Solutions to the book:
Fulton, Algebraic Curves

Meng-Gen Tsai
plover@gmail.com

March 26, 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 $R[x_1, \dots, x_n]$, show that fg is a form of degree $r + s$.*

(b) *Show that any factor of a form in $R[x_1, \dots, x_n]$ 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 $(i) = (i_1, \dots, i_n)$ with $i_1 + \cdots + i_n = r$ and $\sum_{(j)}$ is the summation over $(j) = (j_1, \dots, j_n)$ 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 $(k) = (i_1 + j_1, \dots, i_n + j_n)$ 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 $r + s$.

$\square$

Proof of (b).

(1) Given any form $f \in R[x_1, \dots, x_n]$, 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

$$f = gh = g_0h_0 + \cdots + g_rh_s.$$

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

$$\begin{aligned} a &= p_1 \cdots p_n, \\ b &= q_1 \cdots q_m \end{aligned}$$

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 $q_j = p_iu$ for some $u \in R$. By the irreducibility of p_i and q_j, u is a unit. So

$$z = \frac{a}{b} = \frac{p_1 \cdots \widehat{p_i} \cdots p_n}{q_1 \cdots \widehat{q_j} \cdots q_m} = \frac{p_1 \cdots \widehat{p_i} \cdots p_n}{uq_1 \cdots \widehat{q_j} \cdots q_m}.$$

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

$$\begin{aligned} a &= p_1 \cdots p_n, \\ b &= q_1 \cdots q_m, \\ a' &= p_1' \cdots p_{n'}', \\ b' &= q_1' \cdots q_{m'}' \end{aligned}$$

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
$$f_{(i)} = (x_k - a_k)\underbrace{(\lambda_{(i)}(x_1 - a_1)^{i_1} \cdots (x_k - a_k)^{i_k - 1} \cdots (x_n - a_n)^{i_n})}_{:= g_{(i)} \in k[x_1, \ldots, x_n]}.$$
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 §1.2) and any finite union of algebraic sets is algebraic (Property (4) in §1.2). Thus, every subset of $\mathbf{A}^n(k)$ is algebraic (by (1)).

□

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.

□

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.

□

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. □

Proof of (c). The circle

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

is algebraic again. □

Problem 1.12.

Suppose C is an affine plane curve, and L is a line in $\mathbf{A}^2(k)$, $L \not\subseteq C$. 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 $\mathbf{A}^2(k)$. (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,

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

is finite of no more than n points.

$\square$

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 $\left(0, \frac{\pi}{2}\right) \in L - Y$.

$\square$

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 $(0, 0) \in L - Y$.

□

Proof of (c).

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

(2) *Suppose C is an affine plane curve, and L is a line in $\mathbf{A}^3(k)$, $L \not\subseteq C$. 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 $\mathbf{A}^3(k)$.

(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,

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

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 $k[x_1, \dots, x_n]$, 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 $k[x_1, \dots, x_n]$, we may assume that $\deg_{x_n}(f) > 0$. Hence

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

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

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

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

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

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 Property (6) in §1.3.) *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 Property (8) in §1.3.) *$I(V(S)) \supseteq S$ 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 Property (9) in §1.3.) *$V(I(V(S))) = V(S)$ 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 Properties (6)(8) in §1.3).

   (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 Property (6) in §1.3, $I(V) \supseteq I(W)$ 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 Property (3) in §1.2 and similar argument in (a). By Property (9) in §1.3, $V(I(V)) = V$ 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 $f \in k[x_1, \ldots, x_n]$ such that $f(Q) = 0$ for all $Q \in V$, but $f(P) = 1$. (Hint: $I(V) \neq I(V \cup \{P\})$.)*

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

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

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 $(f(P))^{-1}f \in k[x_1, \dots, x_n]$. 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

$$W = V \cup \{P_1, \dots, P_r\}$$
$$W_i = V \cup \{P_1, \dots, \widehat{P_i}, \dots, P_r\}.$$

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

(2) By (a), there is a polynomial $f_i \in k[x_1, \dots, x_n]$ 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

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

(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 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.

$\square$

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 Properties (6)(8) in §1.3,

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

□

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.

$\square$

1.4. The Hilbert Basis Theorem

Problem 1.22.* (Correspondence theorem for rings)

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 $k[x_1, \ldots, x_n]/I$ 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,

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

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 we can say $y - x^2$ is irreducible in $(\mathbb{C}[y])[x]$.

(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 apply Corollary 1 to Proposition 2 in the next section to (2)(3).

□

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 §1.5, 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 1.31.

(a) *Find the irreducible components of $V(y^2 - xy - x^2y + x^3)$ in $\mathbf{A}^2(\mathbb{R})$, and also in $\mathbf{A}^2(\mathbb{C})$.*

(b) *Do the same for* $V(y^2 - x(x^2-1))$, *and for* $V(x^3 + x - x^2y - y)$.

Proof of (a).

(1) Note that

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

(2) Note that $y - x^2$ and $y - x$ are irreducible in $\mathbb{C}[x,y]$ and thus also in $\mathbb{R}[x,y]$ by the similar argument in Problem 1.25(a). Also, $V(y-x^2)$ and $V(y-x)$ are infinite in $\mathbf{A}^2(\mathbb{R})$ and thus also in $\mathbf{A}^2(\mathbb{C})$.

(3) Therefore, $V(y-x^2)$ and $V(y-x)$ are the irreducible components of $V(y^2 - xy - x^2y + x^3)$ in $\mathbf{A}^2(\mathbb{R})$ and also in $\mathbf{A}^2(\mathbb{C})$.

$\square$

Outline of (b).

(1) The elliptic curve $V(y^2 - x(x+1)(x-1))$ is irreducible over $\mathbf{A}^2(\mathbb{R})$.

(2) The elliptic curve $V(y^2 - x(x+1)(x-1))$ is irreducible over $\mathbf{A}^2(\mathbb{C})$.

(3) The irreducible component of $V(x^3+x-x^2y-y)$ over $\mathbf{A}^2(\mathbb{R})$ is $V(x-y)$.

(4) The irreducible components of $V(x^3+x-x^2y-y)$ over $\mathbf{A}^2(\mathbb{C})$ are $V(x+i)$, $V(x-i)$ and $V(x-y)$.

Proof of (b).

(1) Similar to Problem 1.25. To show $y^2 - x(x+1)(x-1)$ is irreducible in $\mathbb{C}[x,y]$, we write

$$y^2 - x(x+1)(x-1) \in (\mathbb{C}[x])[y].$$

Note that $\mathbb{C}[x]$ is a UFD and $-x(x+1)(x-1)$ is the constant term. As $\mathbb{C}[x]/(x) \cong \mathbb{C}$ is a domain, (x) is prime. Clearly, $x \mid x(x+1)(x-1)$ but $x^2 \nmid x(x+1)(x-1)$. By the Eisenstein's criterion, we can say $y^2 - x(x+1)(x-1)$ is irreducible over $(\mathbb{C}[x])[y]$.

(2) Moreover, $V(y^2 - x(x+1)(x-1))$ is infinite over $\mathbf{A}^2(\mathbb{R})$ and thus also over $\mathbf{A}^2(\mathbb{C})$. ($y = f(x) = \sqrt{x(x+1)(x-1)}$ is continuous and strictly increasing on $[1, \infty)$ in the sense of calculus. As the measure of $[1,\infty)$ is ∞, the set $V(y^2 - x(x+1)(x-1))$ is infinite over $\mathbf{A}^2(\mathbb{R})$.)

(3) By Corollary 1 to Proposition 2, $V(y^2 - x(x^2-1))$ itself is irreducible over $\mathbf{A}^2(\mathbb{R})$ or $\mathbf{A}^2(\mathbb{C})$.

(4) Consider $V(x^3+x-x^2y-y) \subseteq \mathbf{A}^2(\mathbb{R})$.

$$\begin{aligned}V(x^3+x-x^2y-y) &= V((x^2+1)(x-y))\\ &= V(x^2+1) \cup V(x-y)\\ &= \varnothing \cup V(x-y)\\ &= V(x-y).\end{aligned}$$

Here we use that fact that $x^2+1=0$ has no real solution $x \in \mathbb{R}$. Similar to (a), $V(x-y)$ is the only irreducible component of $V(x^3+x-x^2y-y)$ in $\mathbf{A}^2(\mathbb{R})$.

(5) Consider $V(x^3+x-x^2y-y) \subseteq \mathbf{A}^2(\mathbb{C})$.

$$\begin{aligned}V(x^3+x-x^2y-y) &= V((x+i)(x-i)(x-y))\\ &= V(x+i) \cup V(x-i) \cup V(x-y).\end{aligned}$$

Similar to (a), $V(x \pm i)$ and $V(x-y)$ are the irreducible components of $V(x^3+x-x^2y-y)$ in $\mathbf{A}^2(\mathbb{C})$.

$\square$

1.7. Hilbert's Nullstellensatz

Problem 1.32.

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

Proof.

(1) Weak Nullstellensatz: $I = (x^2+1)$ is a proper ideal in $\mathbb{R}[x]$ but $V(I) = \varnothing$.

(2) Hilbert's Nullstellensatz: Let $I = (y^2+x^2(x-1)^2)$ be an ideal in $\mathbb{R}[x,y]$. Hence,

$$\begin{aligned}I(V(I)) &= I(\{(0,0),(1,0)\}) && \text{(Problem 1.26.)}\\ &= (x(x-1), y)\\ &\neq I\\ &= \mathrm{rad}(I).\end{aligned}$$

The last equality holds since f is irreducible in a UFD $\mathbb{R}[x,y]$ and thus I is a prime ideal.

(3) Corollary 1: Same example in the case Hilbert's Nullstellensatz. If $I = (y^2+x^2(x-1)^2)$ is a radical ideal in $\mathbb{R}[x,y]$. Then $I(V(I)) \neq I$.

(4) Corollary 2: Same example in the case Hilbert's Nullstellensatz. If $I = (y^2 + x^2(x-1)^2)$ is a prime ideal in $\mathbb{R}[x,y]$, then

$$V(I) = \{(0,0),(1,0)\} = V(x,y) \cup V(x-1,y)$$

is reducible. Next, consider a prime ideal $J = (x^2 + y^2)$ in $\mathbb{R}[x,y]$. (Use the same argument in Problem 1.26 to get the irreducibility of $x^2 + y^2$.) $V(J) = \{(0,0)\}$ is a point but J is not a maximal ideal (since $J \subsetneq (x^2 + y^2, x) \subsetneq (1)$).

(5) Corollary 3: Same example in Corollary 2.

(6) Corollary 4: Let $I = (x^2+y^2)$ be an ideal in $\mathbb{R}[x,y]$. Then $V(I) = \{(0,0)\}$ is a finite set. But $\mathbb{R}[x,y]/(x^2+y^2)$ is an infinite dimensional vector space over $\mathbb{R}$. In fact, the monomials

$$\{\overline{x^m}, \overline{x^m y} : m = 0,1,2,\ldots\}$$

is a basis for $\mathbb{R}[x,y]/(x^2+y^2)$.

□

Problem 1.33.

(a) *Decompose* $V(x^2+y^2-1, x^2-z^2-1) \subseteq \mathbf{A}^3(\mathbb{C})$ *into irreducible components.*

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

Proof of (a).

(1) Write

$$\begin{aligned}
&V(x^2+y^2-1, x^2-z^2-1)\\
&= V(x^2+y^2-1, y^2+z^2)\\
&= V(x^2+y^2-1, (y+iz)(y-iz))\\
&= V(x^2+y^2-1, y+iz) \cup V(x^2+y^2-1, y-iz).
\end{aligned}$$

By the Hilbert's Nullstellensatz, it suffices to show that $(x^2+y^2-1, y+iz)$ and $(x^2+y^2-1, y-iz)$ are prime.

(2) *Show that* $I = (x^2+y^2-1, y+iz)$ *is prime in* $\mathbb{C}[x,y,z]$. Note that

$$\mathbb{C}[x,y,z]/I \cong \mathbb{C}[x,y]/(x^2+y^2-1)$$

is a ring isomorphism defined by

$$f(x,y,z) + I \mapsto f(x,y,-iy) + (x^2+y^2-1).$$

(Use the similar argument in (b) to prove it is indeed an isomorphism.) So it suffices to show that

$$x^2 + y^2 - 1 \in \mathbb{C}[x, y]$$

is irreducible. (Thus, $\mathbb{C}[x, y]/(x^2+y^2-1) \cong \mathbb{C}[x, y, z]/I$ is a domain, or I is prime.) We can use the similar argument in Problem 1.31 (b) to show $x^2+y^2-1 = y^2+(x+1)(x-1)$ is irreducible as showing the irreducibility of $y^2 - x(x+1)(x-1)$.

(3) Similarly, $I = (x^2 + y^2 - 1, y - iz)$ is prime. Therefore, the irreducible components of $V(x^2 + y^2 - 1, x^2 - z^2 - 1)$ are $V(x^2 + y^2 - 1, y + iz)$ and $V(x^2 + y^2 - 1, y - iz)$.

□

Proof of (b).

(1) Write

$$V = \{(t, t^2, t^3) \in \mathbf{A}^3(\mathbb{C}) : t \in \mathbb{C}\} = V(x^2 - y, x^3 - z).$$

Let $I = (x^2 - y, x^3 - z)$ in $\mathbb{C}[x, y, z]$. By the Hilbert's Nullstellensatz, $I(V) = \mathrm{rad}(I)$. So it suffices to show that $I = (x^2 - y, x^3 - z)$ is prime (and thus V is irreducible).

(2) *Show that*

$$\mathbb{C}[x, y, z]/I \cong \mathbb{C}[t]$$

is a domain, and thus $I = (x^2 - y, x^3 - z)$ is a prime ideal.

(a) Define a ring homomorphism $\alpha : \mathbb{C}[x, y, z]/I \to \mathbb{C}[t]$ by

$$\alpha : f(x, y, z) + I \mapsto f(t, t^2, t^3).$$

α is well-defined since $\alpha((x^2 - y) + I) = 0$ and $\alpha((x^3 - z) + I) = 0$.

(b) *Show that α is surjective.*

$$\alpha : g(x) + I \in \mathbb{C}[x, y, z]/I \mapsto g(t) \in \mathbb{C}[t]$$

for any $g(t)$.

(c) *Show that α is injective.* Suppose $\alpha(f(x, y, z) + I) = 0$. Write

$$\begin{aligned} f(x, y, z) + I &= \sum_{(i)} \lambda_{(i)} x^{i_1} (y - x^2)^{i_2} (z - x^3)^{i_3} + I \\ &= \sum_i \lambda_i x^i + I. \end{aligned}$$

So

$$0 = \alpha(f(x, y, z) + I) = \alpha\left(\sum_i \lambda_i x^i + I\right) = \sum_i \lambda_i t^i.$$

Hence, $\ker(\alpha) = I$.

□

Problem 1.34.

Let R be a UFD.

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

(b) *$x^2 - a \in R[x]$ is irreducible if and only if a is not a square in R.*

Proof of (a).

(1) It is equivalent to show that a monic polynomial of degree two or three in $R[x]$ is reducible if and only if it has one root in R.

(2) Suppose f is reducible of degree 2 or 3. Then there exist nonconstant monic polynomials $g, h \in R[x]$ such that $f = gh$. By

$$\deg(g) + \deg(h) = \deg(f) = 2 \text{ or } 3,$$

we may assume that $\deg(g) = 1$. (Otherwise g or h will be a constant polynomial.) Say $g(x) = x - a$ where $a \in R$. Now

$$f(a) = g(a)h(a) = 0$$

implies that $a \in R$ is a root of f.

(3) Conversely, if $a \in R$ is a root of f, then apply the same argument in Problem 1.7 we can write

$$f = (x - a)g$$

for some $g \in R[x]$. Here $\deg(g) \geq 1$ since $\deg(f) = 1 + \deg(g) \geq 2$. Therefore, f is reducible.

□

Proof of (b). By (a), $x^2 - a \in R[x]$ is reducible $\Longleftrightarrow$ $x^2 - a$ has one root $\alpha \in R$ $\Longleftrightarrow$ $a = \alpha^2$ is a square in R for some $\alpha \in R$. □

Problem 1.35.

Show that $V(y^2 - x(x-1)(x-\lambda)) \subseteq \mathbf{A}^2(k)$ is an irreducible curve for any algebraically closed field k, and any $\lambda \in k$.

Proof.

(1) By the Hilbert's Nullstellensatz, it suffices to show that

$$I = (y^2 - x(x-1)(x-\lambda))$$

is a prime ideal in $k[x, y]$, or show that

$$y^2 - x(x-1)(x-\lambda)$$

is irreducible (since $k[x, y]$ is a UFD).

(2) By Problem 1.34(b), $y^2 - x(x-1)(x-\lambda) \in (\mathbb{C}[x])[y]$ is irreducible if $x(x-1)(x-\lambda)$ is not a square in $\mathbb{C}[x]$. Note that every square in $\mathbb{C}[x]$ is of even degree. So $x(x-1)(x-\lambda)$ cannot be a square in $\mathbb{C}[x]$ since $\deg(x(x-1)(x-\lambda)) = 3$ is odd.

□

Note. $V(y^2 - x(x-1)(x-\lambda))$ is the elliptic curve as Problem 1.31.

Problem 1.36.

Let $I = (y^2 - x^2, y^2 + x^2) \subseteq \mathbb{C}[x, y]$. *Find* $V(I)$ *and* $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I)$.

Proof.

(1) Clearly, $V(I) = \{(0, 0)\}$ is a finite set. By Corollary 4 to the Hilbert's Nullstellensatz,

$$\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I) < \infty.$$

In fact, $\dim_{\mathbb{C}}(\mathbb{C}[x, y]/I) = 4$.

(2) Given any $f + I \in \mathbb{C}[x, y]/I$ where $f \in \mathbb{C}[x, y]$. Write

$$f(x, y) = \sum_i f_i(x) y^i$$

where $f_i(x) = \sum_j a_{ij} x^j \in \mathbb{C}[x]$. Note that

$$\begin{aligned} x^2 &= \frac{1}{2}(y^2 + x^2) - \frac{1}{2}(y^2 - x^2) \in I, \\ y^2 &= \frac{1}{2}(y^2 + x^2) + \frac{1}{2}(y^2 - x^2) \in I. \end{aligned}$$

So

$$\begin{aligned} f(x,y)+I &= \sum_i f_i(x)y^i + I \\ &= f_0(x)+f_1(x)y+I \\ &= \sum_j a_{0j}x^j + \left(\sum_j a_{1j}x^j\right) y + I \\ &= a_{00}+a_{01}x+a_{10}y+a_{11}xy+I \end{aligned}$$

is generated by $\mathscr{B} = \{\overline{1}, \overline{x}, \overline{y}, \overline{xy}\}$.

(3) Note that $\mathscr{B}$ is a basis since any linear combination of elements in $\mathscr{B}$ is not in I. Therefore,

$$\dim_{\mathbb{C}}(\mathbb{C}[x,y]/I) = |\mathscr{B}| = 4.$$

□

Problem 1.37.*

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

Proof.

(1) *Show that every element in $K[x]/(f)$ is generated by $\mathscr{B} = \{\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}\}$.* Given any $\overline{g} \in K[x]/(f)$ with $g \in K[x]$. By the division-with-remainder property of $K[x]$, there are some polynomials $q, r \in K[x]$ such that

$$g = fq + r$$

where $r = 0$ or $\deg(r) < n$ if $r \neq 0$. Therefore,

$$g + (f) = fq + r + (f) = r + (f).$$

Note that $r + (f)$ is generated by $\mathscr{B}$.

(2) *Show that $\mathscr{B}$ is a basis for $K[x]/(f)$ over K.* Suppose

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in (f)$$

for $a_1, \ldots, a_{n-1} \in K$. We can regard any linear combination of $\{1, x, \ldots, x^{n-1}\}$ as a polynomial $r(x)$ in $K[x]$. $r \in (f)$ implies that there exists a polynomial $g \in K[x]$ such that $r = fg$. If $g \neq 0$, then $\deg(r) = \deg(f) + \deg(g) \geq n$, which is impossible. So $g = 0$ and thus $r = fg = 0 \in K[x]$. Therefore, $a_0 = a_1 = \cdots = a_{n-1} = 0 \in K$ and

$$\dim_K(K[x]/(f)) = \deg(f).$$

□

Problem 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 $k[x_1, \ldots, x_n]/I$, and that irreducible algebraic sets (resp. points) correspond to prime ideals (resp. maximal ideals). (See Problem 1.22.)

Proof.

(1) Given any algebraic subset W of V. By the Hilbert's Nullstellensatz,

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

(2) By Corollary 1 to the Hilbert's Nullstellensatz and Problem 1.22(b), we have a one-to-one correspondence such that

$$\begin{aligned} &\{\text{algebraic subsets of } V\} \\ \longleftrightarrow &\{\text{radical ideals containing } I\} \\ \longleftrightarrow &\{\text{radical ideals of } k[x_1, \ldots, x_n]/I\}. \end{aligned}$$

(3) Again by Corollary 2 to the Hilbert's Nullstellensatz and Problem 1.22(b), we have a one-to-one correspondence such that

$$\begin{aligned} &\{\text{irreducible algebraic subsets (resp. points) of } V\} \\ \longleftrightarrow &\{\text{prime (resp. maximal) ideals containing } I\} \\ \longleftrightarrow &\{\text{prime (resp. maximal) ideals of } k[x_1, \ldots, x_n]/I\}. \end{aligned}$$

□

Problem 1.39.

(a) *Let R be a UFD, and let $\mathfrak{p} = (t)$ be a principal proper prime ideal. Show that there is no prime ideal $\mathfrak{q}$ such that $0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$.*

(b) *Let $V = V(f)$ be irreducible hypersurface in $\mathbf{A}^n$. Show that there is no irreducible algebraic set W such that $V \subsetneq W \subsetneq \mathbf{A}^n$.*

Proof of (a).

(1) (Reductio ad absurdum) Suppose that $\mathfrak{q}$ were a prime ideal in R such that $0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$.

(2) *Show that there is an irreducible element in* $\mathfrak{q}$. Given any $q \in \mathfrak{q}$. Since $\mathfrak{q}$ is proper, we can write
$$q = q_1 \cdots q_n$$
as a product of irreducible elements in a UFD. Since $\mathfrak{q}$ is prime, there is one irreducible element $q_i \in \mathfrak{q}$.

(3) Now $q_i \in \mathfrak{q} \subseteq \mathfrak{p} = (t)$. So $q_i = ut$ for some $u \in R$. By the irreducibility of q_i, u is a unit or t is a unit. If u is a unit, then
$$(t) = (q_i) \subseteq \mathfrak{q} \subseteq \mathfrak{p} = (t).$$
So $\mathfrak{q} = \mathfrak{p}$, which is absurd. If t is a unit, then $\mathfrak{p} = (1)$, contrary to the primality of $\mathfrak{p}$.

□

Proof of (b).

(1) We might assume that $k = \overline{k}$. By Corollary 3 to the Hilbert's Nullstellensatz and the irreducibility of $V(f)$, there are an irreducible polynomial $g \in k[x_1, \dots, x_n]$ and an integer $m > 0$ such that
$$f = g^m,$$
and
$$I(V(f)) = (g).$$

(2) (Reductio ad absurdum) Suppose that there were an irreducible algebraic set W such that $V \subsetneq W \subsetneq \mathbf{A}^n$. Then by Corollary 3 to the Hilbert's Nullstellensatz again,
$$(g) = I(V(f)) \supsetneq I(W) \supsetneq (1) \in k[x_1, \dots, x_n].$$
Here $(g) = I(V(f))$ and $I(W)$ are all prime.

(3) Note that (g) is a principal proper prime ideal in a UFD $k[x_1, \dots, x_n]$. By (a), such ideal $I(W)$ cannot be prime, which is absurd.

□

Problem 1.40.

Let $I = (x^2 - y^3, y^2 - z^3) \subseteq k[x, y, z]$. *Define* $\alpha : k[x, y, z] \to k[t]$ *by* $\alpha(x) = t^9$, $\alpha(y) = t^6$, $\alpha(z) = t^4$.

(a) *Show that every element of* $k[x, y, z]/I$ *is the residue of an element* $a + xb + yc + xyd$, *for some* $a, b, c, d \in k[z]$.

(b) *If* $f = a + xb + yc + xyd$, $a, b, c, d \in k[z]$ *and* $\alpha(f) = 0$, *compare like powers of* t *to conclude that* $f = 0$.

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

Proof of (a).

(1) Take any element $\overline{f} \in k[x, y, z]/I$ where $f \in k[x, y, z]$. Regard $f \in (k[y, z])[x]$, By the division-with-remainder property of $(k[y, z])[x]$,

$$f = (x^2 - y^3)q + r$$

where $q, r \in (k[y, z])[x]$ and $r = 0$ or $\deg_x(r) < 2$. In any case, $r = xr_1 + r_0$ for some $r_1, r_0 \in k[y, z]$.

(2) Apply the same argument to (1), we have

$$\begin{aligned} r_0 &= (y^2 - z^3)q_0 + yc + a \\ r_1 &= (y^2 - z^3)q_1 + yd + b \end{aligned}$$

where $q_0, q_1 \in k[y, z]$ and $a, b, c, d \in k[z]$.

(3) By $\overline{r_0} = \overline{yc} + \overline{a}$ and $\overline{r_1} = \overline{yd} + \overline{b}$,

$$\begin{aligned} \overline{f} &= \overline{r} \\ &= \overline{xr_1} + \overline{r_0} \\ &= \overline{x}(\overline{yd} + \overline{b}) + (\overline{yc} + \overline{a}) \\ &= \overline{a} + \overline{b} \cdot \overline{x} + \overline{c} \cdot \overline{y} + \overline{d} \cdot \overline{xy}. \end{aligned}$$

$\square$

Proof of (b). As $0 = \alpha(f) = a + ct^6 + bt^9 + dt^{15} \in k[t]$, $a = b = c = d = 0 \in k$. $\square$

Proof of (c).

(1) $I \subseteq \ker(\alpha)$ is trivial.

(2) *Show that* $\ker(\alpha) \subseteq I$. Take any $f \in \ker(\alpha)$, or $\alpha(f) = 0$. By (a), $f = r + f_1$ where $f_1 \in I$ and $r = a + bx + cy + dxy \in k[x, y, z]$ for some $a, b, c, d \in k[z]$. Note that α is a ring homomorphism. Therefore,

$$0 = \alpha(f) = \alpha(r + f_1) = \alpha(r) + \alpha(g) = \alpha(r).$$

By (b), $r = 0 \in k[x, y, z]$ and thus $f = f_1 \in I$.

(3) Therefore,

$$\alpha : k[x, y, z]/(x^2 - y^3, y^2 - z^3) \hookrightarrow k[t]$$

is injective.

□

1.8. Modules; Finiteness Conditions

Problem 1.41.*

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

Proof.

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

(2) *Show that* $\sum Rs_i = R[s_1, \dots, s_n]$. $\sum Rs_i \subseteq R[s_1, \dots, s_n]$ is trivial. Conversely, take any $v \in R[s_1, \dots, s_n]$. Write

$$v = \sum_{(j)} \overbrace{\underbrace{a_{(j)}}_{\in R} \underbrace{s_1^{j_1} \cdots s_n^{j_n}}_{\in S = \sum Rs_i}}^{\in \sum Rs_i}$$

Here each term $a_{(i)} s_1^{i_1} \cdots s_n^{i_n}$ is in $\sum Rs_i$. As $\sum Rs_i$ is an R-module,

$$v = \sum_{(i)} a_{(i)} s_1^{i_1} \cdots s_n^{i_n} \in \sum Rs_i.$$

□

Note. The converse is not true (by 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.*

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 $v_i \in L$ since L is ring-finite over K.

(2) Apply Proposition 4 in §1.10, L is module-finite (and hence algebraic) over K, that is, $L = K[v_1, \cdots, v_n] = K(v_1, \cdots, v_n)$ is a finitely generated field extension of K.

□

Problem 1.44.*

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

Proof.

(1) (Reductio ad absurdum) Suppose that L were ring-finite over K. Write $L = K[v_1, \ldots, v_m]$ where $v_1, \ldots, v_m \in L = K(x)$. Let $b \in K[x]$ be a common denominator of ring generators $v_1, \ldots, v_m$. (So that all $bv_i \in K[x]$.) Therefore, for any $z \in L = K[v_1, \ldots, v_m]$, there is an integer $n > 0$ such that $b^n z \in K[x]$.

(2) Consider $z = 1/c \in K(x)$, where $c \in K[x]$ doesn't divide b. The existence of c is guaranteed by Problem 1.5. Hence, for any integer $n > 0$

$$b^n z = b^n / c$$

is never in $K[x]$ by the construction of c, which is absurd.

□

Problem 1.45.*

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

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

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

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

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

Proof of (a).

(1) *Show that $T \subseteq \sum Rv_iw_j$.* Given any $t \in T = \sum Sw_j$. There are some $s_j \in S$ such that $t = \sum_j s_jw_j$. As $s_j \in S = \sum Rv_i$, there are some $r_{ij} \in R$ such that $s_j = \sum_i r_{ij}v_i$. Hence,

$$t = \sum_j s_jw_j = \sum_j \left(\sum_i r_{ij}v_i \right) w_j = \sum_{i,j} r_{ij}v_iw_j \in \sum Rv_iw_j.$$

(2) *Show that $T \supseteq \sum Rv_iw_j$.* Take any $\sum r_{ij}v_iw_j \in \sum Rv_iw_j$.

$$\sum r_{ij}v_iw_j = \sum_j \left(\sum_i r_{ij}v_i \right) w_j \in \sum_j Sw_j = T.$$

$\square$

Proof of (b).

(1) Note that $R[x_1, \cdots, x_m]$ is canonically isomorphic to $R[x_1, \cdots, x_{m-1}][x_m]$. Hence $R[x_1, \cdots, x_m]$ is isomorphic to $R[x_1][x_2] \cdots [x_m]$.

(2) Hence,

$$\begin{aligned} T &= S[w_1, \dots, w_m] \\ &= R[v_1, \dots, v_n][w_1, \dots, w_m] \\ &= R[v_1, \dots, v_n][w_1] \cdots [w_m] \\ &= R[v_1] \cdots [v_n][w_1] \cdots [w_m] \\ &= R[v_1, \dots, v_n, w_1, \dots, w_m]. \end{aligned}$$

$\square$

Proof of (c).

(1) By (b), $R(v_1, \ldots, v_n)$ is canonically isomorphic to $R(v_1, \ldots, v_{n-1})(v_n)$. Hence $R(v_1, \ldots, v_n)$ is isomorphic to $R(v_1)\cdots(v_n)$. To see this, note that $R[x_1, \cdots, x_m] \cong R[x_1, \cdots, x_{m-1}][x_m]$ implies that

$$R(x_1, \cdots, x_m) \cong R[x_1, \cdots, x_{m-1}](x_m) \hookrightarrow R(x_1, \cdots, x_{m-1})(x_m).$$

Conversely, for any $a/b \in R(x_1, \cdots, x_{m-1})(x_m)$ where

$$\begin{aligned} a &= \sum_i a_i x_m^i \in R(x_1, \cdots, x_{m-1})[x_m], \\ b &= \sum_j b_j x_m^j \in R(x_1, \cdots, x_{m-1})[x_m] \end{aligned}$$

and $b \neq 0$, there is a nonzero polynomial $c \in R[x_1, \cdots, x_{m-1}]$ such that all ca_i and cb_j are in $R[x_1, \cdots, x_{m-1}]$. Hence,

$$\begin{aligned} \frac{a}{b} &= \frac{\sum_i a_i x_m^i}{\sum_j b_j x_m^j} \\ &= \frac{c\sum_i a_i x_m^i}{c\sum_j b_j x_m^j} \\ &= \frac{\sum_i ca_i x_m^i}{\sum_j cb_j x_m^j} \\ &\in R[x_1, \cdots, x_{m-1}](x_m). \end{aligned}$$

(2) Hence,

$$\begin{aligned} T &= S(w_1, \ldots, w_m) \\ &= R(v_1, \ldots, v_n)(w_1, \ldots, w_m) \\ &= R(v_1, \ldots, v_n)(w_1)\cdots(w_m) \\ &= R(v_1)\cdots(v_n)(w_1)\cdots(w_m) \\ &= R(v_1, \ldots, v_n, w_1, \ldots, w_m). \end{aligned}$$

□

1.9. Integral Elements

Problem 1.46.* (Transitivity of integral extensions)

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

Proof (Hint).

(1) Let $z \in T$, so we have $z^n + a_1 z^{n-1} + \cdots + a_n = 0$, $a_i \in S$. Therefore, z is integral over $R[a_1, \ldots, a_n]$, or $R[a_1, \ldots, a_n, z]$ is module-finite over $R[a_1, \ldots, a_n]$.

(2) *Show that $R[a_1, \ldots, a_n]$ is module-finite over R if all $a_i \in S$.* Note that

$$\begin{aligned}&a_1 \text{ is integral over } R,\\ &a_2 \text{ is integral over } R[a_1] \supseteq R,\\ &\cdots\\ &a_n \text{ is integral over } R[a_1, \ldots, a_{n-1}].\end{aligned}$$

By Proposition 3,

$$\begin{aligned}&R[a_1] \text{ is module-finite over } R,\\ &R[a_1][a_2] \text{ is module-finite over } R[a_1],\\ &\cdots\\ &R[a_1, \ldots, a_{n-1}][a_n] \text{ is module-finite over } R[a_1, \ldots, a_{n-1}].\end{aligned}$$

Also note that $R[a_1, \ldots, a_i] = R[a_1, \ldots, a_{i-1}][a_i]$ if $i > 1$. By the transitive relation of the module-finiteness (Problem 1.45), $R[a_1, \ldots, a_n]$ is module-finite over R.

(3) Again by the transitive relation of the module-finiteness (Problem 1.45), $R[a_1, \ldots, a_n, z]$ is module-finite over R. Hence, $R[a_1, \ldots, a_n, z]$ is a subring of T containing $R[z]$ which is module-finite over R. By Proposition 3, z is integral over R.

□

Problem 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.

(1) Write $S = R[v_1, \ldots, v_m]$ for some $v_i \in S$.

(2) Suppose that S is integral over R. Then all v_i are integral over R. Use the same argument in Problem 1.46, we have

$$S = R[v_1, \ldots, v_n]$$

is module-finite over R.

(3) Conversely, suppose that S is module-finite over R. Take any $v \in S$. Write $v = \sum_i r_i v_i \in S$ since S is module-finite over R. Note that $S = R[v_1, \ldots, v_m]$ is a subring of S itself containing $R[v]$ which is module-finite over R. By Proposition 3, v is integral over R.

$\square$

Problem 1.48.*

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

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

(b) *An algebraically closed field has no module-finite field extensions except itself.*

Proof of (a).

(1) Let $\alpha \in L$ be algebraic over k. Then there is a nonzero polynomial $f(x) \in k[x]$ with $f(\alpha) = 0$. Note that $\deg f \geq 1$.

(2) Since k is algebraically closed, every polynomial is a product of first degree polynomials, say
$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_m)$$
where $c \in k - \{0\}$ and $\alpha_1, \ldots, \alpha_m \in k$. As $f(\alpha) = 0$, $\alpha = \alpha_i \in k$ for some $1 \leq i \leq m$. Hence, $\alpha \in L$ is algebraic over k implies that $\alpha \in k$.

$\square$

Proof of (b).

(1) Suppose that L is module-finite field extensions of an algebraically closed field k.

(2) By Problem 1.41, L is ring-finite over k. By Problem 1.47, L is integral or algebraic over k (since k is a field). By (a), $L = k$.

$\square$

Problem 1.49.*

Let K be a field, $L = K(x)$ the field of rational functions in one variable over K.

(a) *Show that any element of L that is integral over $K[x]$ is already in $K[x]$. (Hint: If $z^n + a_1 z^{n-1} + \cdots + a_n = 0$, write $z = f/g$, f, g relatively prime. Then $f^n + a_1 f^{n-1} g + \cdots + a_n g^n = 0$, So g divides f.)*

(b) *Show that there is no nonzero element $f \in K[x]$ such that for every $z \in L$, $f^n z$ is integral over $K[x]$ for some $n > 0$. (Hint: See Problem 1.44.)*

Proof of (a).

(1) Note that 0 is integral over $K[x]$ and $0 \in K[x]$ trivially.

(2) Now we take any nonzero element $z \in L = K(x)$ which is integral over $K[x]$. So $z^n + a_1 z^{n-1} + \cdots + a_n = 0$ for some $a_1, \ldots, a_n \in K[x]$ and $a_n \neq 0$ (since $z \neq 0$).

(3) Write $z = f/g$, f, g relatively prime in $K[x]$. Then

$$f^n + a_1 f^{n-1} g + \cdots + a_n g^n = 0 \in K[x].$$

Since $a_n \neq 0$, $g \mid f^n$ or $g \mid f$ or $g = 1 \in K$. Therefore, $z = f \in K[x]$.

□

Proof of (b).

(1) (Reductio ad absurdum) Suppose there were a nonzero element $f \in K[x]$ such that for every $z \in L$, $f^n z$ is integral over $K[x]$ for some $n > 0$.

(2) Let $z = 1/g \in K(x)$, where g is an irreducible polynomial not dividing f. The existence of g is guaranteed by Problem 1.5.

(3) By the hypothesis in (1), there is an integer $n > 0$ such that $f^n z$ is integral over $K[x]$. By (a), $f^n z = f^n/g$ is also in $K[x]$. So $g \mid f^n$ or $g \mid f$, which is absurd.

□

Problem 1.50.*

Let K be a subfield of a field L.

(a) *Show that the set of elements of L that are algebraic over K is a subfield of L containing K. (Hint: If $v^n + a_1 v^{n-1} + \cdots + a_n = 0$, and $a_n \neq 0$, then $v(v^{n-1} + \cdots + a_{n-1}) = -a_n$.)*

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

Proof of (a).

(1) Let R be the set of elements of L that are algebraic over K. By Corollary to Proposition 3, R is a subring of L containing K. (Note that K is a field.) So it suffices to show that $v^{-1} \in R$ if $v \in R - \{0\}$.

(2) Since v is algebraic over K, we can write

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

for some $a_1, \ldots, a_n \in K$ and $a_n \neq 0$. So

$$\left(v^{-1}\right)^n + \underbrace{\frac{a_{n-1}}{a_n}}_{\in K} \left(v^{-1}\right)^{n-1} + \cdots + \underbrace{\frac{a_1}{a_n}}_{\in K} \left(v^{-1}\right) + \underbrace{\frac{1}{a_n}}_{\in K} = 0,$$

or v^{-1} is integral over K. Hence, $v^{-1} \in R$.

□

Proof of (b).

(1) By Problem 1.47, L is algebraic over K. Hence, R is algebraic over K.

(2) To show that R is a field, it suffices to show that $v^{-1} \in R$ if $v \in R - \{0\}$. Since v is algebraic over K, we can write

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

for some $a_1, \ldots, a_n \in K$ and $a_n \neq 0$. So

$$v \left(- \underbrace{\frac{1}{a_n}}_{\in K \subseteq R} \underbrace{v^{n-1}}_{\in R} - \cdots - \underbrace{\frac{a_{n-1}}{a_n}}_{\in K \subseteq R} \right) = 1.$$

Here $v^{-1} = \left(-\frac{1}{a_n} v^{n-1} - \cdots - \frac{a_{n-1}}{a_n} \right)$ is the inverse of v in R (since R is a ring containing K).

□

1.10. Field Extensions

Problem 1.51.*

Let K be a field, $f \in K[x]$ an irreducible monic polynomial of degree $n > 0$.

(a) *Show that* $L = K[x]/(f)$ *is a field, and if* $\overline{x}$ *is the residue of* x *in* L*, then* $f(\overline{x}) = 0$.

(b) *Suppose* L' *is a field extension of* K*,* $y \in L'$ *such that* $f(y) = 0$*. Show that the homomorphism from* $K[x]$ *to* L' *that takes* x *to* y *induces an isomorphism of* L *with* $K(y)$.

(c) *With* L'*,* y *as in (b), suppose* $g \in K[x]$ *and* $g(y) = 0$*. Show that* f *divides* g.

(d) *Show that* $f = (x - \overline{x})f_1$*,* $f_1 \in L[x]$.

Proof of (a).

(1) (f) is a prime ideal in a UFD $K[x]$ since f is irreducible. Note that $K[x]$ is also a PID, (f) is maximal (Problem 1.3). Hence $L = K[x]/(f)$ is a field.

(2) $f(\overline{x}) = f(x) + (f(x)) = (f(x)) = \overline{0}$.

$\square$

Proof of (b).

(1) Let $\alpha : K[x] \to L'$ be a homomorphism defined by

$$\alpha\left(\sum a_i x^i\right) = \sum a_i y^i$$

where $a_i \in K$. $\mathrm{im}(\alpha) = K(y)$ clearly.

(2) Note that $\ker(\alpha)$ is an ideal containing (f) since $\alpha(f) = 0$. $\ker(\alpha)$ is proper since $\alpha(1) = 1 \neq 0$. By the maximality of (f), $\ker(\alpha) = (f)$.

(3) Hence, α induces an isomorphism of L with $K(y)$:

$$L = K[x]/(f) \cong K(y) \hookrightarrow L'.$$

$\square$

Proof of (c). By (b), $g \in \ker(\alpha) = (f)$. So $f \mid g$. $\square$

Proof of (d).

(1) By (a), $\overline{x} \in L$ is a root of $f \in L[x]$ (by embedding $K[x]$ in $L[x]$).

(2) Since L is a field, by Problem 1.7(b) we have

$$f = (x - \overline{x})f_1$$

for some $f_1 \in L[x]$.

$\square$

Problem 1.52.* (Splitting fields)

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

Proof.

(1) Let $p(x) \in K[x]$ be an irreducible factor of $f(x) \in K[x]$, and let L' be the field $K[x]/(p(x))$ (by Problem 1.51(a)).

(2) Then we might regard K as a subfield of L' by sending $a \in K$ to $\overline{a} = a + (p(x)) \in L'$.

(3) By Problem 1.51(a), $\overline{x}$ is a root of $p \in L'$; therefore is a root of f.

(4) Induction on n. By (1)(2)(3), there is a field $L' \supseteq K$ such that L' contains a root $\overline{x}$ of $f(x)$, say $f(x) = (x - \overline{x})f_1(x)$ over $L'[x]$ (by Problem 1.51(d)). By induction, there is a field $L \supseteq L'$ such that f_1 splits over L. Hence, f splits over L.

□

Problem 1.53.*

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

Proof.

(1) Since $f \in K[x]$ is irreducible over K, $\gcd(f, f_x)$ is 1 or f. As $\mathrm{char}(K) = 0$, $\deg(f_x) = \deg(f) - 1$. So f does not divide f_x or $\gcd(f, f_x) = 1$. Hence, there are polynomials $g, h \in K[x]$ such that

$$1 = fg + f_x h.$$

This equation is also true in $L[x]$.

(2) Note that

$$\begin{aligned} f &= \prod_{i=1}^{n}(x - x_i) \in L[x], \\ f_x &= \sum_{i=1}^{n}(x - x_1)\cdots\widehat{(x - x_i)}\cdots(x - x_n) \in L[x]. \end{aligned}$$

If $\overline{x}$ were a multiple root of f, then $f(\overline{x}) = f_x(\overline{x}) = 0$. By (1),

$$1 = f(\overline{x})g(\overline{x}) + f_x(\overline{x})h(\overline{x}) = 0,$$

which is absurd.

□

Problem 1.54.*

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

(a) *For any $v \in L$, show that there is a nonzero $a \in R$ such that av is integral over R.*

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

Proof of (a).

(1) Take any $v \in L$, which is algebraic over K. Write

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

for some $a_1, \ldots, a_n \in K$ and $a_n \neq 0$. Since K is the quotient field of R, there is a common denominator $a \in R$ of $a_1, \ldots, a_n$. Here $a \neq 0$ and $aa_i \in R$ for all $1 \leq i \leq n$.

(2) Hence,

$$\begin{aligned} & a^n v^n + a^n a_1 v^{n-1} + \cdots + a^n a_n = 0 \\ \Longleftrightarrow\ & (av)^n + \underbrace{(aa_1)}_{\in R}(av)^{n-1} + \underbrace{a(aa_2)}_{\in R}(av)^{n-2} + \cdots + \underbrace{a^{n-1}(aa_n)}_{\in R} = 0. \end{aligned}$$

av is integral over R.

□

Proof of (b).

(1) Since L be a finite algebraic extension of K, there exists a basis

$$\{w_1, \ldots, w_n\}$$

for L over K (as a vector space).

(2) For each $w_i \in L$, there is a nonzero $a_i \in R$ such that $a_i w_i$ is integral over R (by (a)). So it suffices to show that

$$\{a_1 w_1, \ldots, a_n w_n\}$$

is also a basis for L over K.

(3) Suppose

$$0 = \sum_i \alpha_i (a_i w_i) = \sum_i (\alpha_i a_i) w_i$$

for some $\alpha_1, \ldots, \alpha_n \in K$. Since $\{w_1, \ldots, w_n\}$ is a basis, $\alpha_i a_i = 0$ for all i, or $\alpha_i = 0$ for all i (since all $a_i \neq 0$). Hence $\{a_1 w_1, \ldots, a_n w_n\}$ is linearly independent.

(4) Also, for any $w \in L$, we can write

$$\begin{aligned} w &= \underbrace{\beta_1}_{\in K} w_1 + \cdots + \underbrace{\beta_n}_{\in K} w_n \\ &= \underbrace{\frac{\beta_1}{a_1}}_{\in K} (a_1 w_1) + \cdots + \underbrace{\frac{\beta_n}{a_n}}_{\in K} (a_n w_n) \end{aligned}$$

as a linear combination of $\{a_1 w_1, \ldots, a_n w_n\}$ over K.

□

Chapter 2: Affine Varieties

2.1. Coordinate Rings

Problem 2.1.*

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

Proof.

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

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

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

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

(3) *Show that* $\ker(\alpha) = I(V)$. In fact, given any $f \in k[x_1, \dots, x_n]$, 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,

$$k[x_1, \dots, x_n]/I(V) = \Gamma(V) \cong \{\text{polynomial functions in } \mathscr{F}(V, k)\}$$

as a ring isomorphism.

□

Problem 2.2.*

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

Proof. Repeat Problem 1.38 by replacing $k[x_1, \dots, x_n]/I$ by $\Gamma(V)$. □

Problem 2.3.*

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

(a) *Show that every polynomial function on V restricts to a polynomial function on W.*

(b) *Show that the map from $\Gamma(V)$ to $\Gamma(W)$ defined in part (a) is a surjective homomorphism with kernel $I_V(W)$, so that $\Gamma(W)$ is isomorphic to $\Gamma(V)/I_V(W)$.*

Proof of (a).

(1) Given any polynomial function $f \in \mathscr{F}(V,k)$ on V. There is a polynomial $g \in k[x_1, \ldots, x_n]$ such that $f(P) = g(P)$ for all $P \in V \supseteq W$; thus $f(P) = g(P)$ for all $P \in W$, or $f|_W$ is a polynomial function on W.

(2) The map $\alpha : \{\text{polynomial functions in } \mathscr{F}(V,k)\} \to \{\text{polynomial functions in } \mathscr{F}(W,k)\}$ in (1) is defined by
$$\alpha(f) = f|_W.$$
It is a ring homomorphism.

□

Proof of (b).

(1) Identify $\Gamma(V)$ (resp. $\Gamma(W)$) with the set of all polynomial functions in $\mathscr{F}(V,k)$ (resp. in $\mathscr{F}(W,k)$) by Problem 2.1. The map
$$\alpha : \Gamma(V) \to \Gamma(W)$$
is defined by
$$\alpha(f + I(V)) = f + I(W).$$
It is well-defined by (a).

(2) *Show that α is surjective.* For any $f + I(W) \in \Gamma(W)$, take $f + I(V) \in \Gamma(V)$ and then $\alpha(f + I(V)) = f + I(W)$. (The choice of $f + I(V)$ depends on the representation of $f + I(W)$ and thus might not be unique.)

(3) *Show that $\ker(\alpha) = I_V(W)$, and thus $\Gamma(W) \cong \Gamma(V)/I_V(W)$.* Since α is a surjective homomorphism,
$$\begin{aligned}
\ker(\alpha) &= \Gamma(V)/\Gamma(W) \\
&= (k[x_1, \ldots, x_n]/I(V))/(k[x_1, \ldots, x_n]/I(W)) \\
&= I(W)/I(V) \\
&= I_V(W).
\end{aligned}$$

□

Problem 2.4.*

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

(i) *V is a point.*

(ii) *$\Gamma(V) = k$.*

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

Proof.

(1) (i) $\Longrightarrow$ (ii). By Corollary 2 to the Hilbert's Nullstellensatz in §1.7, $V = \{(a_1, \ldots, a_n)\}$ corresponds to the maximal ideal

$$I(V) = (x_1 - a_1, \ldots, x_n - a_n)$$

in $k[x_1, \ldots, x_n]$. Hence,

$$\Gamma(V) = k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \cong k$$

(by Problem 1.24).

(2) (ii) $\Longrightarrow$ (iii). $\dim_k(\Gamma(V)) = \dim_k(k) = 1 < \infty$.

(3) (iii) $\Longrightarrow$ (i). By Corollary 4 to the Hilbert's Nullstellensatz in §1.7, V is a finite set of points in $\mathbf{A}^n$. Since V is a nonempty variety, V is exactly a point.

$\square$

Problem 2.5.

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

Proof.

(1) $\Gamma(V) = k[x, y]/(f)$ is well-defined since f is irreducible. Define a ring homomorphism $\alpha : k[x] \to \Gamma(V) = k[x, y]/(f)$ by

$$\alpha : g(x) \mapsto g(x) + (f(x, y)).$$

(2) *Show that α is one-to-one.* If there were a nonzero polynomial $g \in k[x]$ such that $\alpha(g) = 0$, then $g = fh$ for some nonzero polynomial $h \in k[x,y]$. Hence

$$0 = \deg_y(g) = \deg_y(f) + \deg_y(h) \geq n > 0,$$

which is absurd. Therefore, α is one-to-one. Hence $k[x]$ may be regarded as a subring of $\Gamma(V)$, and thus the multiplication in $\Gamma(V)$ makes $\Gamma(V)$ a $k[x]$-module.

(3) Given any $g(x,y) + (f(x,y)) \in k[x,y]/(f)$ where $g \in k[x,y] = (k[x])[y]$. By the division-with-remainder property of $(k[x])[y]$,

$$g = fq + r$$

for some $q, r \in (k[x])[y]$ and

$$r = r_1(x)y^{n-1} + \cdots + r_n(x)$$

where $r_1, \ldots, r_n \in k[x]$. Hence

$$\begin{aligned} g + (f) &= fq + r + (f) \\ &= r + (f) \\ &= r_1(x)y^{n-1} + \cdots + r_n(x) + (f) \\ &= \underbrace{r_1(x)}_{\in k[x]}\overline{y}^{n-1} + \cdots + \underbrace{r_n(x)}_{\in k[x]}\overline{1}, \end{aligned}$$

which means that the residues $\overline{1}, \overline{y}, \ldots, \overline{y}^{n-1}$ generate $\Gamma(V)$ over $k[x]$ as a module.

□

2.2. Polynomial Maps

Problem 2.6.*

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

Proof.

(1) *Show that $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi}$.* It is equivalent to show that

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

for all $f \in \mathscr{F}(Z, k)$. In fact,

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

(2) *Show that the composition of polynomial maps is a polynomial map.* Say $V \subseteq \mathbf{A}^n, W \subseteq \mathbf{A}^m, Z \subseteq \mathbf{A}^r$. Since φ (resp. ψ) is a polynomial map, there are polynomials $t_1, \ldots, t_m \in k[x_1, \ldots, x_n]$ (resp. $s_1, \ldots, s_r \in k[x_1, \ldots, x_m]$) such that

$$\begin{aligned}\varphi(P) &= (t_1(P), \ldots, t_m(P))\\ \psi(Q) &= (s_1(Q), \ldots, s_r(Q))\end{aligned}$$

for all $P \in V$ (resp. $Q \in W$). Hence the composition $\psi \circ \varphi$ is

$$\begin{aligned}(\psi \circ \varphi)(P) &= \psi(\varphi(P))\\ &= \psi(t_1(P), \ldots, t_m(P))\\ &= (s_1(t_1(P), \ldots, t_m(P)), \ldots, s_r(t_1(P), \ldots, t_m(P))).\end{aligned}$$

So there are polynomials $y_1, \ldots, y_r \in k[x_1, \ldots, x_n]$ defined by

$$y_i(P) = s_i(t_1(P), \ldots, t_m(P))$$

for all $(a_1, \ldots, a_n) \in \mathbf{A}^n$ such that

$$(\psi \circ \varphi)(P) = (y_1(P), \ldots, y_r(P)).$$

(Note that the composition of polynomials is a polynomials.) Hence $\psi \circ \varphi$ is a polynomial map.

$\square$

Problem 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.

(1) *Show that $\varphi^{-1}(X) = V(\widetilde{\varphi}(I(X)))$ is algebraic.*

$$\begin{aligned}P \in \varphi^{-1}(X) &\Longleftrightarrow \varphi(P) \in X\\ &\Longleftrightarrow f(\varphi(P)) = 0 \,\forall f \in I(X)\\ &\Longleftrightarrow \widetilde{\varphi}(f)(P) = 0 \,\forall f \in I(X)\\ &\Longleftrightarrow g(P) = 0 \,\forall g \in \widetilde{\varphi}(I(X))\\ &\Longleftrightarrow P \in V(\widetilde{\varphi}(I(X))).\end{aligned}$$

Also note that $\widetilde{\varphi}(I(X))$ is an ideal in $k[x_1, \ldots, x_n]$ since φ is a polynomial map.

(2) *If $\varphi^{-1}(X)$ is irreducible, and X is contained in the image of φ, show that X is irreducible.* (Reductio ad absurdum) Suppose that X were reducible or $I(X)$ were not prime. So that there exist two polynomials $f_1, f_2 \notin I(X)$ but $f_1 f_2 \in I(X)$. By definition of $I(X)$, there exist two points $P_1, P_2 \in X$ such that $f_i(P_i) \neq 0$ for $i = 1, 2$.

(3) Since X is contained in the image of φ, there are two corresponding points $Q_1, Q_2 \in \varphi^{-1}(X)$ such that $\varphi(Q_i) = P_i$. So $\widetilde{\varphi}(f_i)(Q_i) = f_i(P_i) \neq 0$, or $\widetilde{\varphi}(f_i) \notin I(\varphi^{-1}(X))$. However

$$\widetilde{\varphi}(f_1)\widetilde{\varphi}(f_2) = \widetilde{\varphi}(f_1 f_2) \in I(\varphi^{-1}(X))$$

since $f_1 f_2 \in I(X)$, contrary to the primality of $I(\varphi^{-1}(X))$.

□

Problem 2.8.

(a) *Show that $\{(t, t^2, t^3) \in \mathbf{A}^3(k) : t \in k\}$ is an affine variety.*

(b) *Show that $V(xz - y^2, yz - x^3, z^2 - x^2 y) \subseteq \mathbf{A}^3(\mathbb{C})$ is a variety. (Hint: $y^3 - x^4$, $z^3 - x^5$, $z^4 - y^5 \in I(V)$. Find a polynomial map from $\mathbf{A}^1(\mathbb{C})$ onto V.)*

Proof of (a).

(1) Let $Y := \{(t, t^2, t^3) \in \mathbf{A}^3(k) : t \in k\}$ be the twisted cubic curve. By Problem 2.7, it suffices to show that there is a polynomial map from $\mathbf{A}^1(k)$ onto Y. Here we use the fact that $\mathbf{A}^1(k)$ is irreducible as $k = \overline{k}$ is infinite (by Problem 1.29).

(2) Define a mapping φ from $\mathbf{A}^1(k)$ to Y by $\varphi(t) = (t, t^2, t^3) \in Y$. φ is a polynomial map. Also, φ is surjective.

□

Note. Also see Problems 1.11 and 1.33 (for the case $k = \mathbb{C}$).

Proof of (b).

(1) We prove for any algebraically closed field k.

(2) Write

$$V = V(xz - y^2, yz - x^3, z^2 - x^2 y),$$
$$Y = \{(t^3, t^4, t^5) \in \mathbf{A}^3(k) : t \in k\}.$$

We want to show that $Y = V$. $Y \subseteq V$ is trivial. Now given any $(x, y, z) \in V$. If $x = 0$, then $y = z = 0$. So $(x, y, z) = (0, 0, 0) \in Y$. If $x \neq 0$, define

$$t = \frac{y}{x} \in k.$$

Hence,

$$\begin{aligned} t^3 &= \frac{y^3}{x^3} = \frac{y(xz)}{x^3} = \frac{yz}{x^2} = \frac{x^3}{x^2} = x, \\ t^4 &= tx = y, \\ t^5 &= ty = \frac{y^2}{x} = \frac{xz}{x} = z. \end{aligned}$$

(3) Same as (a). Define a mapping φ from $\mathbf{A}^1(k)$ to $Y = V$ by $\varphi(t) = (t^3, t^4, t^5) \in Y = V$.

$\square$

Note.

(1) We don't use the hint.

(2) In fact, it is easy to show that

$$Y = V(y^3 - x^4, z^3 - x^5, z^4 - y^5).$$

(3) $I(V)$ is a prime ideal of height 2 in $k[x, y, z]$ which cannot be generated by 2 elements. We say V is **not a local complete intersection**.

Problem 2.9.*

Let $\varphi : V \to W$ be a polynomial map of affine varieties, $V' \subseteq V$, $W' \subseteq W$ subvarieties. Suppose $\varphi(V') \subseteq W'$.

(a) *Show that $\widetilde{\varphi}(I_W(W')) \subseteq I_V(V')$ (see Problems 2.3).*

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

Proof of (a).

(1) It suffices to show that $f \in I_V(V')$ for any $f = \widetilde{\varphi}(g) \in \widetilde{\varphi}(I_W(W'))$ for some $g \in I_W(W')$.

(2) To show $f \in I_V(V')$, it suffices to show that $f(P) = 0$ for all $P \in \varphi(V')$. In fact,

$$f(P) = \widetilde{\varphi}(g)(P) = g(\varphi(P)) = 0$$

since $\varphi(V') \subseteq W'$ and $g \in I_W(W')$.

□

Proof of (b).

(1) Similar to Problem 2.3.

(2) Since φ is a polynomial map, there are polynomials $t_1, \dots, t_m \in k[x_1, \dots, x_n]$ such that
$$\varphi(P) = (t_1(P), \dots, t_m(P)) \in W$$
for all $P \in V$. So that $\varphi|_{V'} : V' \to \varphi(V') \subseteq W'$ is also a polynomial map which is equipped with the same polynomials $t_1, \dots, t_m$ such that
$$\varphi(P) = (t_1(P), \dots, t_m(P)) \in W' \subseteq W$$
for all $P \in V' \subseteq V$. (Note that both V' and W' are affine varieties.)

□

Problem 2.10.*

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

Proof.

(1) Define $t_i \in k[x_1, \dots, x_n]$ by $t_i(x_1, \dots, x_n) = x_i$ for $i = 1, \dots, r$.

(2) Clearly,
$$\mathrm{pr}(P) = (t_1(P), \dots, t_r(P))$$
for $P = (a_1, \dots, a_n) \in \mathbf{A}^n$, and thus pr is a polynomial map.

□

Problem 2.11.

Let $f \in \Gamma(V)$, V *a variety* $\subseteq \mathbf{A}^n$. *Define*
$$G(f) = \{(a_1, \dots, a_n, a_{n+1}) \in \mathbf{A}^{n+1} \\ : (a_1, \dots, a_n) \in V \text{ and } a_{n+1} = f(a_1, \dots, a_n)\},$$
*the **graph** of* f. *Show that* $G(f)$ *is an affine variety, and that the map* $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, f(a_1, \dots, a_n))$ *defines an isomorphism of* V *with* $G(f)$. *(Projection gives the inverse.)*

Proof.

(1) Define $I = I(V)$ as an ideal in $k[x_1, \ldots, x_n]$. Note that

$$G(f) = V\underbrace{(I, x_{n+1} - f)}_{:=J}.$$

Here we can view I as an ideal of $k[x_1, \ldots, x_n, x_{n+1}]$.

(2) To show that $G(f)$ is an affine variety, it suffices to show that

$$I(G(f)) = I(V(J)) = \mathrm{rad}(J)$$

is prime (by Proposition 1 in §1.5 and the Hilbert's Nullstellensatz in §1.7). Suppose $gh \in I(G(f)) = \mathrm{rad}(J)$. Write

$$g = \sum_i g_i x_{n+1}^i = \sum_i g_i(\underbrace{(x_{n+1} - f)}_{\in J} + f)^i,$$

$$h = \sum_j h_j x_{n+1}^j = \sum_j h_j(\underbrace{(x_{n+1} - f)}_{\in J} + f)^j$$

where $g_i, h_j \in k[x_1, \ldots, x_n]$.

(3) Hence

$$\begin{aligned}
\mathrm{rad}(J) &= gh + \mathrm{rad}(J) && (gh \in \mathrm{rad}(J)) \\
&= (g + \mathrm{rad}(J))(h + \mathrm{rad}(J)) \\
&= \left(\sum_i g_i f^i + \mathrm{rad}(J)\right)\left(\sum_j h_j f^j + \mathrm{rad}(J)\right) && (x_{n+1} - f \in J) \\
&= \left(\sum_i g_i f^i\right)\left(\sum_j h_j f^j\right) + \mathrm{rad}(J)
\end{aligned}$$

or

$$\underbrace{\left(\sum_i g_i f^i\right)^N \left(\sum_j h_j f^j\right)^N}_{\in k[x_1, \ldots, x_n]} \in J = (I, x_{n+1} - f)$$

for some positive integer N. So that $\left(\sum_i g_i f^i\right)^N \left(\sum_j h_j f^j\right)^N \in I$.

(4) Since $I = I(V)$ is a prime ideal, we might get $\sum_i g_i f^i \in I \subseteq \mathrm{rad}(J)$. (The case $\sum_j h_j f^j$ is similar.) Hence $\mathrm{rad}(J) = I(G(f))$ is a prime ideal, or $G(f)$ is irreducible.

(5) As $G(f)$ is an affine variety, the map $\alpha : V \to G(f)$ defined by

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

is a polynomial map. (Here $t_1 = x_1, \ldots, t_n = x_n$ and $t_{n+1} = f$.)

(6) By Problem 2.10, the projection map pr is a polynomial map. Also note that $\mathrm{pr} \circ \alpha = 1_V$ and $\alpha \circ \mathrm{pr} = 1_{G(f)}$. Therefore, $V \cong G(f)$ as an affine variety isomorphism.

$\square$

2.3. Coordinate Changes

2.4. Rational Functions and Local Rings

2.5. Discrete Valuation Rings

Problem 2.23.*

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

Proof.

(1) *Show that a uniformizing parameter is unique up to a unit.* Suppose t and t' are two uniformizing parameters for a discrete valuation ring R with the quotient field K. Since R is a DVR, the maximal ideal is

$$\mathfrak{m} = (t) = (s).$$

As $s \in (t)$, there is an element $a \in R$ such that $s = at$. As s is irreducible (by the maximality of $\mathfrak{m}$), a is a unit or t is a unit (which is impossible). Hence $s = at$ for some unit $a \in R$.

(2) For any $z \in K$, write

$$z = ut^n = vs^m$$

for some units u, v and integers $n \geq m$. (The case $n \leq m$ is similar.) Replace $s = at$ to get $ut^n = va^m t^m$. So $t^{n-m} = u^{-1}va^m$ is a unit. Hence, $m = n$, or the order function on K is independent of the choice of uniformizing parameter.

$\square$

Problem 2.24.*

Let $V = \mathbf{A}^1$, $\Gamma(V) = k[x]$, $K = k(V) = k(x)$.

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

(b) *Show that $\mathcal{O}_\infty = \{f/g \in k(x) : \deg(g) \geq \deg(f)\}$ is also a DVR, with uniformizing parameter $t = 1/x$.*

Proof of (a).

(1) By Proposition 7 in §2.4, $\mathcal{O}_a(V)$ is a (Noetherian) local domain. It suffices to show that $t = x - a$ is an irreducible element in $\mathcal{O}_a(V)$ such that every nonzero $z \in \mathcal{O}_a(V)$ might be written uniquely in the form $z = ut^n$, u a unit in $\mathcal{O}_a(V)$, n a nonnegative integer (by Proposition 4).

(2) Write $z = f/g \in \mathcal{O}_a(V)$ where $g(a) \neq 0$. By Problem 1.7,

$$f = \sum_{i=0}^{\deg(f)} \lambda_i (x-a)^i.$$

Let n be the smallest integer such that $\lambda_n \neq 0$. (Such n is existed since z or f is nonzero.) Hence, $f = f_1(x-a)^n$ where $f_1 = \sum_{i=n}^{\deg(f)} \lambda_i (x-a)^{i-n} \neq 0$ and $f_1(a) = \lambda_n \neq 0$. So

$$z = f/g = (f_1/g)(x-a)^n.$$

Here f_1/g is a unit in $\mathcal{O}_a(V)$. Besides, it is easy to show that n is unique by the similar argument in Problem 2.23. Hence, $\mathcal{O}_a(V)$ is a DVR with uniformizing parameter $t = x - a$.

□

Proof of (b).

(1) *Show that $\mathcal{O}_\infty$ is a subring of $k(x)$.* Clearly, $1 = 1/1 \in \mathcal{O}_\infty$. Also, given any $f = a/b, g = c/d \in \mathcal{O}_\infty$. So

$$f - g = a/b - c/d = \frac{ad - bc}{bd} \in \mathcal{O}_\infty$$
$$fg = a/b \cdot c/d = \frac{ac}{bd} \in \mathcal{O}_\infty$$

since

$$\begin{aligned}
\deg(ad - bc) &\leq \max(\deg(ad), \deg(bc)) \\
&\leq \max(\deg(a) + \deg(d), \deg(b) + \deg(c)) \\
&\leq \max(\deg(b) + \deg(d), \deg(b) + \deg(d)) \\
&\leq \deg(b) + \deg(d) \\
&\leq \deg(bd)
\end{aligned}$$

and
$$\deg(ac) = \deg(a) + \deg(c) \le \deg(b) + \deg(d) = \deg(bd).$$
(Here we define $\deg(0) = -\infty$ by convention.) By the subring test, $\mathcal{O}_\infty$ is a subring of $k(x)$.

(2) *Show that $\mathcal{O}_\infty$ is a DVR.* Clearly $\mathcal{O}_\infty$ is not a field since $1/x \in \mathcal{O}_\infty$ but $x = x/1 \notin \mathcal{O}_\infty$. Let $t = 1/x$ be an irreducible element of $\mathcal{O}_\infty$. ($\deg(x) = 1$ implies the irreducibility of t.) Now for any nonzero $f/g \in \mathcal{O}_\infty$, write
$$f/g = ((fx^n)/g)(1/x^n) = ((fx^n)/g)t^n$$
where $n := \deg(g) - \deg(f) \ge 0$. Note that $\deg(fx^n) = \deg(f) + n = \deg(g)$. So $(fx^n)/g$ is a unit since the inverse $g/(fx^n)$ is also in $\mathcal{O}_\infty$. Besides, it is easy to show that n is unique by the similar argument in Problem 2.23. Hence, $\mathcal{O}_\infty$ is a DVR.

□

Note.

(1) The quotient field of $\mathcal{O}_\infty$ is $K = k(V) = k(x)$.

(2) The set of units in $\mathcal{O}_\infty(V)$ is $\{f/g \in k(x) : \deg(g) = \deg(f)\}$.

(3) The maximal ideal of $\mathcal{O}_\infty(V)$ is $\{f/g \in k(x) : \deg(g) > \deg(f)\}$.

Problem 2.25. (p-adic integers)

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

Proof.

(1) Let
$$\mathbb{Z}_p = \{r \in \mathbb{Q} : r = a/b,\ a, b \in \mathbb{Z},\ p \nmid b\}$$
be the set of all p-adic integers.

(2) *Show that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}$.* Clearly, $1 = 1/1 \in \mathbb{Z}_p$ (since $p \nmid 1$). Also, given any $r = a/b, s = c/d \in \mathbb{Z}_p$. So
$$r - s = a/b - c/d = \frac{ad - bc}{bd} \in \mathbb{Z}_p$$
$$rs = a/b \cdot c/d = \frac{ac}{bd} \in \mathbb{Z}_p$$
since $p \nmid b$, $p \nmid d$ and p is a prime number. By the subring test, $\mathbb{Z}_p$ is a subring of $\mathbb{Q}$.

(3) Note that $\mathbb{Z}_p \subseteq \mathbb{Q}$ is a domain and $\mathbb{Z}_p$ is not a field (since $p = p/1 \in \mathbb{Z}_p$ but $p^{-1} = 1/p \notin \mathbb{Z}_p$).

(4) Let $t = p$ be an irreducible element in $\mathbb{Z}_p$. For the irreducibility of $t = p$, we write $p = a/b \cdot c/d = \frac{ac}{bd}$ where $p \nmid b$, $p \nmid d$. So $pbd = ac$ or

$$1 = \operatorname{ord}_p(ac) = \operatorname{ord}_p(a) + \operatorname{ord}_p(c).$$

Here $\operatorname{ord}_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ is defined by $\operatorname{ord}_p(a) = n$ where n is the largest number such that p^n divides a, that is, $p^n \mid a$ and $p^{n+1} \nmid a$. So $(\operatorname{ord}_p(a), \operatorname{ord}_p(c)) = (0,1)$ or $(1,0)$. Hence, a/b or c/d is a unit in $\mathbb{Z}_p$, or p is irreducible in $\mathbb{Z}_p$.

(5) For any nonzero $r = a/b \in \mathbb{Z}_p$, $a \neq 0$ can be written as $a = p^n c$ for some nonnegative integer n and $c \in \mathbb{Z}^+$ uniquely. Hence

$$r = a/b = (c/b)p^n = (c/b)t^n,$$

where c/b is a unit and n is a nonnegative integer. Besides, it is easy to show that n is unique by the similar argument in Problem 2.23. By Proposition 4, $\mathbb{Z}_p$ is a DVR.

(6) *Show that the quotient field of $\mathbb{Z}_p$ is $\mathbb{Q}$.* It suffices to show that r is in the quotient field of $\mathbb{Z}_p$ if $r \in \mathbb{Q} - \mathbb{Z}_p$. Note that $r \neq 0$. Write $r = a/b$ with $\gcd(a,b) = 1$. As $r \notin \mathbb{Z}_p$, $p \mid b$ and $p \nmid a$. Therefore, $1/r = b/a \in \mathbb{Z}_p$, or r is in the quotient field of $\mathbb{Z}_p$.

□

Note.

(1) $p\mathbb{Z}_p$ is the maximal ideal of $\mathbb{Z}_p$.

(2) The residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Problem 2.26.*

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

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

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

Proof of (a).

(1) Suppose t is one uniformizing parameter for R. If $z \in K - R$, then we can write $z = ut^{-n}$ for some unit $u \in R$ and $n \in \mathbb{Z}^+$.

(2) Hence,
$$z^{-1} = u^{-1}t^n.$$
Since u^{-1} is a unit in R and $n > 0$, $z^{-1} \in \mathfrak{m}$.

$\square$

Proof of (b).

(1) (Reductio ad absurdum) Suppose $z \in S - R \subseteq K - R$. By (a), $z^{-1} \in \mathfrak{m}$. So z^{-1} is in the maximal ideal $\mathfrak{m}'$ of S containing $\mathfrak{m}$.

(2) As $\mathfrak{m}'$ is an ideal, $1 = z \cdot z^{-1} \in \mathfrak{m}'$, which is absurd. Therefore, $S = R$.

$\square$

Problem 2.28.*

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

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

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

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

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

Proof.

(1) *Show that $\varphi(1) = 0$.* Note that $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1)$ by (ii). By Property (i) of φ, we cancel $\varphi(1) \in \mathbb{Z}$ on the both side to get $\varphi(1) = 0$.

(2) *Show that $\varphi(-z) = \varphi(z)$ for all $z \in K$, and $\varphi(z^{-1}) = -\varphi(z)$ for all $z \in K - \{0\}$.* Note that $\varphi(-1) = 0$ since $0 = \varphi(1) = \varphi((-1) \cdot (-1)) = \varphi(-1) + \varphi(-1)$ (by (1)). Therefore,
$$\varphi(-z) = \varphi((-1) \cdot z) = \varphi(-1) + \varphi(z) = \varphi(z).$$
Besides,
$$0 = \varphi(1) = \varphi(zz^{-1}) = \varphi(z) + \varphi(z^{-1})$$
if $z \neq 0$. So $\varphi(z^{-1}) = -\varphi(z)$ if $z \neq 0$.

(3) *Show that $R = \{z \in K : \varphi(z) \geq 0\}$ is a ring.*

(a) $R \neq \varnothing$ since $1 \in R$.

(b) If $a, b \in R$, then

$$\varphi(a-b) \geq \min(\varphi(a), \varphi(-b)) = \min(\varphi(a), \varphi(b)) \geq 0$$

(by (2)), or $a - b \in R$.

(c) If $a, b \in R$, then $\varphi(ab) = \varphi(a) + \varphi(b) \geq 0$.

By the subring test, R is a subring of K.

(4) *Show that* $\{z \in K - \{0\} : \varphi(z) = 0\}$ *is the set of all units in* R. Given any $z \in K - \{0\}$, we have

$$0 = \varphi(z) + \varphi(z^{-1})$$

(by (2)). Hence z is a unit in R iff $z, z^{-1} \in R$ iff $\varphi(z) = \varphi(z^{-1}) = 0$.

(5) *Show that* $\mathfrak{m} = \{z \in K : \varphi(z) > 0\}$ *is a maximal ideal of* R.

(a) If $a, b \in \mathfrak{m}$, then $\varphi(a+b) \geq \min(\varphi(a), \varphi(b)) > 0$.

(b) If $a \in \mathfrak{m}$ and $r \in R$, then $\varphi(ra) = \varphi(r) + \varphi(a) \geq \varphi(a) > 0$.

(c) By (a)(b), $\mathfrak{m}$ is an ideal of R.

(d) Note that each proper ideal in R does not have any unit, that is, such proper ideal is contained in $\{z \in K : \varphi(z) > 0\} = \mathfrak{m}$ exactly (by (4)). Therefore, $\mathfrak{m}$ is maximal. (Such maximal ideal $\mathfrak{m}$ is unique and thus R is a local ring.)

(6) *Show that* R *is a DVR.* It suffices to show that there is an irreducible element $t \in R$ such that every nonzero $z \in R$ may be written uniquely in the form $z = ut^n$, u a unit in R, n a nonnegative integer. Since φ is surjective, there is an element $t \in R$ such that $\varphi(t) = 1$. Note that $t \neq 0$ and irreducible (by using Property (ii) of φ). Hence for any nonzero $z \in R$ with $n := \varphi(z) \in \mathbb{Z}$ and $n \geq 0$, the order of $zt^{-n} \in K$ is

$$\varphi(zt^{-n}) = \varphi(z) - n\varphi(t) = n - n \cdot 1 = 0$$

(by (2)). That is, $zt^{-n} = u$ is a unit in R (by (4)). Hence $z = ut^n$ for some unit $u \in R$ and nonnegative integer n. Note that n is uniquely determined by $\varphi(z)$. By Proposition 4, R is a DVR.

(7) *Show that the quotient field of* R *is* K. Since R is a DVR, the quotient field of R is contained in K. Conversely, given any $z \in K$. If $\varphi(z) \geq 0$, then $z \in R \subseteq K$. If $\varphi(z) < 0$, then $\varphi(z^{-1}) = -\varphi(z) > 0$ or $z^{-1} \in R$. Hence $z = 1/z^{-1} \in K$ is in the quotient field of R.

(8) *Show that giving a DVR with quotient field* K *is equivalent to defining an order function on* K. It suffices to show that $\mathrm{ord}(\cdot)$ on K defines an order function φ on K. By Problem 2.29, it suffices to show that

$$\mathrm{ord}(a+b) \geq \min(\mathrm{ord}(a), \mathrm{ord}(b))$$

if $\operatorname{ord}(a) = \operatorname{ord}(b) := n$. Write $a = ut^n, b = vt^n$ where u, v are units in R. Hence,

$$\begin{aligned}
\operatorname{ord}(a+b) &= \operatorname{ord}(ut^n + vt^n) \\
&= \operatorname{ord}((u+v)t^n) \\
&= \operatorname{ord}(u+v) + n \\
&\geq n && (u+v \in R) \\
&= \min(\operatorname{ord}(a), \operatorname{ord}(b)).
\end{aligned}$$

□

Problem 2.29.*

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

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

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

Proof of (a).

(1) Let t be a uniformizing parameter for R. Given any $a, b \in K$. Write $a = ut^n, b = vt^m$ where u, v are units in R and n, m are integers.

(2) Since $\operatorname{ord}(a) < \operatorname{ord}(b)$, $n < m$. Hence,

$$a + b = (u + vt^{m-n})t^n.$$

To show that $\operatorname{ord}(a+b) = \operatorname{ord}(a) = n$, it suffices to show that $u + vt^{m-n}$ is a unit in R.

(3) (Reductio ad absurdum) Suppose that $u + vt^{m-n}$ were not a unit. Since R is local, the maximal ideal (t) contains all nonunit elements in R. Hence, $u + vt^{m-n} \in (t)$. As $m - n > 0$, $vt^{m-n} \in (t)$ and thus a unit $u \in (t)$, contrary to the maximality of (t).

□

Proof of (b).

(1) Might assume that $\operatorname{ord}(a_1) < \operatorname{ord}(a_j)$ (all $j \neq 1$). In particular, $\operatorname{ord}(a_1) < \infty$.

(2) Similar to (a). Let t be a uniformizing parameter for R. Write $a_i = u_i t^{m_i}$ where u_i are units in R and m_i are integers. ($i = 1, \ldots, n$.) Since $\mathrm{ord}(a_1) < \mathrm{ord}(a_j)$ (all $j \neq 1$), $m_1 < m_j$. Hence,

$$a_1 + \cdots + a_n = (u_1 + \underbrace{u_2 t^{m_2 - m_1} + \cdots + u_n t^{m_n - m_1}}_{\in (t)}) t^{m_1}.$$

So $u_1 + u_2 t^{m_2 - m_1} + \cdots + u_n t^{m_n - m_1}$ is a unit in R.

(3) By (1)(2),

$$\mathrm{ord}(a_1 + \cdots + a_n) = \mathrm{ord}(a_1) < \infty,$$

or $a_1 + \cdots + a_n \neq 0$ (since ord is an order function on K).

□

Problem 2.30.*

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

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

(b) *Let t be a uniformizing parameter for R, $z \in R$. Then for any $n \geq 0$ there are unique $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ and $z_n \in R$ such that*

$$z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}.$$

(Hint: For uniqueness use Problem 2.29; for existence use (a) and induction.)

Proof of (a).

(1) Note that

$$k \xrightarrow{i} R \xrightarrow{\pi} R/\mathfrak{m}$$

is an isomorphism.

(2) For $z + \mathfrak{m} \in R/\mathfrak{m}$, there exists the unique $\lambda \in k$ such that

$$z + \mathfrak{m} = \pi(i(\lambda)) = \pi(\lambda) = \lambda + \mathfrak{m}.$$

So $z - \lambda \in \mathfrak{m}$ for one unique $\lambda \in k$.

□

Proof of (b).

(1) Note that
$$\mathfrak{m} = \{z \in K : \mathrm{ord}(z) > 0\}.$$
By (a),
$$z = \lambda_0 + \underbrace{tz_0}_{\in\mathfrak{m}}$$
for one unique $\lambda_0 \in k$ and $z_0 \in R$. Continue this process or by induction, we have the expression
$$z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}.$$

(2) For the uniqueness, suppose
$$0 = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \cdots + \lambda_n t^n + z_n t^{n+1}.$$
Note that
$$\mathrm{ord}(\lambda_i t^i) = \begin{cases} \infty & (\lambda_i = 0) \\ i & (\lambda_i \neq 0) \end{cases}$$
since every nonzero element in k is a unit in $k \subseteq R$. Also, $\mathrm{ord}(z_n t^{n+1}) = \infty$ if $z_n = 0$; $\mathrm{ord}(z_n t^{n+1}) \geq n+1$ if $z_n \neq 0$.

(3) Suppose i_0 is the smallest integer such that $\lambda_{i_0} \neq 0$, then $\mathrm{ord}(\lambda_{i_0} t^{i_0}) = i_0 < \mathrm{ord}(\lambda_j t^j)$ if $i_0 \neq j$ and $\mathrm{ord}(\lambda_{i_0} t^{i_0}) = i_0 < n+1 \leq \mathrm{ord}(z_n t^{n+1})$. By Problem 2.29(b), such i_0 does not exist. Hence all $\lambda_i = 0$. So as R is a domain, z_n is also equal to 0. Therefore, the uniqueness is established.

□

Problem 2.31.

*Let k be a field. The ring of **formal power series** over k, written $k[[x]]$, is defined to be*
$$\left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in k \right\}.$$
(As with polynomials, a rigorous definition is best given in terms of sequences $(a_0, a_1, \ldots)$ of elements in k; here we allow an infinite number of nonzero terms.) Define the sum by
$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i,$$
and the (Cauchy) product by
$$\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) = \sum c_i x^i,$$

where $c_i = \sum_{j+k=i} a_j b_k$. Show that $k[[x]]$ is a ring containing $k[x]$ as a subring. Show that $k[[x]]$ is a DVR with uniformizing parameter x. Its quotient field is denoted $k((x))$.

Proof.

(1) Two formal power series $\sum a_i x^i$ and $\sum b_i x^i$ in $k[[x]]$ are considered equal if $a_i = b_i$ for all integers $i \geq 0$.

(2) The zero element in $k[[x]]$ is $0 = \sum_{i=0}^{\infty} 0x^i$, and the multiplicative identity is

$$1 = 1 + 0x + \cdots + 0x^n + \cdots .$$

Hence, $k[[x]]$ is a ring (by a tedious argument). Moreover, $k[[x]]$ is a domain (again by a tedious argument).

(3) *Show that $k[[x]] \supseteq k[x]$.* In fact, for any $f = \sum_{i=0}^{n} a_i x^i \in k[x]$, we can write

$$f = a_0 + a_1 x + \cdots + a_n x^n + 0x^{n+1} + \cdots \in k[[x]].$$

(4) *Show that $f = \sum_{i=0}^{\infty} a_i x^i$ is a unit in $k[[x]]$ if and only if $a_0 \neq 0$.* Suppose $g = \sum_{i=0}^{\infty} b_i x^i \in k[[x]]$ such that $fg = 1$. Then

$$\begin{aligned} 1 &= a_0 b_0, \\ 0 &= \sum_{j=0}^{k} a_j b_{k-j}. \end{aligned}$$

So f is not a unit in $k[[x]]$ if $a_0 = 0$. Now if $a_0 \neq 0$ then $b_0 := a_0^{-1} \in k$. Then by observing that

$$\begin{aligned} 0 = \sum_{j=0}^{k} a_j b_{k-j} \Longleftrightarrow a_0 b_k &= -\sum_{j=1}^{k} a_j b_{k-j} \\ \Longleftrightarrow b_k &= -b_0 \sum_{j=1}^{k} a_j b_{k-j}, \end{aligned}$$

we can solve $b_1, b_2, \ldots$ by induction, and $(b_0, b_1, \ldots)$ gives the existence of $g \in k[[x]]$.

(5) By (4), $k[[x]]$ is not a field since $x \in k[[x]]$ but $x^{-1} \notin k[[x]]$. Let $t = x$ be an irreducible element in $k[[x]]$. ($\deg(x) = 1$ implies the irreducibility of t.) Hence every nonzero $f \in k[[x]]$ can be written uniquely in the form

$$f = ux^n$$

where n is the smallest integer such that $a_n \neq 0$. By (4),

$$u = a_n + a_{n+1} x + \cdots$$

is a unit in $k[[x]]$ as $a_n \neq 0$. Besides, it is easy to show that n is unique by the similar argument in Problem 2.23. Therefore, $k[[x]]$ is a DVR with uniformizing parameter x.

$\square$

2.6. Forms

Problem 2.33.

Factor $y^3 - 2xy^2 + 2x^2y + x^3$ into linear factors in $\mathbb{C}[x, y]$.

Proof.

(1) Let $f(x, y) = y^3 - 2xy^2 + 2x^2y + x^3$. Then $f_*(x) = 1 - 2x + 2x^3 + x^3$.

(2) Solve $f_*(x) = 0$ over $\mathbb{C}$ by WolframAlpha (a computational knowledge engine) to get

$$\alpha_1 = -\frac{2}{3} - \frac{10}{3}\sqrt[3]{\frac{2}{79 - 3\sqrt{249}}} - \frac{1}{3}\sqrt[3]{\frac{79 - 3\sqrt{249}}{2}}$$
$$\alpha_2 = -\frac{2}{3} + \frac{5}{3}(1 - \sqrt{3}i)\sqrt[3]{\frac{2}{79 - 3\sqrt{249}}} + \frac{1}{6}(1 + \sqrt{3}i)\sqrt[3]{\frac{79 - 3\sqrt{249}}{2}}$$
$$\alpha_3 = -\frac{2}{3} + \frac{5}{3}(1 + \sqrt{3}i)\sqrt[3]{\frac{2}{79 - 3\sqrt{249}}} + \frac{1}{6}(1 - \sqrt{3}i)\sqrt[3]{\frac{79 - 3\sqrt{249}}{2}}.$$

So $f_*(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

(3) Hence,

$$\begin{aligned} f(x, y) &= (f_*)^* \\ &= ((x - \alpha_1)(x - \alpha_2)(x - \alpha_3))^* \\ &= (x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y). \end{aligned}$$

$\square$

Note. If $f(x, y) = y^3 - 2xy^2 + 2x^2y + 4x^3$, then

$$f(x, y) = (x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)$$

where

$$\alpha_1 = -\frac{1}{6} - \frac{7}{6}\sqrt[3]{\frac{1}{37-3\sqrt{114}}} - \frac{1}{6}\sqrt[3]{37-3\sqrt{114}}$$
$$\alpha_2 = -\frac{1}{6} + \frac{7}{12}(1-\sqrt{3}i)\sqrt[3]{\frac{1}{37-3\sqrt{114}}} + \frac{1}{12}(1+\sqrt{3}i)\sqrt[3]{37-3\sqrt{114}}$$
$$\alpha_3 = -\frac{1}{6} + \frac{7}{12}(1+\sqrt{3}i)\sqrt[3]{\frac{1}{37-3\sqrt{114}}} + \frac{1}{12}(1-\sqrt{3}i)\sqrt[3]{37-3\sqrt{114}}.$$

Problem 2.34.

Suppose $f, g \in k[x_1, \dots, x_n]$ are forms of degree r, $r+1$ respectively, with no common factors (k a field). Show that $f+g$ is irreducible.

Proof.

(1) Suppose $f + g = rs \in k[x_1, \dots, x_n]$. Proposition 5 implies that
$$(f+g)^* = (rs)^* \Longrightarrow x_{n+1}f + g = r^*s^*.$$
Note that $\deg_{x_{n+1}}(x_{n+1}f+g) = 1$. So $\deg_{x_{n+1}}(r^*) = 0$ or $\deg_{x_{n+1}}(s^*) = 0$. Might assume $\deg_{x_{n+1}}(r^*) = 0$. (The case $\deg_{x_{n+1}}(s^*) = 0$ is similar.)

(2) Since $\deg_{x_{n+1}}(r^*) = 0$, $r^* \mid f$ and $r^* \mid g$. Note that $\deg_{x_{n+1}}(r^*) = 0$ implies that $r^* = r$ is a form in $k[x_1, \dots, x_n]$. Hence r is a common factor of f and g, or r is a constant in $k[x_1, \dots, x_n]$. So $f+g$ is irreducible.

□

Problem 2.35.*

(a) *Show that there are $d+1$ monomials of degree d in $R[x,y]$, and $1+2+\cdots+(d+1) = \frac{(d+1)(d+2)}{2}$ monomials of degree d in $R[x,y,z]$.*

(b) *Let $V(d,n) = \{$forms of degree d in $k[x_1, \dots, x_n]\}$, k a field. Show that $V(d,n)$ is a vector space over k, and that the monomials of degree d form a basis. So $\dim V(d,1) = 1$; $\dim V(d,2) = d+1$; $\dim V(d,3) = \frac{(d+1)(d+2)}{2}$.*

(c) *Let $\ell_1, \ell_2, \dots$ and $m_1, m_2, \dots$ be sequences of nonzero linear forms in $k[x,y]$, and assume no $\ell_i = \lambda m_j$, $\lambda \in k$. Let $A_{ij} = \ell_1\ell_2\cdots\ell_i m_1 m_2 \cdots m_j$, $i, j \geq 0$ ($A_{00} = 1$). Show that $\{A_{ij} : i+j = d\}$ forms a basis for $V(d,2)$.*

Proof of (a).

(1) All monomials of degree d in $R[x, y]$ are

$$x^d, x^{d-1}y, \cdots, xy^{d-1}, y^d,$$

or of the form $x^i y^j$ with $i, j \geq 0$ and $i+j = d$. So there are $d+1$ monomials of degree d in $R[x, y]$.

(2) Similar to (1), all monomials of degree d in $R[x, y]$ are of the form $x^i y^j z^k$ with $i, j, k \geq 0$ and $i + j + k = d$. By the stars and bars (combinatorics) method, there are

$$\binom{d+3-1}{3-1} = \frac{(d+2)(d+1)}{2}$$

monomials of degree d in $R[x, y, z]$.

$\square$

Proof of (b).

(1) To show $V(d, n)$ is a vector space, it suffices to show that $V(d, n)$ is a subspace of $k[x_1, \ldots, x_n]$ since $k[x_1, \ldots, x_n]$ is a vector space over k.

(2) Note that $0 \in V(d, n)$ is nonempty. For any $f, g \in V(d, n)$ and $a, b \in k$, we have $af + bg \in V(d, n)$. Hence $V(d, n)$ is subspace.

(3) Let

$$\mathscr{B} = \{x_1^{i_1} \cdots x_n^{i_n} : i_1, \ldots, i_n \geq 0, i_1 + \cdots + i_n = d\}.$$

$\mathscr{B}$ is an independent set, and $\mathscr{B}$ generates $V(d, n)$. So $\mathscr{B}$ is a basis for $V(d, n)$.

(4) Similar to (a),

$$\dim_k V(d, n) = |\mathscr{B}| = \binom{d+n-1}{n-1}$$

by the stars and bars (combinatorics) method. In particular, $\dim V(d, 1) = 1$; $\dim V(d, 2) = d + 1$; $\dim V(d, 3) = \frac{(d+1)(d+2)}{2}$.

$\square$

Proof of (c).

(1) *Show that $\mathscr{B}' := \{A_{ij} : i + j = d\}$ is an independent set.* (Reductio ad absurdum) Suppose that there were a nontrivial linear combination of A_{ij} such that

$$\sum_{i+j=d} c_{ij} A_{ij} = 0.$$

(2) Let p be the smallest index i such that $c_{ij} \neq 0$. Write $q := d - p$. So

$$\begin{aligned}
c_{pq}A_{pq} &= -\sum_{\substack{i+j=d\\ i\neq p, j\neq q}} c_{ij}A_{ij} = -\sum_{\substack{i+j=d\\ i>p, j<q}} c_{ij}A_{ij}\\
\Longleftrightarrow A_{pq} &= -\sum_{\substack{i+j=d\\ i>p, j<q}} \frac{c_{ij}}{c_{pq}} A_{ij}\\
\Longleftrightarrow \ell_1\cdots\ell_p m_1\cdots m_q &= -\sum_{\substack{i+j=d\\ i>p, j<q}} \frac{c_{ij}}{c_{pq}} \ell_1\cdots\ell_p\ell_{p+1}\cdots\ell_i m_1\cdots m_j\\
\Longleftrightarrow m_1\cdots m_q &= -\ell_{p+1}\sum_{\substack{i+j=d\\ i>p, j<q}} \frac{c_{ij}}{c_{pq}} \underbrace{\ell_{p+2}\cdots\ell_i}_{:=1 \text{ if } i=p+1} m_1\cdots m_j\\
\Longleftrightarrow \ell_{p+1} &\mid m_1\cdots m_q.
\end{aligned}$$

Since all ℓ_i, m_j are linear forms, $\ell_{p+1} \mid m_j$ for some $1 \leq j \leq q$, which is absurd since no $\ell_i = \lambda m_j$, $\lambda \in k$. Therefore, $\mathscr{B}'$ is an independent set.

(3) Since

$$|\mathscr{B}'| = d + 1 = \dim_k V(d,2),$$

$\mathscr{B}'$ is also a basis for $V(d,2)$.

□

Problem 2.36.

With the above notation, show that

$$\dim V(d,n) = \binom{d+n-1}{n-1},$$

the binomial coefficient.

Proof. See the proof of Problem 2.35(b). □

2.7. Direct Products of Rings

Problem 2.37.

What are the additive and multiplicative identities in $\bigtimes R_i$? Is the map from R_i to $\bigtimes R_i$ taking a_i to $(0,\dots,a_i,\dots,0)$ a ring homomorphism?

Proof.

(1) $(0, \ldots, 0)$ is the additive identity in $\bigtimes R_i$.

(2) $(1, \ldots, 1)$ is the multiplicative identity in $\bigtimes R_i$.

(3) The map $\alpha : R_i \to \bigtimes R_i$ taking a_i to $(0, \ldots, a_i, \ldots, 0)$ is not a ring homomorphism since

$$\alpha(1) = (0, \ldots, 1, \ldots, 0) \neq (1, \ldots, 1),$$

or α is not multiplicative identity preserving (if R_j is not the zero ring for some $j \neq i$).

□

Problem 2.38.*

Show that if $k \subseteq R_i$, and each R_i is finite-dimensional over k, then $\dim\left(\bigtimes R_i\right) = \sum \dim(R_i)$.

Proof.

(1) In the terminology of linear algebra, $\bigtimes R_i$ is the direct sum $\bigoplus R_i$ of R_i.

(2) Hence,

$$\dim_k\left(\bigoplus R_i\right) = \sum \dim_k(R_i).$$

□

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.

□

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

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

(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

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

$\square$

Problem 2.40.* (Chinese remainder theorem)

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

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

$$I_1^n \cap \cdots \cap I_N^n = (I_1 \cdots I_N)^n = (I_1 \cap \cdots \cap I_N)^n$$

for all n.

Proof of (a).

(1) It suffices to show that $I^m + J^n = R$.

(2) Since $I^m + J^n \subseteq R$ is always true, it suffices to show that $I^m + J^n \supseteq R$. In fact,

$$\begin{aligned} R &= R^{m+n-1} && (1 \in R) \\ &= (I+J)^{m+n-1} && (I, J \text{ are comaximal}) \\ &= \sum_{i=0}^{m+n-1} I^i J^{m+n-1-i} && (\text{Problem 2.39}) \\ &\subseteq I^m + J^n \end{aligned}$$

for all positive integers m, n. (If $m = 0$ or $n = 0$, then nothing to prove.)

$\square$

Proof of (b).

(1) *Show that I_i and I_j are comaximal if $i \neq j$.* Note that

$$R = I_i + J_i \subseteq I_i + I_j \subseteq R$$

if $i \neq j$.

(2) *If I_i is comaximal to I_j and $I_{j'}$. Show that I_i is also comaximal to $I_j I_{j'}$.*

$$\begin{aligned} R &= (I_i + I_j)(I_i + I_{j'}) \\ &= I_i(I_i + I_j + I_{j'}) + I_j I_{j'} && (\text{Problem 2.39(a)}) \\ &\subseteq I_i + I_j I_{j'} \subseteq R. \end{aligned}$$

(3) By (2), it is easy to get that I_i and $\prod_{j \neq i} I_j$ are comaximal by induction on the number of I_j for $j \neq i$.

(4) *Show that $I_1 \cdots I_N = I_1 \cap \cdots \cap I_N$.* Induction on N.

$$\begin{aligned} I_1 \cap \cdots \cap I_N &= I_1 \cap (I_2 \cap \cdots \cap I_N) \\ &= I_1 \cap (I_2 \cdots I_N) && (\text{Induction hypothesis}) \\ &= I_1 \cdot (I_2 \cdots I_N) && ((3)) \\ &= I_1 \cdots I_N. \end{aligned}$$

(5) Note that I_i^n and I_j^n are comaximal if $i \neq j$ by (a). We can apply the same argument in (2)(3)(4) to show that

$$I_1^n \cdots I_N^n = I_1^n \cap \cdots \cap I_N^n.$$

(6) Therefore,

$$\begin{aligned} (I_1 \cap \cdots \cap I_N)^n &= (I_1 \cdots I_N)^n && ((4)) \\ &= I_1^n \cdots I_N^n && (\text{Problem 2.39(b)}) \\ &= I_1^n \cap \cdots \cap I_N^n && ((5)). \end{aligned}$$

□

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 $x_1, \ldots, x_m \in I$. 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

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

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

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

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

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

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

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

(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, $\operatorname{rad}(I)$ and $\operatorname{rad}(J)$ are finitely generated. By (1), there is a common integer N such that

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

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

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

(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.

$\square$

Problem 2.42.* (Isomorphism theorems for rings)

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

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

Proof of (a).

(1) Define a map $\alpha : R/I \to R/J$ by $\alpha(r + I) = r + J$.

(2) *Show that α is well-defined.* If $a + I = b + I$, then $a - b \in I \subseteq J$ or $a + J = b + J$. Hence, $\alpha(a + I) = a + J = b + J = \alpha(b + I)$.

(3) *Show that α is a surjective homomorphism.*

(a) *α is addition preserving.*

$$\begin{aligned} \alpha((a + I) + (b + I)) &= \alpha(a + b + I) \\ &= a + b + J \\ &= (a + J) + (b + J) \\ &= \alpha(a + I) + \alpha(b + I). \end{aligned}$$

(b) *α is multiplication preserving.*

$$\begin{aligned} \alpha((a + I)(b + I)) &= \alpha(ab + I) \\ &= ab + J \\ &= (a + J)(b + J) \\ &= \alpha(a + I)\alpha(b + I). \end{aligned}$$

(c) *α is multiplicative identity preserving.* $\alpha(1 + I) = 1 + J$.

(d) α is surjective since for any $a + J \in R/J$ there is an element $a + I \in R/I$ such that $\alpha(a + I) = a + J$.

(4) Note that $\ker(\alpha) = J/I$. So $(R/I)/(J/I) \cong R/J$.

$\square$

Proof of (b).

(1) I is not necessary an ideal of S; IS an ideal of S (and thus S/IS is well-defined).

(2) Define a map $\alpha : R/I \to S/IS$ by $\alpha(r + I) = r + IS$. Note that $I \subseteq IS$ as a subset in S. Apply the same argument in (a), α is well-defined and α is a surjective homomorphism.

(3) Note that $\ker(\alpha) = (R \cap SI)/I$. So $(R/I)/((R \cap SI)/I) \cong S/IS$.

$\square$

Problem 2.45.*

Show that ideals $I, J \subseteq k[x_1, \ldots, x_n]$ (k algebraically closed) are comaximal if and only if $V(I) \cap V(J) = \varnothing$.

Proof.

(1) *Show that $V(I) \cap V(J) = V(I+J)$.*

$$\begin{aligned} P \in V(I) \cap V(J) &\Longleftrightarrow f(P) = 0 \, \forall f \in I \text{ and } g(P) = 0 \, \forall g \in J \\ &\Longleftrightarrow f(P) = 0 \, \forall f \in I + J \\ &\Longleftrightarrow P \in V(I+J). \end{aligned}$$

(2) Hence,

$$\begin{aligned} \varnothing = V(I) \cap V(J) &\Longleftrightarrow \varnothing = V(I+J) && ((1)) \\ &\Longleftrightarrow I + J = k[x_1, \ldots, x_n] && \text{(Weak Nullstellensatz)} \\ &\Longleftrightarrow I \text{ and } J \text{ are comaximal.} \end{aligned}$$

□

Problem 2.46.*

Let $I = (x, y) \subseteq k[x, y]$. Show that

$$\dim_k(k[x,y]/I^n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof.

(1) The set

$$\mathscr{B} = \{x^i y^j + I^n : i, j \in \mathbb{Z}, i, j \geq 0, i + j < n\}$$

generates $k[x,y]/I^n$ as a k-vector space. Besides, each nonzero element in I^n has the degree $\geq n$, and thus $\mathscr{B}$ is an independent set. Therefore, $\mathscr{B}$ is a basis for $k[x,y]/I^n$.

(2) Hence,

$$\dim_k(k[x,y]/I^n) = |\mathscr{B}| = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

□

2.9. Ideals with a Finite Number of Zeros

Problem 2.47.

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

Proof.

(1) Let $\{v_1, \ldots, v_n\}$ be a basis for R over k (as a vector space). Define a k-module homomorphism $\alpha : k[x_1, \ldots, x_n] \to R$ by $\alpha(x_i) = v_i$. Clearly, α is surjective and thus

$$R \cong k[x_1, \ldots, x_n]/\ker(\alpha)$$

as a k-module isomorphism. Note that $\ker(\alpha)$ is an ideal of $k[x_1, \ldots, x_n]$.

(2) Write $I := \ker(\alpha)$. Hence,

$$\dim_k(k[x_1, \ldots, x_n]/I) = \dim_k(R) < \infty.$$

By Corollary 4 to the Hilbert's Nullstellensatz in §1.7, $V(I)$ is finite.

(3) Write $V(I) = \{P_1, \ldots, P_N\}$ and $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbf{A}^n)$. By Proposition 6,

$$R \cong k[x_1, \ldots, x_n]/I \cong \prod_{i=1}^{N} \mathcal{O}_i/I\mathcal{O}_i,$$

which is isomorphic to a direct product of local rings.

□

2.10. Quotient Modules and Exact Sequences

Problem 2.48.*

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

$$0 \to \ker(\varphi) \to M \xrightarrow{\varphi} \operatorname{im}(\varphi) \to 0$$

is exact.

Proof.

(1) *Show that* $\ker(\varphi)$ *is a subgroup of* M. It suffices to show that $a-b \in \ker(\varphi)$ for all $a, b \in \ker(\varphi)$. In fact, $\varphi(a-b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$, or $a - b \in \ker(\varphi)$.

(2) *Show that* $\ker(\varphi)$ *is a submodule of* M. By (1), it suffices to show that $ra \in \ker(\varphi)$ for all $r \in R$ and $a \in \ker(\varphi)$. In fact, $\varphi(ra) = r \cdot \varphi(a) = r \cdot 0 = 0$, or $ra \in \ker(\varphi)$.

(3) *Show that* $\operatorname{im}(\varphi)$ *is a subgroup of* M'. It suffices to show that $a-b \in \operatorname{im}(\varphi)$ for all $a, b \in \operatorname{im}(\varphi)$. As $a, b \in \operatorname{im}(\varphi)$, there are two elements $a', b' \in M$ such that $\varphi(a') = a$ and $\varphi(b') = b$. So $\varphi(a' - b') = \varphi(a') - \varphi(b') = a - b$, or $a - b \in \operatorname{im}(\varphi)$.

(4) *Show that* $\operatorname{im}(\varphi)$ *is a submodule of* M. By (3), it suffices to show that $ra \in \operatorname{im}(\varphi)$ for all $r \in R$ and $a \in \operatorname{im}(\varphi)$. As $a \in \operatorname{im}(\varphi)$, there is one element $a' \in M$ such that $\varphi(a') = a$. So $\varphi(ra') = r\varphi(a') = ra$, or $ra \in \operatorname{im}(\varphi)$.

(5) *Show that*

$$0 \to \ker(\varphi) \xrightarrow{i} M \xrightarrow{\varphi} \operatorname{im}(\varphi) \to 0$$

is exact. Note that $\ker(\varphi) \xrightarrow{i} M$ is the natural inclusion and $M \xrightarrow{\varphi} \operatorname{im}(\varphi)$ is surjective. Also, it is trivial that $\operatorname{im}(i) = \ker(\varphi)$.

$\square$

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 §2.10).

(1) For $i = 0, \ldots, n$, 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 $i = 0, \ldots, n-1$. 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

3.2. Multiplicities and Local Rings

3.3. Intersection Numbers

Chapter 4: Projective Varieties

4.1. Projective Space

4.2. Projective Algebraic Sets

4.3. Affine and Projective Varieties

4.4. Multiprojective Space

Chapter 5: Projective Plane Curves

5.1. Definitions

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

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

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