a polynomial function since $f|_W(x) = f(x) = F(x)$ for all $x \in W$.

(b) Let $\varphi : \Gamma(V) \to \Gamma(W)$ be the map that sends a polynomial function on V to its restriction on W. This is a ring homomorphism because, clearly $\varphi(\lambda) = \lambda$

for all $\lambda \in k$, and because it is a restriction map so it preserves addition and multiplication.

It is a surjective homomorphism because given any function $f \in \Gamma(W)$, we know that there exists a polynomial $F \in k[X_1, ..., X_n]$ such that $f(x) = F(x)$ for all $x \in W$. Hence, if we define $g \in \Gamma(V)$ by $g(x) = F(x)$ for all $x \in V$, then clearly $\varphi(g) = f$. It follows that φ is surjective.

If $f \in \ker(\varphi)$, then it is equivalent to say that f is sent to 0 by φ. Equivalently, it means that $f(x) = 0$ for all $x \in W$. But by definition, this is equivalent to $f \in I_V(W)$ since $I_V(W)$ is the projection of $I(V)$ in $\Gamma(V)$. Thus, $\ker(\varphi) = I_V(W)$. Therefore, by the First Isomorphism Theorem: $\Gamma(V)/I_V(W) = \Gamma(W)$.

2.4. Let $V \subset \mathbb{A}^n$ be a nonempty variety. Show that the following are equivalent: (i) V is a point; (ii) $\Gamma(V) = k$; (iii) $\dim_k \Gamma(V) < \infty$.

Solution If V is a point $(a_1, ..., a_n)$, then $I(V) = (X_1 - a_1, ..., X_n - a_n)$ which implies that $\Gamma(V) = k[X_1, ..., X_n]/(X_1 - a_1, ..., X_n - a_n) = k$. Hence, (i) implies (ii).

Next, if $\Gamma(V) = k$, then clearly $\dim_k \Gamma(V) = \dim_k k = 1 < \infty$. Hence, (ii) implies (iii).

Finally, if $\dim_k \Gamma(V) < \infty$, then $V(I(V)) = V$ is a finite set. But since V is irreducible, then it must be a point. Thus, (iii) implies (i). Therefore, the three propositions are equivalent.

2.5. Let F be an irreducible polynomial in $k[X, Y]$, and suppose F is monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \cdots + a_n(X)$, with $n > 0$. Let $V = V(F) \subset \mathbb{A}^2$. Show that the natural homomorphism from $k[X]$ to $\Gamma(V) = k[X, Y]/(F)$ is one-to-one, so that $k[X]$ may be regarded as a subring of $\Gamma(V)$; show that the residues $\overline{1}, \overline{Y}, ..., \overline{Y}^{n-1}$ generate $\Gamma(V)$ over $k[X]$ as a module.

Solution Both proposition follow from the fact that $\Gamma(V) = k[X, Y]/(F) = k[X][Y]/(F) \cong k[X][Y]_{<n}$ which denotes the ring of polynomials in Y of degree at most $n - 1$ (addition and multiplication modulo F) with coefficients in $k[X]$. Hence, $k[X]$ is simply the subring of "constant" polynomials; and the elements $\overline{1}, \overline{Y}, ..., \overline{Y}^{n-1}$ generate $\Gamma(V)$ because the elements in $\Gamma(V)$ are polynomials of Y of degree at most $n - 1$.

2.2 Polynomial Maps

2.6. Let $\varphi : V \to W$, $\psi : W \to Z$. Show that $\widetilde{\psi \circ \varphi} = \tilde{\phi} \circ \tilde{\psi}$. Show that the composition of polynomial maps is a polynomial map.

Solution For all functions $f \in \mathcal{F}(Z, k)$, we have

$$(\widetilde{\psi \circ \varphi})(f) = f \circ \psi \circ \varphi = \tilde{\varphi}(f \circ \psi) = \tilde{\varphi}(\tilde{\psi}(f)) = (\tilde{\phi} \circ \tilde{\psi})(f).$$

Thus, $\widetilde{\psi \circ \varphi} = \tilde{\phi} \circ \tilde{\psi}$.

Next, suppose that $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ and $Z \subset \mathbb{A}^k$. If φ and ψ are polynomial maps, then there exist polynomials $T_1, ..., T_m \in k[X_1, ..., X_m]$ and polynomials $F_1, ..., F_k \in k[X_1, ..., X_m]$ such that $\varphi(x) = (T_1(x), ..., T_m(x))$ for all $x \in \mathbb{A}^n$ and $\psi(x) = (F_1(x), ..., F_k(x))$ for all $x \in \mathbb{A}^m$. It follows that

$$(\psi \circ \varphi)(x) = \psi(T_1(x), ..., T_m(x)) = (F_1(T_1(x), ..., T_m(x)), ..., F_k(T_1(x), ..., T_m(x)))$$

for all $x \in \mathbb{A}^n$. For all $i = 1, ..., k$, the map that sends $x \in \mathbb{A}^n$ to $F_i(T_1(x), ..., T_m(x))$ is a polynomial because the composition of polynomials is also a polynomial. Therefore, the composition of two polynomial maps is a polynomial map.

2.7. If $\varphi : V \to W$ is a polynomial map, and X is an algebraic subset of W, show that $\varphi^{-1}(X)$ is an algebraic subset of V. If $\varphi^{-1}(X)$ is irreducible, and X is contained in the image of φ, show that X is irreducible. This gives a useful test for irreducibility.

Solution Let $X = V(F_1, ..., F_r)$, then $x \in \varphi^{-1}(X)$ iff $\varphi(x) \in X$, iff $F_i(\varphi(x)) = 0$ for all $i = 1, ..., r$. Therefore, $\varphi^{-1}(X) = V(F_1 \circ \varphi, ..., F_r \circ \varphi)$ which shows that $\varphi^{-1}(X)$ is an algebraic set ($F_i \circ \varphi$ is a polynomial for all i). Suppose now that $\varphi^{-1}(X)$ is irreducible, and X is contained in the image of φ. If $X = X_1 \cup X_2$ where X_1, X_2 are algebraic sets such that X_i is not contained in X_j for $i \neq j$, then $\varphi^{-1}(X) = \varphi^{-1}(X_1) \cup \varphi^{-1}(X_2)$. By the first part of this exercise, we have that both $\varphi^{-1}(X_1)$ and $\varphi^{-1}(X_2)$ are algebraic sets. Moreover, the fact that X is contained in the image of φ implies that $\varphi^{-1}(X_i) \subset \varphi^{-1}(X_j)$ for $i \neq j$ can never happen. Thus, $\varphi^{-1}(X)$ is not irreducible, a contradiction. Therefore, by contradiction, X is irreducible.

2.8. (a) Show that $\{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$ is an affine variety. (b) Show that $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subset \mathbb{A}^3(\mathbb{C})$ is a variety. (*Hint:* $Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5 \in I(V)$. Find a polynomial map from $\mathbb{A}^1(\mathbb{C})$ onto V.)

Solution

(a) Problem 1.33.

(b) Define the polynomial map $\varphi : \mathbb{A}^1(\mathbb{C}) \to \mathbb{A}^3(\mathbb{C})$ that maps a complex number t to (t^3, t^4, t^5). It is easy to verify that $\varphi(t) \in V(I)$ for all $t \in \mathbb{C}$ (which implies that $\varphi^{-1}(V(I)) = \mathbb{A}^1(\mathbb{C})$). Let's show that $V(I)$ is in the image of φ. If $(x, y, z) \in V(I)$, then $xz = y^2$, $yz = x^3$, and $z^2 = x^2y$. If $x = 0$ or $y = 0$, then it is clear that $(x, y, z) = (0, 0, 0) \in \operatorname{im} \varphi$. Otherwise, we have that

$z = y^2/x$ and $z = x^3/y$ which implies that $y^2/x = x^3/y$, and hence, $y^3 = x^4$. If we let t be a cube root of x, then $y^3 = t^{12}$. Since t can be any cube root of x, then we can choose, in particular the cube root such that $y = t^4$. Finally, since $yz = x^3$, then $z = t^9/t^4 = t^5$. Thus, $(x, y, z) = \varphi(t)$ which implies that $V(I) \subset \operatorname{im}\varphi$.

Next, since $\varphi^{-1}(V(I)) = \mathbb{A}^1(\mathbb{C})$ and $\mathbb{A}^1(\mathbb{C})$ is irreducible, then by Problem 2.7, $V(I)$ is irreducible.

2.9. Let $\varphi : V \to W$ be a polynomial map of affine varieties, $V' \subset V$, $W' \subset W$ subvarieties. Suppose $\varphi(V') \subset W'$. (a) Show that $\tilde{\varphi}(I_W(W')) \subset I_V(V')$ (see Problem 2.3). (b) Show that the restriction of φ gives a polynomial map from V' to W'.

Solution

(a) Let $\tilde{\varphi}(f) = f \circ \varphi \in \tilde{\varphi}(I_W(W'))$ with $f \in I_W(W')$, then for all $x \in V'$, $\varphi(x) \in W'$ which implies that $(f \circ \varphi)(x) = 0$ since $f \in I_W(W')$. It follows that $\tilde{\varphi}(f) \in I_V(V')$, and hence, $\tilde{\varphi}(I_W(W')) \subset I_V(V')$.

(b) Follows directly from the fact that $\varphi(V') \subset W'$, and the fact that φ is a polynomial map.

2.10. Show that the *projection map* $\mathrm{pr} = \mathbb{A}^n \to \mathbb{A}^r$, $n \geq r$, defined by $\mathrm{pr}(a_1, ..., a_n) = (a_1, ..., a_r)$ is a polynomial map.

Solution If we let $P_i \in k[X_1, ..., X_n]$ be the polynomial $P_i(X_1, ..., X_n) = X_i$ for all $i = 1, ..., r$, then clearly $\mathrm{pr} = (P_1, ..., P_r)$.

2.11. Let $f \in \Gamma(V)$, V a variety $\subset \mathbb{A}^n$. Define

$$G(f) = \{(a_1, ..., a_n, a_{n+1}) \in \mathbb{A}^{n+1} \mid (a_1, ..., a_n) \in V \text{ and } a_{n+1} = f(a_1, ..., a_n)\},$$

the *graph* of f. Show that $G(f)$ is an affine variety, and that the map $(a_1, ..., a_n) \mapsto (a_1, ..., a_n, f(a_1, ..., a_n))$ defines an isomorphism of V with $G(f)$. (Projection gives the inverse.)

Solution If $V = V(F_1, ..., F_r)$, then $G(f) = V(F_1, ..., F_r, X_{n+1} - f(X_1, ..., X_n))$; hence, it is an algebraic set. Next, consider the map $\varphi : V \to \mathbb{A}^{n+1}$ that maps $(a_1, ..., a_n)$ to $(a_1, ..., a_n, f(a_1, ..., a_n))$. This is a polynomial map with image equal to $G(f)$. Since $\varphi^{-1}(G(f)) = V$ is irreducible, then it follows that $G(f)$ is irreducible by Problem 2.7.

Next, let's show that φ is an isomorphism. Let $\psi : G(f) \to V$ be the projection map. This is a polynomial map by Problem 2.10. Let $v \in V$, then $\psi(\varphi(v)) = \psi(v, f(v)) = v$; let $(x, f(x)) \in G(f)$, then $\varphi(\psi(x, f(x))) = \varphi(x) = (x, f(x))$. Therefore, φ is an isomorphism.

2.12. (a) Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^3) \subset \mathbb{A}^2$ be defined by $\varphi(t) = (t^2, t^3)$. Show that although φ is a one-to-one, onto polynomial map, φ is not an isomorphism.

(*Hint:* $\tilde{\varphi}(\Gamma(V)) = k[T^2, T^3] \subset k[T] = \Gamma(\mathbb{A}^1)$.) (b) Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^2(X+1))$ be defined by $\varphi(t) = (t^2 - 1, t(t^2-1))$. Show that φ is one-to-one and onto, except that $\varphi(\pm 1) = (0,0)$.

Solution

(a) Clearly, φ is a polynomial map. If $\varphi(s) = \varphi(t)$, then $s^2 = t^2$ and $s^3 = t^3$. If $t = 0$, then $s = 0$ and so $t = s$. Otherwise, since $s^2 = t^2$, then $s = \pm t$. If $s = -t$, then cubing both sides gives us $s^3 = -t^3$ which implies that $t^3 = -t^3$, and hence, $t = 0$, a contradiction. It follows that $s = -t$ cannot hold, and hence, $s = t$. Therefore, φ is one-to-one. To show that φ is onto, let $(x, y) \in V$, then $y^2 = x^3$. If we let t be a square root of x, then we get that $y^2 = t^6$. It follows that $y = \pm t^3 = (\pm t)^3$. If $y = t^3$, then we are done since $(x, y) = \varphi(t)$; if $y = (-t)^3$, then we get that $(x, y) = \varphi(-t)$. It follows that φ is onto.

Suppose that there is a polynomial map $\psi : V \to \mathbb{A}^1$ such that $\psi \circ \varphi = id$, then $\tilde{\varphi} \circ \tilde{\psi} = \tilde{id} = id : k[X] \to k[X]$ by Problem 2.6 using the fact that $\Gamma(\mathbb{A}^1) = k[X]$. But this implies that $\operatorname{im} \tilde{\varphi} = k[X]$ which is impossible since $\operatorname{im} \tilde{\varphi} = k[X^2, X^3] \not\supseteq X$. Therefore, ψ cannot exist, and φ cannot be an isomorphism.

(b) If $\varphi(s) = \varphi(t)$, then $s^2 - 1 = t^2 - 1$ and $s(s^2-1) = t(t^2-1)$. Suppose that $s^2 - 1 = t^2 - 1 \neq 0$, then $s(s^2-1) = t(t^2-1)$ directly implies that $s = t$. The case $s^2 - 1 = t^2 - 1 = 0$ implies that $s = \pm 1$ and $t = \pm 1$ which we don't consider here. Next, let $(x, y) \in V$, then $y^2 = x^2(x+1)$. If we let t be a root of the equation $t^2 - 1 = x$, then $y^2 = (t^2-1)^2(t^2-1+1) = [t(t^2-1)]^2$. It follows that $y = \pm t(t^2-1)$. Equivalently, $(x, y) = \varphi(\pm t)$ which, in both cases, implies that $(x, y) \operatorname{im} \varphi$. Therefore, φ is one-to-one and onto, except at ± 1.

2.13. Let $V = V(X^2 - Y^3, Y^2 - Z^3) \subset \mathbb{A}^3$ as in Problem 1.40, $\overline{\alpha} : \Gamma(V) \to k[T]$ induced by the homomorphism α of that problem. (a) What is the polynomial map f from $\mathbb{A}^1$ to V such that $\tilde{f} = \overline{\alpha}$? (b) Show that f is one-to-one and onto, but not an isomorphism.

Solution First, recall that $\alpha : k[X, Y, Z] \to k[T]$ is defined by $\alpha(X) = T^9$, $\alpha(Y) = T^6$, and $\alpha(Z) = T^4$. Since $\ker \alpha = I(V)$, then we have an induced homomorphism $\overline{\alpha} : \Gamma(V) \to k[T]$ such that $\overline{\alpha} \circ \pi = \alpha$ where $\pi : k[X, Y, Z] \to \Gamma(V)$ is the projection map.

(a) By following the proof of Proposition 1 (or simply by looking at the definition of α), we get that $f : \mathbb{A}^1 \to V$ defined by $f(T) = (T^9, T^6, T^4)$ is the polynomial map that satisfies $\tilde{f} = \varphi$.

(b) If $f(s) = f(t)$, then $s^k = t^k$ for $k = 4, 6, 9$. We can assume that $s, t \neq 0$ since otherwise, $s = t$. From $s^4 = t^4$, we get that $s = i^m t$ for some integer $m = 0, 1, 2, 3$ where i denotes a root of -1. Taking both sides to the sixth power gives us $s^6 = (-1)^m t^6$. But since $s^6 = t^6$, then $t^6 = (-1)^m t^6$ which implies that $(-1)^m = 1$, and hence, that $m = 0, 2$. It follows that $s = (-1)^p t$ for some integer $p = 0, 1$. Next, taking the previous equation to the power of nine gives us that $s^9 = (-1)^p t^9$; but since $s^9 = t^9$, then $t^9 = (-1)^p t^9$, and hence $(-1)^p = 1$. It follows that $s = t$. Thus, f is one-to-one.

Let $(x, y, z) \in V$, then $x^2 = y^3$ and $y^2 = z^3$. If we let t be a fourth root of z, then $y^2 = t^{12}$ which implies that $y = \pm t^6$, and hence, that $y = (i^k t)^6$ where i is a root of $\sqrt{-1}$, and k is any of $0, 2$ or $1, 3$. Similarly, if we do the same with the ninth power, we get that $x = (i^k t)^9$ for some k which will correspond to the case of the sixth power. It follows that $(x, y, z) = f(i^k t)$, and hence, f is onto V. Finally, let's show that f is not an isomorphism. Suppose that there is a polynomial map $g : V \to \mathbb{A}^1$ such that $g \circ f = id$, then $\tilde{f} \circ \tilde{g} = \tilde{id} = id : k[T] \to k[T]$ by Problem 2.6 using the fact that $\Gamma(\mathbb{A}^1) = k[T]$. But this implies that $\operatorname{im} \tilde{f} = k[T]$ which is impossible since $\operatorname{im} \tilde{f} = k[T^9, T^6, T^4] \not\ni T$. Therefore, g cannot exist, and hence, f cannot be an isomorphism.

2.3 Coordinate Changes

2.14. A set $V \subset \mathbb{A}^n(k)$ is called a *linear subvariety* of $\mathbb{A}^n(k)$ if $V = V(F_1, ..., F_r)$ for some polynomials F_i of degree 1. (a) Show that if T is an affine change of coordinates on $\mathbb{A}^n$, then V^T is also a linear subvariety of $\mathbb{A}^n(k)$. (b) If $V \neq \varnothing$, show that there is an affine change of coordinates T of $\mathbb{A}^n$ such that $V^T = V(X_{m+1}, ..., X_n)$. (*Hint:* use induction on r.) So V is a variety. (c) Show that the m that appears in part (b) is independent of the choice of T. It is called the dimension of V. Then V is then isomorphic (as a variety) to $\mathbb{A}^m(k)$. (*Hint:* Suppose there were an affine change of coordinates T such that $V(X_{m+1}, ..., X_n)^T = V(X_{s+1}, ..., X_n)$, $m < s$; show that $T_{m+1}, ..., T_n$ would be dependent.)

Solution

(a) If we denote $I = (F_1, ..., F_r)$, then I^T is generated by the elements F^T with $F \in I$. But notice that if $F = \sum_i a_i F_i$, then

$$F^T = \tilde{T}(\sum_i a_i F_i) = \sum_i \tilde{T}(a_i)\tilde{T}(F_i) = \sum_i a_i^T F_i^T$$

which implies that $I^T = (F_1^T, ..., F_r^T)$. Since the F_i's and the T_i's are all linear, then the F_i^T are linear, and hence, $V^T = V(F_1^T, ..., F_r^T)$ is a linear subvariety.

(b) By the Weak-Nullstellensatz, $V \neq \varnothing$ implies that $r \geq 1$. **TODO**

(c) **TODO**

2.15. **TODO**

Solution **TODO**

2.16. **TODO**

Solution **TODO**

2.4 Rational Functions and Local Rings

2.17. Let $V = V(Y^2 - X^2(X+1)) \subset \mathbb{A}^2$, and $\overline{X}$, $\overline{Y}$ the residues of X, Y in $\Gamma(V)$; let $z = \overline{Y}/\overline{X} \in k(V)$. Find the pole sets of z and of z^2.

Solution First, notice that $z^2 = \overline{X+1}$ so its pole set is the empty set. Let's prove that $(0,0)$ is the only element in the pole set of z. Since $z = \overline{Y}/\overline{X}$ and $z = \overline{X(X+1)}/\overline{Y}$, then $(0,0)$ is the only possible element in the pole set. If the pole set is empty, then z must be a rational function, and hence, we have the equality $\overline{Y}/\overline{X} = \overline{p(X,Y)}$ which is equivalent to

$$Y - Xp(X,Y) = q(X,Y)(Y^2 - X^2(X+1))$$

in $k[X, Y]$. Taking $X = 0$ gives us the equation $Y = q(0, Y)Y^2$ which is impossible. Therefore, the pole set of z is composed of $(0, 0)$ only.

2.18. Let $\mathcal{O}_P(V)$ be the local ring of a variety V at a point P. Show that there is a natural one-to-one correspondence between the prime ideals in $\mathcal{O}_P(V)$ and the subvarieties of V that pass through P. (*Hint:* If I is prime in $\mathcal{O}_P(V)$, $I \cap \Gamma(V)$ is prime in $\Gamma(V)$, and I is generated by $I \cap \Gamma(V)$; use Problem 2.2.)

Solution **TODO**

2.19. **TODO**

Solution **TODO**

2.20. In the example given in this section, show that it is impossible to write $f = a/b$, where $a, b \in \Gamma(V)$, and $b(P) \neq 0$ for every P where f is defined. Show that the pole set f is exactly $\{(x, y, z, w) | y = 0 \text{ and } w = 0\}$.

Solution **TODO**

2.21. **TODO**

Solution **TODO**

2.22. **TODO**

Solution **TODO**