Solutions to the book:
Fulton, Algebraic Curves

Meng-Gen Tsai
plover@gmail.com

March 17, 2021

Contents

Chapter 1: Affine Algebraic Sets

1.1. Algebraic Preliminaries

Problem 1.1.*

Let R be a domain.

(a) *If f, g are forms of degree r, s respectively in $R[x_1, \ldots, x_n]$, show that fg is a form of degree $r + s$.*

(b) *Show that any factor of a form in $R[x_1, \ldots, x_n]$ is also a form.*

Proof of (a).

(1) Write

$$f = \sum_{(i)} a_{(i)} x^{(i)},$$
$$g = \sum_{(j)} b_{(j)} x^{(j)},$$

where $\sum_{(i)}$ is the summation over $(i) = (i_1, \ldots, i_n)$ with $i_1 + \cdots + i_n = r$ and $\sum_{(j)}$ is the summation over $(j) = (j_1, \ldots, j_n)$ with $j_1 + \cdots + j_n = s$.

(2) Hence,

$$\begin{aligned} fg &= \sum_{(i)} \sum_{(j)} a_{(i)} b_{(j)} x^{(i)} x^{(j)} \\ &= \sum_{(i),(j)} a_{(i)} b_{(j)} x^{(k)} \end{aligned}$$

where $(k) = (i_1 + j_1, \ldots, i_n + j_n)$ with $(i_1 + j_1) + \cdots + (i_n + j_n) = r + s$. Each $x^{(k)}$ is the form of degree $r + s$ and $a_{(i)} b_{(j)} \in R$. Hence fg is a form of degree $r + s$.

□

Proof of (b).

(1) Given any form $f \in R[x_1, \ldots, x_n]$, and write $f = gh$. *It suffices to show that g is a form as well.* (So does h.)

(2) Write

$$g = g_0 + \cdots + g_r, \qquad h = h_0 + \cdots + h_s$$

where $g_r \neq 0$ and $h_s \neq 0$. So

$$f = gh = g_0 h_0 + \cdots + g_r h_s.$$

Since R is a domain, $R[x_1, \ldots, x_n]$ is a domain and thus $g_r h_s \neq 0$. The maximality of r and s implies that $\deg f = r + s$. Therefore, by the maximality of $r + s$, $f = g_r h_s$, or $g = g_r$, or g is a form.

$\square$

Problem 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.

(1) *Show that every element z of K may be written $z = a/b$, where a, $b \in R$ have no common factors.* Given any $z = a/b \in K$ where $a, b \in R$. Write

$$a = p_1 \cdots p_n,$$
$$b = q_1 \cdots q_m$$

where all $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible in R. (It is possible since R is a UFD.) For each i, suppose $p_i \mid q_j$ for some i, j. Write $q_j = p_i u$ for some $u \in R$. By the irreducibility of p_i and q_j, u is a unit. So

$$z = \frac{a}{b} = \frac{p_1 \cdots \widehat{p_i} \cdots p_n}{q_1 \cdots \widehat{q_j} \cdots q_m} = \frac{p_1 \cdots \widehat{p_i} \cdots p_n}{u q_1 \cdots \widehat{q_j} \cdots q_m}.$$

Continue this method we can write $z = \frac{a'}{b'}$ where a' and b' have no common factors.

(2) Write $z = a/b = a'/b'$ where

(a) $a, b, a', b' \in R$,

(b) a and b have no common factors,

(c) a' and b' have no common factors.

Write

$$a = p_1 \cdots p_n,$$
$$b = q_1 \cdots q_m,$$
$$a' = p'_1 \cdots p'_{n'},$$
$$b' = q'_1 \cdots q'_{m'}$$

where all $p_i, q_j, p'_{i'}, q'_{j'}$ are irreducible in R. As $z = a/b = a'/b'$, $ab' = a'b$ or

$$p_1 \cdots p_n q'_1 \cdots q'_{m'} = p'_1 \cdots p'_{n'} q_1 \cdots q_m.$$

(3) For $i = 1$, $p_1 = u_1 p'_{i'}$ for some unit $u_1 \in R$ since a and b have no common factors and all $p_1, q_j, p'_{i'}$ are irreducible. Hence

$$u_1 \widehat{p_1} p_2 \cdots p_n q'_1 \cdots q'_{m'} = p'_1 \cdots \widehat{p'_{i'}} \cdots p'_{n'} q_1 \cdots q_m.$$

Continue this method, we have $n \leq n'$ and all $p_1, \ldots, p_n$ are canceled.

(4) Conversely, we can apply the argument in (3) to $i' = 1, \ldots n'$ to conclude that $n' \leq n$. Therefore, $n = n'$ and

$$\underbrace{u_1 \cdots u_n}_{\text{a unit in } R} q'_1 \cdots q'_{m'} = q_1 \cdots q_m.$$

Hence, $b = ub'$ where $u = u_1 \cdots u_n$ is a unit in R. Similarly, $a = va'$ where v is a unit in R. So the representative of $z \in K$ is unique up to units of R.

□

Problem 1.3.*

Let R be a PID. Let $\mathfrak{p}$ be a nonzero, proper, prime ideal in R.

(a) *Show that $\mathfrak{p}$ is generated by an irreducible element.*

(b) *Show that $\mathfrak{p}$ is maximal.*

Proof of (a).

(1) Let $\mathfrak{p} = (a)$ be a nonzero, proper, prime ideal in R. It suffices to show that a is irreducible.

(2) Suppose $a = bc$. By the primality of $\mathfrak{p}$, $b \in \mathfrak{p}$ or $c \in \mathfrak{p}$. Suppose $b \in \mathfrak{p} = (a)$. (The case $c \in \mathfrak{p}$ is similar.) Then there is a $d \in R$ such that $b = ad$. Hence, $a = bc = adc$ or $(1 - dc)a = 0$.

(3) Since R is a domain, $1 = dc$ or $a = 0$. $a = 0$ implies that $\mathfrak{p} = (0)$ is a zero ideal, contrary to the assumption. Therefore, $1 = dc$, or c is a unit, or a is irreducible.

□

Proof of (b).

(1) Given any ideal $I = (b)$ of R containing $\mathfrak{p} = (a)$. As the generator a of $\mathfrak{p}$ is in $\mathfrak{p} \subseteq I$, there is some $c \in R$ such that $a = bc$. By the irreducibility of a (in (a)), b is a unit or c is a unit.

(2) b is a unit implies that $I = R$. c is a unit implies that $I = \mathfrak{p}$. In any case, we conclude that $\mathfrak{p}$ is maximal.

□

Problem 1.4.*

Let k be an infinite field, $f \in k[x_1, \ldots, x_n]$. Suppose $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. Show that $f = 0$. (Hint: Write

$$f = \sum f_i x_n^i, \qquad f_i \in k[x_1, \ldots, x_{n-1}].$$

Use induction on n, and the fact that $f(a_1, \ldots, a_{n-1}, x_n)$ has only a finite number of roots if any $f_i(a_1, \ldots, a_{n-1}) \neq 0$.)

Proof.

(1) Induction on n. The case $n = 1$. (Reductio ad absurdum) If there were a nonzero $f \in k[x_1]$ such that $f(a) = 0$ for all $a \in k$. Note that f has at most $\deg f < \infty$ roots, contrary to the infinity of k.

(2) Assume that the conclusion holds for $n-1$, then for any $f \in k[x_1, \ldots, x_n]$ we can write
$$f = \sum f_i x_n^i, \qquad f_i \in k[x_1, \ldots, x_{n-1}]$$
as $f \in (k[x_1, \ldots, x_{n-1}])[x_n]$. Suppose $f(a_1, \ldots, a_n) = 0$ for all $a_1, \ldots, a_n \in k$. For fixed $a_1, \ldots, a_{n-1}$, the polynomial $f(a_1, \ldots, a_{n-1}, x_n) \in k[x_n]$ has all distinct roots in an infinite field k. By (1), $f(a_1, \ldots, a_{n-1}, x_n) = 0 \in k[x_n]$, or each $f_i(a_1, \ldots, a_{n-1}) = 0$. As all $a_1, \ldots, a_{n-1}$ run over k, we can apply the induction hypothesis each $f_i(x_1, \ldots, x_{n-1}) = 0 \in k[x_1, \ldots, x_{n-1}]$. Hence, $f = 0 \in k[x_1, \ldots, x_n]$.

□

Note. If k is a finite field of order $q = p^k$, then the polynomial $f(x) = x^q - x$ has q distinct roots in k.

Problem 1.5.*

Let k be any field. Show that there are an infinitely number of irreducible monic polynomials in $k[x]$. (Hint: Suppose $f_1, \dots, f_n$ were all of them, and factor $f_1 \cdots f_n + 1$ into irreducible factors.)

Proof (Due to Euclid).

(1) If $f_1, \dots, f_n$ were all irreducible monic polynomials, then we consider

$$g = f_1 \cdots f_n + 1 \in k[x].$$

So there is an irreducible monic polynomial $f = f_i$ dividing g for some i since

$$\deg g = \deg f_1 + \cdots + \deg f_n \geq 1$$

and $k[x]$ is a UFD.

(2) However, f would divide the difference

$$g - f_1 \cdots f_{i-1} f_i f_{i+1} \cdots f_n = 1,$$

contrary to $\deg f_i \geq 1$.

□

Problem 1.6.*

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

Proof (Due to Euclid).

(1) Let k be an algebraically closed field. If $a_1, \dots, a_n$ were all elements in k, then we consider a monic polynomials

$$f(x) = (x - a_1) \cdots (x - a_n) + 1 \in k[x].$$

(2) Since k is algebraically closed, there is an element $a \in k$ such that $f(a) = 0$. By assumption, $a = a_i$ for some $1 \leq i \leq n$, and thus $f(a) = f(a_i) = 1$, contrary to the fact that a field is a commutative ring where $0 \neq 1$ and all nonzero elements are invertible.

□

Problem 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*

$$f = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}, \qquad \lambda_{(i)} \in k.$$

(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 of (a).

(1) Regard $k[x_1, \ldots, x_n]$ as $(k[x_1, \ldots, x_{n-1}])[x_n]$. Since $(k[x_1, \ldots, x_{n-1}])[x_n]$ is a Euclidean domain with a function

$$f \in (k[x_1, \ldots, x_{n-1}])[x_n] \mapsto \deg_{x_n} f \in \mathbb{Z}_{\geq 0}$$

satisfying the division-with-remainder property.

(2) Apply the division algorithm for f and nonzero $x_n - a_n$ to produce a quotient q and remainder r with $f = (x_n - a_n)q + r$ and either $r = 0$ or $\deg_{x_n}(r) < \deg_{x_n}(x_n - a_n) = 1$. That is, $r \in k[x_1, \ldots, x_{n-1}]$ is a constant in $(k[x_1, \ldots, x_{n-1}])[x_n]$. Continue this process to get that f is of the form

$$f = \sum_{i_n} f_{i_n} (x_n - a_n)^{i_n}$$

where $f_{i_n} \in k[x_1, \ldots, x_{n-1}]$.

(3) Use the same argument in (2) for each $f_{i_n} \in k[x_1, \ldots, x_{n-1}]$, we have

$$\begin{aligned}
f_{i_n} &= \sum_{i_{n-1}} \underbrace{f_{i_n, i_{n-1}}}_{\in k[x_1, \ldots, x_{n-2}]} (x_{n-1} - a_{n-1})^{i_{n-1}} \\
f_{i_n, i_{n-1}} &= \sum_{i_{n-2}} \underbrace{f_{i_n, i_{n-1}, i_{n-2}}}_{\in k[x_1, \ldots, x_{n-3}]} (x_{n-2} - a_{n-2})^{i_{n-2}}, \\
&\cdots \\
f_{i_n, \ldots, i_2} &= \sum_{i_1} \underbrace{f_{i_n, \ldots, i_1}}_{\in k} (x_1 - a_1)^{i_1}.
\end{aligned}$$

Note that $f_{i_n, \ldots, i_1} \in k$, we can write

$$f = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}, \qquad \lambda_{(i)} \in k.$$

by replacing all $f_{i_n, \ldots, i_k}$ by $f_{i_n, \ldots, i_{k-1}}$ for $k = n, n-1, \ldots, 2$.

(4) Or use the induction on n.

$\square$

Proof of (b).

(1) Write
$$f = \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}, \qquad \lambda_{(i)} \in k$$
by (a).

(2) As $f(a_1, \cdots, a_n) = 0$, $\lambda_{(i)} = 0$ if all $i_1, \ldots, i_n$ are zero, that it, there is no nonzero constant term in the representation of f. Hence, for each term
$$f_{(i)} := \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}$$
with $\lambda_{(i)} \neq 0$, there exists one $i_k > 0$ for some $1 \leq k \leq n$. So we can write
$$f_{(i)} = (x_k - a_k)\underbrace{\left(\lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_k - a_k)^{i_k - 1} \cdots (x_n - a_n)^{i_n}\right)}_{:= g_{(i)} \in k[x_1, \ldots, x_n]}.$$
Note that the expression of $f_{(i)}$ is not unique since there may exist more than one $i_k > 0$ as $1 \leq k \leq n$.

(3) Now we iterate each nonzero term in f, apply the factorization in (2), and then group by each $x_k - a_k$. Therefore, we can write
$$f = \sum_{i=1}^{n}(x_i - a_i)g_i$$
for some $g_1 \in k[x_1, \ldots, x_n]$.

(4) The expression of f is not unique. For example, take $f(x, y) = x^2 + 2xy + y^2 \in k[x, y]$. As $f(0, 0) = 0$, we can write
$$\begin{aligned} f(x, y) &= x \cdot \underbrace{(x + 2y)}_{g_1} + y \cdot \underbrace{y}_{g_2}, \text{ or} \\ &= x \cdot \underbrace{(x + y)}_{g_1} + y \cdot \underbrace{(x + y)}_{g_2}, \text{ or} \\ &= x \cdot \underbrace{x}_{g_1} + y \cdot \underbrace{(2x + y)}_{g_2}. \end{aligned}$$

$\square$

1.2. Affine Space and Algebraic Sets

Problem 1.8.*

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

Proof.

(1) *Show that* $k[x]$ *is a PID if* k *is a field.*

   (a) Let I be an ideal of $k[x]$.

   (b) If $I = \{0\}$ then $I = (0)$ and I is principal.

   (c) If $I \neq \{0\}$, then take f to be a polynomial of minimal degree in I. It suffices to show that $I = (f)$. Clearly, $(f) \subseteq I$ since I is an ideal. Conversely, for any $g \in I$,

   $$g(x) = f(x)h(x) + r(x)$$

   for some $h, r \in k[x]$ with $r = 0$ or $\deg r < \deg f$ (as $k[x]$ is a Euclidean domain). Now as

   $$r = g - fh \in I,$$

   $r = 0$ (otherwise contrary to the minimality of f), we have $g = fh \in (f)$ for all $g \in I$.

(2) Let Y be an algebraic subset of $\mathbf{A}^1(k)$, say $Y = V(I)$ for some ideal I of $k[x]$. Since $k[x]$ is a PID, $I = (f)$ for some $f \in k[x]$.

   (a) If $f = 0$, then $I = (0)$ and $Y = V(0) = \mathbf{A}^1(k)$.

   (b) If $f \neq 0$, then $f(x) = 0$ has finitely many roots in k, say $a_1, \ldots, a_m \in k$. Hence,

   $$Y = V(I) = V(f) = \{f(a) = 0 : a \in k\} = \{a_1, \ldots, a_m\}$$

   is a finite subsets of $\mathbf{A}^1(k)$.

   By (a)(b), the result is established.

□

Notes.

(1) By the Hilbert basis theorem, $k[x]$ is Noetherian as k is Noetherian. Hence, for any algebraic subset $Y = V(I)$ of $\mathbf{A}^1(k)$, we can write $I = (f_1, \cdots, f_m)$. Note that

   $$Y = V(I) = V(f_1) \cap \cdots \cap V(f_m).$$

   Now apply the same argument to get the same conclusion.

(2) Suppose $k = \overline{k}$. $\mathbf{A}^1(k)$ is irreducible, because its only proper closed subsets are finite, yet it is infinite (because k is algebraically closed, hence infinite).

Problem 1.9.

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

Proof.

(1) Every subset of $\mathbf{A}^n(k)$ is finite since $|\mathbf{A}^n(k)| = |k|^n$ is finite.

(2) Note that $V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\} \subseteq \mathbf{A}^n(k)$ (property (5) in this section) and any finite union of algebraic sets is algebraic (property (4) in this section). Thus, every subset of $\mathbf{A}^n(k)$ is algebraic (by (1)).

$\square$

Problem 1.10.

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

Proof.

(1) Let $k = \mathbb{Q}$ be an infinite field. $V(x - a) = \{a\}$ is an algebraic sets for all $a \in \mathbb{Q}$. In particular, $V(x - a) = \{a\}$ is algebraic for all $a \in \mathbb{Z}$.

(2) Note that
$$Y := \bigcup_{a \in \mathbb{Z}} V(x - a) = \mathbb{Z}$$
is a countable union of algebraic sets. Since Y is a proper subset of $k = \mathbb{Q}$, it cannot be algebraic by Problem 1.8.

$\square$

Problem 1.11.

Show that the following are algebraic sets:

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

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

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

Proof of (a).

(1) The twisted cubic curve

$$Y = \{(t, t^2, t^3) \in \mathbf{A}^3(k) : t \in k\} = V(x^2 - y) \cap V(x^3 - z)$$

is algebraic. We say that Y is given by the parametric representation $x = t$, $y = t^2$, $z = t^3$.

(2) The generators for the ideal $I(Y)$ are $x^2 - y$ and $x^3 - z$.

(3) Y is an affine variety of dimension 1.

(4) The affine coordinate ring $A(Y)$ is isomorphic to a polynomial ring in one variable over k.

$\square$

Proof of (b). The circle

$$\{(\cos(t), \sin(t)) \in \mathbf{A}^2(\mathbb{R}) : t \in \mathbb{R}\} = V(x^2 - y^2 - 1)$$

is algebraic. $\square$

Proof of (c). The circle

$$\{(r, \theta) : r = \sin(\theta)\} = V(x^2 + y^2 - y)$$

is algebraic again. $\square$

Problem 1.12.

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

Proof.

(1) Say $L = V(y - (ax + b))$ be a line in $\mathbb{A}^2(k)$. (The case $L = V(x - (ay + b))$ is similar.)

(2) Note that $L \not\subseteq C$ implies that $(y - (ax + b)) \nmid f$. Hence, the polynomial

$$g : x \mapsto f(x, ax + b) \in k[x]$$

is nonzero and $\deg g \leq n$. Therefore, the number of roots of g in k is no more than n.

(3) Hence,

$$\begin{aligned}
L \cap C &= V(y-(ax+b)) \cap V(f) \\
&= \{(x,y) \in \mathbb{A}^2(k) : y = ax+b \text{ and } f(x,y)=0\} \\
&= \{(x,y) \in \mathbb{A}^2(k) : f(x,ax+b)=0\}
\end{aligned}$$

is finite of no more than n points.

□

Problem 1.13.

Show that each of the following sets is not algebraic:

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

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

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

Proof of (a).

(1) (Reductio ad absurdum) If

$$Y := \{(x,y) \in \mathbf{A}^2(\mathbb{R}) : y = \sin(x)\}$$

were algebraic, then there is a subset S of $\mathbb{R}[x,y]$ such that

$$Y = V(S) = \bigcap_{f \in S} V(f).$$

(2) $S \neq \varnothing$ since $Y \neq \mathbf{A}^2(\mathbb{R})$. ($(89,64) \in \mathbf{A}^2(\mathbb{R}) - Y$.)

(3) Take a fixed line $L = V(y)$ in $\mathbf{A}^2(\mathbb{R})$. For each affine curve $f \in S$, we have

$$V(f) \cap L \supseteq \bigcap_{f \in S} V(f) \cap L = Y \cap L = \{(n\pi, 0) \in \mathbf{A}^2(\mathbb{R}) : n \in \mathbb{Z}\},$$

which is infinite. By problem 1.12, $y \mid f$. As f runs over S, $Y \subseteq V(y) = L$, contradicts that $\left(0, \frac{\pi}{2}\right) \in L - Y$.

□

Proof of (b).

(1) Similar to (a). (Reductio ad absurdum) If

$$Y := \{(x,y) \in \mathbf{A}^2(\mathbb{C}) : |x|^2 + |y|^2 = 1\}$$

were algebraic, then there is a subset S of $\mathbb{C}[x,y]$ such that

$$Y = V(S) = \bigcap_{f \in S} V(f).$$

(2) $S \neq \varnothing$ since $Y \neq \mathbf{A}^2(\mathbb{C})$. ($(89, 64) \in \mathbf{A}^2(\mathbb{C}) - Y$.)

(3) Take a fixed line $L = V(x)$ in $\mathbf{A}^2(\mathbb{C})$. For each affine curve $f \in S$, we have

$$V(f) \cap L \supseteq \bigcap_{f \in S} V(f) \cap L = Y \cap L = \{(0,y) \in \mathbf{A}^2(\mathbb{C}) : |y| = 1\},$$

which is infinite (since Y contains a unit circle in the complex plane). By problem 1.12, $x \mid f$. As f runs over S, $Y \subseteq V(x) = L$, contradicts that the origin $(0,0) \in L - Y$.

$\square$

Proof of (c).

(1) Similar to (a) and (b).

(2) *Suppose C is an affine plane curve, and L is a line in $\mathbb{A}^3(k)$, $L \not\subseteq C$. Suppose $C = V(f)$, $f \in k[x,y,z]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points.* The proof is similar to Problem 1.12.

  (a) Say $L = V(y - (ax+b), z - (cx+d))$ be a line in $\mathbb{A}^3(k)$.

  (b) Note that $L \not\subseteq C$ implies that $(y-(ax+b)) \nmid f$ and $(z-(cx+d)) \nmid f$. Hence, the polynomial

$$g : x \mapsto f(x, ax+b, cx+d) \in k[x]$$

  is nonzero and $\deg g \leq n$. Therefore, the number of roots of g in k is no more than n.

  (c) Hence,

$$\begin{aligned} L \cap C &= V(y - (ax+b), z - (cx+d)) \cap V(f) \\ &= \{(x,y) \in \mathbb{A}^2(k) : y = ax+b, z = cx+d \text{ and } f(x,y) = 0\} \\ &= \{(x,y) \in \mathbb{A}^2(k) : f(x, ax+b, cx+d) = 0\} \end{aligned}$$

  is finite of no more than n points.

(3) (Reductio ad absurdum) If

$$Y := \{(\cos(t), \sin(t), t) \in \mathbf{A}^3(\mathbb{R}) : t \in \mathbb{R}\}$$

were algebraic, then there is a subset S of $\mathbb{R}[x, y, z]$ such that

$$Y = V(S) = \bigcap_{f \in S} V(f).$$

(4) $S \neq \varnothing$ since $Y \neq \mathbf{A}^3(\mathbb{R})$. ($(1989, 6, 4) \in \mathbf{A}^3(\mathbb{R}) - Y$.)

(5) Take a fixed line $L = V(x-1, y)$ in $\mathbf{A}^3(\mathbb{R})$. For each affine curve $f \in S$, we have

$$V(f) \cap L \supseteq \bigcap_{f \in S} V(f) \cap L = Y \cap L = \{(1, 0, 2n\pi) \in \mathbf{A}^3(\mathbb{R}) : n \in \mathbb{Z}\},$$

which is infinite. By (2), $(x-1) \mid f$ and $y \mid f$. As f runs over S, $Y \subseteq V(x-1, y) = L$, contradicts that $(1, 0, \pi) \in L - Y$.

□

Supplement. *A circular disk of radius* 1 *in the plane xy rolls without slipping along the x axis. The figure described by a point of the circumference of of the disk is called a **cycloid**. The parametrized curve $\alpha : \mathbb{R} \to \mathbb{R}^2$ is*

$$\begin{cases} x = t - \sin t \\ y = 1 - \cos t. \end{cases}$$

The cycloid is not algebraic (as (a)).

Problem 1.14.*

Let f be a nonconstant polynomial in $k[x_1, \ldots, x_n]$, k algebraically closed. Show that $\mathbf{A}^n(k) - V(f)$ is infinite if $n \geq 1$, and $V(f)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite. (Hint: See Problem 1.4.)

Proof.

(1) *Show that $\mathbf{A}^n(k) - V(f)$ is infinite if $n \geq 1$.* Since f is a nonconstant polynomial in $k[x_1, \ldots, x_n]$, we may assume that $\deg_{x_n}(f) > 0$. Hence

$$x_n \mapsto f(1, \ldots, 1, x_n)$$

is a nonconstant polynomial of degree $\deg_{x_n}(f) > 0$ in $k[x_n]$. So f has finitely many roots in k, say $\xi_1, \ldots, \xi_m$ ($m \geq 0$). Hence,

$$(1, \ldots, 1, x_n) \neq 0$$

whenever $x_n \neq \xi_m$. Such subset in $\mathbf{A}^1(k)$ is infinite since $k = \overline{k}$ (Problem 1.6). Therefore,

$$\begin{aligned}\mathbf{A}^n(k) - V(f) &= \{(a_1, \ldots, a_n) \in \mathbf{A}^n(k) : f(a_1, \ldots, a_n) \neq 0\} \\ &\supseteq \{a_n \in \mathbf{A}^1(k) : f(1, \ldots, 1, x_n) \neq 0\}\end{aligned}$$

is infinite.

(2) *Show that $V(f)$ is infinite if $n \geq 2$.*

(a) Similar to (1). Since f is a nonconstant polynomial in $k[x_1, \ldots, x_n]$, we may assume that $m := \deg_{x_n}(f) > 0$. Write

$$f = \sum_{i=0}^{m} f_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Note that each f_i is well-defined since $n \geq 2$.

(b) If f_n is constant in $k[x_1, \ldots, x_{n-1}]$, then f_n is nonzero (since $m > 0$) or $V(f_n) = \varnothing$. If f_n is nonconstant in $k[x_1, \ldots, x_{n-1}]$, then the set $\mathbf{A}^{n-1}(k) - V(f_n)$ is infinite by (1). In any case,

$$\mathbf{A}^{n-1}(k) - V(f_n)$$

is infinite.

(c) For each $P = (a_1, \ldots, a_{n-1}) \in \mathbf{A}^{n-1}(k) - V(f_n)$,

$$g_P : x_n \mapsto f(P, x_n) = f(a_1, \ldots, a_{n-1}, x_n)$$

defines a polynomial in $k[x_n]$ of degree $m > 0$. Since $k = \overline{k}$, g_P has at least one root $Q \in k$. Hence

$$V(f) \supseteq \{(P, Q) \in \mathbf{A}^n(k) : P \in \mathbf{A}^{n-1}(k) - V(f_n), g_P(Q) = 0\}$$

is infinite since the set $\mathbf{A}^{n-1}(k) - V(f_n)$ is infinite.

Note. It is not true if $k \neq \overline{k}$. For example, $V(x^2 + y^2 + 1) = \varnothing$ in $\mathbf{A}^2(\mathbb{R})$.

(3) Note that

$$\mathbf{A}^n(k) - V(S) = \mathbf{A}^n(k) - \bigcap_{f \in S} V(f) = \bigcup_{f \in S} (\mathbf{A}^n(k) - V(f)).$$

Thus the complement of any proper algebraic set is infinite by (1).

□

Problem 1.15.*

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

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

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

Proof.

(1) Write

$$\begin{aligned} V = V(S_V) &= \{P \in \mathbf{A}^n(k) : f(P) = 0\, \forall f \in S_V\} \\ W = V(S_W) &= \{Q \in \mathbf{A}^m(k) : g(Q) = 0\, \forall g \in S_W\}, \end{aligned}$$

where $S_V \subseteq k[x_1, \ldots, x_n]$ and $S_W \subseteq k[y_1, \ldots, y_m]$. It suffices to show that

$$V \times W = V(S),$$

where $S \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ is the union of S_V and S_W.

(2) Here we can identify S_V with the subset of $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ by noting that

$$k[x_1, \ldots, x_n] \hookrightarrow (k[y_1, \ldots, y_m])[x_1, \ldots, x_n] = k[x_1, \ldots, x_n, y_1, \ldots, y_m].$$

Here we regard k as a subring of $k[y_1, \ldots, y_m]$. Similar treatment to S_W.

(3) By construction, $V \times W \subseteq V(S)$. Conversely, given any $(P, Q) \in V(S) \subseteq \mathbf{A}^{n+m}(k)$, we have $h(P, Q) = 0$ for all $h \in S = S_V \cup S_W$ (by (2)). By construction, $f(P) = 0$ for all $f \in S_V$ since f only involve $x_1, \ldots, x_n$. Hence, $P \in V$. Similarly, $Q \in W$. Therefore, $(P, Q) \in V \times W$.

□

1.3. The Ideal of a Set of Points

Problem 1.16.*

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

Proof.

(1) (Proof of Equation (6) in this section.) *Show that if $X \subseteq Y$, then $I(X) \supseteq I(Y)$.* If $f \in I(Y)$ then $f(P) = 0$ for all $P \in Y$. So $f(P) = 0$ for all $P \in X \subseteq Y$ or $f \in I(X)$.

(2) (Proof of Equation (8) in this section.) *$I(V(S)) \supseteq S$ for any set S of polynomials; $V(I(X)) \supseteq X$ for any set X of points.*

   (a) If $f \in S$ then f vanishes on $V(S)$, hence $f \in IV(S)$.

   (b) If $P \in X$ then every polynomial in $I(X)$ vanishes at P, so P belongs to the zero set of $I(X)$.

(3) (Proof of Equation (9) in this section.) *$V(I(V(S))) = V(S)$ 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, $I = I(V(I))$.*

   (a) In each case, it suffices to show that the left side is a subset of the right side. (by Equations (6)(8) in this section).

   (b) If $P \in V(S)$ then $f(P) = 0$ for all $f \in I(V(S))$, so $P \in V(I(V(S)))$.

   (c) If $f \in I(X)$ then $f(P) = 0$ for all $P \in V(I(X))$. Thus f vanishes on $V(I(X))$, so $f \in I(V(I(X)))$.

(4) *Show that $V = W$ if and only if $I(V) = I(W)$.*

   (a) By Equation (6) in this section, $I(V) \supseteq I(W)$ if $V \subseteq W$ and $I(V) \subseteq I(W)$ if $V \supseteq W$. Thus, $I(V) = I(W)$ if $V = W$.

   (b) Conversely, $I(V) = I(W)$ implies that $V(I(V)) = V(I(W))$ by Equation (3) in the previous section and similar argument in (a). By Equation (9) in this section, $V(I(V)) = V$ and $V(I(W)) = W$. Thus, $V = W$.

□

Problem 1.17.*

(a) *Let V be an algebraic set in $\mathbf{A}^n(k)$, $P \in \mathbf{A}^n(k)$ a point not in V. Show that there is a polynomial $f \in k[x_1, \dots, x_n]$ such that $f(Q) = 0$ for all $Q \in V$, but $f(P) = 1$. (Hint: $I(V) \neq I(V \cup \{P\})$.)*

(b) *Let $P_1, \dots, P_r$ be distinct points in $\mathbf{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $f_1, \dots, f_r \in I(V)$ such that $f_i(P_j) = 0$ if $i \neq j$, and $f_i(P_i) = 1$. (Hint: Apply (a) to the union of V and all but one point.)*

(c) *With $P_1, \dots, P_r$ and V as in (b), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $g_i \in I(V)$ with $g_i(P_j) = a_{ij}$ for all i and j. (Hint: Consider $\sum_j a_{ij} f_j$.)*

Proof of (a).

(1) Since $I(V) \supsetneq I(V \cup \{P\})$ (by Problem 1.16), there is a polynomial $f \in k[x_1, \ldots, x_n]$ such that $f(Q) = 0$ for all $Q \in V$, but $f(P) \neq 0$.

(2) Since k is a field, $(f(P))^{-1} \in k$. Consider the polynomial $(f(P))^{-1} f \in k[x_1, \ldots, x_n]$. It is well-defined. Also, $((f(P))^{-1} f)(Q) = (f(P))^{-1} f(Q) = 0$ for all $Q \in V$, but $(f(P))^{-1} f)(P) = (f(P))^{-1} f(P) = 1$.

□

Proof of (b).

(1) For $1 \leq i \leq$, define

$$W = V \cup \{P_1, \ldots, P_r\}$$
$$W_i = V \cup \{P_1, \ldots, \widehat{P}_i, \ldots, P_r\}.$$

Here $W = W_i \cup \{P_i\} \neq W_i$.

(2) By (a), there is a polynomial $f_i \in k[x_1, \ldots, x_n]$ such that $f_i(Q) = 0$ for all $Q \in W_i$, but $f_i(P_i) = 1$. Here $f_i \in I(V)$ and $f_i(P_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta.

□

Proof of (c).

(1) For each $1 \leq i \leq r$, define

$$g_i = \sum_j a_{ij} f_j \in k[x_1, \ldots, x_n].$$

(2) $g_i \in I(V)$ since g_i is a linear combination of f_j and $I(V)$ is an ideal.

(3) Also,

$$g_i(P_j) = \sum_{j'} a_{ij'} f_{j'}(P_j) = \sum_{j'} a_{ij'} \delta_{j'j} = a_{ij}.$$

□

Problem 1.18.*

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

Proof.

(1) *Show that* $(a+b)^{n+m} \in I$ *if* $a^n \in I$, $b^m \in I$. By the binomial theorem,

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

For each term $a^i b^{n+m-i}$, either $i \geq n$ holds or $n+m-i \geq m$ holds, and thus $a^i b^{n+m-i} \in I$ (since $a^n \in I$, $b^m \in I$ and I is an ideal). Hence, the result is established.

(2) *Show that* $\mathrm{rad}(I)$ *is an ideal.*

  (a) $0 \in \mathrm{rad}(I)$ since $0 = 0^1 \in I$ for any ideal in R.
  (b) $(a+b)^{n+m} \in I$ if $a^n \in I$, $b^m \in I$ by (1).
  (c) $(-a)^{2n} = (a^n)^2 \in I$ if $a^n \in I$ (since I is an ideal).
  (d) $(ra)^n = r^n a^n \in I$ if $a^n \in I$ and $r \in R$ (since I is an ideal and R is commutative).

(3) *Show that* $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$. It suffices to show $\mathrm{rad}(\mathrm{rad}(I)) \subseteq \mathrm{rad}(I)$. Given any $a \in \mathrm{rad}(\mathrm{rad}(I))$. By definition $a^n \in \mathrm{rad}(I)$ for some positive integer n. Again by definition $(a^n)^m = a^{nm} \in I$ for some positive integer m. As nm is a postive integer, $a \in \mathrm{rad}(I)$.

(4) *Show that every prime ideal* $\mathfrak{p}$ *is radical.* Given any $a \in \mathrm{rad}(\mathfrak{p})$, that is, $a^n \in \mathfrak{p}$ for some positive integer. Write $a^n = aa^{n-1}$ if $n > 1$. By the primality of $\mathfrak{p}$, $a \in \mathfrak{p}$ or $a^{n-1} \in \mathfrak{p}$. If $a \in \mathfrak{p}$, we are done. If $a^{n-1} \in \mathfrak{p}$, we continue this descending argument (or the mathematical induction) until the power of a is equal to 1. Hence $\mathfrak{p}$ is radical.

□

Problem 1.19.

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

Proof.

(1) *Show that* $I = (x^2+1)$ *is a prime ideal in* $\mathbb{R}[x]$. Given any $fg \in I$. It suffices to show that $f \in I$ or $g \in I$. By definition of I, there is a polynomial $h \in \mathbb{R}[x]$ such that $fg = (x^2+1)h$. So $(x^2+1) \mid f$ or $(x^2+1) \mid g$ since x^2+1 is irreducible in a unique factorization domain $\mathbb{R}[x]$. Therefore, $f \in I$ or $g \in I$.

(2) *Show that* I *is not the ideal of any set in* $\mathbf{A}^1(\mathbb{R})$. Since x^2+1 has no roots in $\mathbb{R}$, I cannot be the ideal of any nonempty set in $\mathbf{A}^1(\mathbb{R})$. Besides, $I(\varnothing) = (1) \neq (x^2+1)$.

□

Problem 1.20.*

Show that for any ideal I in $k[x_1, \ldots, x_n]$, $V(I) = V(\mathrm{rad}(I))$, and $\mathrm{rad}(I) \subseteq I(V(I))$.

Proof.

(1) *Show that $V(I) = V(\mathrm{rad}(I))$.* Since $I \subseteq \mathrm{rad}(I)$, it suffices to show that $V(I) \subseteq V(\mathrm{rad}(I))$. Given any $P \in V(I)$. For any $f \in \mathrm{rad}(I)$, $f^n \in I$ for some positive integer $n > 0$. Note that

$$0 = (f^n)(P) = f(P)^n$$

since $f^n \in I$ and $P \in V(I)$. As k is a domain, $f(P)^n = 0$ implies $f(P) = 0$. So $P \in V(\mathrm{rad}(I))$.

(2) By Equations (6) and (8) in this section,

$$I(V(I)) = I(V(\mathrm{rad}(I))) \supseteq \mathrm{rad}(I).$$

□

Note.

(1) By the Hilbert's Nullstellensatz, $I(V(I)) = \mathrm{rad}(I)$ if $k = \overline{k}$.

(2) Take $I = (x^2 + 1)$ as an ideal in $\mathbb{R}[x]$. Note that $I(V(I)) = I(\varnothing) = (1)$ and $\mathrm{rad}(I) = I = (x^2 + 1)$. So the equality in $\mathrm{rad}(I) \subsetneq I(V(I))$ might not hold if $k \neq \overline{k}$. (See Problem 1.19.)

Problem 1.21.*

Show that $I = (x_1 - a_1, \ldots, x_n - a_n) \subseteq k[x_1, \ldots, x_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[x_1, \ldots, x_n]/I$ is an isomorphism.

Proof.

(1) *Show that I is a maximal ideal.* Suppose that J is an ideal such that $J \supsetneq I$. Take any $f \in J - I$. By Problem 1.7(a),

$$f = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}.$$

As $f \notin I$, there is a nonzero constant term in f, say $\lambda \in k - \{0\}$. Note that $f - \lambda \in I \subsetneq J$. Hence,

$$\lambda = f - (f - \lambda) \in J$$

since J is an ideal. As $\lambda \neq 0$, $J = k[x_1, \ldots, x_n]$ is not a proper ideal containing I.

(2) Let $\varphi : k \to k[x_1, \ldots, x_n]/I$ be the natural homomorphism. (That is, $\varphi : \lambda \to \lambda + I \in k[x_1, \ldots, x_n]/I$.)

(3) *Show that φ is surjective.* Given any $f + I \in k[x_1, \ldots, x_n]/I$. By Problem 1.7(a),

$$f = \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}.$$

So

$$\begin{aligned} f + I &= \sum \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} + I \\ &= \left(f(a_1, \ldots, a_n) + \sum_{\text{nonconstant}} \lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \right) + I \\ &= f(a_1, \ldots, a_n) + I. \end{aligned}$$

(Here the summation over all nonconstant terms is in I.) Hence

$$\varphi : f(a_1, \ldots, a_n) \in k \mapsto f + I.$$

(4) *Show that φ is injective.* $\ker(\varphi) = \{\lambda \in k : \lambda \in I\} = k \cap I = \{0\}$ since I is a proper ideal.

(5) By (2)(3)(4), $\varphi : k \to k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)$ is an isomorphism.

□

1.4. The Hilbert Basis Theorem

Problem 1.22.*

Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism.

(a) *Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containing I, and for every ideal J of R containing I, $\pi(J) = J'$ is an ideal of R/I. This sets up a natural one-to-one correspondence between $\{$ideals of $R/I\}$ and $\{$ideals of R that contain $I\}$.*

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

(c) *Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[x_1, \dots, x_n]/I$ is Noetherian.*

Proof of (a).

(1) *Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containing I.*

   (a) *Show that J contains I.* Note that $\pi^{-1}(0) = I \subseteq \pi^{-1}(J') = J$. So J contains I. In particular, $J \neq \varnothing$ since $I \neq \varnothing$.

   (b) *Show that J is a additive subgroup of R.* It suffices to show that $a - b \in J$ for any $a \in J$ and $b \in J$. Actually,

   $$\pi(a-b) = \pi(a) - \pi(b) \in J'$$

   implies $a - b \in \pi^{-1}(J') = J$.

   (c) *Show that for every $r \in R$ and every $a \in J$, the product $ra \in J$.* In fact,

   $$\pi(ra) = \pi(r)\pi(a) \in J'$$

   implies $ra \in \pi^{-1}(J') = J$.

(2) *Show that for every ideal J of R containing I, $\pi(J) = J'$ is an ideal of R/I.*

   (a) *Show that J' is nonempty.* Note that $\pi(a) = 0 \in \pi(I) \subseteq \pi(J) = J'$ for any $a \in I$. So J' is nonempty since J is nonempty.

   (b) *Show that J' is a additive subgroup of R/I.* It suffices to show that $\pi(a) - \pi(b) \in J'$ for any $\pi(a) \in J'$, $\pi(b) \in J'$, $a \in J$ and $b \in J$. It is trivial since

   $$\pi(a) - \pi(b) = \pi(a-b) \in \pi(J) = J',$$

   π is a ring homomorphism and J is an ideal.

   (c) *Show that for every $\pi(r) \in R/I$ ($r \in R$) and every $\pi(a) \in J'$ ($a \in J$), the product $\pi(r)\pi(a) \in J'$.* It is trivial since

   $$\pi(r)\pi(a) = \pi(ra) \in \pi(J) = J',$$

   π is a ring homomorphism and J is an ideal.

(3) By (1)(2), we setup the correspondence between

$$\{\text{ideals of } R/I\} \longleftrightarrow \{\text{ideals of } R \text{ that contain } I\}.$$

Note that this correspondence preserves the subset relation, and thus this correspondence is one-to-one.

□

Proof of (b).

(1) *Show that J' is radical if J is radical.* It suffices to show that $(a+I)^n = a^n + I \in J'$ implies that $a + I \in J'$. Note that

$$(a+I)^n = a^n + I \in J'$$

implies that $a^n \in J$ or $a \in J$ since J is radical. Hence $a + I \in J/I = J'$.

(2) *Show that J is radical if J' is radical.* It suffices to show that $a^n \in J$ implies that $a \in J$. Note that

$$\pi(a^n) = \pi(a)^n \in J'$$

implies that $\pi(a) \in J'$ since J' is radical. $a \in \pi^{-1}(J') = J$.

(3) *Show that J' is prime if J is prime.* It suffices to show that $(a+I)(b+I) = ab + I \in J'$ implies that $a + I \in J'$ or $b + I \in J'$. Note that

$$(a+I)(b+I) = ab + I \in J'$$

implies that $ab \in J$. So $a \in J$ or $b \in J$ by the primality of J. Hence $a + I \in J'$ or $b + I \in J'$.

(4) *Show that J is prime if J' is prime.* It suffices to show that $ab \in J$ implies that $a \in J$ or $b \in J$. Note that

$$\pi(ab) = \pi(a)\pi(b) \in J'$$

implies that $\pi(a) \in J'$ or $\pi(b) \in J'$ by the primality of J'. So $a \in \pi^{-1}(J') = J$ or $b \in \pi^{-1}(J') = J$.

(5) *Show that J' is maximal if J is maximal.* Suppose $\mathfrak{m}$ is an ideal containing J'. By (a), $\pi^{-1}(\mathfrak{m})$ is an ideal containing J. So $\pi^{-1}(\mathfrak{m}) = J$ or $\pi^{-1}(\mathfrak{m}) = R$ by the maximality of J. Hence, $\mathfrak{m} = \pi(J) = J'$ or $\mathfrak{m} = \pi(R) = R/I$.

(6) *Show that J is maximal if J' is maximal.* Suppose $\mathfrak{m}$ is an ideal containing J. By (a), $\pi(\mathfrak{m})$ is an ideal containing J'. So $\pi(\mathfrak{m}) = J'$ or $\pi(\mathfrak{m}) = R/I$ by the maximality of J'. Hence, $\mathfrak{m} = \pi^{-1}(J') = J$ or $\mathfrak{m} = \pi^{-1}(R/I) = R$.

□

Note.

(1) Note that

$$R/J \cong (R/I)/(J/I)$$

if J is an ideal of R such that $I \subseteq J$.

(2) Hence, J is prime iff $R/J \cong (R/I)/(J/I)$ is a domain iff J/I is prime.

(3) Also, J is maximal iff $R/J \cong (R/I)/(J/I)$ is a field iff J/I is maximal.

Proof of (c).

(1) *Show that J' is finitely generated if J is.* Suppose J is generated by $a_1, \ldots, a_m$. It suffices to show that J' is generated by

$$a_1 + I, \ldots, a_m + I \in J/I.$$

Given any $a + I \in J'$ where $a \in J$. Write $a = \sum_{1 \leq i \leq m} r_i a_i$ for some $r_i \in R$. Then

$$a + I = \sum r_i a_i + I = \sum (r_i + I)(a_i + I)$$

is generated by $a_1 + I, \ldots, a_m + I$.

(2) *Show that that R/I is Noetherian if R is Noetherian.* Note that R is an ideal of itself.

(3) *Show that any ring of the form $k[x_1, \ldots, x_n]/I$ is Noetherian.* By the corollary to the Hilbert basis theorem, $k[x_1, \ldots, x_n]$ is Noetherian. By (2), the ring $k[x_1, \ldots, x_n]/I$ is Noetherian.

□

1.5. Irreducible Components of an Algebraic Set

Problem 1.23.

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

Proof.

(1) Let R be any Noetherian ring. Let $\mathscr{S}$ be any collection of ideals containing R itself. Then the only maximal member of $\mathscr{S}$ is R, which is not a maximal ideal.

(2) Or let R be any Noetherian ring and R is not a field. ($R = k[x_1, \ldots, k_n]$ where k is a field for example.) Let $\mathscr{S} = \{(0)\}$. Then the only maximal member of $\mathscr{S}$ is (0), which is not maximal since R is not a field.

□

Problem 1.24.

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

Proof.

(1) Say I be any proper ideal in a Noetherian ring. Let

$$\mathscr{S} = \{\text{proper ideals that contain } I\}.$$

Apply the lemma to $\mathscr{S}$ to get that $\mathscr{S}$ has a maximal member $\mathfrak{m} \in \mathscr{S}$.

(2) *Show that* $\mathfrak{m}$ *is maximal.* Since $\mathfrak{m} \in \mathscr{S}$, $\mathfrak{m}$ is a proper ideal in R. Suppose $\mathfrak{m}' \supseteq \mathfrak{m}$ is a proper ideal containing $\mathfrak{m}$. As $\mathfrak{m}$ contains I, $\mathfrak{m}'$ also contains I or $\mathfrak{m}' \in \mathscr{S}$. By the maximality of $\mathfrak{m}$, $\mathfrak{m}' \subseteq \mathfrak{m}$. So $\mathfrak{m}' = \mathfrak{m}$.

$\square$

Problem 1.25.

(a) *Show that* $V(y - x^2) \subseteq \mathbf{A}^2(\mathbb{C})$ *is irreducible, in fact,* $I(V(y - x^2)) = (y - x^2)$.

(b) *Decompose* $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subseteq \mathbf{A}^2(\mathbb{C})$ *into irreducible components.*

Proof of (a).

(1) Let $I = (y - x^2)$ be an ideal of $\mathbb{C}[x, y]$. Since $\mathbb{C}$ is algebraically closed,

$$I(V(I)) = \mathrm{rad}(I)$$

by the Hilbert's Nullstellensatz. It suffices to show that I is prime, or to show that $y - x^2$ is prime. Since $\mathbb{C}[x, y]$ is a UFD, it suffices to show that $y - x^2$ is irreducible.

(2) *Show that* $y - x^2$ *is irreducible in* $\mathbb{C}[x, y]$. Write

$$y - x^2 \in (\mathbb{C}[y])[x].$$

Note that $\mathbb{C}[y]$ is a UFD and y is the constant term. If we can show that y is prime in $\mathbb{C}[y]$, then by the Eisenstein's criterion then we can say $y - x^2$ is irreducible over $\mathbb{C}[y]$.

(3) As $\mathbb{C}[y]/(y) \cong \mathbb{C}$ is a field or a domain, (y) is maximal or prime. Hence, $y - x^2$ is irreducible.

(4) Or use Corollary 1 to Proposition 2 in the next section.

□

Proof of (b).

(1) Write

$$\begin{aligned}
Y &:= V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \\
&= V((y^2 - x)(y^2 + x), (y^2 - x^2)(y^2 + x)) \\
&= V(y^2 + x) \cup V(y^2 - x, y^2 - x^2) \\
&= V(y^2 + x) \cup V(y^2 - x, x(x-1)) \\
&= V(y^2 + x) \cup V(x, y) \cup V(y+1, x-1) \cup V(y-1, x-1).
\end{aligned}$$

(2) Here $V(y^2 + x)$ is irreducible as (a). Besides, $V(x, y)$, $V(y+1, x-1)$ and $V(y-1, x-1)$ are irreducible since all corresponding ideals are maximal (by the Hilbert's Nullstellensatz and Problem 1.21).

□

Problem 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.

(1) *Show that f is an irreducible polynomial.*

(a) Suppose
$$f = (f_2(x)y^2 + f_1(x)y + f_0(x)) \cdot g(x)$$
for some $f_i(x), g(x) \in \mathbb{R}[x]$. So
$$f_2(x)g(x) = 1, \qquad f_1(x)g(x) = 0, \qquad f_0(x)g(x) = x^2(x-1)^2.$$
Hence,
$$f_2(x)y^2 + f_1(x)y + f_0(x) = uf, \qquad g(x) = u^{-1},$$
where u is a unit in $\mathbb{R}$.

(b) Suppose
$$f = (f_1(x)y + f_0(x)) \cdot (g_1(x)y + g_0(x))$$

for some $f_i(x), g_j(x) \in \mathbb{R}[x]$. So

$$\begin{aligned} f_1(x)g_1(x) &= 1, \\ f_1(x)g_0(x) + f_0(x)g_1(x) &= 0, \\ f_0(x)g_0(x) &= x^2(x-1)^2. \end{aligned}$$

So $f_1(x) = u$, $g_1(x) = u^{-1}$ for some unit $u \in \mathbb{R}$. Hence,

$$u^2 g_0(x)^2 = -x^2(x-1)^2,$$

which is absurd since $\mathbb{R}$ is not algebraically closed.

(c) By (a)(b), f is irreducible in $\mathbb{R}[x, y]$.

(2) *Show that $V(f)$ is reducible.* $V(f) = \{(0,0),(1,0)\} = V(x,y) \cup V(x-1,y)$. Here $V(x,y)$ and $V(x-1,y)$ are all proper algebraic sets in $V(f)$.

□

Problem 1.27.

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

Proof.

(1) Write two decompositions of V, W into irreducible components as

$$\begin{aligned} V &= V_1 \cup \cdots \cup V_r, \\ W &= W_1 \cup \cdots \cup W_s, \end{aligned}$$

(2) For each irreducible component V_i of V, consider $V_i \cap W$:

$$V_i \cap W = (V_i \cap W_1) \cup \cdots \cup (V_i \cap W_s).$$

By the irreducibility of V_i, there is only one j such that $V_i \cap W_j = V_i$ and other intersections are empty. Therefore, each irreducible component V_i is contained in some irreducible component W_j of W.

□

Problem 1.28.

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

Proof.

(1) (Reductio ad absurdum) If

$$V_i \subseteq \bigcup_{j \neq i} V_j$$

for some i, then

$$V = V_1 \cup \cdots \cup \widehat{V_i} \cup \cdots \cup V_r$$

is another decomposition of an algebraic set into irreducible components.

(2) By Theorem 2 in this section, the number of irreducible components is unique determined, contrary to the assumption and (1).

□

Problem 1.29.*

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

Proof.

(1) (Reductio ad absurdum) If $\mathbf{A}^n(k)$ were reducible, then $\mathbf{A}^n(k) = V_1 \cup V_2$ where V_1, V_2 are algebraic sets in $\mathbf{A}^n(k)$, V_1 and V_2 are nonempty and proper in $\mathbf{A}^n(k)$.

(2) Take $P_i \in V_i$ for $i = 1, 2$. By Problem 1.17, there are two polynomials $f_1, f_2 \in k[x_1, \ldots, x_n]$ such that $f_i(Q) = 0$ for all $Q \in V_i$ and $f_1(P_2) = f_2(P_1) = 1$.

(3) By construction, $(f_1 f_2)(a_1, \ldots, a_n) = 0$ for any $a_1, \ldots, a_n \in k$. As k is infinite, $f_1 f_2 = 0$ by Problem 1.4. Since $k[x_1, \ldots, x_n]$ is a domain, $f_1 = 0$ or $f_2 = 0$, contrary to $f_1(P_2) = f_2(P_1) \neq 0$.

□

Note. $\mathbf{A}^n(k)$ is reducible if k is finite.

1.6. Algebraic Subsets of the Plane

Problem 1.30.

Let $k = \mathbb{R}$.

(a) *Show that $I(V(x^2 + y^2 + 1)) = (1)$.*

(b) *Show that every algebraic subset of $\mathbf{A}^2(\mathbb{R})$ is equal to $V(f)$ for some $f \in \mathbb{R}[x, y]$.*

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

Proof of (a). $I(V(x^2 + y^2 + 1)) = I(\varnothing) = (1)$ since $x^2 + y^2 + 1 \geq 1$ is never zero for any $x, y \in \mathbb{R}$. $\square$

Proof of (b).

(1) Given any algebraic subset V of $\mathbf{A}^2(\mathbb{R})$. $V = V(1)$ if $V = \varnothing$. $V = V(0)$ if $V = \mathbf{A}^2(\mathbb{R})$. Now suppose V is a nonempty proper algebraic subset V of $\mathbf{A}^2(\mathbb{R})$. Write $V = V_1 \cup \cdots \cup V_m$, where each V_i is irreducible. Here $V_i \neq \varnothing$ and $V_i \neq \mathbf{A}^2(\mathbb{R})$ for all i.

(2) As $k = \mathbb{R}$ is infinite, Corollary 2 to Proposition 2 implies that each V_i is either a point or an irreducible plane curves $V(f_i)$, where f_i is an irreducible polynomial and $V(f_i)$ is infinite.

(3) If $V_i = \{(a_i, b_i)\}$ is a point, then define
$$f_i(x, y) = (x - a_i)^2 + (x - b_i)^2.$$
By the property of $\mathbb{R}$, $V_i = V(f_i)$.

(4) Define $f = f_1 \cdots f_m \in \mathbb{R}[x, y]$. Hence,
$$\begin{aligned} V &= V_1 \cup \cdots \cup V_m \\ &= V(f_1) \cup \cdots \cup V(f_m) \\ &= V(f_1 \cdots f_m) \\ &= V(f). \end{aligned}$$

$\square$

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

1.7. Hilbert's Nullstellensatz

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

1.8. Modules; Finiteness Conditions

Problem 1.41.*

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

Proof.

(1) $S = \sum Rs_i$ for some $s_1, \ldots, s_n \in S$ since S is module-finite over R.

(2) Let I be the minimal subset of $\{s_1, \ldots, s_n\}$ which also spans S, say $\{t_1, \ldots, t_m\}$ with $m \leq n$. Clearly we can write

$$S = R[t_1, \ldots, t_m],$$

that is, S is ring-finite over R.

(3) The converse is not true (Problem 1.42).

□

Problem 1.42.

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

Proof.

(1) $S = R[x]$ is ring-finite over R by definition (as $x \in S$).

(2) (Reductio ad absurdum) If $S = \sum Rs_i$ for some $s_1, \dots, s_n \in S$ were module-finite over R. Any element $s \in \sum Rs_i$ is of degree

$$\deg s \leq \max_{1 \leq i \leq n} \deg s_i := m.$$

So that $x^{m+1} \in S = R[x]$ but not in $\sum Rs_i$, which is absurd.

□

Problem 1.43.* (WIP)

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

Proof.

(1) $L = K[v_1, \cdots, v_n]$ for some $v_i \in L$. To show $L = K[v_1, \cdots, v_n] = K(v_1, \cdots, v_n)$, it suffices to show that all v_i are algebraic over L.

(2)

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

1.9. Integral Elements

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

1.10. Field Extensions

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

Chapter 2: Affine Varieties

2.1. Coordinate Rings

Problem 2.1.*

Show that the map which associates to each $f \in k[x_1, \ldots, x_n]$ a polynomial function in $\mathscr{F}(V, k)$ is a ring homomorphism whose kernel is $I(V)$.

Proof.

(1) Define a map $\alpha : k[x_1, \ldots, x_n] \to \mathscr{F}(V, k)$. Every polynomial $f \in k[x_1, \ldots, x_n]$ defines a function from V to k by

$$\alpha(f)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$$

for all $(a_1, \ldots, a_n) \in V$.

(2) α is a ring homomorphism by construction in (1).

(3) *Show that* $\ker(\alpha) = I(V)$. In fact, given any $f \in k[x_1, \ldots, x_n]$, we have $\alpha(f) = 0$ (sending all $a \in V$ to $0 \in k$) if and only if $f(a) = 0$ for all $a \in V$ if and only if $f \in I(V)$.

(4) Hence $k[x_1, \ldots, x_n]/I(V) = \Gamma(V) \hookrightarrow \mathscr{F}(V, k)$ is an injective homomorphism.

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

2.2. Polynomial Maps

2.3. Coordinate Changes

2.4. Rational Functions and Local Rings

2.5. Discrete Valuation Rings

2.6. Forms

2.7. Direct Products of Rings

2.8. Operations with Ideals

Problem 2.39.*

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

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

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

Proof of (a).

(1) Note that $(I_1 + I_2)J$ and $I_1 J + I_2 J$ are ideals.

(2) *Show that* $(I_1 + I_2)J \subseteq I_1 J + I_2 J$. Given any
$$(x_1 + x_2)y \in (I_1 + I_2)J$$
where $x_i \in I_i$ and $y \in J$. It suffices to show that $(x_1 + x_2)y \in I_1 J + I_2 J$ (by (1)). In fact,
$$(x_1 + x_2)y = x_1 y + x_2 y \in I_1 J + I_2 J.$$

(3) *Show that* $(I_1 + I_2)J \supseteq I_1 J + I_2 J$. Given any
$$x_1 y_1 + x_2 y_2 \in I_1 J + I_2 J$$
where $x_i \in I_i$ and $y_i \in J$. It suffices to show that $x_1 y_1 + x_2 y_2 \in (I_1 + I_2)J$ (by (1)). In fact,
$$x_1 y_1 + x_2 y_2 = (x_1 + \underbrace{0}_{\in I_2})y_1 + (\underbrace{0}_{\in I_1} + x_2)y_2 \in (I_1 + I_2)J$$

since $(I_1 + I_2)J$ is an ideal.

$\square$

Proof of (b).

(1) Note that $(I_1 \cdots I_N)^n$ and $I_1^n \cdots I_N^n$ are ideals.

(2) *Show that* $(I_1 \cdots I_N)^n \subseteq I_1^n \cdots I_N^n$. Given any

$$x = x_1 \cdots x_n$$

where $x_i \in I_1 \cdots I_N$. It suffices to show that $x \in I_1^n \cdots I_N^n$ (by (1)). For each $x_i \in I_1 \cdots I_N$, write

$$x_i = \sum_{j(i)} x_{j(i),1} \cdots x_{j(i),N}$$

where $x_{j(i),k} \in I_k$ for $1 \leq k \leq N$. Hence

$$\begin{aligned}
x &= x_1 \cdots x_n \\
&= \left(\sum_{j(1)} x_{j(1),1} \cdots x_{j(1),N} \right) \cdots \left(\sum_{j(n)} x_{j(n),1} \cdots x_{j(n),N} \right) \\
&= \sum_{j(1),\dots,j(n)} (x_{j(1),1} \cdots x_{j(1),N}) \cdots (x_{j(n),1} \cdots x_{j(n),N}) \\
&= \sum_{j(1),\dots,j(n)} (\underbrace{x_{j(1),1} \cdots x_{j(n),1}}_{\in I_1^n}) \cdots (\underbrace{x_{j(1),N} \cdots x_{j(n),N}}_{\in I_N^n}) \\
&\in I_1^n \cdots I_N^n.
\end{aligned}$$

(3) *Show that* $(I_1 \cdots I_N)^n \supseteq I_1^n \cdots I_N^n$. Given any

$$x = x_1 \cdots x_N \in I_1^n \cdots I_N^n$$

where $x_i \in I_i^n$ $(1 \leq i \leq N)$. It suffices to show that $x \in (I_1 \cdots I_N)^n$ (by (1)). For each $x_i \in I_i^n$, write

$$x_i = \sum_{j(i)} x_{j(i),1} \cdots x_{j(i),n}$$

where $x_{j(i),k} \in I_i$ for $1 \leq k \leq n$. Hence

$$
\begin{aligned}
x &= x_1 \cdots x_N \\
&= \left(\sum_{j(1)} x_{j(1),1} \cdots x_{j(1),n} \right) \cdots \left(\sum_{j(N)} x_{j(N),1} \cdots x_{j(N),n} \right) \\
&= \sum_{j(1),\dots,j(N)} (x_{j(1),1} \cdots x_{j(1),n}) \cdots (x_{j(N),1} \cdots x_{j(N),n}) \\
&= \sum_{j(1),\dots,j(N)} \underbrace{(x_{j(1),1} \cdots x_{j(N),1})}_{\in I_1 \cdots I_N} \cdots \underbrace{(x_{j(1),n} \cdots x_{j(N),n})}_{\in I_1 \cdots I_N} \\
&\in (I_1 \cdots I_N)^n.
\end{aligned}
$$

□

Problem 2.41.*

Let I, J be ideals in R. Suppose I is finitely generated and $I \subseteq \operatorname{rad}(J)$. Show that $I^n \subseteq J$ for some n.

Proof.

(1) Let I be generated by $x_1, \dots, x_m \in I$. As $I \subseteq \operatorname{rad}(J)$, there are integers $n_i > 0$ such that $x_i^{n_i} \in J$.

(2) Let $N = n_1 + \cdots + n_m$. Given any $x = \sum_{i=1}^m r_i x_i \in I$, so

$$
\begin{aligned}
x^N &= \left(\sum_{i=1}^m r_i x_i \right)^N \\
&= \sum_{k_1+\cdots+k_m=N} \binom{N}{k_1,\dots,k_m} r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m}.
\end{aligned}
$$

(3) Note that for each term there is some j such that $k_j \geq n_j$. Hence,

$$
\begin{aligned}
& x_j^{k_j} = x_j^{k_j - n_j} x_j^{n_j} \in J && (J \text{ is an ideal}) \\
\Longrightarrow\ & r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m} \in J \text{ for each term} && (J \text{ is an ideal}) \\
\Longrightarrow\ & x^N \in J. && (J \text{ is an ideal}) \\
\Longrightarrow\ & I^N \subseteq J.
\end{aligned}
$$

□

Supplement. *(Exercise 1.13 in the textbook: Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry.) Suppose that I is an ideal in a commutative ring. Show that if* $\mathrm{rad}(I)$ *is finitely generated, then for some integer N we have* $(\mathrm{rad}(I))^N \subseteq I$*. Conclude that in a Noetherian ring the ideals I and J have the same radical iff there is some integer N such that $I^N \subseteq J$ and $J^N \subseteq I$. Use the Nullstellensatz to deduce that if $I, J \subseteq S = k[x_1, \ldots, x_n]$ are ideals and k is algebraically closed, then $Z(I) = Z(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.*

Proof.

(1) *Show that if* $\mathrm{rad}(I)$ *is finitely generated, then for some integer N we have* $(\mathrm{rad}(I))^N \subseteq I$. Say $x_1, \ldots, x_m \in \mathrm{rad}(I)$ generate $\mathrm{rad}(I)$.

(a) For each i, there exists an integer $n_i > 0$ such that $x_i^{n_i} \in I$ (since $\mathrm{rad}(I)$ is radical).

(b) Let $N = n_1 + \cdots + n_m$. Given any $x = \sum_{i=1}^m r_i x_i \in \mathrm{rad}(I)$, so

$$\begin{aligned} x^N &= \left(\sum_{i=1}^m r_i x_i \right)^N \\ &= \sum_{k_1 + \cdots + k_m = N} \binom{N}{k_1, \ldots, k_m} r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m}. \end{aligned}$$

(c) Note that for each term there is some j such that $k_j \geq n_j$. Hence,

$$\begin{aligned} & x_j^{k_j} = x_j^{k_j - n_j} x_j^{n_j} \in I && (I \text{ is an ideal}) \\ \Longrightarrow\ & r_1^{k_1} x_1^{k_1} \cdots r_m^{k_m} x_m^{k_m} \in I \text{ for each term} && (I \text{ is an ideal}) \\ \Longrightarrow\ & x^N \in I. && (I \text{ is an ideal}) \\ \Longrightarrow\ & (\mathrm{rad}(I))^N \subseteq I. \end{aligned}$$

(2) *Show that in a Noetherian ring the ideals I and J have the same radical iff there is some integer N such that $I^N \subseteq J$ and $J^N \subseteq I$.*

(a) ($\Longrightarrow$) Since in a Noetherian ring every ideal is finitely generated, $\mathrm{rad}(I)$ and $\mathrm{rad}(J)$ are finitely generated. By (1), there is a common integer N such that

$$(\mathrm{rad}(I))^N \subseteq I \quad \text{and} \quad (\mathrm{rad}(J))^N \subseteq J.$$

Note that $I^N \subseteq (\mathrm{rad}(I))^N$ and $J^N \subseteq (\mathrm{rad}(J))^N$. Since $\mathrm{rad}(I) = \mathrm{rad}(J)$ by assumption,

$$\begin{aligned} I^N &\subseteq (\mathrm{rad}(I))^N = (\mathrm{rad}(J))^N \subseteq J, \\ J^N &\subseteq (\mathrm{rad}(J))^N = (\mathrm{rad}(I))^N \subseteq I. \end{aligned}$$

(b) ($\Longleftarrow$) It suffices to show that $\operatorname{rad}(I) \subseteq \operatorname{rad}(J)$. $\operatorname{rad}(J) \subseteq \operatorname{rad}(I)$ is similar. Given any $x \in \operatorname{rad}(I)$, there is an integer $M > 0$ such that $x^M \in I$. Hence $x^{MN} \in I^N \subseteq J$, or $x \in \operatorname{rad}(J)$.

(3) *Show that if $I, J \subseteq S = k[x_1, \dots, x_n]$ are ideals and k is algebraically closed, then $Z(I) = Z(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.* Note that S is Noetherian and we can apply part (2). By the Nullstellensatz, $Z(I) = Z(J)$ iff $\operatorname{rad}(I) = \operatorname{rad}(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.

□

2.9. Ideals with a Finite Number of Zeros

2.10. Quotient Modules and Exact Sequences

Problem 2.51.

Let

$$0 \longrightarrow V_1 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0$$

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

Proof (Proposition 7 in this section).

(1) For $i = 0, \dots, n$, by the rank-nullity theorem for a linear transformation $\varphi_i : V_i \to V_{i+1}$, we have

$$\dim V_i = \dim \operatorname{im}(\varphi_i) + \dim \ker(\varphi_i).$$

(Here $V_0 = V_{n+1} := 0$ by convention.)

(2) By the exactness of the sequence, we have

(a) $\operatorname{im}(\varphi_i) = \ker(\varphi_{i+1})$ for $i = 0, \dots, n-1$. In particular, $\ker(\varphi_1) = \operatorname{im}(\varphi_0) = 0$.

(b) $\ker(\varphi_n) = V_n$.

Hence,

$$\begin{aligned}
\sum_{i=1}^{n-1}(-1)^i \dim(V_i) &= \sum_{i=1}^{n-1}(-1)^i \dim \operatorname{im}(\varphi_i) + \sum_{i=1}^{n-1}(-1)^i \dim \ker(\varphi_i) \\
&= \sum_{i=1}^{n-1}(-1)^i \dim \ker(\varphi_{i+1}) + \sum_{i=1}^{n-1}(-1)^i \dim \ker(\varphi_i) \\
&= (-1)^{n-1} \dim \underbrace{\ker(\varphi_n)}_{=V_n} + (-1)^1 \dim \underbrace{\ker(\varphi_1)}_{=0} \\
&= -(-1)^n \dim V_n,
\end{aligned}$$

or $\sum(-1)^i \dim(V_i) = 0$.

□

2.11. Free Modules

Chapter 3: Local Properties of Plane Curves

3.1. Multiple Points and Tangent Lines

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

3.2. Multiplicities and Local Rings

3.3. Intersection Numbers

Chapter 4: Projective Varieties

4.1. Projective Space

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

4.2. Projective Algebraic Sets

4.3. Affine and Projective Varieties

4.4. Multiprojective Space

Chapter 5: Projective Plane Curves

5.1. Definitions

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

5.2. Linear Systems of Curves

5.3. Bézout's Theorem

5.4. Multiple Points

5.5. Max Noether's Fundamental Theorem

5.6. Applications of Noether's Theorem

Chapter 6: Varieties, Morphisms, and Rational Maps

6.1. The Zariski Topology

6.2. Varieties

6.3. Morphisms of Varieties

6.4. Products and Graphs

6.5. Algebraic Function Fields and Dimension of Varieties

6.6. Rational Maps

Chapter 7: Resolution of Singularities

7.1. Rational Maps of Curves

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

7.2. Blowing up a Point in $\mathbf{A}^2$

7.3. Blowing up a Point in $\mathbf{P}^2$

7.4. Quadratic Transformations

7.5. Nonsingular Models of Curves

Chapter 8: Riemann-Roch Theorem

8.1. Divisors

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

□

8.2. The Vector Spaces $L(D)$

8.3. Riemann's Theorem

8.4. Derivations and Differentials

8.5. Canonical Divisors

8.6. Riemann-Roch Theorem