Algebraic Curves: Notes and Solutions

Aven Bross

September 24, 2018

1 Affine Algebraic Sets

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 $r + s$.

Proof. Since F, G are forms $F = \sum_{i=1}^{m} a_i X^{(i)}$ and $G = \sum_{j=1}^{l} b_j X^{(j)}$ with $a_i, b_j \in k$ and $X^{(i)}, X^{(j)}$ monomials of degree r, s for each $(i), (j)$, respectively. Observe

$$FG = \sum_{i=1}^{m} \sum_{j=1}^{l} a_i b_j X^{(i)} X^{(j)}.$$

Note each term is a monomial of degree $r + s$. Thus FG is a form. □

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

Proof. Suppose F is a form of degree n and $G, H \in R[X_1, \ldots, X_n]$ such that $GH = F$. Then $G = G_0 + G_1 + \ldots + G_r$ and $H = H_0 + H_1 + \ldots H_s$ with $r + s = n$, G_i, H_j forms of degree i, j for each $i \in \{0, \ldots, r\}$, $j \in \{0, \ldots, s\}$, and $G_r, H_s \neq 0$.

Let i, j be the least integers such that $G_i, H_j \neq 0$. Then $G_i H_j$ is a term of F with degree $i + j$. Since F is a form it must be that $i + j = n$ and hence $i = r, j = s$. □

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.

Proof. Let $z = a/b \in K$. Since R is a UFD we have $a = p_1 \dots p_n, b = q_1 \dots q_m$ with $p_1, \dots p_n, q_1, \dots, q_m \in R$ irreducible. Suppose $q_i \mid p_j$ for some i, j. Then $p_j = uq_i$ for some unit $u \in R$. So

$$z = \frac{a}{b} = \frac{p_1 \dots p_j \dots p_n}{q_1 \dots q_j \dots q_m} = \frac{p_1 \dots uq_i \dots p_n}{q_1 \dots q_i \dots q_m} = \frac{up_1 \dots p_{j-1}p_{j+1} \dots p_n}{q_1 \dots q_{i-1}q_{i+1} \dots q_m}.$$

By induction we may reduce a, b such that $\gcd(a, b) = 1$. That is, if $u \in R$ such that $u \mid a$ and $u \mid b$, then u is a unit.

Now suppose $z = a/b = c/d \in K$ such that $\gcd(a, b) = \gcd(c, d) = 1$. So $ad = bc$. Since $a \mid bc$ and $\gcd(a, b) = 1$, it must be that $a \mid c$. Thus $c = ra$ for some $r \in R$. Moreover, $d = rb$. Since $\gcd(c, d) = 1$, r is a unit. Thus the representation is unique up to units of R. □

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.

Proof. Since R is a PID, $P = (a)$ for some $a \in P$. Suppose $a = rs$ for some $r, s \in R$. Since P is prime we may assume, without loss of generality, $r = ac$, $c \in R$. Thus $a = acs$. So $cs = 1$ and s is a unit. Thus a is irreducible. □

(b) Show that P is maximal.

Proof. Suppose $Q = (b)$ is an ideal of R such that $P \subset Q$. Then $a = br$, $r \in R$. Since a is irreducible by part (a), one of b or r must be a unit. If r is a unit then $P = (a) = (b) = Q$. If b is a unit then $bb^{-1} = 1 \in Q$, so $Q = (1) = R$. Thus P is maximal. □

1.4.* Let k be an infinite field, $F \in k[X_1, \dots, X_n]$. Suppose $F(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in k$. Show that $F = 0$.

Proof. Suppose $n = 1$, that is, $F \in k[X]$. Then since F has infinitely many roots, $F = 0$.

Suppose $n > 1$ and the statement holds for $k[X_1, \dots, X_{n-1}]$. Observe we may write

$$F = \sum_{i=0}^{\deg(F)} F_i X_n^i$$

where $F_i \in k[X_1, \ldots, X_{n-1}]$ for each i. Let $a_1, \ldots, a_{n-1} \in k$. If $F_i(a_1, \ldots, a_{n-1}) \neq 0$ for any i then $F(a_1, \ldots, a_{n-1}, X_n)$ has finitely many roots. So $F_i(a_1, \ldots, a_{n-1}) = 0$ for each i. Thus by the inductive hypothesis, $F_i = 0$ for each i and $F = 0$. □

1.5.* Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[X]$.

Proof. Suppose there exist only finitely many irreducible monic polynomials $F_1, \ldots, F_n$. Let $F_{n+1} = F_1 \ldots F_n + 1$. Let G be an irreducible polynomial dividing F_{n+1}. Since $G \neq F_i$ for any i, we have a contradiction. □

1.6* Show that any algebraically closed field is infinite.

Proof. Let k be an algebraically closed field. By Problem 1.5 there are infinitely many irreducible polynomials in $k[X]$. But since k is algebraically closed the irreducible polynomials are precisely those of the form $(X - a)$, $a \in k$. Thus k is 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

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

Proof. Observe since $K[X_1]$ is a Euclidean domain we may repeatedly divide by $(X_1 - a_1)$ $a, b \in k$ and write $F = \sum_{i=0}^{\deg(F)} \lambda_i (X_1 - a_1)^i$, $\lambda_i \in k$.

Suppose $n > 1$ and the statement holds for $k[X_1, \ldots, X_{n-1}]$. Then we may write

$$F = \sum \mu_{(i)}(X_1 - a_1)^{i_1} \ldots (X_{n-1} - a_{n-1})^{i_{n-1}} G_{(i)},\ \mu_{(i)} \in k, G_{(i)} \in k[X_n].$$

Moreover, for each (i) we may write $G_{(i)} = \sum_{j=0}^{\deg(G_{(i)})} \mu_j (X_n - a_n)^j$, each $\mu_j \in k$. By expanding and grouping by multidegree (i) we therefore may write

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

□

(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 $k[X_1, \ldots, X_n]$.

Proof. By part (a) we may write

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

Since $(a_1, \dots, a_n)$ is a root of F the above sum has no constant term, that is, for each (i) we have $i_j \geq 1$ for some $j \in \{1, \dots, n\}$. Hence we may regroup the sum in the form

$$F = \sum_{i=1}^{n} (X_i - a_i)G_i.$$

□

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

Proof. Suppose $A = V(S)$ for some $S \subset k[X]$. If $S = \emptyset$ then $A = \mathbb{A}^1(k)$. Otherwise let $F \in S$. Note $A \subset V(F)$. Since F has finitely many roots, $V(F)$ is finite. Thus A is finite.

Conversely, by (4) any finite subset of $\mathbb{A}^1(k)$ is algebraic. □

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

Proof. Since k is finite, $\mathbb{A}^n(k)$ is finite. Thus every subset of $\mathbb{A}^n(k)$ is finite and therefore algebraic by (4). □

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

Let $F_n = (x - n)^2 \in \mathbb{R}[X]$, $n \in \mathbb{Z}$. We claim $S = \bigcup_{n \in \mathbb{Z}} V(F_n) \subset \mathbb{R}$ is not algebraic in $\mathbb{A}^2(k)$.

Proof. Suppose S is algebraic. Then $S \subset V(F)$ for some $F \in \mathbb{R}[X]$. Observe $V(X) \cap S = \mathbb{Z}$. Thus $V(X) \cap V(F)$ is infinite, a contradiction. □

1.11. Show that the following are algebraic sets:

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

Observe $V(X - Y^2, X - Z^3) = \{(t, t^2, t^3) \in \mathbb{A}^3(k) \mid t \in k\}$.

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

It is easy to check $V(X^2 + Y^2 - 1) = \{(\cos(t), \sin(t)) \in \mathbb{A}^2(k) \mid t \in \mathbb{R}\}$.

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

It is can be verified that this is the set $V(X^2 + (Y - 1/2)^2 - 1/4)$.

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.

Proof. Suppose $L = V(aY + bX + c)$, where $a, b, c \in k$ and at least one of a or b is nonzero. Without loss of generality, suppose $a \neq 0$. Then $L = V(Y - dX - e)$, where $d = -b/a$ and $e = -c/a$.

If $(x, y) \in L$ then $y = dx + e$. Thus if $(x, y) \in L \cap C$ then $F(x, y) = F(x, dx + e) = 0$. Observe $F(X, dX + e) \in k[X]$ with degree n. Thus $F(X, dX + e)$ has at most n roots and $L \cap C$ contains at most n points. □

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

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

Proof. Suppose $A = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin(x)\} = V(S)$, $S \subset \mathbb{R}[X, Y]$. Clearly $A \neq \mathbb{A}^2(\mathbb{R})$, so $S \neq \emptyset$. Let $F \in S$. Then $A \subset V(F)$. But $A \cap V(Y) = \{(2\pi t, 0) \mid t \in \mathbb{Z}\}$ is infinite. Thus $V(F) \cap V(Y) \supset A \cap V(Y)$ is infinite, a contradiction to Problem 1.12. □

(b) $\{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\}$;

Proof. Suppose $A = \{(z, w) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 + |w|^2 = 1\} = V(S)$, $S \subset \mathbb{C}(Z, W)$. Clearly $S \neq \emptyset$. Let $F \in S$. Observe $A \cap V(W) = \{(z, 0) \in \mathbb{A}^2(\mathbb{C}) \mid |z|^2 = 1\}$, an infinite set. Thus $V(F) \cap V(W)$ is infinite, a contradiction to Problem 1.12. □

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

Proof. Suppose $A = \{\cos(t), \sin(t), t) \in \mathbb{A}^3(\mathbb{R}) \mid t \in \mathbb{R}\} = V(S)$, $S \subset \mathbb{R}[X_1, X_2, X_3]$. Clearly $S \neq \emptyset$. Let $F \in S$. Note $A \subset V(F)$. So $F(\cos(t), \sin(t), t) = 0$ for all $t \in \mathbb{R}$. Thus for any $\theta \in [0, 2\pi)$,

$$F(\cos(\theta + 2n\pi), \sin(\theta + 2n\pi), \theta + 2n\pi) = F(\cos(\theta), \sin(\theta), \theta + 2n\pi).$$

for any $n \in \mathbb{Z}$. But fixing θ this gives $G(X) = F(\cos(\theta), \sin(\theta), X) \in \mathbb{R}[X]$ with $G(n) = 0$ for any $n \in \mathbb{Z}$. This is a contradiction as G must have finitely many roots in $\mathbb{R}$. □

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 $n \geq 1$.

Proof. Suppose $n = 1$. Then $F \in k[X]$ and F has finitely many roots. Since k is algebraically closed, k is infinite by Problem 1.6. Thus $\mathbb{A}^1(k) \setminus V(F)$ is infinite.

Suppose $n > 1$. Let $a_1, \ldots, a_{n-1} \in k$. Then $G = F(a_1, \ldots, a_{n-1}, X_n) \in k[X_n]$. Note G has finitely many roots $b_1, \ldots, b_m$. Observe

$$\mathbb{A}^n(k) \setminus V(F) \supset \{(a_1, \ldots, a_{n-1}, x) \in \mathbb{A}^n(k) \mid x \in k \setminus \{b_1, \ldots, b_m\}\}.$$

Therefore $\mathbb{A}^n(k) \setminus V(F)$ is infinite. □

Show $V(F)$ is infinite if $n \geq 2$.

Proof. Since F is nonconstant there exists $i \in \{1, \ldots, n\}$ such that

$$G = F(a_1, \ldots, a_{i-1}, X_i, a_{i+1} \ldots, a_n) \in k[X_i]$$

is nonconstant, with arbitrary $a_1, \ldots, a_{i-1}a_{i+1} \ldots a_n \in k$. Since k is algebraically closed and G nonconstant, G has a root in k. Thus for each selection of $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in k$, k infinite, there is a distinct root of F in $\mathbb{A}^n(k)$. Thus $V(F)$ is infinite. □

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

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

is an algebraic set.

Proof. Let $V = V(A)$, $W = V(B)$ with $A \subset k[X_1, \ldots, X_n]$, $B \subset k[X_1, \ldots, X_m]$. Let us define $\varphi : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_{n+m}]$ by

$$\varphi(F)(X_1, \ldots, X_n) = F(X_1, \ldots, X_n).$$

Similarly define $\psi : k[X_1, \ldots, X_m] \to k[X_1, \ldots, X_{n+m}]$ by

$$\psi(F)(X_1, \ldots, X_m) = F(X_{n+1}, \ldots, X_{n+m}).$$

It is simple to see

$$V \times W = V(\varphi(A) \cup \psi(B)).$$

□

(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, $I = I(V(I))$.

Proof. Suppose $P \in V(I(V(S)))$. Then $F(P) = 0$ for all $F \in I(V(S))$. In particular, by (8), $F(P) = 0$ for all $F \in S \subset I(V(S))$. So $P \in V(S)$. Thus $V(I(V(S))) \subset V(S)$.

Suppose $P \in V(S)$. Then $F(P) = 0$ for all $F \in I(V(S))$ by definition. Thus $P \in V(I(V(S)))$. Hence $V(S) = V(I(V(S)))$.

Suppose $F \in I(V(I(X)))$. Then $F(P) = 0$ for all $P \in V(I(X))$. In particular, by (8), $F(P) = 0$ for all $P \in X \subset V(I(X))$. Thus $F \in I(X)$. So $I(V(I(X))) \subset I(X)$.

Suppose $F \in I(X)$. By definition of $V(I(X))$, $F(P) = 0$ for all $P \in V(I(X))$. Thus $F \in I(V(I(X)))$. Hence $I(X) = I(V(I(X)))$. □

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

Proof. Suppose $V = W$. Then by (6), $I(V) = I(W)$. Conversely, suppose $I(V) = I(W)$. Then by (9), $V(I(V)) = V$ and $V(I(W)) = W$. By (3), since $I(V) = I(W)$, $V(I(V)) = V(I(W))$. Therefore $V = W$. □

1.17.* (a) Let V be an algebraic set in $\mathbb{A}^n(k)$, $P \in \mathbb{A}^n(k)$ a point not in V. Show that there is a polynomial $F \in k[X_1, \ldots, X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$.

Proof. Since $P \notin V$, there exists $F \in I(V)$ such that $F(P) \neq 0$. Moreover, $F(Q) = 0$ for all $Q \in V$ by definition of $I(V)$. Since k is a field there exists $(F(P))^{-1} \in k$ such that $(F(P))^{-1}F(P) = 1$. Let $G = (F(P))^{-1}F$. Observe $G(Q) = (F(P))^{-1}F(Q) = 0$ for all $Q \in V$ and $G(P) = (F(P))^{-1}F(P) = 1$. □

(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 $F_i(P_i) = 1$.

Proof. Let $i \in \{1, \ldots, r\}$. Let $W_i = V \cup \{P_1, \ldots, P_r\} \setminus \{P_i\}$. Since $P_i \notin W_i$, by (a) there exists $F_i \in I(W_i)$ such that $F_i(P_j) = 0$ for all $j \neq i$, and $F_i(P_i) = 1$. □

(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.

Proof. Let $F_1, \ldots, F_r$ be as in (b). For each $i \in \{1, \ldots, r\}$ define $G_i = \sum_{j=1}^{r} a_{ij} F_j$. Then for $i, j \in \{1, \ldots, r\}$,

$$G_i(P_j) = \sum_{l=1}^{r} a_{il} F_l(P_j) = a_{ij}.$$

□

1.18.* Let I be an ideal in a ring R. If $a^n \in I$, $b^m \in I$, show that $(a+b)^{n+m} \in I$.

Proof. By the binomial theorem observe

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

If $i < m$ then $n+m-i > n$. Therefore each term of the sum has either a^n or b^m as a factor. Since $a^n, b^m \in I$, $(a+b)^{n+m} \in I$. □

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

Proof. Suppose $a, b \in \mathrm{Rad}(I)$, that is, suppose $a^n, b^m \in I$ for some $n, m \in \mathbb{N}$. By our result above, $(a+b)^{n+m} \in I$. Thus $a+b \in \mathrm{Rad}(I)$. Moreover if $a \in \mathrm{Rad}(I)$, then $-a \in \mathrm{Rad}(I)$. Thus $\mathrm{Rad}(I)$ is an abelian group.

Now suppose $a \in \mathrm{Rad}(I)$, with $a^n \in I$, $n \in \mathbb{N}$. Let $r \in R$. Clearly $(ra)^n = r^n a^n \in I$ and thus $ra \in \mathrm{Rad}(I)$. Thus $\mathrm{Rad}(I)$ is an ideal.

Finally, suppose $r \in R$ such that $r^n \in \mathrm{Rad}(I)$, $n \in \mathbb{N}$. Then $(r^n)^m \in I$ for some $m \in \mathbb{N}$. So $r^{nm} \in I$ and $r \in \mathrm{Rad}(I)$. Thus $\mathrm{Rad}(I)$ 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 $\mathbb{A}^1(\mathbb{R})$.

Proof. Note X^2+1 is irreducible as it is degree 2 and has no roots in $\mathbb{R}$. Therefore (X^2+1) is a prime ideal. Moreover, since X^2+1 has no roots in $\mathbb{R}$, $X^2+1 \notin I(V(S))$ for any $S \subset \mathbb{A}^1(\mathbb{R})$, $S \neq \emptyset$. Additionally, $I(V(\emptyset)) = \mathbb{R}[X] \neq (X^2+1)$. Thus (X^2+1) is not the ideal of any set in $\mathbb{A}^1(\mathbb{R})$. □

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

Proof. It is clear $I \subset \mathrm{Rad}(I)$, so $V(\mathrm{Rad}(I)) \subset V(I)$. Suppose $P \in V(I)$. Let $F \in \mathrm{Rad}(I)$. Then $F^n \in I$. Therefore $(F(P))^n = 0$. Thus $F(P) = 0$, since there are no zero divisors in k. Thus $P \in V(\mathrm{Rad}(I))$. So $V(I) = V(\mathrm{Rad}(I))$.

Observe by the result above we have $I(V(I)) = I(V(\mathrm{Rad}(I)))$. Therefore by (8), $\mathrm{Rad}(I) \subset I(V(I))$. □

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.

Proof. Suppose J is an ideal such that $I \subset J$. Let $F \in J$. By Problem 1.7 we may write

$$F = \sum \lambda_(i)(X_1 - a_1)^{i_1} \ldots (X - a_n)^{i_n}.$$

If F has no constant term clearly $F \in I$. Suppose $F \notin I$, that is, suppose F has a nonzero constant term $c \in k$. Then we may write $F = G + c$ with $G \in I$. Thus $F - G = c \in J$. So $1 \in J$ and $J = k[X_1, \ldots, X_n]$. Therefore $J = I$ or $J = k[X_1, \ldots, X_n]$. So I is maximal.

Let $\varphi : k \to k[X_1, \ldots, X_n]/I$ be the natural homomorphism. Let $F + I \in k[X_1, \ldots, X_n]/I$. By the same argument above we may write $F = G + c$ with $G \in I$, $c \in k$. Thus $F + I = c + I = \varphi(c)$. So φ is surjective. Moreover, $\ker \varphi = I \cap k = \{0\}$. Thus φ is injective. Hence φ is an isomorphism. □

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, $\pi^{-1}(J') = R$ 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 that contain I.

Proof. Suppose J' is an ideal of R/I. Since φ is a ring homomorphism, $\varphi^{-1}(J') = J$ is an abelian group. Suppose $r \in R$, $j \in J$. Then observe $\varphi(rj) = \varphi(r)\varphi(j) \in J'$. Thus $rj \in \varphi^{-1}(J') = J$. So J is an ideal.

Suppose J is an ideal of R. Note $\varphi(J) = J'$ is an abelian group. Let $j+I \in \varphi(J)$, $r+I \in R/I$. Observe since $j \in J$, $rj \in J$. Thus $(j + I) + (r + I) = rj + I = \varphi(rj) \in \varphi(J) = J'$. Thus J' is an ideal. □

(b) Show that J' is a radical ideal if and only if J is radical. Similarly for prime and maximal ideals.

Proof. Suppose J' is radical. Suppose $r \in R$ such that $r^n \in J$. Then $\varphi(r^n) = \varphi(r)^n \in J'$. Thus $\varphi(r) \in J'$. Thus $r \in \varphi^{-1}(J') = J$.

Conversely, suppose J is radical. Let $r+I \in R/I$ such that $r^n+I \in J'$. Then $r^n \in \varphi^{-1}(J') = J$ and hence $r \in J$. So $\varphi(r) = r + I \in J'$.

Suppose J' is prime. Let $a, b \in R$ such that $ab \in J$. Then $\varphi(ab) = \varphi(a)\varphi(b) \in J'$. So one of $\varphi(a)$ or $\varphi(b)$ must be in J'. Thus one of a or b must be in J.

Conversely, suppose J is prime. Let $a + I, b + I \in R/I$ such that $ab + I \in J'$. Then $ab \in J$. So one of a or b must be in J and therefore one of $a + I$ or $b + I$ must be in J'.

Suppose J' is maximal. Suppose there exists a proper ideal K of R such that $J \subsetneq K$. Then by (a), $\varphi(K)$ is a proper ideal of R/I properly containing J', a contradiction. So J is maximal.

Conversely, suppose J is maximal. Suppose there exists a proper ideal K' of R/I such that $J' \subsetneq K'$. Then by (a), $J' \subsetneq \varphi^{-1}(K') \subsetneq R$, a contradiction. So J' is maximal. □

(c) Show that J' is finitely generated if J is. Conclude that R/I is Noetheerian if R is Noetherian. Any ring of the form $k[X_1, \ldots, X_n]/I$ is Noetherian.

Proof. Suppose J is finitely generated by $\{j_1, \ldots, j_n\} \subset J$. Then for any $j \in J$ we have $j = r_1 j_1 + \ldots + r_n j_n$, $r_1, \ldots, r_n \in R$. Thus for any $j + I \in J'$ we have

$$j + I = (r_1 j_1 + \ldots + r_n j_n) + I = (r_1 + I)(j_1 + I) + \ldots + (r_n + I)(j_n + I).$$

That is, J' is generated by $\{j_1 + I, \ldots, j_n + I\}$.

Therefore if R is Noetherian, so is R/I. Since $k[X_1, \ldots, X_n]$ is Noetherian, $k[X_1, \ldots, X_n]/I$ is Noetherian for any ideal I. □

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

Take $\mathcal{P} = \{(x^n) \mid n > 0\}$ and note all ideals in $\mathcal{P}$ are properly contained in the maximal ideal $(x, 2)$.

1.24. Show that every proper ideal in a Noetherian ring is contained in a maximal ideal.

Proof. Let P be a prime ideal in a Noetherian ring R. Let

$$\mathcal{P} = \{I \subset R \mid I \text{ is an ideal, } P \subset I\}$$

The maximal element of $\mathcal{P}$ is a maximal ideal of R. □

Lemma 1.1. If R is a PID then the prime ideals of $R[X]$ are precisely those of the form (0), $(F(X))$ where F is irreducible, and $(P, F(X))$ where P is a prime ideal and $F(X) + P$ is irreducible over $(R/P)[X]$.

Proof. Let I be a non-zero prime ideal of $R[X]$.

Suppose $J = I \cap R \neq \{0\}$. Then

$$R[X]/I \cong (R[X]/J[X])/(I/J[X]) \cong (R/J)[X]/(I/(J[X])).$$

Since R/J is a field, $(R/J)[X]$ is a Euclidean Domain. Thus $I/(J[X]) = (F(X) + J[X])$ for some $F \in R[X]$, of minumum degree, such that $F + J[X]$ is irreducible over $(R/J)[X]$. Therefore $I = (J, F(X))$.

Suppose $I \cap R = \{0\}$. Let $F \in I$ be of minimum degree. Suppose $G \in I$ such that $\gcd(F, G) = 1$. By Gauss' Lemma $\gcd(F, G) = 1$ in $K[X]$ where K is the field of fractions of R. Since $K[X]$ is a Euclidean domain, there exist $A, B \in K[X]$ such that $A(X)F(X) + B(X)G(X) = 1 \in K[X]$. If we let $\alpha \in R \setminus \{0\}$ be a common denominator for the coefficients of A, B then $\alpha A(X)F(X) + \alpha B(X)G(X) = \alpha$. Therefore $\alpha \in I$, a contradiction. Thus $F \mid G$ for all $G \in I$. So $I = (F)$. □

1.25. (a) Show that $V(Y - X^2) \subset \mathbb{A}^2(\mathbb{C})$ is irreducible, in fact, $I(V(Y - X^2)) = (Y - X^2)$.

Proof. Note $Y - X^2$ is irreducible in $\mathbb{C}(Y)[X]$. Thus by Gauss' lemma $Y - X^2$ is reducible in $\mathbb{C}[Y][X] = \mathbb{C}[X, Y]$. □

(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.

Proof. Let $V = V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3)$. Observe $Y^4 - X^2 = (Y^2 - X)(Y^2 + X)$ and $Y^4 - X^2Y^2 + XY^2 - X^3 = (Y^2 - X^2)(Y^2 + X) = (Y - X)(Y + X)(Y^2 + X)$. Thus

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

Observe if $Y - X = 0$ or $Y + X = 0$ then $Y^2 = X^2$. So $X^2 - X = 0$ and $X = 0$ or 1.

$$\begin{aligned} V(Y^2 - X, (Y - X)(Y + X)) &= V(X, Y) \cup V(X - 1, Y^2 - 1) \\ &= V(X, Y) \cup V(X - 1, Y - 1) \cup V(X - 1, Y + 1). \end{aligned}$$

By Lemma 1.1, these are all irreducible varieties. Thus

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

□

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

Proof. Observe $Y^2 + X^2(X - 1)^2$ is irreducible in $k(Y)[X]$ and thus irreducible in $k[X, Y]$. However, $V(F) = \{(0, 0), (1, 0)\} = V(X, Y) \cup V(X - 1, Y)$. □

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

Proof. Let $V = V_1 \cup \ldots \cup V_n$ and $W = W_1 \cup \ldots \cup W_m$ be the decomposition of each into irreducible algebraic sets. Let $i \in \{1, \ldots, n\}$. Suppose $V_i \not\subset W_j$ for any $j \in \{1, \ldots, m\}$. Then since $V \subset W$ it must be that $V_i \subset (\bigcup_k W_{j_k})$. But then $(V_i \cap W_{j_1}), \ldots, (V_i \cap W_{j_k}$ is a decomposition of V_i into proper algebraic subsets, a contradiction. □

1.28. If $V = V_1 \cup \ldots \cup V_r$ is the decomposition of an algebraic set into irreducible components, show that $V_i \not\subset \bigcup_j \neq iV_j$.

Proof. Suppose $V_i \subset V_j$ for some $j \neq i$. Then $V_i \cap V_j$ and $V_i \cap \left(\bigcup_{k \neq j} V_k\right)$ is a decomposition of V_i into proper algebraic subsets, a contradiction. □

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

Proof. Suppose k is an infinite field. Suppose $\mathbb{A}^k = V_1 \cup V_2$. Then $V_1 \subset V(F)$ and $V_2 \subset V(G)$ for some nonzero $F, G \in k[X_1, \ldots, X_n]$. So $\mathbb{A}^k = V(F) \cup V(G) = V(FG)$. By Problem 1.4, $FG = 0$, thus $F = 0$ or $G = 0$, a contradiction. □

1.30. Let $k = \mathbb{R}$.

(a) Show that $I(V(X^2+Y^2+1)) = (1)$.

Proof. Observe $a^2+b^2+1 \geq 1$ for all $a, b \in \mathbb{R}$. Thus $I(V(X^2+Y^2+1)) = I(\emptyset) = (1)$. $\square$

(b) Show every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to $V(F)$ for some $F \in \mathbb{R}[X,Y]$.

Proof. By Corollary 2, it suffices to show points are $V(F)$ for some $F \in \mathbb{R}[X,Y]$. Let $(a_1, a_2) \in \mathbb{A}^2(\mathbb{R})$. Define $F = (X-a_1)^2 + (Y-a_2)^2$. Observe that $V(F) = \{(a_1, a_2)\}$. $\square$

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

Observe that $Y^2 - XY - X^2Y + X^3 = (Y-X)(Y-X^2)$. So $V(Y^2 - XY - X^2Y + X^3) = V(Y-X) \cup V(Y-X^2)$. Since $Y-X$ and $Y-X^2$ are irreducible over both $\mathbb{R}$ and $\mathbb{C}$, these are irreducible components

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

In $K[X]$ observe that $X(X^2-1) \in (X)$ and $X(X^2-1) \notin (X^2)$. Therefore $Y^2 - X(X^2-1)$ is irreducible in $K[X][Y]$ by Eisenstein's criterion. Since $Y^2 - X(X^2-1)$ has infinitely many solutions over both the real and complex numbers, $V(Y^2 - X(X^2-1))$ is itself irreducible in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^2(\mathbb{C})$.

Observe that $X^3 + X - X^2Y - Y = (X^2+1)(X-Y)$. Note that X^2+1 has no solutions in $\mathbb{R}$. Thus in $\mathbb{A}^2(\mathbb{R})$ we have $V(X^3 + X - X^2Y - Y) = V(X-Y)$, which is irreducible. In $\mathbb{C}$ we have $X^3 + X - X^2Y - Y = (X-i)(X+i)(X-Y)$ and $V(X^3 + X - X^2Y - Y) = V(X-i) \cup V(X+i) \cup V(X-Y)$.

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

For the Weak Nullstellensatz, observe $(X^2+1) \subset \mathbb{R}[X]$ is a proper ideal but $V(X^2+1) = \emptyset$.

For the Strong Nullstellensatz, consider Problem 1.26. Let $F = Y^2 + X^2(X-1)^2 \in \mathbb{R}[X,Y]$. Note $V(F) = \{(0,0),(1,0)\}$. Thus $I(V(F)) = (X(X-1), Y) \neq \mathrm{Rad}(F) = F$. This is also a counterexample to Corollary 1.

For Corollaries 2 and 3 we again consider Problem 1.26. Observe $F = Y^2 + X^2(X-1)^2$ is irreducible, so (F) is prime. But $V(F) = V(X,Y) \cup V(X-1,Y)$. Let $G = X^2+1$. Additionally if $G = X^2+1$, then (G) is a maximal ideal but $V(G) = \emptyset$.

For Corollary 4 let $I = (Y^2 + X(X-1)^2)$. Above we saw $V(I) = \{(0,0),(1,0)\}$. However, $k[X,Y]/I$ has the infinite linearly independent subset $\{\overline{1}, \overline{Y}, \overline{Y}^2, \ldots\}$.

1.33 (a) Decompose $V(X^2+Y^2-1, X^2-Z^2-1) \subset \mathbb{A}^3(\mathbb{C})$ into irreducible components.

Observe that $(X^2+Y^2-1)-(X^2-Z^2+1) = Y^2+Z^2$. Therefore $(Y+iZ)(Y-iZ) \in (X^2+Y^2+1, X^2-Z^2-1)$. If $Y+iZ = X^2+Y^2-1 = 0$ we have $Y = -iZ$. So $X^2-Z^2-1 = 0$. The same is true if $Y-iZ = X^2+Y^2-1 = 0$. Therefore $V(X^2+Y^2-1, X^2-Z^2-1) = V(X^2+Y^2-1, Y+iZ) \cup V(X^2+Y^2, Y-iZ)$. Observe

$$\begin{aligned}\mathbb{C}[X,Y,Z]/(X^2+Y^2-1, X+iZ) &\cong (\mathbb{C}[X,Z]/(X+iZ))[Y]/(X^2+Y^2-1)\\ &\cong \mathbb{C}[X,Y]/(X^2+Y^2-1).\end{aligned}$$

We may observe that X^2+Y^2-1 is irreducible over $\mathbb{C}[X][Y]$. Therefore $\mathbb{C}[X,Y]/(X^2+Y^2-1)$ is an integral domain and $(X^2+Y^2-1, X+iZ)$ is a prime ideal. So $V(X^2+Y^2-1, X+iZ)$ is irreducible. A similar argument follows for $V(X^2+Y^2-1, X-iZ)$.

(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.

Note that $V = V(Y-X^2, Z-X^3)$. We will show that $(Y-X^2, Z-X^3)$ is a prime ideal by showing that $\mathbb{C}[X,Y,Z]/(Y-X^2, Z-X^3)$ is an integral domain. Observe

$$\begin{aligned}\mathbb{C}[X,Y,Z]/(Y-X^2, Z-X^3) &\cong (\mathbb{C}[X,Y]/(Y-X^2))[Z]/(Z-X^3) &(1)\\ &\cong \mathbb{C}[X,Z]/(Z-X^3) &(2)\\ &\cong \mathbb{C}[X]. &(3)\end{aligned}$$

Step 1 follows from the third isomorphism theorem (numbering from Dummit and Foote). Step 2 follows from the homomorphism $Y \mapsto X^2$. Step 3 follows from the homomorphism $Z \mapsto X^3$.

1.34. Let R be a UFD.

(a) Show a monic polynomial of degree two or three in $R[X]$ is irreducible if and only if it has no roots in R.

Proof. Let $F \in R[X]$ with $2 \leq \deg(F) \leq 3$.

Suppose $G, H \in R[X]$ are nonconstant such that $F = GH$. Note that G and H must be monic. Since $\deg(F) = \deg(G) + \deg(H)$, one of $\deg(G)$ or $\deg(H)$ must be 1. Therefore one is of the form $X-a$, $a \in R$. So a is a root of F.

Suppose $a \in R$ is a root of F. Then by the division algorithm there exists $G \in R[X]$ such that $F(X) = (X-a)G(X)$. □

(b) The polynomial $X^2 - a$ is irreducible if and only if a is not a square in R.

Proof. Note that $X^2 - a$ has a root in R if and only if a is a square in R. Therefore the result follows from part (a). □

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 $\lambda \in k$.

Proof. Note $Y^2 - X(X-1)(X-\lambda)$ has no root in $k[X]$, and therefore it is irreducible over $k[X,Y]$. □

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

Note that $X^2, Y^2 \in I$. Thus since it is easy to see $(X^2, Y^2) \supset I$, $I = (X^2, Y^2)$. Observe that $\mathbb{C}[X,Y]/(X^2,Y^2)$ is spanned by the linearly independent set $\{\overline{1}, \overline{X}, \overline{Y}, \overline{XY}\}$.

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

Proof. Let $F = \sum_{i=0}^{n} a_i x^i$. Then $\overline{X}^n = \sum_{i=0}^{n-1} \overline{-a_n^{-1} a_i x^i}$. By induction, $\overline{X}^m$ is a linear combination of the linearly independent set $\{\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}\}$. □

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

Proof. Let $U \subset V$ be an algebraic set. Then $I(U)$ is a radical ideal in R such that $I \subset I(V) \subset I(U)$. Thus by Problem 22 (the Fourth Isomorphism Theorem in Dummit and Foote), $\overline{I(U)}$ is a radical ideal in R/I.

Similarly, if $\overline{J}$ is a radical ideal in R/I then J is a radical ideal in R with $I \subset J$. Thus $V(J) \subset V(I)$.

We prove the final statements by noting that an ideal $J \supset I$ in R is prime (resp. maximal) if and only if $\overline{J}$ is prime (resp. maximal) in R/I. □

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 $0 \subset Q \subset P$, $Q \neq 0$, $Q \neq P$.

Proof. Suppose $Q \subset P$ is a prime ideal. Let $q \in Q$, $q \neq 0$. Let $q = p_0 p_1 \dots p_k$ with $p_0, \dots, p_k$ irreducible. For any i note that if $p_i \in P$ then $p_i = ut$ for some unit u.

Suppose, with renumbering, that $p_0, \dots, p_l \notin P$ and $p_{l+1}, \dots, p_k \in P$, were $0 \leq l \leq k$. Note that since $q \in P$, $l < k$. Moreover, since $p_0 \dots p_l \notin Q$, it must be that $p_{l+1} \dots p_k \in Q$. But $p_{l+1} \dots p_k = ut^{k-l}$ for some unit u. So it must be that $t^{k-l} \in Q$. But Q is prime, so therefore $t \in Q$. Thus $Q = P$. □

(b) Let $V = V(F)$ be irreducible. Show that there is no irreducible algebraic set W such that $V \subset W \subset \mathbb{A}^n$, $W \neq V$, $W \neq \mathbb{A}^n$.

Proof. Observe if F is reducible then, by Corollary 4, $F = G^n$ and $I(V(F)) = (G)$ is prime. If $V \subset W \subset \mathbb{A}^n$, then $0 \subset I(W) \subset I(V) = (G)$. Therefore by part (a) $I(W) = 0$ or $I(W) = I(V)$. □

Bonus (Exercise 1.9 from Gathman's notes). Prove that every affine variety $X \subset \mathbb{A}^n$ consisting of finitely many points is the zero locus of n polynomials.

Note. For this exercise I used more standard notation (lowercase $f, g, \dots$ for polynomials, etc.) to match the notation used by Gathmann.

Proof. Let $X = \{p_1, \dots, p_r\}$ with each $p_i = (a_{i1}, \dots, a_{in}) \in \mathbb{A}^n$. We will define $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ such that $X = V(f_1, \dots, f_n)$.

Let $S = \{1, \dots, r\}$. Define $f_1 = \prod_{i \in S}(x_1 - a_{i1})$.

Let $i \in S$. Define the polynomial

$$g_i(x_1) = \frac{\prod_{j \in S \setminus \{i\}}(x_1 - a_{j1})}{\prod_{j \in S \setminus \{i\}}(a_{i1} - a_{j1})}.$$

Suppose $f_1 = 0$, that is, $x_1 = a_{k1}$ for some k. Then $g_i(x_1) = 0$ for all $i \neq k$ and $g_k(x_1) = 1$.

Let $d \in \{2, \dots, n\}$. Define the polynomial

$$f_d(x_1, \dots, x_n) = \prod_{i \in S}(x_d - a_{id}) - \sum_{i \in S}\left[g_i(x_1)(x_d - a_{id}) \left(\prod_{j \in S \setminus \{i\}} (x_d - a_{jd}) + 1 \right) \right].$$

Suppose $f_1 = 0$, that is, $x_1 = a_{k1}$ for some k. Then $g_i(x_1) = 0$ for all $i \neq k$ and $g_k(x_1) = 1$.

Therefore

$$f_d(x_1,\ldots,x_n) = \prod_{i\in S}(x_d - a_{id}) - (x_d - a_{id})\left(\prod_{j\in S\setminus\{i\}}(x_d - a_{jd}) + 1\right) = (x_d - a_{kd}).$$

Thus $X = V(f_1,\ldots,f_n)$. □

1.40. Let $I = (X^2 - Y^3, Y^2 - Z^3) \subset k[X,Y,X]$. Define $\alpha : k[X,Y,Z] \to k[T]$ by $\alpha(X) = T^9$, $\alpha(Y) = T^6$, and $\alpha(Z) = T^4$.

(a) Show that every element of $k[X,Y,Z]/I$ is the residue of an element $A+XB+YC+XYD$, for soem $A, B, C, D \in K[Z]$.

Proof. Observe that $\overline{X}^2 = \overline{Y}^3$ and $\overline{Y}^2 = \overline{Z}^3$. Thus for $n, m \geq 2$ we may write $\overline{X}^n$ and $\overline{Y}^m$ as the residue of a polynomial in $k[Z]$. □

(b) If $F = A + XB + YC + XYD$, $A, B, C, D \in k[Z]$ such that $\alpha(F) = 0$, show $F = 0$.

Proof. We may factor out T's to find $\alpha(F) = \alpha(A)+T^9\alpha(B)+T^6\alpha(C)+T^15\alpha(D)$. Observe $4n = 6 + 4m$ and $9 + 5n = 15 + 4m$ have no integer solutions. Thus it must be that $A = B = C = D = 0$. □

(c) Show that $\ker\alpha = I$, so I is prime, $V(I)$ is irreducible, and $I(V(I)) = I$.

Proof. By (b) we know $\ker\alpha \subset I$. It remains to show $I \subset \ker\alpha$. Observe $\alpha(X^2 - Y^3) = T^{18} - T^{18} = 0$ and $\alpha(Y^2 - Z^3) = T^{12} - T^{12} = 0$. Thus if $F \in I$, $\alpha(F) = 0$, and $F \in \ker\alpha$.

Since $\ker\alpha = I$, by the first isomorphism theorem $k[X,Y,Z]/I \cong \text{Im }\alpha \subset k[T]$. Since $k[T]$ is an integral domain, so is $k[X,Y,Z]/I$; therefore I is prime. Thus $V(I)$ is irreducible and $I(V(I)) = I$. □

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

Proof. Suppose S is module finite over R. Then $S = \{r_1s_1 + \ldots + r_ns_n \mid r_i \in R\}$ for some $s_1,\ldots,s_n \in S$. Thus $s = R[s_1,\ldots,s_n]$. □

1.42. Show $S = R[X]$ is ring-finite over R, but not module finite.

Proof. Clearly $R[X]$ is ring finite by definition. Observe for any finite set $B \subset R[X]$ there exists a polynomial $F \in B$ of maximum degree n. No polynomial in $R[X]$ of degree $n+1$ or more is in the submodule generated by B. □

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

Proof. Suppose $L = K[v_1, \ldots, v_n]$, with $v_1, \ldots, v_n \in L$. Then $L = K(v_1, \ldots, v_n)$ and L is a finitely generated field extension of K. □

1.44.* Show $L = K(X)$ is a finitely generated field extension of K, but is not ring-finite over K.

Proof. It suffices to show L is not ring-finite over K. Suppose $L = K[v_1, \ldots, v_n]$, with $v_1, \ldots, v_n \in L$. Let $b \in K[X]$ be a common denominator for $v_1, \ldots, v_n$. Let $c \in K[X]$ such that $c \not| b$. Then $1/c \in L$, so $1/c = a_1 v_1 + \ldots + a_n v_n$ for some $a_1, \ldots, a_n \in K$. But $b(a_1 v_1 + \ldots + a_n v_n) \in K[X]$, while $b/c \notin K[X]$, a contradiction. □

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 $T = \sum Rv_i w_j$.

Proof. Let $x \in T$. Then $x = \sum_{j=1}^{m} s_j w_j$, each $s_j \in S$. Moreover, $s_j = \sum_{i=1}^{n} r_i v_i$, each $r_i \in R$. Thus $x = \sum Rv_i w_j$. □

(b) If $S = R[v_1, \ldots, v_n]$ and $T = S[w_1, \ldots, w_m]$, then $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.

Proof. Note that if $F \in T$ then $F = G(w_1, \ldots, w_m)$ for some $G \in S[X_1, \ldots, X_n]$. Each coefficient of G is in $S = R[v_1, \ldots, v_n]$. Evaluating we have $F \in R[v_1, \ldots, v_n, w_1, \ldots, w_m]$. The converse follows by factoring. □

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

$$T = R(v_1, \ldots, v_n, w_1, \ldots, w_m).$$

Proof. Let $K = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$. The elements $v_1, \ldots, v_n, w_, \ldots, w_m$ are contained in an extension field L of R. Observe that T is a subfield of L containing $v_1, \ldots, v_n, w_, \ldots, w_m$, thus $K \subset T$.

Clearly $S \subset K$. Moreover, $w_1, \ldots, w_m \in K$. So $T \subset K$. So $T = K$. □

Proposition 3. Let R be a subring of a domain S, $v \in S$. Then the following are equivalent:

1. v is integral over R;
2. $R[v]$ is module finite over R;
3. there is a subring R' of S, $R[v] \subset R'$, such that R' is module finite over R.

We provide a detailed proof of *(3) ⇒ (1)* to clarify Fulton's proof.

Proof. Since R' is module finite over R, $R' = \sum_{i=1}^{n} Rw_i$ for some $w_1, \ldots, w_n \in R'$. For each i observe $w_i v \in R'$, so we may write $w_i v = \sum_{j=1}^{n} a_{i,j} w_j$ for some $a_{i,1}, \ldots, a_{i,n} \in R$. Let F be the field of fractions for S and define $A \in F^{n \times n}$ as

$$A = \begin{bmatrix} v - a_{1,1} & -a_{1,2} & \ldots & -a_{1,n} \\ -a_{2,1} & v - a_{2,2} & \ldots & -a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n,1} & -a_{n,2} & \ldots & v - a_{n,n} \end{bmatrix}$$

Note that v appears only along the diagonal of A, so we may write $\det(A) = v^n + r_{n-1}v^{n-1} + \ldots + r_1 v + r_0$, for some $r_0, \ldots, r_{n-1} \in R$.

Let $w = (w_1, \ldots, w_n) \in F^n$. Then

$$Aw = \left[\sum_{j=1}^{n} (\delta_{i,j} v - a_i) w_j\right]_{i \in \{1,\ldots,n\}}$$

where $\delta_{i,j} = 0$ if $i \neq j$, and $\delta_{i,i} = 1$. Observe

$$\sum_{j=1}^{n} (\delta_{i,j} v - a_i) w_j = w_i v - \sum_{j=1}^{n} a_{i,j} w_j = 0.$$

Since $w \neq 0$, A is nonsingular. Thus

$$v^n + r_{n-1}v^{n-1} + \ldots + r_1 v + r_0 = \det(A) = 0.$$

So v is integral over R. □

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.

Proof. Let $v \in T$. Then there exists $f \in S[X]$ such that $F(v) = 0$. Let $F = X^n +$

$a_{n-1}X^{n-1} + \ldots + a_0,\ a_0, \ldots, a_{n-1} \in S$. Note that $a_0, \ldots, a_{n-1}$ are each integral over R. Thus $R[a_0, \ldots, a_{n-1}]$ is module finite over R by inductively applying problem 1.45(a) and proposition 3. Observe that v is integral over $R[a_0, \ldots, a_{n-1}]$. Therefore by problem 1.45(a) and proposition 3, $R[a_0, \ldots, a_{n-1}][v]$ is module finite over R. Since $R[v] \subset R[a_0, \ldots, a_{n-1}][v]$, v is integral over R by proposition 3. □

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.

Proof. Suppose $S = R[v_1, \ldots, v_n]$ is integral over R. Then by inductively applying problem 1.45(a) and proposition 3 wwe have S module finite over R.

Suppose S is module finite over R. Let $v \in S$. Then $R[v] \subset S$ and v is integral over R by proposition 3. □

1.49.* Let L be a field, and k an algebraically closed subfield of L.

(a) Show that any element of L that is algebraic over k is in k.

Proof. Let $v \in L$ such that $F(v) = 0$ for some nonzero $F \in k[X]$. Since k is algebraically closed, $F(X) = \prod_{i=1}^{n}(X - a_i)$ for $a_1, \ldots, a_n \in k$. Thus $v = a_i$ for some i. □

(b) An algebraically closed field has no module finite field extension other than itself.

Proof. Suppose L is a module finite field extension of k. Let $v \in L$. Since $k[v] \subset L$, v is algebraic over k by Proposition 3. Thus $v \in k$ by part (a). So $L = k$. □

1.49.* Let K be a field, $L = K(X)$.

(a) Show any element of L that is integral over $K[X]$ is already in $K[X]$.

Proof. Suppose $H/G \in K(X)$, with H, G relatively prime, such that

$$\left(\frac{H}{G}\right)^n + F_{n-1}\left(\frac{H}{G}\right)^{n-1} + \ldots + F_0 = 0,$$

where $F_0, \ldots, F_{n-1} \in K[X]$. So

$$H^n + F_{n-1}H^{n-1}G + \ldots + F_0G^n = 0.$$

Therefore

$$H^n = G(-F_{n-1}H^{n-1} - \ldots - F_0G^{n-1})$$

and $G \mid H$. Thus it must be that $G \in K$ and $H/G \in K[X]$. □

(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 $n > 0$.

Proof. By part (a) this would imply that fo each $G \in K[X]$, there exists $n > 0$ such that $F^n/G \in K[X]$. But clearly we may select a nonunit $G \in K[X]$ that is relatively prime to F, a contradiction. □

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.

Proof. By the Corollary of Proposition 3 we have that the set of elements algebraic over K is a ring containing K. Thus it suffices to show if $v \in L$ is algebraic over K then so is v^{-1}.

Suppose $v \in L \setminus \{0\}$ such that $v^n + a_{n-1} + \ldots + a_0 = 0$, with $a_0, \ldots, a_{n-1} \in K$. Observe

$$0 = v^n + a_{n-1} + \ldots + a_0 = v^n \left(1 + \frac{1}{v}a_{n-1} + \ldots + a_0\frac{1}{v^n}\right).$$

Since $v \neq 0$, $v^n \neq 0$, it must be that

$$0 = 1 + \frac{1}{v}a_{n-1} + \ldots + a_0\frac{1}{v^n} = a_0\left(a_0^{-1} + \ldots + (v^{-1})^n\right).$$

So $a_0^{-1} + \ldots + (v^{-1})^n = 0$ and v^{-1} is algebraic over K. □

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

Proof. Let $v \in R \setminus \{0\}$. It suffices to show $v^{-1} \in R$. Since $K[v] \subset R \subset L$ and L is module finite over K, by Proposition 3, v is integral over K. Thus $F(v) = v^n + a_{n-1} + \ldots + a_0 = 0$, with $a_0, \ldots, a_{n-1} \in K$. Suppose $F(X)$ is irreducible, and therefore $a_0 \neq 0$. Then

$$v(v^{n-1} + \ldots + a_1) = -a_0.$$

So

$$v(v^{n-1} + \ldots + a_1)(-a_0^{-1}) = 1.$$

Therefore $v^{-1} = (v^{n-1} + \ldots + a_1)(-a_0^{-1}) \in R$. $\square$

Proposition 4. If a field L is a ring finite over a subfield K, then L is module finite, and hence algebraic over K.

We provide a detailed proof below to clarify Fulton's proof.

Proof. Suppose a field L is ring finite over a subfield K, that is, $L = K[v_1, \ldots, v_n]$ for $v_1, \ldots, v_n \in L$. We proceed by induction on n, the ring dimension of L over K.

Suppose $n = 1$, that is $L = K[v]$. Let us define $\varphi : K[X] \to K[v]$ by $X \mapsto v$. Since $K[X]$ is a PID, $\ker \varphi = (F)$ for some $F \in K[X]$. Since $K[X]/(F) = L$ is a field, (F) is maximal. if $F = 0$, $K[X] \cong K[v] = L$ and therefore $K(X) \cong K[X]$, a contradiction by Problem 1.44. Thus $F \neq 0$ and $F(v) = 0$. So v is algebraic over K and $L = K[v]$ is module finite over K by Proposition 3.

Suppose the proposition holds for all m such that $1 \leq m < n$. Observe that

$$L = K[v_1, \ldots, v_{n+1}] = K(v_{n+1})[v_1, \ldots, v_n].$$

Thus by the inductive hypothesis, L is module finite over $K(v_{n+1})$. It suffices to show v_{n+1} is algebraic over K.

Observe that for each $i \in \{1, \ldots, n\}$ there exists $F_i \in K(v_{n+1})[X]$, with $F_i(X) = X^{m_i} + a_{i,m_i-1}X^{m_i-1} + \ldots + a_{i,0}$, such that $F_i(v_i) = 0$. Observe that there exists $a \in K[v_{n+1}]$ such that $aa_{i,j} \in K[v_{n+1}]$ for all i, j. For each i note that

$$0 = a^{m_i}F_i(v_i) = (av_i)^{m_i} + aa_{i,m_i-1}(av_i)^{m_i-1} + \ldots + a^{m_i}a_{i,0} = G(av_i).$$

By our selection of a, observe that $G \in K[v_{n+1}][X]$. So av_i is integral over $K[v_{n+1}]$ for each i. Therefore $K[av_1, \ldots, av_n, v_{n+1}]$ is integral over $K[v_{n+1}]$. Moreover, for each $z \in L = K[v_1, \ldots, v_{n+1}]$ there exists $m > 0$ such that $a^m z \in K[av_1, \ldots, av_n, v_{n+1}]$. In particular this is true for $K(v_{n+1}) \subset L$.

Suppose v_{n+1} is transcendental over K. Then $K(v_{n+1}) \cong K(X)$. But the existence of a is a contradiction to Problem 1.49(b). Thus v_{n+1} is algebraic over K and L is module finite over K. $\square$

Note. The following "category theoretic" result will be quite usefull in subsequent problems.

Lemma 1.2 (descending to a quotient)**.** Suppose R, S, T are groups (or rings, modules) and $\pi : R \to S$, $\varphi : R \to T$ are group (or ring, module) homomorphisms such that $\ker \pi \subset \ker \varphi$. Then there exists an induced homomorphism $\widetilde{\varphi} : \pi(R) \to T$ such that $\widetilde{\varphi} \circ \pi = \varphi$. Moreover, $\ker \widetilde{\varphi} = \pi(\ker \varphi)$.

Proof. Suppose $a, b \in R$ such that $\pi(a) = \pi(b)$. Then $a - b \in \ker \pi \subset \ker \varphi$. So $a + \ker \varphi = b + \ker \varphi$ and $\varphi(a) = \varphi(b)$. Thus the map $\widetilde{\varphi} : \pi(R) \to T$ defined by $\pi(a) \mapsto \varphi(a)$ is well defined homomorphism. □

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

(a) Show that $L = K[X]/(F)$ is a field, and if x is residue of X in L, then $F(x) = 0$.

Proof. Since $K[X]$ is a PID, (F) is maximal and $K[X]/(F)$ is a field. Let φ be the homomorphism $K[X] \to K[X]/(F)$. Observe that $F(x) = F(\varphi(X)) = \varphi(F(X)) = 0$. □

(b) Suppose L' is a field extension of K, $y \in L'$ such that $F(y) = 0$. Show the homomorphism $\varphi : K[X] \to L'$ defined by $X \mapsto y$ induces an isomorphism $L \to K(y)$.

Proof. Since $F(y) = 0$, $(F) \subset \ker \varphi$. Thus by Lemma 1.2 there exists an induced homomorphism $\widetilde{\varphi} : L \to K(y)$. Now suppose $\ker \varphi \neq (F)$. Then $\ker \varphi = K[X]$ since (F) is maximal, a contradiction. Thus $\ker \varphi = (F)$ and thus $\widetilde{\varphi}$ is an injective homomorphism. Moroever, $\widetilde{\varphi}(L) = \varphi(K[X])$ is a subfield of $K(y)$ containing K and y. So $\widetilde{\varphi}(L) = K(y)$ and $\widetilde{\varphi}$ is an isomorphism. □

(c) With L', y as in (b), suppose $G \in K[X]$ and $G(y) = 0$. Show that F divides G.

Proof. Observe that $G \in \ker \varphi = (F)$. So $F \mid G$. □

(d) Show that $F = (X - x)F_1, F_1 \in L[X]$.

Proof. Observe that $X - x$ is irreducible in $L[X]$ and $F(x) = 0$. By (c), $X - x \mid F$. □

1.52. Let K be a field and $F \in K[X]$. Show there is a field L containing K such that $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$.

Proof. Assume F is monic. Let us proceed by induction on n, the degree of F.

If $n = 1$ then $F = X - x$, $x \in K$.

Suppose the statement is true for all monic polynomials in $K[X]$ of degree less than n. If F is reducible, the statement follows by the inductive hyptothesis. Suppose F is irreducible. Then $L = K[X]/(F)$ is a field. Let x be the image of X in L. Then $F(x) = 0$ in L, so $F = G(X - x)$ for some $G \in L[X]$ of degree less than n. Thus by the inductive hypothesis, there exists an extension field M of L such that the statemenet holds. But since L is an extension field of K, M is also an extension field of K. □

1.53.* Suppose K is a field of characteristic zero, and F is an irreducible 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 the x_i are distinct.

Proof. Suppose some of the x_i's are equal, that is, there exists $x \in L$ such that $(X-x)^m \mid F$ for some $m > 1$. Then $F = (X-x)^m G$ for some $G \in L[X]$. Observe $F_X = m(X-x)^{m-1}G + (X-x)^m G_X$. Since K is of characteristic zero, $F_X \neq 0$. Observe $F_X(X) = 0$. By Problem 1.51(c), this implies $F \mid F_X$, a contradiction since $0 < \deg F_X < \deg F$. □

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 there is a nonzero $a \in R$ such that av is integral over R.

Proof. Let $v \in L$. Then $v^n + a_{n-1}v^{n-1} + \ldots + a_0 = 0$, for $a_i \in K$. Let a be the common denominator of $a_0, \ldots, a_{n-1}$. Then $(av)^n + aa_{n-1}(av)^{n-1} + \ldots + a^n a_0 = 0$. Thus av is integral over R. □

(b) Show that there is a basis $v_1, \ldots, v_n$ or L over K such that each v_i is integral over R.

Proof. Let $w_1, \ldots, w_n$ be a basis for L over K. By (a) there exist $a_1, \ldots, a_n$ such that $a_1w_1, \ldots, a_nw_n$ are all integral over R. Let $v \in L$. Then $v = \sum_{i=1}^{n} b_i w_i$, for $b_i \in K$. So $v = \sum_{i=1}^{n} b_i a_i^{-1}(a_i w_i)$. So $a_1w_1, \ldots, a_nw_n$ spans L and hence is a basis for L over K. □

2 Affine Varieties

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

Proof. Clearly the map is a ring homorphism. Suppose $F \in k[X_1, \ldots, X_n]$ such that F is the zero function in $\mathcal{F}(V, k)$. Then $F(P) = 0$ for all $P \in V$. Thus $F \in I(V)$. Similarly, if $F \in I(V)$ then F is the zero function. □

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

Proof. Recall there is a one to one correspondence between radical, prime, and maximal ideals $J/I(V)$ in $\Gamma(V)$ and radical, prime, and maximal ideals J in $k[X_1, \ldots, X_n]$ such that $I(V) \subset J$. Observe that that W is an algebraic subset, subvariety, or point of V, if and only if $I(W)$ is a radical, prime, or maximal ideal in $k[X_1, \ldots, X_n]$ with $I(V) \subset I(W)$. □

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.

Proof. Suppose $f \in \mathcal{F}(V, k)$ is a polynomial function. Then there exists $F \in k[X_1, \ldots, X_n]$ such that $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in V$. Since $W \subset V$, $f|_W \in \mathcal{F}(W, k)$ is polynomial as well. In terms of coordinate rings, this restriction map defines a homomorphism $\varphi : \Gamma(V) \to \Gamma(W)$ where $\varphi(F + I(V)) = F + I(W)$. □

(b) Show the map $\varphi : \Gamma(V) \to \Gamma(W)$ defined in (a) is surjective with kernel $I_V(W)$, so $\Gamma(W) \cong \Gamma(V)/I_V(W)$.

Proof. Let $\pi_V : k[X_1, \ldots, X_n] \to \Gamma(V)$ and $\pi_W : k[X_1, \ldots, X_n] \to \Gamma(W)$ be the natural homomorphisms. Since π_W, π_V are surjective and $\ker \pi_V \subset \ker \pi_W$, by descending to the quotient (Lemma 1.2) there exists a surjective homomorphism $\widetilde{\pi_W} : \Gamma(V) \to \Gamma(W)$ with $\ker \widetilde{\pi_W} = \pi_W(I(V)) = I_V(W)$. Moreover, $\widetilde{\pi_W}(F + I(V)) = \pi_W(F) = F + I(W) = \varphi(F + I(V))$. So $\widetilde{\pi_W} = \varphi$. □

Note. The proofs of the theorems below heavily use the standard isomorphism theorems for modules.

Lemma 2.1. If N is a submodule of a finitely generated R-module M, then M/N is finitely generated.

Proof. Let $\{s_1, \ldots, s_n\}$ be a generating set for M. Then $\{s_1 + N, \ldots, s_n + N\}$ generates M/N. □

Lemma 2.2. Suppose N is a submodule of an R-module M and $N, M/N$ are finitely generated over R. Then M is finitely generated over R.

Proof. Let $N = \sum Ra_i$, $M/N = \sum R(b_i + N)$. We will show that $M = \sum Ra_i + \sum Rb_i$. If $x \in M$ then clearly $x + N \in M/N$. Therefore $x + N = \sum_{i=1}^{m} r_i b_i + N$ for some $r_i \in R$. Therefore $x - \sum_{i=1}^{m} r_i b_i = y \in N$. Moreover, $y = \sum_{i=1}^{n} s_i a_i$ for some $s_i \in R$. Therefore $x = \sum_{i=1}^{m} r_i b_i + \sum_{i=1}^{n} s_i a_i$. □

Definition 2.3. A module is Noetherian if every submodule is finitely generated.

Lemma 2.4. Suppose N is a submodule of an R-module M. Then M is Noetherian if and only if $N, M/N$ are Noetherian. Equivalently if N, M, P are R-modules and

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

is exact, then M is Noetherian if and only if N, P are Noetherian.

Proof. Suppose M is Noetherian. Then N is clearly Noetherian since submodules of N are submodules of M. Moreover, any submodule L of M/N is R-module isomorphic to L'/N, where L' is some submodule of M containing N. Since L' is finitely generated, L is finitely generated by Lemma 2.1. Hence M/N is Noetherian as well.

Suppose conversely that $N, M/N$ are Noetherian. Let L be a submodule of M. Then $L \cap N$ is a submodule of N and hence is finitely generated. Moreover, $L/(L \cap N)$ is isomorphic to $(L + N)/N$. Since $(L + N)/N$ is a submodule of M/N, $(L + N)/N$ is finitely generated. Thus $L \cap N$ and $L/(L \cap N)$ are both finitely generated, and hence L is finitely generated by Lemma 2.2.

The result may be reinterpreted in terms of the exact sequence above by noting that P is R-module isomorphic to M/N. □

Lemma 2.5. If R is a Noetherian ring, then R^n is Noetherian as an R-module for all $n \geq 1$.

Proof. If $n = 1$ then R is Noetherian as an R-modules since it is a Noetherian ring (the R-submodules of R are precisely the ideals of R).

Suppose that R^n is a Noetherian R-module for some $n \geq 1$. Observe that R^{n+1}/R is R-module isomorphic to R^n, where R is identified with the $(n+1)$th copy of R in R^{n+1}. Since R^n, R are each Noetherian R-modules, R^{n+1} is Noetherian by Lemma 2.4. □

Lemma 2.6. If R is a Noetherian ring and M is an R-module, M is Noetherian if and only if it is finitely generated over R.

Proof. If M is Noetherian, then it is finitely generated by definition. Suppose M is generated by the finite set $\{s_1, \ldots, s_n\}$. Note that there exists a natural surjective R-module homomorphism $\varphi : R^n \to M$ mapping 1 in the kth copy of R to s_k. Thus M is R-module isomorphic to $R^n/\ker\varphi$. By Lemma 2.5, R^n is Noetherian. Hence M is Noetherian by Lemma 2.4. □

Lemma 2.7. Let K be a field and $R \supset K$ an integral domain. Let L be the field of fractions of R. Then R is module finite over K if and only if L is a finite field extension of K.

Proof. Suppose R is module finite over K and $\{v_1, \ldots, v_n\}$ a basis for R. Note that since R is module finite over K, $v_1, \ldots, v_n$ are each algebraic over K. So $K(v_1, \ldots, v_n)$ is a finite extension of K. Since $R \subset K(v_1, \ldots, v_n)$, $L \subset K(v_1, \ldots, v_n)$. Thus L is a finite extension of K.

Suppose L is a finite extension of K. Since fields are Noetherian, L is Noetherian as a K-module by Lemma 2.6. Thus since $K \subset R \subset L$, R is a finitely generated K-module. □

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

1. V is a point;
2. $\Gamma(V) = k$;
3. $\dim_k \Gamma(V) < \infty$.

Proof. (1) ⇔ (2). Suppose $V = \{(a_1, \ldots, a_n)\} \subset \mathbb{A}^n$. Then $I(V) = (X_1 - a_1, \ldots, X_n - a_n)$. Therefore $\Gamma(V) = k$. Conversely, suppose $\Gamma(V) = k$. Then $I(V)$ is maximal. Since k is algebraically closed, $I(V) = (X - a_1, \ldots, X - a_n)$. Thus V is a point.

(2) ⇔ (3). Clearly if $\Gamma(V) = k$, then $\dim_k \Gamma(V) = 1$. Conversely, suppose $\dim_k \Gamma(V) < \infty$. Let L be the field of fractions for $\Gamma(V)$. By Lemma 2.7, L is finite field extension of k. Since k is algebraically closed, by Problem 1.48, $L = k$. Thus $\Gamma(V) = L = k$. □

2.5. Let F be an irreducible polynomial in $k[X,Y]$, and suppose F is monic in Y: $F = Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X)$, with $n > 0$. Let $V = V(F) \subset \mathbb{A}^2$. Show that the natural homomorphism from $k[X]$ to $\Gamma(V) = k[X,Y]/I(F)$ 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.

Proof. Observe that if $n = 0$, then $F(X,Y) = 1$ is constant, $(F) = k[X,Y]$, and $k[X,Y]/(F)$ is the trivial ring. Thus suppose $n \geq 1$.

Note that the natural homomorphism $k[X] \to \Gamma(V)$ maps $G \mapsto G + (F)$. Suppose $G, H \in k[X]$ such that $H + (F) = G + (F)$, that is, $H - G \in (F)$. Observe that $F \nmid H - G$, since $n \geq 1$, so $G - H = 0$ and $G = H$. So the map is one-to-one.

Let $G + (F) \in \Gamma(V)$. Observe we have $Y^n + (F) = -a_1(X)Y^{n-1} - \ldots - a_0(X) + (F)$. Hence for any $m > 0$, $Y^m + (F) = \sum_{i=0}^{n-1} b_{m,i}(X)Y^i$ for some $b_{m,i} \in k[X]$. Thus $\overline{1}, \overline{Y}, \ldots, \overline{Y}^{n-1}$ generate $\Gamma(V)$ over $k[X]$ as a module. □

Bonus problem 2.a. Show the map $\widetilde{\varphi} : \mathcal{F}(W,k) \to \mathcal{F}(V,k)$ is a homomorphism.

Proof. Observe that for any $f, g \in \mathcal{F}(W,k)$ and any $x \in W$,

$$\begin{aligned}((f+g) \circ \varphi)(x) &= f(\varphi(x)) + g(\varphi(x)) \\ &= (f \circ \varphi)(x) + (g \circ \varphi)(x) \\ &= ((f \circ \varphi) + (g \circ \varphi))(x).\end{aligned}$$

Therefore $\widetilde{\varphi}(f+g) = \widetilde{\varphi}(f) + \widetilde{\varphi}(g)$. Similarly, $\widetilde{\varphi}(fg) = \widetilde{\varphi}(f)\widetilde{\varphi}(g)$. □

Bonus problem 2.b. If $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ determine a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, the T_i are uniquely determined by T.

Proof. Suppose $F \in k[X_1, \ldots, X_n]$ such that $F(P) = T_i(P)$ for all $P \in \mathbb{A}^n$. Then $(F - T_i)(P) = 0$ for all $P \in \mathbb{A}^n$. So $F = T_i$ by Problem 1.4. □

Bonus problem 2.c. Let $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ be a varieties. Let $\varphi : V \to W$ be a polynomial map. Then $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$ is a homomorphism. Moreover, $F + I(W) \mapsto F \circ \varphi + I(V)$.

Proof. Suppose φ is defined by the polynomials $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$. For any polynomial $F \in k[X_1, \ldots, X_m]$, $\widetilde{\varphi}(F) = F \circ \varphi = F(T_1, \ldots, T_m)$ is a polynomial in $k[X_1, \ldots, X_n]$.

We will now show that $\widetilde{\varphi}$ induces a well defined homomorphism $\Gamma(W) \to \Gamma(V)$, that is, if $F + I(W), G + I(W) \in \Gamma(W)$ then $\widetilde{\varphi}(F) + I(V) = \widetilde{\varphi}(G) + I(V)$. Let $H \in I(W)$. Observe that $(H \circ \varphi)(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$. Thus $\widetilde{\varphi}(H) \in I(V)$. Thus, by Problem 2.a, the map is a well defined homomorphism.

Although a slight abuse of notation, we use $\widetilde{\varphi}$ to refer to the homomorphism $\Gamma(W) \to \Gamma(V)$ induced by $\widetilde{\varphi}$. This falls in line with the dual use of $\Gamma(V)$ as both the ring $k[X_1, \ldots, X_n]/I(V)$ and the set of all polynomial maps in $\mathcal{F}(V, k)$. □

Note. Recall that Fulton assumes all homomorphisms fix the field k. That is, the following statement is a bijection between polynomial maps and homomorphisms of coordinate rings that fix k.

Proposition 1. Let $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ be affine varieties. There is a one-to-one correspondence between the polynomial maps $\varphi : V \to W$ and the homomorphisms $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$. Any such φ is the restriction of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$.

Proof. By Problem 2.c, each polynomial map $V \to W$ induces a homomorphism $\Gamma(W) \to \Gamma(V)$. Moreover, any polynomial map $V \to W$ is the restriciton of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$. Thus it remains to prove the converse.

Let $\alpha : \Gamma(W) \to \Gamma(V)$ be a homomorphism. For each $i \in \{1, \ldots, m\}$ select $T_i \in k[X_1, \ldots, X_n]$ such that $T_i + I(V) = \alpha(X_i + I(W))$. Let $T : \mathbb{A}^n \to \mathbb{A}^m$ be the polynomial map defined by $(T_1, \ldots, T_m)$. Let $\widetilde{T} : k[X_1, \ldots, X_m] \to k[X_1, \ldots, X_n]$ be the homomorphism defined by $F \mapsto F \circ T$. Let $\pi_V : k[X_1, \ldots, X_n] \to \Gamma(V)$ and $\pi_W : k[X_1, \ldots, X_m] \to \Gamma(W)$ be the natural homomorphisms.

$$\begin{array}{ccc} k[X_1, \ldots, X_m] & \xrightarrow{\widetilde{T}} & k[X_1, \ldots, X_n] \\ \downarrow{\scriptstyle \pi_W} & & \downarrow{\scriptstyle \pi_V} \\ \Gamma(W) & \xrightarrow{\quad\alpha\quad} & \Gamma(V) \end{array}$$

Observe that

$$\begin{aligned} \pi_V(\widetilde{T}(F)) &= \pi_V(F(T_1, \ldots, T_m)) \\ &= F(T_1, \ldots, T_m) + I(V) \\ &= F(\alpha(X_1 + I(W)), \ldots, \alpha(X_m + I(W))) + I(V) \\ &= \alpha(F + I(W)) \\ &= \alpha(\pi_W(F)). \end{aligned}$$

Thus the diagram above commutes. In particular, $\pi_V(\widetilde{T}(I(W))) = \alpha(\pi_W(I(W))) = 0 + I(V)$. Thus $\widetilde{T}(I(W)) \subset I(V)$.

Let $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Suppose $F \in I(W)$. Then $F(T(a_1, \ldots, a_n)) = \widetilde{T}(F)(a_1, \ldots, a_n) = 0$, since $\widetilde{T}(F) \in I(V)$. Thus $T(a_1, \ldots, a_n) \in W$.

Observe that $\widetilde{T|_V}$ is the same as the homomorphism resulting from applying Lemma 1.2 to π_W and $\pi_V \circ \widetilde{T}$. Thus $T|_V : V \to W$ is a polynomial map such that $\widetilde{T|_V} = \alpha$. □

Corollary. Let V, W be affine varieties. Then V is isomorphic to W if and only if $\Gamma(V)$ is isomorphic to $\Gamma(W)$.

Proof. Suppose $V \cong W$, that is, there exist polynomial maps $\varphi : V \to W$ and $\psi : W \to V$ such that $\psi \circ \varphi = \mathrm{id}_V$ and $\varphi \circ \psi = \mathrm{id}_W$. Note that $\mathrm{id}_{\Gamma(V)} = \widetilde{\mathrm{id}_V} = \widetilde{\psi \circ \varphi}$. Thus by Problem 2.6, $\mathrm{id}_{\Gamma(V)} = \widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$. Similarly, $\mathrm{id}_{\Gamma(W)} = \widetilde{\psi} \circ \widetilde{\varphi}$. Thus $\widetilde{\varphi}, \widetilde{\psi}$ are isomorphisms and $\Gamma(V) \cong \Gamma(W)$.

Conversely, suppose $\Gamma(V) \cong \Gamma(W)$, that is, there exist isomorphisms $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$ and $\widetilde{\psi} : \Gamma(V) \to \Gamma(W)$ such that $\widetilde{\varphi} \circ \widetilde{\psi} = \mathrm{id}_{\Gamma(V)}$ and $\widetilde{\psi} \circ \widetilde{\varphi} = \mathrm{id}_{\Gamma(W)}$. By Proposition 1, $\widetilde{\varphi}, \widetilde{\psi}$ are induced by some polynomial maps $\varphi : V \to W$ and $\psi : W \to V$. Since $\widetilde{\varphi} \circ \widetilde{\psi} = \mathrm{id}_{\Gamma(V)}$, $F \circ (\psi \circ \varphi) + I(V) = F + I(V)$ for any $F + I(V) \in \Gamma(V)$. In particular, this is true for $\sum_{i=1}^n X_i + I(V)$. Thus $(\psi \circ \varphi)(a_1, \ldots, a_n) = (a_1, \ldots, a_n) + F(a_1, \ldots, a_n)$ for some $F \in I(V)$. Thus $(\psi \circ \varphi)(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$ for every $(a_1, \ldots, a_n) \in V$. So $\psi \circ \varphi = \mathrm{id}_V$. A similar argument shows $\varphi \circ \psi = \mathrm{id}_W$, and therefore $V \cong W$. □

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 a polynomial map is a polynomial map.

Proof. Let $\varphi : V \to W$, $\psi : W \to Z$. Let $f \in \mathcal{F}(Z, k)$. Observe that

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

Therefore $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$. It is simple to verify that composing polynomial maps results in a polynomial map. □

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

Proof. Observe that if $P \in \varphi^{-1}(X)$ then $\varphi(P) \in X$. Thus $F(\varphi(P)) = 0$ for all $F \in I(X)$. Moreover, if $F(\varphi(P)) = 0$, then $\varphi(P) \in X$, and $P \in \varphi^{-1}(X)$. So $\varphi^{-1}(X) = V(\widetilde{\varphi}(I(X)))$.

Suppose that $\varphi^{-1}(X)$ is irreducible and $X \subset \varphi(V)$. Suppose that $I_W(X)$ is not prime, that is, there exist $f, g \in \Gamma(W) \setminus I_W(X)$ such that $fg \in I_W(X)$. Since $f, g \notin I_W(X)$ there exist $P, Q \in X$ such that $f(P) \neq 0$, $g(Q) \neq 0$. Since $X \subset \varphi(V)$, there exist $P', Q' \in \varphi^{-1}(V)$ such that $\varphi(P') = P$, $\varphi(Q') = Q$. Therefore $(f \circ \varphi)(P') = f(P) \neq 0$ and $\widetilde{\varphi}(f) \notin I_V(\varphi^{-1}(X))$. Similarly, $\widetilde{\varphi}(g) \notin I_V(\varphi^{-1}(X))$. But, $\widetilde{\varphi}(f)\widetilde{\varphi}(g) = \widetilde{\varphi}(fg) \in I_V(\varphi^{-1}(X))$. So $I_V(\varphi^{-1}(X))$ is not prime, a contradiction to the assumption that $\varphi^{-1}(X)$ is irreducible. □

2.8. (a) Show that $\{t, t^2, t^3\} \subset \mathbb{A}^3(k)\}$ is an affine variety.

Proof. Let $\varphi : \mathbb{A}^1(k) \to \mathbb{A}^3(k)$ be defined by $t \mapsto (t, t^2, t^3)$. Observe φ is a polynomial map. Let $V = V(X - Y^2, X - Z^3) = \{(t, t^2, t^3) \in \mathbb{A}^3(k)\}$. Note that $\varphi(\mathbb{A}^1(k)) = V$ and $\varphi^{-1}(V) = \mathbb{A}^1(k)$. Recall $\mathbb{A}^1(k)$ is irreducible by Problem 1.29. Therefore V is irreducible by Problem 2.7. □

(b) Show that $V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subset \mathbb{A}^3(\mathbb{C})$ is a variety.

Proof. Let $V = V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$. It is simple to compute that $Y^3 - X^4, Z^3 - X^5, z^4 - Y^5 \in I(V)$. Suppose $(a, b, c) \in V$. Then $b^3 = a^4$, that is, $b = t^4$ whenever t is a third root of a in $\mathbb{C}$. Similalry, $c = s^5$ where s is a third root of a. Since $c^4 = b^5$ we have $s^{20} = t^{20}$. But $t^3 = a = s^3$. Thus $t(s^{20}) = t(t^{20}) = (t^3)^7 = (s^3)^7 = s(s^{20})$. So $t = s$ and $(a, b, c) = (t^3, t^4, t^5)$. Moreover, for any $t \in \mathbb{C}$, observe that $(t^3, t^4, t^5) \in V$. Let $\varphi : \mathbb{A}^1(\mathbb{C}) \to \mathbb{A}^3(\mathbb{C})$ be the polynomial map defined by $t \mapsto (t^3, t^4, t^5)$. Then $V = \varphi(\mathbb{A}^1(\mathbb{C}))$ and thus V is irreducible by Problem 2.7. □

2.9.* Let $\varphi : V \to W$ be a polynomial map of affine varieties, and let $V' \subset V$, $W' \subset W$ be subvarieites. Suppose $\varphi(V') \subset W'$.

(a) Show that $\widetilde{\varphi}(I_W(W')) \subset I_V(V')$.

Proof. Suppose $f \in I_W(W')$. Then $f(P) = 0$ for all $P \in \varphi(V') \subset W'$. Thus $\widetilde{\varphi}(f) \in I_V(V')$. □

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

Proof. The restriction of any polynomial map is a polynomial map by the proof of Proposition 1. Thus since $\varphi(V') \subset W'$, $\varphi|_{V'}$ is a polynomial map $V' \to W'$. □

2.10.* Show that the projection map $\mathbb{A}^n \to \mathbb{A}^r$ with $n \geq r$ is a polynomial map.

Proof. The projection map is defined by the polynomials $T_i = X_i$. □

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

$$(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n, f(a_1, \ldots, a_n))$$

defines an isomorphism of V with $G(f)$.

Proof. Let $\varphi : \mathbb{A}^n \to G(f)$ be the map defined above. It is immediate that ϕ is a bijection with inverse $\pi|_{G(f)}$, where $\pi : \mathbb{A}^{n+1} \to \mathbb{A}^n$ is the projection map. Since both are polynomial maps, φ is an isomorphism. □

2.12. (a) $\varphi : \mathbb{A}^1 \to V = V(Y^2 - X^3) \subset \mathbb{A}^2$ 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.

Proof. Observe if $(a, b) \in V$ the $a^3 = b^2$. Since k is algebraically closed, there exists $t \in k$ such that $t^2 = a$. So $b^2 = t^6$ and $b = \pm t^3$. Thus either $\varphi(t) = (a, b)$ or $\varphi(-t) = (a, b)$. So φ is onto.

Suppose $t, s \in \mathbb{A}^1$ such that $\varphi(t) = \varphi(s)$. Then $t^2 = s^2$ and $t^3 = s^3$. Thus $t(t^2) = s(s^2) = s(t^2)$, and $t = s$. Therefore φ is one-to-one.

It remains to show that φ is not an isomorphism, that is, its inverse is not a polynomial map. Observe that $\widetilde{\varphi}(f) = f(T^2, t^3)$ for every $f \in \Gamma(V)$. Therefore $\widetilde{\varphi}(\Gamma(V)) \subset (T^2, T^3) \subsetneq k[T] = \Gamma(\mathbb{A}^1)$. Thus $\widetilde{\varphi} : \Gamma(V) \to \Gamma(\mathbb{A}^1)$ is not an isomorphism. Hence φ is not an isomorphism by Proposition 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 $\varphi(\pm 1) = (0, 0)$.

Proof. Let $(a, b) \in V$. Then $b^2 = a^2(a+1)$. Let $t \in k$ such that $t^2 = a+1$. Then $a = t^2 - 1$, $b = (t^2-1)t$. Therefore $\varphi(t) = (a, b)$. So φ is onto.

Suppose $t, s \in k$ such that $\varphi(t) = \varphi(s)$. Then $(t^2-1) = (s^2-1)$. Moreover, $(t^2-1)t = (s^2-1)s$. If $t^2 - 1 \neq 0$, then $t = s$. If $t^2 - 1 = 0$, then $t = \pm 1$, $s = \pm 1$. Therefore φ is one-to-one and onto, except that $\varphi(\pm 1) = (0, 0)$. □

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

Proof. Let $f : \mathbb{A}^1 \to \mathbb{A}^3$ be the polynomial map (T^9, T^6, T^3). Observe that $f(\mathbb{A}^1) \subset V$ so $f : \mathbb{A}^1 \to V$ is a polyomal map such that $\widetilde{f} = \overline{\alpha}$. □

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

Proof. First note that f is clearly one-to-one. Suppose $(a, b, c) \in V$. Let $t \in k$ such that $t^4 = c$. Then $b^2 = c^3 = t^{12}$, so $b = \pm t^6$. Moreover, $a^2 = b^3 = \pm t^{18}$, so $a = \pm t^9$, or $\pm t^9\sqrt{-1}$. Therefore (a, b, c) is either $(\pm t^9, t^6, t^4)$, or $(\pm t^9\sqrt{-1}, -t^6, t^4)$. Thus (a, b, c) is equal to either $f(\pm t)$ or $f(\pm t\sqrt{-1})$. So f is onto.

It remains to show that f is not an isomorphism. By Proposition 1 it suffices to observe that $\widetilde{f}$ is not an isomorphism, since $\widetilde{f}(\Gamma(V)) \subset (T^9, T^6, T^4) \subsetneq k[T] = \Gamma(\mathbb{A}^1)$. □

Lemma 2.8. Let $F \in k[X_1, \ldots, X_n]$ be a polynomial of degree 1. Then there exists an affine change of coordinates $T : \mathbb{A}^n \to \mathbb{A}^n$ such that $F^T = X_m$.

Proof. Suppose that $F = \sum_{i=1}^n a_i X_i + a_0$ with $a_1, \ldots, a_n \in k \setminus \{0\}$. We will define an affine change of coordinates $T = T' \circ T''$ with T' a linear map and T'' a translation. Let $T_i'' = X_i$ for $i \neq n$ and $T_n'' = X_n - a_0$. Define T' by setting $T_i' = X_i$ for $i < d$, $T_d' = a_d^{-1} X_d$, and $T_i' = a_i^{-1} X_i - a_i^{-1} X_{i-1}$ for $i > d$. Observe that T' is defined by the following matrix in $k^{n \times n}$,

$$T' = \begin{bmatrix} 1 & 0 & 0 & \ldots & \ldots & 0 \\ 0 & a_1^{-1} & 0 & \ldots & \ldots & 0 \\ 0 & -a_2^{-1} & a_2^{-1} & \ldots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & -a_{n-1}^{-1} & a_{n-1}^{-1} & 0 \\ 0 & \ldots & \ldots & 0 & -a_n^{-1} & a_n^{-1} \end{bmatrix}$$

Note that T' is upper triangular, and therefore invertible. So $T = T' \circ T''$ is an affine change of coordinates. Observe that

$$\begin{aligned} F^T &= \left(\sum_{i=1}^{n} a_i(T_i)\right) + a_0 \\ &= \left(\sum_{i=1}^{n-1} a_i(T_i'(X_i)\right) + a_n(T_n'(X_n - a_0) + a_0 \\ &= a_1(a_1^{-1}X_1) + \left(\sum_{i=2}^{n-1} a_i(a_i^{-1}X_i - a_i^{-1}X_{i-1})\right) + a_n(a_n^{-1}(X_n - a_0) - a_n^{-1}X_{n-1}) + a_0 \\ &= X_n. \end{aligned}$$

□

2.14.* A set $V \subset \mathbb{A}^n(k)$ 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 $\mathbb{A}^n$ the V^T is also a linear subvariety of $\mathbb{A}^n$.

Proof. Let $T = (T_1, \ldots, T_n)$ be an affine change of coordinates, and $V = V(F_1, \ldots, F_r)$ a linear subvariety of $\mathbb{A}^n$. Then $I(V) = (F_1, \ldots, F_r)$, since $F_1, \ldots, F_r$ are of degree 1. Note that $F_1^T, \ldots, F_r^T$ are also degree 1. So $I(V)^T = (F_1^T, \ldots, F_r^T)$. therefore $V^T = V(I(V)^T) = V(F_1^T, \ldots, F_r^T)$. □

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

Proof. Suppose $r = 1$, that is, $V = V(F)$. Let $F = \sum_{i=1}^n a_i X_i + a_0$. Let T' be an affine change of coordinates relabeling varables such that $F^U = \sum_{i=d+1}^n a_i X_i + a_0$ with $a_{d+1}, \ldots, a_n \in k \setminus \{0\}$. By Lemma 2.8 there exists an affine change of coordinates U on $\mathbb{A}^{n-d}$, defined by polynomials $U_d, \ldots, U_n \in k[X_d, \ldots, X_n]$ such that $(F^{T'})^U = X_n$. Let T'' be the affine change of coordinates defined by $T_i = X_i$ if $i < d$ and $T_i = U_i$ if $i \geq d$. Let I_d be the $d \times d$ identity matrix and observe that T'' is represented by the following upper triangular matrix

$$T'' = \begin{bmatrix} I_d & 0 \\ 0 & U \end{bmatrix}$$

Thus T'' is invertible and $T = T'' \circ T'$ is an affine change of coordinates such that $F^T = X_n$. Thus $V^T = V(X_n)$.

Let $r \geq 1$. Suppose for any $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ there exists affine change of coordinates T such that $V(F_1, \ldots, F_r)^T = V(X_{m+1}, \ldots, X_n)$ for some $m \geq 0$. Let $F_1, \ldots, F_{r+1} \in k[X_1, \ldots, X_n]$ and $V = V(F_1, \ldots, F_{r+1})$. By the inductive hypothesis there exists affine change of coordinates T' such that $V(F_1, \ldots, F_r)^T = V(X_{m+1}, \ldots, X_n)$. Therefore $V^{T'} = V(F_{r+1}^{T'}, X_{m+1}, \ldots, X_n)$. If $F_{r+1}^{T'} \in (X_{m+1}, \ldots, X_n)$ we are done. Otherwise, let us select $G \in k[X_1, \ldots, X_m]$ such that

$$F_{r+1}^{T'} + (X_{m+1}, \ldots, X_n) = G + (X_{m+1}, \ldots, X_n).$$

Then $V^{T'} = V(G, X_{m+1}, \ldots, X_n)$. By the same method as the base case, we may construct an affine change of coordinates T'' on $\mathbb{A}^n$, such that $G^{T''} = X_m$ and $X_i^{T''} = X_i$ for all $i > m$. Thus if we define $T = T'' \circ T'$, then $V^T = V(X_m, \ldots, X_n)$. □

(c) Show that the m appearing in part (b) is independent of the choice of T. Thus V is isomorphic to $\mathbb{A}^m(k)$.

Proof. Suppose there exist change of coordinates T, U such that $V^T = V(X_{m+1}, \ldots, X_n)$ and $V^U = V(X_{d+1}, \ldots, X_n)$. Observe that $T|_{V^T} : V^T \to V$ and $U|_{V^U} : V^U \to V$ are each isomorphisms. So

$$k[X_1, \ldots, X_m] \cong \Gamma(V^T) \cong \Gamma(V) \cong \Gamma(V^U) \cong k[X_1, \ldots, X_d].$$

Therefore $m = d$. Moreover, $\Gamma(\mathbb{A}^m) \cong k[X_1, \ldots, X_m] \cong \Gamma(V)$. □

Lemma 2.9. Let T be an affine change of coordinates on $\mathbb{A}^n$ and $S \subset k[X_1, \ldots, X_n]$. If $I(S) \neq I(S \setminus \{F_i\})$ for some $i \in \{1, \ldots, r\}$, then $I(S)^T \neq I(S \setminus \{F_i\})^T$.

Proof. Suppose $G \in I(S)$. Observe that if $\widetilde{T}(G) \in I(S \setminus \{F_i\})^T$, then $\widetilde{T}^{-1}(\widetilde{T}(G)) = G \in I(S \setminus \{F_i\})$. □

Definition 2.10. Let R be a ring, $A \subset R$, and $I = I(A)$. We say A is a *minimal generating set* for I if for all $B \subset I$ such that $I = I(B)$, $|B| \geq |A|$.

Lemma 2.11. Suppose $V = V(F_1, \ldots, F_r)$ is a linear subvariety of $\mathbb{A}^n$. If $\{F_1, \ldots, F_r\}$ is a minimal generating set for $I(V)$, then V has dimension $n - r$.

Proof. By Problem 2.14 there exists an affine change of coordinates T on $\mathbb{A}^n$ such that $V^T = V(X_{m+1}, \ldots, X_n)$. Also, $V^T = V(I(V)^T) = V(F_1^T, \ldots, F_r^T)$. Since $\{F_1, \ldots, F_r\}$ is a

minamal generating set for $I(V)$, by Lemma 2.9, $\{F_1^T, \ldots, F_r^T\}$ is a minimal generating set for $I(V)^T$. Therefore $n - (m+1) + 1 = r$ and $m = n - r$. □

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

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

Proof. Let $T_i = \sum_{j=1}^n c_{i,j} X_i + c_{i,0}$. Note that $T_i(P) = \sum_{j=1}^n c_{i,j} a_j + c_{i,0}$ and $T_i(Q) = \sum_{j=1}^n c_{i,j} b_j + c_{i,0}$. Let M be the line between $T(P)$ and $T(Q)$. Let $t \in k$. Let

$$O = \left(\sum_{j=1}^n c_{1,j}(a_j + t(b_j - a_j) + c_{1,0}, \ldots, \sum_{j=1}^n c_{n,j}(a_j + t(b_j - a_j) + c_{n,0} \right) \in M$$

Let $O' = (a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) \in L$. Observe $T(O') = O$ and thus T is a bijection between L and $T(L) = M$. □

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

Proof. Let L be the line between P and Q defined above. Observe that $(X_1, \ldots, X_n) \in L$ if and only if there exists $t \in k$ such that $X_i = a_i + t(b_i - a_i)$ every i. Since P, Q are distinct points, there must exist $i \in \{1, \ldots, n\}$ such that $a_i \neq b_i$. Therefore we may solve for t and find $t = \frac{X_i}{b_i - a_i} - \frac{a_i}{b_i - a_i}$. So $(X_1, \ldots, X_n) \in L$ if and only if $F_j = (b_i - a_i)(X_j - a_j) - (b_j - a_j)(X_i - a_i) = 0$ for all $j \neq i$. Therefore $L = V(\{F_j \mid j \in \{1, \ldots, n\} \setminus \{i\}\})$. Thus L is a linear subvariety of $\mathbb{A}^n$. Observe that $\{F_j \mid j \in \{1, \ldots, n\} \setminus \{i\}\}$ is a minimal generating set (Definition 2.10) for $I(L)$. Therefore, by Lemma 2.11, L has dimension 1.

Suppose V is a linear subvariety of dimension 1. Then there exists an affine change of coordinates T such that $V^T = V(X_2, \ldots, X_n)$. Note that V^T is the line between $P = (0, 0, \ldots, 0)$ and $Q = (1, 0, \ldots, 0)$. Thus, by part (a), $T(V^T) = V$ is the line between $T(P)$ and $T(Q)$. □

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

Proof. By Lemma 2.11, in $\mathbb{A}^2$ a variety has dimension 1 if and only if it is a hyperplane. Thus, by part (b), 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 $T(L_i) = L_i'$, $i = 1, 2$.

Proof. Let $U_P, U_{P'}$ be the translations sending P, P' to the origin. Let v_1, v_2 be unit vectors along $U_P(L_1), U_P(L_2)$. Similarly let u_1, u_2 be unit vectors along $U_{P'}(L_1'), U_{P'}(L_2')$. Note that $\{v_1, v_2\}$ and $\{u_1, u_2\}$ are each a basis for $\mathbb{A}^2$. Let T' be the linear map defined by $v_i \mapsto u_i$. Then $T = U_{P'}^{-1} \circ T' \circ U_P$ is an affine change of coordinates such that $T(P) = P'$ and $T(L_i) = L_i'$, $i = 1, 2$. □

Lemma 2.12. Let V ba an algebraic set in $\mathbb{A}^n$, and L a linear subvariety of dimension 1. Then either $L \subset V$ or $V \cap L$ is finite.

Proof. Suppose $L = V(X_2, \ldots, X_n)$. Let $F \in I(V)$. Note that $V \subset V(F)$. Observe that the set $V(F) \cap L$ is the set of solutions to $F(X_1, 0, \ldots, 0)$, a polynomial of one variable. Thus either $F(X_1, 0, \ldots, 0) = 0$ and $F \in I(L)$, or $V(F) \cap L$ is finite.

Suppose L is any linear subvariety of dimension 1. By 2.14(b), there exists an affine change of coordinates T such that $L^T = V(X_2, \ldots, X_n)$. So by the result above, either $L^T \subset V^T$ or $V^T \cap L^T$ is finite. Thus $L \subset V$ or $V \cap L$ is finite. □

Note. The lemma above also has a proof using Corollary 4 of the Nullstellensatz, by showing that $k[X_1, \ldots, X_n]/I(V \cap L)$ is a finite dimensional vector space over k.

2.16. Give $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ the usual topology.

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

Proof. Let $P, Q \in \mathbb{C}^n \setminus S$ be distinct points. Let R be the set of all points on lines between P or Q and a point in S, lines in $\mathbb{R}^{2n}$, not dimension 1 linear subvarieties of $\mathbb{A}^n(\mathbb{C})$. Since S is finite, $R \neq \mathbb{C}^n$. Therefore we may pick a point $O \in \mathbb{C}^n \setminus R$. Observe that neither the line segment from P to O nor the line segment from O to Q contain a point in S. Thus there is a path from P to Q in $\mathbb{C}^n \setminus S$. □

(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.

Proof. If $V = \mathbb{A}^n(\mathbb{C})$ then $\mathbb{A}^n(\mathbb{C}) \setminus V = \emptyset$ and is therefore path connected. Suppose $V \subsetneq \mathbb{A}^n(\mathbb{C})$. Let $P, Q \in \mathbb{A}^n(\mathbb{C}) \setminus V$, $P \neq Q$, and let L be the line between P and Q, in the sense of linear subvariety of dimension 1. By Lemma 2.12, $V \cap L$ is finite. Moreover, L is isomorphic to $\mathbb{A}^1(\mathbb{C})$. Note that polynomial maps are continuous with respect to the topology on $\mathbb{C}^n$,

so L is in fact homeomorphic to $\mathbb{A}^1(C)$. Therefore $L \setminus V$ is homeomorphic to $\mathbb{C}$ with a finite set removed. Thus $L \setminus V$ is path connected by part (a). Therefore $\mathbb{A}^n(\mathbb{C}) \setminus V$ is path connected. □

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 $z = \overline{X}/\overline{Y} \in k(V)$. Find the pole sets of z and z^2.

The pole set of z is $\{(0,0)\}$.

Proof. First observe that $z = \overline{Y}/\overline{X} = \overline{Y}/^2\overline{XY} = \overline{X(X+1)}/\overline{Y}$. Therefore z is clearly defined at all points (x, y) where $x \neq 0$ or $y \neq 0$. It remains to show that z is not defined at $(0, 0)$.

Suppose $\overline{F}/\overline{G} = \overline{Y}/\overline{X}$ for some $F, G \in k[X, Y]$. Then $\overline{YG} = \overline{XF}$ and $YG - XF \in (Y^2 - X^2(X+1))$. So $YG - XF = H(Y^2 - X^2(X+1))$ for some $H \in k[X, Y]$. Hence $Y(G - HY) = X(F - HX(X+1))$. So $G - HY \in (X)$. Therefore $0 = G(0,0) - (HY)(0,0) = G(0,0)$. □

The pole set of z^2 is empty.

Proof. Observe that $z = \overline{Y}^2/\overline{X}^2 = \overline{X^2(X+1)}/\overline{X}^2 = \overline{X+1}$. □

2.18. Let $\mathcal{O}_P(V)$ be the local ring of a variety V at a point P. Show that there is a natural one-to-one correspondence between the prie ideals in $\mathcal{O}_P(V)$ and the subvarieties of V that pass through P.

Proof. It suffices to show that there is a one-to-one correspondence between prime ideals in $\mathcal{O}_P(V)$ and prime ideals in $\Gamma(V)$ containing in $I(P)$.

Note from Proposition 3 that an ideal $I \subset \mathcal{O}_P(V)$ is generated by $I \cap \Gamma(V)$. Thus if I is prime, then $J = I(I \cap \Gamma(V))$ is a prime ideal in $\Gamma(V)$.

Suppose $J \subset \Gamma(V)$ is a prime ideal, $I(P) \subset J$. Note that $I(J)$, the ideal generated by J in $\mathcal{O}_P(V)$, is a proper ideal since J does not contain any units. Suppose $a/b, c/d \in \mathcal{O}_P(V)$ such that $(ac)/(bd) \in I(J)$. Since $1/b, 1/d, 1/(bd)$ are units, they are not in $I(J)$. Thus $ac \in I(J)$ and therefore $ac \in J$. So a or c must be in $J \subset I(J)$. Thus $I(J)$ is prime. □

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 U to k. Show that this function determines f uniquely.

Proof. Suppose $f = a/b = c/d$, $a, b, c, d \in \Gamma(V)$. Observe that for all $P \in U$, $f(P)$, $f(P)b(P)d(P) = a(P)d(P) = c(P)b(P)$. Moreover, for all $P \in V \setminus U$, $0 = a(P)d(P) = c(P)b(P)$. Therefore $ad = cb$. So $a/b = c/d$. □

2.20. Let V and f be as in the example given in this section.

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

Proof. Clearly f is defined everywhere $y \neq 0$ or $w \neq 0$. It remains to show that f is not defined when $y = w = 0$.

Suppose $f = \overline{F}/\overline{G}$. Then $\overline{XG} = \overline{YF}$ and $XG - YF \in (XW - YZ)$. Thus $XG - YF = H(XW - YZ)$ and $X(G - HW) = Y(F - HZ)$, $H \in k[X, Y, Z, W]$. So $G - HW \in (Y)$. Let $P = (x, 0, z, 0)$, $x, z \in k$. Observe that $G(P) - (HW)(P) = 0$. Since $(HW)(P) = H(P)(0) = 0$, $G(P) = 0$. Thus f is not defined at P for any choice of representative. □

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.

Proof. Suppose $f = \overline{F}/\overline{G}$ such that $\overline{F}/\overline{G}$ is defined at all points f is defiend. By the same argument above, $G - HW \in (Y)$. So if $Y = 0$, $G = HW$. If $W = 0$, then $G = AY$, $A \in k[X, Y, Z, W]$. So $G = AY + HW$.

Since $\overline{F}/\overline{G}$ is defined at all points f is defined, $V(G) \cap V$ is the pole set of f. Thus $I(V(G) \cap V) = (Y, W)$, since (Y, W) is the ideal of the pole set. However, for any choice of A, H, observe that $I(V(G) \cap V) = (AY + HW, XW - YZ) \neq (Y, W)$, a contradiction. □

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 writter $\widetilde{\varphi}$) from $\mathcal{O}_Q(W)$ to $\mathcal{O}_P(V)$. (Note that $\widetilde{\varphi}$ may not extend to all of $k(W)$.) Show that $\widetilde{\varphi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$.

Proof. Suppose $\psi : \mathcal{O}_Q(W) \to \mathcal{O}_P(V)$ is a homomorphism such that $\psi(a) = \widetilde{\varphi}(a)$ for any $a \in \Gamma(W)$. If a is a unit in $\mathcal{O}_Q(W)$ then $\psi(a^{-1}) = \psi(a)^{-1} = \widetilde{\varphi}(a)^{-1}$. So for any $a/b \in \mathcal{O}_Q(W)$, $\psi(a/b) = \widetilde{\varphi}(a)/\widetilde{\varphi}(b)$. Therefore $\widetilde{\varphi}$ extends uniquely to a homomorphism $\mathcal{O}_Q(W) \to \mathcal{O}_P(V)$.

Suppose $f \in \mathfrak{m}_Q(W)$. Then $\widetilde{\varphi}(f)(P) = f(Q) = 0$. So $\widetilde{\varphi}(\mathfrak{m}_Q(W)) \subset \mathfrak{m}_P(V)$. □

Lemma 2.13. Suppose W is a subvariety of a variety V, and P is a point in W. Then the natural homomorphism $\pi : \Gamma(V) \to \Gamma(W)$ extends uniquely to a homomorphism $\mathcal{O}_P(V) \to \mathcal{O}_P(W)$.

Proof. Note that $\pi : \Gamma(V) \to \Gamma(W)$ is the homomorphism induced by the inclusion polynomial map $W \hookrightarrow V$. Thus by Problem 2.21, π extends uniquely to a homomorphism $\mathcal{O}_P(V) \to \mathcal{O}_P(W)$. □

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

Proof. Since $\widetilde{T} : \Gamma(\mathbb{A}^n) \to \Gamma(\mathbb{A}^n)$ is an isomorphism, it extends uniquely to an isomorphism $\widetilde{T} : \mathcal{O}_Q(\mathbb{A}^n) \to \mathcal{O}_P(\mathbb{A}^n)$, by Problem 2.21.

Let $\pi_V : \mathcal{O}_Q(\mathbb{A}^n) \to \mathcal{O}_Q(V)$ and $\pi_{V^T} : \mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V^T)$ be the natural homomorphisms (see Lemma 2.13). Observe that $\ker(\pi_{V^T} \circ \widetilde{T}) \subset \mathcal{O}_Q(\mathbb{A}^n)$ is equal to the ideal generated by $\ker(\pi_{V^T} \circ \widetilde{T}) \cap \Gamma(\mathbb{A}^n)$, similarly for $\ker \pi_V$. Thus since $\ker \pi_V \cap \Gamma(\mathbb{A}^n) = \ker(\pi_{V^T} \circ \widetilde{T}) \cap \Gamma(\mathbb{A}^n)$, $\ker \pi_V = \ker(\pi_{V^T} \circ \widetilde{T})$. So $\pi_{V^T} \circ \widetilde{T}$ descends, by Lemma 1.2, to an isomorphism $\mathcal{O}_Q(V) \to \mathcal{O}_P(V^T)$. □

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

Proof. Suppose t, s are uniformizing parameters on R. Note that $s = ut$, with u a unit. Let $z \in K$. Observe that $z = vt^n$, $n \in \mathbb{Z}$, v a unit in R. So $z = vu^{-n}(ut)^n = vu^{-n}s^n$. □

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 $\mathcal{O}_a(V)$ is a DVR, with uniformizing parameter $t = X - a$.

Proof. Recall that all local rings of points are Noetherian and local. Moreover, $\mathfrak{m}_a(V) = (X - a)$, so the maximal ideal of $\mathfrak{m}_a(V)$ is principal with generator $X - a$. □

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

Proof. Observe that $F/G \in \mathcal{O}_\infty$ is a unit if and only if $\deg(F) = \deg(G)$. Let $F/G \in \mathcal{O}_\infty$, $n = \deg(G) - \deg(F)$. Then $(1/X^n)(FX^n/G) = F/G$ and FX^n/G is a unit. Therefore $1/X$ is a uniformizing parameter for $\mathcal{O}_\infty$. □

2.25. Let $p \in \mathbb{Z}$ be a prime number. Show $\{r \in \mathbb{Q} \mid r = a/b,\ a, b \in \mathbb{Z},\ p \nmid b\}$ is a DVR with quotient field $\mathbb{Q}$.

Proof. Let $r = a/b \in \mathbb{Q}$ such that $p \nmid b$. Let $c \in \mathbb{Z}$ such that $a = p^n c$, $n \geq 0$, $p \nmid c$. Then $r = p^n c/b$ and c/b is a unit. Thus the set is a DVR with uniformizing parameter p. Moreover, the quotient field is $\{p^n a/b \mid n, a, b \in \mathbb{Z},\ p \nmid a,\ p \nmid b\} = \mathbb{Q}$. □

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

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

Proof. We may write $z = ut^n$, with u a unit and $(t) = \mathfrak{m} \subset R$. Since $z \notin R$, $n < 0$. Therefore $z^{-1} = u^{-1}z^{-n} \in R$. □

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

Proof. Let $\mathfrak{m}' = (s)$ be the maximal ideal of S. Suppose $s \in R$. Then since $\mathfrak{m} \subset \mathfrak{m}'$, $\mathfrak{m}' = \mathfrak{m}$ and $S = R$. Suppose $s \notin R$. Then by part (a), $s^{-1} \in R \subset S$ and s is a unit in S, a contradiction. □

2.27. Show that the DVR's of Problem 2.24 are the only DVR's with quotient field $k(X)$ that contain k.

Proof. Suppose $R \supset k$ is a DVR with field of fractions $k(X)$. Let $(t) = \mathfrak{m} \subset R$ be the maximal ideal of R. Observe that we may treat R as a subring of its field of fractions $k(X)$.

Suppose $X \in R$. Then the inclusion map $i : k[X] \hookrightarrow R$ is a natural injective homomorphism. Moreover, So $i^{-1}(\mathfrak{m})$ is either $k[X]$ or a maximal ideal of $k[X]$ by Problem 1.22. Thus $\mathfrak{m} = (X - a)$ for some $a \in k$.

Suppose $X \notin R$. Then $X = ut^{-n}$ for some $n > 0$. Since X is not a square, $n = 1$. Therefore $1/X = ut$ and $\mathfrak{m} = (1/X)$. □

Show that those of Problem 2.25 are the only DVR's with quotient field $\mathbb{Q}$.

Proof. Suppose R is a DVR with field of fractions $\mathbb{Q}$. Observe that $\mathbb{Z} \subset R \subset \mathbb{Q}$. Thus the inclusion map $i : \mathbb{Z} \to R$ is a natural injective homomorphism. So $i^{-1}(\mathfrak{m})$ is a maximal ideal in $\mathbb{Z}$. Thus $\mathfrak{m} = (p)$ for some prime p. □

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

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

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

3. $\varphi(a+b) \geq \min(\varphi(a), \varphi(b))$.

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 ord : $K \to Z \cup \{\infty\}$ is an order function on K. Giving a DVR with a quotient field K is equivalent to defining an order function on K.

Proof. Suppose φ is an order function on a field K and R is the set defined above. Observe that $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1)$. Thus $\varphi(1) = 0$. Similarly $\varphi(-1) = 0$. Thus for any $a \in K$, $\varphi(a) = \varphi(-a)$. Thus R is closed under multiplication and addition. Moreover, a is a unit in R, that is $a^{-1} \in R$, if and only if $\varphi(a) = 0$.

Next we will show that $\mathfrak{m}$ is an ideal. Let $a, b \in \mathfrak{m}$. Observe that $\varphi(a-b) \geq \min(\varphi(a), \varphi(b)) > 0$. So $\mathfrak{m}$ is an additive group. Moreover, if $a \in \mathfrak{m}, r \in R$, then $\varphi(ar) > \varphi(a)$. So $ar \in \mathfrak{m}$ and $\mathfrak{m}$ is an ideal.

It remains to show that $\mathfrak{m}$ is principal. If $\mathfrak{m} = \{0\}$ then we are done. Suppose $\mathfrak{m} \neq \{0\}$. Then $\phi(\mathfrak{m} \setminus \{0\}) \neq \emptyset$ and, by the well ordering principle, we may select $p \in \mathfrak{m} \setminus \{0\}$ such that for all $a \in \mathfrak{m}$, $\varphi(p) \leq \varphi(a)$. Then for $a \in \mathfrak{m}$, $\varphi(ap^{-1}) \geq 0$. So $a = p(ap^{-1})$ and $p \mid a$. Thus $\mathfrak{m} = (p)$. So R is a DVR.

Converseley suppose that R is a DVR with quotient field K. It is immediate that ord satisfies (i) and (ii). To see that ord satisfies (iii), see Problem 2.29(a). □

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 $\text{ord}(a+b) = \text{ord}(a)$.

Proof. Let t be the uniformizing parameter for R. Then $a = ut^n, b = vt^m$ with $n, m \in \mathbb{Z}$ and u, v units of R. Suppose without loss of generality that $n \leq m$. Then $a + b = t^n(u + vt^{m-n})$ and $\text{ord}(a+b) = n = \text{ord}(a)$. □

(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 $a_1 + \ldots + a_n \neq 0$.

Proof. It suffices to show that for any $\text{ord}(a + 1 + \ldots + a_n) = \min_{1 \leq i \leq n}(\text{ord}(a_i))$. If $n = 2$, the statement follows from part (a). Suppose that for $n \geq 2$, $\text{ord}(a_1 + \ldots + a_n) = \min_{1 \leq i \leq n}(\text{ord}(a_i)) = m \in \mathbb{Z} \cup \{\infty\}$. Let $a_{n+1} \in K$. By part (a), $\text{ord}(a_1 + \ldots + a_{n+1}) = \min(m, \text{ord}(a_{n+1})) = \min_{1 \leq i \leq n+1}(\text{ord}(a_i))$. □

2.30.* Let R be a DVR with maximal ideal $\mathfrak{m}$, and quotient field K. Suppose k is a subfield of R, and that the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism.

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

Proof. Let $z \in R$. Let $\pi : R \to R/\mathfrak{m}$ be the natural homomorphism. Since the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism, there is a unique $\lambda \in k$ such that $\pi(z) = \pi(\lambda)$, that is, $z - \lambda \in \mathfrak{m}$. □

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

Proof. Let $z \in R$. By part (a) there exists a unique $\lambda_0 \in k$ such that $z - \lambda_0 \in \mathfrak{m}$, that is, $z = \lambda_0 + z_0 t$ for some $z_0 \in R$. So the statement holds for $n = 0$.

Suppose for $n \geq 0$ that $z = \lambda_0 + \ldots + \lambda_n t^n + z_n t^{n+1}$. By part (a) there exists $\lambda_{n+1} \in k$, $z_{n+1} \in R$ such that $z_n = \lambda_{n+1} + z_{n+1} t$. Thus $z = \lambda_0 + \ldots + \lambda_n t^n + \lambda_{n+1} t^{n+1} + z_{n+1} t^{n+2}$.

It remains to show uniqueness. Suppose $z = \lambda_0 + \ldots + \lambda_n t^n + z_n t^{n+1} = \sigma_0 + \ldots + \sigma_n t^n + w_n t^{n+1}$, with $\lambda_i, \sigma_i \in k$ for each i, and $z_n, w_n \in R$. Then $0 = (\lambda_0 - \sigma_0) + \ldots + (\lambda_n - \sigma_n) t^n + (z_n - w_n) t^{n+1}$. By 2.29b, $\lambda_i - \sigma_i = 0$ for each i, and $z_n - w_n = 0$. □

2.31. Let k be a field. The ring of formal power series over k, written $k[[X]]$, is defined to be $\{\sum_{i=0}^{\infty} a_i X^i \mid a_i \in k\}$. Define the sum by $\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$, and the product $(\sum a_i X^i)(\sum b_i X^i) = \sum c_i X^i$, where $c_i = \sum_{j+k=i} a_j b_k$. Show that $k[[X]]$ is a ring containing $k[X]$ as a subring.

Proof. It is simple to verify that $k[[X]]$ is an additive group with additive identity 0, and $-\sum a_i X^i = \sum (-a_i) X^i$. Note that multiplication is a well defined binary operation on $k[[X]]$ with identity 1. It remains to show that multiplication is associative and distributes over addition. To show associativity observe that

$$\begin{aligned}
\left(\sum a_i X^i\right)\left(\left(\sum b_i X^i\right)\left(\sum c_i X^i\right)\right) &= \left(\sum a_i X^i\right)\left(\sum \left(\sum_{j+k=i} b_j c_k\right) X^i\right) \\
&= \left(\sum \left(\sum_{j+k=i} a_j \left(\sum_{l+d=k} b_l c_d\right)\right) X^i\right) \\
&= \left(\sum \left(\sum_{j+l+d=i} a_j b_l c_d\right) X^i\right)
\end{aligned}$$

$$= \left(\sum \left(\sum_{j+k=i} c_j \left(\sum_{l+d=k} a_l b_d \right) \right) X^i \right)$$
$$= \left(\sum \left(\sum_{j+k=i} a_j b_k \right) X^i \right) \left(\sum c_i X^i \right)$$
$$= \left(\left(\sum a_i X^i \right) \left(\sum b_i X^i \right) \right) \left(\sum c_i X^i \right).$$

To show multiplication distributes observe that

$$\begin{aligned}
\left(\sum a_i X^i \right) \left(\sum b_i X^i + \sum c_i X^i \right) &= \sum \left(\sum_{k=0}^{i} a_k (b_{i-k} + c_{i-k}) \right) X^i \\
&= \sum \left(\sum_{k=0}^{i} (a_k b_{i-k} + a_k c_{i-k}) \right) X^i \\
&= \sum \left(\sum_{k=0}^{i} a_k b_{i-k} X^i + \sum_{k=0}^{i} a_k c_{i-k} X^i \right) \\
&= \sum \left(\sum_{k=0}^{i} a_k b_{i-k} \right) X^i + \sum \left(\sum_{k=0}^{i} a_k c_{i-k} \right) X^i \\
&= \left(\sum a_i X^i \right) \left(\sum b_i X^i \right) + \left(\sum a_i X^i \right) \left(\sum c_i X^i \right).
\end{aligned}$$

Finally, note that the definition of multiplication for series agrees with the definition of multiplication for finite sums. Thus we can define an inclusion map $k[X] \hookrightarrow k[[x]]$ by $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{\infty} a_i X^i$ with $a_i = 0$ for all $i > n$. So $k[[X]]$ contains a copy of $k[X]$ as a subring. □

Show that $k[[X]]$ is a DVR with uniformizing parameter X. Its quotientfield is denoted $k((X))$.

Proof. We will show that every element of $k[[X]]$ may be written as uX^t where u is a unit in $k[[X]]$. It suffices to show that $\sum a_i X^i$ is a unit if and only if $a_0 \neq 0$.

Suppose $\sum a_i X^i \in k[[X]]$ is a unit, that is, $(\sum a_i X^i)(\sum b_i X^i) = 1$. Then it must be that $a_0 b_0 = 1$, thus a_0, b_0 are each nonzero. Conversely suppose $\sum a_i X^i \in k[[X]]$, $a_0 \neq 0$. Define $\sum b_i X^i \in k[[X]]$ by $b_0 = a_0^{-1}$ and $b_i = -a_0^{-1} \sum_{k=1}^{i} a_k b_{i-k}$ for $i > 0$. Observe that

$$\left(\sum a_i X^i \right) \left(\sum b_i X^i \right) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) X^i$$

$$
\begin{aligned}
&= a_0 a_0^{-1} + \sum_{i=1}^{\infty} \left(a_0 b_i + \sum_{k=1}^{i} a_k b_{i-k} \right) X^i \\
&= 1 + \sum_{i=1}^{\infty} \left(a_0 \left(-a_0^{-1} \sum_{k=1}^{i} a_k b_{i-k} \right) + \sum_{k=1}^{i} a_k b_{i-k} \right) X^i \\
&= 1 + \sum_{i=1}^{\infty} \left(-\sum_{k=1}^{i} a_k b_{i-k} + \sum_{k=1}^{i} a_k b_{i-k} \right) X^i \\
&= 1.
\end{aligned}
$$

□

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

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

Proof. Let $\varphi : R \to k[[X]]$ be the map defined above. Let $z, w \in R$, $\varphi(z) = \sum \lambda_i X^i$, $\varphi(w) = \sum \sigma_i X^i$. If $z = w$ then $\lambda_i = \sigma_i$ for each i. Conversely, if $\lambda_k \neq \sigma_k$ for some k then $z \neq w$; in fact, $z - w = z_k t^k$, $z_k \in R$, and $\operatorname{ord}(z - w) = k$. Thus the map is well defined and one-to-one.

It remains to show that φ is a homomorphism. Let $z, w \in R$, and write $z = \lambda_0 + \ldots + \lambda_k t^k + z_{k+1} t^{k+1}$, $w = \sigma_0 + \ldots + \sigma_k t^k + w_{k+1} t^{k+1}$, with $\lambda_0, \ldots, \lambda_k, \sigma_0, \ldots, \sigma_k \in k$ and $z_{k+1}, w_{k+1} \in R$. Then

$$
\begin{aligned}
zw &= (\lambda_0 + \ldots + \lambda_k t^k + z_{k+1} t^{k+1})(\sigma_0 + \ldots + \sigma_k t^k + w_{k+1} t^{k+1}) \\
&= \lambda_0 \sigma_0 + \left(\sum_{j+l=1} \lambda_j \sigma_l \right) t + \ldots + \left(\sum_{j+l=k} \lambda_j \sigma_l \right) t^k + (\ldots) t^{k+1}.
\end{aligned}
$$

By the uniqueness of coefficients in Problem 2.30, this shows that if $zw = \gamma_0 + \ldots + \gamma_k t^k + h_{k+1} t^{k+1}$, with $\gamma_0, \ldots, \gamma_k \in k$, $h_{k+1} \in R$, then $\gamma_i = \sum_{j+l=i} \lambda_j \sigma_l$. So $\varphi(zw) = \varphi(z)\varphi(w)$. □

(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.

Proof. Let $z \in K \setminus R$. Since $z^{-1} \in R$, we naturally extend ϕ by defining $\phi(z) = \phi(z^{-1})^{-1}$. Since ϕ is injective on R, this extension is a well defined injective homomorphism $K \hookrightarrow k((X))$.

It suffices to show $\mathrm{ord}_R(z) = \mathrm{ord}_{k[[X]]}(\phi(z))$ for all $z \in R$. But this is clealy the case since $\mathrm{ord}_R(z) = k$, $\mathrm{ord}_{k[[X]]}(\phi(z)) = k$, where k is the least integer such that $\lambda_k \neq 0$. $\square$

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

Note that $(1-X), (1-X)(1+X^)) \notin \mathfrak{m}_0 = (X)$, so they are invertible. By our explicit construction of the power series inverses in Problem 2.31, we find

$$(1-X)^{-1} = \sum X^i,\ (1+X^2)^{-1} = \sum (-1)^i X^{2i}.$$

Therefore

$$(1-X)(1+X^2)^{-1} = \sum (-1)^i X^{2i} - \sum (-1)^i X^{2i+1} = \sum (-1)^{\lceil i/2 \rceil} X^i.$$

Proposition 5. (1) $(FG)_* = F_* G_*$; $(fg)^* = f^* g^*$.

Proof. It is immediate that $(FG)_* = F_* G_*$. Let $f = f_0 + \ldots + f_d$, $g = g_0 + \ldots + g_l$, where f_i, g_i are forms of degree i. Then

$$fg = \sum_{k=0}^{dl} \sum_{i=0}^{k} f_i g_{k-i},$$

where $f_i = 0, g_j = 0$ if $i > d$, $j > l$. Observe that

$$(fg)^* = \sum_{k=0}^{dl} X_{n+1}^k \sum_{i=0}^{k} f_i g_{k-i} = \sum_{k=0}^{dl} \sum_{i=0}^{k} (X_{n+1}^i f_i)(X_{n+1}^{k-i} g_{k-i}) = f^* g^*.$$

$\square$

(2) If $F \neq 0$ and r is the highest power of X_{n+1} that divides F, then $X_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

Proof. Write $F = G X_{n+1}^r$, with G a form and $X_{n+1} \nmid G$. Then $F_* = G_*$. Moreover, $G_* = G = G^*$. Thus $(F_*)^* = G$.

To show the second result, recall that

$$f^* = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Thus $(f^*)_* = f^*(X_1, \ldots, X_n, 1) = f$. □

(3) $(F+G)_* = F_* + G_*$; $X_{n+1}^t (f+g)^* = X_{n+1}^r f^* X_{n+1}^s g^*$, where $r = \deg(g)$, $s = \deg(f)$, and $t = r + s - \deg(f+g)$.

Proof. It is immediate that $(F+G)_* = F_* + G_*$. Let r, s, t be defined as above. Observe that

$$(f+g)^* = X_{n+1}^{\deg(f+g)} f\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) + X_{n+1}^{\deg(f+g)} g\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

and

$$f^* = X_{n+1}^{\deg(f)} f\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right),\ g^* = X_{n+1}^{\deg(g)} g\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Since $\deg(f+g) \leq \deg(f) + \deg(g)$, $t \geq 0$ and $X_{n+1}^t (f+g)^* = X_{n+1}^r f^* X_{n+1}^s g^*$. □

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

We note that factoring $F(X,Y) = Y^3 - 2XY^2 + 2X^2Y + X^3$ is the same as factoring $F(X,1)$ or $F(1,Y)$. Unfortunately, neither factors nicely, so we will simply note that $F(X,Y) = (X - Y\lambda_1)(X - Y\lambda_2)(X - Y\lambda_3)$, where $\lambda_1, \lambda_2, \lambda_3$ are the roots to $F(X,1)$ in $\mathbb{C}$.

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

Proof. Suppose $F + G = HJ$ for some $H, J \in k[X_1, \ldots, X_n]$. By Proposition 5, $(F+G)^* = X_{n+1}F + G = H^*G^* = (HG)^*$. Since $X_{n+1}F + G$ is degree 1 as a polynomial in X_{n+1}, one of H^*, G^* must be of degree 0 as a polynomial in X_{n+1}. Therefore one of H^*, G^* divides F and G and is therefore constant, since F, G share no common factors. Thus one of H, G are constant. Hence $F + G$ is irreducible. □

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

Proof. A monomial of degree d in $R[X,Y]$ is of the form X^iY^j, $i + j = d$. There are $d+1$ options for i and $j = d - i$.

A monomial of degree d in $R[X,Y,Z]$ is of the form F_iZ^j where F_i is a monomial of degree i in $R[X,Y]$ and $i + j = d$. There are $i+1$ monomials of degree i in $R[X,Y]$. Thus there are $1 + 2 + \ldots + (d+1) = (d+1)(d+2)/2$ 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 the monomials of degree d form a basis.

Proof. It is immediate that $V(d,n)$ is a vector space with the natural addition and scalar multiplication operations. Clearly the monomials of degree d span $V(d,n)$ and are linearly indpendent over k. Thus they form a basis. □

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

It suffices to show that $\{A_{ij} \mid i+j=d\}$ is a linearly independent set.

Proof. Suppose to the contrary that

$$0 = \sum_{i+j=d} a_{ij} L_1 \dots L_i M_1 \dots M_j, \ a_{ij} \in k \setminus \{0\}.$$

Then

$$L_1 \dots L_d = \sum_{i+j=d, j>0} a_{ij} L_1 \dots L_i M_1 \dots M_j.$$

So

$$L_1 \dots L_d = M_1 \sum_{i+j=d-1} a_{ij} L_1 \dots L_i M_2 \dots M_j.$$

Thus, since $L_1, \dots, L_d, M_1$ are all linear, $M_1 = \lambda L_i$, a contradiction. □

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

Proof. There are n variables, whose powers must add up to d. This is counted by

$$\left(\binom{n}{d}\right) = \binom{d+n-1}{n-1}.$$

□

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 $(0,\dots,a_i,\dots,0)$ a ring homomorphism?

The additive identity is $(0,0,\dots,0)$ and the multiplicative identity is $(1,1,\dots,1)$. The inclusion map $i_{R_i} : R_i \hookrightarrow \prod R_j$ is an injective homomorphism.

Proof. Clearly $(0,\dots,a_i,\dots,0)+(0,\dots,b_i,\dots,0)=(0,\dots,a_i+b_i,\dots,0)$, and similarly for multiplication. □

2.38.* Show that if $k \subset R_i$, and each R_i is finite dimensional over k, then $\dim(\prod R_i) = \sum \dim R_i$.

Proof. Let R, S be rings, $\{r_i\}, \{s_j\}$ finite basis for R, S over k. Then $\{(r_i,0)\} \cup \{(0,s_j)\}$ is clearly a linearly independent spanning set for $R \times S$. Thus $\dim(R \times S) = \dim R + \dim S$. The result then follows by induction. □

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

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

Proof. Suppose $x = (i_1 + i_2)j \in (I_1 + I_2)J$. Then $x = i_1j + i_2j \in I_1J + I_2J$. Suppose $x = i_1j_1 + i_2j_2 \in I_1J + I_2J$. Then $i_1j_1, i_2j_2 \in (I_1 + I_2)J$ and thus $x \in (I_1 + I_2)J$. So $(I_1 + I_2)J = I_1J + I_2J$. □

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

Proof. Observe that $(a_1 \dots a_N)^n = a_1^n \dots a_N^n$ where $a_k \in I_k$. Thus $(I_1 \dots I_N)^n = I_1^n \dots I_N^n$. □

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.

Proof. Let $a \in I, b \in J$ such that $a + b = 1$. Then $ab \in I, b^2 \in J^2$ and $ab + b^2 = b$. Thus $a, b \in I + J^2$ and therefore $1 \in I + J^2$.

By induction, the above implies that I^m and J^n are comaximal for all m, n. □

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

Proof. This follows from part (a) and the fact that $I \cap J = IJ$ when I, J are comaximal. □

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

Proof. Let $I = (a_1, \ldots, a_N)$. Since $I \subset \mathrm{Rad}(J)$ for each i, $a_i^{n_i} \in J$ for some $n_i \geq 1$. If we take $n = N \cdot \max\{n_i \,|\, 1 \leq i \leq N\}$ then, by the multinomial theorem and pigeon hole principle, $I^n = ((a_1) + \ldots + (a_N))^n \subset (a_1)^{n_1} + \ldots + (a_N)^{n_N} \subset J$. □

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.

Proof. This follows from applying Lemma 1.2 to the natural maps $R \to R/I$, $R \to R/J$. □

(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.

Proof. Define $\varphi : R \to S/IS$ by $r \mapsto r + IS$. Note that this is a well defined homomorphism since $I \subset IS$. Moreover, $\varphi(I) = \{0 + IS\} \subset S/IS$. Thus we may apply Lemma 1.2 to the natural map $R \to R/I$ and the map $\varphi : R \to S/IS$ and yield the desired result. □

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

Proof. Observe that if $f = F/G \in \mathcal{O}$, then $f \in \mathfrak{m}$, that is $f(P) = 0$, if and only if $F(P) = 0$. Moreover, $F(P) = 0$ if and only if $F \in I(P) = I$. So $\mathfrak{m} = I\mathcal{O}$. □

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 $k[X_1, \ldots, X_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Show that there is a homomoprhism φ from $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n)$ to $\mathcal{O}_P(V)/J'\mathcal{O}_P(V)$, and that φ is an isomorphism. In particular, $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$ is isomorphic to $\mathcal{O}_P(V)$.

Proof. Observe that by Lemma 2.13 the homomorphism $\varphi : \Gamma(\mathbb{A}^n) \to \Gamma(V)$ extends naturally to a homomorphism $\varphi' : \mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)$. Moreover, note that $J' = \varphi(J)$, thus $\varphi'(J\mathcal{O}_P(\mathbb{A}^n)) = J'\mathcal{O}_P(V)$. Let $\pi : \mathcal{O}_P(\mathbb{A}^n) \to J\mathcal{O}_P(\mathbb{A}^n)$ and $\pi_V : \mathcal{O}_P(V) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$ be the natural homomorphisms.

$$\begin{array}{ccc} \mathcal{O}_P(\mathbb{A}^n) & \xrightarrow{\quad\varphi'\quad} & \mathcal{O}_P(V) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_V} \\ \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) & \longrightarrow & \mathcal{O}_P(V)/J'\mathcal{O}_P(V) \end{array}$$

Observe that $\ker \pi = J\mathcal{O}_P(\mathbb{A}^n) = \varphi'^{-1}(J'\mathcal{O}_P(V)) = \ker \pi_V \circ \varphi'$. Thus by Lemma 1.2, the homomorphism $\pi_V \circ \varphi'$ induces an isomorphism $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$. □

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

Proof. Note that $V(I) \cap V(J) = V(I + J)$. By the weak Nullstellensatz, $V(I + J) = \emptyset$ if and only if $I + J = k[X_1, \ldots, X_n]$. Thus $I + J$ are comaximal if and only if $V(I) \cap V(J) = \emptyset$. □

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

Proof. Observe that the residues of monomials of degree $d < n$ span $k[X, Y]/I^n$ and are linearly independent over k. By Problem 2.35(a) there are $d + 1$ monomials of degree d. Therefore $k[X, Y]/I^n$ is of dimension $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. □

Lemma 2.14. Let $V \subset \mathbb{A}^n$ be an algebraic set. Then $\dim_k(k[X_1, \ldots, X_n]/I(V))$ is finite if and only if V is finite.

Proof. Let us decompose $V(I)$ into irreducible algebraic sets $V(I) = \bigcup_{i=1}^m V_i$.

Suppose V is finite, that is, each V_i is a point. Therefore the ideals $I(V_1), \ldots, I(V_n)$ are distinct maximal ideals. In particular, they are pairwise comaximal. Thus, by the Chinese Remainder Theorem,

$$k[X_1, \ldots, X_n]/I(V) \cong k[X_1, \ldots, X_n]/I(V_1) \times \ldots \times k[X_1, \ldots, X_n]/I(V_m) \cong k^m$$

Conversely, suppose $\dim_k(k[X_1, \ldots, X_n]/I(V)) = d < \infty$. Since $I(V_i) \supset I(V)$ for each i, $\dim_k(k[X_1, \ldots, X_n]/I(V_i))$ is finite. Thus, by Problem 2.4, $k[X_1, \ldots, X_n]/I(V_i) \cong k$ for each i and the result follows as above. Moreover, $d = m$. □

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.

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for R over k. Let $\varphi : k[X_1, \ldots, X_n] \to R$ be the natural map sending $X_i \mapsto v_i$. Then φ is a surjective ring homomorphism (and thus also a surjective vector space homomorphism over k). Let $I = \ker \phi$. Note that $\dim_k(R) = \dim_k(k[X_1, \ldots, X_n]/I)$. By Lemma 2.14 $V(I)$ is finite. Then by Proposition 6,

$$R \cong k[X_1, \ldots, X_n]/I \cong \prod_{i=1}^N \mathcal{O}_i/I\mathcal{O}_i.$$

□

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

$$0 \longrightarrow \ker(\varphi) \longrightarrow M \xrightarrow{\varphi} \mathrm{im}(\varphi) \longrightarrow 0$$

is exact.

Proof. The map $\phi : M \to im(\phi)$ is surjective by definition and similarly $\ker \phi \hookrightarrow M$ is the inclusion map and therefore injective. □

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 $\overline{\varphi} \circ \pi = \varphi$.

Proof. See Lemma 1.2. □

(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

$$0 \longrightarrow N/P \longrightarrow M/P \longrightarrow M/N \longrightarrow 0$$

is exact ("Second Noether Isomorphism Theorem").

Proof. The map $N/P \hookrightarrow M/P$ is the natural inclusion map. The map $\varphi : M/P \to M/N$ exists by part (a). Again by part (a) $\ker \varphi = \ker(\varphi \circ \pi)$ where $\pi : M \to M/P$ is the natural homomorphism. Thus the sequence is exact. □

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

Proof. Observe that

$$0 \longrightarrow W/U \longrightarrow V/U \longrightarrow V/W \longrightarrow 0$$

is exact by part (b). The result then follows by Proposition 7. □

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

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

Proof. Note that ideals of a ring R are clearly R-submodules of R. Therefore the result follows from part (b). □

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

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^{n+1} \longrightarrow \mathcal{O}/\mathfrak{m}^n \longrightarrow 0.$$

Proof. Observe that $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n \subset \mathcal{O}$. Thus the result follows by part (d). □

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

Proof. By (b) $R/\mathfrak{m}^n$ has dimension n over k. Moreover, by 2.49(e), the following sequence is exact

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^{n+1} \longrightarrow R/\mathfrak{m}^n \longrightarrow 0.$$

Thus, by Proposition 7,

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_k(R/\mathfrak{m}^{n+1}) - \dim_k(R/\mathfrak{m}^n) = n + 1 - n = 1.$$

□

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

Proof. By Problem 2.30 $R = \{\lambda_0 + \ldots + \lambda_{n-1}t^{n-1} + z^n t^n\}$, where t is the uniformizing parameter. Therefore $R/\mathfrak{m}^n$ has spanning linearly indpendent set $\{t^d \,|\, 0 \leq d \leq n-1\}$. □

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

Proof. If $(z) = \mathfrak{m}^n$ then $z = ut^n$ and $\text{ord}(z) = n$. □

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

Proof. For $n = 2$ the statment is trivial. Proposition 7 proves the statement for such sequences with $n = 3, 4$. Suppose $n > 4$ and the statement holds for all such exact sequences

of length less than n (and at least 2). For $1 \leq k \leq n-1$, let $\varphi_k : V_k \to V_{k+1}$ be the homomorphism from the exact sequence. Define $W = \ker \phi_{n-1} = \text{im}\phi_{n-2}$. Then

$$0 \longrightarrow V_1 \longrightarrow \ldots \longrightarrow V_{n-2} \longrightarrow W \longrightarrow 0 \text{ and } 0 \longrightarrow V_{n-1} \longrightarrow V_n \longrightarrow W \longrightarrow 0$$

are exact. The second sequence gives us that $\dim W = \dim V_{n-1} - \dim V_n$. Therefore, by the first sequence,

$$0 = \sum_{i=1}^{n-2} (-1)^i \dim V_i + (-1)^{n-1}(W) = \sum_{i=1}^{n} (-1)^i \dim V_i.$$

□

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 isomomrphism of $N/(N \cap P)$ onto $(N+P)/P$ ("First Noether Isomorphism Theorem").

Proof. Observe that for $n, m \in N$, $n - m \in P$ if and only if $n - m \in N \cap P$. Thus the map $\varphi : N/(N \cap P) \to (N+P)/P$ defined by $n + (N \cap P) \mapsto n + P$ is a well defined injective R-module homomorphism. Moreover, if $x \in N + P$ then $x = n + p$ for some $n \in N$, $p \in P$. So $x + P = n + P = \varphi(n + (N \cap P))$. So φ is surjective. □

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 $T(V)/T(W)$.

Proof. Let $\pi : V \to V/W$ and $\pi_T : T(V) \to T(W)$ be the natural homomorphisms. Observe that $\ker \pi_T \circ T = W = \ker \pi$. Thus by Lemma 1.2, $\pi_T \circ T$ induces an isomorphism $V/W \to T(V)/T(W)$. □

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

Proof. Note that $T(V), W$ are both submodules of V. Therefore both results follow from Problem 2.52. □

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

Proof. Observe that V/W is isomorphic to $T(V)/T(W)$ since T is an isomorphism. Therefore $\dim V/W = \dim T(V)/T(W) = n$. Note that $W \subset W + T(V) \subset V$ and V/W is finite dimensional. Therefore by Problem 2.49(c),

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

Similarly, $T(W) \subset W \cap T(V) \subset T(V)$ and thus

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

By part (b), $\dim T(V)/(W \cap T(V)) = \dim(W + T(V))/W$, yielding the desired equality $\dim V/(W + T(V)) = \dim(W \cap T(V))/T(W)$. □

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

Proof. Observe that $(V/T(W))/(W/T(W)) \cong T/W$ by the second isomorphism theorem for modules. Since $W/T(W)$ and T/W are finitely dimensional, Lemma 2.2 implies that $V/T(W)$ is finitely dimensional. Since $T(V) \subset W + T(V) \subset V$, Problem 2.49(c) shows

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

Moreover, since $W/T(W)$ is finite dimensional and $T(W) \subset W \cap T(V) \subset W$,

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

By part (b),

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

By part (c),

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

Therefore

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

□

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

It means that every element of M may be written as a sum $\sum_{i=1}^{n} a_i m_i$, where $a_1, \ldots, a_n \in R$.

2.55. Let $F = X^n + a_1X^{n-1} + \ldots + a_n$ be a monic polynomial in $R[X]$. Show that $R[X]/(F)$ is a free R-module with basis $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$, where $\overline{X}$ is the residue of X.

Proof. Let $X = \{\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}\}$. Observe that the natural R-module homomorphism $M_X \to R[X]/(F)$ is surjective with trivial kernel, and thus an isomorphism. □

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.

Proof. The first statement is immediate from Problem 2.54. Let M be an arbitrary R-module and X a (possibly infinite) set of generators for M. Then there exists a natural surjective homomorphism $\pi : M_X \to M$ and $M_X/\ker\pi$ is isomorphic to M. □

3 Local Properties of Plane Curves

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

Proof. Observe that $C_X = 3X^2$ and $C_Y = 2Y$. Thus if $C_X = C_Y = 0$, then $X = Y = 0$. Moreover, $C(0, 0) = 0$ so $P = (0, 0)$ is the only multiple point on C.

Observe that $D_X = -3X^2 - 2X$ and $D_Y = 2Y$. Thus if $D_X = D_Y = 0$, then $Y = 0$ and $X = 0$ or $X = -2/3$. Moreover, $D(0, 0) = 0$ and $D(-2/3, 0) \neq 0$. So $P(0, 0)$ is the only multiple point on D.

Observe that $E_X = 4(X^2+Y^2)X+6XY$ and $E_Y = 4(X^2+Y^2)Y+3X^2-2Y$. If $E_X = 0$ then either $X = 0$, $X^2 = -Y^2$, or $4(X^2 + Y^2) = -6Y$. If $X = 0$ and $E_Y = 0$ then $4Y^3 - 2Y^2 = 0$ and hence $Y = 0$ or $Y = 1/2$. If $X^2 = -Y^2$ and $E_Y = 0$ then $-3Y^2 - 2Y^2 = 0$ and $Y = 0$. If $4(X^2 + Y^2) = -6Y$ and $E_Y = 0$ then, with a bit more computation, $Y = 0$ or $Y = -9/14$. This gives us several possible multiple points, but checking we find only $P = (0, 0)$ is on E.

Observe that $F_X = 6(X^2 + Y^2)^2X - 8XY^2$ and $F_Y = 6(X^2 + Y^2)^2Y - 8X^2Y$. If $F_X = 0$ then $X = 0$ or $6(X^2 + Y^2)^2 = 8Y^2$. If $F_Y = 0$ then $Y = 0$ or $6(X^2 + Y^2)^2 = 8X^2$. Suppose that $F_X = F_Y = 0$. If $X = 0$ or $Y = 0$ then $X = Y = 0$. It remains to consider the case $6(X^2 + Y^2)^2 = 8Y^2$ and $6(X^2 + Y^2)^2 = 8X^2$. Note that this gives us $X^2 = Y^2$. Substituting we have $24X^4 = 8X^2$ and thus $X = \pm\sqrt{1/3}$. However, $D(\pm\sqrt{1/3}, \pm\sqrt{1/3}) \neq 0$. So $P = (0, 0)$ is the only multiple point on D. □

3.2. Find the multiple points on 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 (d) that is contained in $\mathbb{A}^2(\mathbb{R}) \subset \mathbb{A}^2(\mathbb{C})$.

We compute the above using the following sage file.

```
# compute_multiple_points.sage
# Author: Aven Bross (kieroda@gmail.com)

def compute_multiple_point_ideal(f, R):
    x, y = R.gens()
    I = (f, f.derivative(x), f.derivative(y))*R
    return I.groebner_basis()

R, (x, y) = CC['x','y'].objgens()

a = y^3-y^2+x^3-x^2+3*x*y^2+3*x^2*y+2*x*y
b = x^4+y^4-x^2*y^2
c = x^3+y^3-3*x^2-3*y^2+3*x*y+1
d = y^2+(x^2-5)*(4*x^4-20*x^2+25)

Ia = compute_multiple_point_ideal(a, R)
Ib = compute_multiple_point_ideal(b, R)
Ic = compute_multiple_point_ideal(c, R)
Id = compute_multiple_point_ideal(d, R)

# Plot the real part of curve (d)

Pd = implicit_plot(y^2+(x^2-5)*(4*x^4-20*x^2+25), \
        (y, -12, 12), (x, -3, 3))
```

For each curve F we compute a Groebner basis for the ideal (F, F_X, F_Y). This gives us a clear view of the set of points where all three are zero, that is, the multiple points of the curve. We produce the following

```
sage: Ia
[y^2, x - y]
sage: Ib
[y^5, x*y^3, x^3 + (-0.50000000000000)*x*y^2, \
    x^2*y + (-2.0000000000000)*y^3]
sage: Ic
[x - 1.00000000000000, y - 1.00000000000000]
sage: Id
[x^2 - 2.50000000000000, y]
```

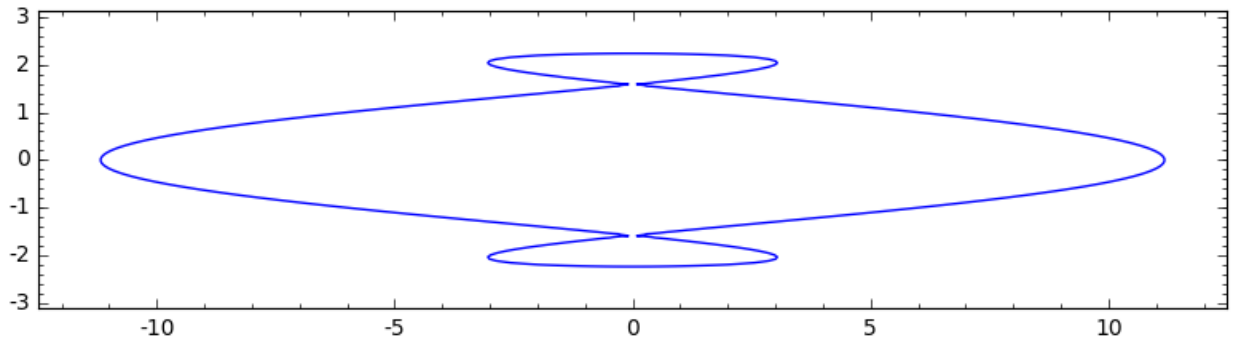

Figure 1: The real part of the curve from 3.2 (d), drawn with X on the vertical axis.

Therefore the curve in (a) has one double point at $(0,0)$, and the curve in (b) has one quadruple point at $(0,0)$. The curve in (c) has a multiple point at $(1,1)$ and, computing

```
sage: c(x+1, y+1)
x^3 + y^3 + 3.000000000000000*x*y
```

we find that $(1,1)$ is a double point. Finally, the curve in (d) has multiple points at $(\pm\sqrt{5/2}, 0)$. Similarly to above, we compute `d(x+sqrt(2.5), y)` and `d(x-sqrt(2.5), y)` to see that each is a double point.

A sketch of the real part of the curve from (d) is shown in Figure 1, with both double points clearly visible.

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).

Proof. Suppose F has degree n and $P = (a, b)$ is a point on F of multiplicity n. Then F^T is a form of degree n, where $T(X, Y) = (X + a, Y + b)$ is the translation mapping $(0, 0) \mapsto P$. Thus by the Corollary to Proposition 5 in Section 2.6 we may factor

$$F^T = F(X + a, Y + b) = \prod_{i=1}^{n} (c_i X + d_i Y).$$

Obesrve that $F = (F^T)^{T^{-1}}$ and thus

$$F = F^T(X - a, Y - b) = \prod_{i=1}^{n} (c_i(X - a) + d_i(Y - b)).$$

That is, F consists of n lines through P. □

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

Proof. Suppose $(0,0)$ is an ordinary double point on curve F of degree n. Then

$$F = F_n + F_{n-1} + \ldots + (c_1X + d_1Y)(c_2X + d_2Y).$$

Observe

$$F_{XY} = (F_n)_{XY}$$

□

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

3.6. Irreducible curves with given tangent lines L_i of multiplicity r_i may be constructed as follwos: if $\sum r_i = m$, let $F = \prod L_i^{r_i} + F_{m+1}$, where F_{m+1} is chose to make F irreducible (see Problem 2.34).

Proof. Clearly F has tangent lines L_i with multiplicity r_i. Moreover, $\prod L_i^{r_i}$ is a form of degree m. Thus if F_{m+1} is a form of degree $m+1$ such none of the L_i's are a factor of F_{m+1}, then F is irreducible by Problem 2.34. □

3.7. (a) Show that the real part of the curve E of the examples 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 equation 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 π/n is a linear transformation that takes the curve onto itself.)

(c) Analyze the singularities that 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 $\mathbb{A}^2(\mathbb{C})$.