Chapter 1

Affine Algebraic Sets

1.1 Algebraic Preliminaries

Problems

1.1. Let R be a domain.

(a) If F, G are forms of degree r, s respectively in $R[X_1, \ldots, X_n]$, show that FG is a form of degree $r+s$.

(b) Show that any factor of a form in $R[X_1, \ldots, X_n]$ is also a form.

Solution. (a) *Proof.* Suppose F, G are forms of degree r, s respectively. Then

$$F(X_1, \ldots, X_n) = \sum a_I X_1^{i_1} \ldots X_n^{i_n}$$

and

$$G(X_1, \ldots, X_n) = \sum b_J X_1^{j_1} \ldots X_n^{j_n},$$

where $\sum i_k = r$ and $\sum j_k = s$. Then

$$FG(X_1, \ldots, X_n) = \sum_{i,j} a_I b_J X_1^{i_1+j_1} \ldots X_n^{i_n+j_n},$$

and we see that every monomial in this expression has degree $\sum i_k + j_k = \sum i_k + \sum j_k = r + s$, so FG is a form of degree $r+s$. $\square$

(b) *Proof.* Let H be a form of degree d and suppose $H = FG$ where $F = F_0 + F_1 + \cdots + F_d$ where F_i is a form of degree i. Similarly $G = G_0 + G_1 + \cdots + G_d$ where G_j is a form of degree j. Then $H = FG = \sum_{i,j=0}^{d} F_i G_j$, and since H is homogeneous of degree d and $F_i G_j$ is homogeneous of degree $i+j$ by (a), we must have that $F_iG_j = 0$ unless $i+j = d$. So, $H = FG = \sum_{i=0}^{d} F_iG_{d-i}$. Suppose F_I and F_J are not equal to zero. Suppose G_K is not equal to zero. Then $I + K = J + K = d$, so $I = J$. So, $F_i \neq 0$ for only one index. Thus, $F = F_i$ is a form of degree i. Reversing F and G, Thus, $G = G_{d-i}$ is a form of degree $d - i$. So F, G are homogeneous. □

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. *Proof.* Let $z \in K$. Then $z = x/y$ for some $x, y \in R$, $y \neq 0$. Since R is a UFD, write $x = x_1 \ldots x_n$ and $y = y_1 \ldots y_m$ where each x_i and y_j is irreducible.

If x, y have a common factor, they must have a common irreducible factor, and it follows that x_i and y_j are associates for some $i = i_0, j = j_0$. Consequently x_{i_0}/y_{j_0} is a unit. The existence result follows by an inductive argument on the number of irreducible factors.

Suppose $z = x/y = x'/y'$ where x and y have no common factor and x' and y' have no common factor. Then $xy' = x'y$. If x_i is an irreducible factor of x, then x_i must divide $x'y$. Since x and y have no common factors, x_i divides x', so x_i is an irreducible factor of x'. So every irreducible factor of x divides x'. Reversing the roles of x and x', every irreducible factor of x' divides x. This forces x and x' to be associates. Similarly, y and y' are associates. This proves the result. □

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) *Proof.* Let P be a nonzero, proper, prime ideal in a PID R. Say $P = (x)$. Since P is nonzero and proper, x is nonzero and not a unit.

Suppose x is reducible, say $x = yz$ for nonunits $y, z \in R$. Since P is a prime ideal, either $y \in P$ or $z \in P$. If $y \in P$, then x divides y, and it follows that x and y are associates and z is a unit. This is a contradiction. Similarly, if $z \in P$, then x divides z, and it follows that x and z are associates and y is a unit. This is also a contradiction.

Hence x is irreducible. □

(b) *Proof.* Let $P = (x)$ be a prime ideal. By part (a), x is irreducible. Suppose $I = (y)$ is an ideal with $P \subset I \subset R$. Since $P \subset I$, y must divide x, and since x is irreducible, either y is a unit or y is an associate of x. But if y is a unit, then $I = R$. If y is an associate of x, then $I = P$. Hence, P is a maximal ideal. □

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

Solution. *Proof.* We proceed by induction on n. If $n = 1$, then by the Fundamental Theorem of Algebra, a nonzero F of degree d can have at most d roots. Since $F(a) = 0$ for all $a \in k$ and k is infinite, $F \equiv 0$.

Assume that if $F(a_1, \ldots, a_{n-1}) = 0$ for all $a_1, \ldots, a_{n-1} \in k$, then $F \equiv 0$.

Suppose $F(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Write $F = \sum F_i X_n^i$ where $F_i \in k[X_1, \ldots, X_{n-1}]$. Then $F(a_1, \ldots, a_{n-1}, X_n) = \sum_i F_i(a_1, \ldots, a_{n-1}) X_n^i$ has infinitely many roots, so we conclude that $F_i(a_1, \ldots, a_{n-1}) \equiv 0$ for all $a_1, \ldots, a_{n-1} \in k$ and for all i. By our inductive hypothesis, $F_i = 0$ for all i, so $F = 0$. □

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

Solution. *Proof.* Suppose $F_1, \ldots, F_n$ is a complete list of irreducible monic polynomials in $k[X]$. Let $F = F_1 \cdots F_n + 1$. Then F is a monic polynomial. Since $k[X]$ is a UFD, F must have an irreducible factor, G, and this must be one of the F_i's since $F_1, \ldots, F_n$ is a complete list of irreducible monic polynomials in $k[X]$. It now follows that G divides 1 which is absurd. So, there are an infinite number of irreducible monic polynomials in $k[X]$. □

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

Solution. *Proof.* If k is algebraically closed, for any $\lambda \in k$, $x - \lambda$ is an irreducible monic polynomial in $k[X]$. Since k is algebraically closed, all irreducible monic polynomials are of this form. By Problem 1.5, k must be infinite. □

1.7. Let k be a field, $F \in k[X_1, \ldots, X_n]$, $a_1, \ldots, a_n \in k$.

(a) Show that

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

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

Solution. (a) *Proof.* We proceed by induction on n. Suppose $F \in k[X]$. Let $a \in k$. By the Division Algorithm, $F(X) = (X-a)G_1(X) + r_0$, where $\deg(G_1) = \deg(F) - 1$ and $r_0 \in k$. Continuing, we get $G_i = (X-a)G_{i+1} + r_i$, with $\deg(G_i) = \deg(F) - i$ and $r_i \in k$. Of course, G_d is a constant r_d. Splicing all these together gives

$$F(X) = r_d(X-a)^d + r_{d-1}(X-a)^{d-1} + \cdots + r_0.$$

Now suppose $F \in k[X_1, \ldots, X_n]$. Considering $F \in k[X_1, \ldots, X_{n-1}][X_n]$, we may write

$$F = \sum_{i=0}^{d} r_{i_n}(X_n - a_n)^{i_n},$$

with $r_{i_n} \in k[X_1, \ldots, X_{n-1}]$. The result follows by mathematical induction. $\square$

(b) *Proof.* If $F(a_1, \ldots, a_n) = 0$, then in the expression

$$F = \sum_I \lambda_{(i)}(X_1 - a_1)^{i_1} \ldots (X_n - a_n)^{i_n}$$

we must have $\sum_j i_j \geq 1$, for each multi-index $I = (i_1, \ldots, i_n)$. Let

$$\Lambda_j = \{I \mid i_j \geq 1 \text{ and } i_1, \ldots, i_{j-1} = 0\}.$$

Then each multi-index I belongs to exactly one of $\Lambda_1, \ldots, \Lambda_n$. If $I \in \Lambda_j$, we can factor out $(X_j - a_j)$ and leave a polynomial. Then

$$\begin{aligned} F &= \sum_I \lambda_I(X_1 - a_1)^{i_1} \ldots (X_n - a_n)^{i_n} \\ &= \sum_{j=1}^{n} \sum_{I \in \Lambda_j} \lambda_I(X_1 - a_1)^{i_1} \ldots (X_n - a_n)^{i_n} \\ &= \sum_{j=1}^{n} (X_j - a_j) \sum_{I \in \Lambda_j} \lambda_I(X_1 - a_1)^{i_1} \ldots (X_j - a_j)^{i_j - 1} \ldots (X_n - a_n)^{i_n} \end{aligned}$$

Now let $G_j = \sum_{i \in \Lambda_j} \lambda_I(X_1 - a_1)^{i_1} \ldots (X_j - a_j)^{i_j - 1} \ldots (X_n - a_n)^{i_n}$, to get

$$F = \sum_{j=1}^{n} (X_j - a_j) G_j(X_1, \ldots, X_n).$$

$\square$

1.2 Affine Space and Algebraic Sets

Problems

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. *Proof.* Let $X = V(S)$ be an algebraic set. If $S = \{0\}$ then $X = \mathbb{A}^1(k)$. If there is a nonzero $F \in S$, then X is contained in the zero set of the polynomial F, and is therefore finite.

Conversely, given any finite set in $\mathbb{A}^1(k)$, we can easily construct a polynomial vanishing precisely on that set. □

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

Solution. *Proof.* Let k be a finite field. Since k is finite, so is $\mathbb{A}^n(k)$, and so every subset of $\mathbb{A}^n(k)$ is also finite. Since the finite union of algebraic sets is also algebraic, it suffices to show that $\{(a_1, \dots, a_n)\} \in \mathbb{A}^n(k)$ is algebraic. However, the set $\{(a_1, \dots, a_n)\}$ is the zero set of the ideal $(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n) \subset k[X_1, \dots, X_n]$. □

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

Solution. *Proof.* Consider $\mathbb{N} \subset \mathbb{C}$. Since each point of $\mathbb{C}$ is an algebraic set, $\mathbb{N}$ is a countable union of algebraic subsets of $\mathbb{C}$. However $\mathbb{N}$ is not algebraic since the only algebraic sets in $\mathbb{C}$ are the whole space and finite sets of points by Problem 1.8.

□

1.11. Show that the following are algebraic sets:

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

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

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

Solution. (a) *Proof.* The set $\{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$ is cut out by the polynomials $Y - X^2, Z - X^3$.

□

(b) *Proof.* The set $\{(\cos(t), \sin(t)) \in \mathbb{A}^2(\mathbb{R}) \mid t \in \mathbb{R}\}$ is cut out by the polynomial $X^2 + Y^2 - 1$.

□

(c) *Proof.* The set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = \sin(\theta)$ also satisfies the equation $r^2 = r\sin(\theta)$. Converting this to Cartesian coordinates, we have $x^2 + y^2 = y$, so this set is cut out by the single polynomial $X^2 + Y^2 - Y$.

□

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. *Proof.* Let 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. For a line L in $\mathbb{A}^2(k)$, suppose $L = V(Y - (aX + b))$, which we can always do by a change of coordinates if necessary. The x-coordinates of the points of intersection of L and C are given by the polynomial $F(X, aX + b) \in k[X]$. Since $L \not\subset C$, the polynomial $F(X, aX + b)$ is not identically zero. By the Fundamental Theorem of Algebra, this equation has at most n roots. Of course, once x is fixed, y is fixed as well. Consequently, $L \cap C$ consists of at most 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) $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\}$.

Solution. (a) *Proof.* Were the set $\{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin(x)\}$ an algebraic set, then its intersection with the algebraic set cut out by $\{Y\}$ would also be an algebraic set. But this set is $\{(k\pi, 0) : k \in \mathbb{Z}\}$, which is a countably infinite subset of $\mathbb{A}^1(\mathbb{R})$ and therefore not an algebraic set by Problem 1.8. □

(b) *Proof.* Suppose the set $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$ is algebraic. Then its intersection with the algebraic set $V(w) = \{(z, 0) \in \mathbb{A}^2(\mathbb{C})\}$. But this intersection is the set $\{(z, 0) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 = 1\}$, which is infinite. Since $V(w) = \{(z, 0) \in \mathbb{A}^2(\mathbb{C})\}$ is isomorphic to $\mathbb{A}^1(\mathbb{C})$, the proper algebraic subsets here are finite by Problem 1.8. □

(c) *Proof.* Were the set $\{(\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) \,|\, t \in \mathbb{R}\}$ an algebraic set, then its intersection with the algebraic set cut out by $\{X - 1\}$ would also be an algebraic set. But this set is $\{(1, 0, 2k\pi) : k \in \mathbb{Z}\}$ may be considered as a countably infinite subset of $\mathbb{A}^1(\mathbb{R})$ and therefore not an algebraic set by Problem 1.8. □

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

Solution. *Proof.* Suppose $\mathbb{A}^n(k) \setminus V(F)$ is finite. Since every finite set is algebraic, we can find a polynomial G vanishing precisely on $\mathbb{A}^n(k) \setminus V(F)$. Then FG vanishes on all of $\mathbb{A}^n(k)$. If follows by Problem 1.4 that $FG \equiv 0$. Since $k[X_1, \ldots, X_n]$ is a domain, $F \equiv 0$ or $G \equiv 0$. But $F \not\equiv 0$ by hypothesis, and if $G \equiv 0$, then $V(F) = \emptyset$. But F is a non-constant polynomial, and since k is algebraically closed, F must have a root. This is a contradiction. So, $\mathbb{A}^n(k) \setminus V(F)$ is infinite.

We prove $V(F)$ is infinite for $n \geq 2$. Since F is nonconstant, F must contain at least one variable. We suppose F contains X. Since $n \geq 2$, there must be at least one more variable. Call it Y (which may or may not appear in F). Fix all the remaining variables of F, if any, and treat F as a function of X and Y.

Suppose F does not contain Y. Then F is a nonconstant polynomial in X alone. Since k is algebraically closed, F must have a root, x_0. Then the set $\{(x_0, a) \,|\, a \in k\}$ lies in $V(F)$. Since k is algebraically closed, this set is infinite. The proof is analogous if F contains Y but not X and the proof is easier if F contains both X and Y. □

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

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

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

Solution. *Proof.* Let $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ define an algebraic set V, and let G_1, $\ldots$,$G_t \in k[X_1, \ldots, X_n]$ define an algebraic set W. We consider all the F_i's and G_j's as elements of $k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ and claim that $V \times W$ is the set of common zeros of

$$\mathscr{S} = \{F_1, \ldots F_s, G_1, \ldots, G_t\}.$$

If $(a_1, \ldots, a_n, b_1, \ldots, b_m) \in V(\mathscr{S})$, then $F_i(a_1, \ldots, a_n) = 0 = G_j(b_1, \ldots, b_m)$ for all i, j, so $(a_1, \ldots, a_n) \in V$ and $(b_1, \ldots, b_m) \in W$. The reverse inclusion is clear. So $V \times W$ is an algebraic set in $\mathbb{A}^{n+m}$. □

1.3 The Ideal of a Set of Points

Problems

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. *Proof.* From Section 1.2, item (3) and Section 1.3, item (6), we know that $V \subset W$ if and only if $I(W) \subset I(V)$. Reversing the roles of V and W and putting these two inclusions together yields the result. □

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 $F \in k[X_1, \ldots X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$. (*Hint:* $I(V) \neq I(V \cup \{P\})$.)

(b) Let $P_1, \ldots, P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, \ldots, F_r \in I(V)$ 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 $P_1, \ldots, P_r$ 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) *Proof.* Let $V \subset \mathbb{A}^n(k)$ be an algebraic set and $P \in \mathbb{A}^n(k)$, $P \notin V$. Then $V \subsetneq V \cup \{P\}$, so $I(V \cup \{P\}) \subsetneq I(V)$ by Problem 1.16. Hence, there exists $G \in I(V)$ such that $G \notin I(V \cup \{P\})$. Since $G \in I(V)$, $G(Q) = 0$ for all $Q \in V$. Since $G \notin I(V \cup \{P\})$ and G vanishes on V, $G(P)$ cannot be zero. Let $F = G/G(P) \in k[X_1, \ldots, X_n]$. Then F vanishes on V and $F(P) = 1$. □

(b) *Proof.* Let $P_1, \ldots, P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. For each i, $1 \leq i \leq r$, let $W_i = V \cup \{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots P_r\}$. Since $P_i \notin W_i$, by part (a) there exists $F_i \in I(W_i) \subseteq I(V)$ so that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$. □

(c) *Proof.* Let $a_{ij} \in k$ for $1 \leq i, j \leq r$. Let $P_1, \ldots, P_r$ be distinct points in $\mathbb{A}^n(k)$, not in an algebraic set V. By (b), we can find $F_1, \ldots, F_r$ in $I(V)$ so that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$.

Let $G_i = \sum_k a_{ik} F_k$. Then $G_i(P_j) = \sum_k a_{ik} F_k(P_j) = \sum_k a_{ik} \delta_{jk} = a_{ij}$.

□

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 $\text{Rad}(I)$ is an ideal, in fact a radical ideal. Show that any prime ideal is radical.

Solution. *Proof.* Let I be an ideal in a ring R and suppose $a, b \in \text{Rad}(I)$. By definition of the radical, we have $a^n, b^m \in I$ for some natural numbers n, m. Then $(a+b)^{n+m} = \sum_{i+j=n+m} c_{ij} a^i b^j$, where $c_{ij} \in \mathbb{N}$. Now, if $i < n$ and $j < m$, then $i + j < n + m$, so we see that every term in this sum must have $i \geq n$ or $j \geq m$. If $i \geq n$, then $a^i = a^{i-n} a^n \in I$ and if $j \geq m$, then $b^j = b^{j-m} b^m \in I$. So every term of the sum is in I, whereby $(a+b)^{n+m} \in I$. Hence $a + b \in \text{Rad}(I)$.

Likewise, if $r \in R$ and $a \in \text{Rad}(I)$, then $a^n \in I$ for some $n \in \mathbb{N}$. Then $(ra)^n = r^n a^n \in I$, and it follows that $ra \in \text{Rad}(I)$. So $\text{Rad}(I)$ is an ideal in R.

Suppose $a^n \in \text{Rad}(I)$. Then $(a^n)^m \in I$ for some m. But this says $a^{nm} \in I$, so $a \in \text{Rad}(I)$. So, $\text{Rad}(I)$ is a radical ideal.

Let $\mathfrak{p}$ be a prime ideal. Suppose $a \in \text{Rad}(\mathfrak{p})$. Then $a^n \in \mathfrak{p}$ and since $\mathfrak{p}$ is a prime ideal, $a \in \mathfrak{p}$. So, $\mathfrak{p}$ is a radical ideal. □

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. *Proof.* Consider $I = (X^2 + 1) \subset \mathbb{R}[X]$. Suppose $FG \in I$ for some $F, G \in k[X, Y]$. Then $X^2 + 1$ is a divisor of FG. Since $X^2 + 1$ is irreducible in $\mathbb{R}[X]$, $X^2 + 1$ is a divisor of F or $X^2 + 1$ is a divisor of G. This says F or G lies in I. So, I is a prime ideal, and therefore a radical ideal.

Since $X^2 + 1$ has no root in $\mathbb{R}$, $V(I) = \emptyset$. Then $I(V(I)) = I(\emptyset) = \mathbb{R}[X]$. However, if I were the ideal of an algebraic set, then by item (9) in Section 1.3, $I(V(I)) = I$. Since $I \neq \mathbb{R}[X]$, I is not the ideal of an algebraic set. □

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

Solution. *Proof.* Since $I \subset \text{Rad}(I)$, we have $V(\text{Rad}(I)) \subset V(I)$ by item (3) in Section 1.2. Let $P \in V(I)$ and let $F \in \text{Rad}(I)$. Then $F^n \in I$ for some $n \in \mathbb{N}$, so $F^n(P) = (F(P))^n = 0$, since $P \in V(I)$. Hence $F(P) = 0$. Since $F \in \text{Rad}(I)$ is arbitrary, $P \in V(\text{Rad}(I))$. Since $P \in V(I)$ is arbitrary, $V(I) \subset V(\text{Rad}(I))$. Putting these two inclusions together, we have $V(I) = V(\text{Rad}(I))$.

Let $F \in \text{Rad}(I)$. Then $F^n \in I$ for some natural number n. Let P be any point in $V(I)$. Since $F^n \in I$ and $P \in V(I)$, $F^n(P) = 0$. So, $F(P) = 0$. Since P is arbitrary, $F \in I(V(I))$ and since $F \in \text{Rad}(I)$ is arbitrary, $\text{Rad}(I) \subset I(V(I))$. □

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

Solution. *Proof.* If we prove the second part, it follows that I is maximal since $k \cong k[X_1, \ldots, X_n]/I$ is a field.

Define $\varphi : k \to k[X_1, \ldots, X_n]/I$ by $\varphi(\lambda) = \overline{\lambda}$, where we use a bar to denote the residue class. It's clear that φ is a homomorphism. It is equally clear that

φ is injective since every element of I has degree at least one. We show that φ is surjective.

Let F be any polynomial in $k[X_1, \dots, X_n]$. By Problem 1.7(a), we can write $F = \sum_{(i)} \lambda_{(i)}(X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n}$. Let F' be the constant polynomial $\lambda_{(0)}$. By Problem 1.7(b), $F - F' \in I$, so $\overline{F} = \overline{F'}$. Since $\overline{F'} = \overline{\lambda_{(0)}} = \varphi(\lambda_{(0)})$, it follows that $\overline{F}$ is in the image of φ. Since $F \in k[X_1, \dots, X_n]$ is arbitrary, φ is surjective. □

1.4 The Hilbert Basis Theorem

Problems

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 containing I, and for every ideal J of R containing 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 which 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 $k[X_1, \dots, X_n]/I$ is Noetherian.

Solution. (a) *Proof.* For $\pi : R \to R/I$ and $J' \subset R/I$ an ideal, let $J = \pi^{-1}(J')$. If $a, b \in J$, then $\pi(a), \pi(b) \in J'$, so $\pi(a + b) = \pi(a) + \pi(b) \in J'$, so $a + b \in J$. Similarly, $ra \in J$ for $r \in R$, $a \in J$. So J is an ideal. It's clear that $J \supset I$.

Let J' be an ideal in R/I. Let $J = \pi^{-1}(J') \subset R$. Since π is surjective, $\pi(\pi^{-1}(J')) = J'$. Thus π sets up a natural one-to-one correspondence between {ideals of R/I} and {ideals of R which contain I}.

□

(b) *Proof.* Suppose $J' \subset R/I$ is radical and say $F \in \mathrm{Rad}(J)$. Then $F^n \in J$ whereby $\overline{F}^n \in J'$ for some natural number n, so $\overline{F} \in \mathrm{Rad}(J') = J'$. Then $F \in J$ by definition of J. So J is radical. The reverse inclusion and the proofs for prime and maximal ideals are similar. □

(c) *Proof.* Suppose J is finitely generated. Say the set $\{x_1, \dots, x_n\}$ generates J. Then we claim the set $\{\overline{x}_1, \dots, \overline{x}_n\}$ generates J', as is easily seen. It follows that R/I is Noetherian whenever R is Noetherian.

It follows from this result and the Hilbert Basis Theorem that any ring of the form $k[X_1, \dots, X_n]/I$ is Noetherian. □

1.5 Irreducible Components of an Algebraic Set

Problems

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. Let $R = k[X, Y]$ and let $I = (X)$. Let $\mathscr{S} = \{I^n | n \in \mathbb{N}\}$. Then R is a Noetherian ring, $\mathscr{S}$ is a collection of ideals, but no maximal member of $\mathscr{S}$ is a maximal ideal—since $\mathscr{S}$ contains no maximal ideals.

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 which contain I}.)

Solution. Let R be a Noetherian ring and let I be a proper ideal in R. Let $\mathscr{S}$ be the collection of proper ideals containing I. The collection $\mathscr{S}$ is not empty since $I \in \mathscr{S}$. Let M be a maximal member of $\mathscr{S}$. I claim that M is a maximal ideal.

Suppose M is not a maximal ideal. Then there exists an ideal M' so that $M \subsetneq M' \subsetneq R$. But then $M' \in \mathscr{S}$, which contradicts the maximality of M in $\mathscr{S}$. So, M is a maximal ideal.

Since I and R are arbitrary, every proper ideal in a Noetherian ring is contained in a maximal ideal.

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) By Proposition 1, $V(Y - X^2)$ is irreducible if and only if $I(V(Y - X^2))$ is a prime ideal. Since $Y - X^2$ is irreducible, $(Y - X^2)$ is a prime ideal. So it suffices to prove the second statement: that $I(V(Y - X^2)) = (Y - X^2)$. It is clear that $(Y - X^2) \subseteq I(V(Y - X^2))$.

If G vanishes on $V(Y - X^2)$, then $V(Y - X^2) \cap V(G)$ is infinite. By Proposition 2 in Section 1.6, $Y - X^2$ and G must have a common factor. Since $Y - X^2$ is irreducible, $G \in (Y - X^2)$. So, $I(V(Y - X^2)) = (Y - X^2)$. It now follows that $V(Y - X^2)$ is irreducible.

(b) First, we have $Y^4 - X^2 = 0$, so $Y^2 - X = 0$ or $Y^2 + X = 0$. Both these polynomials are irreducible, so the irreducible components of $V(Y^4 - X^2)$ are $V(Y^2 - X)$ and $V(Y^2 + X)$—two smooth conics.

We can factor the second polynomial as

$$Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 + X)(Y - X)(Y + X). \tag{1.1}$$

Comparing these, we see that the variety $V(Y^2 + X)$ is contained in the variety in question.

If a point of $V(Y^4 - X^2Y^2 + XY^2 - X^3)$ is not in $V(Y^2 + X)$, we must have $Y^2 - X^2 = 0$, so that $Y^2 = X^2$. Since the point is not in $V(Y^2 + X)$, it must lie in $V(Y^2 - X)$, so $X = Y^2$. Substituting this into the equation $Y^2 - X^2 = 0$, we have

$$X - X^2 = X(1 - X) = 0.$$

This gives $X = 0$ or $X = 1$. Since $X = Y^2$, $X = 0$ gives the point $(0, 0)$, which is already in the other component. Since $X = Y^2$, $X = 1$ gives the points $(1, \pm 1)$.

So, we see that

$$V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) = V(Y^2 + X) \cup \{(1, \pm 1)\}.$$

This is the union of an irreducible curve and two points.

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

Solution. The polynomial $F = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ can be written $F = Y^2 + (X(X - 1))^2$, and over the complex numbers, this factors as

$$F = [Y + iX(X - 1)][Y - iX(X - 1)],$$

and each of these factors is irreducible over the complex numbers. Since $\mathbb{C}[X, Y]$ is a unique factorization domain and neither of these factors lies in $\mathbb{R}[X, Y]$, F is irreducible over $\mathbb{R}$.

Since we are working over the real numbers, $F = 0$ if and only if $Y = 0$ and $X(X - 1) = 0$. So, we see that $V(F) = \{(0, 0), (1, 0)\}$, which is reducible.

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

Solution. *Proof.* Let V, W be algebraic sets in $\mathbb{A}^n(k)$, $V \subset W$.

Let $W = \bigcup_{i=1}^n C_i$ be the decomposition of W into irreducible components.

Let C be any irreducible component of V. Then

$$C = \bigcup_{i=1}^{n} C_i \cap C$$

Since C is irreducible, $C = C_i \cap C$ for some $1 \leq i \leq n$. This says $C \subset C_i$. So, any irreducible component of V is contained in some 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 $V_i \not\subset \bigcup_{j \neq i} V_j$.

Solution. *Proof.* Let $V = V_1 \cup \cdots \cup V_r$ be the decomposition of an algebraic set into irreducible components.

Suppose $V_i \subset \bigcup_{j \neq i} V_j$. Then

$$V_i = \bigcup_{j \neq i} (V_i \cap V_j)$$

Since V_i is irreducible, $V_i = V_i \cap V_j \subset V_j$ for some $j \neq i$. But this contradicts the fact that $V = V_1 \cup \cdots \cup V_r$ is the decomposition. □

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

Solution. *Proof.* Suppose $F \in k[X_1, \ldots, X_n]$ vanishes on $\mathbb{A}^n(k)$. Then by Problem 1.4, $F \equiv 0$. So $I(\mathbb{A}^n(k)) = \{0\}$, which is a prime ideal in $k[X_1, \ldots, X_n]$. Hence $\mathbb{A}^n(k)$ is irreducible by Proposition 1. □

1.6 Algebraic Subsets of the Plane

Problems

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 $F \in \mathbb{R}[X, Y]$.

This indicates why we usually require that k be algebraically closed.

Solution. (a) Let $k = \mathbb{R}$. Since $X^2 + Y^2 + 1 = 0$ has no solution in $\mathbb{A}^2(\mathbb{R})$, $V(X^2 + Y^2 + 1) = \emptyset$. Thus $I(V(X^2 + Y^2 + 1)) = I(\emptyset) = \mathbb{R}[X, Y]$. That is, $I(V(X^2 + Y^2 + 1)) = (1)$.

(b) It is sufficient to show that irreducible algebraic subsets of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

By Corollary 2 in Section 1.6, the irreducible algebraic subsets of $\mathbb{A}^2(\mathbb{R})$ are singleton points, irreducible plane curves, the empty set, and all of $\mathbb{A}^2(\mathbb{R})$.

Certainly, irreducible plane curves, the empty set, and all of $\mathbb{A}^2(\mathbb{R})$ are of the form $V(F)$ for some $F \in \mathbb{R}[X, Y]$.

Let $S = \{(a, b)\}$ be a set of consisting of a point in $\mathbb{A}^2(\mathbb{R})$. Let $F(X, Y) = (X - a)^2 + (Y - b)^2$. Then

$$\begin{aligned} V(F) &= V\left((X-a)^2 + (Y-b)^2\right) \\ &= \{(a, b)\} \\ &= S. \end{aligned}$$

This proves the result.

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 $V(Y^2 - X(X^2 - 1))$, and for $V(X^3 + X - X^2Y - Y)$.

Solution. (a) We factor

$$Y^2 - XY - X^2Y + X^3 = (Y - X)(Y - X^2).$$

So, $V(Y^2 - XY - X^2Y + X^3)$ is the union of a line $Y = X$ and an irreducible conic $Y = X^2$ in either $\mathbb{A}^2(\mathbb{R})$ or $\mathbb{A}^2(\mathbb{C})$.

(b) Were the degree three polynomial $Y^2 - X(X^2 - 1)$ to factor, it would have to factor into the product of a linear polynomial and a quadratic polynomial. Then $V(Y^2 - X(X^2 - 1))$ would contain a line, which is doesn't. So, $Y^2 - X(X^2 - 1)$ is irreducible and $V(Y^2 - X(X^2 - 1))$ is an irreducible cubic in either $\mathbb{A}^2(\mathbb{R})$ or $\mathbb{A}^2(\mathbb{C})$ by Corollary 1.

We factor

$$X^3 + X - X^2Y - Y = (X - Y)(X^2 + 1).$$

So, $V(Y^2 - XY - X^2Y + X^3)$ is the line $Y = X$ in $\mathbb{A}^2(\mathbb{R})$.

In $\mathbb{A}^2(\mathbb{C})$, we have

$$X^3 + X - X^2Y - Y = (X - Y)(X^2 + 1) = (X - Y)(X + i)(X - i)).$$

So, $V(Y^2 - XY - X^2Y + X^3)$ is the union of three lines, $Y = X$, $X = \pm i$, in $\mathbb{A}^2(\mathbb{C})$.

1.7 Hilbert's Nullstellensatz

Problems

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

Solution. If $k = \mathbb{R}$, then $I = (X^2 + 1)$ is a proper ideal in $\mathbb{R}[X]$, but $V(I) = \emptyset$. This gives a counterexample to the Weak Nullstellensatz. Also, $I(V(I)) = I(\emptyset) = \mathbb{R}[X]$, which is not $\text{Rad}(I) = I$. This gives a counterexample to the Nullstellensatz and Corollary 1, since $I = (X^2 + 1)$ is a radical ideal. This also gives a counterexample to Corollary 3 since $I(V(X^2 + 1)) \neq (X^2 + 1)$.

The ideal $I = (X^2 + 1)$ is a maximal ideal in $\mathbb{R}[X]$, but $V(I) = \emptyset$ is not a point. This also gives a counterexample to Corollary 2.

Let $I = (X^2 + Y^2) \subset \mathbb{R}[X, Y]$. Then $V(I) = \{(0, 0)\}$. However, in the ring $\mathbb{R}[X, Y]/(X^2 + Y^2)$, the set $\{X^n \mid n \in \mathbb{N}\}$ is an infinite linearly independent set over $\mathbb{R}$. This gives a counterexample to Corollary 4.

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 $V = \{(t, t^2, t^3) \in \mathbb{A}^3(\mathbb{C}) \mid t \in \mathbb{C}\}$. Find $I(V)$, and show that V is irreducible.

Solution. I'm not sure these solutions are correct.

(a) For any point $(x, y, z) \in V(X^2 + Y^2 - 1, X^2 - Z^2 - 1)$, we must have $x^2 + y^2 - 1 = 0$ and $x^2 - z^2 - 1 = 0$. Subtracting these two equations, we have $y^2 + z^2 = 0$. So, the point must satisfy $y = \pm iz$. The variety $V(X^2 + Y^2 - 1, X^2 - Z^2 - 1)$ equals

$$V(X^2 + Y^2 - 1, (Y + iZ)(Y - iZ)) \\ = V(X^2 + Y^2 - 1, Y + iZ) \cup V(X^2 + Y^2 - 1, Y - iZ)$$

Each of the polynomials $Y \pm iZ$ defines a plane in $A^3(\mathbb{C})$. Intersecting this with the surface $X^2 + Y^2 - 1$ yields a nondegenerate conic in the plane. Hence, each of the components are irreducible.

(b) It's clear that $(Y - X^2, Z - X^3) \subset I(V)$. Let $F(X, Y, Z) \in I(V)$. We consider $F(X, Y, Z) \in \mathbb{C}(X, Y)[Z]$ and apply the Division Algorithm. There exist Q_1, $R_1 \in \mathbb{C}(X, Y)[Z]$ so that

$$F(X, Y, Z) = (Z - X^3)Q_1(X, Y, Z) + R_1$$

where the degree of R_1 is zero in Z. Hence, $R_1 \in \mathbb{C}(X, Y)$.

Since F is a polynomial, Q_1 and R_1 must also be polynomials, so $R_1 \in \mathbb{C}[X, Y]$.

We treat R_1 and an element of $\mathbb{C}(X)[Y]$. By the Division Algorithm, there exist Q_2, $R_2 \in \mathbb{C}(X)[Y]$ so that

$$R_1(X, Y) = (Y - X^2)Q_2(X, Y) + R_2$$

where the degree of R_2 is zero in Y. Hence, $R_2 \in \mathbb{C}(X)$. Since $R_1 \in \mathbb{C}[X, Y]$ is a polynomial, Q_2 and R_2 must also be polynomials, so $R_2 \in \mathbb{C}[X]$.

Now, we have

$$F(X, Y, Z) = (Z - X^3)Q_1(X, Y, Z) + (Y - X^2)Q_2(X, Y) + R_2(X).$$

Since this polynomial vanishes on the set $\{(t, t^2, t^3) \mid t \in \mathbb{C}\}$, we see that $R_2(t) = 0$ for all $t \in \mathbb{C}$. But this implies that $R_2 \equiv 0$. So, we have

$$F(X, Y, Z) = (Z - X^3)Q_1(X, Y, Z) + (Y - X^2)Q_2(X, Y),$$

so that $F(X, Y, Z) \in I(Y - X^2, Z - X^3)$. This proves that $I(V) = (Y - X^2, Z - X^3)$.

Now,

$$\mathbb{C}[X, Y, Z]/(Y - X^2, Z - X^3) \cong \mathbb{C}[X],$$

which is an integral domain, so $I(V) = (Y - X^2, Z - X^3)$ is prime and V is irreducible.

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) $X^2 - a \in R[X]$ is irreducible if and only if a is not a square in R.

Solution. Let R be a UFD.

(a) ($\Leftarrow$) Let F be a reducible monic polynomial of degree two or three $R[X]$. Since F is reducible, it has a factor. Since F has degree two or three, F must have a linear factor. Since F is monic, this linear factor must be monic. So, this F must have a factor of the form $X - \lambda$ for $\lambda \in R$. Then λ is a root of F.

($\Rightarrow$) Let F be a monic polynomial of degree two or three $R[X]$ and suppose F has a root λ in R.

Considering F as being in $K[X]$, where K is the field of fractions of R, and applying the Division Algorithm, we can write

$$F(X) = (X - \lambda)q(X) + r$$

where $q(X) \in K[X]$ and $r \in K$. Evaluating this equation at $X = \lambda$ and noting that λ is a root of F, we have $r = 0$ so that $F(X) = (X - \lambda)q(X)$. So, F is reducible in $K[X]$. By Gauss' Lemma, F is also reducible in $R[X]$.

(b) By part (a), $X^2 - a \in R[X]$ is irreducible if and only if it has no root in R. However, any root of this polynomial is a square root of a. So, $X^2 - a \in R[X]$ is irreducible if and only if a is not a square 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. By the previous problem, the polynomial $Y^2 - X(X-1)(X-\lambda)$ in $k[X,Y] = k[X][Y]$ is irreducible since $X(X-1)(X-\lambda)$ is not a square in $k[X]$.

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. It's easy to see that $I = (X^2, Y^2)$, so $V(I) = \{(0,0)\}$. The dimension of $\mathbb{C}[X,Y]/I$ over k is four, a basis being $\{1, X, Y, XY\}$.

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

Solution. *Proof.* If F has degree n, then $F(X) = \sum_0^n a_i X^i$ with $a_n \neq 0$. So

$$\overline{X}^n = -\sum_{i=0}^{n-1} (a_i/a_n)\overline{X}^i,$$

whereby $\overline{X}^n$ is in the span of $1, \overline{X}, \dots, \overline{X}^{n-1}$ over K in $K[X]/(F)$. An inductive argument now shows this set spans $K[X]/(F)$ over K.

If $\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}$ are dependent, then $\sum_{i=0}^{n-1} \lambda_i \overline{X}^i = 0$, so F divides $\sum_{i=0}^{n-1} \lambda_i X^i$. But this is impossible since $\deg(F) = n > n-1$. So $\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}$ is a basis for $K[X]/(F)$ over K. □

1.38. Let $R = k[X_1, \dots, X_n]$, 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 $k[X_1, \dots, X_n]/I$, and that irreducible algebraic sets (resp. points) correspond to prime ideals (resp. maximal ideals). (See Problem 1.22)

Solution. *Proof.* By Problem 1.22, radical ideals in $k[X_1, \dots, X_n]/I$ are in one-to-one correspondence with radical ideals in $k[X_1, \dots, X_n]$ containing I. By Corollary 1 to the Nullstellensatz, there is a one-to-one correspondence between radical ideals containing I and algebraic subsets of $V(I)$. Further, by Problem 1.22, prime and maximal ideals correspond to irreducible varieties and points, respectively. □

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) *Proof.* Let R be a UFD and let $P = (t)$ be a principal, proper, prime ideal. If $P = (0)$, there's nothing to prove, so we assume $t \neq 0$. Let Q be a nonzero prime ideal contained in P. For a nonzero $x \in Q$, we must have $x = t^n u$ for some $u \in R$ and $n \in \mathbb{N}$, with $t \nmid u$. Since Q is a prime ideal, either $t \in Q$ or $u \in Q$. Since t does not divide u, u is not in Q, so $t \in Q$. This shows that $Q = P$. □

(b) Let $V = V(F)$ be an irreducible hypersurface in $\mathbb{A}^n$. By Corollary 3, $I(V) = (F)$ and since $V(F)$ is irreducible, this ideal is a prime ideal. Suppose there is irreducible algebraic set W such that $V \subset W \subset \mathbb{A}^n$. Then we have $0 \subset I(W) \subset I(V) \subset k[X_1, \ldots, X_n]$. By part (a), $I(W) = 0$ or $I(W) = I(V)$. That is, $W = V$ or $W = \mathbb{A}^n$.

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 the $\mathrm{Ker}(\alpha) = I$, so I is prime, $V(I)$ is irreducible, and $I(V(I)) = I$.

Solution. (a) Let

$$F(X, Y, Z) = \sum_{ijk} a_{ijk} X^i Y^j Z^k.$$

be in $k[X, Y, Z]$. We group these terms into four groups following these rules:

(i) Terms with i even and j even.
(ii) Terms with i odd and j even.
(iii) Terms with i even and j odd.
(iv) Terms with i odd and j odd.

For terms of type (i), we have $a_{(2\ell)(2m)k} X^{2\ell} Y^{2m} Z^k$. Modulo I we can rewrite these terms as

$$\begin{aligned} a_{(2\ell)(2m)k} X^{2\ell} Y^{2m} Z^k &= a_{(2\ell)(2m)k} (X^2)^\ell (Y^2)^m Z^k \\ &= a_{(2\ell)(2m)k} (Y^3)^\ell (Z^3)^m Z^k \\ &= a_{(2\ell)(2m)k} Y^{3\ell} Z^{3m+k}. \end{aligned}$$

Now, if $\ell = 2p$ is even, say, we can write this as

$$\begin{aligned} a_{(4p)(2m)k} Y^{6p} Z^{3m+k} &= a_{(4p)(2m)k} (Y^6)^p Z^{3m+k} \\ &= a_{(4p)(2m)k} (Z^9)^p Z^{3m+k} \\ &= a_{(4p)(2m)k} Z^{9p+3m+k}. \end{aligned}$$

So, terms of this form can be expressed in terms solely in Z.

Now, if $\ell = 2p+1$ is odd, say, we can write this as

$$\begin{aligned} a_{(4p+2)(2m)k} Y^{6p+3} Z^{3m+k} &= a_{(4p+2)(2m)k} Y \cdot Y^{6p+2} Z^{3m+k} \\ &= a_{(4p+2)(2m)k} Y \cdot (Y^2)^{3p+1} Z^{3m+k} \\ &= a_{(4p+2)(2m)k} Y \cdot (Z^3)^{3p+1} Z^{3m+k} \\ &= a_{(4p+2)(2m)k} Y Z^{9p+3m+k+3}. \end{aligned}$$

So, terms of this form can be expressed Y times a power of Z.

For terms of type (ii), we have $a_{(2\ell+1)jk} X^{2\ell+1} Y^{2m} Z^k$. Modulo I we can rewrite these terms as

$$\begin{aligned} a_{(2\ell+1)jk} X^{2\ell+1} Y^{2m} Z^k &= a_{(2\ell+1)jk} X \cdot X^{2\ell} Y^{2m} Z^k \\ &= a_{(2\ell+1)jk} X \cdot (X^2)^\ell Y^{2m} Z^k \\ &= a_{(2\ell+1)jk} X \cdot (Y^3)^\ell Y^{2m} Z^k \\ &= a_{(2\ell+1)jk} X Y^{2m+3\ell} Z^k \end{aligned}$$

Now, if $\ell = 2p$ is even, say, we can write this as

$$\begin{aligned} a_{(4p+1)jk} X Y^{2m+6p} Z^k &= a_{(4p+1)jk} X (Y^2)^m (Y^6)^p Z^k \\ &= a_{(4p+1)jk} X (Z^3)^m (Z^9)^p Z^k \\ &= a_{(4p+1)jk} X Z^{3m+9p+k}. \end{aligned}$$

So, terms of this form can be expressed X times a power of Z.

Now, if $\ell = 2p+1$ is odd, say, we can write this as

$$\begin{aligned} a_{(2\ell+1)jk} X Y^{2m+6p+3} Z^k &= a_{(2\ell+1)jk} X (Y^6)^p (Y^2)^m (Y^2) Y Z^k \\ &= a_{(2\ell+1)jk} X (Z^9)^p (Z^3)^m (Z^3) Y Z^k \\ &= a_{(2\ell+1)jk} X Y Z^{9p+3m+3} \end{aligned}$$

So, terms of this form can be expressed XY times a power of Z.

For terms of type (iii), we have $a_{(2\ell)(2m+1)k} X^{2\ell} Y^{2m+1} Z^k$. Modulo I we can rewrite these terms as

$$\begin{aligned}
a_{(2\ell)(2m+1)k}X^{2\ell}Y^{2m+1}Z^k &= a_{(2\ell)(2m+1)k}YX^{2\ell}Y^{2m}Z^k \\
&= a_{(2\ell)(2m+1)k}Y(X^2)^\ell(Y^2)^mZ^k \\
&= a_{(2\ell)(2m+1)k}Y(Y^3)^\ell(Z^3)^mZ^k \\
&= a_{(2\ell)(2m+1)k}Y(Y^{3\ell})Z^{3m+k}
\end{aligned}$$

Now, if $\ell = 2p$ is even, say, we can write this as

$$\begin{aligned}
a_{(2\ell)(2m+1)k}Y(Y^{3\ell})Z^{3m+k} &= a_{(6p)(2m+1)k}Y(Y^{6p})Z^{3m+k} \\
&= a_{(6p)(2m+1)k}Y(Y^6)^pZ^{3m+k} \\
&= a_{(6p)(2m+1)k}Y(Z^9)^pZ^{3m+k} \\
&= a_{(6p)(2m+1)k}YZ^{9p+3m+k}.
\end{aligned}$$

So, terms of this form can be expressed Y times a power of Z.

Now, if $\ell = 2p + 1$ is odd, say, we can write this as

$$\begin{aligned}
a_{(2\ell)(2m+1)k}XY(Y^{3\ell})Z^{3m+k} &= a_{(4p+2)(2m+1)k}XY(Y^{6p+3})Z^{3m+k} \\
&= a_{(4p+2)(2m+1)k}XY(Y^6)^pY^3Z^{3m+k} \\
&= a_{(4p+2)(2m+1)k}X(Y^6)^pY^4Z^{3m+k} \\
&= a_{(4p+2)(2m+1)k}X(Y^6)^p(Y^2)^2Z^{3m+k} \\
&= a_{(4p+2)(2m+1)k}X(Z^9)^p(Z^3)^2Z^{3m+k} \\
&= a_{(4p+2)(2m+1)k}XZ^{9p+3m+k+6}.
\end{aligned}$$

So, terms of this form can be expressed X times a power of Z.

For terms of type (iv), we have $a_{(2\ell+1)(2m+1)k}X^{2\ell+1}Y^{2m+1}Z^k$. Modulo I we can rewrite these terms as

$$\begin{aligned}
a_{(2\ell+1)(2m+1)k}X^{2\ell+1}Y^{2m+1}Z^k &= a_{(2\ell+1)(2m+1)k}XYX^{2\ell}Y^{2m}Z^k \\
&= a_{(2\ell+1)(2m+1)k}XY(X^2)^\ell(Y^2)^mZ^k \\
&= a_{(2\ell+1)(2m+1)k}XY(Y^3)^\ell(Z^3)^mZ^k \\
&= a_{(2\ell+1)(2m+1)k}XY(Y^{3\ell})Z^{3m+k}
\end{aligned}$$

Now, if $\ell = 2p$ is even, say, we can write this as

$$\begin{aligned}
a_{(2\ell)(2m+1)k}XY(Y^{3\ell})Z^{3m+k} &= a_{(6p)(2m+1)k}XY(Y^{6p})Z^{3m+k} \\
&= a_{(6p)(2m+1)k}XY(Y^6)^pZ^{3m+k} \\
&= a_{(6p)(2m+1)k}XY(Z^9)^pZ^{3m+k} \\
&= a_{(6p)(2m+1)k}XYZ^{9p+3m+k}.
\end{aligned}$$

So, terms of this form can be expressed XY times a power of Z.

Now, if $\ell = 2p+1$ is odd, say, we can write this as

$$\begin{aligned} a_{(2\ell)(2m+1)k}XY(Y^{3\ell})Z^{3m+k} &= a_{(4p+2)(2m+1)k}XY(Y^{6p+3})Z^{3m+k} \\ &= a_{(4p+2)(2m+1)k}XY(Y^6)^pY^3Z^{3m+k} \\ &= a_{(4p+2)(2m+1)k}X(Y^6)^pY^4Z^{3m+k} \\ &= a_{(4p+2)(2m+1)k}X(Y^6)^p(Y^2)^2Z^{3m+k} \\ &= a_{(4p+2)(2m+1)k}X(Z^9)^p(Z^3)^2Z^{3m+k} \\ &= a_{(4p+2)(2m+1)k}XZ^{9p+3m+k+6}. \end{aligned}$$

So, terms of this form can be expressed X times a power of Z.

It now follows 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) Suppose $F = A + XB + YC + XYD$, $A, B, C, D \in k[Z]$ is in the kernel of α. Then

$$0 = \alpha(F) = A(T^4) + T^9B(T^4) + T^6C(T^4)) + T^{15}D(T^4).$$

Looking only at the terms where the power of T is congruent to zero mod four, we have $A(T^4) = 0$, so $A = 0$. Looking only at the terms where the power of T is congruent to one mod four, we have $T^9B(T^4) = 0$, so $B = 0$. Looking only at the terms where the power of T is congruent to two mod four, we have $T^6C(T^4) = 0$, so $C = 0$. Looking only at the terms where the power of T is congruent to three mod four, we have $T^{15}D(T^4) = 0$, so $D = 0$. Hence, $F = 0$.

(c) Since $\alpha(X^2 - Y^3) = (T^9)^2 - (T^6)^3 = 0$ and $\alpha(Y^2 - Z^3) = (T^6)^2 - (T^4)^3 = 0$, we see that $I \subset \ker\alpha$.

Suppose $F \in \ker\alpha$. Modulo I, F is congruent to $A + XB + YC + XYD$. We have

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

By part (b), $A + XB + YC + XYD = 0$. But then F is congruent to 0 mod I, so $F \in I$. This proves that $\mathrm{Ker}(\alpha) = I$.

1.8 Modules; Finiteness Conditions

Problems

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

Solution. *Proof.* If $S = \sum Rs_i$, then $S = R[s_1, \ldots, s_n]$, so S is ring finite over R. $\square$

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

Solution. Let $S = R[X]$ (the ring of polynomials in one variable). The ring S is ring-finite by definition. The elements $\{X^n \mid n = 0, 1, 2, \ldots\}$ is an infinite set that is linearly independent over R, so 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. *Proof.* Since L is ring-finite over K, there are elements $\ell_1, \ldots, \ell_n \in L$ so that $L = K[\ell_1, \ldots, \ell_n]$. Since L is a field, we must have $L = K[\ell_1, \ldots, \ell_n] = K(\ell_1, \ldots, \ell_n)$, so L is a finitely generated field extension of K. $\square$

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, there 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. *Proof.* $L = K(X)$ is a finitely generated field extension of K by definition. If L is a ring-finite extension of K, there exist elements $\ell_1, \ldots, \ell_n \in L$ so that $L = K[\ell_1, \ldots, \ell_n] = K(X)$. Suppose $\ell_i = f_i/g_i$ with $f_i, g_i \in K[X]$. Let $b = \prod_{i=1}^n g_i$. Then for any $z \in L$, there is a natural number n so that $b^n z \in K[X]$.

Now, choose $z = 1/c$ where $c \in K[X]$ is irreducible and c does not divide b in $K[X]$. Then $b^n z \notin K[X]$ for any n. This contradiction shows that $L = K(X)$ is not ring-finite over K. $\square$

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 $T = \sum Rv_i w_j$.

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

$$T = R[v_1, \ldots, v_n, w_1, \ldots, w_m].$$

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

So each of the three finiteness conditions is a transitive relation.

Solution. *Proof.* Let $t \in T$. Then $t = \sum s_i w_i$ for some $s_i \in S$. For each i, $s_i = \sum r_{ij} v_j$, for some $r_{ij} \in R$. Hence $t = \sum_{ij} r_{ij} v_j w_i$. This shows $T = \sum Rv_i w_j$.

The other two results are shown similarly. $\square$

1.9 Integral Elements

Problems

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 $z \in T$, $z^n + a_1 z^{n-1} + \cdots + a_n = 0$, $a_i \in S$. Then $R[a_1, \ldots, a_n, z]$ is module-finite over R.)

Solution. *Proof.* Let R be a subring of S, S a subring of (a domain) T, so that S is integral over R and T is integral over S. Let $z \in T$. Then $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ with $a_1, \ldots, a_n \in S$. Then, since S is integral over R, $R[a_1, \ldots, a_n]$ is module-finite over R. Since z is integral over $R[a_1, \ldots, a_n]$, $R[a_1, \ldots, a_n, z]$ is module-finite over $R[a_1, \ldots, a_n]$. Hence, by Problem 1.45, $R[a_1, \ldots, a_n, z]$ is module-finite over R, so z is integral over R. Since $z \in T$ is arbitrary, 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. *Proof.* Let S be a domain which is ring-finite over R.

($\Rightarrow$) Suppose S is module-finite over R and let $z \in S$. Then S is a subring of itself which is module-finite over R, so z is integral over R, by Proposition 3. Since $z \in S$ is arbitrary, S is integral over R.

($\Leftarrow$) Suppose S is integral over R. Since S is ring-finite over R by hypothesis, suppose $S = R[s_1, \ldots, s_n]$, for some $s_1, \ldots, s_n \in S$. Since S is integral over R, each s_i is integral over R, so $R[s_i]$ is module-finite over R. Hence we have a chain

$$R \subset R[s_1] \subset R[s_1, s_2] \subset \cdots \subset R[s_1, \ldots, s_n] = S,$$

with each element of the chain after the first module-finite over its predecessor. By transitivity of module finiteness from Problem 1.45(a), S is module-finite over R. □

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) *Proof.* Suppose $z \in L$ is algebraic over k. So $a_n z^n + \cdots + a_0 = 0$ for some $a_i \in k$. Consider $F(X) = a_n X^n + \cdots + a_0$ in $k[X]$. Since k is algebraically closed, $F(X)$ factors into linear terms $F(X) = \epsilon \prod_{i=1}^{n}(X - \lambda_i)$, with $\epsilon, \lambda_i \in k$. Since $F(z) = 0$, we see that $z = \lambda_i$ for some i, so $z \in k$. □

(b) *Proof.* Suppose L is a module-finite field extension of k. By Problem 1.47, every element of L is algebraic over k, hence, by (a), is in k. So $L = k$. □

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 which 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) *Proof.* Let $z \in L$ be integral over $K[X]$. Write $z = F/G$ with $F, G \in K[X]$ relatively prime. Then, if z satisfies the relation $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ for $a_1 \ldots, a_n \in k[X]$, then $F^n + a_1 F^{n-1} G + a_n G^n = 0$. So G must divide F. Since F and G are relatively prime by assumption, G must be a unit in $k[X]$. It follows that $z \in k[X]$. □

(b) *Proof.* Suppose there is a nonzero F so that for every $z \in L$, $F^n z$ is integral over $K[X]$ for some $n > 0$. Let $z = 1/G$, where G is irreducible and G does not divide F. Then since $F^n/G \in L$ is presumed integral over $k[X]$, it must be in $k[X]$ by part (a). But since G is irreducible and does not divide F, this is impossible. □

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 $v(v^{n-1} + \ldots) = -a_n$.)

(b) Suppose L is module-finite over K, and $K \subset R \subset L$. Show that R is a field.

Solution. (a) *Proof.* Let $S = \{\ell \in L \,|\, \ell \text{ is algebraic over } K\}$. Certainly $S \supset K$. Let $\ell \in S$, $\ell \neq 0$. Then

$$a_n \ell^n + \cdots + a_0 = 0,$$

where $a_i \in K$, $a_n \neq 0$. If we take this polynomial to be irreducible, then we have $a_0 \neq 0$. Then

$$1 = \ell \left[-\frac{a_n}{a_0} \left(\ell^{n-1} + \frac{a_{n-1}}{a_n} \ell^{n-2} + \cdots + \frac{a_1}{a_n} \right) \right].$$

Since S is a ring over K, we see $\ell \in S$ is invertible, so S is a field. □

(b) *Proof.* Let $r \in R$, $r \neq 0$. Since $R \subset L$ and L is module-finite over K, r is integral over K. So there is a equation

$$r^n + a_1 r^{n-1} + \cdots + a_n = 0$$

with $a_n \neq 0$. Then

$$1 = r \cdot \left[\left(\frac{-1}{a_n} \right) (r^{n-1} + \cdots + a_{n-1}) \right],$$

so r is invertible. Hence R is a field. □

1.10 Field Extensions

Problems

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' which 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. Let K be a field, $F \in K[X]$ an irreducible monic polynomial of degree $n > 0$.

(a) *Proof.* $F(x)$ is the residue of $F(X)$ in L, but this is zero. Since F is irreducible, (F) is maximal, so L is a field. □

(b) *Proof.* Let $L' \supset K$ be a field extension, $y \in L'$ with $F(y) = 0$. There is a homomorphism $K[X] \to K[y] \subset L'$ taking X to y extending the inclusion $K \hookrightarrow L'$. Since $F(y) = 0$, this homomorphism factors through L. So, we have $\varphi : L \to K[y]$. The kernel of φ is a prime ideal in L, a field, so it must be the zero ideal. Also, since $F(y) = 0$ with $F \in K[X]$, y is algebraic over K, $K[y] = K(y)$. Thus $\varphi : L \to K(y)$ is an isomorphism. □

(c) *Proof.* Suppose $y \in L'$ induces $\varphi : L \to L'$. Say $G(y) = 0$ with $G \in K[X]$. Then the image of $\overline{G(X)}$ in L' is zero, and we know this map is injective, so $\overline{G(X)} = 0$ in L, whereby F divides G. □

(d) *Proof.* Let x be the residue of X in $L = K[X]/(F)$. Then we know that $F(x) = 0$ in L. By the Factor Theorem, since x is a root of F (in L), $X - x$ is a factor of F (in $L[X]$). So there exists $F_1 \in L[X]$ with $F = (X - x)F_1$, $F_1 \in L[X]$. □

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. *Proof.* We may assume F is irreducible in $K[X]$ and of degree at least two. Let $L = K[X]/(F)$. By Problem 51(a), L is an extension field of K, $F(x) = 0$, and by Problem 51(d), $F = (X - x)F_1$ with $F_1 \in L[x]$. Since $\deg F_1 < \deg F$, induction on the degree completes the proof. □

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. *Proof.* Let $G = \dfrac{\partial F}{\partial X}$. If F has multiple roots, then F and G share a root, say y. Then $G(y) = 0$, and by Problem 51(c), F divides G. But $\deg G < \deg F$, so this is impossible. □

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 $v_1, \ldots, v_n$ for L over K (as a vector space) such that each v_i is integral over R.

Solution. Let R be a domain with quotient field K, and let L be a finite algebraic extension of K.

(a) *Proof.* Let v be in L. Then v is algebraic over K, so $a_0v^n + a_1v^{n-1} + \cdots + a_n = 0$, with $a_i \in K$. Let $z \in R$ be the product of all the denominators in the a_i's. Let $a = a_0^{n-1}z^n \in R$. We have

$$\begin{aligned}
a_0v^n + a_1v^{n-1} + \cdots + a_n &= 0 \\
a(a_0v^n + a_1v^{n-1} + \cdots + a_n) &= 0 \\
a_0^{n-1}z^na_0v^n + a_0^{n-1}z^na_1v^{n-1} + \cdots + a_0^{n-1}z^na_{n-1}v + a_0^{n-1}z^na_n &= 0 \\
(a_0zv)^n + a_1z(a_0zv)^{n-1} + \cdots + a_0^{n-2}a_{n-1}z^{n-1}(a_0zv) + a_0^{n-1}z^na_n &= 0
\end{aligned}$$

We see that $y = a_0zv$ satisfies the equation $y^n + b_1y^{n-1} + \cdots + b_n = 0$, where $b_i \in R$ for all i. So it is integral over R. □

(b) *Proof.* Let $w_1, \ldots, w_n$ be a basis for L over K (as a vector space). Since L is finite dimensional over K, each w_i is algebraic over K. By Problem 54(a), there exist a_i so that $a_i w_i$ is integral over R. Let $v_i = a_i w_i$. Then $v_1, \ldots, v_n$ is a basis for L over K with v_i integral over R for all i. □

Chapter 2

Affine Varieties

2.1 Coordinate Rings

Problems

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

Solution. *Proof.* Let V be a variety. Define a map φ taking $F \in k[X_1, \ldots, X_n]$ to a polynomial function by restriction to V:

$$\varphi : k[X_1, \ldots, X_n] \to \Gamma(V)$$
$$\varphi(F) \mapsto F|_V.$$

For F, $G \in k[X_1, \ldots, X_n]$, $(F + G)_V = F|_V + G|_V$ and $(FG)_V = F|_V G|_V$. So, φ is a ring homomorphism. Since every regular function is the restriction of a polynomial defined on all of $\mathbb{A}^n$, this mapping is surjective. The kernel of this mapping is all polynomials whose restriction to V is identically zero, i.e. $I(V)$. So, $\Gamma(V) \cong k[X_1, \ldots, X_n]/I(V)$. □

2.2. Let $V \subset \mathbb{A}^n$ be a variety. A *subvariety* of V is a variety $W \subset \mathbb{A}^n$ which 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. *Proof.* Let $V \subset \mathbb{A}^n$ be a variety with ideal $I(V)$. It is a fundamental fact of ring theory that ideals in $k[X_1, \ldots, X_n]$ containing $I(V)$ are in one-to-one correspondence with ideals in $\Gamma(V) = k[X_1, \ldots, X_n]/I(V)$, and radical ideals (resp. prime ideals, maximal ideals) correspond to radical ideals (resp. prime ideals, maximal ideals). Hence, there is a one-to-one correspondence between radical ideals (resp. prime ideals, maximal ideals) in $k[X_1, \ldots, X_n]$ containing $I(V)$ and radical ideals (resp. prime ideals, maximal ideals) in $\Gamma(V)$. But by Chapter 1, Section 3, there is one-to-one correspondence between algebraic subsets (resp. varieties, points) of V and radical (resp. prime ideals, maximal ideals) ideals in $k[X_1, \ldots, X_n]$ containing $I(V)$.

Hence, there is a one-to-one correspondence of radical ideals in $\Gamma(V)$ and algebraic subsets of V, a one-to-one correspondence of prime ideals in $\Gamma(V)$ and subvarieties of V, and a one-to-one correspondence of maximal ideals in $\Gamma(V)$ and points in of V.

□

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 $I_V(W)$, so that $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$.

Solution. Let W be a subvariety of a variety V, and let $I_V(W)$ be the ideal of $\Gamma(V)$ corresponding to W.

(a) *Proof.* Let $f \in \Gamma(V)$. Then f, as an equivalence class of polynomials, is represented by a polynomial $F \in k[X_1, \ldots, X_n]$. Then $F|_W$ is a regular function on W by definition. So, f restricted to W is a regular function on W. □

(b) *Proof.* Let $\varphi : \Gamma(V) \to \Gamma(W)$ be the restriction map in part (a). It's easy to see that φ is a ring homomorphism.

First, let $f \in \Gamma(W)$. Then f, as an equivalence class of polynomials, is represented by a polynomial $F \in k[X_1, \ldots, X_n]$. The polynomial F, when restricted to V, gives a regular function on V which restricts to f. This shows φ is surjective.

Let $f \in \Gamma(V)$ be in the kernel of φ. Then f, as an equivalence class of polynomials, is represented by a polynomial $F \in k[X_1, \ldots, X_n]$. Since f lies in the kernel of φ, $F|_W$ is zero. This says $f|_W \equiv 0$, so $f \in I_V(W)$. The reverse inclusion is similar. So, $\text{Ker}(\varphi) = I_V(W)$.

By the first isomorphism theorem, $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$. □

2.4. Let $V \subset \mathbb{A}^n$ be a nonempty a variety. Show that the following are equivalent:

(i) V is a point;

(ii) $\Gamma(V) = k$;

(iii) $\dim_k(\Gamma(V)) < \infty$.

Solution. *Proof.* (i)⇒(ii):
Suppose V is a point $(a_1, \ldots, a_n)$. Then $I(V) = (x_1 - a_1, \ldots, x_n - a_n)$ and $\Gamma(V) = k[X_1, \ldots, X_n]/I(V) = k$ by the Nullstellensatz.

(ii)⇒(iii):
Suppose $\Gamma(V) = k$. Then $\dim_k(\Gamma(V)) = \dim_k(k) = 1$.

(iii)⇒(i): Suppose $\dim_k(\Gamma(V)) < \infty$. Since $\dim_k(\Gamma(V)) < \infty$, $k(V)$, the quotient field of $\Gamma(V)$, is also finite dimensional over k. Hence $k(V)$ is algebraic over k. Since k is algebraically closed, this means $k(V)$ is isomorphic to k. Hence, for each x_i there is $a_i \in k$ such that $x_i \equiv a_i \mod I(V)$. Since $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal, we have $I(V) = (x_1 - a_1, \ldots, x_n - a_n)$, so that V is the point $(a_1, \ldots, a_n)$. □

2.5. Let F be an irreducible polynomial in $k[X, Y]$, and suppose F is monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \ldots$, 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 $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ generate $\Gamma(V)$ over $k[X]$ as a module.

Solution. *Proof.* Let F be an irreducible polynomial in $k[X, Y]$, and suppose F is monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \ldots$, with $n > 0$. Let $V = V(F) \subset \mathbb{A}^2$.

Define $\varphi : k[X] \to \Gamma(V) = k[X, Y]/(F)$ by taking a polynomial in $k[X]$ to its equivalence class of the polynomial in $\Gamma(V)$. Suppose $\varphi(p) = 0$. Then F divides p. Since Y^n, $n > 0$, appears in F and $p \in k[X]$, this is only possible if $p = 0$. So the map φ is injective. This means we may consider $k[X]$ as a subring of $\Gamma(V)$.

We note that in $\Gamma(V) = k[X, Y]/(F)$

$$0 = \overline{F} = \overline{Y}^n + a_1(X)\overline{Y}^{n-1} + \cdots + a_{n-1}(X)\overline{Y} + a_n(X)$$

so $\overline{Y}^n$ is dependent on $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ over $k[X]$. By induction, $\overline{Y}^m$ is dependent on $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ over $k[X]$ for all $m \geq n$. This shows $\Gamma(V)$ is generated by $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ over $k[X]$.

□

2.2 Polynomial Maps

Problems

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

Solution. *Proof.* Let $\varphi : V \to W$, $\psi : W \to Z$ be polynomial maps of varieties. Then φ induces $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$, ψ induces $\widetilde{\psi} : \Gamma(Z) \to \Gamma(W)$, and $\psi \circ \varphi$ induces $\widetilde{\psi \circ \varphi} : \Gamma(Z) \to \Gamma(V)$.

Let $f \in \Gamma(Z)$ and let F be any polynomial representing f. Then

$$\begin{aligned}\widetilde{\psi \circ \varphi}(f) &= F \circ \psi \circ \varphi|_V \\ &= \widetilde{\varphi}(F \circ \psi)|_V \\ &= \widetilde{\varphi}(\widetilde{\psi}(F))|_V \\ &= \widetilde{\varphi} \circ \widetilde{\psi}(f).\end{aligned}$$

Hence $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$. □

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. *Proof.* Let $\varphi : V \to W$ is a polynomial map, and X is an algebraic subset of W.

Suppose $X = V(F_1, \ldots, F_n)$ for $F_1, \ldots, F_n \in k[X_1, \ldots, X_n]$. Suppose φ is given by polynomials $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$.

The point $P = (P_1, \ldots, P_n)$ is in $\varphi^{-1}(X)$ if and only if $\varphi(P_1, \ldots, P_n)$ is in X. This happens if and only if $(T_1(P_1, \ldots, P_n), \ldots, T_m(P_1, \ldots, P_n))$ is in X. This happens if and only if $F_i(T_1(P_1, \ldots, P_n), \ldots, T_m(P_1, \ldots, P_n) = 0$ for all $1 \le i \le n$. This happens if and only if $F_i(T_1, \ldots, T_m)$ is zero on $(P_1, \ldots, P_n)$ for all $1 \le i \le n$. But this says $\varphi^{-1}(X)$ is cut out by

$$F_1(T_1, \ldots, T_m), \ldots, F_n(T_1, \ldots, T_m).$$

Since F_i and T_j are polynomials for all i, j, $\varphi^{-1}(X)$ is an algebraic set.

Suppose X is contained in the image of φ and $\varphi^{-1}(X)$ is irreducible. Then $I = (F_1(T_1, \ldots, T_m), \ldots, F_n(T_1, \ldots, T_m))$ is a prime ideal in $\Gamma(V)$, where we purposefully identify the polynomials $F_i(T_1, \ldots, T_m)$ with the regular functions they define on V. Since the inverse image of a prime ideal under a homomorphism is also a prime ideal, $J = \widetilde{\varphi}^{-1}(I)$ is likewise a prime ideal. But $\widetilde{\varphi}^{-1}(I) = (F_1, \ldots, F_n)$, so that $V(J) = X$. This shows 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) *Proof.* Let $\varphi : \mathbb{A}^1(k) \to \mathbb{A}^3(k)$ be defined by $\varphi(t) = (t, t^2, t^3)$. The image of this map is the set V in question. Since $\varphi^{-1}(V) = \mathbb{A}^1(k)$, which is irreducible, V is irreducible by the result of the last problem. □

(b) *Proof.* Let $\varphi : \mathbb{A}^1(k) \to \mathbb{A}^3(k)$ by $\varphi(t) = (t^{12}, t^{16}, t^{20})$. We'll show that the image of φ is $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$.

For $P = \varphi(t) = (t^{12}, t^{16}, t^{20})$, we have

$$\begin{aligned} XZ - Y^2 &= t^{12} \cdot t^{20} - (t^{16})^2 = 0 \\ YZ - X^3 &= t^{16} \cdot t^{20} - (t^{12})^3 = 0 \\ Z^2 - X^2Y &= (t^{20})^2 - (t^{12})^2 \cdot t^{16} = 0. \end{aligned}$$

So, the image of φ is contained in $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$.

On the other hand, suppose $P = (a, b, c) \in V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$. Then

$$ac = b^2 \tag{2.1}$$
$$bc = a^3 \tag{2.2}$$
$$c^2 = a^2 b. \tag{2.3}$$

Solving (2.1) and (2.2) for c and doing some algebra, we get $a^4 = b^3$. Solving (2.2) and (2.3) for b and doing some algebra, we get $a^5 = c^3$. Now, let $a = t^{12}$, then $P = (t^{12}, t^{16}, t^{20}) = \varphi(t)$. This shows $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$ is contained in the image of φ.

Since φ is a polynomial map onto $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$ and $\mathbb{A}^1(k)$ is irreducible, $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$ is irreducible by the result of the last problem. □

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 $\widetilde{\varphi}(I_W(W')) \subset I_V(V')$ (See Problem 2.3).

(b) Show that the restriction of φ gives a polynomial map from V' to W'.

Solution. 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) *Proof.* By Problem 2.3, the regular map $\varphi : V \to W$ restricted to V' is also a polynomial map, which we also call φ. So, we have $\varphi : V' \to W$. Since $\varphi(V') \subset W'$ and φ remains a polynomial map, we have that $\varphi : V' \to W'$, whereby $\widetilde{\varphi} : \Gamma(W') \to \Gamma(V')$. By Problem 2.3, $\Gamma(V') \cong \Gamma(V)/I_V(V')$ and $\Gamma(W') \cong \Gamma(W)/I_W(W')$. So,

$$\widetilde{\varphi} : \Gamma(W') \cong \Gamma(W)/I_W(W') \to \Gamma(V') \cong \Gamma(V)/I_V(V'),$$

we must have $\widetilde{\varphi}(I_W(W')) \subset I_V(V')$

□

(b) *Proof.* We showed this in part (a).

□

2.10. Show that the *projection map* $\text{pr} : \mathbb{A}^n \to \mathbb{A}^r$, $n \geq r$, defined by

$$\text{pr}(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$$

is a polynomial map.

Solution. *Proof.* In the projection map $\text{pr} : \mathbb{A}^n \to \mathbb{A}^r$, $n \geq r$, defined by

$$\text{pr}(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$$

every coefficient function is a polynomial in $a_1, \ldots, a_n$. So, pr is a polynomial map. □

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

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

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

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

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

the graph of f.

Suppose V is the zero set of the functions $F_1, \ldots, F_m$ in $k[X_1, \ldots, X_n]$.

Since f is in $\Gamma(V)$, f is the residue of some F in $k[X_1, \ldots, X_n]$. The graph $G(f)$ is the zero locus of the set

$$\{F_1, \ldots, F_m, X_{n+1} - F(X_1, \ldots, X_n)\},$$

so $G(f)$ is an algebraic set.

Define a map $\varphi : V \to G(f)$ by $(a_1, \ldots, a_n) \to (a_1, \ldots, a_n, f(a_1, \ldots, a_n))$. Since the coordinate functions are regular functions, this map is regular. By Problem 2.7, since V is a variety and φ is surjective, $G(f)$ is irreducible. So, $G(f)$ is a variety. The inverse map to φ is the projection map $\text{pr}(a_1, \ldots, a_n, a_{n+1}) = (a_1, \ldots, a_n)$. So, $G(f)$ is isomorphic to V. □

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: $\widetilde{\varphi}(\Gamma(V)) = k[T^2, T^3] \subset k[T] = \Gamma(\mathbb{A}^1)$.)

(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. Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^3) \subset \mathbb{A}^2$ be defined by $\varphi(t) = (t^2, t^3)$.

(a) *Proof.* Suppose $\varphi(t) = \varphi(s)$. Then $t^2 = s^2$ and $t^3 = s^3$. These imply that $t = s$, so φ is injective.

Let $P = (a, b)$ be on $V(Y^2 - X^3)$. If $a = 0$, the $\varphi(0) = (0, 0) = P$. If $a \neq 0$, let $t = b/a$. Then $t^2 = b^2/a^2 = a^3/a^2 = a$, since $a^3 = b^2$. Then, $\phi(t) = (t^2, t^3) = (a, b) = P$. So, φ is surjective.

However, $\widetilde{\varphi}(\Gamma(V)) = k[T^2, T^3] \subset k[T]$. The polynomial T is integral over $k[T^2, T^3]$, but doesn't lie in $k[T^2, T^3]$, so $k[T^2, T^3]$ is not integrally closed in $k(T)$. But $k[T]$ is integrally closed in $k(T)$, so $k[T^2, T^3]$ is properly contained in $k[T]$. So, φ is not an isomorphism. $\square$

(b) *Proof.* Let $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^2(X + 1))$ be defined by $\varphi(t) = (t^2 - 1, t(t^2 - 1))$. Define $\psi : V \to \mathbb{A}^1$ by $\psi(X, Y) = Y/X$. The maps φ and ψ are inverse regular maps on $\mathbb{A}^1 \setminus \{\pm 1\}$ and $V \setminus \{(0, 0)\}$, respectively. Consequently, φ is one-to-one and onto this set. It's easy to check that $\varphi(\pm 1) = (0, 0)$. $\square$

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 $\widetilde{f} = \overline{\alpha}$?

(b) Show that f is one-to-one and onto, but not an isomorphism.

Solution. 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 $\alpha(X) = T^9$, $\alpha(Y) = T^6$, $\alpha(Z) = T^4$. Since the ideal $(X^2 - Y^3, Y^2 - Z^3)$ is contained in the kernel of α, α induces $\overline{\alpha} : \Gamma(V) \to k[T]$.

(a) *Proof.* The polynomial map $f : \mathbb{A}^1 \to V$ is given by $f(t) = (t^9, t^6, t^4)$. Then

$$\tilde{f} : \Gamma(V) \to \Gamma(\mathbb{A}^1) \cong k[t]$$

is given by $\tilde{f}(g)(t) = g(t^9, t^6, t^4)$. Then

$$\begin{aligned}\tilde{f}(g)(t) = g(f(t)) &= g(t^9, t^6, t^4) \\ &= g(\alpha(X), \alpha(Y), \alpha(Z)) = \alpha(g(X, Y, Z)) = \overline{\alpha}(g)(t).\end{aligned}$$

So, $\widetilde{f} = \overline{\alpha}$. $\square$

(b) *Proof.* Suppose $f : \mathbb{A}^1 \to V$ is given by $f(t) = (t^9, t^6, t^4)$. Then if $X \neq 0$, $Y \neq 0$, or $Z \neq 0$, then all three are nonzero and

$$t = XZ/Y^2 = YZ/X = X/Z^2, \tag{2.4}$$

so f is one-to-one provided $X \neq 0$. On the other hand, If $X = 0$, then $X = Y = Z = 0$, and then $t = 0$, so f is injective.

We have $f(0) = (0, 0, 0)$. Otherwise, X, Y, and Z are not zero. In this case, we let $t = XZ/Y^2$. By Equations 2.4, $f(t) = (X, Y, Z)$. This shows f is surjective.

The image of $\overline{\alpha}$ in $k[T]$ is $k[T^4, T^6, T^9]$. The element T is integral over $k[T^4, T^6, T^9]$, but does not lie in it, so $k[T^4, T^6, T^9]$ is not integrally closed in $k(T)$. Since $k[T]$ is integrally closed in $k(T)$, it follows that f is not an isomorphism. □

2.3 Coordinate Changes

Problems

2.14. A set $V \subset \mathbb{A}^n(k)$ is called a *linear subvariety* of $\mathbb{A}^n(k)$ if $V = V(F_1, \ldots, F_r)$ for some polynomials F_i of degree 1.

(a) Show that if T is an affine change of coordinates on $\mathbb{A}^n(k)$, then V^T is also a linear subvariety of $\mathbb{A}^n(k)$.

(b) If $V \neq \emptyset$, show that there is an affine change of coordinates T of $\mathbb{A}^n$ such that $V^T = V(X_{m+1}, \ldots, X_n)$. (*Hint:* Use induction on r). So V is a variety.

(c) Show that the m which 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 $V(X_{m+1}, \ldots, X_n)^T = V(X_{s+1}, \ldots, X_n)$, $m < s$; show that $T_{m+1}, \ldots, T_n$ would be dependent.)

Solution. (a) *Proof.* Let $V = V(F_1, \ldots, F_r)$ be a linear subvariety in $\mathbb{A}^n(k)$, so that $F_1, \ldots, F_r$ are linear polynomials. Say $F_i = \sum_{j=1}^n a_{ij}x_j + b_i$.

Let T be an affine change of coordinates on $\mathbb{A}^n(k)$. Say $T(\vec{x}) = M\vec{x} + \vec{c}$, where $M \in \mathrm{GL}_n(k)$ and $\vec{c} \in \mathbb{A}^n(k)$. Then we have

$$T(\vec{x}) = \begin{pmatrix} T_1(\vec{x}) \\ \vdots \\ T_n(\vec{x}) \end{pmatrix}$$

where

$$T_\ell(x_1, \ldots, x_n) = \sum_{k=1}^{n} m_{\ell k} x_k + c_\ell,$$

for $1 \le j \le n$. Then V^T is the zero set of the polynomials F_1^T, ..., F_r^T, which we compute:

$$\begin{aligned} F_i^T(\vec{x}) &= F_i(T(\vec{x})) \\ &= \sum_{\ell=1}^{n} a_{i\ell} T_\ell(\vec{x}) + b_i \\ &= \sum_{\ell=1}^{n} a_{i\ell} \left(\sum_{k=1}^{n} m_{\ell k} x_k + c_\ell \right) + b_i \\ &= \left(\sum_{k=1}^{n} \sum_{\ell=1}^{n} a_{i\ell} m_{\ell k} x_k \right) + \left(\sum_{\ell=1}^{n} a_{i\ell} c_\ell \right) + b_i \end{aligned}$$

which is a linear polynomial. So, V^T is a linear subvariety of $\mathbb{A}^n(k)$.

□

(b) *Proof.* Let $V \subset \mathbb{A}^n(k)$ be a nonempty linear subvariety of $\mathbb{A}^n(k)$ given by $V = V(F_1, \ldots, F_m)$ for some polynomials F_i of degree 1. Without loss of generality, we may assume that m is minimal so that $V = V(F_1, \ldots, F_m)$. This means the linear functions $F_1, \ldots, F_m$ are linearly independent.

Define a change of coordinates by

$$T(X_j) = \begin{cases} X_j & \text{for } 1 \le j \le m \\ F_{j-m}(X_1, \ldots, X_n) & \text{for } m+1 \le j \le n \end{cases}$$

Then $V^T = V(X_{m+1}, \ldots, X_n)$ □

(c) *Proof.* By the choice of m as minimal so that $V = V(F_1, \ldots, F_m)$, this makes m unique. □

2.15. Let $P = (a_1, \ldots, a_n)$, $Q = (b_1, \ldots, b_n)$ be distinct points of $\mathbb{A}^n$. The *line* through P and Q is defined to be $\{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) \mid t \in k\}$.

(a) Show that if L is the line through P and Q, and T is an affine change of coordinates, then $T(L)$ is the line through $T(P)$ and $T(Q)$.

(b) Show that a line is a linear subvariety of dimension 1, and that a linear subvariety of dimension 1 is the line through any two of its points.

(c) Show that, in $\mathbb{A}^2$, a line is the same thing as a hyperplane.

(d) Let $P, P' \in \mathbb{A}^2$, L_1, L_2 two distinct lines through P, L_1', L_2' distinct lines through P'. Show that there is an affine change of coordinates T of $\mathbb{A}^2$ such that $T(P) = P'$ and $T(L_i) = L_i'$, $i = 1, 2$.

Solution. Let $P = (a_1, \ldots, a_n)$, $Q = (b_1, \ldots, b_n)$ be distinct points of $\mathbb{A}^n$. The line through P and Q is defined to be $\{(a_1+t(b_1-a_1), \ldots, a_n+t(b_n-a_n)) \mid t \in k\}$.

(a) *Proof.* Let T be an affine change of coordinates on $\mathbb{A}^n(k)$. Say $T(\vec{x}) = M\vec{x} + \vec{c}$, where $M \in \mathrm{GL}_n(k)$ and $\vec{c} \in \mathbb{A}^n(k)$. Then we have

$$T(\vec{x}) = \begin{pmatrix} T_1(\vec{x}) \\ \vdots \\ T_n(\vec{x}) \end{pmatrix}$$

where

$$T_\ell(x_1, \ldots, x_n) = \sum_{k=1}^{n} m_{\ell k} x_k + c_\ell,$$

for $1 \leq j \leq n$. Then the image of the line under T has component functions

$$\begin{aligned} T_\ell(x_1, \ldots, x_n) &= \sum_{k=1}^{n} m_{\ell k}(a_k + t(b_k - a_k)) + c_\ell, \\ &= \sum_{k=1}^{n} m_{\ell k} a_k + t \sum_{k=1}^{n} m_{\ell k}(b_k - a_k) + c_\ell, \\ &= \left(\sum_{k=1}^{n} m_{\ell k} a_k + c_\ell \right) + t \left[\left(\sum_{k=1}^{n} m_{\ell k} b_k + c_\ell \right) - \left(\sum_{k=1}^{n} m_{\ell k} a_k + c_\ell \right) \right], \\ &= T(a) + t\,[T(b) - T(a)]\,. \end{aligned}$$

This is the line through $T(a)$ and $T(b)$. □

(b) *Proof.* Mark, start here and finish this problem.

Suppose $P = (a_1, \ldots, a_n)$, $Q = (b_1, \ldots, b_n)$ are distinct points of $\mathbb{A}^n$. The line through P and Q is given by $\{(a_1+t(b_1-a_1), \ldots, a_n+t(b_n-a_n)) \mid t \in k\}$.

Define $T : \mathbb{A}^n(k) \to \mathbb{A}^n(k)$ by

□

(c) *Proof.* In $\mathbb{A}^2(k)$, a line through P and Q is defined to be

$$\{(a_1 + t(b_1 - a_1), a_2 + t(b_2 - a_2)) \mid t \in k\}.$$

It's easily checked that this set is the variety given by the linear equation

$$(b_2 - a_2)X - (b_1 - a_1)Y = a_1 b_2 - a_2 b_1.$$

So, every line is a hyperplane in $\mathbb{A}^2(k)$.

Conversely, suppose we take a hyperplane $AX + BY = C$ in $\mathbb{A}^2(k)$. If $A \neq 0$ and $B \neq 0$, this is the line between $(0, C/B)$ and $(C/A, 0)$. If $A = 0$, then $B \neq 0$ and this is the line between $(0, C/B)$ and $(1, C/B)$. If $B = 0$, then $A \neq 0$ and this is the line between $(C/A, 0)$ and $(C/A, 1)$.

□

(d) *Proof.* Let $P, P' \in \mathbb{A}^2$, L_1, L_2 two distinct lines through P, L_1', L_2' distinct lines through P'.

Let T_1 be the translation of $\mathbb{A}^2$ taking P to $(0,0)$. Let M be the matrix taking the vector $T(\vec{v}_{L_i})$ to the vector $T(\vec{v}_{L_i'})$. Let T_2 be the translation of $\mathbb{A}^2$ taking $(0,0)$ to P'.

We note that T_i is the identity on each vector in $\mathbb{A}^2$ since all it does is translate the vector, hence changing neither its magnitude nor direction.

Then the change of coordinates $T = T_2 \circ M \circ T_1$ take P to P' and takes L_1, L_2 to L_1', L_2', respectively.

Mark, check this.

□

2.16. Let $k = \mathbb{C}$. Give $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ the usual topology (obtained by identifying $\mathbb{C}$ with $\mathbb{R}^2$, and hence $\mathbb{C}^n$ with $\mathbb{R}^{2n}$). Recall that a topological space X is *path-connected* if for any $P, Q \in X$, there is a continuous function $\gamma : [0,1] \to X$ such that $\gamma(0) = P$, $\gamma(1) = Q$.

(a) Show that $\mathbb{C} \setminus S$ is path-connected for any finite set S.

(b) Let V be an algebraic set in $\mathbb{A}^n(\mathbb{C})$. Show that $\mathbb{A}^n(\mathbb{C}) \setminus V$ is path-connected. (*Hint:* If $P, Q \in \mathbb{A}^n(\mathbb{C}) \setminus V$, let L be the line through P and Q. Then $L \cap V$ is finite, and L is isomorphic to $\mathbb{A}^1(\mathbb{C})$.)

Solution. (a) *Proof.* Let $S = \{P_1, \dots P_k\}$ be a finite set in $\mathbb{C}$. For any point $P \in S$, let $\delta = \frac{1}{2}\min_{1 \leq i < j \leq k}\{d(P_i, P_j)\}$.

Let Q_1, Q_2 be distinct points in $\mathbb{C} \setminus S$ and construct the line segment ℓ between Q_1 and Q_2. If no point of S lies on ℓ, we're done, since $\ell \subset \mathbb{C} \setminus S$.

If some $P_i \in S$ lies on ℓ, draw the circle C_i of radius δ around P_i. Alter the path of the segment of ℓ through the diameter d_i of C_i to go around the arc of the circle C_i from one end of the diameter to the other. Then continue along ℓ. By the choice of δ, no point of S lies on this arc. The new adjusted path from Q_1 to Q_2 lies in $\mathbb{C} \setminus S$.

So, $\mathbb{C} \setminus S$ is locally path-connected.

□

(b) *Proof.* Let V be an algebraic set in $\mathbb{A}^n(\mathbb{C})$. Let $P, Q \in \mathbb{A}^n(\mathbb{C}) \setminus V$ and let L be the line through P and Q. Then L is isomorphic to $\mathbb{A}^1(\mathbb{C})$ and since $L \cap V$ is an algebraic set in L, $L \cap V$ must be finite. By part (a), $\mathbb{A}^1(\mathbb{C}) \setminus L \cap V$ is path-connected. It follows that $L \setminus V$ is path-connected, so there is a path from P to Q lying in $A^n(\mathbb{C}) \setminus V$. That is, $A^n(\mathbb{C}) \setminus V$ is path-connected.

□

2.4 Rational Functions and Local Rings

Problems

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. *Proof.* Since $Y^2 - X^2(X+1)$ is in the ideal of V, $\overline{Y}^2 - \overline{X}^2(\overline{X}+1) = 0$, so

$$\frac{\overline{Y}}{\overline{X}} = \frac{\overline{X}(\overline{X}+1)}{\overline{Y}}$$

in $k(V)$. So, z may be represented as $\overline{Y}/\overline{X}$ whenever $\overline{X} \neq 0$ and z may be represented as $\overline{X}(\overline{X}+1)/\overline{Y}$ whenever $\overline{Y} \neq 0$. So, the pole set of z is the single point $(0,0)$.

Also, $z^2 = \overline{Y}^2/\overline{X}^2$ and

$$\frac{\overline{Y}^2}{\overline{X}^2} = \overline{X} + 1.$$

Since $\overline{X} + 1 \in \Gamma(V)$ is defined everywhere, the pole set of z^2 is empty. □

2.18. Let $\mathscr{O}_P(V)$ 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 $\mathscr{O}_P(V)$ and the subvarieties of V which pass through P. (*Hint:* If I is prime in $\mathscr{O}_P(V)$, $I \cap \Gamma(V)$ is prime in $\Gamma(V)$, and I is generated by $I \cap \Gamma(V)$); use Problem 2.2.)

Solution. *Proof.* Let $\mathfrak{m}_P \subset \Gamma(V)$ be the ideal of regular functions vanishing at P. Then $\mathscr{O}_P(V)$ is isomorphic to the localization of $\Gamma(V)$ at $\mathfrak{m}_P$. However, the prime ideals in the localization of $\Gamma(V)$ at $\mathfrak{m}_P$ are in one-to-one correspondence with prime ideals in $\Gamma(V)$ contained in $\mathfrak{m}_P$. But these prime ideals are in one to one correspondence with subvarieties of V containing P. □

2.19. Let f be a rational function on a variety V. Let

$$U = \{P \in V \mid f \text{ is defined at } P\}.$$

Then f defines a function from U to k. Show that this function determines f uniquely. So a rational function may be considered as a type of function, but only on the complement of an algebraic subset of V, not on V itself.

Solution. *Proof.* If $P \in U$, write $f = a/b$ for $a, b \in \Gamma(V)$ with $b(P) \neq 0$. Define $\widetilde{f}(P) = a(P)/b(P)$. If $f = a'/b'$ with $a', b' \in \Gamma(V)$ with $b'(P) \neq 0$, then $a/b = a'/b'$ wherever both these functions are defined. In particular, $a(P)/b(P) = a'(P)/b'(P)$, so $\widetilde{f}$ is well-defined for every $P \in U$ where $b(P) \neq 0$ and $b'(P) \neq 0$

Suppose f and f' are rational functions on V with the same domain of definition U so that $\widetilde{f} = \widetilde{f'}$. Write $f = a/b$ and $f' = a'/b'$ where $a, b, a', b' \in \Gamma(V)$. Let O be the subset of V where $bb' \neq 0$. Then $O \subset U$ and since $\widetilde{f} = \widetilde{f'}$, we must have that $a/b = a'/b'$ on O. So $ab' - a'b = 0$ on O. Now, bb' vanishes on $V \setminus O$ by the definition of O, so $bb'(ab' - a'b)$ is identically zero on V. Since b and b' are not identically zero on V and V is irreducible, we conclude that $ab' - a'b$ is identically zero on V. Hence $f = f'$. This shows that the regular function defined on the domain of definition by a rational function actually determines the rational function. □

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 of f is exactly $\{(x, y, z, w) \mid y = 0 \text{ and } w = 0\}$.

Solution. *Proof.* Let $V = V(XW - YZ) \subset \mathbb{A}^4(k)$. $\Gamma(V) = k[X, Y, Z, W]/(XW - YZ)$. Let $\overline{X}, \overline{Y}, \overline{Z}, \overline{W}$ be the residues of X, Y, Z, W in $\Gamma(V)$. Then $\overline{X}/\overline{Y} = \overline{Z}/\overline{W} = f \in k(V)$ is defined at $P = (x, y, z, w) \in V$ if $y \neq 0$ or $w \neq 0$.

Suppose that $f = a/b$ where $a, b \in \Gamma(V)$ and b is nowhere zero on the domain of definition U of f. Suppose b is represented by the polynomial $B(x, y, z, w)$. Setting $y = 0$ and $w = 0$, we get the algebraic set $\{(x, 0, z, 0) \mid B(x, 0, z, 0) = 0\}$. By Problem 1.14, this set is infinite. But this is the set where the zero locus of B meets the points where f is undefined. This is a contradiction. □

Mark, check this. No, this isn't right.

2.21. Let $\varphi : V \to W$ be a polynomial map of affine varieties, $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$ the induced map on coordinate rings. Suppose $P \in V$, $\varphi(P) = Q$. Show that $\widetilde{\varphi}$ extends uniquely to a ring homomorphism (also written $\widetilde{\varphi}$) from $\mathscr{O}_Q(W)$ to $\mathscr{O}_P(V)$. (Note that $\widetilde{\varphi}$ may not extend to all of $k(W)$.) Show that $\widetilde{\varphi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$.

Solution. *Proof.* Recall that $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$ is defined by taking a regular function $f \in \Gamma(W)$ and sending it to $\widetilde{\varphi}(f) = f \circ \varphi$. We recall the natural ring homomorphism

$$\psi : \Gamma(V) \to \mathscr{O}_P(V)$$

given by $\psi(f) = f/1$. Composing, we having a ring homomorphism

$$\omega : \Gamma(W) \xrightarrow{\widetilde{\varphi}} \Gamma(V) \xrightarrow{\psi} \mathscr{O}_P(V).$$

Suppose that $f \in \Gamma(W)$ does not vanish at Q. Then under this composition of maps, f goes to $\widetilde{\varphi}(f)/1 = (f \circ \varphi)/1$ and at P we have that

$$[(f \circ \varphi)/1](P) = (f \circ \varphi)(P)/1 = f(Q)/1 \neq 0.$$

Thus, every element which is not in $\mathfrak{m}_Q \subset \Gamma(W)$ maps to a unit in $\mathscr{O}_P(V)$ under ω. This means we can define a homomorphism

$$\widetilde{\psi} : \mathscr{O}_Q(W) \to \mathscr{O}_P(V)$$

making the following diagram commute:

$$\begin{array}{ccc} \Gamma(W) & \xrightarrow{\widetilde{\varphi}} & \Gamma(V) \\ \varphi \downarrow & & \downarrow \psi \\ \mathscr{O}_Q(W) & \xrightarrow{\widetilde{\psi}} & \mathscr{O}_P(V) \end{array}$$

by $\widetilde{\psi}(f/g) = \widetilde{\varphi}(f)\widetilde{\varphi}(g)^{-1}$. It is easily seen that this is the only way to define $\widetilde{\psi}$ as a ring homomorphism so that the diagram commutes, so $\widetilde{\psi}$ is unique.

Note that if $f/g \in \mathfrak{m}_Q(W)$, the maximal ideal of $\mathscr{O}_Q(W)$, then f vanishes at Q. But then $\widetilde{\varphi}(f) = f \circ \varphi$ vanishes at P, so $\widetilde{\psi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$. □

2.22. Let $T : \mathbb{A}^n \to \mathbb{A}^n$ be an affine change of coordinates, $T(P) = Q$. Show that $\widetilde{T} : \mathscr{O}_Q(\mathbb{A}^n) \to \mathscr{O}_P(\mathbb{A}^n)$ is an isomorphism. Show that $\widetilde{T}$ induces an isomorphism from $\mathscr{O}_Q(V)$ to $\mathscr{O}_P(V^T)$ if $P \in V^T$, for V a subvariety of $\mathbb{A}^n$.

Solution. *Proof.* If $T : \mathbb{A}^n \to \mathbb{A}^n$ is an affine change of coordinates, let $S : \mathbb{A}^n \to \mathbb{A}^n$ be the inverse affine change of coordinates, i.e. $S = T^{-1}$. Let $\widetilde{\varphi}_P : \Gamma(\mathbb{A}^n) \to \mathscr{O}_P(\mathbb{A}^n)$ be the natural ring homomorphism from above. Then we have the following commutative diagram:

$$\begin{array}{ccccc} \Gamma(\mathbb{A}^n) & \xrightarrow{\widetilde{T}} & \Gamma(\mathbb{A}^n) & \xrightarrow{\widetilde{S}} & \Gamma(\mathbb{A}^n) \\ \widetilde{\varphi}_Q \downarrow & & \widetilde{\varphi}_P \downarrow & & \widetilde{\varphi}_Q \downarrow \\ \mathscr{O}_Q(\mathbb{A}^n) & \xrightarrow{\widetilde{T}_Q} & \mathscr{O}_P(\mathbb{A}^n) & \xrightarrow{\widetilde{S}_P} & \mathscr{O}_Q(\mathbb{A}^n) \end{array}$$

Since the top horizontal sequence of maps is the identity, so is the bottom horizontal sequence of maps. Hence $\widetilde{T}$ induces an isomorphism of the local rings $\mathscr{O}_P(\mathbb{A}^n)$ and $\mathscr{O}_Q(\mathbb{A}^n)$.

Similarly, if $V \subset \mathbb{A}^n$ is a variety, then $T : V^T \to V$, and exactly the same argument shows that $\widetilde{T}$ induces an isomorphism of the local rings $\mathscr{O}_Q(V)$ and $\mathscr{O}_P(V^T)$. □

2.5 Discrete Valuation Rings

Problems

2.23. Show that the order function on K is independent of the choice of uniformizing parameter.

Solution. *Proof.* Suppose that t and t' are uniformizing parameters for R, and let $z \in K$. If we write $z = ut^n$, we note that

$$\operatorname{ord}(z) = \operatorname{ord}(ut^n) = \operatorname{ord}(u) + \operatorname{ord}(t^n) = 0 + n \operatorname{ord}(t) = n,$$

so it suffices to show that $\operatorname{ord}(t) = \operatorname{ord}(t')$. Since t is a uniformizing parameter for R and $t' \in \mathfrak{m}$, we can write $t' = ut^n$ for some $n \in \mathbb{N}$. Similarly, since t' is a uniformizing parameter for R and $t \in \mathfrak{m}$, we can write $t = vt'^m$ for some $m \in \mathbb{N}$. Then

$$t = vt'^m = v(ut^n)^m = vu^m t^{nm},$$

and hence $nm = 1$. This forces $n = m = 1$, since $n, m \in \mathbb{N}$. So, $\operatorname{ord}(t) = \operatorname{ord}(t')$, and we're done. □

2.24. Let $V = \mathbb{A}^1$, $\Gamma(V) = k[X]$, $K = k(V) = k(X)$.

(a) For each $a \in k = V$, show that $\mathscr{O}_a(V)$ is a DVR with uniformizing parameter $t = X - a$.

(b) Show that $\mathscr{O}_\infty = \{F/G \in k(X) \mid \deg G \geq \deg F\}$ is also a DVR, with uniformizing parameter $t = 1/X$.

Solution. (a) *Proof.* Let $f = F(X)/G(X) \in k(X)$, $f \neq 0$. Using long division, we may write uniquely $F(X) = \sum_0^n a_i(X-a)^i$ and $G(X) = \sum_0^n b_i(X-a)^i$. If a_n and b_m are the smallest nonzero coefficients in each of these polynomials, we may write uniquely

$$F(X) = \sum_0^n a_i(X-a)^i = P(X)(X-a)^n$$

$$G(X) = \sum_0^n b_i(X-a)^i = Q(X)(X-a)^m$$

where $P(a) \neq 0$ and $Q(a) \neq 0$. Hence $f = (P/Q)(X-a)^{n-m}$, and P/Q is a unit in $\mathscr{O}_a(V)$. Since $X - a \in \Gamma(V) = k[X]$ is irreducible, we see that $\mathscr{O}_a(V)$ is a DVR with uniformizing parameter $X - a$. □

(b) *Proof.* Let $f = F/G \in \mathscr{O}_\infty$. Suppose that $\deg F = n$ and $\deg G = m$ with $m \geq n$. Then we can uniquely write

$$\begin{aligned} \frac{F}{G} &= \frac{FX^{m-n}}{G}\frac{1}{X^{m-n}} \\ &= \frac{FX^{m-n}}{G}t^{m-n} \end{aligned}$$

Since $\deg FX^{m-n} = \deg F + m - n = m = \deg G$, FX^{m-n}/G is a unit in $\mathscr{O}_\infty(V)$. Since $t = 1/X$ is irreducible in $\mathscr{O}_\infty(V)$, $\mathscr{O}_\infty(V)$ is a DVR with uniformizing parameter $t = 1/X$. □

2.25. Let $p \in \mathbb{Z}$ be a prime number. Show that $\{r \in \mathbb{Q} \,|\, r = a/b,\ a, b \in \mathbb{Z}, p$ doesn't divide $b\}$ is a DVR with quotient field $\mathbb{Q}$.

Solution. *Proof.* Let $p \in \mathbb{Z}$ be a prime number. Let $\mathbb{Z}_{(p)} = \{r \in \mathbb{Q} \,|\, r = a/b,\ a, b \in \mathbb{Z}, p$ doesn't divide $b\}$. Let $\mathfrak{m} = (p)$, the principal ideal in $\mathbb{Z}_{(p)}$ generated by p. If $r \in \mathbb{Z}_{(p)}$, $r \neq 0$. We can write $r = a/b$ with $a, b \in \mathbb{Z}, p$ doesn't divide b, and $(a, b) = 1$. By the Fundamental Theorem of Arithmetic, $a = up^n$ where $n \in \mathbb{N} \cup \{0\}$, $u \in \mathbb{Z}$, $p \nmid u$. Then $r = \frac{u}{b}p^n$. Then $\frac{u}{b}$ is a unit in $\mathbb{Z}_{(p)}$, p is irreducible, and $\mathfrak{m}$ is the set of non-units in $Z_{(p)}$. This shows $Z_{(p)}$ is a DVR. It's easy to see the quotient field of $Z_{(p)}$ is $\mathbb{Q}$. □

2.26. Let R be a DVR with quotient field K; let $\mathfrak{m}$ be the maximal ideal of R.

(a) Show that if $z \in K$, $z \notin R$, then $z^{-1} \in \mathfrak{m}$.

(b) Suppose $R \subset S \subset K$, and S is also a DVR. Suppose the maximal ideal of S contains $\mathfrak{m}$. Show that $S = R$.

Solution. (a) *Proof.* Let $z \in K \setminus R$. Let t be a uniformizing parameter for R and write $z = ut^n$ for some unit $u \in R$ and some $n \in \mathbb{Z}$. Note that if $n \geq 0$ then $z \in R$, which contradicts the assumption that $z \notin R$. Hence $n < 0$. Let $m = -n > 0$. Then $z^{-1} = u^{-1}t^m$ and since $m > 0$, $z^{-1} \in \mathfrak{m}$. □

(b) *Proof.* Let $z \in S \subset K$. We may assume that $z \neq 0$ since $0 \in R$. By the result of part (a), since R is a DVR, either $z \in R$ or $z^{-1} \in R$. If $z \in R$, we're done, so assume that $z^{-1} \in R$ and $z \notin R$. It follows then from part (a) that $z^{-1} \in \mathfrak{m} \subset \mathfrak{m}_S$, where $\mathfrak{m}$ is the maximal ideal in R and $\mathfrak{m}_S$ is the maximal ideal in S. But then $1 = zz^{-1} \in \mathfrak{m}_S$, which is absurd, since $\mathfrak{m}_S$ is a maximal ideal in S. Hence, we must have that $z \in R$, so $R = S$. □

2.27. Show that the DVR's of Problem 2.24 are the only DVR's with quotient field $k(X)$ that contain k. Show that those of Problem 2.25 are the only DVR's with quotient field $\mathbb{Q}$.

Solution. *Proof.* Let R be a DVR containing k with quotient field $k(X)$.

Let $\mathfrak{m} = (t)$ be its maximal ideal where t is a uniformizing parameter.

By Problem 2.26, if $x \notin R$, then $x^{-1} \in \mathfrak{m} \subset R$. Hence $x^{-1} = ut^n$ for some $n \in \mathbb{N}$. However, x^{-1} is irreducible, so this forces $\mathfrak{m} = (x^{-1})$.

Otherwise, $x \in R$, so that $k[X] \subset R$. Since $t \in R$ must irreducible, $t = x - a$ for some $a \in k$, up to a unit multiple.

Hence, the only DVR's containing k with quotient field $k(X)$ are the ones in Problem 2.24.

Let R be a DVR with quotient field $\mathbb{Q}$. We note that $\mathbb{Z} \subset R$.

Let $\mathfrak{m} = (t)$ be its maximal ideal where t is a uniformizing parameter. Write $t = a/b$ where $a, b \in \mathbb{Z}$, with a, b relatively prime. Since $b \in \mathbb{Z} \subset R$, $bt = a \in \mathfrak{m}$. This forces b to be a unit and $\mathfrak{m} = (a)$. Since a must be irreducible, $a = p$ for some prime number.

Hence, the only DVR's with quotient field $\mathbb{Q}$ have are the ones in Problem 2.25. □

2.28. An *order function* on a field K is a function φ from K onto $\mathbb{Z} \cup \{\infty\}$, satisfying:

(a) $\varphi(a) = \infty$ if and only if $a = 0$.

(b) $\varphi(ab) = \varphi(a) + \varphi(b)$.

(c) $\varphi(a + b) \geq \min\{\varphi(a), \varphi(b)\}$.

Show that $R = \{z \in K \mid \varphi(z) \geq 0\}$ is a DVR with maximal ideal $\mathfrak{m} = \{z \mid \varphi(z) > 0\}$, and quotient field K. Conversely, show that if R is a DVR with quotient field K, then the function $\mathrm{ord} : K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K. Giving a DVR with quotient field K is the same thing as defining an order function on K.

Solution. *Proof.* ($\Rightarrow$) Suppose that $\varphi : K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K. Let $R = \{z \in K \mid \varphi(z) \geq 0\}$. Let $a, b \in R$. Then $\varphi(a+b) \geq \min\{\varphi(a), \varphi(b)\} \geq 0$ so $a + b \in R$. Similarly, $\varphi(ab) = \varphi(a) + \varphi(b) \geq 0$, so $ab \in R$. Also,

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1),$$

and it follows that $\varphi(1) = 0$, so that $1 \in R$. It is trivial to see that $0 \in R$. Notice that if $z \in K$, $z \neq 0$, then

$$0 = \varphi(1) = \varphi(zz^{-1}) = \varphi(z) + \varphi(z^{-1}), \tag{$*$}$$

so that $\varphi(z^{-1}) = -\varphi(z)$. This implies that $\varphi(-1) = 0$. Then, $\varphi(a-b) = \varphi(a+(-b)) \geq \min\{\varphi(a), \varphi(-b)\}$, but $\varphi(-b) = \varphi(-1 \cdot b) = \varphi(-1)+\varphi(b) = \varphi(b)$, so $\varphi(a-b) \geq \min\{\varphi(a), \varphi(b)\} \geq 0$, so $a-b \in R$. This is sufficient to show that R is a commutative ring with identity.

Suppose that $z \in R$, $z \neq 0$. Then from equation $(*)$, we have $z^{-1} \in R$ if and only if $\varphi(z) = 0$, so the set $\mathfrak{m} = \{z \,|\, \varphi(z) > 0\}$ consists of all nonunits in R. If a, $b \in \mathfrak{m}$ then

$$\varphi(a-b) = \varphi(a+(-b)) \geq \min\{\varphi(a), \varphi(-b)\} = \min\{\varphi(a), \varphi(b)\} > 0,$$

so $a - b \in \mathfrak{m}$. Also, if $r \in R$, then

$$\varphi(ar) = \varphi(a) + \varphi(r) > 0,$$

so $ar \in \mathfrak{m}$. It follows that $\mathfrak{m}$ is an ideal in R. Hence R is a DVR with maximal ideal $\mathfrak{m}$. Now, the quotient field of R is contained in the field K. Since φ is onto, choose $t \in K$ satisfy $\varphi(t) = 1$. Now, if $z \in K$ with $\varphi(z) = -n < 0$, then $z = zt^n/t^n$, and zt^n and t^n are both in R, with $t^n \neq 0$. It follows that K is the quotient field of R.

($\Leftarrow$) Suppose that R is a DVR with quotient field K. Let t be a uniformizing parameter for R. Define $\varphi(0) = \infty$. If $z \in K$, $z \neq 0$, write $z = ut^n$, where u is a unit in R and $n \in \mathbb{Z}$. Define $\varphi(z) = n$. We show that $\varphi : K \to \mathbb{Z} \cup \{\infty\}$ is an order function on K.

First, it is clear that $\varphi(a) = \infty$ if and only if $a = 0$. Let $a, b \in K$. Write $a = ut^n$ and $b = vt^m$ for some units $u, v \in R$, and integers n and m, where we assume $n \geq m$. Then $a + b = ut^n + vt^m = t^m(ut^{n-m} + v)$, and $(ut^{n-m} + v)$ is a unit in R. Certainly $(ut^{n-m} + v)$ is in R since $n \geq m$, and if $(ut^{n-m} + v)$ is not a unit in R, then $(ut^{n-m} + v) \in \mathfrak{m}$. But then it follows that $v \in \mathfrak{m}$, which is impossible. So, we see that $\varphi(a+b) = m = \min\{\varphi(a), \varphi(b)\}$. Simlarly, $ab = (ut^n)(vt^m) = (uv)t^{n+m}$, and uv is a unit in R, so $\varphi(ab) = n+m = \varphi(a)+\varphi(b)$. Thus, φ is an order function on K. □

2.29. Let R be a DVR with quotient field K, ord the order function on K.

(a) If $\text{ord}\,(a) < \text{ord}\,(b)$, show that $\text{ord}\,(a+b) = \text{ord}\,(a)$.

(b) If $a_1, \ldots, a_n \in K$, and for some i, $\text{ord}\,(a_i) < \text{ord}\,(a_j)$ for all $j \neq i$, then $a_1 + \cdots + a_n \neq 0$.

Solution. (a) *Proof.* By the inequality, $a \neq 0$, and if b is zero, the result is clear, so we may assume that $a, b \neq 0$. Choose a uniformizing parameter t for R, and write $a = ut^n$ and $b = vt^m$ for u, v units in R and n, $m \in \mathbb{Z}$, with $n < m$. Then $a+b = ut^n+vt^m = t^n(u+vt^{m-n})$. Now, $u+vt^{m-n} \in R$ and if $u + vt^{m-n} \in \mathfrak{m}$, then $u \in \mathfrak{m}$, since $m - n > 0$. This contradicts the fact that u is a unit in R. We conclude that $\text{ord}\,(a+b) = n = \text{ord}\,(a)$. □

(b) *Proof.* Without loss of generality, we assume that $\operatorname{ord}(a_1) < \operatorname{ord}(a_j)$ for all $j > 1$. Note that this implies that $a_1 \neq 0$. We prove by induction that $\operatorname{ord}(a_1 + \cdots + a_i) = \operatorname{ord}(a_1)$ for all $1 \leq i \leq n$. If $i = 1$, the statement is trivially true. If $i = 2$, the statement $\operatorname{ord}(a_1 + a_2) = \operatorname{ord}(a_1)$ follows from part (a). Suppose the statement is true for $i = k < n$. Let $a = a_1 + \cdots + a_k$. Then $\operatorname{ord}(a) = \operatorname{ord}(a_1)$, by the induction hypothesis. Letting $b = a_{k+1}$ we see that $\operatorname{ord}(a) < \operatorname{ord}(b)$, so that by part (a), $\operatorname{ord}(a + b) = \operatorname{ord}(a)$. But this says that $\operatorname{ord}(a_1 + \cdots + a_{k+1}) = \operatorname{ord}(a_1)$. This concludes the induction. Hence, $\operatorname{ord}(a_1 + \cdots + a_n) = \operatorname{ord}(a_1)$. But since $a_1 \neq 0$, we conclude that $\operatorname{ord}(a_1 + \cdots + a_n)$ is finite, so $a_1 + \cdots + a_n$ cannot be zero. □

2.30. Let R be a DVR with maximal ideal $\mathfrak{m}$, and quotient field K, and suppose a field k is a subring of R, and that the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism of k with $R/\mathfrak{m}$ (as for example in Problem 2.24). Verify the following assertions:

(a) For any $z \in R$, there is a unique $\lambda \in k$ such that $z - \lambda \in \mathfrak{m}$.

(b) Let t be a uniformizing parameter for R, $z \in R$. Then for any $n \geq 0$ there are unique $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ and $z_n \in R$ such that $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}$.

Solution. (a) *Proof.* Let $z \in R$ and let $\overline{z}$ be the residue of z in $R/\mathfrak{m}$. Since the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism, there is a unique $\lambda \in k$ so that the image of λ in $R/\mathfrak{m}$ is $\overline{z}$. Hence, there is a unique $\lambda \in k$ so that $z - \lambda \in \mathfrak{m}$, as desired. □

(b) *Proof.* Let t be a uniformizing parameter and let $z \in R$. We proceed by induction on n. By part (a), there is a unique $\lambda_0 \in k$ so that $z - \lambda_0 \in \mathfrak{m}$. Since $\mathfrak{m}$ is a principal ideal generated by t, we can write $z - \lambda_0 = z_0 t$ for some $z_0 \in R$. The uniqueness of z_0 follows from the fact that R is a domain. This proves the statement for $n = 0$. Assume the statement is true for $n = l$. Then we can write

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_l t^l + z_l t^{l+1},$$

where $\lambda_0, \lambda_1, \ldots, \lambda_l \in k$ and $z_l \in R$ are unique. By part (a), we can find a unique $\lambda_{l+1} \in k$ so that $z_l - \lambda_{l+1} \in \mathfrak{m}$. Write $z_l - \lambda_{l+1} = z_{l+1} t$. It then follows just as before that z_{l+1} is unique, and

$$\begin{aligned} z =& \lambda_0 + \lambda_1 t + \cdots + \lambda_l t^l + z_l t^{l+1} \\ & \lambda_0 + \lambda_1 t + \cdots + \lambda_l t^l + (\lambda_{l+1} + z_{l+1} t) t^{l+1} \\ & \lambda_0 + \lambda_1 t + \cdots + \lambda_{l+1} t^{l+1} + z_{l+1} t^{l+2} \end{aligned}$$

This shows that the statement is true for $n = l + 1$, and so concludes the induction. □

2.31. Let k be a field. The ring of formal power series over k, written $k[[X]]$, is defined to be $\{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in k\}$. (As with polynomials, a rigorous definition is best given in terms of sequence $(a_0, a_1, \dots)$ of elements of k; here we allow an infinite number of nonzero terms.) Define the sum $\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$, and the product by $\left(\sum a_i X^i\right)\left(\sum b_i X^i\right) = \sum c_i X^i$, where $c_i = \sum_{j+k=i} a_j b_k$. Show that $k[[X]]$ is a ring containing $k[X]$ as a subring. Show that $k[[X]]$ is a DVR with uniformizing parameter X. Its quotient field is denoted $k((X))$.

Solution. *Proof.* The proof that $k[[X]]$ is a ring with $k[X]$ as a subring is left to the reader. We show that $k[[X]]$ is a DVR with uniformizing parameter X.

Let $\mathfrak{m} = \{\sum_0^{\infty} a_i X^i \in k[[X]] \mid a_0 = 0\}$. We have to show that $\mathfrak{m}$ is an ideal and contains all the nonunits of $k[[X]]$. If $a = \sum_0^{\infty} a_i X^i$ and $b = \sum_0^{\infty} b_i X^i$ are in $\mathfrak{m}$, then $a - b = \sum_0^{\infty} (a_i - b_i) X^i$. Since $a_0 = b_0 = 0$, we see that $a_0 - b_0 = 0$, so $a - b \in \mathfrak{m}$. This shows that $\mathfrak{m}$ is subgroup of $k[[X]]$. Suppose that $r = \sum_0^{\infty} r_i X^i$ is in $k[[X]]$. Then

$$ra = \left(\sum_0^{\infty} r_i X^i\right)\left(\sum_0^{\infty} a_i X^i\right) = \sum_0^{\infty} c_i X^i,$$

where $c_i = \sum_{j+k=i} a_j r_k$. So, $c_0 = a_0 r_0 = 0$, since $a_0 = 0$. This shows that $\mathfrak{m}$ is an ideal.

Now we show that $a = \sum_0^{\infty} a_i X^i$ is a unit $k[[X]]$ if and only if $a_0 \neq 0$. This will show that $\mathfrak{m}$ consists precisely of all the nonunits in $k[[X]]$, and that will conclude the proof, since $\mathfrak{m}$ is certainly a principal ideal in $k[[X]]$ generated by X, as is easily seen.

Suppose that $a = \sum_0^{\infty} a_i X^i$ has $a_0 = 0$. Then if $b = \sum_0^{\infty} b_i X^i$, then $(ab)_0 = a_0 b_0 = 0$, so there cannot exist a $b \in k[[X]]$ with $ab = 1$. Hence a is a nonunit.

Now suppose that $a = \sum_0^{\infty} a_i X^i$ has $a_0 \neq 0$. We'll construct the inverse of a, $b = \sum_0^{\infty} b_i X^i$ by choosing $b_0, b_1, \dots$ inductively. Let $1 = \sum_0^{\infty} c_i X^i$, where $c_i = \sum_{j+k=i} a_j b_k$, denote the product of a and b. As noted above, we must have $c_0 = a_0 b_0 = 1$, so choose $b_0 = a_0^{-1}$. Now, $0 = c_1 = a_1 b_0 + a_0 b_1 = (a_1/a_0) + a_0 b_1$, so choose $b_1 = -a_1/a_0^2$. Suppose that we have chosen $b_0, b_1, \dots, b_n$ so that $c_0 = 1$ and $c_i = 0$ if $1 \leq i \leq n$. Then

$$\begin{aligned} 0 = c_{n+1} &= \sum_{j+k=n+1} a_j b_k \\ &= a_0 b_{n+1} + a_1 b_n + \cdots + a_{n+1} b_0. \end{aligned}$$

Thus, we choose $b_{n+1} = -(a_1 b_n + \cdots + a_{n+1} b_0)/a_0$. This concludes the induction and shows that we can construct an element $b \in k[[X]]$ so that $ab = 1$. Hence a is a unit. $\square$

2.32. Let R be a DVR satisfying the conditions of Problem 2.30. Any $z \in R$ then determines a power series $\sum \lambda_i X^i$, if $\lambda_0, \lambda_1, \dots$ are determined as in Problem 2.30(b).

(a) Show that the map $z \to \sum \lambda_i X^i$ is a one-to-one ring homomorphism of R into $k[[X]]$. We often write $z = \sum \lambda_i t^i$, and call this the *power series expansion* of z in terms of t.

(b) Show that the homomorphism extends to a homomorphism of K into $k((X))$, and that the order function on $k((X))$ restricts to that on K.

(c) Let $a = 0$ in Problem 2.24, $t = X$. Find the power series expansions of $z = (1-X)^{-1}$ and of $(1-X)(1+X^2)^{-1}$.

Solution. (a) *Proof.* From Problem 2.30, we've already shown that any $z \in R$ determines a power series $\sum \lambda_i X^i$, with $\lambda_0, \lambda_1, \ldots$ in k. This gives a map $\varphi : R \to k[[X]]$. If $z \in \mathfrak{m} \subset R$, then $\lambda_0 = 0$, so $\varphi(z) \in \mathfrak{m} \subset k[[X]]$. Conversely, if $z \notin \mathfrak{m} \subset R$, then $\lambda_0 \neq 0$, so $\varphi(z) \notin \mathfrak{m} \subset k[[X]]$. From our previous work, it is easy to see that $\operatorname{ord}(z) = n$ if $z = ut^n$, with u a unit in R. But then $\varphi(z) = \varphi(ut^n) = \varphi(u)\varphi(t)^n = \varphi(u)X^n$, where $\varphi(u)$ is a unit in $k[[X]]$. It follows that the order function on R is induced by the order function on $k[[X]]$. Note that the kernel of φ consists of those z for which $\lambda_i = 0$ for all i, which says that t^n divides z for all n. It follows that the order of z is infinite, so $z = 0$. Hence φ is injective. □

(b) *Proof.* (a)

$$z = \frac{1}{1-X} = 1 + X + X^2 + X^3 + \cdots + X^n + \ldots.$$

(b)

$$\begin{aligned} z = \frac{1-X}{1+X^2} &= (1-X)\sum_0^\infty (-1)^n X^{2n} \\ &= \sum_0^\infty (-1)^n X^{2n} - \sum_0^\infty (-1)^n X^{2n+1} \\ &= 1 - X - X^2 + X^3 + X^4 - X^5 - X^6 + X^7 + X^8 - \ldots \end{aligned}$$

□

2.6 Forms

Problems

2.33. Factor $Y^3 - 2XY^2 + 2X^2Y + X^3$ into linear factors in $\mathbb{C}[X, Y]$.

Solution. Let r_1, r_2, r_3 be the three roots of $1 - 2X + 2X^2 + X^3$. Then

$$1 - 2X + 2X^2 + X^3 = (X - r_1)(X - r_2)(X - r_3).$$

But then

$$Y^3 - 2XY^2 + 2X^2Y + X^3 = (X - r_1Y)(X - r_2Y)(X - r_3Y).$$

2.34. Suppose $F, G \in k[X_1, \dots, X_n]$ are forms of degree $r, r+1$ respectively, with no common factors (k a field). Show that $F + G$ is irreducible.

Solution. *Proof.* Let $F, G \in k[X_1, \dots, X_n]$ are forms of degree $r, r+1$ respectively, with no common factors.

Suppose $F + G = HK$, where $H, K \in k[X_1, \dots, X_n]$. Write $H = H_0 + H_1 + \cdots + H_k$ and $G = G_0 + G_1 + \cdots + G_\ell$, where H_i, G_i are forms of degree i with $H_k \neq 0$ and $G_\ell \neq 0$.

Looking at the terms of degree $r+1$ on both sides, we see that $G = H_k G_\ell$, which implies that $k + \ell = r + 1$. So, $\ell = r - k + 1$.

Now look at the terms of degree r on both sides, we see that

$$H_k G_{r-k} + H_{k-1} G_{r-k+1} = F.$$

We know that $H_k \neq 0$ and $G_{r-k+1} \neq 0$. This forces one of G_{r-k} and H_{k-1} to be zero. Otherwise the product contains homogeneous terms of degree $r - 1$, which is contradiction. Suppose $H_{k-1} = 0$.

Now look at the terms of degree $r - 1$ on both sides, we see that

$$H_k G_{r-k-1} + H_{k-1} G_{r-k} + H_{k-2} G_{r-k+1} = H_k G_{r-k-1} + H_{k-2} G_{r-k+1} = 0$$

We know that $H_k \neq 0$ and $G_{r-k+1} \neq 0$. This forces one of G_{r-k-1} and H_{k-2} to be zero. Otherwise the product contains homogeneous terms of degree $r-3$, which is contradiction. If $G_{r-k-1} \neq 0$, then the product has nonzero homogeneous term $H_k G_{r-k-1}$ of degree $r-1$, which is a contradiction. Hence $H_{k-2} = 0$.

Continuing inductively, we see that $H_{k-1} = H_{k-2} = \cdots = H_0 = 0$. Hence, $H = H_k$.

Then G must equal $G_{r-k+1} + G_{r-k}$, so that $F = G_{r-k} H_k$ and $G = G_{r-k+1} H_k$. This contradicts the hypothesis that F and G have no common factor.

Hence, $F + G$ is irreducible. □

2.35. (a) Show that there are $d + 1$ monomials of degree d in $R[X, Y]$, and $1 + 2 + \cdots + (d+1) = (d+1)(d+2)/2$ monomials of degree d in $R[X, Y, Z]$.

(b) Let $V(d, n) = \{\text{forms of degree } d \text{ in } k[X_1, \dots X_n]\}$, k a field. Show that $V(d, n)$ is a vector space over k, and that the monomials of degree d form a basis. Show that $\dim(V(d, 1)) = 1$; $\dim(V(d, 2)) = d + 1$; $\dim(V(d, 3)) = (d+1)(d+2)/2$.

(c) Let $L_1, L_2, \ldots$ and $M_1, M_2, \ldots$ be sequences of nonzero linear forms in $k[X,Y]$, and assume no $L_i = \lambda M_j$, $\lambda \in k$. Let $A_{ij} = L_1 L_2 \ldots L_i M_1 M_2 \cdots M_j$, $i, j \geq 0$ ($A_{00} = 1$). Show that $\{A_{ij} \mid i + j = d\}$ forms a basis for $V(d, 2)$.

Solution. (a) *Proof.* Every monomial of degree d in $R[X,Y]$ has the form $X^j Y^{d-j}$ for $0 \leq j \leq d$. There are $d+1$ choices of j, so there are $d+1$ monomials of degree d in $R[X,Y]$.

Every monomial of degree d in $R[X,Y,Z]$ has the form $M^j Z^{d-j}$ for $0 \leq j \leq d$, where M^j is a form of degree j in $R[X,Y]$. The number of choices of M^j is $j+1$, so the number of monomials of degree d in $R[X,Y,Z]$ is

$$\sum_0^d (j+1) = \sum_1^{d+1} j = \frac{(d+1)(d+2)}{2}.$$

□

(b) This is silly.

(c) *Proof.* □

2.36. With the above notation, show that $\dim(V(d,n)) = \binom{d+n-1}{n-1}$, the binomial coefficient.

Solution. *Proof.* Take $d+n-1$ boxes and remove $n-1$ of them. This gives you d boxes grouped into n groups (possibly containing zero boxes). Those numbers of boxes in each of those groups, $i_1, \ldots, i_n$, represent the exponents of $x_1, \ldots, x_n$. Then you have monomials $x_1^{i_1} \cdots x_n^{i_n}$, which is all the monomials of degree d. (Proof due to J. Harris.) □

2.7 Direct Products of Rings

Problems

2.37. What are the additive and multiplicative identities in $\prod R_i$? Is the map from R_i to $\prod R_j$ taking a_i to $(0, \ldots, a_i, \ldots, 0)$ a ring homomorphism?

Solution. The additive identity is $(0, \ldots, 0)$. The multiplicative identity is $(1, \ldots, 1)$. The map taking R_i to $\prod R_j$ is not a ring homomorphism since it does not take the multiplicative identity of R_i to the multiplicative identity of $\prod R_j$.

2.38. Show that if $k \subset R_i$, and each R_i is finite-dimensional over k, show that $\dim\left(\prod_1^n R_i\right) = \sum_1^n \dim\left(R_i\right)$.

Solution. *Proof.* The case $n = 1$ being trivial. For $n = 2$, we have an exact sequence of vector spaces and linear maps

$$0 \to R_1 \xrightarrow{f} R_1 \times R_2 \xrightarrow{g} R_2 \to 0.$$

given by $f(x) = (x, 0)$ and $g(x, y) = y$.

Then $\dim_k(R_1) - \dim_k(R_1 \times R_2) + \dim_k(R_2) = 0$, so that

$$\dim_k(R_1 \times R_2) = \dim_k(R_1) + \dim_k(R_2).$$

The result follows by induction. □

2.8 Operations with Ideals

Problems

2.39. Prove the following relations among ideals I_i, J, in a ring R:

(a) $(I_1 + I_2)J = I_1J + I_2J$.

(b) $(I_1 \cdots I_N)^n = I_1^n \cdots I_N^n$.

Solution. (a) *Proof.* First, $I_1, I_2 \subset I_1 + I_2$, so $I_1J, I_2J \subset (I_1 + I_2)J$. Hence $I_1J + I_2J \subset (I_1 + I_2)J$. On the other hand, it's clear that $(I_1 + I_2)J \subset I_1J + I_2J$. Hence $(I_1 + I_2)J = I_1J + I_2J$. □

(b) *Proof.* This follows from the fact that R is a commutative ring. □

2.40. (a) Suppose I, J are comaximal ideals in R. Show that $I + J^2 = R$. Show that I^m and J^n are comaximal for all m, n.

(b) Suppose $I_1, \ldots, I_N$ are ideals in R, and I_i and $J_i = \bigcap_{j \neq i} I_j$ are comaximal for all i. Show that $I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n$ for all n.

Solution. (a) *Proof.* Suppose I and J are comaximal ideals in R. Then there exist elements $x \in I$, $y \in J$ so that $x + y = 1$. Then

$$y^2 = (1 - x)^2 = 1 - 2x + x^2 \equiv 1 \mod I$$

So, $I + J^2 = 1$.

$$y^n = (1-x)^n = \sum_{k=0}^{n} (-x)^{n-k} = 1 + \sum_{k=0}^{n-1} (-x)^{n-k} \equiv 1 \mod I$$

So, $I + J^n = 1$.

Now, reversing the roles of I and J and replacing J by J^n, we get $I^m + J^n = 1$ for all m, n.

□

(b) *Proof.* This is proved in A-M. □

2.41. Let I, J be ideals in a ring R. Suppose I is finitely generated and $I \subset \text{Rad}(J)$. Show that $I^n \subset J$ for some n.

Solution. *Proof.* This is proved in A-M. □

2.42. (a) Let $I \subset J$ be ideals in a ring R. Show that there is a natural ring homomorphism from R/I onto R/J.

(b) Let I be an ideal in a ring R, R a subring of a ring S. Show that there is a natural ring homomorphism from R/I to S/IS.

Solution. *Proof.* Let $I \subset J$ be ideals in a ring R.

We have the natural surjective quotient map $R \xrightarrow{q} R/J$. Since $I \subset J$, this homomorphism factors through the quotient to give a surjective homomorphism $R/I \to R/J$. □

(a) *Proof.* Let I be an ideal in a ring R, R a subring of a ring S. We have a composition of homomorphisms give by $R \hookrightarrow S \xrightarrow{q} S/IS$. The ideal $I \subset R$ maps to zero in S/IS, so this maps factors through the quotient R/I to give a homomorphism $R/I \to S/IS$. □

2.43. Let $P = (0, \dots, 0) \in \mathbb{A}^n$, $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Let $I \subset k[X_1, \dots, X_n]$ be the ideal generated by $X_1, \dots, X_n$. Show that $I\mathscr{O} = \mathfrak{m}$, so $I^r\mathscr{O} = \mathfrak{m}^r$ for all r.

Solution. *Proof.* Let $P = (0, \dots, 0) \in \mathbb{A}^n$, $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$. Let $I \subset k[X_1, \dots, X_n]$ be the ideal generated by $X_1, \dots, X_n$.

Then $\mathfrak{m}$ consists of those rational functions $F/G \in \mathscr{O}$ where $F, G \in k[X_1, \dots, X_n]$, $F(P) = 0$ and $G(P) \neq 0$. By Problem 1.7, we can write

$$F(X_1, \dots, X_n) = \sum X_i F_i$$

for some $F_i \in k[X_1, \ldots, X_n]$. Then we have

$$\frac{F}{G} = \frac{\sum X_i F_i}{G} = \sum X_i \frac{F_i}{G},$$

showing this rational function lies in $I\mathscr{O}$.

In the other direction, each element of $I\mathscr{O}$ can be written as

$$\sum X_i \frac{F_i}{G_i},$$

where $F_i, G_i \in k[X_1, \ldots, X_n]$, with $G_i(P) \neq 0$ for all i. Since each of the summands vanishes at P, the sum lies in $\mathfrak{m}$.

This shows $I\mathscr{O} = \mathfrak{m}$. It now follows by Problem ? that $I^r\mathscr{O} = \mathfrak{m}^r$. □

2.44. Let V be a variety in $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$, $P \in V$, and let J be an ideal of $k[X_1, \ldots, X_n]$ which contains I. Let J' be the image of J in $\Gamma(V)$. Show that there is a natural homomorphism φ from $\mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n)$ to $\mathscr{O}_P(V)/J'\mathscr{O}_P(V)$, and that φ is an isomorphism. In particular, $\mathscr{O}_P(\mathbb{A}^n)/I\mathscr{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$.

Solution. *Proof.* Suppose V is a variety in $\mathbb{A}^n$, $I = I(V) \subset k[X_1, \ldots, X_n]$, $P \in V$, and suppose J is an ideal of $k[X_1, \ldots, X_n]$ which contains I. Let J' be the image of J in $\Gamma(V)$.

We have the natural quotient map $k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/I \cong \Gamma(V)$. Since both $k[X_1, \ldots, X_n]$ and $\Gamma(V)$ are integral domains, this map extends uniquely to a ring homomorphism on the quotient fields:

$$k(\mathbb{A}^n) = k(X_1, \ldots, X_n) \to \mathscr{O}(V).$$

If we limit this homomorphism to the subring $\mathscr{O}_P(\mathbb{A}^n) \subset k(\mathbb{A}^n)$ and limit the codomain to its image in $k(\mathbb{A}^n)$, we get

$$\mathscr{O}_P(\mathbb{A}^n) \to \mathscr{O}_P(V).$$

Notice that this map is surjective by definition.

We compose this with the natural quotient map to get

$$\mathscr{O}_P(\mathbb{A}^n) \to \mathscr{O}_P(V) \xrightarrow{q} \mathscr{O}_P(V)/J'\mathscr{O}_P(V).$$

Since J is contained in the kernel of this homomorphism, this homomorphism factors uniquely through the quotient ring:

$$\varphi : \mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n) \to \mathscr{O}_P(V)/J'\mathscr{O}_P(V).$$

Since the quotient map is surjective, φ is surjective.

Mark, check the following paragraph.

Let r represent an element $x \in \mathscr{O}_P(\mathbb{A}^n)/J\mathscr{O}_P(\mathbb{A}^n)$ that maps to zero under φ. Then $r \in J'\mathscr{O}_P(V)$. This implies that $r \in J\mathscr{O}_P(\mathbb{A}^n)$, so $x = 0$. Hence, φ is injective. □

2.45. Show that ideals $I, J \subset k[X_1, \ldots, X_n]$ (k algebraically closed) are comaximal if and only if $V(I) \cap V(J) = \emptyset$.

Solution. *Proof.* ($\Rightarrow$) Suppose I, J are comaximal. Then $I + J = (1)$. If $P \in V(I) \cap V(J)$, then every element of I and every element of J vanishes at P. But then every element of $I + J$ vanishes at P, so 1 vanishes at P, a contradiction.

($\Leftarrow$) Suppose $V(I) \cap V(J) = \emptyset$. Then $V(I+J) = V(I \cup J) = V(I) \cap V(J) = \emptyset$. By the Weak Nullstellensatz, $I + J = (1)$, so I and J are comaximal.

□

2.46. Let $I = (X, Y) \subset k[X, Y]$. Show that $\dim_k (k[X, Y]/I^n) = 1+2+\cdots+n = \frac{n(n+1)}{2}$.

Solution. *Proof.* The vector space $k[X, Y]/I^n$ is generated by monomials in X and Y of degree at most $n-1$. The number of these is the number monomials of the form $X^i Y^j 1^{n-i-j-1}$, that is, the number of monomials of degree exactly $n-1$ in three variables. By Problem 2.36, this number is $\binom{n-1+3-1}{3-1} = \binom{n+1}{2} = \frac{n(n+1)}{2}$.

□

2.9 Ideals With a Finite Number of Zeros

Problem

2.47. Suppose R is a ring containing k, and R is finite dimensional over k. Show that R is isomorphic to a direct product of local rings.

Solution. *Proof.* Suppose R is a ring containing k, and R is finite dimensional over k. Let $x_1, \ldots, x_n$ be a basis for R over k. Since R is finite dimensional over k, each x_i is integral over k. Hence, $k[x_1, \ldots, x_n]$ is integral over k and there is a surjective morphism $\varphi : k[x_1, \ldots, x_n] \to R$. If we let I be the kernel of φ, then R is isomorphic to $k[x_1, \ldots, x_n]/I$.

Since R is isomorphic to $k[x_1, \ldots, x_n]/I$ and is finite dimensional over k, R is an Artin ring. (See A-M, Theorem 6.10.) By the structure theorem for Artin rings, R is uniquely (up to isomorphism) a finite direct product of Artin local rings. (See A-M, Theorem 8.7.) □

2.10 Quotient Modules and Exact Sequences

Problems

2.48. Verify that for any R-module homomorphism $\varphi : M \to M'$, $\operatorname{Ker}(\varphi)$ and $\operatorname{Im}(\varphi)$ are submodules of M and M', respectively. Show that

$$0 \to \operatorname{Ker}(\varphi) \to M \xrightarrow{\varphi} \operatorname{Im}\varphi \longrightarrow 0$$

is exact.

Solution. *Proof.* This is one of the fundamental exact sequences for modules. □

2.49. (a) Let N be a submodule of M, $\pi : M \to M/N$ the natural homomorphism. Suppose $\varphi : M \to M'$ is a homomorphism of R-modules, and $\varphi(N) = 0$. Show that there is a unique homomorphism $\overline{\varphi} : M/N \to M'$ such that $\overline{\varphi} \circ \pi = \varphi$.

(b) If N and P are submodules of a module M, with $P \subset N$, then there are natural homomorphisms from M/P onto M/N and from N/P into M/P. Show that the resulting sequence

$$0 \to N/P \to M/P \to M/N \to 0$$

is exact ("Second Noether Isomorphism Theorem").

(c) Let $U \subset W \subset V$ be vector spaces, with V/U finite-dimensional. Then $\dim(V/U) = \dim(V/W) + \dim(W/U)$.

(d) If $J \subset I$ are ideals in a ring R, there is a natural exact sequence of R-modules:

$$0 \to I/J \to R/J \to R/I \to 0.$$

(e) If $\mathscr{O}$ is a local ring with maximal ideal $\mathfrak{m}$, there is a natural exact sequence of $\mathscr{O}$-modules:

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^n \to 0.$$

Solution. (a) *Proof.* Define $\overline{\varphi} : M/N \to M'$ by $\overline{\varphi}(m + N) = \varphi(m)$. Since $\varphi(N) = 0$, this map is well-defined. From this definition, we have $\overline{\varphi}\circ\pi = \varphi$ and this is the only way to define such $\overline{\varphi}$. □

(b) *Proof.* This is one of the fundamental isomorphism theorems for modules. □

(c) *Proof.* We have an exact sequence of finite dimensional vector spaces

$$0 \to W/U \to V/U \to V/W \to 0.$$

It follows that $\dim(V/U) = \dim(V/W) + \dim(W/U)$.

□

(d) *Proof.* This is one of the fundamental isomorphism theorems for modules. □

(e) *Proof.* We have $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n \subset \mathscr{O}$. Then by part (d), we have

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^n \to 0.$$

□

2.50. Let R be a DVR satisfying the conditions of Problem 2.30. Then $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an R-module, and so also a k-module, since $k \subset R$.

(a) Show that $\dim_k\left(\mathfrak{m}^n/\mathfrak{m}^{n+1}\right) = 1$ for all $n \geq 0$.

(b) Show that $\dim_k(R/\mathfrak{m}^n) = n$ for all $n > 0$.

(c) Let $z \in R$. Show that $\operatorname{ord}(z) = n$ if $(z) = \mathfrak{m}^n$, and hence that $\operatorname{ord}(z) = \dim_k(R/(z))$.

Solution. (a) *Proof.* Suppose t is a uniformizing parameter of R. Then $\mathfrak{m} = (t)$ and $\mathfrak{m}^n = (t^n)$. Then $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is generated by t^n, so it has dimension 1. □

(b) *Proof.* The vector space $R/\mathfrak{m}^n$ has basis $\{1, t, t^2, \ldots, t^{n-1}\}$. The dimension of this space is n. □

(c) *Proof.* If $\operatorname{ord}(z) = n$, then $z = ut^n$ where $u \in R$ is a unit. But then $(z) = (t^n) = (t)^n = \mathfrak{m}^n$. By part (b), $\operatorname{ord}(z) = \dim_k(R/(z))$. □

2.51. Let $0 \to V_1 \to \cdots \to V_n \to 0$ be an exact sequence of finite-dimensional vector spaces. Show that $\sum(-1)^i \dim(V_i) = 0$.

Solution. *Proof.* This is proved in A-M. □

2.52. Let N, P be submodules of a module M. Show that the subgroup $N+P = \{n + p \,|\, n \in N, p \in P\}$ is a submodule of M. Show that there is a natural R-module isomorphism of $N/N \cap P$ onto $N + P/P$ ("First Noether Isomorphism Theorem").

Solution. *Proof.* This is one of the fundamental isomorphism theorems for modules. □

2.53. Let V be a vector space, W a subspace, $T : V \to V$ a one-to-one linear map such that $T(W) \subset W$, and assume V/W and $W/T(W)$ are finite-dimensional.

(a) Show that T induces an isomorphism of V/W with $T(V)/T(W)$

(b) Construct an isomorphism between $T(V)/(W \cap T(V))$ and $(W+T(V))/W$, and an isomorphism between $W/(W \cap T(V))$ and $(W+T(V))/T(V)$.

(c) Use Problem 2.49(c) to show that $\dim(V/(W+T(V))) = \dim((W \cap T(V))/T(W))$.

(d) Conclude finally that $\dim(V/T(V)) = \dim(W/T(W))$.

Solution. Let V be a vector space, W a subspace, $T : V \to V$ a one-to-one linear map such that $T(W) \subset W$, and assume V/W and $W/T(W)$ are finite-dimensional.

(a) *Proof.* Define $\varphi : V/W \to T(V)/T(W)$ by $\varphi(v+W) = T(v) + T(W)$. Suppose $v + W = v' + W$. Then $v - v' \in W$, so $T(v) - T(v') = T(v - v') \in T(W)$, so $T(v) + T(W) = T(v') + T(W)$. Thus, φ is well-defined.

For $v_1, v_2 \in V$ and $\lambda, \mu \in k$, we have

$$\begin{aligned}\varphi(\lambda v_1 + \mu v_2) &= T(\lambda v_1 + \mu v_2) + T(W) \\ &= (\lambda T(v_1) + \mu T(v_2)) + T(W) \\ &= \lambda(T(v_1) + T(W)) + \mu(T(v_2) + T(W)) \\ &= \lambda\varphi(v_1) + \mu\varphi(v_2).\end{aligned}$$

Thus φ is a linear map of vector spaces.

The map φ is surjective by construction.

Suppose $\varphi(v+W) = 0$. Then $\varphi(v) = T(v) \in T(W)$. Since T is injective, $v \in W$, so $v + W = W$. So, φ is injective. □

(b) *Proof.* Consider the composition of morphisms

$$T(V) \to W + T(V) \to (W + T(V))/W.$$

This map is surjective and the kernel of this morphism consists of $W \cap T(V)$. Hence

$$T(V)/W \cap T(V) \cong (W + T(V))/W$$

Consider the composition of morphisms

$$W \to W + T(V) \to (W + T(V))/T(V).$$

This map is surjective and the kernel of the composition is $W \cap T(V)$. So

$$W/W \cap T(V) \cong (W + T(V))/T(V).$$

□

(c) *Proof.* By part (a), $\dim(V/W) = \dim(T(V)/T(W))$.

We have $W \subset W + T(V) \subset V$. Since V/W is finite dimensional, by Problem 2.49(c),

$$\dim(V/W) = \dim(V/(W + T(V))) + \dim((W + T(V))/W)\,.$$

We have $W \cap T(V) \subset W + T(V) \subset V$. Since V/W is finite dimensional, by Problem 2.49(c),

$$\dim(V/W \cap T(V)) = \dim(V/(W + T(V))) + \dim((W + T(V))/W \cap T(V))\,.$$

□

(d) *Proof.* We have an inclusion of vector spaces $T(W) \subset W \subset V$, which gives us an exact sequence of vector spaces

$$0 \to W/T(W) \to V/T(W) \to V/W \to 0 \tag{2.5}$$

Since V/W and $W/T(W)$ are finite dimensional, so is $V/T(W)$, and we have

$$\dim(V/T(W)) = \dim(V/W) + \dim(W/T(W)) \tag{2.6}$$

We have an inclusion of vector spaces $T(W) \subset T(V) \subset V$, which gives us an exact sequence of vector spaces

$$0 \to T(V)/T(W) \to V/T(W) \to V/T(V) \to 0 \tag{2.7}$$

We showed $V/T(W)$ is finite dimensional by exact sequence (2.5). This together with exact sequence (2.7) shows that $T(V)/T(W)$ and $V/T(V)$ are also finite dimensional. We then have

$$\dim(V/T(W)) = \dim(V/T(V)) + \dim(T(V)/T(W))\,. \tag{2.8}$$

We know from part (a) that V/W in isomorphic to $T(V)/T(W)$, so

$$\dim(V/W) = \dim(T(V)/T(W))\,. \tag{2.9}$$

Substituting (2.9) into (2.8), we have

$$\dim(V/T(W)) = \dim(V/T(V)) + \dim(V/W)\,. \tag{2.10}$$

Comparing equations (2.6) and (2.10), we have that

$$\dim(V/T(V)) = \dim(W/T(W))$$

as desired. □

Mark, think about this again and use (b) and (c) to prove (d).

2.11 Free Modules

Problems

2.54. What does M being free on $m_1, \dots, m_n$ say in terms of the elements of M?

Solution. Let $X = \{m_1, \dots, m_n\}$. Then the free module on $m_1, \dots, m_n$ is

$$M_X = \{\varphi : X \to R\}$$

If $\varphi(m_i) = r_i$, there is a correspondence between elements of M_X and elements of M of the form $\sum r_i m_i$. The module M is free on X if $M = M_X$.

So, M is free on $m_1, \dots, m_n$ means

$$M = \left\{ \sum r_i m_i \mid r_i \in R \right\}.$$

2.55. Let $F = X^n + a_1 X^{n-1} + \cdots + a_n$ be a monic polynomial in $R[X]$. Show that $R[X]/(F)$ is a free R-module with basis $\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}$, where $\overline{X}$ is the residue of X.

Solution. *Proof.* I've proved this somewhere before. □

2.56. Show that a subset X of a module M generates M if and only if the homomorphism $M_X \to M$ is onto. Every module is isomorphic to a quotient of a free module.

Solution. *Proof.* ($\Rightarrow$) Suppose a subset X of a module M generates M. Let $m \in M$. Then there exist $r_i \in R$ so that $m = \sum r_i x_i$ for some finite subset $\{x_i\} \subset X$. Let $\varphi \in M_X$ be given by

$$\varphi(x) = \begin{cases} r_i & \text{if } x = x_i \\ 0 & \text{otherwise} \end{cases}$$

The natural homomorphism $M_X \to M$ takes φ to m. So, the natural morphism is surjective.

($\Leftarrow$) Let $X \subset M$ and suppose the natural morphism $M_X \to M$ is surjective. Then for $m \in M$, there exists $\varphi \in M_X$ so that φ maps onto m under the natural morphism. But then $m = \sum_{x \in X} \varphi(x) x$. So, X generated M. □

Chapter 3

Local Properties of Plane Curves

3.1 Multiple Points and Tangent Lines

Problems

3.1. Prove that in the above example $P = (0, 0)$ is the only multiple point on the curves C, D, E, and F.

Solution. (C) $Y^2 - X^3$. We have $F_Y = 2Y$ and $F_X = -3X^2$. We see $F_X = F_Y = 0$ only at the point $(0, 0)$, so $(0, 0)$ is the only singular point.

(D) $Y^2 - X^3 - X^2$. We have $F_Y = 2Y$ and $F_X = -3X^2 - 2X$. We see $F_X = F_Y = 0$ only at the points $(0, 0)$ and $(-2/3, 0)$. However, the latter point is not on the curve, so $(0, 0)$ is the only singular point.

(E) $(X^2 + Y^2)^2 + 3X^2Y - Y^3$. We have $F_Y = 4Y(X^2 + Y^2) + 3X^2 - 3Y^2$ and $F_X = 4X(X^2 + Y^2) + 6XY$. Setting these equal to zero and solving using MAPLE, the only singular point is $(0, 0)$.

(F) $(X^2 + Y^2)^3 - 4X^2Y^2$. We have $F_Y = 6Y(X^2 + Y^2) - 8X^2Y$ and $F_X = 6X(X^2 + Y^2) - 8XY^2$. Setting these equal to zero and solving using MAPLE, the only singular point is $(0, 0)$.

3.2. Find the multiple points, and the tangent lines at the multiple points, for each of the following curves:

(a) $Y^3 - Y^2 + X^3 - X^2 + 3XY^2 + 3X^2Y + 2XY$

(b) $X^4 + Y^4 - X^2Y^2$

(c) $X^3 + Y^3 - 3X^2 - 3Y^2 + 3XY + 1$

(d) $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25)$

Sketch the part of the curve in part (d) that is contained in $\mathbb{A}^2(\mathbb{R}) \subset \mathbb{A}^2(\mathbb{C})$.

Solution. (a) Taking the two partial derivatives F_X and F_Y, as well as F equal to zero, we get the only singular point is $(0,0)$. The tangent lines are given by the lowest power terms of F: $2XY - Y^2 - X^2 = -(X - Y)^2$. So this curve has a double tangent line $X - Y = 0$.

(b) Taking the two partial derivatives F_X and F_Y, as well as F equal to zero, we get the only singular point is $(0,0)$. The tangent lines are given by the lowest power terms of F: $X^4 + Y^4 - X^2Y^2 = 0$. So this curve has four tangent lines at $Y = \pm\sqrt{\frac{1}{2} \pm \frac{\sqrt{3}}{2}i}\ X$.

(c) Taking the two partial derivatives F_X and F_Y, as well as F equal to zero, we get the only singular point is $(1,1)$. Making the change of variables $X = U+1$, $Y = V+1$, we get the polynomial $F^T(U,V) = U^3+V^3+3UV$, which has a singularity of multiplicity 2 at $(0,0)$. The tangent lines are given by the lowest power terms of F: $3UV = 0$. So the curve F^T has tangent lines at $(0,0)$ given by $U = 0$ and $V = 0$. So the curve F has tangent lines at $(1,1)$ given by $X = 1$ and $Y = 1$.

(d) Taking the two partial derivatives F_X and F_Y, as well as F equal to zero, we get the two singular points: $(\pm\sqrt{5/2}, 0)$.

Let $u = x \pm \sqrt{5/2}$ and making this substitution into F, we get each of these points is an ordinary double point.

3.3. If a curve F of degree n has a point P of multiplicity n, show that F consists of n lines through P (not necessarily distinct).

Solution. *Proof.* Without loss of generality, we may assume $P = (0,0)$. Since F has degree n and $(0,0)$ has multiplicity n, we have $F(X,Y) = F_n(X,Y) = \sum a_i X^i Y^{n-i}$. Since every form in two variables can be factored into linear factors, we have F is a product of n linear factors. So, its zero set is n (not necessarily distinct) lines.

□

3.4. Let P be a double point on a curve F. Show that P is a node if and only if $F_{XY}(P)^2 \neq F_{XX}(P)F_{YY}(P)$.

Solution. *Proof.* Without loss of generality, we may assume $P = (0,0)$. Since F has a double point at P, F has the form $aX^2 + bXY + cY^2$ plus higher order terms. We note that $F_{XX}(0,0) = 2a$, $F_{XY}(0,0) = b$ and $F_{YY}(0,0) = 2c$.

The curve F has a node at P if and only if $aX^2 + bXY + cY^2$ is not a perfect square. Thinking of F has a function of X with coefficients in $k(Y)$, we see that $aX^2 + bXY + cY^2$ is not a perfect square if and only if its discriminant is not zero. That is, $(bY)^2 - 4(a)(cY^2) = (b^2 - 4ac)Y^2 \neq 0$. So, the point P is a node if and only if $b^2 - 4ac = F_{XY}^2 - 4(\frac{1}{2}F_{XX})(\frac{1}{2}F_{YY}) = F_{XY}^2 - F_{XX}F_{YY}$ is not equal to zero. □

3.5. (char$(k) = 0$). Show that $m_P(F)$ is the smallest integer m such that for some $i + j = m$, $\dfrac{\partial^m F}{\partial X^i \partial Y^j}(P) \neq 0$. Find an explicit description for the leading form for F at P in terms of these derivatives.

Solution. The leading form for F is

$$F_m(X,Y) = \sum_{i=0}^{m} \frac{\partial^m F/\partial X^i \partial Y^{m-i}}{i!(m-i)!}(X,Y).$$

From this, we see that $m_P(F)$ is the smallest integer m such that for some $i + j = m$, $\dfrac{\partial^m F}{\partial X^i \partial Y^j}(P) \neq 0$.

3.6. Irreducible curves with given tangent lines L_i of multiplicity r_i may be constructed as follows: if $\sum r_i = m$, let $F = \prod L_i^{r_i} + F_{m+1}$, where F_{m+1} is chosen to make F irreducible (See Problem 34 of Chapter 2.)

Solution. *Proof.* This follows immediately from Problem 34 of Chapter 2.

□

3.7. (a) Show that the real part of the curve E of the example is the set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r,θ) satisfy the equation $r = -\sin(3\theta)$. Find the polar equations for the curve F.

(b) If n is an odd integer ≥ 1, show that the equation $r = \sin(n\theta)$ defines the real part of a curve of degree $n+1$ with an ordinary n-tuple point at $(0,0)$. (Use the fact that $\sin(n\theta) = \mathrm{Im}(e^{in\theta})$ to get the equation; note that rotation by $2\pi/n$ is a linear transformation which takes the curve into itself.)

(c) Analyze the singularities which arise by looking at $r^2 = \sin^2(n\theta)$, n even.

(d) Show that the curves constructed in (b) and (c) are all irreducible in $\mathbb{A}^2(\mathbb{C})$. (*Hint:* Make the polynomials homogeneous with respect to a variable Z, and use Section 6 of Chapter 2.)

Solution. (a) *Proof.* We first compute $\sin(3\theta)$:

$$\begin{aligned}\sin(3\theta) &= \sin(2\theta+\theta)\\ &= \sin(2\theta)\cos\theta + \sin\theta\cos(2\theta)\\ &= 2\sin\theta\cos\theta\cdot\cos\theta + \sin\theta\cdot(\cos^2\theta - \sin^2\theta)\\ &= 2\sin\theta\cos^2\theta + \sin\theta\cos^2\theta - \sin^3\theta\\ &= 3\sin\theta\cos^2\theta - \sin^3\theta.\end{aligned}$$

We view the polynomial $(X^2+Y^2)^2+3X^2Y-Y^3$ as lying in $\mathbb{R}[X,Y]$ and convert it to polar coordinates. We get

$$\begin{aligned}(X^2+Y^2)^2+3X^2Y-Y^3 &= (r^2)^2 + 3(r\cos\theta)^2\cdot r\sin\theta - (r\sin\theta)^3\\ &= r^4 + 3r^3\cos^2\theta\sin\theta - r^3\sin^3\theta,\end{aligned}$$

which has the same zero set as $r + 3\cos^2\theta\sin\theta - \sin^3\theta = r + \sin(3\theta)$.

□

(b) *Proof.* We convert the curve $r = \sin(n\theta)$ to rectangular coordinates.

$$\begin{aligned} r &= \sin(n\theta)\\ &= \frac{1}{2i}(e^{in\theta} - e^{-in\theta})\\ &= \frac{1}{2i}((e^{i\theta})^n - (e^{-i\theta})^n)\\ r^{n+1} &= r^n\cdot\frac{1}{2i}((e^{i\theta})^n - (e^{-i\theta})^n)\\ (r^2)^{(n+1)/2} &= \frac{1}{2i}((re^{i\theta})^n - (re^{-i\theta})^n)\\ (x^2+y^2)^{(n+1)/2} &= \frac{1}{2i}((x+iy)^n - (x-iy)^n).\end{aligned}$$

We see that this is a polynomial of degree $n+1$ and, since the lowest order term centered at $(0,0)$ has degree n, $(0,0)$ is an n-tuple multiple point. Since rotation by $2\pi/n$ rotates the curve onto itself, this rotation takes a tangent line to another tangent line. Since n is odd, none of these n rotations carries a tangent line back onto itself except the last one. Indeed, after j rotations, the curve has turned $2\pi j/n$ radians. A tangent line is carried onto itself if this is a multiple of π. If $2\pi j/n = k\pi$, then $2j = kn$. Since n is odd, this forces k to be even, so the n rotations of the tangent line are distinct. This implies the curve has n distinct tangent lines, so $(0,0)$ is an ordinary n-tuple point. □

(c) *Proof.* We convert $r^2 = \sin^2(n\theta)$, n even, into rectangular coordinates.

$$\begin{aligned}
r^2 &= \sin^2(n\theta) \\
&= \left[\frac{1}{2i}(e^{in\theta} - e^{-in\theta})\right]^2 \\
&= -\frac{1}{4}\left(e^{2in\theta} - 2 + e^{-2in\theta}\right) \\
&= -\frac{1}{4}\left((e^{i\theta})^{2n} - 2 + (e^{-i\theta})^{2n}\right) \\
r^{2n+2} &= -\frac{1}{4} \cdot r^{2n}\left((e^{i\theta})^{2n} - 2 + (e^{-i\theta})^{2n}\right) \\
r^{2n+2} &= -\frac{1}{4}\left((re^{i\theta})^{2n} - 2(r^2)^n + (re^{-i\theta})^{2n}\right) \\
(x^2+y^2)^{n+1} &= -\frac{1}{4}\left((x+iy)^{2n} - 2(x^2+y^2)^n + (x-iy)^{2n}\right).
\end{aligned}$$

We see that this is a polynomial of degree $2n+2$ and, since the lowest order term centered at $(0,0)$ has degree $2n$, $(0,0)$ is an $2n$-tuple multiple point. Since rotation by π/n rotates the curve onto itself, this rotation takes a tangent line to another tangent line. After n rotations, each tangent line has rotated π radians, so it returns to itself. This implies the curve has n distinct tangent lines, so $(0,0)$ is an non-ordinary $2n$-tuple point. □

(d) *Proof.* Following the hint, we make the two equations from parts (b) and (c) homogeneous:

$$\begin{aligned}
(X^2+Y^2)^{(n+1)/2} &= \frac{1}{2i}Z((X+iY)^n - (X-iY)^n) \\
(X^2+Y^2)^{n+1} &= -\frac{1}{4}Z^2\left((X+iY)^{2n} - 2(X^2+Y^2)^n + (X-iY)^{2n}\right)
\end{aligned}$$

Mark, finish this.

□

3.8. Let $T : \mathbb{A}^2 \to \mathbb{A}^2$ be a polynomial map, $T(Q) = P$.

(a) Show that $m_Q(F^T) \geq m_P(F)$.

(b) Let $T = (T_1, T_2)$, and define $J_Q T = (\partial T_i / \partial X_j(Q))$ to be the *Jacobian* matrix of T at Q. Show that $m_Q(F^T) = m_P(F)$ if $J_Q T$ is invertible.

(c) Show that the converse of (b) is false: Let $T = (X^2, Y)$, $F = Y - X^2$, $P = Q = (0, 0)$.

Solution. Let $T : \mathbb{A}^2 \to \mathbb{A}^2$ be a polynomial map, $T(Q) = P$. Without loss of generality, we can assume $P = Q = (0, 0)$.

(a) *Proof.* Let $F = F_m + F_{m+1} + \cdots + F_d$ be the defining equation for the curve containing P. Suppose $T : \mathbb{A}^2 \to \mathbb{A}^2$ is given by $T(X, Y) = (T_1(X, Y), T_2(X, Y))$, where T_1 and T_2 are polynomials. Then $F^T = F_m \circ T + F_{m+1} \circ T + \cdots + F_d \circ T$. The smallest power of this polynomial is the smallest power of the composition of F_m and T. Since $T(Q) = P$, T_1 and T_2 have degree at least one, so the smallest degree monomial in F^T has degree at least m. So, $m_Q(F^T) \geq m_P(F)$. □

(b) *Proof.* Mark, I don't think this proof is correct.

Let $J_Q T = (\partial T_i / \partial X_j(Q))$ to be the Jacobian matrix of T at Q. By the Chain Rule, we have

$$\begin{bmatrix} \frac{\partial F_m \circ T}{\partial X_1} & \frac{\partial F_m \circ T}{\partial X_2} \end{bmatrix}(Q) = \begin{bmatrix} \frac{\partial F_m}{\partial T_1}(P) & \frac{\partial F_m}{\partial T_2}(P) \end{bmatrix} \begin{bmatrix} \frac{\partial T_1}{\partial X_1}(Q) & \frac{\partial T_1}{\partial X_2}(Q) \\ \frac{\partial T_2}{\partial X_1}(Q) & \frac{\partial T_2}{\partial X_2}(Q) \end{bmatrix}$$

If $J_Q T$ is invertible, then the matrix

$$\begin{bmatrix} \frac{\partial F_m \circ T}{\partial X_1} & \frac{\partial F_m \circ T}{\partial X_2} \end{bmatrix}(Q)$$

and the matrix

$$\begin{bmatrix} \frac{\partial F_m}{\partial X_1} & \frac{\partial F_m}{\partial X_2} \end{bmatrix}(P)$$

have the same rank. This forces $m_Q(F^T) = m_P(F)$. □

(c) *Proof.* Let $T = (X^2, Y)$, $F = Y - X^2$, $P = Q = (0, 0)$. Then $F^T(X, Y) = F(X^2, Y) = Y - X^4$.

We compute

$$\begin{bmatrix} \frac{\partial T_i}{\partial X_j} \end{bmatrix} = \begin{bmatrix} 2X & 0 \\ 0 & 1 \end{bmatrix},$$

which is singular at $(0, 0)$. However, both curves are nonsingular at $(0, 0)$, so $m_Q(F^T) = m_P(F) = 1$.

□

3.9. Let $F \in k[X_1, \ldots, X_n]$ define a hypersurface $V(F) \subset \mathbb{A}^n$. Let $P \in \mathbb{A}^n$.

(a) Define the multiplicity $m_P(F)$ of F at P.

(b) If $m_P(F) = 1$, define the tangent hyperplane to F at P.

(c) Examine $F = X^2 + Y^2 - Z^2$, $P = (0, 0, 0)$. Is it possible to define tangent hyperplanes at multiple points?

Solution. (a) Let $F \in k[X_1, \ldots, X_n]$ define a hypersurface $V(F) \subset \mathbb{A}^n$. Let $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$. Write

$$F(X_1, \ldots, X_n) = \sum_J c_J \prod_i (X_i - a_i)^{j_i}.$$

where J ranges over all n-tuples $(j_1, \ldots, j_n)$ and only finitely many of the c_J's are nonzero. The multiplicity of F at P is the degree of the smallest nonzero form in this expression.

(b) *Proof.* Suppose $m_P(F) = 1$. Then the constant term is zero and the degree one form is not. For J's corresponding to degree one, we just have $j_k = 1$ for exactly one k and $j_i = 0$ for $i \neq k$. So, the lowest degree nonzero form in the expansion of F has the form

$$\sum_k c_k (X_k - a_k).$$

Setting this equal to zero gives the equation of the tangent hyperplane to the hypersurface $V(F)$ at P. □

(c) *Proof.* Probably not since the form of lowest degree in three (or more) variables usually doesn't factor into linear factors. □

3.10. Show that an irreducible plane curve has only a finite number of multiple points. Is this true for hypersurfaces?

Solution. *Proof.* Let an irreducible plane curve be defined by $F(X, Y) = 0$. Then F is irreducible and $I(V(F)) = (F)$. If $V(F)$ has infinitely many multiple points, then $V(F)$ and $V(F_X)$ have infinitely many points of intersection. By Proposition 2 of Section 6 of Chapter 1, F and F_X must have a common factor, and since F is irreducible, F must divide F_X. Since the degree of F in X is larger than the degree of F_X in X, this is not possible.[1] So, there are only finitely many points where F and F_X are both zero. It follows that $V(F)$ has only finitely many multiple points. □

In $\mathbb{A}^3(k)$, the hypersurface defined by the polynomial $X^2 - Y^2$ is the union of two planes meeting in a line, so this hypersurface has a line of singular points.

[1] It is possible for F to divides F_X if $F_X \equiv 0$. However, if $F_X \equiv 0$, then k has characteristic p and F is a polynomial in X^p. But then F is not irreducible.

3.11. Let $V \subset \mathbb{A}^n$ be an affine variety, $P \in V$. The *tangent space* $T_P(V)$ is defined to be $\{(v_1, \ldots, v_n) \in \mathbb{A}^n \mid \text{for all } G \in I(V), \sum G_{X_i}(P)v_i = 0\}$. If $V = V(F)$ is a hypersurface, F irreducible, show that $T_P(V) = \{(v_1, \ldots, v_n) \mid \sum F_{X_i}(P)v_i = 0\}$. How does the dimension of $T_P(V)$ relate to the multiplicity of F at P?

Solution. *Proof.* Let $V = V(F)$ be a hypersurface with F irreducible. Fix $P \in V$. First, we have $I(V) = (F)$ by Corollary 3 to the Nullstellensatz. Let $G \in I(V)$. Then $G = FH$. Then

$$\begin{aligned} G_{X_i} &= F_{X_i}H + FH_{X_i} \\ G_{X_i}(P) &= F_{X_i}(P)H(P) + F(P)H_{X_i}(P) \\ &= F_{X_i}(P)H(P) \\ \sum G_{X_i}(P)v_i = 0 &\Leftrightarrow H(P)\sum F_{X_i}(P)v_i = 0. \end{aligned}$$

Certainly it's possible for $H(P)$ to be zero, but there certainly exist H so that $H(P)$ is not zero. Hence,

$$\sum G_{X_i}(P)v_i = 0 \Leftrightarrow \sum F_{X_i}(P)v_i = 0$$

So, we see the tangent space $T_P(V)$ is given by

$$\{(v_1, \ldots, v_n) \in \mathbb{A}^n \mid \sum F_{X_i}(P)v_i = 0\}.$$

From this, if P is a simple point of V, then $T_P(V)$ is a hyperplane in $\mathbb{A}^n$, so $\dim(T_P(V)) = n-1$. On the other hand, if P is a singular point of V, then the form of degree 1 in F vanishes, so $F_{X_i}(P) = 0$ for all $1 \leq i \leq n$. In this case, $T_P(V)$ is all of $\mathbb{A}^n$, so $\dim(T_P(V)) = n$.

□

3.2 Multiplicities and Local Rings

Problems

3.12. A simple point P on a curve F is called a *flex* if $\text{ord}_P^F(L) \geq 3$,where L is the tangent to F at P. The flex is called *ordinary* if $\text{ord}_P(L) = 3$, a *higher* flex otherwise.

(a) Let $F = Y - X^n$. For which n does F have a flex at $P = (0,0)$, and what kind of flex?

(b) Suppose $P = (0,0)$, $L = Y$ is the tangent line, $F = Y + aX^2 + \cdots$. Show that P is a flex on F if and only if $a = 0$. Give a simple criterion for calculating $\text{ord}_P^F(Y)$, and therefore for determining if P is a higher flex.

Solution. (a) *Proof.* For $F = Y - X^n$ with $n \geq 2$, the tangent line is $Y = 0$. Since $P = (0,0)$ is a smooth point, we can choose any line through P not tangent to $V(F)$ at P as the uniformizing parameter. We choose X. Then $\text{ord}_P^F(L) = n$. So, P is an ordinary flex if $n = 3$ and a higher flex if $n \geq 4$. □

(b) *Proof.* Suppose $P = (0,0)$, $L = Y$ is the tangent line, $F = Y + aX^2 + \cdots$. Since $\partial F/\partial Y = 1 \neq 0$, the Implicit Function Theorem means X is a local parameter. The quadratic term here is $aX^2 + bXY + cY^2$. Since $L = Y$ is tangent to the curve, the order of contact of this line with the curve is at least two, so the valuation of Y is at least two. It follows that the valuation of XY is at least three and the valuation of Y^2 is at least four. Hence, $P = (0,0)$ is flex if and only if $a = 0$. □

3.13. With the notation of Theorem 2 in Chapter 3, and $\mathfrak{m} = \mathfrak{m}_P(F)$, show that $\dim_k\left(\mathfrak{m}^n/\mathfrak{m}^{n+1}\right) = n + 1$ for $0 \leq n < m_P(F)$. In particular, P is a simple point if and only if $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) = 1$; otherwise $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) = 2$.

Solution. *Proof.* If $0 \leq n < m_P(F)$, then $F \in I^{n+1} \subseteq I^n$, so

$$\mathscr{O}/\mathfrak{m}^n \cong \mathscr{O}_P(F)/I^n\mathscr{O}_P(F) \cong \mathscr{O}_P(\mathbb{A}^2)/(I^n, F)\mathscr{O}_P(\mathbb{A}^2) \cong k[X,Y]/(I^n, F) \cong k[X,Y]/(I^n)$$

and this vector space over k has dimension $n(n+1)/2$.

Using the exact sequence

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^{n+1} \to \mathscr{O}/\mathfrak{m}^n,$$

we see that

$$\begin{aligned}\dim\left(\mathfrak{m}^n/\mathfrak{m}^{n+1}\right) &= \dim\left(\mathscr{O}/\mathfrak{m}^{n+1}\right) - \dim\left(\mathscr{O}/\mathfrak{m}^n\right) \\ &= \frac{(n+2)(n+1)}{2} - \frac{n(n+1)}{2} \\ &= n+1.\end{aligned}$$

□

3.14. Let $V = V(X^2 - Y^3, Y^2 - Z^3) \subset \mathbb{A}^3$, $P = (0,0,0)$, $\mathfrak{m} = \mathfrak{m}_P(V)$. Show that $\dim_k\left(\mathfrak{m}/\mathfrak{m}^2\right) = 3$. (See Problem 40 in Chapter 1.)

Solution. *Proof.* By Problem 40(a) in Chapter 1, every element of $\Gamma(V)$ can be written as the residue of $A + XB + YC + XYD$ where $A, B, C, D \in k[Z]$. □

Mark, finish this one.

3.15. (a) Let $\mathscr{O} = \mathscr{O}_P(\mathbb{A}^2)$ for some $P \in \mathbb{A}^2$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^2)$. Calculate $\chi(n) = \dim_k\left(\mathscr{O}/\mathfrak{m}^n\right)$.

(b) Let $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^r(k))$. Show that $\chi(n)$ is a polynomial of degree r in n, with leading coefficient $1/r!$. (See Problem 2.36.)

Solution. (a) *Proof.* From the work for Theorem 2, we have

$$\mathcal{O}/\mathfrak{m}^n \cong k[X,Y]/I^n$$

so

$$\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[X,Y]/I^n) = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n.$$

□

(b) *Proof.* From the work for Theorem 2,

$$\begin{aligned}\chi(n) &= \dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[X_1,\dots,X_r]/I^n)\\ &= \binom{n+r-1}{r} = \frac{(n+r-1)(n+r-2)\cdots(n+1)n}{r!}.\end{aligned}$$

From this we see that $\chi(n)$ is a polynomial in n of degree r with leading coefficient $1/r!$. □

3.16. Let $F \in k[X_1,\dots,X_r]$ define a hypersurface in $\mathbb{A}^r$. Write $F = F_m + F_{m+1} + \dots$, and let $m = m_P(F)$ where $P = (0,\dots,0)$. Suppose F is irreducible, and let $\mathcal{O} = \mathcal{O}_P(V(F))$, $\mathfrak{m}$ its maximal ideal. Show that $\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n)$ is a polynomial of degree $r-1$ for sufficiently large n, and that the leading coefficient of χ is $m_P(F)/(r-1)!$.

Can you find a definition for the multiplicity of a local ring which makes sense in all the cases you know?

Solution. *Proof.* From the proof of Theorem 2, we have an analogous result

$$\mathcal{O}/\mathfrak{m}^n \cong k[X_1,\dots,X_r]/(I^n, F).$$

Using the analogous exact sequence to the one used in the proof of Theorem 2,

$$0 \to k[X_1,\dots,X_r]/I^{n-m} \xrightarrow{\psi} k[X_1,\dots,X_r]/I^n \xrightarrow{\phi} k[X_1,\dots,X_r]/(I^n,F) \to 0,$$

we see that

$$\begin{aligned}\chi(n) &= \dim_k(k[X_1,\dots,X_r]/(I^n,F))\\ &= \dim_k(k[X_1,\dots,X_r]/I^n) - \dim_k\left(k[X_1,\dots,X_r]/I^{n-m}\right)\\ &= \binom{n+r-1}{r} - \binom{n-m+r-1}{r}.\end{aligned}$$

In this expression, the n^r cancels. The next term is the n^{r-1} term, so this is a polynomial of degree $r-1$ in n. The coefficient of n^{r-1} is

$$\begin{aligned}
&\frac{1+2+\cdots+(r-1)}{r!} - \frac{m+(m+1)+(m+2)+\cdots+(m+r-1)}{r!} \\
&= \frac{1+2+\cdots+(r-1)}{r!} - \frac{-rm+(1+2+(r-1))}{r!} \\
&= \frac{rm}{r!} \\
&= \frac{m}{(r-1)!},
\end{aligned}$$

proving the result. □

3.3 Intersection Numbers

Problems

3.17. Find the intersection numbers of various pairs of curves from the examples of Section 3.1, at the point $P = (0,0)$.

Solution. A: $Y - X^2$ B: $Y^2 - X^3 + X$ C: $Y^2 - X^3$ D: $Y^2 - X^3 - X^2$

(a) $A \cap B$ at $P(0,0)$

$$\begin{aligned}
I(P, A\cap B) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(A,B)\right) \\
&= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(Y-X^2, Y^2-X^3+X)\right).
\end{aligned}$$

The curves A and B are nonsingular and meet transversely at $(0,0)$. So, $I(A\cap B, P) = m_F(P)m_G(P) = 1$.

(b) $A \cap C$ at $P(0,0)$

$$\begin{aligned}
I(P, A\cap C) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(A,B)\right) \\
&= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(Y-X^2, Y^2-X^3)\right)
\end{aligned}$$

The curve C is singular at $(0,0)$ and the two curves share the tangent Y. We'll replace C by $E = C - YA = X^2(Y-X)$. Then

$$I(A\cap C, P) = I(A\cap E, P) = 2I(A\cap X, P) + I(A\cap (Y-X), P) = 3.$$

(c) $A \cap C$ at $Q(1,1)$

$$\begin{aligned}
I(Q, A\cap C) &= \dim_k \left(\mathscr{O}_Q(\mathbb{A}^2)/(A,B)\right) \\
&= \dim_k \left(\mathscr{O}_Q(\mathbb{A}^2)/(Y-X^2, Y^2-X^3)\right)
\end{aligned}$$

(d) $C \cap D$ at $P(0,0)$

$$\begin{aligned} I(P, C \cap D) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(A, B) \right) \\ &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(Y^2 - X^3, Y^2 - X^3 - X^2) \right) \end{aligned}$$

3.18. Give a proof of Property 8 which use only Properties 1–7.

Solution. *Proof.* □

3.19. A line L is tangent to a curve F at a point P if and only if $I(P, F \cap L) > m_P(F)$.

Solution. *Proof.*

$$I(P, F \cap L) = \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, L) \right)$$

□

3.20. If P is a simple point on F, then $I(P, F \cap (G + H)) \geq \min(I(P, F \cap G), I(P, F \cap H))$. Give an example to show that this may be false if P is not simple on F.

Solution. *Proof.* Suppose $I(P, F \cap G) = m$ and $I(P, F \cap H) = n$. Then

$$\begin{aligned} I(P, F \cap G)) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, G) \right) \\ &= m \end{aligned}$$

and

$$\begin{aligned} I(P, F \cap H) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, H) \right) \\ &= n \end{aligned}$$

$$I(P, F \cap (G + H)) = \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, G + H) \right)$$

□

3.21. Let F be an affine plane curve. Let L be a line which is not a component of F. Suppose $L = \{(a + tb, c + td) \mid t \in k\}$. Define $G(T) = F(a + Tb, c + Td)$. Factor $G(T) = \epsilon \prod (T - \lambda_i)^{e_i}$, λ_i distinct. Show that there is a natural one-to-one correspondence between the λ_i and the points $P_i \in L \cap F$. Show that under this correspondence, $I(P_i, L \cap F) = e_i$. In particular, $\sum I(P, L \cap F) \leq \deg(F)$.

Solution. *Proof.* □

3.22. Suppose P is a double point on a curve F, and suppose F has only one tangent L at P.

(a) Show that $I(P, F \cap L) \geq 3$. The curve F is said to have a(n ordinary) *cusp* at P if $I(P, F \cap L) = 3$.

(b) Suppose $P = (0,0)$, and $L = Y$. Show that P is a cusp if and only if $F_{XXX}(P) \neq 0$. Give some examples.

(c) Show that if P is a cusp on F, then F has only one component passing through P.

Solution. Suppose P is a double point on a curve F, and suppose F has only one tangent L at P.

(a) *Proof.* We compute

$$\begin{aligned} I(P, F \cap L)) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, L)\right) \\ &= \end{aligned}$$

□

(b) *Proof.* Suppose $P = (0,0)$, and $L = Y$. We compute

$$\begin{aligned} I(P, F \cap Y)) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, Y)\right) \\ &= \end{aligned}$$

□

(c) *Proof.* Suppose $P = (0,0)$, $L = Y$, and P is a cusp on F. Assume more than one component of F passes through P. We compute

$$\begin{aligned} I(P, F \cap L)) &= \dim_k \left(\mathscr{O}_P(\mathbb{A}^2)/(F, L)\right) \\ &= \end{aligned}$$

□

3.23. A point P on a curve F is called a *hypercusp* if $m_P(F) > 1$, F has only one tangent line L at P, and $I(P, L \cap F) = m_P(F) + 1$. Generalize the results of the preceding problem to this case.

Solution. A point P on a curve F is called a *hypercusp* if $m_P(F) > 1$, F has only one tangent line L at P, and $I(P, L \cap F) = m_P(F) + 1$.

Proof. □

3.24. The object of this problem is to find a property of the local ring $\mathscr{O}_P(F)$ that determines whether or not P is an ordinary multiple point on F.

Let F be an irreducible plane curve, $P = (0,0)$, $m = m_P(F) > 1$. Let $\mathfrak{m} = \mathfrak{m}_P(F)$. For $G \in k[X,Y]$, denote its residue in $\Gamma(F)$ by g; and for $g \in \mathfrak{m}$, denote its residue in $\mathfrak{m}/\mathfrak{m}^2$ by $\overline{g}$.

(a) Show that the map from {forms of degree 1 in $k[X,Y]$} to $\mathfrak{m}/\mathfrak{m}^2$ taking $aX+bY$ to $\overline{ax+by}$ is an isomorphism of vector spaces (See Problem 3.13).

(b) Suppose P is an ordinary multiple point, with tangents $L_1, \ldots, L_m$. Show that $I(P, F \cap L_i) > m$ and $\overline{\ell}_i \neq \lambda \overline{\ell}_j$ for all $i \neq j$, all $\lambda \in k$.

(c) Suppose there are $G_1, \ldots, G_m \in k[X,Y]$ such that $I(P, F \cap G_i) > m$ and $\overline{g}_i \neq \lambda \overline{g}_j$ for all $i \neq j$, and all $\lambda \in k$. Show that P is an ordinary multiple point on F. (*Hint:* Write $G_i = L_i +$ higher terms. $\overline{\ell}_i = \overline{g}_i \neq 0$, and L_i is the tangent to G_i, so L_i is tangent to F by Property **??** of intersection numbers. Thus F has m tangents at P.)

(d) Show that P is an ordinary multiple point on F if and only if there are $g_1, \ldots, g_m \in \mathfrak{m}$ such that $\overline{g}_i \neq \lambda \overline{g}_j$ for all $i \neq j$, $\lambda \in k$, and $\dim(\mathscr{O}_P(F)/(g_i)) > m$.

Solution. (a) *Proof.* ☐

(b) *Proof.* ☐

(c) *Proof.* ☐

(d) *Proof.* ☐

Chapter 4

Projective Varieties

4.1 Projective Space

Problems

4.1. What points in $\mathbb{P}^2$ do not belong to two of the three sets U_1, U_2, U_3?

Solution. *Proof.* The complement of the union of U_1 and U_2 is the intersection the complements. The complement of U_1 is $\{[0 : Y : Z] : Y, Z \in k,\text{ one not zero}\}$ and the complement of U_2 is $\{[X : 0 : Z] : X, Z \in k,\text{ one not zero}\}$. The intersection of these two complements is $\{[0 : 0 : Z] : X \in k, Z \neq 0\} = \{[0 : 0 : 1]\}$. The other two are similar. □

4.2. Let $F \in k[X_1, \ldots, X_{n+1}]$ (k infinite). Write $F = \sum F_i$, F_i a form of degree i. Let $P \in \mathbb{P}^n(k)$, and suppose $F(x_1, \ldots, x_{n+1}) = 0$ for every choice of homogeneous coordinates $(x_1, \ldots, x_{n+1})$ for P. Show that each $F_i(x_1, \ldots, x_{n+1}) = 0$ for all homogeneous coordinates for P. (*Hint:* Consider $G(\lambda) = F(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum \lambda^i F_i(x_1, \ldots, x_{n+1})$ for fixed $(x_1, \ldots, x_{n+1})$.)

Solution. *Proof.* Let $F \in k[X_1, \ldots, X_{n+1}]$ (k infinite). Write $F = \sum F_i$, F_i a form of degree i. Let $P \in \mathbb{P}^n(k)$, and suppose $F(x_1, \ldots, x_{n+1}) = 0$ for every choice of homogeneous coordinates $(x_1, \ldots, x_{n+1})$ for P.

Consider $G(\lambda) = F(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum \lambda^i F_i(x_1, \ldots, x_{n+1})$ for fixed $(x_1, \ldots, x_{n+1})$.

This a polynomial in λ with infinitely many roots, so the polynomial is identically zero. This says that $F_i(x_1, \ldots, x_{n+1}) = 0$ for all i. Since $(x_1, \ldots, x_{n+1})$ are arbitrary homogeneous coordinates, $F_i(x_1, \ldots, x_{n+1}) = 0$ for all i and for all homogeneous coordinates $(x_1, \ldots, x_{n+1})$ for P. □

4.3. (a) Show that the definitions of this section carry over without change to the case where k is an arbitrary field.

(b) If k_0 is a subfield of k, show that $\mathbb{P}^n(k_0)$ may be identified with a subset of $\mathbb{P}^n(k)$.

Solution. (a) *Proof.* I don't understand the question since k is an arbitrary field to start with. □

(b) *Proof.* Let k_0 be a subfield of k. Then

$$\mathbb{P}^n(k_0) = \{[x_0 : \cdots : x_n] \,|\, x_i \in k_0, \text{ one nonzero}\}$$

Since $k_0 \subset k$, the above set is a subset of

$$\mathbb{P}^n(k) = \{[x_0 : \cdots : x_n] \,|\, x_i \in k, \text{ one nonzero}\}$$

□

4.2 Projective Algebraic Sets

Problems

4.4. Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$. Show that I is prime if and only if the following condition is satisfied: for any forms $F, G \in k[X_1, \ldots, X_{n+1}]$, if $FG \in I$, then $F \in I$ or $G \in I$.

Solution. *Proof.* Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$.

($\Leftarrow$) Suppose I is a homogeneous prime ideal. Suppose F, G are forms in $k[X_1, \ldots, X_{n+1}]$ and $FG \in I$. Since I is prime, either F or G is in I.

($\Rightarrow$) Suppose for any forms $F, G \in k[X_1, \ldots, X_{n+1}]$, if $FG \in I$, then $F \in I$ or $G \in I$.

Suppose P, $Q \in k[X_1, \ldots, X_{n+1}]$ with $PQ \in I$. Write $P = P_i + \cdots + P_d$ and $Q = Q_j + \cdots + Q_e$ be P and Q written as a sum of forms with P_i, $Q_j \neq 0$.

Assume neither P nor Q lies in I. Let $i \leq k \leq d$ be the largest integer with P_k not in I. Let $j \leq \ell \leq e$ be the smallest integer with Q_ℓ not in I. Then the form of degree $k + \ell$ in PQ is

$$P_k Q_\ell + P_{k+1} Q_{\ell-1} + P_{k+2} Q_{\ell-2} + \cdots$$

Since $PQ \in I$ and I is homogeneous, this element is in I, and by the choice of k and ℓ, $P_k Q_\ell \in I$. By hypothesis then, P_k or Q_ℓ is in I. This contradicts the choice of k and ℓ. So, either P or Q lies in I. That is, I is a prime ideal. □

4.5. If I is a homogeneous ideal, show that $\mathrm{Rad}(I)$ is also homogeneous.

Solution. *Proof.* Let I be a homogeneous ideal. Suppose $P \in \mathrm{Rad}(I)$. Write $P = P_0 + \cdots + P_d$ as a sum of forms. Since $P \in \mathrm{Rad}(I)$, $P^n \in I$ for some $i \in \mathbb{Z}$. The highest powered form of P^n is P_d^n and since I is homogeneous, $P_d^n \in I$. But then $P_d \in \mathrm{Rad}(I)$. Subtracting P_d from P, we have $P - P_d \in \mathrm{Rad}(I)$. The result follows by induction. □

4.6. State and prove the projective analogues of properties (1)–(10) of Chapter 1, Sections 2 and 3.

(1) If I is the homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$ generated by S, then $V(S) = V(I)$; so every algebraic set is equal to $V(I)$ for some ideal I.

(2) If $\{I_\alpha\}$ is any collection of homogeneous ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$; so the intersection of any collection of algebraic sets is an algebraic set.

(3) If $I \subset J$, then $V(I) \supset V(J)$.

(4) $V(FG) = V(F) \cup V(G)$ for any polynomials F, G.

$$V(I) \cup V(J) = V(\{FG \,|\, F \in I, G \in J\});$$

so any finite union of algebraic sets is an algebraic set.

(5) $V(0) = \mathbb{A}^n(k)$; $V(1) = \emptyset$; $V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$ for $a_i \in k$. So any finite subset of $\mathbb{A}^n(k)$ is an algebraic set.

(6) If $X \subset Y$ then $I(X) \supset I(Y)$.

(7) $I(\emptyset) = k[X_1, \ldots, X_n]$. $I(\mathbb{A}^n(k)) = (0)$ if k is an infinite field. $I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$ for $a_1, \ldots, a_n \in k$.

(8) $I(V(S)) \supset S$ for any set S of polynomials; $V(I(X)) \supset X$ for any set X of points.

(9) $V(I(V(S))) = V(S)$ for any set S of polynomials, and $I(V(I(X))) = I(X)$ for any set X of points. So if V is an algebraic set, $V = V(I(V))$, and if I is the ideal of an algebraic set, $I = I(V(I))$.

Solution. *Proof.* (1) Since $S \subset I$, we have $V(I) \subset V(S)$. However, every element of I is a linear combination of elements of S, so if every element of S vanishes at P, so does every element of I.

(2) If $\{I_\alpha\}$ is any collection of homogeneous ideals, then $I_\alpha \subset \bigcup_\alpha I_\alpha$ for all α, so $V(\bigcup_\alpha I_\alpha) \subset \bigcap_\alpha V(I_\alpha)$.

If $P \in V(I_\alpha)$ for all α, then every element of I_α vanishes at P for every α. But this says that $P \in V(\bigcup_\alpha I_\alpha)$. Hence, $\bigcap_\alpha V(I_\alpha) \subset V(\bigcup_\alpha I_\alpha)$.

So, $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.

(3) Suppose $I \subset J$ and $P \in V(J)$. Since $P \in V(J)$, every element of J vanishes at P. However, $I \subset J$, so every element of I vanishes at P. But this says $P \in V(I)$. Hence, $V(J) \subset V(I)$.

(4) Let $F, G \in k[x_1, \ldots, x_{n+1}]$. For $P \in V(FG)$, the product $F(P)G(P) = 0$. Hence, either $F(P) = 0$ or $G(P) = 0$, so that $P \in V(F)$ or $P \in V(G)$. Thus, we see that $V(FG) \subset V(F) \cup V(G)$.

Suppose $P \in V(F) \cup V(G)$. Then $F(P) = 0$ or $G(P) = 0$, hence $F(P)G(P) = 0$, and $P \in V(FG)$. Thus, we see that $V(F) \cup V(G) \subset V(FG)$. Hence $V(FG) = V(F) \cup V(G)$.

Let I, J be homogeneous ideals in $k[x_1, \ldots, x_{n+1}]$. First, $IJ \subset I$ and $IJ \subset J$, so $IJ \subset I \cap J$. Hence

$$V(I \cap J) = V(I) \cup V(J) \subset V(IJ).$$

Let $P \in V(IJ)$. If $P \in V(I)$, we are done, so assume $P \notin V(I)$. Then there exists $F \in I$ so that $F(P) \neq 0$. But since $P \in V(IJ)$, it follows that $F(P)G(P) = 0$ for all $G \in J$, and since $F(P) \neq 0$, we must have that $G(P) = 0$ for all $G \in J$, whereby $P \in V(J)$. Thus, we see that $P \in V(IJ) \subset V(I) \cup V(J)$. It follows that $V(IJ) = V(I) \cup V(J)$.

So, any intersection of algebraic sets is an algebraic set and any finite union of algebraic sets is an algebraic set.

(5) (5) is clear.

(6) Suppose $P \in X \subset Y$ and $F \in I(Y)$. Since $P \in Y$, $F(P) = 0$, and this is true for all $F \in I(Y)$. Hence, F vanishes on X, so $F \in I(X)$. Hence, $I(Y) \subset I(X)$.

□

4.7. Show that each irreducible component of a cone is also a cone.

Solution. *Proof.* □

4.8. Let $V = \mathbb{P}^1$, $\Gamma_h(V) = k[X, Y]$. Let $t = X/Y \in k(V)$, and show that $k(V) = k(t)$. Show that there is a natural one-to-one correspondence between the points of $\mathbb{P}^1$ and the DVR's with quotient field $k(V)$ which contain k (See Problem 2.2.27); which DVR corresponds to the point at infinity?

Solution. *Proof.* Define a homomorphism $h : k(V) \to k(t)$ as follows. For $f = P/Q \in k(V)$ with $\deg P = \deg Q = d$, divide the numerator and denominator by X^d and replace Y/X by t. This gives a homomorphism. The inverse homomorphism is given by taking $q(t) \in k(t)$, substituting Y/X for t and multiplying the numerator and denominator by a high enough power of X to clear all denominators in the complex fraction. This shows $k(V) = k(t)$.

From Problem 2.27, we know all the DVRs in $k(t)$ are $\mathscr{O}_a(V)$ with uniformizing parameter $t = X - a$ for $a \in k$ and $\mathscr{O}_\infty$ with uniformizing parameter $t = 1/X$. The one-to-one correspondence is given as follows. For $[a:1] \in \mathbb{P}^1$, assign the DVR $\mathscr{O}_a(V)$. Then assign the remain point of $\mathbb{P}^1$, $[1:0]$, the DVR $\mathscr{O}_\infty$. □

4.9. Let I be a homogeneous ideal in $k[X_1, \ldots, X_{n+1}]$, and

$$\Gamma = k[X_1, \ldots, X_{n+1}]/I.$$

Show that the forms of degree d in Γ form a finite-dimensional vector space over k.

Solution. *Proof.* The set of monomials of degree d in $n+1$ variables forms a finite dimensional vector space over k with basis $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} X_{n+1}^{d - \sum_j i_j}$. This vector space has dimension $\binom{n+d}{d}$. The natural quotient homomorphism

$$k[X_1, \ldots, X_{n+1}] \to k[X_1, \ldots, X_{n+1}]/I = \Gamma.$$

shows that Γ is a vector space over k of dimension at most $\binom{n+d}{d}$. □

4.10. Let $R = k[X,Y,Z]$, $F \in R$ an irreducible form of degree n, $V = V(F) \subset \mathbb{P}^2$, $\Gamma = \Gamma_h(V)$.

(a) Construct an exact sequence $0 \to R \overset{\psi}{\to} R \overset{\varphi}{\to} \Gamma \to 0$, where ψ is multiplication by F.

(b) Show that

$$\dim_k \{\text{forms of degree } d \text{ in } \Gamma\} = dn - \frac{1}{2}n(n-3)$$

if $d > n$.

Solution. Let $R = k[X,Y,Z]$, $F \in R$ an irreducible form of degree n, $V = V(F) \subset \mathbb{P}^2$, $\Gamma = \Gamma_h(V)$.

(a) *Proof.* Define $\psi : R \to R$ by $\psi(G) = FG$ and let $\varphi : R \to \Gamma$ to be the natural quotient map. It's easy to see that both ψ and φ are ring homomorphisms. Since R is an integral domain and $F \neq 0$, ψ is injective. The map φ is surjective since every quotient map is surjective. Since the image of ψ is contained in the ideal (F), $\operatorname{Im}\psi \subset \operatorname{Ker}(\varphi)$. If $\phi(G) = 0$, then $G \in (F)$, so that there exists $H \in R$ such that $G = FH$. Then $G = \psi(H)$. Thus, $\operatorname{Ker}(\phi) \subset \operatorname{Im}\psi$. This shows that $\operatorname{Ker}(\phi) = \operatorname{Im}\psi$, so that the sequence $0 \to R \overset{\psi}{\to} R \overset{\varphi}{\to} \Gamma \to 0$, is exact. □

(b) *Proof.* Let Γ_d denote the forms of degree d in Γ. Then the exact sequence from part (a), yields $0 \to R_{d-n} \overset{\psi}{\to} R_d \overset{\varphi}{\to} \Gamma_d \to 0$, where R_m are the forms of degree m in R. Now, the dimension of R_m is $\binom{m+2}{2}$. So

$$\begin{aligned}\dim(\Gamma_d) = \dim(R_d) - \dim(R_{d-n}) &= \binom{d+2}{2} - \binom{d-n+2}{2} \\ &= dn - \frac{1}{2}n(n-3).\end{aligned}$$

□

4.11. A set $V \subset \mathbb{P}^n(k)$ is called a *linear subvariety* of $\mathbb{P}^n(k)$ if $V = V(H_1, \ldots, H_r)$, where each H_i is a form of degree 1.

(a) Show that if T is a projective change of coordinates, then $V^T = T^{-1}(V)$ is also a linear subvariety.

(b) Show that there is a projective change of coordinates T of $\mathbb{P}^n$ such that $V^T = V(X_{m+2}, \ldots, X_{n+1})$, so V is a variety.

(c) Show that the m which appears in part (b) is independent of the choice of T. It is called the *dimension* of V ($m = -1$ if $V = \emptyset$).

Solution. If V is an algebraic set in $\mathbb{P}^n$, then $T^{-1}(V)$ is also an algebraic set in $\mathbb{P}^n$; we write V^T for $T^{-1}(V)$. If $V = V(F_1, \ldots, F_r)$, and $T = (T_1, \ldots, T_{n+1})$, T_i forms of degree 1, then $V^T = V(F_1^T, \ldots, F_r^T)$, where $F_i^T = F_i(T_1, \ldots, T_{n+1})$.

(a) *Proof.* Let $V \subset \mathbb{P}^n(k)$ is be a linear subvariety of $\mathbb{P}^n(k)$ given by $V = V(H_1, \ldots, H_r)$, where each H_i is a form of degree 1. Let $T : \mathbb{P}^n \to \mathbb{P}^n$ be a projective change of coordinates. Then T is given by $T = (T_1, \ldots, T_{n+1})$ where T_i are forms of degree 1. Then $V^T = T^{-1}V$ is given by $(H_1^T, \ldots, H_{n+1}^T)$. Since the composition of two forms of degree 1 is a form of degree 1, V^T is a linear subvariety. □

(b) *Proof.* □

(c) *Proof.* □

4.12. Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbb{P}^n$, $m \leq n$. Show that $H_1 \cap H_2 \cap \cdots \cap H_m \neq \emptyset$.

Solution. *Proof.* A hyperplane in $\mathbb{P}^n$ corresponds to a n-dimensional vector space in $\mathbb{A}^{n+1}$ by considering homogeneous coordinates as affine coordinates. But the intersection of $m \leq n$, n-dimensional vector spaces in $\mathbb{A}^{n+1}$ has dimension at least 1, so the $H_1 \cap H_2 \cap \cdots \cap H_m \neq \emptyset$. □

4.13. Let $P = [a_1 : \cdots : a_{n+1}]$, $Q = [b_1 : \cdots : b_{n+1}]$ be distinct points of $\mathbb{P}^n$. The *line* L through P and Q is defined by

$$L = \{[\lambda a_1 + \mu b_1 : \cdots : \lambda a_{n+1} + \mu b_{n+1}] \,|\, \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\}$$

Prove the projective analogue of Problem 2.15.

Solution. *Proof.* □

4.14. Let P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) be three points in $\mathbb{P}^2$ not lying on a line. Show that there is a projective change of coordinates $T : \mathbb{P}^2 \to \mathbb{P}^2$ such that $T(P_i) = Q_i$, $i = 1, 2, 3$. Extend this to $n + 1$ points in $\mathbb{P}^n$, not lying in a hyperplane.

Solution. *Proof.* □

4.15. Show that any two distinct lines in $\mathbb{P}^2$ intersect in one point.

Solution. *Proof.* □

4.16. Let L_1, L_2, L_3 (resp. M_1, M_2, M_3) be lines in $\mathbb{P}^2(k)$ that do not all pass through a point. Show that there is a projective change of coordinates $T : \mathbb{P}^2 \to \mathbb{P}^2$ such that $T(L_i) = M_i$. (*Hint:* Let $P_i = L_j \cap L_k$, $Q_i = M_j \cap M_k$, i, j, k distinct, and apply Problem 4.14.)

Solution. *Proof.* □

4.17. Let z be a rational function on a projective variety V. Show that the pole set of z is an algebraic subset of V.

Solution. *Proof.* □

4.18. Let $H = V(\sum a_i X_i)$ be a hyperplane in $\mathbb{P}^n$. Note that $(a_1, \ldots, a_{n+1})$ is determined by H up to a constant.

(a) Show that assigning $[a_1 : \cdots : a_{n+1}] \in \mathbb{P}^n$ to H sets up a natural one-to-one correspondence between {hyperplanes in $\mathbb{P}^n$} and $\mathbb{P}^n$. If $P \in \mathbb{P}^n$, let P^* be the corresponding hyperplane; if H is a hyperplane, H^* denotes the corresponding point.

(b) Show that $P^{**} = P$ and $H^{**} = H$. Show that $P \in H$ if and only if $H^* \in P^*$.

This is the well-know *duality* of projective space.

Solution. (a) *Proof.* □

(b) *Proof.* □

4.3 Affine and Projective Varieties

Problems

4.19. If $I = (F)$ is the ideal of an affine hypersurface, show that $I^* = (F^*)$.

Solution. *Proof.* □

4.20. Let $V = V(Y - X^2, Z - X^3) \subset \mathbb{A}^3$. Prove:

(a) $I(V) = (Y - X^2, Z - X^3)$.

(b) $ZW - XY \in I(V)^* \subset k[X, Y, Z, W]$, but $ZW - XY \notin ((Y - X^2)^*, (Z - X^3)^*)$. So if $I(V) = (F_1, \ldots, F_r)$, it does not follow that $I(V)^* = (F_1^*, \ldots, F_r^*)$.

Solution. (a) *Proof.* □

(b) *Proof.* □

4.21. Show that if $V \subset W \subset \mathbb{P}^n$ are varieties, and V is a hypersurface, then $W = V$ or $W = \mathbb{P}^n$ (See Problem 1.1.39).

Solution. *Proof.* □

4.22. Suppose V is a variety in $\mathbb{P}^n$ and $V \supset H_\infty$. Show that $V = \mathbb{P}^n$ or $V = H_\infty$. If $V = \mathbb{P}^n$, $V_* = \mathbb{A}^n$, while if $V = H_\infty$, $V_* = \emptyset$.

Solution. *Proof.* □

4.23. Find all subvarieties in $\mathbb{P}^1$ and in $\mathbb{P}^2$.

4.24. Let $P = [0 : 1 : 0] \in \mathbb{P}^2(k)$. Show that the lines through P consist of the following:

(a) The "vertical" lines $L_\lambda = V(X - \lambda Z) = \{[\lambda : t : 1] \,|\, t \in k\} \cup \{P\}$.

(b) The line at infinity $L_\infty = V(Z) = (\{[x : y : 0] \,|\, x, y \in k\}$.

Solution. (a) *Proof.* □

(b) *Proof.* □

4.25. Let $P = [x : y : z] \in \mathbb{P}^2$.

(a) Show that $\{(a, b, c) \in \mathbb{A}^3 \,|\, ax + by + cz = 0\}$ is a hyperplane in $\mathbb{A}^3$.

(b) Show that for any finite set of points in $\mathbb{P}^2$, there is a line not passing through any of them.

Solution. (a) *Proof.* □

(b) *Proof.* □

4.4 Multiprojective Space

Problems

4.26. (a) Define maps $\varphi_{i,j} : \mathbb{A}^{n+m} \to U_i \times U_j \subset \mathbb{P}^n \times \mathbb{P}^m$. Using $\varphi_{n+1,m+1}$, define the "biprojective closure" of an algebraic set in $\mathbb{A}^{n+m}$. Prove an analogue of Proposition **??** of Section 4.3.

(b) Generalize part (a) to maps

$$\varphi : \mathbb{A}^{n_1} \times \cdots \times \mathbb{A}^{n_r} \times \mathbb{A}^m \to \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m.$$

Show that this sets up a correspondence between {nonempty affine varieties in $\mathbb{A}^{n_1+\cdots+m}$} and {varieties in $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$ which intersect $U_{n_1+1} \times \cdots \times \mathbb{A}^m$}. Show that this correspondence preserves function fields and local rings.

Solution. (a) *Proof.* □

(b) *Proof.* □

4.27. Show that the pole set of a rational function on a variety in any multispace is an algebraic subset.

Solution. *Proof.* □

4.28. For simplicity of notation, in this problem we let $X_0, \ldots, X_n$ be coordinates for $\mathbb{P}^n$, $Y_0, \ldots, Y_m$ coordinates for $\mathbb{P}^m$, and $T_{00}, T_{01}, \ldots, T_{0m}, T_{10}, \ldots, T_{nm}$ coordinates for $\mathbb{P}^N$, where $N = (n+1)(m+1) - 1 = n + m + nm$.

Define $S : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$ as follows:

$$S([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]) = [x_0y_0 : x_0y_1 : \cdots : x_ny_m)].$$

S is called the *Segre imbedding* of $\mathbb{P}^n \times \mathbb{P}^m$ in $\mathbb{P}^{n+m+nm}$.

(a) Show that S is a well-defined, one-to-one mapping.

(b) Show that if W is an algebraic subset of $\mathbb{P}^N$, then $S^{-1}(W)$ is an algebraic subset of $\mathbb{P}^n \times \mathbb{P}^m$.

(c) Let $V = V(\{T_{ij}T_{k\ell} - T_{i\ell}T_{kj} \mid i, k = 0, \ldots, n; j, \ell = 0, \ldots, m\} \subset \mathbb{P}^N$. Show that $S(\mathbb{P}^n \times \mathbb{P}^m) = V$. In fact, $S(U_i \times U_j) = V \cap U_{ij}$, where $U_{ij} = \{[t] \mid t_{ij} \neq 0\}$.

(d) Show that V is a variety.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

Chapter 5

Projective Plane Curves

5.1 Definitions

Problems

5.1. Let F be a projective plane curve. Show that a point P is a multiple point of F if and only if $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$.

Solution. *Proof.* □

5.2. Show that the following curves are irreducible; find their multiple point, and the multiplicities and tangents at the multiple points.

(a) $XY^4 + YZ^4 + XZ^4$.

(b) $X^2Y^3 + X^2Z^3 + Y^2Z^3$.

(c) $Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \in k$.

(d) $X^n + Y^n + Z^n$, $n > 0$.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

5.3. Find all the points of intersection of the following pairs of curves, and the intersection numbers at these points:

(a) $Y^2Z - X(X-2Z)(X+Z)$ and $Y^2 + X^2 - 2XZ$.

(b) $(X^2+Y^2)Z + X^3 + Y^3$ and $X^3 + Y^3 - 2XYZ$.

(c) $Y^5 - X(Y^2 - XZ)^2$ and $Y^4 + Y^3Z - X^2Z^2$.

(d) $(X^2+Y^2)^2 + 3X^2YZ - Y^3Z$ and $(X^2+Y^2)^3 - 4X^2Y^2Z^2$.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

5.4. Let P be a simple point on F. Show that the tangent line to F at P is $F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$.

Solution. *Proof.* □

5.5. Let $P = [0:1:0]$, F a curve of degree n, $F = \sum F_i(X,Z)Y^{n-i}$, F_i a form of degree i. Show that $m_P(F)$ is the smallest m such that $F_m \neq 0$, and the factors of F_m determine the tangents to F at P.

Solution. *Proof.* □

5.6. For any F, $P \in F$, show that $m_P(F_X) \geq m_P(F) - 1$.

Solution. *Proof.* □

5.7. Show that two plane curves with no common components intersect in a finite number of points.

Solution. *Proof.* □

5.8. Let F be an irreducible curve.

(a) Show that F_X, F_Y, or $F_Z \neq 0$.

(b) Show that F has only a finite number of multiple points.

Solution. (a) *Proof.* □

(b) *Proof.* □

5.9. (a) Let F be an irreducible conic, $P = [0 : 1 : 0]$ a simple point on F, and $Z = 0$ the tangent line to F at P. Show that $F = aYZ - bX^2 - cXZ - dZ^2$, $a, b \neq 0$. Find a projective change of coordinates T so that $F^T = YZ - X^2 - c'XZ - d'Z^2$. Find T' so that $(F^T)^{T'} = YZ - X^2$. ($T' = (X, Y + c'X + d'Z, Z)$).

(b) Show that, up to projective equivalence, there is only one irreducible conic. Any irreducible conic is nonsingular.

Solution. (a) *Proof.* □

(b) *Proof.* □

5.10. Let F be an irreducible cubic: $P = [0 : 0 : 1]$ a cusp on F, $Y = 0$ the tangent line to F at P. Show that $F = aY^2Z - bX^3 - cX^2Y - dXY^2 - eY^3$. Find projective changes of coordinates (i) to make $a = b = 1$ (ii) to make $c = 0$ (change X to $X - \frac{c}{3}Y$) (iii) to make $d = e = 0$ (Z to $Z + dX + eY$).

Up to projective equivalence, there is only one irreducible cubic with a cusp: $Y^2Z = X^3$. It has no other singularities.

Solution. *Proof.* □

5.11. Up to projective equivalence, there is only one irreducible cubic with a node: $XYZ = X^3 + Y^3$. It has no other singularities.

Solution. *Proof.* □

5.12. (a) Assume $[0 : 1 : 0] \notin F$, F a curve of degree n. Show that $\sum_P I(P, F \cap X) = n$.

(b) Show that if F is a curve of degree n, L a line not contained in F, then

$$\sum I(P, F \cap L) = n.$$

Solution. (a) *Proof.* □

(b) *Proof.* □

5.13. Prove that an irreducible cubic is either nonsingular or has at most one double point (a node or a cusp). (*Hint:* Use Problem 5.12, where L is a line through two multiple points; or use Problems 5.10 and 5.11.)

Solution. *Proof.* □

5.14. Let $P_1, \dots, P_n \in \mathbb{P}^2$. Show that there are an infinite number of lines passing through P_1, but not through $P_2, \dots, P_n$. If P_1 is a simple point on F, we may take these lines transversal to F at P_1.

Solution. *Proof.* □

5.15. Let C be an irreducible projective plane curve, $P_1, \dots, P_n$ simple points on C, $m_1, \dots, m_n$ integers. Show that there is a $z \in k(C)$ with $\text{ord}_{P_i}^C(z) = m_i$ for $i = 1, \dots n$. (*Hint:* Take lines L_i as in Problem 5.14 for P_i, and a line L_0 not through any P_j, and let $z = \prod L_i^{m_i} L_0^{-\sum m_i}$.)

Solution. *Proof.* □

5.16. Let F be an irreducible curve in $\mathbb{P}^2$. Suppose $I(P, F \cap Z) = 1$, and $P \neq [1:0:0]$. Show that $F_X(P) \neq 0$. (*Hint:* If not, use Euler's Theorem to show that $F_Y(P) = 0$; but Z is not tangent to F at P.)

Solution. *Proof.* □

5.2 Linear Systems of Curves

Problems

5.17. Let $P_1, P_2, P_3, P_4 \in \mathbb{P}^2$. Let V be the linear system of conics passing through these points. Show that $\dim(V) = 2$ if $P_1, \dots, P_4$ lie on a line, and $\dim(V) = 1$ otherwise.

Solution. *Proof.* □

5.18. Show that there is only one conic passing through the five points $[0:0:1]$, $[0:1:0]$, $[1:0:0]$, $[1:1:1]$, and $[1:2:3]$; show that is is nonsingular.

Solution. *Proof.* □

5.19. Consider the nine points $[0:0:1]$, $[0:1:1]$, $[1:0:1]$, $[1:1:1]$, $[0:2:1]$, $[2:0:1]$, $[1:2:1]$, $[2:1:1]$, and $[2:2:1] \in \mathbb{P}^2$ (Sketch). Show that there are an infinite number of cubics passing through these points.

Solution. *Proof.* □

5.3 Bézout's Theorem

Problems

5.20. Check your answers of Problem 5.3 with Bézout's Theorem.

Solution. *Proof.* □

5.21. Show that every nonsingular projective plane curve is irreducible. Is this true for affine curves?

Solution. *Proof.* □

5.22. Let F be an irreducible curve of degree n. Assume $F_X \neq 0$. Apply Corollary **??** to F and F_X, and conclude that $\sum m_P(F)(m_P(F)-1) \leq n(n-1)$. In particular, F has at most $\frac{1}{2}n(n-1)$ multiple points. (See Problems 5.6, 5.8.)

Solution. *Proof.* □

5.23. A problem about flexes (See Problem 3.12): Let F be a projective plane curve of degree n, and assume F contains no lines.

Let $F_i = F_{X_i}$ and $F_{ij} = F_{X_iX_j}$, forms of degree $n-1$ and $n-2$ respectively. We can form a 3×3 matrix with the entry in the (i, j)th place being F_{ij}. Let H be the determinant of this matrix, a form of degree $3(n-2)$. This H is called the *Hessian* of F. The following theorem shows the relationship between flexes and the Hessian.

Theorem. $(\text{char}\,(k) = 0)$

(1) $P \in H \cap F$ *if and only if* P *is either a flex or a multiple point of* F*.*

(2) $I(P, H \cap F) = 1$ *if and only if* P *is an ordinary flex.*

Proof. (Outline)

(a) Let T be a projective change of coordinates. Then the Hessian of $F^T = (\det(T))^2(H^T)$. So we can assume $P = [0 : 0 : 1]$; write $f(X, Y) = F(X, Y, 1)$ and $h(X, Y) = H(X, Y, 1)$.

(b) $(n-1)F_j = \sum_i X_iF_{ij}$ (Use Euler's Theorem).

(c) $I(P, f \cap h) = I(P, f \cap g)$ where $g = f_y^2 f_{xx} + f_x^2 f_{yy} - 2f_xf_yf_{xy}$ (*Hint:* Perform row and column operations on the matrix for h. Add x times the first row plus y times the second row to the third row, then apply part (b). Do the same with the columns. Then calculate the determinant.)

(d) If P is a multiple point on F then $I(P, f \cap g) > 1$.

(e) Suppose P is a simple point, $Y = 0$ is the tangent line to F at P, so $f = y + ax^2 + bxy + cy^2 + dx^3 + ex^2y + \cdots$. Then P is a flex if and only if $a = 0$, and P is an ordinary flex if and only if $a = 0$ and $d \neq 0$. A short calculation shows that $g = 2a + 6dx + (8ac - 2b^2 + 2e)y +$ higher terms, which concludes the proof.

□

Corollary. (1) *A nonsingular curve of degree > 2 always has a flex.*

(2) *A nonsingular cubic has nine flexes, all ordinary.*

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

(e) *Proof.* □

(1) *Proof.* □

(2) *Proof.* □

5.24. (char $(k) = 0$).

(a) Let $[0 : 1 : 0]$ be a flex on an irreducible cubic F, $Z = 0$ the tangent line to F at $[0 : 1 : 0]$. Show that $F = ZY^2 + bYZ^2 + cYXZ +$ terms in X, Z. Find a projective change of coordinates (using $Y \to Y - \frac{b}{2}Z - \frac{c}{2}X$) to get F to the form $ZY^2 =$ cubic in X, Z.

(b) Show that any irreducible cubic is projectively equivalent to one of the following: $Y^2Z = X^3$, $Y^2Z = X^2(X + Z)$, or $Y^2Z = X(X - Z)(X - \lambda Z)$, $\lambda \in k$, $\lambda \neq 0, 1$. (See Problems 5.10, 5.11.)

Solution. (a) *Proof.* □

(b) *Proof.* □

5.4 Multiple Points

Problems

5.25. Let F be a projective plane curve of degree n with no multiple components, and c simple components. Show that

$$\sum \frac{m_P(m_P-1)}{2} \leq \frac{(n-1)(n-2)}{2} + c - 1 \leq \frac{n(n-1)}{2}.$$

(*Hint:* Let $F = F_1F_2$; consider separately the points on one F_i or on both.)

Solution. *Proof.* □

5.26. ($\operatorname{char}(k) = 0$). Let F be an irreducible curve of degree n in $\mathbb{P}^2$. Suppose $P \in \mathbb{P}^2$, with $m_P(F) = r \geq 0$. Then for all but a finite number of lines L through P, L intersects F in $n-r$ distinct points other than P. We outline a proof:

(a) We may assume $P = [0:1:0]$. If $L_\lambda = \{[\lambda : t : 1] \mid t \in k\} \cup \{P\}$, we need only consider the L_λ. $F = A_r(X,Z)Y^{n-r} + \cdots + A_n(X,Z)$, $A_r \neq 0$. (See Problems 4.24, 5.5).

(b) Let $G_\lambda(t) = F(\lambda, t, 1)$. It is enough to show that for all but a finite number of λ, G_λ has $n-r$ distinct points.

(c) Show that G_λ has $n-r$ distinct roots if $A_r(\lambda, 1) \neq 0$, and $F \cap F_Y \cap L_\lambda = \{P\}$ (See Problem 1.53).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

5.27. Show that Problem 5.26 remains true if F is reducible, provided it has no multiple components.

Solution. *Proof.* □

5.28. ($\operatorname{char}(k) = p > 0$): $F = X^{p+1} - Y^pZ$, $P = [0:1:0]$. Find $L \cap F$ for all lines L passing through P. Show that every line which is tangent to F at a simple point passes through P!

Solution. *Proof.* □

5.5 Max Noether's Fundamental Theorem

Problems

5.29. Fix F, G, and P. Show that in cases **??** and **??**—but not **??**—of Proposition **??** the conditions on H are equivalent to Noether's conditions.

Solution. *Proof.* □

5.30. Let F be an irreducible projective plane curve. Suppose $z \in k(F)$ is defined at every $P \in F$. Show that $z \in k$. (*Hint:* Write $z = H/G$, and use Noether's Theorem).

Solution. *Proof.* □

5.6 Applications of Noether's Theorem

Problems

5.31. If in Pascal's Theorem we let some adjacent vertices coincide (the side being a tangent), we get many new theorems:

(a) State and sketch what happens if $P_1 = P_2$, $P_3 = P_4$, $P_5 = P_6$.

(b) Let $P_1 = P_2$, the other four distinct.

(c) From (b) deduce a rule for constructing the tangent to a given conic at a given point, using only a straight-edge.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

5.32. Suppose the intersections of the opposite sides of a hexagon lie on a straight line. Show that the vertices lie on a conic.

Solution. *Proof.* □

5.33. Let C be an irreducible cubic, L a line such that $L \cdot C = P_1 + P_2 + P_3$, P_i distinct. Let L_i be the tangent line to C at P_i: $L_i \cdot C = 2P_i + Q_i$ for some Q_i. Show that Q_1, Q_2, Q_3 lie on a line (L^2 is a conic!)

Solution. *Proof.* □

5.34. Show that a line through two flexes on a cubic passes through a third flex.

Solution. *Proof.* □

5.35. Let C be any irreducible cubic, or any cubic without multiple components, C^{o} the set of simple points of C, $O \in C^{\mathrm{o}}$. Show that the same definition as above makes C^{o} into an abelian group.

Solution. *Proof.* □

5.36. Let C be an irreducible cubic, O a simple point on C giving rise to the addition $\oplus$ on the set C^{o} of simple points. Suppose another O' gives rise to an addition $\oplus'$. Let $Q = \varphi(O, O')$, and define $\alpha : (C, O, \oplus) \to (C, O', \oplus')$ by $\alpha(P) = \varphi(Q, P)$. Show that α is a group isomorphism. So the structure of the group is independent of the choice of O.

Solution. *Proof.* □

5.37. In Proposition **??**, suppose O is a flex on C.

(a) Show that the flexes form a subgroup of C; as an abelian group, this subgroup is isomorphic to $\mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

(b) Show that the flexes are exactly the elements of order three in the group. (i.e., exactly those elements P such that $P \oplus P \oplus P = O$).

(c) Show that a point P is of order two in the group if and only if the tangent to C at P passes through O.

(d) Let $C = Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \neq 0{,}1$, $O = [0 : 1 : 0]$. Find the points of order two.

(e) Show that the points of order two on a nonsingular cubic form a group isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

(f) Let C be a nonsingular cubic, $P \in C$. How many lines through P are tangent to C at some point $Q \neq P$? (The answer depends on whether P is a flex or not.)

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

(e) *Proof.* □

(f) *Proof.* □

5.38. Let C be a nonsingular cubic given by the equation $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$, $O = [0 : 1 : 0]$. Let $P_i = [x_i : y_i : 1]$, $i = 1, 2, 3$, and suppose $P_1 \oplus P_2 = P_3$. If $x_1 \neq x_2$, let $\lambda = (y_1 - y_2)/(x_1 - x_2)$; if $P_1 = P_2$ and $y_1 \neq 0$, let $\lambda = (3x_1^2 + 2ax_1 + b)/(2y_1)$. Let $\mu = y_i - \lambda x_i$, $i = 1, 2$. Show that $x_3 = \lambda^2 - a - x_1 - x_2$, and $y_3 = -\lambda x_3 - \mu$. This gives an easy method for calculating in the group.

Solution. *Proof.* □

5.39. (a) Let $C = Y^2Z - X^3 - 4XZ^2$, $O = [0 : 1 : 0]$, $A = [0 : 0 : 1]$, $B = [2 : 4 : 1]$, $C = [2 : -4 : 1]$. Show that $\{0, A, B, C\}$ form a subgroup of C which is cyclic of order 4.

(b) Let $C = Y^2Z - X^3 - 43XZ^2 - 166Z^3$. Let $O = [0 : 1 : 0]$, $P = [3 : 8 : 1]$. Show that P is an element of order 7 in C.

Solution. (a) *Proof.* □

(b) *Proof.* □

5.40. Let k_0 be a subfield of k. If V is an affine variety, $V \subset \mathbb{A}^n(k)$, a point $P = (a_1, \ldots, a_n) \in V$ is *rational* over k_0, if each $a_i \in k_0$. If $V \subset \mathbb{P}^n(k)$ is projective, a point $P \in V$ is rational over k_0 if for some homogeneous coordinates $(a_1, \ldots, a_{n+1})$ for P, each $a_i \in k_0$.

A curve F of degree d is said to be *rational* over k_0 if the corresponding point in $\mathbb{P}^{d(d+3)/2}$ is rational over k_0.

Suppose a nonsingular cubic C is rational over k_0. Let $C(k_0)$ be the set of points of C which are rational over k_0.

(a) If $P, Q \in C(k_0)$ then $\varphi(P, Q) \in C(k_0)$.

(b) If $0 \in C(k_0)$, then $C(k_0)$ forms a subgroup of C. (If $k_0 = \mathbb{Q}$, $k = \mathbb{C}$, this has important applications to number theory.)

Solution. (a) *Proof.* □

(b) *Proof.* □

5.41. Let C be a nonsingular cubic, O a flex on C. Let $P_1, \ldots, P_{3m} \in C$. Show that $P_1 \oplus \cdots \oplus P_{3m} = O$ if and only if there is a curve F of degree m such that $F \cdot C = \sum_{i=1}^{3m} P_i$. (*Hint:* Use induction on m. Let $L \cdot C = P_1 + P_2 + Q$, $L' \cdot C = P_3 + P_4 + R$, $L'' \cdot C = Q + R + S$, and apply induction to S, $P_5, \ldots, P_{3m}$; use Noether's Theorem).

Solution. *Proof.* □

5.42. Let C be a nonsingular cubic, F, F' curves of degree m such that $F \cdot C = \sum_{i=1}^{3m} P_i$, $F' \cdot C = \sum_{i=1}^{3m-1} P_i + Q$. Show that $P_{3m} = Q$.

Solution. *Proof.* □

5.43. For which points P on a nonsingular cubic C does there exist a nonsingular conic which intersects C only at P?

Solution. *Proof.* □

Chapter 6

Varieties, Morphisms, and Rational Maps

Problems

6.1. Let $Z \subset Y \subset X$, X a topological space. Give Y the induced topology. Show that the topology induced by Y on Z is the same as that induced by X on Z.

Solution. *Proof.* □

6.2. (a) Let X be a topological space, $X = \bigcup_{\alpha \in \mathscr{A}} U_\alpha$, U_α open in X. Show that a subset W of X is closed if and only if each $W \cap U_\alpha$ is closed (in the induced topology) in U_α.

(b) Suppose similarly $Y = \bigcup_{\alpha \in \mathscr{A}} V_\alpha$, V_α open in Y, and suppose $f : X \to Y$ is a mapping such that $f(U_\alpha) \subset V_\alpha$. Show that f is continuous if and only if the restriction of f to each U_α is a continuous function from U_α to V_α.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.3. (a) Let V be an affine variety, $f \in \Gamma(V)$. Considering f as a function from V to $k = \mathbb{A}^1$, show that f is continuous.

(b) Show that any polynomial map of affine varieties is continuous.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.4. Let $U_i \subset \mathbb{P}^n$, $\varphi_i : \mathbb{A}^n \to U_i$ as in Chapter **??**. Give U_i the topology induced from $\mathbb{P}^n$.

(a) Show that φ_i is a homeomorphism.

(b) Show that a set $W \subset \mathbb{P}^n$ is closed if and only if each $\varphi_i^{-1}(W)$ is closed in $\mathbb{A}^n$, $i = 1, \ldots, n+1$.

(c) Show that if $V \subset \mathbb{A}^n$ is an affine variety, then the projective closure V^* of V is the closure of $\varphi_{n+1}(V)$ in $\mathbb{P}^n$.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

6.5. Any infinite subset of a plane curve V is dense in V. Any one-to-one mapping from one irreducible plane curve onto another is a homeomorphism.

Solution. *Proof.* □

6.6. Let X be a topological space, $f : X \to \mathbb{A}^n$ a mapping. Then f is continuous if and only if for each hypersurface $V = V(F)$ of $\mathbb{A}^n$, $f^{-1}(V)$ is closed in X. A mapping $f : X \to k = \mathbb{A}^1$ is continuous if and only if $f^{-1}(\lambda)$ is closed for any $\lambda \in k$.

Solution. *Proof.* □

6.7. Let V be an affine variety, $f \in \Gamma(V)$.

(a) Show that $V(f) = \{P \in V \mid f(P) = 0\}$ is a closed subset of V, and $V(f) \neq V$ unless $f = 0$.

(b) Suppose U is a dense subset of V and $f(P) = 0$ for all $P \in U$. Then $f = 0$.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.8. Let U be an open subset of a variety V, $z \in k(V)$. Suppose $z \in \mathscr{O}_P(V)$ for all $P \in U$. Show that $U_z = \{P \in U \mid z(P) \neq 0\}$ is open, and that the mapping from $U \to k = \mathbb{A}^1$ defined by $P \mapsto z(P)$ is continuous.

Solution. *Proof.* □

6.1 Varieties

Problems

6.9. Let $X = \mathbb{A}^2 \setminus \{(0,0)\}$, an open subvariety of $\mathbb{A}^2$. Show that $\Gamma(X) = \Gamma(\mathbb{A}^2) = k[X,Y]$.

Solution. *Proof.* □

6.10. Let U be an open subvariety of a variety X, Y a closed subvariety of U. Let Z be the closure of Y in X.

(a) Z is a closed subvariety of X.

(b) Y is an open subvariety of Z.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.11. (a) Show that every family of closed subsets of a variety has a minimal member.

(b) Show that if a variety is a union of a collection of open subsets, it is a union of a finite number of these subsets. (All varieties are "quasi-compact".)

Solution. (a) *Proof.* □

(b) *Proof.* □

6.12. Let X be a variety, $z \in k(X)$. Show that the pole set of z is closed. If $z \in \mathscr{O}_P(X)$, there is a neighborhood U of P such that $z \in \Gamma(U)$; so $\mathscr{O}_P(X)$ is the union of all $\Gamma(U)$, where U runs through all neighborhoods of P.

Solution. *Proof.* □

6.2 Morphisms of Varieties

Problems

6.13. Let R be a domain with quotient field K, $f \neq 0$ in R. Let $R[1/f] = \{a/f^n \mid a \in R, n \in \mathbb{Z}\}$, a subring of K.

(a) Show that if $\varphi : R \to S$ is any ring homomorphism such that $\varphi(f)$ is a unit in S, then φ extends uniquely to a ring homomorphism from $R[1/f]$ to S.

(b) Show that the ring homomorphism from $R[X]/(Xf - 1)$ to $R[1/f]$ which takes X to $1/f$ is an isomorphism.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.14. Let X, Y be varieties, $f : X \to Y$ a function. Let $X = \bigcup_\alpha U_\alpha$, $Y = \bigcup_\alpha V_\alpha$, with U_α, V_α open subvarieties, and suppose $f(U_\alpha) \subset V_\alpha$ for all α.

(a) f is a morphism if and only if each restriction $f_\alpha : U_\alpha \to V_\alpha$ of f is a morphism.

(b) If each U_α, V_α is affine, f is a morphism if and only if each $\widetilde{f}(\Gamma(V_\alpha)) \subset \Gamma(U_\alpha)$.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.15. (a) If Y is an open or closed subvariety of X, the inclusion $i : Y \to X$ is a morphism.

(b) The composition of morphisms is a morphism.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.16. Let $f : X \to Y$ be a morphism of varieties, $X' \subset X$, $Y' \subset Y$ subvarieties (open or closed). Assume $f(X') \subset Y'$. Then the restriction of f to X' is a morphism from X' to Y'. (Use Problems 6.14 and 2.9.)

Solution. *Proof.* □

6.17. (a) Show that $\mathbb{A}^2 \setminus \{(0,0)\}$ is not an affine variety (See Problem 6.9).

(b) The union of two open affine subvarieties of a variety may not be affine.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.18. Show that the natural map π from $\mathbb{A}^{n+1} \setminus \{(0, \dots, 0)\}$ to $\mathbb{P}^n$ is a morphism of varieties, and that a subset U of $\mathbb{P}^n$ is open if and only if $\pi^{-1}(U)$ is open.

Solution. *Proof.* □

6.19. Let X be a variety, $f \in \Gamma(X)$. Let $\varphi : X \to \mathbb{A}^1$ be the mapping defined by $\varphi(P) = f(P)$ for $P \in X$.

(a) Show that for $\lambda \in k$, $\varphi^{-1}(\lambda)$ is the pole set of $z = 1/(f - \lambda)$.

(b) Show that φ is a morphism of varieties.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.20. Let $A = \mathbb{P}^{n_1} \times \cdots \times \mathbb{A}^n$, $B = \mathbb{P}^{m_1} \times \cdots \times \mathbb{A}^m$. Let $y \in B$, V a closed subvariety of A. Show that $V \times \{y\} = \{(x, y) \in A \times B \,|\, x \in V\}$ is a closed subvariety of $A \times B$, and that the map $V \to V \times \{y\}$ taking x to (x, y) is an isomorphism.

Solution. *Proof.* □

6.21. Any variety is the union of a finite number of open affine subvarieties.

Solution. *Proof.* □

6.22. Let X be a projective variety in $\mathbb{P}^n$, and let H be a hyperplane in $\mathbb{P}^n$ that doesn't contain X.

(a) Show that $X \setminus (H \cap X)$ is isomorphic to an affine variety $X_* \subset \mathbb{A}^n$.

(b) If L is the linear form defining H, and ℓ is its image in $\Gamma_h(X) = k[x_1, \dots, x_{n+1}]$, then $\Gamma(X_*)$ may be identified with $k[x_1/\ell, \dots, x_{n+1}/\ell]$. (*Hint:* Change coordinates so $L = X_{n+1}$.)

Solution. (a) *Proof.* □

(b) *Proof.* □

6.23. Let $P, Q \in X$, X a variety. Show that there is an affine open set V on X that contains P and Q. (*Hint:* See the proof of the Corollary to Proposition **??**, and use Problem (c).)

Solution. *Proof.* □

6.24. Let X be a variety, P, Q two distinct points of X. Show that there is an $f \in k(X)$ that is defined at P and at Q, with $f(P) = 0$, $f(Q) \neq 0$. (Problem 6.23, 1.17). So $f \in \mathfrak{m}_P(X)$, $1/f \in \mathscr{O}_Q(X)$. The local rings $\mathscr{O}_P(X)$, as P varies in X, are distinct.

Solution. *Proof.* □

6.25. Show that $[x_1 : \cdots : x_n] \to [x_1 : \cdots : x_n : 0]$ gives an isomorphism of $\mathbb{P}^{n-1}$ with $H_\infty \subset \mathbb{P}^n$. If a variety V in $\mathbb{P}^n$ is contained in H_∞, V is isomorphic to a variety in $\mathbb{P}^{n-1}$. Any projective variety is isomorphic to a closed subvariety $V \subset \mathbb{P}^n$ (for some n) such that V is not contained in any hyperplane in $\mathbb{P}^n$.

Solution. *Proof.* □

6.3 Products and Graphs

Problems

6.26. (a) Let $f : X \to Y$ be a morphism of varieties such that $f(X)$ is dense in Y. Show that the homomorphism $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one.

(b) If X and Y are affine, show that $f(X)$ is dense in Y if and only if $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one. Is this true if Y is not affine?

Solution. (a) *Proof.* □

(b) *Proof.* □

6.27. Let U, V be open subvarieties of a variety X.

(a) Show that $U \cap V$ is isomorphic to $(U \times V) \cap \Delta_X$.

(b) If U and V are affine, show that $U \cap V$ is affine. (Compare Problem 6.17.)

Solution. (a) *Proof.* □

(b) *Proof.* □

6.28. Let $d \geq 1$, $N = \frac{(d+1)(d+2)}{2}$, and let $M_1, \ldots, M_N$ be the monomials of degree d in X, Y, Z (in some order). Let $T_1, \ldots, T_N$ be homogeneous coordinates for $\mathbb{P}^{N-1}$. Let $V = V(\sum_{i=1}^{N} M_i(X,Y,Z)T_i) \subset \mathbb{P}^2 \times \mathbb{P}^{N-1}$, and let $\pi : V \to \mathbb{P}^{N-1}$ be the restriction of the projection map.

(a) Show that V is an irreducible closed subvariety of $\mathbb{P}^2 \times \mathbb{P}^{N-1}$, and π is a morphism.

(b) For each $t = (t_1, \ldots, t_N) \in \mathbb{P}^{N-1}$, let C_t be the corresponding curve (Section 5.2). Show that $\pi^{-1}(t) = C_t \times \{t\}$.

We may thus think of $\pi : V \to \mathbb{P}^{N-1}$ as a "universal family" of curves of degree d. Every curve appears as a fiber $\pi^{-1}(t)$ over some $t \in \mathbb{P}^{N-1}$

Solution. (a) *Proof.* □

(b) *Proof.* □

6.29. Let V be a variety, and suppose V is also a group, i.e., there are mappings $\varphi : V \times V \to V$ (multiplication or addition), and $\psi : V \to V$ (inverse) satisfying the group axioms. If φ and ψ are morphisms, V is said to be an *algebraic group*. Show that each of the following is an algebraic group:

(a) $\mathbb{A}^1 = k$, with the usual addition on k; this group is often denoted G_a.

(b) $\mathbb{A}^1 \setminus \{(0)\} = k \setminus \{(0)\}$, with the usual multiplication on k: this is denoted G_m.

(c) $\mathbb{A}^n(k)$ with addition; likewise $M_n(k) = \{n \text{ by } n \text{ matrices}\}$ under addition may be identified with $\mathbb{A}^{n^2}(k)$.

(d) $\mathrm{GL}_n(k) = \{\text{invertible } n \times n \text{ matrices}\}$ is an affine open subvariety of $M_n(k)$, and a group under multplication.

(e) C a nonsingular plane cubic, $O \in C$, $\oplus$ the resulting addition (See Problem 5.38).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

(e) *Proof.* □

6.30. (a) Let $C = V(Y^2Z - X^3)$ be a cubic with a cusp, $C^o = C \setminus \{[0:0:1]\}$ the simple points, a group with $O = [0:1:0]$. Show that the map $\varphi : G_a \to C^o$ given by $\varphi(t) = [t : 1 : t^3]$ is an isomorphism of algebraic groups.

(b) Let $C = V(X^3 + Y^3 - XYZ)$ be a cubic with a node, $C^{\circ} = C \setminus \{[0:0:1]\}$, $O = [1:1:0]$. Show that $\varphi : G_m \to C^{\circ}$ defined by $\varphi(t) = (t, t^2, 1 - t^3)$ is an isomorphism of algebraic groups.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.4 Algebraic Function Fields and Dimension of Varieties

Problems

6.31. (Theorem of the Primitive Element) Let K be a field of characteristic zero, L a finite (algebraic) extension of K. Then there is a $z \in L$ such that $L = K(z)$.

Outline of Proof:

Step (i) Suppose $L = K(x, y)$. Let F and G be monic irreducible polynomials in $K[T]$ such that $F(x) = 0$, $G(y) = 0$. Let L' be a field in which $F = \prod_{i=1}^{n}(T - x_i)$, $G = \prod_{j=1}^{m}(T - y_i)$, $x = x_1$, $y = y_1$, $L' \supset L$ (See Problems 1.52, 1.53). Choose $\lambda \neq 0$ in K so that $\lambda x + y \neq \lambda x_i + y_j$ for all $i \neq 1$, $j \neq 1$. Let $z = \lambda x + y$, $K' = K(z)$. Set $H(T) = G(z - \lambda T) \in K'[T]$. Then $H(x) = 0$, $H(x_i) \neq 0$ if $i > 0$. Therefore $(H, F) = (T - x) \in K'[T]$. Then $x \in K'$, so $y \in K'$, so $L = K'$.

Step (ii) If $L = K(x_1, \ldots, x_n)$, use induction on n to find $\lambda_1, \ldots, \lambda_n \in K$ such that $L = K(\sum \lambda_i x_i)$.

Solution. *(i)* *Proof.* □

(ii) *Proof.* □

6.32. Let $L = K(x_1, \ldots, x_n)$ as in Problem 6.31. Suppose $k \subset K$ is an algebraically closed subfield, and $V \subsetneq \mathbb{A}^n(k)$ is an algebraic set. Show that $L = K(\sum \lambda_i x_i)$ for some $(\lambda_1, \ldots, \lambda_n) \in \mathbb{A}^n \setminus V$.

Solution. *Proof.* □

6.33. The notion of transcendence degree is analogous to the idea of the dimension of a vector space. If $k \subset K$, we say that $x_1, \ldots, x_n \in K$ are *algebraically independent* if there is no nonzero polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(x_1, \ldots, x_n) = 0$. By methods entirely analogous to those for bases of vector spaces, one can prove:

(a) Let $x_1, \ldots, x_n \in K$, K a finitely generated extension of k. Then $x_1, \ldots, x_n$ is a minimal set such that K is algebraic over $k(x_1, \ldots, x_n)$ if and only if $x_1, \ldots, x_n$ is a maximal set of algebraically independent elements of K. Suvch $\{x_1, \ldots, x_n\}$ is called a *transcendence basis* of K over k.

(b) Any algebraically independent set may be completed to a transcendence basis. Any set $\{x_1, \ldots, x_n\}$ such that K is algebraic over $k(x_1, \ldots, x_n)$ contains a transcendence basis.

(c) $\operatorname{tr.deg}_k(K)$ is the number of elements in any transcendence basis of K over k.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

6.34. Show that $\dim(\mathbb{A}^n) = \dim(\mathbb{P}^n) = n$.

Solution. *Proof.* □

6.35. Let Y be a closed subvariety of a variety X. Then $\dim(Y) \leq \dim(X)$, with equality if and only if $Y = X$.

Solution. *Proof.* □

6.36. Let $K = k(x_1, \ldots, x_n)$ be a function field in n variables over k.

(a) Show that there is an affine variety $V \subset \mathbb{A}^n$ with $k(V) = K$.

(b) Show that we may find $V \subset \mathbb{A}^{r+1}$ with $k(V) = K$, $r = \dim(V)$. (Assume $\operatorname{char}(k) = 0$ if you wish).

Solution. (a) *Proof.* □

(b) *Proof.* □

6.5 Rational Maps

Problems

6.37. Let $C = V(X^2 + Y^2 - Z^2) \subset \mathbb{P}^2$. For each $t \in k$, let L_t be the line between $P_0 = [-1 : 0 : 1]$ and $P_t = [0 : t : 1]$. (Sketch this.)

(a) If $t \neq \pm 1$, show that $L_t \cdot C = P_0 + Q_t$, where $Q_t = [1 - t^2 : 2t : 1 + t^2]$.

(b) Show that the map $\varphi : \mathbb{A}^1 \setminus \{\pm 1\} \to C$ taking t to Q_t extends to an isomorphism of $\mathbb{P}^1$ with the projective closure of C.

(c) Any irreducible conic in $\mathbb{P}^2$ is rational; in fact, a conic is isomorphic to $\mathbb{P}^1$.

(d) Give a prescription for finding all integer solutions (x, y, z) to the Pythagorean equation $X^2 + Y^2 = Z^2$.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

6.38. An irreducible cubic with a multiple point is rational (Problems 6.30, 5.10, 5.11).

Solution. *Proof.* □

6.39. $\mathbb{P}^n \times \mathbb{P}^m$ is birationally equivalent to $\mathbb{P}^{n+m}$. Show that $\mathbb{P}^1 \times \mathbb{P}^1$ is not isomorphic to $\mathbb{P}^2$. (*Hint:* $\mathbb{P}^1 \times \mathbb{P}^1$ has closed subvarieties of dimension one which do not intersect.)

Solution. *Proof.* □

6.40. If there is a dominating rational map from X to Y, then $\dim(Y) \leq \dim(X)$.

Solution. *Proof.* □

6.41. Every n-dimensional variety is birationally equivalent to a hypersurface in $\mathbb{A}^{n+1}$ (or $\mathbb{P}^{n+1}$).

Solution. *Proof.* □

6.42. Suppose X, Y varieties, $P \in X$, $Q \in Y$, with $\mathscr{O}_P(X)$ isomorphic (over k) to $\mathscr{O}_Q(Y)$. Then there are neighborhoods U of P on X, V of Q on Y, such that U is isomorphic to V. This is another justification for the assertion that properties of X near P should be determined by the local ring $\mathscr{O}_P(X)$.

Solution. *Proof.* □

6.43. Let C be a projective curve, $P \in C$. Then there is a birational morphism $f : C \to C'$, C' a projective plane curve, such that $f^{-1}(f(P)) = \{P\}$. We outline a proof:

(a) We can assume: $C \subset \mathbb{P}^{n+1}$ Let $T, X_1, \ldots, X_n, Z$ be coordinates for $\mathbb{P}^{n+1}$; Then $C \cap V(T)$ is finite; $C \cap V(T, Z) = \emptyset$; $P = [0 : \cdots : 0 : 1]$; and $k(C)$ is algebraic over $k(u)$, where $u = \overline{T}/\overline{Z} \in k(C)$.

(b) For each $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$, let $\varphi_\lambda : C \to \mathbb{P}^2$ be defined by $\varphi_\lambda([t : x_1 : \cdots : x_n : z]) = [t : \sum \lambda_i x_i : z]$. Then φ_λ is a well-defined morphism, and $\varphi_\lambda(P) = [0 : 0 : 1]$. Let C' be the closure of $\varphi_\lambda(C)$.

(c) The variable λ can be chosen so φ_λ is a birational morphism from C to C', and $\varphi_\lambda^{-1}([0 : 0 : 1]) = \{P\}$. (Use Problem 6.32 and the fact that $C \cap V(T)$ is finite).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

6.44. Let $V = V(X^2 - Y^3, Y^2 - Z^3) \subset \mathbb{A}^3$, $f : \mathbb{A}^1 \to V$ as in Problem 2.13.

(a) Show that f is birational, so V is a rational curve.

(b) Show that there is no neighborhood of $(0, 0, 0)$ on V which is isomorphic to an open subvariety of a plane curve. (See Problem 3.14).

Solution. (a) *Proof.* □

(b) *Proof.* □

6.45. Let C, C' be curves, F a rational map from C' to C. Prove:

(a) Either F is dominating, or F is constant (i.e., for some $P \in C$, $F(Q) = P$, all $Q \in C'$).

(b) If F is dominating, then $k(C')$ is a finite algebraic extension of $\widetilde{F}(k(C))$.

Solution. (a) *Proof.* □

(b) *Proof.* □

6.46. Let $k(\mathbb{P}^1) = k(T)$, $T = X/Y$ (Problem 4.8). For any variety V, and $f \in k(V)$, $f \notin k$, the subfield $k(f)$ generated by f is naturally isomorphic to $k(T)$. Thus a nonconstant $f \in k(V)$ corresponds to a homomorphism from $k(T)$ to $k(V)$, and hence to a dominating rational map from V to $\mathbb{P}^1$. The corresponding map is usually denoted also by f. If this rational map is a morphism, show that the pole set of f is just $f^{-1}([1:0])$.

Solution. *Proof.* □

6.47. (*The dual curve*). Let F be an irreducible projective plane curve of degree $n > 1$. Let $\Gamma_h(F) = k[X,Y,Z]/(F) = k[x,y,z]$, and let $u, v, w \in \Gamma_h(F)$ be the residues of F_X, F_Y, F_Z, respectively. Define $\alpha : k[U,V,W] \to \Gamma_h(F)$ by letting $\alpha(U) = u$, $\alpha(V) = v$, $\alpha(W) = w$. Let I be the kernel of α.

(a) Show that I is a homogeneous prime ideal in $k[U,V,W]$, so $V(I)$ is a closed subvariety of $\mathbb{P}^2$.

(b) Show that for any simple point P on F, $[F_X(P) : F_Y(P) : F_Z(P)]$ is in $V(I)$, so $V(I)$ contains the points corresponding to tangent lines to F at simple points.

(c) If $V(I) \subset \{[a : b : c]\}$, use Euler's Theorem to show that F divides $aX + bY + cZ$, which is impossible. Conclude that $V(I)$ is a curve. It is called the *dual curve* of F.

(d) Show that the dual curve is the only irreducible curve containing all the points of (b). (See Walker's "Algebraic Curves" for more about the dual curves when char $(k) = 0$.)

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

Chapter 7

Resolution of Singularities

7.1 Rational Maps of Curves

Problems

7.1. Show that any curve has only a finite number of multiple points.

Solution. *Proof.* □

7.2 Blowing up a Point in $\mathbb{A}^2$

Problems

7.2. (a) For each of the curves F in Section 3.1, find F'; show that F' is nonsingular in the first five examples, but not in the sixth.

(b) Let $F = Y^2 - X^5$. What is F'? What is $(F')'$? What must be done to resolve the singularity of the curve $Y^2 = X^{2n+1}$?

Solution. (a) *Proof.* □

(b) *Proof.* □

7.3. Let F be any plane curve with no multiple components. Generalize the results of this section to F.

Solution. *Proof.* □

7.4. Suppose P is an ordinary multiple point on C, $f^{-1}(P) = \{P_1, \ldots, P_r\}$. With the notation of Step (2), show that $F_Y = \sum_i \prod_{j \neq i}(Y - \alpha_j X) + (F_{r+1})_Y + \cdots$, so $F_Y(x, y) = x^{r-1}(\sum_i \prod_{j \neq i}(z - \alpha_j) + x + \cdots)$. Conclude that $\mathrm{ord}_{P_i}^{C'}(F_Y(x, y)) = r - 1$ for $i = 1, \ldots, r$.

Solution. *Proof.* □

7.5. Let P be an ordinary multiple point on C, $f^{-1}(P) = \{P_1, \ldots, P_r\}$, $L_i = Y - \alpha_i X$ the tangent line corresponding to $P_i = (0, \alpha_i)$. Let G be a plane curve with image g in $\Gamma(C) \subset \Gamma(C')$.

(a) Show that $\mathrm{ord}_{P_i}^{C'}(g) \geq m_P(G)$, with equality if L_i is not tangent to G at P.

(b) If $s \leq r$, and $\mathrm{ord}_{P_i}^{C'}(g) \geq s$ for each $i = 1, \ldots, r$, show that $m_P(G) \geq s$. (*Hint:* How many tangents would G have otherwise?)

Solution. (a) *Proof.* □

(b) *Proof.* □

7.6. If P is an ordinary cusp on C, show that $f^{-1}(P) = \{P_1\}$, where P_1 is a simple point on C'.

Solution. *Proof.* □

7.3 Blowing Up Points in $\mathbb{P}^2$

Problems

7.7. Suppose $P_1 = [0 : 0 : 1]$, $P_1' = [a_{11} : a_{12} : 1]$, and

$$T = (aX + bY + a_{11}Z, cX + dY + a_{12}Z, eX + fY + Z).$$

Show that $T_1 = ((a - a_{11}e)X + (b - a_{11}f)Y, (c - a_{12}e)X + (d - a_{12}f)Y)$ satisfies $T_1 \circ f_1 = f_1' \circ T$. Use this to prove Step (3) above.

Solution. *Proof.* □

7.8. Suppose $P_1 = [0 : 0 : 1]$, $T_1 = (aX + bY, cX + dY)$. Show that $T = (aX + bY, cX + dY, Z)$ satisfies $f_1 \circ T = T_1 \circ f_1$. Use this to prove Step (4).

Solution. *Proof.* □

7.9. Let $C = V(X^4 + Y^4 - XYZ^2)$. Write down equations for a nonsingular curve X in some $\mathbb{P}^N$ which is birationally equivalent to C. (Use the Segre imbedding.)

Solution. *Proof.* □

7.4 Quadratic Transformations

Problems

7.10. Let $F = 8X^3Y + 8X^3Z + 4X^2YZ - 10XY^3 - 10XY^2Z - 3Y^3Z$. Show that F is in good position, and that $F' = 8Y^2Z + 8Y^3 + 4XY^2 - 10X^2Z - 10X^2Y + 3X^3$. Show that F and F' have real parts as in the example, and find the multiple points of F and F'.

Solution. *Proof.* □

7.11. Find a change of coordinates T so that $(Y^2Z - X^3)^T$ is in excellent position, and $T(0, 0, 1) = (0, 0, 1)$. Calculate the quadratic transformation.

Solution. *Proof.* □

7.12. Find a quadratic transformation of $Y^2Z^2 - X^4 - Y^4$ with only ordinary multiple points. Do the same with $Y^4 + Z^4 - 2X^2(Y - Z)^2$.

Solution. *Proof.* □

7.13. (a) Show that in the lemma, we may choose T in such a way that for a given finite set S of points of F $(P \notin S)$, $T^{-1}(S) \cap V(XYZ) = \emptyset$. Then there is a neighborhood of S on F which is isomorphic to an open set on $(F^T)'$.

(b) If S is finite set of simple points on a plane curve F, there is a curve F' with only ordinary multiple points, and a neighborhood U of S on F, and an open set U' on F' consisting entirely of simple points, such that U is isomorphic to U'.

Solution. (a) *Proof.* □

(b) *Proof.* □

7.14. (a) What happens to the degree, and to $g^*(F)$, when a quadratic transformation is centered at: (i) an ordinary multiple point (ii) a simple point (iii) a point not on F?

(b) Show that the curve F' of Problem (b) may be assumed to have arbitrarily large degree.

Solution. (a) *Proof.* □

(b) *Proof.* □

7.15. Let $F = F_1, \dots, F_m$ be a sequence of quadratic transformations of F, such that F_m has only ordinary multiple points. Let $P_{i1}, P_{i2}, \dots$ be the points as in part **??** of Step **??** introduced in going from F_{i-1} to F_i (called "neighboring singularities"; see Walker's "Algebraic Curves", Chap. III, §7.6, 7.7). If $n = \deg(F)$, show that

$$(n-1)(n-2) \geq \sum_{P \in F} m_P(F)(m_P(F)-1) + \sum_{i,j} m_{P_{ij}}(F_i)(m_{P_{ij}}(F_i)-1).$$

Solution. *Proof.* □

7.16. (a) Show that everything in this section, including Theorem **??**, goes through for any plane curve with no multiple components.

(b) If F and G are two curves with no common components, and no multiple components, apply (a) to the curve FG. Show that there are sequences of quadratic transformations $F = F_1, \dots, F_s = F'$, $G = G_1, \dots, G_s = G'$, where F' and G' have only ordinary multiple points, and no tangents in common at points of intersection. Show that

$$\deg(F)\deg(G) = \sum m_P(F)m_P(G) + \sum_{i,j} m_{P_{ij}}(F_i)m_{P_{ij}}(G_i),$$

where P_{ij} are the neighboring singularities of FG, determined as in Problem 7.15.

Solution. (a) *Proof.* □

(b) *Proof.* □

7.5 Nonsingular Models of Curves

Problems

7.17. (a) Show that for any irreducible curve C (projective or not) there is a nonsingular curve X and a birational morphism f from X onto C. What conditions on X will make it unique?

(b) Let $f : X \to C$ as in (a), and let C° be the set of simple points of C. Show that the restriction of f to $f^{-1}(C^{\circ})$ gives an isomorphism of $f^{-1}(C^{\circ})$ with C°.

Solution. (a) *Proof.* □

(b) *Proof.* □

7.18. Show that for any place P of a curve C, and choice t of uniformizing parameter for $\mathscr{O}_P(X)$, there is a homomorphism $\varphi : k(C) \to k((T))$ taking t to T (See Problem 2.32). Show how to recover the place from φ. (In many treatments of curves, a place is defined to be a suitable equivalence class of "power series expansions".)

Solution. *Proof.* □

7.19. Let $f : X \to C$ as above, C a projective plane curve. Suppose P is an ordinary multiple point of multiplicity r on C, $Q_1, \ldots, Q_r$ the places on X centered at P. Let G be any projective plane curve, and let $s \leq r$. Show that $m_P(G) \geq s$ if and only if $\text{ord}_{Q_i}(G) \geq s$ for $i = 1, \ldots, r$. (See Problem 7.5.)

Solution. *Proof.* □

7.20. Let R be a domain with quotient field K. The *integral closure* R' of R is $\{z \in k \mid z \text{ is integral over } R\}$.

(a) If R is a DVR, then $R' = R$.

(b) If $R'_\alpha = R_\alpha$, then $(\cap R_\alpha)' = (\cap R_\alpha)$.

(c) With $f : X \to C$ as in Lemma **??**, show that $\Gamma(f^{-1}(U)) = \Gamma(U)'$ for all open sets U of C. This gives another algebraic characterization of X.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

7.21. Let X be a nonsingular projective curve, $P_1, \ldots, P_s \in X$.

(a) Show that there is projective plane curve C with only ordinary multiple points, and a birational morphism $f : X \to C$ such that $f(P_i)$ is simple on C for each i. (Hint: if $f(P_i)$ is multiple, do a quadratic transform centered at $f(P_i)$.)

(b) For any $m_1, \ldots, m_r \in \mathbb{Z}$, show that there is a $z \in k(X)$ such that $\text{ord}_{P_i}(z) = m_i$ (Problem 5.15).

(c) Show that the curve C of Part (a) may be found with arbitrarily large degree (Problem 7.14).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

7.22. Let P be a node on an irreducible plane curve F, and let L_1, L_2 be the tangents to F at P. P is called a *simple node* if $I(P, L_i \cap F) = 3$ for $i = 1, 2$. Let H be the Hessian of F.

(a) If P is a simple node on F, show that $I(P, F \cap H) = 6$. (Hint: Let $P = (0, 0, 1)$, $F_* = xy + \ldots$, and use Proposition **??** to show that all monomials of degree ≥ 4 may be ignored. See Problem 5.23).

(b) If P is a cusp on F, show that $I(P, F \cap H) = 8$. (See Problem 7.6).

(c) Use (a) and (b) to show that every cubic has one, three, or nine flexes; then Problem 5.24 gives another proof that every cubic is projectively equivalent to one of the type $Y^2 Z =$ cubic in X and Z.

(d) If the curve F has degree n, and i flexes (all ordinary), and δ simple nodes, and k cusps, and no other singularities, then $i + 6\delta + 8k = 3n(n-2)$. This is one of "Plücker's formulas" (See Walker's "Algebraic Curves" for the others).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

Chapter 8

Riemann-Roch Theorem

Problems

8.1. Let $X = C = \mathbb{P}^1$, $k(X) = k(t)$, where $t = X_1/X_2$, X_1, X_2 homogeneous coordinates on $\mathbb{P}^1$.

(a) Calculate div (t).

(b) Calculate div (f/g), f, g relatively prime in $k[t]$.

(c) Prove Proposition **??** directly in this case.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

8.2. Let $X = C = V(Y^2Z - X(X - Z)(X - \lambda Z)) \subset \mathbb{P}^2$, $\lambda \in k$, $\lambda \neq 0, 1$. Let $x = X/Z$, $y = Y/Z \in K$; $K = k(x, y)$. Calculate div (x), div (y).

Solution. *Proof.* □

8.3. Let $C = X$ be a nonsingular cubic.

(a) Let $P, Q \in C$. Show that $P \equiv Q$ if and only if $P = Q$. (*Hint:* Lines are adjoints of degree 1.)

(b) Let $P, Q, R, S \in C$. Show that $P + Q \equiv R + S$ if and only if the line through P and Q intersects the line through R and S in a point on C (If $P = Q$ use the tangent line).

(c) Let P_0 be a fixed point on C, thus defining an addition $\oplus$ on C (Chapter 5, Section 5.6). Show that $P \oplus Q = R$ if and only if $P + Q \equiv R + P_0$. Use this to give another proof of Proposition **??** of Section 5.6).

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

8.4. Let C be a cubic with a node. Show that for any two simple points P, Q on C, $P \equiv Q$.

Solution. *Proof.* □

8.5. Let C be a nonsingular quartic, $P_1, P_2, P_3 \in C$. Let $D = P_1 + P_2 + P_3$. Let L, L' lines such that $L \cdot C = P_1 + P_2 + P_4 + P_5$, $L' \cdot C = P_1 + P_3 + P_6 + P_7$.

Suppose these seven points are distinct. Show that D is not linearly equivalent to any other effective divisor. (*Hint:* Apply the residue theorem to the conic LL'.) Investigate in a similar way other divisors of small degree on quartics with various types of multiple points.

Solution. *Proof.* □

8.6. Let $D(X)$ be the group of divisors on X, $D_0(X)$ the subgroup consisting of divisors of degree zero, and $P(X)$ the subgroup of $D_0(X)$ consisting of divisors of rational functions. Let $C_0(X) = D_0(X)/P(X)$ be the quotient group. It is the *divisor class group* on X.

(a) If $X = \mathbb{P}^1$, then $C_0(X) = 0$.

(b) Let $X = C$ be a nonsingular cubic. Pick $P_0 \in C$, defining $\oplus$ on C. Show that the map from C to $C_0(X)$ which sends P to the residue class of the divisor $P - P_0$ is an isomorphism from $(C, \oplus)$ onto $C_0(X)$.

Solution. (a) *Proof.* □

(b) *Proof.* □

8.7. When do two curves G, H, have the same divisor (C and X fixed)?

Solution. *Proof.* □

8.1 The Vector Spaces $L(D)$

Problems

8.8. If $D \leq D'$, then $\ell(D') \leq \ell(D) + \deg(D' - D)$, i.e. $\deg(D) - \ell(D) \leq \deg(D') - \ell(D')$.

Solution. *Proof.* □

8.9. Let $X = \mathbb{P}^1$, t as in Problem 8.1. Calculate $L(r(t)_0)$ explicitly, and show that $\ell(r(t)_0) = r + 1$.

Solution. *Proof.* □

8.10. Let $X = C$ be a cubic, x, y as in Problem 8.2. Let $z = x^{-1}$. Show that $L(r(z)_0) \subset k[x, y]$, and show that $\ell(r(z)_0) = 2r$ if $r > 0$.

Solution. *Proof.* □

8.11. Let D be a divisor. Show that $\ell(D) > 0$ if and only if D is linearly equivalent to an effective divisor.

Solution. *Proof.* □

8.12. Show that $\deg(D) = 0$ and $\ell(D) > 0$ if and only if $D \equiv 0$.

Solution. *Proof.* □

8.13. Suppose $\ell(D) > 0$, and let $f \neq 0$, $f \in L(D)$. Show that $f \notin L(D - P)$ for all but a finite number of P. So $\ell(D - P) = \ell(D) - 1$ for all but a finite number of P.

Solution. *Proof.* □

8.2 Riemann's Theorem

Problems

8.14. Calculate the genus of each of the following curves:

(a) $X^2Y^2 - Z^2(X^2+Y^2)$.

(b) $(X^3+Y^3)Z^2 + X^3Y^2 - X^2Y^3$.

(c) The two curves of Problem 7.12.

(d) $(X^2-Z^2)^2 - 2Y^3Z - 3Y^2Z^2$.

Solution. (a)

(b)

(c)

(d)

8.15. Let $D = \sum n_P P$ be an effective divisor, $S = \{P \in X \mid n_P > 0\}$, $U = X \setminus S$. Show that $L(rD) \subset \Gamma(U, \mathscr{O}_X)$ for all $r \geq 0$.

Solution. *Proof.* □

8.16. Let U be any open set on X, $\emptyset \neq U \neq X$. Then $\Gamma(U, \mathscr{O}_X)$ is infinite dimensional over k.

Solution. *Proof.* □

8.17. Let X, Y be nonsingular projective curves, $f : X \to Y$ a dominating morphism. Prove that $f(X) = Y$. (*Hint:* If $P \in Y \setminus f(X)$, then $\widetilde{f}(\Gamma(Y \setminus \{P\})) \subset \Gamma(X) = k$; apply Problem 8.16.)

Solution. *Proof.* □

8.18. Show that a morphism from a projective curve X to a curve Y is either constant or surjective; if it is surjective, Y must be projective.

Solution. *Proof.* □

8.19. If $f : C \to V$ is a morphism from a projective curve to a variety V, then $f(C)$ is a closed subvariety of V. (*Hint:* Consider C' = closure of $f(C)$ in V.)

Solution. *Proof.* □

8.20. Let C be the curve of Problem 8.14(b), and let P be a simple point on C. Show that there is a $z \in \Gamma(C \setminus \{P\})$ with $\operatorname{ord}_P(z) \geq -12$, $z \notin k$.

Solution. *Proof.* □

8.21. Let $C_0(X)$ be the divisor class group of X. Show that $C_0(X) = 0$ if and only if X is rational.

Solution. *Proof.* □

8.3 Derivations and Differentials

Problems

8.22. Generalize Proposition **??** to function fields in n variables.

Solution. *Proof.* □

8.23. With $\mathscr{O}$, t as in Proposition **??**, let $\varphi : \mathscr{O} \to k[[T]]$ be the corresponding homomorphism (Problem 2.32). Show that, for $f \in \mathscr{O}$, φ takes the derivative of f to the "formal derivative" of $\varphi(f)$. Use this to give another proof of Proposition **??**, and of the fact that $\Omega_k(K) \neq 0$ in Proposition **??**.

Solution. *Proof.* □

8.4 Canonical Divisors

Problems

8.24. Show that if $g > 0$, then $n \geq 3$ (notation as in Proposition **??**).

Solution. *Proof.* □

8.25. Let $X = \mathbb{P}^1$, $K = k(t)$ as in Problem 8.1. Calculate div (dt), and show directly that the above corollary holds when $g = 0$.

Solution. *Proof.* □

8.26. Show that for any X there is a curve C birationally equivalent to X satisfying the conditions of Proposition **??** (See Problem 7.21).

Solution. *Proof.* □

8.27. Let $X = C$, x, y as in Problem 8.2. Let $\omega = y^{-1}\, dx$. Show that div $(\omega) = 0$.

Solution. *Proof.* □

8.28. Show that if $g > 0$, there are effective canonical divisors.

Solution. *Proof.* □

8.5 Riemann-Roch Theorem

Problems

8.29. Let D be any divisor, $P \in X$. Then $\ell(W - D - P) \neq \ell(W - D)$ if and only if $\ell(D + P) = \ell(D)$.

Solution. *Proof.* □

8.30. (Reciprocity Theorem of Brill-Noether). Suppose D and D' are divisors, and $D + D' = W$ is a canonical divisor. Then $\ell(D) - \ell(D') = \frac{1}{2}(\deg(D) - \deg(D'))$.

Solution. *Proof.* □

8.31. Let D be a divisor with $\deg(D) = 2g - 2$ and $\ell(D) = g$. Show that D is a canonical divisor. So these properties characterize canonical divisors.

Solution. *Proof.* □

8.32. Let $P_1, \dots, P_m \in \mathbb{P}^2$, $r_1, \dots, r_m$ non-negative integers. Let $V(d; r_1P_1, \dots, r_mP_m)$ be the space of curves F of degree d with $m_{P_i}(F) \geq r_i$. Suppose there is a curve C of degree n with ordinary multiple points $P_1, \dots, P_m$, and $m_{P_i}(C) = r_i + 1$; and suppose $d \geq n - 3$. Show that (as a projective space) $\dim(V)(d; r_1P_1, \dots, r_mP_m) = \frac{1}{2}d(d+3) - \frac{1}{2}\sum(r_i+1)r_i$. Compare with Theorem **??**.

Solution. *Proof.* □

8.33. (Linear Series). Let D be a divisor, and let V be a subspace of $L(D)$ (as a vector space). The set of effective divisors $\{\operatorname{div}(F)+D \mid f \in V\}$ is called a *linear series.* If $f_1, \dots, f_{r+1}$ is a basis for V, then the correspondence $\operatorname{div}(\sum \lambda_i f_i) + D \mapsto (\lambda_1, \dots, \lambda_{r+1})$ sets up a one-to-one correspondence between the linear series and $\mathbb{P}^r$. If $\deg(D) = n$, the series is often called a g_n^r. The series is called *complete* if $V = L(D)$, i.e. every effective divisor linearly equivalent to D appears. Show that, with C, E as in Section **??**, the series $\{\operatorname{div}(G) - E \mid G$ is an adjoint of degree n not containing $C\}$ is complete.

Solution. *Proof.* □

8.34. Show that there are curves of every positive genus. (*Hint:* Consider affine plane curves $y^2a(x) + b(x) = 0$, where $\deg(a) = g$, $\deg(b) = g+2$).

Solution. *Proof.* □

8.35. Show that every curve of genus 2 is birationally equivalent to a plane curve of order 4 with one double point.

Solution. *Proof.* □

8.36. Let $f : X \to Y$ be a nonconstant (therefore surjective) morphism of projective nonsingular curves, corresponding to a homomorphism $\widetilde{f}$ of $k(Y)$ into $k(X)$. The integer $n = [k(X) : k(Y)]$ is called the *degree* of f. If $P \in X$, $f(P) = Q$, let $t \in \mathscr{O}_Q(Y)$ be a uniformizing parameter. The integer $e(P) = \operatorname{ord}_P(t)$ is called the *ramification index* of f at P.

(a) For each $Q \in Y$, show that $\displaystyle\sum_{f(P)=Q} e(P)P$ is an effective divisor of degree n. (See Proposition **??**).

(b) $(\operatorname{char}(k) = 0)$. With t as above, show that $\operatorname{ord}_P(dt) = e(P) - 1$.

(c) $(\operatorname{char}(k) = 0)$. If g_X (resp. g_Y) is the genus of X (resp. Y), show that $2g_X - 2 = (2g_Y - 2)n + \sum_{P \in X}(e(P) - 1)$. (*Hurwitz Formula*).

(d) For all but a finite number of $P \in X$, $e(P) = 1$. The points $P \in X$ (and $f(P) \in Y$) where $e(P) > 1$ are called *ramification points.* If $Y = \mathbb{P}^1$, $n > 1$, show that there are always some ramification points.

If $k = \mathbb{C}$, a nonsingular projective curve has a natural structure of a one-dimensional compact complex analytic manifold, and hence a two-dimensional real analytic manifold. From the Hurwitz Formula (c) with $Y = \mathbb{P}^1$ it is easy to prove that the genus defined here is the same as the topological genus ($= \frac{1}{2}\dim_{\mathbb{R}}(H_1(X, \mathbb{R}))$ of this manifold. (See Lang's "Algebraic Functions".)

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

8.37. (*Weierstrass Points;* assume char $(k) = 0$). Let P be a point on a nonsingular curve X of genus g. Let $N_r = N_r(P) = \ell(rP)$.

(a) $1 = N_0 \leq N_1 \leq \cdots \leq N_{2g-1} = g$. So there are exactly g numbers $0 < n_1 < n_2 < \cdots < n_g < 2g$ such that there is no $z \in k(X)$ with a pole only at P, and $\text{ord}_P(z) = -n_i$. These n_i are called the *Weierstrass gaps,* $(n_1, \ldots, n_g)$ the *gap sequence* at P. The point P is called a Weierstrass point if the gap sequence at P is anything but $(1, 2, \ldots, g)$ i.e. if $\sum_{i=1}^{g}(n_i - i) > 0$.

(b) The following are equivalent:

i) P is a Weierstrass point.

ii) $\ell(gP) > 1$.

iii) $\ell(W - gP) > 0$.

iv) There is a differential ω on X with div $(\omega) \geq gP$.

(c) If r, s are not gaps at P, then $r + s$ is not a gap.

(d) If 2 is not a gap at P, the sequence is $(1, 3, \ldots, 2g-1)$. Such a Weierstrass point (if $g > 1$) is called *hyperelliptic.* X has a hyperelliptic Weierstrass point if and only if there is a morphism $f : X \to \mathbb{P}^1$ of degree 2. Such an X is called a hyperelliptic curve.

(e) n is a gap at P if and only if there is a differential of the first kind ω with $\text{ord}_P(\omega) = n - 1$.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

(e) *Proof.* □

8.38. Fix $z \in K$, $z \notin k$. For $f \in K$, denote the derivative of f with respect to z by f'; let $f^{(0)} = f$, $f^{(1)} = f', f^{(2)} = (f')'$, etc. For $f_1, \ldots, f_r \in K$, let $W(f_1, \ldots, f_r) = \det(() f_j^{(i)})$, $i = 0, \ldots, r-1$, $j = 1, \ldots, r$. (The "Wronskian"). Let $\omega_1, \ldots, \omega_g$ be a basis of $\Omega(0)$. Write $\omega_i = f_i \, dz$, and let $h = W(f_1, \ldots, f_g)$.

(a) h is independent of choice of basis, up to multiplication by a constant.

(b) If $t \in K$ and $\omega_i = e_i \, dt$, then $h = W(e_1, \ldots, e_g)(t')^{1+\cdots+g}$.

(c) There is a basis $\omega_1, \ldots, \omega_g$ for $\Omega(0)$ such that $\operatorname{ord}_P(\omega_i) = n_i - 1$, where $(n_1, \ldots, n_g)$ is the gap sequence at P.

(d) $\operatorname{ord}_P(h) = \sum(n_i - i) - \frac{1}{2}g(g+1) \operatorname{ord}_P(dz)$ (*Hint:* Let t be a uniformizing parameter at P and look at lowest degree terms in the determinant.)

(e) $\sum_{P,i}(n_i(P) - i) = (g-1)g(g+1)$, so there are a finite number of Weierstrass points. Every curve of genus > 1 has Weierstrass points.

Solution. (a) *Proof.* □

(b) *Proof.* □

(c) *Proof.* □

(d) *Proof.* □

(e) *Proof.* □