Solutions to the book: *Fulton, Algebraic Curves*

Meng-Gen Tsai
plover@gmail.com

July 15, 2021

Contents

Chapter 1: Affine Algebraic Sets

1.1. Algebraic Preliminaries

Problem 1.1.*

Let R be a domain.

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

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

Proof of (a).

(1) Write

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

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

(2) Hence,

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

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

□

Proof of (b).

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

(2) Write

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

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

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

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.

□

Problem 1.2.*

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

Proof.

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

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

where all $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible in R. (It is possible since R is a UFD.) For each i, suppose $p_i \mid q_j$ for some i, j. Write $q_j = p_iu$ 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

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

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

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

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

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

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

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

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

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

□

Problem 1.3.*

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

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

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

Proof of (a).

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

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

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

□

Proof of (b).

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

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

□

Problem 1.4.*

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

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

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

Proof.

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

(2) Assume that the conclusion holds for $n-1$, then for any $f \in k[x_1, \ldots, x_n]$ we can write

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

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

□

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

Problem 1.5.*

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

Proof (Due to Euclid).

(1) If $f_1, \ldots, f_n$ 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 $a_1, \ldots, a_n$ 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.

□

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
$$\begin{aligned} f(x, y) &= x \cdot \underbrace{(x + 2y)}_{g_1} + y \cdot \underbrace{y}_{g_2}, \text{ or} \\ &= x \cdot \underbrace{(x + y)}_{g_1} + y \cdot \underbrace{(x + y)}_{g_2}, \text{ or} \\ &= x \cdot \underbrace{x}_{g_1} + y \cdot \underbrace{(2x + y)}_{g_2}. \end{aligned}$$

□

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.

□

Problem 1.13.

Show that each of the following sets is not algebraic:

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

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

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

Proof of (a).

(1) (Reductio ad absurdum) If

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

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

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

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

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

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

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

□

Proof of (b).

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

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

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

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

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

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

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

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

□

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

Proof.

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

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

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

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

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

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

is infinite.

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

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

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

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

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

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

is infinite.

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

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

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

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

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

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

(3) Note that

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

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

□

Problem 1.15.*

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

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

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

Proof.

(1) Write

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

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

□

Proof of (b).

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

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

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

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

□

Proof of (c).

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

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

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

(3) Also,

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

□

Problem 1.18.*

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

Proof.

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

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

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

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

(a) $0 \in \mathrm{rad}(I)$ since $0 = 0^1 \in I$ for any ideal in R.

(b) $(a+b)^{n+m} \in I$ if $a^n \in I$, $b^m \in I$ by (1).

(c) $(-a)^{2n} = (a^n)^2 \in I$ if $a^n \in I$ (since I is an ideal).

(d) $(ra)^n = r^n a^n \in I$ if $a^n \in I$ and $r \in R$ (since I is an ideal and R is commutative).

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

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

□

Problem 1.19.

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

Proof.

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

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

□

Problem 1.20.*

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

Proof.

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

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

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

(2) By 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.

□

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 $\mathfrak{m}' = \mathfrak{m}$.

□

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 $x, y \in \mathbb{R}$. □

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,

$$\begin{aligned} V &= V_1 \cup \cdots \cup V_m \\ &= V(f_1) \cup \cdots \cup V(f_m) \\ &= V(f_1 \cdots f_m) \\ &= V(f). \end{aligned}$$

□

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 $\mathbf{A}^2(\mathbb{C})$.

□

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 $\mathbf{A}^2(\mathbb{C})$.

□

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,

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

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 $\iff$ $x^2 - a$ has one root $\alpha \in R$ $\iff$ $a = \alpha^2$ 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

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

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 $g \in k[x_1, \ldots, x_n]$ 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,

$$(g) = I(V(f)) \supsetneq I(W) \supsetneq (1) \in k[x_1, \ldots, x_n].$$

Here $(g) = I(V(f))$ and $I(W)$ are all prime.

(3) Note that (g) is a principal proper prime ideal in a UFD $k[x_1, \ldots, x_n]$. 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

$$r_0 = (y^2 - z^3)q_0 + yc + a$$
$$r_1 = (y^2 - z^3)q_1 + yd + b$$

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 $\overline{r_1} = \overline{yd} + \overline{b}$,

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

□

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

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 $s_1, \ldots, s_n \in S$ since S is module-finite over R.

(2) *Show that* $\sum Rs_i = R[s_1, \ldots, s_n]$. $\sum Rs_i \subseteq R[s_1, \ldots, s_n]$ is trivial. Conversely, take any $v \in R[s_1, \ldots, s_n]$. 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 $s_1, \ldots, s_n \in S$ 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 $S = R[v_1, \ldots, v_n]$, $T = S[w_1, \ldots, w_m]$, show that $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.*

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

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

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 $\sum r_{ij}v_iw_j \in \sum Rv_iw_j$.

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

□

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,

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

□

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

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

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.

□

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 $\alpha \in k$.

□

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), $L = k$.

□

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

□

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 $K(y)$:

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

□

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

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 $f_1 \in L[x]$.

□

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

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

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,

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

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 $f \in k[x_1, \ldots, x_n]$ a polynomial function in $\mathscr{F}(V, k)$ is a ring homomorphism whose kernel is $I(V)$.

Proof.

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

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

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

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

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

(4) Hence,

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

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 $k[x_1, \ldots, x_n]/I$ 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 α : {polynomial functions in $\mathscr{F}(V,k)$} $\to$ {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.

□

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.

□

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.*

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

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 $\varphi(t) = (t^3, t^4, t^5) \in Y = V$.

□

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 $t_1, \ldots, t_m \in k[x_1, \ldots, x_n]$ such that

$$\varphi(P) = (t_1(P), \ldots, t_m(P)) \in W$$

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 $t_1, \ldots, t_m$ such that

$$\varphi(P) = (t_1(P), \ldots, t_m(P)) \in W' \subseteq W$$

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* $\mathrm{pr}(a_1, \ldots, a_n) = (a_1, \ldots, a_r)$ *is a polynomial map.*

Proof.

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

(2) Clearly,

$$\mathrm{pr}(P) = (t_1(P), \ldots, t_r(P))$$

for $P = (a_1, \ldots, a_n) \in \mathbf{A}^n$, and thus pr is a polynomial map.

□

Problem 2.11.

Let $f \in \Gamma(V)$, V *a variety* $\subseteq \mathbf{A}^n$. *Define*

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

the ***graph*** *of* f. *Show that* $G(f)$ *is an affine variety, and that the map* $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n, f(a_1, \ldots, a_n))$ *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.

□

Problem 2.12.

(a) *Let $\varphi : \mathbf{A}^1 \to V = V(y^2 - x^3) \subseteq \mathbf{A}^2$ be defined by $\varphi(t) = (t^2, t^3)$. Show that although φ is a one-to-one, onto polynomial map, φ is not an isomorphism. (Hint: $\widetilde{\varphi}(\Gamma(V)) = k[t^2, t^3] \subsetneq k[t] = \Gamma(\mathbf{A}^1)$.)*

(b) *Let $\varphi : \mathbf{A}^1 \to V = V(y^2 - x^2(x+1))$ be defined by $\varphi(t) = (t^2 - 1, t(t^2 - 1))$. Show that φ is one-to-one and onto, except that $\varphi(\pm 1) = (0, 0)$.*

Proof of (a).

(1) Similar to Problem 2.8(a), φ is a polynomial map.

(2) Similar to Problem 2.8(a) again,

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

Hence the map $\varphi : t \mapsto (t^2, t^3)$ is surjective.

(3) *Show that φ is injective.* Suppose $(t^2, t^3) = (s^2, s^3)$ for some $t, s \in k$. If $t = 0$, then $s = 0$. If $t \neq 0$, then $t = \frac{t^3}{t^2} = \frac{s^3}{s^2} = s$. In any case, $t = s$ whenever $(t^2, t^3) = (s^2, s^3)$.

(4) *Show that φ is not an isomorphism.* It suffices to show that $\widetilde{\varphi}(\Gamma(V)) \subsetneq \Gamma(\mathbf{A}^1)$ by Proposition 1. For any $f \in \Gamma(V)$,

$$\widetilde{\varphi}(f)(t) = (f \circ \varphi)(t) = f(t^2, t^3) \in k[t^2, t^3].$$

Hence,

$$\widetilde{\varphi}(\Gamma(V)) \subseteq k[t^2, t^3] \subsetneq k[t] = \Gamma(\mathbf{A}^1).$$

(Here note that $t \notin k[t^2, t^3]$ but $t \in k[t]$.)

□

Proof of (b).

(1) *Write*

$$Y = \{(t^2 - 1, t(t^2 - 1)) \in \mathbf{A}^2(k) : t \in k\}.$$

Show that $Y = V$. Similar to Problem 2.8(a). It suffices to show that $(x, y) \in Y$ for any $(x, y) \in V$. If $x = 0$, then $y = 0$ or $(x, y) = (0, 0) \in Y$

whenever $t = \pm 1$. (In fact, $(0,0) = (t^2-1, t(t^2-1))$ iff $t^2 - 1 = 0$ iff $t = \pm 1$ in any field.) If $x \neq 0$, define

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

So $y = tx$ and thus

$$0 = y^2 - x^2(x+1) = t^2x^2 - x^2(x+1) = x^2(t^2 - (x+1)).$$

Since $x \neq 0$ and k is a field, we have

$$t^2 - (x+1) = 0 \Longleftrightarrow x = t^2 - 1.$$

Hence, $y = tx = t(t^2-1)$ and therefore $(x,y) \in Y$.

(2) By (1), φ is surjective and $\varphi(\pm 1) = (0,0)$.

(3) *Show that φ is injective except that $\varphi(\pm 1) = (0,0)$.* Given $t, s \in k$. It suffices to show that $t = s$ whenever $(t^2-1, t(t^2-1)) = (s^2-1, s(s^2-1)) \neq (0,0)$. In fact, by assumption we have $t^2 - 1 = s^2 - 1 \neq 0$ by assumption. Therefore,

$$t = \frac{t(t^2-1)}{t^2-1} = \frac{s(s^2-1)}{s^2-1} = s.$$

□

Problem 2.13.

Let $V = V(x^2 - y^3, y^2 - z^3) \subseteq \mathbf{A}^3$ as in Problem 1.40, $\overline{\alpha} : \Gamma(V) \to k[t]$ induced by the homomorphism α of that problem.

(a) *What is the polynomial map f from $\mathbf{A}^1$ to V such that $\widetilde{f} = \overline{\alpha}$?*

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

Proof of (a).

(1) *Write*

$$Y = \{(t^9, t^6, t^4) \in \mathbf{A}^3(k) : t \in k\}.$$

Show that $Y = V$. Similar to Problem 2.8(a). It suffices to show that $(x,y,z) \in Y$ for any $(x,y,z) \in V$. If $x = 0$, then $y = z = 0$ or $(x,y,z) = (0,0,0) \in Y$ by taking $t = 0$. If $x \neq 0$, define

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

Hence,

$$t^9 = \frac{y^9 z^9}{x^9} = \frac{y^{15}}{x^9} = \frac{x^{10}}{x^9} = x,$$
$$t^6 = \frac{y^6 z^6}{x^6} = \frac{y^5 z^6}{x^6} y = \frac{y^9}{x^6} y = \frac{x^6}{x^6} y = y,$$
$$t^4 = \frac{y^4 z^4}{x^4} = \frac{y^4 z^3}{x^4} z = \frac{y^6}{x^4} z = \frac{x^4}{x^4} z = z.$$

(2) Define a mapping $f : \mathbf{A}^1 \to \mathbf{A}^3$ by

$$f : t \mapsto (t^9, t^6, t^4).$$

f is a polynomial map by construction. By (1), $f : \mathbf{A}^1 \to f(\mathbf{A}^1) = V$ and thus $\widetilde{f} = \overline{\alpha}$ by the definition of α.

□

Proof of (b).

(1) Similar to Problem 2.12(a).

(2) f is surjective by the proof of (a).

(3) *Show that f is injective.* Suppose $(t^9, t^6, t^4) = (s^9, s^6, s^4)$ for some $t, s \in k$. If $t = 0$, then $s = 0$. If $t \neq 0$, then $t = \frac{t^6 t^4}{t^9} = \frac{s^6 s^4}{s^9} = s$. In any case, $t = s$ whenever $(t^9, t^6, t^4) = (s^9, s^6, s^4)$.

(4) *Show that f is not an isomorphism.* It suffices to show that $\widetilde{f}(\Gamma(V)) \subsetneq \Gamma(\mathbf{A}^1)$ by Proposition 1. For any $g \in \Gamma(V)$,

$$\widetilde{f}(g)(t) = (g \circ f)(t) = g(t^9, t^6, t^4) \in k[t^4, t^6, t^9].$$

Hence,

$$\widetilde{\varphi}(\Gamma(V)) \subseteq k[t^4, t^6, t^9] \subsetneq k[t] = \Gamma(\mathbf{A}^1).$$

(Here note that $t \notin k[t^4, t^6, t^9]$ but $t \in k[t]$.)

□

2.3. Coordinate Changes

Problem 2.14.* (Linear subvariety)

*A set $V \subseteq \mathbf{A}^n(k)$ is called a **linear subvariety** of $\mathbf{A}^n(k)$ if $V = V(f_1, \ldots, f_r)$ for some polynomials f_i of degree 1.*

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

(b) *If $V \neq \varnothing$, show that there is an affine change of coordinates t of $\mathbf{A}^n$ such that $V^t = V(x_{m+1}, \ldots, x_n)$. (Hint: use induction on r.) So V is a variety.*

(c) *Show that the m that appears in part (b) is independent of the choice of t. It is called the* ***dimension*** *of V. Then V is then isomorphic (as a variety) to $\mathbf{A}^m(k)$. (Hint: Suppose there were an affine change of coordinates t such that $V(x_{m+1}, \ldots, x_n)^t = V(x_{s+1}, \ldots, x_n)$, $m < s$; show that $t_{m+1}, \ldots, t_n$ would be dependent.)*

Proof of (a).

(1) Say $t = (t_1, \ldots, t_n)$ is an affine change of coordinates, and $V = V(f_1, \ldots, f_r)$ for some polynomials f_i of degree 1.

(2) *Show that V is a variety and thus $I(V) = (f_1, \ldots, f_r)$ by the Hilbert's Nullstellensatz.* $V(f_1, \ldots, f_r)$ is the set of all solutions of the system of linear equations:

$$\begin{aligned} f_1 &= a_{11}x_1 + \cdots + a_{1n}x_n - b_1 = 0, \\ &\cdots \\ f_r &= a_{r1}x_1 + \cdots + a_{rn}x_n - b_r = 0. \end{aligned}$$

Write $Ax = b$ and $V = V(Ax = b)$ where

$$A = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rn} \end{pmatrix}}_{\in \mathsf{M}_{r\times n}(k)}, \qquad x = \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{\in \mathsf{M}_{n\times 1}(k)}, \qquad b = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}}_{\in \mathsf{M}_{r\times 1}(k)}.$$

(3) The Gaussian elimination in linear algebra says that $(A|b)$ has the same solutions as its reduced row echelon form $(A'|b')$, that is, $V(Ax = b) = V(A'x = b')$.

(4) If $V(f_1, \ldots, f_r) = \varnothing$, nothing to do. If $V(f_1, \ldots, f_r) \neq \varnothing$, then

$$V(f_1, \ldots, f_r) = V(g_1, \ldots, g_m)$$

where $m = \operatorname{rank}(A)$ is the number of nonzero rows in A' ($m \leq r, n$) and $g_i = a'_{i1}x_1 + \cdots + a'_{in}x_n - b'_i$ for $1 \leq i \leq m$. (a'_{ij} is the entry of the matrix A'.)

(5) Now given any $f+I(V) \in k[x_1,\ldots,x_n]/I(V)$, we replace the leading term x_{i_1} of g_1 by $x_{i_1}-g_1$ to get

$$f+I(V) = f(x_1,\cdots,\underbrace{x_{i_1}-g_1}_{i_1\text{th position}},\cdots,x_n)+I(V) := f_1+I(V)$$

where $f_1 \in k[x_1,\ldots,\widehat{x_{i_1}}\ldots,x_n]$. Continue this process to replace each leading term x_{i_j} of g_j by $x_{i_j}-g_j$ to get one by one to get

$$f+I(V) = f_1+I(V) \text{ where } f_1 \in k[x_1,\ldots,\widehat{x_{i_1}}\ldots,x_n].$$
$$\cdots$$
$$f_{m-1}+I(V) = f_m+I(V) \text{ where } f_m \in k[x_1,\ldots,\widehat{x_{i_1}},\ldots,\widehat{x_{i_m}}\ldots,x_n].$$

Hence, a routine shows that there is a ring isomorphism

$$\alpha : k[x_1,\ldots,x_n]/I(V) \to \underbrace{k[x_1,\ldots,\widehat{x_{i_1}},\ldots,\widehat{x_{i_m}}\ldots,x_n]}_{\text{a domain}}$$

sending f to f_m. Therefore, V is a variety.

(6) As $I(V)=(f_1,\ldots,f_r)$, $I(V)^t=(f_1^t,\ldots,f_r^t)$ where each f_i^t is linear. Thus $V^t=V(I(V)^t)=V(f_1^t,\ldots,f_r^t)$ is also a linear subvariety of $\mathbf{A}^n(k)$.

□

Proof of (b).

(1) Suppose $A \in \mathsf{M}_{r\times n}(k)$ is of rank $n-m$. Linear algebra says that there exist invertible matrices $B \in \mathsf{M}_{r\times r}(k)$ and $C \in \mathsf{M}_{n\times n}(k)$ such that $D=BAC$, where

$$D = BAC = \underbrace{\begin{pmatrix} O_1 & O_2 \\ O_3 & I_{n-m} \end{pmatrix}}_{\in \mathsf{M}_{r\times n}(k)}$$

in which $I_{n-m} \in \mathsf{M}_{(n-m)\times(n-m)}(k)$ is the identity matrix and O_1, O_2, and O_3 are zero matrices.

(2) Let t' be the linear map corresponding to the matrix C. So

$$\begin{aligned} V^{t'} &= V(Ax=b)^{t'} \\ &= V(ACx=b) \\ &= V(BACx=Bb) && (B\text{: invertible}) \\ &= V(Dx=Bb) \\ &= V(-\beta_1,\cdots,-\beta_m,x_{m+1}-\beta_{m+1},\cdots,x_n-\beta_n) && (V\neq\varnothing) \\ &= V(x_{m+1}-\beta_{m+1},\cdots,x_n-\beta_n) \end{aligned}$$

where $Bb = \underbrace{\begin{pmatrix}\beta_1\\ \vdots \\ \beta_n\end{pmatrix}}_{\in \mathsf{M}_{n\times 1}(k)}$.

(3) Let t'' be the translation corresponding to the matrix Bb. Let $t = t'' \circ t'$ be the desired affine change of coordinates. Therefore,

$$\begin{aligned} V^t &= (V^{t'})^{t''} \\ &= V(x_{m+1} - \beta_{m+1}, \cdots, x_n - \beta_n)^{t''} \\ &= V(x_{m+1}, \cdots, x_n). \end{aligned}$$

□

Proof of (c).

(1) Linear algebra says that the rank of any matrix is uniquely determined. Therefore, $\dim(V) = n - \text{rank}(A|b) = n - \text{rank}(A'|b')$ is uniquely determined.

(2) V is then isomorphic to $\mathbf{A}^m(k)$ as a variety.

□

Problem 2.15.* (Line)

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

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

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

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

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

Proof of (a).

(1) Write $t = (t_1, \ldots, t_n)$ as

$$t_i = \sum_j c_{ij} x_j + c_{i0}.$$

Take any point $P_s = (a_1 + s(b_1 - a_1), \ldots, a_n + s(b_n - a_n)) \in L$ for some $s \in k$. (In particular, $P_0 = P$ and $P_1 = Q$.)

(2) As

$$\begin{aligned} t_i(P_s) &= \sum_j c_{ij}(a_j + s(b_j - a_j)) + c_{i0} \\ &= \left(\sum_j c_{ij}a_j + c_{i0}\right) \\ &\quad + s\left[\left(\sum_j c_{ij}b_j + c_{i0}\right) - \left(\sum_j c_{ij}a_j + c_{i0}\right)\right] \\ &= t_i(P) + s(t_i(Q) - t_i(P)), \end{aligned}$$

we have

$$\begin{aligned} t(L) = \{&(t_1(P) + s(t_1(Q) - t_1(P)), \ldots, t_n(P) + s(t_n(Q) - t_n(P))) \\ &: s \in k\}. \end{aligned}$$

Moreover, $t(P) \in t(L)$ as $s = 0$ and $t(Q) \in t(L)$ as $s = 1$. Therefore, $t(L)$ is the line through $t(P)$ and $t(Q)$.

□

Proof of (b).

(1) Note that $a_\alpha \neq b_\alpha$ for some $1 \leq \alpha \leq n$ since $P \neq Q$. Write

$$L = V\left(x_i = a_i + \frac{x_\alpha - a_\alpha}{b_\alpha - a_\alpha}(b_i - a_i) : 1 \leq i \leq n\right).$$

(Here we solve $s = \frac{x_\alpha - a_\alpha}{b_\alpha - a_\alpha}$ and then replace s in the equation $x_i = a_i + t(b_i - b_i)$.) By Problem 2.14, L is a linear subvariety.

(2) Note that

$$\begin{aligned} n - \dim(L) &= \text{the rank of the corresponding augmented matrix } (A'|b') \\ &= \text{the maximal number of the linearly independent rows of } (A'|b') \\ &= n - 1, \end{aligned}$$

which is uniquely determined. Therefore, $\dim(V) = 1$.

(3) Conversely, $\dim(V) = 1$ implies that $\operatorname{rank}(A'|b') = n - 1$. So all leading terms are all x_i except only one x_j for some j. Hence V is of the form

$$V = (x_i + a_{ij}x_j = b_i)$$

for $1 \leq i \leq n$ and $i \neq j$. So

$$\begin{aligned} V &= \{(b_1 - a_{1j}s, \ldots, \underbrace{s}_{j\text{th position}}, \ldots, b_n - a_{nj}s) : s \in k\} \\ &= \{(b_1 + s((b_1 - a_{1j}) - b_1), \ldots, \underbrace{0 + s(1-0)}_{j\text{th position}}, \ldots, \\ &\qquad (b_n + s((b_n - a_{nj}) - b_n) : s \in k\} \end{aligned}$$

is a line passing

$$\begin{aligned} P &= (b_1, \ldots, 0, \ldots, b_n) \\ Q &= (b_1 - a_{1j}, \ldots, 1, \ldots, b_n - a_{nj}) \end{aligned}$$

with $P \neq Q$ (since they are different in the jth position). (Here we can change P and Q to any two different points on V.)

□

Proof of (c).

(1) A line $L \subseteq \mathbf{A}^2$ is $V(x + ay = b)$ or $V(x + ay = b)$ by (b). In any case, L is a hyperplane in $\mathbf{A}^2$.

(2) Conversely, given any hyperplane $V = V(ax + by + c = 0) \subseteq \mathbf{A}^2$ where a and b are not all zero. Might assume that $a \neq 0$. (The case $b \neq 0$ is similar.) So

$$V = \left\{ \left(-\frac{c}{a} - \frac{b}{a}s, s \right) : s \in k \right\}$$

is a line passing $\left(-\frac{c}{a}, 0\right)$ and $\left(-\frac{c+b}{a}, 1\right)$.

□

Proof of (d).

(1) It suffices to show that there is a bijective affine change of coordinates t of $\mathbf{A}^2$ such that $t(P) = (0,0)$, $t(L_1) = V(x = 0)$ and $t(L_2) = V(y = 0)$. Write $P = (p_1, p_2)$ and $L_i = a_i x + b_i y + c_i$ for $i = 1, 2$.

(2) Let $t'' = (t''_1, t''_2)$ be a translation defined by

$$\begin{pmatrix} t''_1 \\ t''_2 \end{pmatrix} = \begin{pmatrix} x - p_1 \\ y - p_2 \end{pmatrix}.$$

So ${L_1}^{t''} = a_1 x + b_1 y$ and ${L_2}^{t''} = a_2 x + b_2 y$. Let

$$A = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

and $t' = (t'_1, t'_2)$ be a linear map defined by

$$\begin{pmatrix} t'_1 \\ t'_2 \end{pmatrix} = \frac{1}{\det(A)} \begin{pmatrix} b_2 & -b_1 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

(t' is well-defined since L_1 and L_2 are distinct lines and thus $\det(A) \neq 0$.) Write $t = (t_1, t_2) = t' \circ t''$. So

$$\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = \frac{1}{\det(A)} \begin{pmatrix} b_2 & -b_1 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} x - p_1 \\ y - p_2 \end{pmatrix}$$

and

$$L_1^t = ({L_1}^{t''})^{t'} = x$$
$$L_2^t = ({L_2}^{t''})^{t'} = y.$$

(3) Conversely, define an affine change of coordinates $s = (s_1, s_2)$ of $\mathbf{A}^2$ by

$$\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} a_1 x + b_1 y + c_1 \\ a_2 x + b_2 y + c_2 \end{pmatrix}$$

so that $x^s = L_1$ and $y^s = L_2$.

(4) By (2)(3), the statement in (1) is established.

□

Problem 2.16.

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

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

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

Proof of (a).

(1) Regard $\mathbb{C}^n$ as $\mathbb{R}^{2n}$. Given any $P, Q \in \mathbb{C}^n - S$. Write $S := \{P_1, \ldots, P_m\} \subseteq \mathbb{C}^n$.

(2) Let L_{P_i} (resp. L'_{P_i}) be a line passing P (resp. Q) and P_i for every $P_i \in S$. (It is well-defined since P, Q are not in S.) So $\mathscr{C} := \{L_{P_i} : P_i \in S\}$ (resp. $\mathscr{C}' := \{L'_{P_i} : P_i \in S\}$) is a collection of finitely many lines.

(3) Consider a unit sphere $\mathbb{S}^{2n-1}(P)$ centered at P.

$$\left(\bigcup_{L_i \in \mathscr{C}} L_i\right) \bigcap \mathbb{S}^{2n-1}(P)$$

is again a finite set (of order $\leq 2|S| = 2m$). Since $\mathbb{S}^{2n-1}$ is infinite, we can always take a line L passing P and some point in $\mathbb{S}^{2n-1}(P)$ where $L \cap S = \varnothing$.

(4) Similarly, we take a line L' passing Q and some point in $\mathbb{S}^{2n-1}(Q)$ where $L' \cap S = \varnothing$ and $L' \cap L \neq \varnothing$. (There are only two points in $\mathbb{S}^{2n-1}(Q)$ such that $L' \cap L = \varnothing$. Note that $\mathbb{S}^{2n-1}$ is infinite.)

(5) Take any point $A \in L' \cap L$. So there is a path from P to A (on a segment containted in L) and then to Q (on a segment containted in L'). Therefore, $\mathbb{C}^n - S$ is path-connected.

□

Proof of (b).

(1) Given any $P, Q \in \mathbf{A}^n(\mathbb{C}) - V$. Let L be the line through P and Q. To show $\mathbf{A}^n(\mathbb{C}) - V$ is path-connected, it suffices to show that

$$L - V = L - (V \cap L)$$

is path-connected.

(2) Similar to Problem 1.12, we have $V \cap L$ is finite. In fact, write $V = (f_1, \ldots, f_r)$ and $L = \{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) : t \in k\}$ where $P = (a_1, \ldots, a_n)$ and $Q = (b_1, \ldots, b_n)$. Then

$$\begin{aligned} V \cap L &= \bigcap_i (V(f_i) \cap L) \\ &= \bigcap_i \{f_i(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) = 0 : t \in k\} \\ &= \bigcap_i \text{ finite set} \\ &= \text{finite set.} \end{aligned}$$

Here $f_i(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n))$ is a nonzero polynomial since $P, Q \notin V(f_i)$.

(3) Note that the path-connectedness is a topological invariant under homeomorphisms. Since any line is homeomorphic to $\mathbb{C}^1$, $L - V$ is homeomorphic to $\mathbb{C}^1 - S$ for some finite set S (by (2)). By (a), $L - V$ is path-connected and so is $\mathbf{A}^n(\mathbb{C}) - V$.

□

2.4. Rational Functions and Local Rings

Problem 2.17.

Let $V = V(y^2 - x^2(x+1)) \subseteq \mathbf{A}^2$, and $\overline{x}, \overline{y}$ the residues of x, y in $\Gamma(V)$; let $z = \overline{y}/\overline{x} \in k(V)$. Find the pole sets of z and of z^2.

Proof.

(1) *Show that the pole set of z is $\{(0,0)\}$.*

(a) Since V is irreducible by Problem 2.12(b), V is a variety. Note that the pole set of z is

$$\bigcap_{z=\overline{f}/\overline{g}} V(\overline{g}).$$

(b) By (a), $\{(0,0)\}$ contains the the pole set of z. (As the denominator $x = 0$, we solve the equation $y^2 - x^2(x+1) = 0$ to get $y = 0$.)

(c) (Reductio ad absurdum) If $(0,0)$ were not a pole, then there were $\overline{f}, \overline{g} \in \Gamma(V)$ such that $z = \overline{y}/\overline{x} = \overline{f}/\overline{g}$ where $\overline{g}(0,0) \neq 0$. So

$$\begin{aligned}
& z = \overline{y}/\overline{x} = \overline{f}/\overline{g} \\
\Longrightarrow\ & \overline{xf} = \overline{yg} \\
\Longrightarrow\ & xf - yg \in (y^2 - x^2(x+1)) \\
\Longrightarrow\ & xf - yg = h(y^2 - x^2(x+1)) \text{ for some } h \\
\Longrightarrow\ & y(g + hy) = x(f + hx(x+1)) \in (x) \\
\Longrightarrow\ & g + hy \in (x) \\
\Longrightarrow\ & g(0,0) = 0,
\end{aligned}$$

which is absurd.

(2) *Show that the pole set of z^2 is empty.* Note that $z^2 = \overline{y^2}/\overline{x^2} = \overline{x+1}$. So the pole set of z^2 is

$$\bigcap_{z^2=\overline{f}/\overline{g}} V(\overline{g}) = \varnothing.$$

□

Problem 2.18.

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

is prime in $\Gamma(V)$, and I is generated by $I \cap \Gamma(V)$; use Problem 2.2.)

Proof.

(1) Write $P = (a_1, \ldots, a_n)$ and $\mathfrak{m} := (x_1 - a_1, \ldots, x_n - a_n)$. It suffices to show that there is a natural one-to-one correspondence between the prime ideals in $\mathscr{O}_P(V)$ and prime ideals in $\Gamma(V)$ which is contained in $I(V(P)) = \mathfrak{m}$ by Problem 2.2.

(2) If $\mathfrak{p}$ is prime in $\mathscr{O}_P(V)$, $\mathfrak{p} \cap \Gamma(V)$ is prime in $\Gamma(V)$ since $\Gamma(V)$ is a subring of $\mathscr{O}_P(V)$. Note that $\mathfrak{p} \subseteq \mathfrak{m}_P(V)$ and thus

$$\mathfrak{p} \cap \Gamma(V) \subseteq \mathfrak{m}_P(V) \cap \Gamma(V) = (x_1 - a_1, \ldots, x_n - a_n).$$

(3) Conversely, if $\mathfrak{q}$ is prime in $\Gamma(V)$ which is contained in $\mathfrak{m}$ then we need to show that $\mathfrak{p} := \mathfrak{q}\mathscr{O}_P(V)$ is prime in $\mathscr{O}_P(V)$.

(4) Note that $\mathfrak{p}$ is proper (since $\mathfrak{q} \subseteq \mathfrak{m}$). Suppose $\frac{a}{b}\frac{c}{d} \in \mathfrak{p}$ with $b(P) \neq 0$ and $d(P) \neq 0$. Hence

$$ac = \frac{a}{b}\frac{c}{d} \cdot (bd) \in \mathfrak{p} \cap \Gamma(V) = \mathfrak{q}.$$

By the primality of $\mathfrak{q}$, might assume that $a \in \mathfrak{q}$. (The case $c \in \mathfrak{q}$ is the same.) So that $\frac{a}{b} = a \cdot \frac{1}{b} \in \mathfrak{q}\mathscr{O}_P(V) = \mathfrak{p}$. Therefore, $\mathfrak{p}$ is prime.

□

Problem 2.19.

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

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

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

Proof.

(1) Write $f = a/b \in k(V)$ with $b(P) \neq 0$. Define $f : U \to k$ by $f : P \mapsto f(P) = a(P)/b(P)$.

(2) *Show that this function is well-defined.* Given any $P \in U$. Suppose that $f = a/b = c/d$ with $b(P) \neq 0$ and $d(P) \neq 0$. So, $ad = bc \in \Gamma(V)$ implies that $a(P)d(P) = b(P)c(P)$. So, $a(P)/b(P) = c(P)/d(P)$ (since $b(P) \neq 0$ and $d(P) \neq 0$). Therefore, $f : U \to k$ is well-defined.

□

Problem 2.20. (Quadric surface)

Let

$$V = V(xw - yz) \subseteq \mathbf{A}^4(k),$$

and

$$\Gamma(V) = k[x, y, z, w]/(xw - yz).$$

Let $\overline{x}, \overline{y}, \overline{z}, \overline{w}$ *be the residues of* x, y, z, w *in* $\Gamma(V)$*. Then*

$$\overline{x}/\overline{y} = \overline{z}/\overline{w} = f \in k(V)$$

is defined at $P = (x, y, z, w) \in V$ *if* $y \neq 0$ *or* $w \neq 0$*. Show that it is impossible to write* $f = a/b$*, where* $a, b \in \Gamma(V)$*, and* $b(P) \neq 0$ *for every* P *where* f *is defined. Show that the pole set of* f *is exactly* $\{(x, y, z, w) : y = 0 \text{ and } w = 0\}$*.*

Proof.

(1) Note that the pole set of f is

$$\bigcap_{f=\overline{a}/\overline{b}} V(\overline{b}) \subseteq \{(x, y, z, w) \in \mathbf{A}^4(k) : y = w = 0\}.$$

(2) *Show that* f *is not defined at the origin* $O = (0, 0, 0, 0)$*.* (Reductio ad absurdum) Suppose $f = \overline{x}/\overline{y} = \overline{a}/\overline{b}$ with $\overline{b}(O) \neq 0$. So $\overline{bx} - \overline{ay} = 0$, or

$$bx - ay = g(xw - yz)$$

for some $g \in k[x, y, z, w]$. Take 1-forms on the both sides to get

$$b(O)x - a(O)y = 0 \in k[x, y, z, w],$$

or $a(O) = b(O) = 0$, which is absurd.

(3) *Show that it is impossible to write* $f = \overline{a}/\overline{b}$*, where* $\overline{a}, \overline{b} \in \Gamma(V)$*, and* $\overline{b}(P) \neq 0$ *for every* P *where* f *is defined.* (Reductio ad absurdum) Consider the polynomial

$$\beta(y, w) := b(0, y, 0, w) \in k[y, w].$$

β is not a constant polynomial since $V(\beta) = \{(0, 0)\}$ by (1)(2). By Problem 1.14, $V(\beta) = \{(0, 0)\}$ is infinite, which is absurd.

(4) *Show that the pole set of* f *is exactly* $\{(x, y, z, w) : y = 0 \text{ and } w = 0\}$*.* (Reductio ad absurdum) Given any $P = (x_0, 0, z_0, 0) \in \{(x, y, z, w) : y = 0 \text{ and } w = 0\}$. Suppose $f = \overline{x}/\overline{y} = \overline{a}/\overline{b}$ where $\overline{b}(P) \neq 0$. Similar to (2),

$$bx - ay = g(xw - yz)$$

for some $g \in k[x, y, z, w]$. So

$$b(P)x_0 = b(P)x_0 - a(P) \cdot 0 = g(P)(x_0 \cdot 0 - 0 \cdot z_0) = 0.$$

As $b(P) \neq 0$, $x_0 = 0$. Similarly, $z_0 = 0$ by noting that $bz - aw = h(xw - yz)$ for some $h \in k[x, y, z, w]$. Hence $P = (0, 0, 0, 0)$, contrary to (2).

□

Note. It is equal to the Segre embedding of $\mathbf{P}^1 \times \mathbf{P}^1$ in $\mathbf{P}^3$, for suitable choice of coordinates.

Problem 2.21.*

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

Proof.

(1) Define $\widetilde{\varphi} : \mathscr{O}_Q(W) \to \mathscr{O}_P(V)$ by

$$\widetilde{\varphi} : a/b \mapsto \widetilde{\varphi}(a)/\widetilde{\varphi}(b).$$

It is well-defined since $b(Q) \neq 0$ implies that

$$\widetilde{\varphi}(b)(P) = b(\varphi(P)) = b(Q) \neq 0.$$

(2) Note that $\widetilde{\varphi}$ may not extend to all of $k(W)$ since $\widetilde{\varphi} : k(W) \to k(V)$ might not be well-defined if $\widetilde{\varphi}(b) = 0$ for all $b \in \Gamma(W)$.

(3) *Show that $\widetilde{\varphi}(\mathfrak{m}_Q(W)) \subseteq \mathfrak{m}_P(V)$.* Take any $a/b \in \mathfrak{m}_Q(W)$ with $a(Q) = 0$ and $b(Q) \neq 0$. As

$$\widetilde{\varphi}(a)(P) = a(\varphi(P)) = a(Q) = 0,$$

we have $\widetilde{\varphi}(a/b) \in \mathfrak{m}_P(V)$.

□

Problem 2.22.*

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

Proof.

(1) Since $\widetilde{t} : \Gamma(\mathbf{A}^n) \to \Gamma(\mathbf{A}^n)$ is a ring isomorphism, it extends uniquely to a ring isomorphism (also written $\widetilde{t}$) from $\mathscr{O}_Q(\mathbf{A}^n)$ to $\mathscr{O}_P(\mathbf{A}^n)$ by Problem 2.21.

(2) Note that $\mathscr{O}_Q(V) \hookrightarrow \mathscr{O}_Q(\mathbf{A}^n)$, $\mathscr{O}_P(V^t) \hookrightarrow \mathscr{O}_P(\mathbf{A}^n)$, and $\widetilde{t}(\mathscr{O}_Q(V)) = \mathscr{O}_P(V^t)$, $\widetilde{t} : \mathscr{O}_Q(V) \to \mathscr{O}_P(V^t)$ is an isomorphism.

□

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.

□

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 $\mathscr{O}_a(V)$ is a DVR with uniformizing parameter $t = x - a$.*

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

Proof of (a).

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

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

□

Proof of (b).

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

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

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

$$\deg(ac) = \deg(a) + \deg(c) \leq \deg(b) + \deg(d) = \deg(bd).$$

(Here we define $\deg(0) = -\infty$ by convention.) By the subring test, $\mathscr{O}_\infty$ is a subring of $k(x)$.

(2) *Show that $\mathscr{O}_\infty$ is a DVR.* Clearly $\mathscr{O}_\infty$ is not a field since $1/x \in \mathscr{O}_\infty$ but $x = x/1 \notin \mathscr{O}_\infty$. Let $t = 1/x$ be an irreducible element of $\mathscr{O}_\infty$. ($\deg(x) = 1$ implies the irreducibility of t.) Now for any nonzero $f/g \in \mathscr{O}_\infty$, write

$$f/g = ((fx^n)/g)(1/x^n) = ((fx^n)/g)t^n$$

where $n := \deg(g) - \deg(f) \geq 0$. 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 $\mathscr{O}_\infty$. Besides, it is easy to show that n is unique by the similar argument in Problem 2.23. Hence, $\mathscr{O}_\infty$ is a DVR.

□

Note.

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

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

(3) The maximal ideal of $\mathscr{O}_\infty(V)$ 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

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

Here $\mathrm{ord}_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ is defined by $\mathrm{ord}_p(a) = n$ 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 $(\mathrm{ord}_p(a), \mathrm{ord}_p(c)) = (0, 1)$ 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 $n > 0$, $z^{-1} \in \mathfrak{m}$.

□

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, $S = R$.

□

Problem 2.27.

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

Proof (Problem 2.26).

(1) *Show that $\mathscr{O}_a(V)$ and $\mathscr{O}_\infty$ are the only DVR's with quotient field $k(x)$ that contain k.*

(a) Let $k \subseteq R \subsetneq k(x)$ be a DVR with quotient field $k(x)$, $\mathfrak{m}$ be the unique maximal ideal of R. $\mathfrak{m} \neq (0)$ and the set of units in R is $R - \mathfrak{m}$.

(b) There are two possible cases: $x \in R$ or $x \notin R$.

(c) Suppose $x \in R$. So R contains $k[x]$ as a subring. Consider the subset

$$S := \{x - a \in k[x] : a \in k\} \cap \mathfrak{m} \subseteq \mathfrak{m}.$$

Suppose there were two distinct elements $x - a, x - b \in S$. Then $1 \in \mathfrak{m}$, contrary to the maximality of $\mathfrak{m}$. Suppose $S = \varnothing$, then every $x - a$ is a unit in R. Since $k = \overline{k}$, $R = k(x)$ is a field, which is absurd. Hence, there is only one $x - a \in \mathfrak{m}$ for one unique $a \in k$ and other $x - b$ with $b \neq a$ is a unit in R. Thus, $R \supseteq \mathscr{O}_a(V)$ and $\mathfrak{m}$ contains $(x - a)\mathscr{O}_a(V)$, which is the maximal ideal of $\mathscr{O}_a(V)$. By Problem 2.26, $R = \mathscr{O}_a(V)$.

(d) If $x \notin R$, then $x - a \notin R$ whenever $a \in k \subseteq R$. Hence $(x - a)^{-1} \in \mathfrak{m}$ whenever $a \in k$ by Problem 2.26(a). Next, given any $f/g \in \mathscr{O}_\infty$, by $k = \overline{k}$ we have

$$f/g = \underbrace{u}_{\in k} \underbrace{\frac{x - \alpha_1}{x - \beta_1}}_{\in R} \cdots \underbrace{\frac{x - \alpha_n}{x - \beta_n}}_{\in R} \underbrace{\frac{1}{x - \beta_{n+1}}}_{\in \mathfrak{m}} \cdots \underbrace{\frac{1}{x - \beta_m}}_{\in \mathfrak{m}},$$

where $n := \deg(f)$, $m := \deg(g)$ and $n \leq m$. Here

$$\frac{x - \alpha_i}{x - \beta_i} = \underbrace{1}_{\in k} + \underbrace{\frac{\beta_i - \alpha_i}{x - \beta_i}}_{\in \mathfrak{m} \subseteq R} \in R.$$

Therefore, $R \supseteq \mathscr{O}_\infty$ and $\mathfrak{m}$ contains the maximal ideal $x^{-1}\mathscr{O}_\infty$ of $\mathscr{O}_\infty$. By Problem 2.26, $R = \mathscr{O}_\infty$.

(2) *Show that $\mathbb{Z}_p$ are the only DVR's with quotient field $\mathbb{Q}$.*

(a) Let $R \subsetneq \mathbb{Q}$ be a DVR with quotient field $\mathbb{Q}$, $\mathfrak{m}$ be the unique maximal ideal of R. $\mathfrak{m} \neq (0)$ and the set of units in R is $R - \mathfrak{m}$.

(b) Note that $R \subseteq \mathbb{Q}$ contains $\mathbb{Z}$ as a subring. Consider the subset

$$S := \{p \in \mathbb{Z} : p \text{ is a prime number}\} \cap \mathfrak{m} \subseteq \mathfrak{m}.$$

(c) Suppose there were two distinct prime integers $p, q \in S$. By the Bézout's identity, there exist integers a and b such that $pa + qb = 1$. $1 \in \mathfrak{m}$, contrary to the maximality of $\mathfrak{m}$.

(d) Suppose no prime integer were in S, then every prime integer is a unit in R. By the fundamental theorem of arithmetic, $R = \mathbb{Q}$ is a field, which is absurd.

(e) By (c)(d), $p \in \mathfrak{m}$ for one unique prime $p \in \mathbb{Z}$. Thus, $R \supseteq \mathbb{Z}_p$ by the definition of $\mathbb{Z}_p$ and $\mathfrak{m}$ contains $p\mathbb{Z}_p$, which is the maximal ideal of $\mathbb{Z}_p$. By Problem 2.26, $R = \mathbb{Z}_p$.

□

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

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

□

Problem 2.29.*

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

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

(b) *If $a_1, \ldots, a_n \in K$, and for some i,* $\mathrm{ord}(a_i) < \mathrm{ord}(a_j)$ *(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 $\mathrm{ord}(a) < \mathrm{ord}(b)$, $n < m$. Hence,

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

To show that $\mathrm{ord}(a+b) = \mathrm{ord}(a) = n$, 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 $\mathrm{ord}(a_1) < \mathrm{ord}(a_j)$ (all $j \neq 1$). In particular, $\mathrm{ord}(a_1) < \infty$.

(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. (Formal power series)

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

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

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.

□

Problem 2.32. (Power series expansion)

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

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

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

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

Proof of (a).

(1) Define the map $\alpha : R \to k[[x]]$ by

$$\alpha : z \mapsto \sum_{i=0}^{\infty} \lambda_i x^i$$

where λ_i are determined as in Problem 2.30(b).

(2) *Show that α is well-defined and one-to-one.* Write

$$\alpha(z) = \sum_{i=0}^{\infty} \lambda_i x^i = \sum_{i=0}^{\infty} \lambda_i' x^i.$$

If there were $\lambda_n \neq \lambda_n'$ for some n, then Problem 2.30(b) implies that two expressions of z

$$\begin{aligned} z &= \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1} \\ &= \lambda_0' + \lambda_1' t + \cdots + \lambda_n' t^n + z_n' t^{n+1} \end{aligned}$$

are the same. That is, $\lambda_n = \lambda_n'$, which is absurd. Hence, α is well-defined. Also, $0 = 0 + 0t + 0t^2 + \cdots + 0t^n + 0t^{n+1}$ implies that α is one-to-one.

(3) *Show that α is addition preserving.* Given $a, b \in R$. By Problem 2.30(b),

$$a + b = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + c_n t^{n+1}$$

and

$$\begin{aligned} a &= \mu_0 + \mu_1 t + \cdots + \mu_n t^n + a_n t^{n+1} \\ b &= \nu_0 + \nu_1 t + \cdots + \nu_n t^n + b_n t^{n+1} \end{aligned}$$

for any integer $n \geq 0$. So

$$a + b = \underbrace{(\mu_0 + \nu_0)}_{\in k} + \underbrace{(\mu_1 + \nu_1)}_{\in k} t + \cdots + \underbrace{(\mu_n + \nu_n)}_{\in k} t^n + \underbrace{(a_n + b_n)}_{\in R} t^{n+1}.$$

Since the expression of $a + b$ is unique (by Problem 2.30(b)),

$$\lambda_i = \mu_i + \nu_i$$

for all $i = 0, 1, \ldots, n$. Since n is arbitrary, $\lambda_i = \mu_i + \nu_i$ is true for all nonnegative integers. Hence, $\alpha(a + b) = \alpha(a) + \alpha(b)$.

(4) *Show that α is multiplication preserving.* Given $a, b \in R$. By Problem 2.30(b),

$$ab = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + c_n t^{n+1}$$

and

$$\begin{aligned} a &= \mu_0 + \mu_1 t + \cdots + \mu_n t^n + a_n t^{n+1} \\ b &= \nu_0 + \nu_1 t + \cdots + \nu_n t^n + b_n t^{n+1} \end{aligned}$$

for any integer $n \geq 0$. So

$$\begin{aligned} ab = &\underbrace{(\mu_0 \nu_0)}_{\in k} + \underbrace{(\mu_1 \nu_0 + \mu_0 \nu_1)}_{\in k} t + \cdots \\ &+ \underbrace{(\mu_n \nu_0 + \mu_{n-1} \nu_1 + \cdots + \mu_1 \nu_{n-1} + \mu_0 \nu_n)}_{\in k} t^n \\ &+ \underbrace{(\text{other terms})}_{\in R} t^{n+1}. \end{aligned}$$

Since the expression of $a + b$ is unique (by Problem 2.30(b)),

$$\lambda_i = \sum_{j+k=i} \mu_j \nu_k$$

for all $i = 0, 1, \ldots, n$. Since n is arbitrary, $\lambda_i = \sum_{j+k=i} \mu_j + \nu_k$ is true for all nonnegative integers. Hence, $\alpha(ab) = \alpha(a)\alpha(b)$.

(5) *Show that α is multiplicative identity preserving.* Note that

$$1 = \underbrace{1}_{\in k} + \underbrace{0}_{\in k} t + \cdots + \underbrace{0}_{\in k} t^n + \underbrace{0}_{\in k} t^{n+1}$$

for every nonnegative integer n. Hence $\alpha : 1 \mapsto 1 \in k[[x]]$.

(6) By (3)(4)(5), α is a ring homomorphism.

□

Proof of (b).

(1) Define the mapping β from K to $k((x))$ by

$$\beta : a/b \mapsto \alpha(a)/\alpha(b)$$

where $a, b \in R$ and $b \neq 0$.

(2) β is well-defined since:

(a) $\alpha(b) \neq 0$ if $b \neq 0$ by the injectivity of α.

(b) The value of $\beta(a/b)$ is independent of the choice of $a/b \in K$ since α is a ring homomorphism.

(3) Also, β is a ring homomorphism since α is a ring homomorphism.

(4) To show that the order function on $k((x))$ restricts to that on K, it suffices to show that

$$\mathrm{ord}_R(z) = \mathrm{ord}_{k[[x]]}(\alpha(z)).$$

In fact,

$$\begin{aligned} m := \mathrm{ord}_R(z) &\iff z = \lambda_m t^m + \cdots + \lambda_n t^n + z_n t^{n+1} \text{ with } \lambda_m \neq 0 \\ &\iff \alpha(z) = \lambda_m x^m + \cdots \text{ with } \lambda_m \neq 0 \\ &\iff \mathrm{ord}_{k[[x]]}(\alpha(z)) = m. \end{aligned}$$

□

Proof of (c).

(1) In calculus we have

$$(1-x)^{-1} = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$$

for $|x| < 1$. In the ring of formal power series $k[[x]]$, $1 - x$ is a unit (by (4) in the proof of Problem 2.31) and satisfies

$$(1-x)\left(\sum_{i=0}^{\infty} x^i\right) = 1 \in k[[x]].$$

Hence, the power expansion of $(1-x)^{-1}$ is

$$(1-x)^{-1} = \sum_{i=0}^{\infty} x^i \in k((x)).$$

(2) Note that $1+x^2$ is a unit in $k[[x]]$ and satisfies

$$(1+x^2)\left(\sum_{i=0}^{\infty}(-1)^i x^{2i}\right) = 1 \in k[[x]].$$

Hence, the power expansion of $(1-x)(1+x^2)^{-1}$ is

$$\begin{aligned}(1-x)\left(\sum_{i=0}^{\infty}(-1)^i x^{2i}\right) &= \left(\sum_{i=0}^{\infty}(-1)^i x^{2i}\right) - x\left(\sum_{i=0}^{\infty}(-1)^i x^{2i}\right) \\ &= \sum_{i=0}^{\infty}(-1)^i x^{2i} + \sum_{i=0}^{\infty}(-1)^{i+1} x^{2i+1} \\ &= \sum_{i=0}^{\infty}(-1)^i x^i \in k[[x]].\end{aligned}$$

□

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,

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

□

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

Proof.

(1) Suppose $f + g = rs \in k[x_1, \ldots, x_n]$. 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 $k[x_1, \ldots, x_n]$. Hence r is a common factor of f and g, or r is a constant in $k[x_1, \ldots, x_n]$. 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 $k[x_1,\ldots,x_n]\}$, 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 $\ell_1,\ell_2,\ldots$ and $m_1,m_2,\ldots$ 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^iy^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 $x^iy^jz^k$ 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 $R[x,y,z]$.

□

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, $\dim V(d,1)=1$; $\dim V(d,2)=d+1$; $\dim V(d,3)=\frac{(d+1)(d+2)}{2}$.

□

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

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

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 $(0, \ldots, a_i, \ldots, 0)$ 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) $(I_1 + I_2)J = I_1J + I_2J$.

(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 $I_1J + I_2J$ are ideals.

(2) *Show that* $(I_1 + I_2)J \subseteq I_1J + I_2J$. 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 $(x_1 + x_2)y \in I_1J + I_2J$ (by (1)). In fact,

$$(x_1 + x_2)y = x_1y + x_2y \in I_1J + I_2J.$$

(3) *Show that* $(I_1 + I_2)J \supseteq I_1J + I_2J$. Given any

$$x_1y_1 + x_2y_2 \in I_1J + I_2J$$

where $x_i \in I_i$ and $y_i \in J$. It suffices to show that $x_1y_1 + x_2y_2 \in (I_1 + I_2)J$ (by (1)). In fact,

$$x_1y_1 + x_2y_2 = (x_1 + \underbrace{0}_{\in I_2})y_1 + (\underbrace{0}_{\in I_1} + x_2)y_2 \in (I_1 + I_2)J$$

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 $1 \le k \le N$. 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 $x_i \in I_i^n$ $(1 \le i \le N)$. 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 $1 \le k \le n$. Hence

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

□

Problem 2.40.* (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 $I_1, \ldots, I_N$ 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.)

□

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

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

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

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

(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) ($\implies$) 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) ($\impliedby$) 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 $I, J \subseteq S = k[x_1, \ldots, x_n]$ 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.* Note that S is Noetherian and we can apply step (2). By the Nullstellensatz, $Z(I) = Z(J)$ iff $\mathrm{rad}(I) = \mathrm{rad}(J)$ iff $I^N \subseteq J$ and $J^N \subseteq I$ for some N.

□

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

□

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 $(R/I)/((R \cap SI)/I) \cong S/IS$.

□

Problem 2.43.*

Let $P = (0, \ldots, 0) \in \mathbf{A}^n$, $\mathscr{O} = \mathscr{O}_P(\mathbf{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbf{A}^n)$. Let $I = (x_1, \ldots, x_n) \subseteq k[x_1, \ldots, x_n]$ be the ideal generated by $x_1, \ldots, x_n$. Show that $I\mathscr{O} = \mathfrak{m}$, so $I^r\mathscr{O} = \mathfrak{m}^r$ for all r.

Proof.

(1) By the defintion

$$\mathfrak{m} = \{f \in \mathscr{O} : f(P) = 0\},$$

$I\mathscr{O} \subseteq \mathfrak{m}$. Conversely, by Problem 1.7(b) we have $I\mathscr{O} \supseteq \mathfrak{m}$.

(2) By Problem 2.39(b),

$$\mathfrak{m}^r = (I\mathscr{O})^r = I^r\mathscr{O}^r = I^r\mathscr{O}.$$

Here $\mathscr{O}^r = \mathscr{O}$ since $1 \in \mathscr{O}$.

□

Problem 2.44.*

Let V be a variety in $\mathbf{A}^n$, $I = I(V) \subseteq k[x_1, \ldots, x_n]$, $P \in V$, and let J be an ideal of $k[x_1, \ldots, x_n]$ that contains I. Let J' be the image of J in $\Gamma(V)$. Show that there is a natural homomorphism φ from $\mathscr{O}_P(\mathbf{A}^n)/J\mathscr{O}_P(\mathbf{A}^n)$ to $\mathscr{O}_P(V)/J'\mathscr{O}_P(V)$, and that φ is an isomorphism. In particular, $\mathscr{O}_P(\mathbf{A}^n)/I\mathscr{O}_P(\mathbf{A}^n)$ is isomorphic to $\mathscr{O}_P(V)$.

Proof.

(1) Define φ from $\mathscr{O}_P(\mathbf{A}^n)/J\mathscr{O}_P(\mathbf{A}^n)$ to $\mathscr{O}_P(V)/J'\mathscr{O}_P(V)$ by

$$\varphi : a/b + J\mathscr{O}_P(\mathbf{A}^n) \mapsto \overline{a}/\overline{b} + J'\mathscr{O}_P(V).$$

It is well-defined since $\varphi(J\mathscr{O}_P(\mathbf{A}^n)) = J'\mathscr{O}_P(V)$ and $b(P) \neq 0$ implies that $\overline{b}(P) \neq 0$.

(2) Note that V is a subvariety of $\mathbf{A}^n$. So $\varphi : \Gamma(\mathbf{A}^n) \to \Gamma(V)$ is a ring homomorphism by Problem 2.3 and then φ extends uniquely to a ring homomorphism by using the similar argument in Problem 2.21.

(3) φ is surjective since $\mathscr{O}_P(\mathbf{A}^n) \hookrightarrow \mathscr{O}_P(V)$ and $\varphi(J\mathscr{O}_P(\mathbf{A}^n)) = J'\mathscr{O}_P(V)$. φ is injective since $\varphi(J\mathscr{O}_P(\mathbf{A}^n)) = J'\mathscr{O}_P(V)$. Hence $\varphi : \mathscr{O}_P(\mathbf{A}^n)/J \to \mathscr{O}_P(\mathbf{A}^n)$ is isomorphic. In particular, $\mathscr{O}_P(\mathbf{A}^n)/I\mathscr{O}_P(\mathbf{A}^n) \cong \mathscr{O}_P(V)$ (by taking $J = I$ and noting that $J' = I' = 0$).

□

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

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

(2) Hence,

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

□

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 $\mathscr{O}_i = \mathscr{O}_{P_i}(\mathbf{A}^n)$. By Proposition 6,
$$R \cong k[x_1, \ldots, x_n]/I \cong \prod_{i=1}^{N} \mathscr{O}_i/I\mathscr{O}_i,$$
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 $\mathrm{im}(\varphi)$ are submodules of M and M' respectively. Show that

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

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* $\mathrm{im}(\varphi)$ *is a subgroup of* M'. It suffices to show that $a-b \in \mathrm{im}(\varphi)$ for all $a, b \in \mathrm{im}(\varphi)$. As $a, b \in \mathrm{im}(\varphi)$, 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 $a - b \in \mathrm{im}(\varphi)$.

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

(5) *Show that*

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

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

□

Problem 2.49.*

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

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

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

is exact.

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

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

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

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

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

Proof of (a).

(1) Define $\overline{\varphi} : M/N \to M'$ by

$$\overline{\varphi}(m+N) = \varphi(m).$$

$\overline{\varphi}$ is well-defined since $m+N = n+N$ implies that $m-n \in N \subseteq \ker(\varphi)$.

(2) $\overline{\varphi}$ is a homomorphism of R-modules since φ is a homomorphism of R-modules.

(3) $\overline{\varphi} \circ \pi = \varphi$ by construction.

(4) Suppose there is a homomorphism $\psi : M/N \to M'$ such that $\psi \circ \pi = \varphi$. For any $m+N \in M/N$, we have

$$\overline{\varphi}(m+N) = \varphi(m) = (\psi \circ \pi)(m) = \psi(\pi(m)) = \psi(m+N).$$

That is, $\psi = \overline{\varphi}$.

□

Proof of (b).

(1) Define $\pi : M/P \twoheadrightarrow M/N$ by

$$\pi : \underbrace{m+P}_{\in M/P} \mapsto \underbrace{m+N}_{\in M/N}.$$

(a) *Show that π is well-defined.* If $m+P = n+P \in M/P$, then $m-n \in P \subseteq N$ or $m+N = n+N \in M/N$.

(b) π is a module homomorphism since M/N is a module.

(c) π is surjective by construction.

(2) Define $i : N/P \hookrightarrow M/P$ by

$$i : \underbrace{m+P}_{\in N/P} \mapsto \underbrace{m+P}_{\in M/P}.$$

(a) *Show that i is well-defined.* If $m+P = n+P \in N/P$, then $m, n \in N \subseteq M$ and $m-n \in P$. So $m+P = n+P \in M/P$.

(b) i is a module homomorphism since M/P is a module.

(c) i is injective by construction.

(3) To show that $0 \to N/P \to M/P \to M/N \to 0$ is exact, it suffices to show that $\ker(\pi) = \operatorname{im}(i) = N/P$ (by the injectivity of i). It is trivial since

$$m+P \in \ker(\pi) \iff m \in N \iff m+P \in N/P.$$

□

Proof of (c).

(1) By (b),

$$0 \to W/U \to V/U \xrightarrow{\varphi} V/W \to 0$$

is exact.

(2) By the rank-nullity theorem for a linear transformation,

$$\dim V/U = \dim \operatorname{im}(\varphi) + \dim \ker(\varphi) = \dim V/W + \dim W/U.$$

□

Proof of (d).

(1) Regard R as a R-module and I, J as submodules of a R-module R.

(2) As $J \subseteq I$, by (b) we have

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

□

Proof of (e).

(1) Note that $\mathfrak{m}^{n+1} \subseteq \mathfrak{m}^n$ are ideals in a local ring $\mathscr{O}$.

(2) By (d), there is a natural exact sequence of $\mathscr{O}$-modules:

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

□

Problem 2.50.*

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

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

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

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

Proof of (a).

(1) By Problem 2.49(e),

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

is exact.

(2) By the rank-nullity theorem (Proposition 3),

$$\begin{aligned} \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) &= \dim_k(R/\mathfrak{m}^{n+1}) - \dim_k(R/\mathfrak{m}^n) \\ &= (n+1) - n \qquad ((b)) \\ &= 1. \end{aligned}$$

□

Proof of (b).

(1) Let t be a uniformizing parameter for R, $z \in R$. By Problem 2.30(b), there are unique $\lambda_0, \ldots, \lambda_{n-1} \in k$ and $z_{n-1} \in R$ such that

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_{n-1} t^{n-1} + z_{n-1} t^n.$$

Hence we can define a map $\varphi : R/\mathfrak{m}^n \to k^n$ by

$$\varphi : z + \mathfrak{m}^n \mapsto (\lambda_0, \ldots, \lambda_{n-1}).$$

(2) φ is well-defined by the uniqueness of the expression of z in Problem 2.30(b). φ is a k-module homomorphism and φ is surjective (since $k \subseteq R$). φ is injective by the uniqueness of the expression of z in Problem 2.30(b).

(3) Hence, $R/\mathfrak{m}^n \cong k^n$ or $\dim_k(R/\mathfrak{m}^n) = n$ for $n > 0$. (It is also true for $n = 0$ since $\dim_k(\{0\}) = 0$.)

□

Proof of (c).

(1) Note that $\mathfrak{m}^n = (t^n)$ as $\mathfrak{m} = (t)$ where t is a uniformizing parameter for R.

(2) Since $(z) = (t^n) = \mathfrak{m}^n$, $\mathrm{ord}(z) = n$ by Problem 2.28. (Here $\mathrm{ord}(z) \geq n$ by $z \in (t^n)$ and $n \geq \mathrm{ord}(z)$ by $t^n \in (z)$.)

(3) Hence,

$$\mathrm{ord}(z) = n = \dim_k(R/\mathfrak{m}^n) = \dim_k(R/(z))$$

by (b).

□

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

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

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

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

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

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

□

Problem 2.52.* (Isomorphism theorems for modules)

Let N, P be submodules of a module M. Show that the subgroup

$$N + P = \{n + p : n \in N, p \in P\}$$

is a submodule of M. Show that there is a natural R-module isomorphism of $N/(N \cap P)$ onto $(N + P)/P$.

Proof.

(1) *Show that $N+P$ is a submodule of M.* Given any $n_1+p_1, n_2+p_2 \in N+P$,

$$(n_1 + p_1) + (n_2 + p_2) = \underbrace{n_1 + n_2}_{\in N} + \underbrace{p_1 + p_2}_{\in P} \in N + P.$$

Given any $n + p \in N + P$ and $r \in R$,

$$r(n + p) = \underbrace{rn}_{\in N} + \underbrace{rp}_{\in P} \in N + P.$$

Here we use the fact that N and P are modules.

(2) Define a module homomorphism $\varphi : N \to M/P$ by

$$\varphi : m \mapsto m + P.$$

$\ker(\varphi) = N \cap P$ and $\operatorname{im}(\varphi) = \{m + P : m \in N\} = (N + P)/P$. By Problem 2.48, φ induces a natural R-module isomorphism of $N/\ker(\varphi) = N/(N \cap P)$ onto $\operatorname{im}(\varphi) = (N + P)/P$ (which is sending $m + (N \cap P)$ to $m + P$).

□

Problem 2.53.*

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

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

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

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

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

Proof of (a).

(1) Define a map $\overline{T} : V/W \to T(V)/T(W)$ by

$$\overline{T} : v + W \mapsto T(v) + T(W).$$

(2) *Show that $\overline{T}$ is well-defined.* Suppose $u + W = v + W \in V/W$. So $u - v \in W$. So $T(u - v) = T(u) - T(v) \in T(W)$ (since T is a linear map). Hence, $T(u) + T(W) = T(v) + T(W)$.

(3) $\overline{T}$ is a linear map since T is a linear map.

(4) $\overline{T}$ is surjective by construction. Also, $\overline{T}$ is injective since T is injective. Therefore, $\overline{T} : V/W \xrightarrow{\sim} T(V)/T(W)$ is isomorphic.

□

Proof of (b).

(1) Put $N = T(V)$ and $P = W$ in Problem 2.52 to get

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

(2) Put $N = W$ and $P = T(V)$ in Problem 2.52 to get

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

□

Proof of (c).

(1) Note that $W \subseteq W+T(V) \subseteq V$ as vector spaces and V/W is finite-dimensional. By Problem 2.49(c),

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

(2) Similarly, $T(V) \subseteq W \cap T(V) \subseteq T(W)$ as vector spaces and $T(V)/T(W)$ is finite-dimensional (since $V/T(W)$ is finite-dimensional and $T(V)/T(W)$ is a subspace of $V/T(W)$). Again by Problem 2.49(c),

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

(3) By (a),

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

By (b),

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

Hence, the result is established by (1)(2).

□

Proof of (d).

(1) Note that $V/T(V)$ is finite-dimensional. By Problem 2.49(c),

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

(2) Similarly,

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

(3) By (b),

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

By (c),

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

Hence, the result is established by (1)(2).

□

2.11. Free Modules

Problem 2.54.

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

Proof.

(1) Any element $m \in M$ can be written uniquely as

$$m = \sum_{i=1}^{n} r_i m_i$$

for some $r_i \in R$ (which is analogous to the vector space).

(2) The number of members in a basis for M is called the **rank** of M. That is, $n = \text{rank}(M)$.

□

Problem 2.55.

Let $f = x^n + a_1x^{n-1} + \cdots + a_n$ be a monic polynomial in $R[x]$. Show that $R[x]/(f)$ is a free R-module with basis $\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}$, where $\overline{x}$ is the residue of x.

Proof.

(1) Given any $\overline{g} \in R[x]/(f)$ where

$$g = b_0x^m + b_1x^{m-1} + \cdots + b_m \in R[x],$$

it suffices to show that $\overline{g}$ is a linear combination of

$$\mathscr{B} := \{\overline{1}, \overline{x}, \ldots, \overline{x}^{n-1}\}.$$

(2) By the division-with-remainder property of $R[x]$,

$$g = fq + r$$

where $q, r \in R[x]$ with $r = c_0x^{n-1} + \cdots + c_{n-1}$. Hence,

$$\overline{g} = \overline{f}\overline{q} + \overline{r} = \overline{r} = c_0\overline{x}^{n-1} + \cdots + c_{n-1}\overline{1}$$

is a linear combination of $\mathscr{B}$.

□

Problem 2.56.

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

Proof.

(1) If X generates M, then for any $m \in M$ we can write

$$m = \sum_{x \in X} a_x x$$

as a finite sum where $a_x \in R$ and $x \in X \subseteq M$. Define $\varphi_x \in M_X$ by $\varphi_x(y) = \delta_{xy}$ where δ_{xy} is the Kronecker delta. Hence, the homomorphism $\alpha : M_X \to M$ maps the finite sum $\varphi := \sum_{x \in X} a_x\varphi_x$ to $\sum_{x \in X} a_x x = m$.

(2) Conversely, if the homomorphism $\alpha : M_X \to M$ is onto, then for any $m \in M$ there is a finite sum $\varphi := \sum_{x \in X} a_x \varphi_x$ such that $\alpha(\varphi) = m$. Hence,

$$m = \alpha(\varphi) = \alpha\left(\sum_{x \in X} a_x \varphi_x\right) = \sum_{x \in X} a_x x$$

is generated by X.

(3) Let

$$F = \bigoplus_{m \in M} R$$

be a free module. Define a map $\varphi : F \to M$ by

$$\varphi : (0, \ldots, 0, \underbrace{1}_{m\text{th position}}, 0, \ldots 0) \mapsto m.$$

φ is well-defined. φ is a module homomorphism. φ is surjective. Hence

$$M \cong F/ker(\varphi)$$

is isomorphic to a quotient of a free module.

□

Chapter 3: Local Properties of Plane Curves

3.1. Multiple Points and Tangent Lines

Problem 3.1.

Prove that in the above examples $P = (0,0)$ is the only multiple point on the curves $c = y^2 - x^3$, $d = y^2 - x^3 - x^2$, $e = (x^2+y^2)^2 + 3x^2y - y^3$, and $f = (x^2+y^2)^3 - 4x^2y^2$.

Proof.

(1)

$$\frac{\partial c}{\partial x} = -3x^2 = 0$$
$$\frac{\partial c}{\partial y} = 2y = 0$$

implies that $(x,y) = (0,0)$. Note that $c(0,0) = \frac{\partial f}{\partial c}(0,0) = \frac{\partial c}{\partial y}(0,0) = 0$. So $(x,y) = (0,0)$ is the only multiple point on c.

(2)

$$\frac{\partial d}{\partial x} = -3x^2 - 2x = 0$$
$$\frac{\partial d}{\partial y} = 2y = 0$$

implies that $(x,y) = (0,0) \in d$ is the only multiple point on d. (Note that $(x,y) = \left(-\frac{2}{3}, 0\right) \notin d$.)

(3)

$$\frac{\partial e}{\partial x} = 4x(x^2+y^2) + 6xy = 0$$
$$\frac{\partial e}{\partial y} = 4y(x^2+y^2) + 3x^2 - 3y^2 = 0$$

implies that $x = 0$ or $4(x^2+y^2) + 6y = 0$.

(a) $x = 0$ implies that $(x,y) = (0,0)$ or $(0,1)$. Note that $(0,1)$ is a simple point (since $\frac{\partial e}{\partial y}(0,1) = 1$).

(b) $4(x^2+y^2)+6y=0$ implies that $x^2+y^2=-\frac{3y}{2}$ and thus

$$\begin{aligned}0&=4y(x^2+y^2)+3x^2-3y^2\\&=4y\left(-\frac{3y}{2}\right)+3x^2-3y^2\\&=3(x^2-3y^2).\end{aligned}$$

$(x,y)\in e$ implies that

$$\begin{aligned}0&=(x^2+y^2)^2+3x^2y-y^3\\&=(3y^2+y^2)^2+3(3y^2)y-y^3\\&=8y^3(2y+1).\end{aligned}$$

So $(x,y)=(0,0)$ or $\left(\pm\frac{\sqrt{3}}{2},-\frac{1}{2}\right)$. Note that $\frac{\partial e}{\partial x}\left(\pm\frac{\sqrt{3}}{2},-\frac{1}{2}\right)\neq 0$.

Therefore, $(x,y)=(0,0)$ is the only multiple point on e.

(4)

$$\begin{aligned}\frac{\partial f}{\partial x}&=6x(x^2+y^2)^2-8xy^2=x(6(x^2+y^2)^2-8y^2)=0\\\frac{\partial f}{\partial y}&=6y(x^2+y^2)^2-8x^2y=y(6(x^2+y^2)^2-8x^2)=0\end{aligned}$$

implies that $(x,y)=(0,0)$ or $6(x^2+y^2)^2=8x^2=8y^2$. $6(x^2+y^2)^2=8x^2=8y^2$ implies that $x^2=y^2$. So $(x,y)\in f$ implies that $x^2=y^2=\frac{1}{2}$, contrary that $6=6(x^2+y^2)^2\neq 8x^2=4$. Therefore, $(x,y)=(0,0)$ is the only multiple point on f.

□

Problem 3.2.

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

(a) $y^3-y^2+x^3-x^2+3xy^2+3x^2y+2xy$.

(b) $x^4+y^4-x^2y^2$.

(c) $x^3+y^3-3x^2-3y^2+3xy+1$.

(d) $y^2+(x^2-5)(4x^4-20x^2+25)$.

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

Proof of (a).

(1) Let $f = y^3 - y^2 + x^3 - x^2 + 3xy^2 + 3x^2y + 2xy \in k[x, y]$. So

$$\frac{\partial f}{\partial x} = 3x^2 + 6xy + 3y^2 - 2x + 2y = 0$$
$$\frac{\partial f}{\partial y} = 3x^2 + 6xy + 3y^2 + 2x - 2y = 0$$

implies that

$$6(x + y)^2 = 0$$
$$-4(x - y) = 0$$

Note that $f(0, 0) = \frac{\partial f}{\partial x}(0, 0) = \frac{\partial f}{\partial y}(0, 0) = 0$. Hence, $(x, y) = (0, 0)$ is the only multiple point on f.

(2) Write $f = (y^3 + 3xy^2 + 3x^2y + x^3) + (-x^2 + 2xy - y^2)$. The tangent lines at $(x, y) = (0, 0)$ is the linear factors of $-x^2 + 2xy - y^2 = -(x - y)^2$. Hence, the line $x - y = 0$ is the only tangent line at $(x, y) = (0, 0)$ of the multiplicity $= 2$.

□

Proof of (b).

(1) Let $f = x^4 + y^4 - x^2y^2 \in k[x, y]$. So

$$\frac{\partial f}{\partial x} = 4x^3 - 2xy^2 = 0$$
$$\frac{\partial f}{\partial y} = 4y^3 - 2x^2y = 0$$

implies that $(x, y) = (0, 0)$. Note that $f(0, 0) = \frac{\partial f}{\partial x}(0, 0) = \frac{\partial f}{\partial y}(0, 0) = 0$. Hence, $(x, y) = (0, 0)$ is the only multiple point on f.

(2) The tangent lines at $(x, y) = (0, 0)$ is the linear factors of $x^4 + y^4 - x^2y^2$. Hence, there are four distinct tangent lines

$$x \pm \sqrt{\frac{1 \pm \sqrt{-3}}{2}} y$$

at $(x, y) = (0, 0)$. Each tangent line is simple.

□

Proof of (c).

(1) Let $f = x^3 + y^3 - 3x^2 - 3y^2 + 3xy + 1 \in k[x, y]$. So

$$\frac{\partial f}{\partial x} = 3(x^2 - 2x + y) = 0$$
$$\frac{\partial f}{\partial y} = 3(y^2 - 2y + x) = 0$$

implies that $(x - y)(x + y - 3) = 0$.

(2) The case $x - y = 0$. Take $x = y$ in $3x^2 - 6x + 3y = 0$ to get $(x, y) = (1, 1), (0, 0)$. $(x, y) = (1, 1)$ is a multiple point on f since $f(1, 1) = \frac{\partial f}{\partial x}(1, 1) = \frac{\partial f}{\partial y}(1, 1) = 0$. $(x, y) = (0, 0)$ is impossible since $f(0, 0) = 1 \neq 0$.

(3) The case $x + y - 3 = 0$. Take $x = -y + 3$ in f to get $1 = 0$, which is absurd.

(4) By (2)(3), the only multiple point on f is $(x, y) = (1, 1)$.

(5) Let $t(x, y) = (x + 1, y + 1)$. Then

$$f^t = f(x + 1, y + 1) = x^3 + y^3 + 3xy.$$

The tangent lines at $(x, y) = (1, 1)$ is the linear factors of $x^3 + y^3 + 3xy$. Hence, there are two distinct simple tangent lines x and y at $(x, y) = (1, 1)$.

□

Proof of (d).

(1) Let $f = y^2 + (x^2 - 5)(4x^4 - 20x^2 + 25) \in k[x, y]$. So

$$\frac{\partial f}{\partial x} = 2x(2x^2 - 5)(6x^2 - 25) = 0$$
$$\frac{\partial f}{\partial y} = 2y = 0$$

implies that there are only two multiple points

$$(x, y) = \left(\pm\sqrt{\frac{5}{2}}, 0\right)$$

on f.

(2) Let $t(x, y) = \left(x + \sqrt{\frac{5}{2}}, y\right)$. Then

$$\begin{aligned} f^t &= f\left(x + \sqrt{\frac{5}{2}}, y\right) \\ &= 4x^6 + 12\sqrt{10}x^5 + 110x^4 + 20\sqrt{10}x^3 - 100x^2 + y^2. \end{aligned}$$

The tangent lines at $(x, y) = \left(\sqrt{\frac{5}{2}}, 0\right)$ is the linear factors of $-100x^2 + y^2 = -(10x + y)(10x - y)$. Hence, there are two distinct simple tangent lines

$$10x \pm y$$

at $(x, y) = \left(\sqrt{\frac{5}{2}}, 0\right)$.

(3) Similarly, there are also two distinct simple tangent lines

$$10x \pm y$$

at $(x, y) = \left(-\sqrt{\frac{5}{2}}, 0\right)$.

□

Problem 3.3.

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

Proof.

(1) Might assume that $P = (0, 0)$. (Note that any translation of f preserves the degree of f.)

(2) Write

$$f = f_m + f_{m+1} + \cdots + f_n$$

where f_i is a form in $k[x, y]$. Since m is the multiplicity of f at P, $m = n$. Hence, f is a form in two variables of degree n, or f consists of n lines through P.

□

Problem 3.4.

Let P be a double point on a curve f. Show that P is a node if and only if

$$\frac{\partial^2 f}{\partial x \partial y}(P)^2 \neq \frac{\partial^2 f}{\partial x^2}(P) \cdot \frac{\partial^2 f}{\partial y^2}(P).$$

Proof.

(1) Might assume that $P = (0, 0)$ is a double point on f. Write

$$f = f_2 + f_3 + \cdots + f_n \in k[x, y]$$

(where f_i is a form in $k[x, y]$), and

$$f_2 = ax^2 + bxy + cy^2 \in k[x, y].$$

(2) P is a node if and only if the discriminant

$$b^2 - 4ac \neq 0.$$

Note that

$$\begin{aligned}\frac{\partial^2 f}{\partial x \partial y}(P) &= b,\\ \frac{\partial^2 f}{\partial x^2}(P) &= 2a,\\ \frac{\partial^2 f}{\partial y^2}(P) &= 2c.\end{aligned}$$

Hence, P is a node if and only if

$$b^2 - 4ac = b^2 - (2a)(2c) = \frac{\partial^2 f}{\partial x \partial y}(P)^2 - \frac{\partial^2 f}{\partial x^2}(P) \cdot \frac{\partial^2 f}{\partial y^2}(P) \neq 0.$$

□

Problem 3.5.

($\mathrm{char}(k) = 0$*) Show that $m_P(f)$ is the smallest integer m such that for some $i + j = m$,*

$$\frac{\partial^m f}{\partial x^i \partial y^j}(P) \neq 0.$$

Find an explicit description for the leading form for f at P in terms of these derivatives.

Proof.

(1) Might assume that $P = (0, 0)$. Write $f = f_0 + f_1 + \cdots + f_n$ where f_i is a form in $k[x, y]$. Consider any form f_m of f. Write

$$f_m = c_m x^m + c_{m-1} x^{m-1} y + \cdots + c_0 y^m$$

where $c_i \in k$ and not all c_i are zero.

(2) Similar to Problem 3.4, $\frac{\partial^m f}{\partial x^i \partial y^j}(P) = c_i i! j!$. Here $i + j = m$. Hence,

$$c_i = \frac{1}{i!j!} \frac{\partial^m f}{\partial x^i \partial y^j}(P) = \frac{1}{m!} \binom{m}{i} \frac{\partial^m f}{\partial x^i \partial y^j}(P)$$

and thus

$$f_m = \frac{1}{m!} \sum_{i=0}^{m} \binom{m}{i} \frac{\partial^m f}{\partial x^i \partial y^j}(P) x^i y^j.$$

(3) Suppose m is the smallest integer such that for some $i+j=m$,

$$\frac{\partial^m f}{\partial x^i \partial y^j}(P) \neq 0.$$

Then $f_0 = f_1 = \cdots = f_{m-1} = 0$ and $f_m \neq 0$ in $k[x,y]$ by (2). Therefore, $m = m_P(f)$. The explicit description for the leading form f_m for f at P is already stated in (2).

□

Problem 3.6.

Irreducible curves with given tangent lines ℓ_i of multiplicity r_i may be constructed as follows: if $\sum r_i = m$, let $f = \prod \ell_i^{r_i} + f_{m+1}$, where f_{m+1} is chosen to make f irreducible (see Problem 2.34).

Proof.

(1) Let $f_m = \prod \ell_i^{r_i} \in k[x,y]$. Problem 1.4 implies that there exists a point $P = (a,b)$ such that $f_m(P) \neq 0$ since $f_m \neq 0 \in k[x,y]$.

(2) Let $\ell : bx - ay = 0$ and $f_{m+1} = \ell^{m+1}$. Since $(a,b) \neq (0,0)$, $\deg(\ell) = 1$. Also, $\ell_i \nmid \ell$ by (1). Hence, f_m and f_{m+1} have no common factors. By Problem 2.34, $f = f_m + f_{m+1}$ is irreducible.

□

Problem 3.7.

(a) *Show that the real part of the curve e of the examples is the set of points in $\mathbf{A}^2(\mathbb{R})$ whose polar coordinates (r,θ) satisfy the equation $r = -\sin(3\theta)$. Find the polar equation for the curve f.*

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

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

(d) *Show that the curves constructed in (b) and (c) are all irreducible in $\mathbf{A}^2(\mathbb{C})$. (Hint: Make the polynomials homogeneous with respect to a variable z, and use §2.6.)*

Proof of (a).

(1) De Moivre's theorem implies that

$$\begin{aligned}\cos(n\theta) + i\sin(n\theta) &= (\cos\theta + i\sin\theta)^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (\cos\theta)^{n-k} i^k (\sin\theta)^k \\ &= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n}{2k} (\cos\theta)^{n-2k} (\sin\theta)^{2k} \\ &\quad + i \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} (\cos\theta)^{n-2k-1} (\sin\theta)^{2k+1}.\end{aligned}$$

Hence,

$$\sin(n\theta) = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} (\cos\theta)^{n-2k-1} (\sin\theta)^{2k+1}.$$

In particular,

$$\sin(3\theta) = 3\cos^2\theta\sin\theta - \sin^3\theta.$$

(2) $r = -\sin(3\theta)$ implies that

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

Hence, $r = -\sin(3\theta)$ implies that

$$(x^2 + y^2)^2 = -3x^2y + y^3$$

in $\mathbf{A}^2(\mathbb{R})$.

(3) As $f(x, y) = (x^2 + y^2)^3 - 4x^2y^2$, $f(r\cos\theta, r\sin\theta) = 0$ implies that

$$r^6 = 4r^4\cos^2\theta\sin^2\theta = r^4\sin^2 2\theta$$

or

$$r^2 = \sin^2 2\theta.$$

□

Proof of (b).

(1) By (a), $r = \sin(n\theta)$ with odd $n \geq 1$ implies that

$$\begin{aligned} r = \sin(n\theta) &= \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} (\cos\theta)^{n-2k-1} (\sin\theta)^{2k+1} \\ \Longrightarrow r^{n+1} &= \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} (r\cos\theta)^{n-2k-1} (r\sin\theta)^{2k+1} \\ \Longrightarrow (x^2+y^2)^{\frac{n+1}{2}} &= \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1}. \end{aligned}$$

Hence, $r = \sin(n\theta)$ defines the real part of a curve

$$\alpha : (x^2+y^2)^{\frac{n+1}{2}} - \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1}$$

of degree $n+1$.

(2) Note that $(0,0) \in \alpha$. Since

$$\begin{aligned} \frac{\partial\alpha}{\partial x} &= (n+1)(x^2+y^2)^{\frac{n-1}{2}} x \\ &\quad - \sum_{k=0}^{\frac{n-3}{2}} (-1)^k (n-2k-1) \binom{n}{2k+1} x^{n-2k-2} y^{2k+1} \\ \frac{\partial\alpha}{\partial y} &= (n+1)(x^2+y^2)^{\frac{n-1}{2}} y \\ &\quad - \sum_{k=0}^{\frac{n-1}{2}} (-1)^k (2k+1) \binom{n}{2k+1} x^{n-2k-1} y^{2k}, \end{aligned}$$

$\frac{\partial\alpha}{\partial x}(0,0) = \frac{\partial\alpha}{\partial y}(0,0) = 0$. $(0,0)$ is a multiple point.

(3) The tangents at $(0,0)$ are the linear factors of

$$\sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1}.$$

Clearly, y is a tangent line at $(0,0)$. Note that rotation by $\frac{\pi}{n}$ is a linear transformation that takes the curve into itself. Hence, all tangents at $(0,0)$ are

$$\ell_k : \sin\frac{k\pi}{n} x - \cos\frac{k\pi}{n} y$$

for $k = 0, 1, \ldots, n-1$. All ℓ_k are pairwise distinct, and thus $(0,0)$ is an ordinary n-tuple point.

□

Proof of (c).

(1) Similar to (b), $r^2 = \sin^2(n\theta)$ defines the real part of a curve

$$\beta : (x^2+y^2)^{n+1} - \left(\sum_{k=0}^{\frac{n-2}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1} \right)^2$$

of degree $2n+2$.

(2) Note that

$$\beta(0,0) = \frac{\partial \beta}{\partial x}(0,0) = \frac{\partial \beta}{\partial y}(0,0) = 0.$$

Hence, $(0,0)$ is a multiple point.

(3) Similar to (b), all tangents at $(0,0)$ are

$$\ell_k : \sin \frac{k\pi}{n} x - \cos \frac{k\pi}{n} y$$

of multiplicity $= 2$ for $k = 0, 1, \ldots, n-1$.

□

Proof of (d).

(1) The case n is odd.

(a) Consider

$$\alpha : (x^2+y^2)^{\frac{n+1}{2}} - \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1}.$$

(b) Since

$$\begin{aligned} \alpha_{n+1} &:= (x^2+y^2)^{\frac{n+1}{2}} \\ &= (x+iy)^{\frac{n+1}{2}} (x-iy)^{\frac{n+1}{2}} \\ \alpha_n &= \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1} \\ &= c \prod_{k=0}^{n-1} \left(\sin \frac{k\pi}{n} x - \cos \frac{k\pi}{n} y \right) \end{aligned}$$

(with some $c \in \mathbb{C}$), α_{n+1} and α_n have no common factors in $\mathbb{C}[x,y]$. By Problem 2.34, α is irreducible.

(2) The case n is even.

(a) Consider

$$\beta : \underbrace{(x^2+y^2)^{n+1}}_{:=\beta_{2n+2}} - \underbrace{\left(\sum_{k=0}^{\frac{n-2}{2}}(-1)^k\binom{n}{2k+1}x^{n-2k-1}y^{2k+1}\right)^2}_{:=\beta_{2n}}.$$

(b) Similar to the proof of Problem 2.34, suppose $\beta = \beta_{2n} + \beta_{2n+2} = rs \in \mathbb{C}[x,y]$. So

$$(\beta_{2n}+\beta_{2n+2})^* = (rs)^* \Longrightarrow z^2\beta_{2n} + \beta_{2n+2} = r^*s^*.$$

Note that $\deg_z(z^2\beta_{2n}+\beta_{2n+2}) = 2$. So $\deg_z(r^*) = 0, 1, 2$.

(c) The case $\deg_z(r^*) = 0, 2$ is similar to the proof of Problem 2.34 because β_{2n} and β_{2n+2} have no common factors in $\mathbb{C}[x,y]$.

(d) The case $\deg_z(r^*) = 1$. (So $\deg_z(s^*) = 1$.) Write $r = r_p + r_{p+1}$ and $s = s_q + s_{q+1}$. Hence, $\beta = rs$ implies that

$$r_p s_q = -\left(\sum_{k=0}^{\frac{n-2}{2}}(-1)^k\binom{n}{2k+1}x^{n-2k-1}y^{2k+1}\right)^2$$

$$r_p s_{q+1} + r_{p+1}s_q = 0$$

$$r_{p+1}s_{q+1} = (x^2+y^2)^{n+1} = (x+iy)^{n+1}(x-iy)^{n+1}.$$

Since $n+1$ is odd and $x \pm iy \nmid -\left(\sum_{k=0}^{\frac{n-2}{2}}(-1)^k\binom{n}{2k+1}x^{n-2k-1}y^{2k+1}\right)^2$, $r_p s_{q+1} + r_{p+1}s_q = 0$ implies that $r_p = s_q = 0$, which is absurd.

(e) By (b)(c)(d), β is irreducible over $\mathbb{C}$.

□

Problem 3.8.

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

(a) *Show that $m_Q(f^t) \geq m_P(f)$.*

(b) *Let $t = (t_1, t_2)$, and define*

$$J_Q t = \left(\frac{\partial t_i}{\partial x_j}(Q)\right)$$

*to be the **Jacobian matrix** of t at Q. Show that $m_Q(f^t) = m_P(f)$ if $J_Q t$ is invertible.*

(c) *Show that the converse of (b) is false: let* $t = (x^2, y)$, $f = y - x^2$, $P = Q = (0, 0)$.

Proof of (a).

(1) Might assume that $P = Q = (0, 0)$. Write $t = (t_1, t_2)$ and thus $(0, 0) = t(0, 0) = (t_1(0, 0), t_2(0, 0))$. So there is no nonzero constant term in t_i $(i = 1, 2)$.

(2) Might assume that $f \neq 0$ (since there is nothing to prove when $f = 0$). Write $f = f_m + f_{m+1} + \cdots + f_n$ where f_i is a form in $k[x, y]$ and $f_m \neq 0$. So,

$$f(t_1(x, y), t_2(x, y)) = f_m(t_1(x, y), t_2(x, y)) + \cdots + f_n(t_1(x, y), t_2(x, y))$$

has the multiplicity $= \infty$ or $\geq m = m_P(f)$. In any case, $m_Q(f^t) \geq m_P(f)$.

□

Proof of (b).

(1) Might assume that $P = Q = (0, 0)$. Since $J_Q t$ is invertible,

$$\begin{pmatrix} \frac{\partial t_1}{\partial x}(Q) & \frac{\partial t_1}{\partial y}(Q) \end{pmatrix} \neq 0,$$
$$\begin{pmatrix} \frac{\partial t_2}{\partial x}(Q) & \frac{\partial t_2}{\partial y}(Q) \end{pmatrix} \neq 0$$

(as vectors). Hence t_1 (resp. t_2) has the multiplicity $= 1$.

(2) Define

$$s = (s_1, s_2) : \mathbf{A}^2 \to \mathbf{A}^2$$

be a polynomial map such that s_i is the linear term of t_i. Note that $J_Q s = J_Q t$ is invertible and $m_Q(f^s) = m_Q(f^t)$ for any f.

(3) *Show that* $m_Q(f^s) = m_Q(f^t)$ *for any* $f \in k[x, y]$. Might assume that $f \neq 0$ (since there is nothing to prove when $f = 0$). Write $f = f_m + f_{m+1} + \cdots + f_n$ where f_i is a form in $k[x, y]$ and $f_m \neq 0$. Since

$$m_Q(f_i^t) = m_Q(f_i^s) = i \text{ or } \infty,$$

$m_Q(f^s) = m_Q(f^t)$.

(4) Since $J_Q s$ is invertible, s^{-1} is also a polynomial map with an invertible Jacobian matrix $J_Q s^{-1}$. By (a),

$$m_Q(f^s) \geq m_P(f) = m_P((f^s)^{s^{-1}}) = m_Q(f^s)$$

or $m_Q(f^s) = m_P(f)$. Therefore, $m_Q(f^t) = m_Q(f^s) = m_P(f)$.

□

Proof of (c). $m_P(f) = 1$ and $m_Q(f^t) = 1$ since $f^t = y - x^4$. However,

$$J_Q t = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

is not invertible. □

Problem 3.9.

Let $f \in k[x_1, \ldots, x_n]$ define a hypersurface $V(f) \subseteq \mathbf{A}^n$. Let $P \in \mathbf{A}^n$.

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

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

(c) *Examine $f = x^2 + y^2 - z^2$, $P = (0, 0, 0)$. Is it possible to define tangent hyperplanes at multiple points?*

Proof of (a).

(1) Let $P = (0, \ldots, 0)$. Write $f = f_m + f_{m+1} + \cdots + f_n$, where f_i is a form in $k[x_1, \ldots, x_n]$ of degree i, $f_m \neq 0$. We define m to be the multiplicity of f at $P = (0, \ldots, 0)$, write $m = m_P(f)$.

(2) To extend these definitions to a point $P = (a_1, \ldots, a_n) \neq (0, \ldots, 0)$, let t be the translation that takes $(0, \ldots, 0)$ to P, i.e.,

$$t(x_1, \ldots, x_n) = (x_1 + a_1, \ldots, x_n + a_n).$$

Then

$$f^t = f(x_1 + a_1, \ldots, x_n + a_n).$$

Define $m_P(f)$ to be $m_{(0,\ldots,0)}(f^t)$, i.e., write $f^t = g_m + g_{m+1} + \cdots$, g_i forms, $g_m \neq 0$, and let $m = m_P(f)$.

□

Proof of (b).

(1) Let $P = (0, \ldots, 0)$. Write $f = f_m + f_{m+1} + \cdots + f_n$, where f_i is a form in $k[x_1, \ldots, x_n]$ of degree i, $f_m \neq 0$. If $m = 1$, then $f_m = f_1$ is a hyperplane. Hence, we can define the tangent hyperplane to f at P to be f_1.

(2) Similar to (a), the tangent hyperplane to f at $P = (a_1, \ldots, a_n) \neq (0, \ldots, 0)$ is g_1 where

$$f^t = g_1 + g_2 + \cdots$$

and $t(x_1, \ldots, x_n) = (x_1 + a_1, \ldots, x_n + a_n)$.

□

Proof of (c).

(1) No.

(2) *Show that $x^2+y^2-z^2$ is irreducible over k.* (Reductio ad absurdum) Suppose $x^2+y^2-z^2$ were reducible. By Problem 1.1, we can write

$$x^2+y^2-z^2=(a_1x+a_2y+a_3z)(b_1x+b_2y+b_3z)$$

for some $a_i, b_i \in k$ $(i=1,2,3)$. Expanding out the right hand side and comparing coefficients to get

$$\begin{aligned} &a_1b_1=a_2b_2=-a_3b_3=1\\ &a_1b_2+a_2b_1=a_2b_3+a_3b_2=a_3b_1+a_1b_3=0. \end{aligned}$$

So $a_i, b_i \neq 0$ for all i and

$$b_1=\frac{-a_1}{a_3}b_3=\frac{-a_1}{a_3}\cdot\frac{-a_3}{a_2}b_2=\frac{-a_1}{a_3}\cdot\frac{-a_3}{a_2}\cdot\frac{-a_2}{a_1}b_1=-b_1.$$

Hence, $b_1=0$, which is absurd.

(3) Since $x^2+y^2-z^2$ is irreducible over any field k with $\mathrm{char}(k)=0$, it is impossible to define tangent hyperplanes at $(0,0,0)$.

□

Problem 3.10.

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

Proof.

(1) Let $f \in k[x,y]$ be an irreducible plane curve, and

$$V=V\left(f,\frac{\partial f}{\partial x},\frac{\partial f}{\partial y}\right)$$

be the set of the multiple (singular) points of f. Moreover, V is an algebraic set.

(2) Suppose $\frac{\partial f}{\partial x}\neq 0$ (since not all $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are zero). It is nothing to do if $\frac{\partial f}{\partial x}$ is a nonzero constant. Suppose $\deg(\frac{\partial f}{\partial x})\geq 1$. Since f is irreducible and $\deg\left(\frac{\partial f}{\partial x}\right)=\deg f-1$, f and $\frac{\partial f}{\partial x}$ have no common factors. By Proposition 2 in §1.6, $V\left(f,\frac{\partial f}{\partial x}\right)$ is a finite set. Hence, $V\subseteq V\left(f,\frac{\partial f}{\partial x}\right)$ is finite as a subset of a finite set.

(3) The conclusion is not true for hypersurfaces when $n \geq 3$. Consider $f = x_2^2 - x_1^3 \in k[x_1, \ldots, x_n]$. The set of the multiple (singular) points of f is

$$\{(0, 0, a_3, \ldots, a_n) : a_3, \ldots, a_n \in k\},$$

which is infinite as k is infinite.

□

Problem 3.11. (Tangent space)

*Let $V \subseteq \mathbf{A}^n$ be an affine variety, $P \in V$. The **tangent space** $T_P(V)$ is defined to be*

$$\left\{(v_1, \ldots, v_n) \in \mathbf{A}^n : \sum_i \frac{\partial g}{\partial x_i}(P) v_i = 0 \ \forall g \in I(V)\right\}.$$

If $V = V(f)$ is a hypersurface, f irreducible, show that

$$T_P(V) = \left\{(v_1, \ldots, v_n) \in \mathbf{A}^n : \sum_i \frac{\partial f}{\partial x_i}(P) v_i = 0\right\}.$$

How does the dimension of $T_P(V)$ relate to the multiplicity of f at P?

Proof.

(1) By the Hilbert's Nullstellensatz, the irreducibility of f implies that $I(V) = I(V(f)) = (f)$.

(2) Let

$$W = \left\{(v_1, \ldots, v_n) \in \mathbf{A}^n : \sum_i \frac{\partial f}{\partial x_i}(P) v_i = 0\right\}.$$

$W \supseteq T_P(V)$ is true since $f \in I(V) = (f)$.

(3) *Show that $W \subseteq T_P(V)$.* Given any $(v_1, \ldots, v_n) \in W$. Now for any $g \in I(V) = (f)$, there exists a $h \in k[x_1, \ldots, x_n]$ such that $g = fh$. Hence,

$$\begin{aligned}
\sum_i \frac{\partial g}{\partial x_i}(P) v_i &= \sum_i \frac{\partial (fh)}{\partial x_i}(P) v_i \\
&= \sum_i \left(\frac{\partial (f)}{\partial x_i}(P) h(P) + \underbrace{f(P)}_{=0} \frac{\partial h}{\partial x_i}(P) \right) v_i \\
&= h(P) \underbrace{\sum_i \frac{\partial f}{\partial x_i}(P) v_i}_{=0} \\
&= 0
\end{aligned}$$

implies that $(v_1, \ldots, v_n) \in T_P(V)$.

(4) By definition of $T_P(V)$,

$$\dim_k(T_P(V)) = \begin{cases} n-1 & \text{if } m_P(f) = 1 \\ n & \text{if } m_P(f) > 1. \end{cases}$$

□

3.2. Multiplicities and Local Rings

Problem 3.12. (Flex)

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

(a) *Let $f = y - x^n$. For which n does f have a flex at $P = (0,0)$, and what kind of flex?*

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

Proof of (a).

(1) When $n = 0$ or 1, the tangent line L to f at any point is $L = f$ itself. So

$$\mathrm{ord}_P^f(L) = \mathrm{ord}_P^f(f) = \mathrm{ord}_P^f(0) = \infty.$$

P is a higher flex.

(2) When $n > 1$, the tangent line L to f at $P = (0,0)$ is $L = y$. So

$$\mathrm{ord}_P^f(L) = \mathrm{ord}_P^f(y) = \mathrm{ord}_P^f(x^n) = n.$$

Here x is a uniformizing parameter for $\mathscr{O}_P(f)$ since the line x is not tangent to f (Theorem 1). Hence, P is a flex if $n \geq 3$, P is an ordinary flex if $n = 3$, and P is a higher flex if $n > 3$.

□

Proof of (b).

(1) Since y is the tangent line, $\mathrm{ord}_P^f(y) \geq 2$. By Problem 2.29(a),

$$\mathrm{ord}_P^f(y) = \mathrm{ord}_P^f(ax^2 + \cdots) = 2$$

if and only if $a \neq 0$. Hence, P is flex iff $\mathrm{ord}_P^f(y) \geq 3$ iff $a = 0$.

(2) In general,

$$\mathrm{ord}_P^f(y) = \mathrm{ord}_P^f(ax^2 + \cdots) = m_P(ax^2 + \cdots) = m_P(f - y).$$

Hence, P is a higher flex if $f - y$ has no nonzero form of degree 3.

□

Problem 3.13.*

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

Proof.

(1) From the exact sequence

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

it suffices to show that

$$\dim_k(\mathscr{O}/\mathfrak{m}^n) = \frac{n(n+1)}{2}$$

as $0 \leq n < m_P(f)$. (Problem 2.49 and Proposition 7 in §2.10.)

(2) We may assume that $P = (0, 0)$. Similar to the proof of Theorem 2, we are reduced to calculating the dimension of $k[x, y]/(I^n, f)$. Let $m = m_P(f)$. By the definition of m,

$$f \in \underbrace{(x, y)}_{=I}^m = I^m.$$

So if $0 \leq n < m_P(f)$, then $f \in I^m \subseteq I^n$ and thus $(I^n, f) = I^n$. Therefore,

$$\begin{aligned} \dim_k(\mathscr{O}/\mathfrak{m}^n) &= \dim_k(k[x, y]/(I^n, f)) \\ &= \dim_k(k[x, y]/I^n) \\ &= \frac{n(n+1)}{2}. \qquad \text{(Problem 2.46)} \end{aligned}$$

So

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

(3) P is a simple point if $m = m_P(f) = 1$ by definition. Note that

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \begin{cases} 1 & \text{if } m = 1 \text{ (Theorem 1)} \\ 2 & \text{if } m > 1 \text{ ((2))}. \end{cases}$$

Therefore, P is a simple iff $m = 1$ iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

□

Problem 3.14.

Let $V = V(x^2-y^3, y^2-z^3) \subseteq \mathbf{A}^3$, $P = (0,0,0)$, $\mathfrak{m} = \mathfrak{m}_P(V)$. *Find* $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$. *(See Problem 1.40.)*

Proof.

(1) $\mathfrak{m} = (x, y, z)$.

(2) Write $\mathscr{O} = \mathscr{O}_P(V)$. By Problem 1.40(a), every element of $\mathscr{O}$ is of the form

$$\overline{a} + \overline{x}\overline{b} + \overline{yc} + \overline{xy}\overline{d}$$

for some $a, b, c, d \in k[z]$.

(3) By (1)(2), $\{\overline{1}\}$ (resp. $\{\overline{1}, \overline{z}, \overline{y}, \overline{z}\}$) is a basis for $\mathscr{O}/\mathfrak{m}$ (resp. $\mathscr{O}/\mathfrak{m}^2$). Hence, $\dim_k(\mathscr{O}/\mathfrak{m}) = 1$ (resp. $\dim_k(\mathscr{O}/\mathfrak{m}^2) = 4$). Therefore,

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathscr{O}/\mathfrak{m}^2) - \dim_k(\mathscr{O}/\mathfrak{m}) = 3$$

by Proposition 7 in §2.10.

(4) By Theorem I.5.1 in *Robin Hartshorne, Algebraic Geometry*,

$$3 = \dim_k(\mathfrak{m}/\mathfrak{m}^2) + \mathrm{rank}J = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

Here the Jacobian matrix of V at P

$$J = \left[\frac{\partial f_i}{\partial x_j}(P)\right] = \begin{pmatrix} 2x & -3y^2 & 0 \\ 0 & 2y & -3z^2 \end{pmatrix}_{P=(0,0,0)} = 0$$

has rank zero.

□

Problem 3.15.

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

(b) *Let* $\mathscr{O} = \mathscr{O}_P(\mathbf{A}^r(k))$. *Show that* $\chi(n)$ *is a polynomial of degree* r *in* n, *with leading coefficient* $\frac{1}{r!}$ *(see Problem 2.36).*

Proof of (a). Might assume that $P = (0,0)$. By Problem 2.46, the Hilbert-Samuel polynomial is

$$\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n) = \dim_k(k[x,y]/(x,y)^n) = \frac{n(n+1)}{2}.$$

□

Proof of (b).

(1) Might assume that $P = (0, \ldots, 0)$. Similar to (a),

$$\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n) = \dim_k(k[x_1, \ldots, x_r]/(x_1, \ldots, x_r)^n).$$

(2) Since

$$\mathscr{B} = \{x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} : i_1 + \cdots + i_r < n\}$$

is a basis for $k[x_1, \ldots, x_r]/(x_1, \ldots, x_r)^n$,

$$\dim_k(k[x_1, \ldots, x_r]/(x_1, \ldots, x_r)^n) = |\mathscr{B}|.$$

(3) By the stars and bars (combinatorics) method (as Problem 2.35(b)),

$$\begin{aligned}
|\mathscr{B}| &= |\{(i_1, \ldots i_r) : i_1 + \cdots + i_r \leq n\}| \\
&\quad - |\{(i_1, \ldots i_r) : i_1 + \cdots + i_r = n\}| \\
&= |\{(i_1, \ldots i_r, j) : i_1 + \cdots + i_r + j = n\}| \\
&\quad - |\{(i_1, \ldots i_r) : i_1 + \cdots + i_r = n\}| \\
&= \binom{n+r}{r} - \binom{n+r-1}{r-1} \\
&= \binom{n+r-1}{r} \\
&= \frac{1}{r!}(n+r-1)(n+r-2)\cdots(n+1)(n).
\end{aligned}$$

So

$$\chi(n) = \frac{1}{r!}(n+r-1)(n+r-2)\cdots(n+1)(n)$$

is a polynomial of degree r in n, with leading coefficient $\frac{1}{r!}$.

(4) By Problem 2.36, we can also deduce that

$$\begin{aligned}
\dim_k(k[x_1, \ldots, x_r]/(x_1, \ldots, x_r)^n) &= \sum_{i=0}^{n-1} \dim_k V(i, r) \\
&= \sum_{i=0}^{n-1} \binom{i+r-1}{r-1} \\
&= \binom{n+r-1}{r}
\end{aligned}$$

by the Pascal's identity.

□

Problem 3.16.

Let $f \in k[x_1, \ldots, x_r]$ define a hypersurface in $\mathbf{A}^r$. Write $f = f_m + f_{m+1} + \cdots$, and let $m = m_P(f)$ where $P = (0, \ldots, 0)$. Suppose f is irreducible, and let $\mathscr{O} = \mathscr{O}_P(V(f))$, $\mathfrak{m}$ its maximal ideal. Show that $\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n)$ is a polynomial of degree $r-1$ for sufficiently large n, and that the leading coefficient of χ is $\frac{m_P(f)}{(r-1)!}$. Can you find a definition for the multiplicity of a local ring that makes sense in all the cases you know?

Proof.

(1) Similar to the proof of Theorem 2. By Problem 2.43,

$$\mathfrak{m}^n = I^n \mathscr{O}$$

where $I = (x_1, \ldots, x_r) \subseteq k[x_1, \ldots, x_r]$. Since $V(I^n) = \{P\}$,

$$k[x_1, \ldots, x_r]/(I^n, f) \cong \mathscr{O}_P(\mathbf{A}^r)/(I^n, f)\mathscr{O}_P(\mathbf{A}^r) \cong \mathscr{O}/I^n\mathscr{O} \cong \mathscr{O}/\mathfrak{m}^n$$

(Corollary 2 to Proposition 6 in §2.9 and Problem 2.44).

(2) So we are reduced to calculating the dimension of $k[x_1, \ldots, x_r]/(I^n, f)$. As $n \geq m = m_P(f)$, there is a natural ring homomorphism

$$\varphi : k[x_1, \ldots, x_r]/I^n \to k[x_1, \ldots, x_r]/(I^n, f)$$

and a k-linear map

$$\psi : k[x_1, \ldots, x_r]/I^{n-m} \to k[x_1, \ldots, x_r]/I^n$$

defined by $\overline{g} \mapsto \overline{fg}$. It is easy to verify that the sequence

$$0 \to k[x_1, \ldots, x_r]/I^{n-m} \xrightarrow{\psi} k[x_1, \ldots, x_r]/I^n \xrightarrow{\varphi} k[x_1, \ldots, x_r]/(I^n, f) \to 0$$

is exact.

(3) By Problem 3.15,

$$\begin{aligned}
&\dim_k(k[x_1, \ldots, x_r]/(I^n, f)) \\
&= \binom{n+r-1}{r} - \binom{n-m+r-1}{r} \\
&= \frac{1}{r!}\left((n+r-1)\cdots n - (n-m+r-1)\cdots(n-m)\right) \\
&= \frac{1}{r!}\left(n^{r-1}(rm) + \cdots\right) \\
&= \frac{m}{(r-1)!}n^{r-1} + \cdots .
\end{aligned}$$

Therefore, $\chi(n) = \dim_k(\mathscr{O}/\mathfrak{m}^n)$ is a polynomial of degree $r-1$ for $n \geq m$, and that the leading coefficient of χ is $\frac{m_P(f)}{(r-1)!}$.

(4) It is reasonable to define the multiplicity of a Noetherian local ring $\mathscr{O}$ by

$$(d!) \cdot (\text{leading coefficient of } \chi(n))$$

for sufficiently large n, where d is the dimension (or Krull dimension) of $\mathscr{O}$. (Note that the dimension of a hypersurface in $\mathbf{A}^r$ is $r-1$.)

□

3.3. Intersection Numbers

Problem 3.17.

Find the intersection numbers of various pairs of curves

(a) $a = y - x^2$

(b) $b = y^2 - x^3 + x$

(c) $c = y^2 - x^3$

(d) $d = y^2 - x^3 - x^2$

(e) $e = (x^2 + y^2)^2 + 3x^2y - y^3$

(f) $f = (x^2 + y^2)^3 - 4x^2y^2$

at the point $P = (0, 0)$.

Proof.

(1) Note that Example in §3.3 shows that $I(P, e \cap f) = 14$. Also,

$$\begin{aligned}
I(P, a \cap b) &= m_P(a)m_P(b) = 1 \cdot 1 = 1 \\
I(P, a \cap d) &= m_P(a)m_P(d) = 1 \cdot 2 = 2 \\
I(P, b \cap c) &= m_P(b)m_P(c) = 1 \cdot 2 = 2 \\
I(P, b \cap d) &= m_P(b)m_P(d) = 1 \cdot 2 = 2 \\
I(P, b \cap e) &= m_P(b)m_P(e) = 1 \cdot 3 = 3 \\
I(P, c \cap d) &= m_P(c)m_P(d) = 2 \cdot 2 = 4 \\
I(P, d \cap e) &= m_P(d)m_P(e) = 2 \cdot 3 = 6 \\
I(P, d \cap f) &= m_P(d)m_P(f) = 2 \cdot 4 = 8
\end{aligned}$$

by Property (5).

(2) *Show that* $I(P, a \cap c) = 3$.

$$\begin{aligned}
I(P, a \cap c) &= I(P, a \cap (c + (-x^2 - y)a)) && \text{(Property (7))} \\
&= I(P, a \cap x^3(x-1)) \\
&= 3I(P, a \cap x) + I(P, a \cap (x-1)) && \text{(Property (6))} \\
&= 3I(P, a \cap x) && \text{(Property (2))} \\
&= 3. && \text{(Property (5))}
\end{aligned}$$

(3) *Show that* $I(P, a \cap e) = 4$.

$$\begin{aligned}
I(P, a \cap e) &= I(P, a \cap (e + (x^2 + 2y^2 + 4y)a)) && \text{(Property (7))} \\
&= I(P, a \cap y^2(y^2 + y + 4)) \\
&= 2I(P, a \cap y) + I(P, a \cap (y^2 + y + 4)) && \text{(Property (6))} \\
&= 2I(P, a \cap y) && \text{(Property (2))} \\
&= 2I(P, (a - y) \cap y) && \text{(Property (7))} \\
&= 2I(P, (-x^2) \cap y) \\
&= 4. && \text{(Property (5))}
\end{aligned}$$

(4) *Show that* $I(P, a \cap f) = 6$. Similar to (3). Let

$$q_4 = x^4 + 3x^2y^2 + 3y^4 + x^2y + 3y^3 - 3y^2.$$

So

$$\begin{aligned}
I(P, a \cap f) &= I(P, a \cap \underbrace{(f + q_4 a)}_{\text{(Property (7))}}) \\
&= I(P, a \cap y^3(y^3 + 3y^2 + 3y - 3)) \\
&= \overbrace{3\underbrace{I(P, a \cap y)}_{=2 \text{ (by (3))}} + \underbrace{I(P, a \cap (y^3 + 3y^2 + 3y - 3))}_{=0 \text{ (Property (2))}}}^{\text{(Property (6))}} \\
&= 6.
\end{aligned}$$

(5) *Show that* $I(P, b \cap f) = 6$. Similar to (3). Let

$$q_5 = -x^6 - 3x^5 - x^3y^2 - x^4 - 3x^2y^2 - y^4 + 3x^3 + xy^2 + 3x^2.$$

So

$$\begin{aligned}
&I(P, b \cap f) \\
&= I(P, b \cap \underbrace{(f + q_5 b)}_{\text{(Property (7))}}) \\
&= I(P, b \cap x^3(x^6 + 3x^5 - 5x^3 - 4x^2 + 3x + 3)) \\
&= \overbrace{3\underbrace{I(P, b \cap x)}_{=2} + \underbrace{I(P, b \cap (x^6 + 3x^5 - 5x^3 - 4x^2 + 3x + 3))}_{=0 \text{ (Property (2))}}}^{\text{(Property (6))}} \\
&= 6.
\end{aligned}$$

Here

$$I(P, b \cap x) = I(P, (b + (x^2 - 1)x) \cap x) = I(P, y^2 \cap x) = 2.$$

(6) *Show that* $I(P, c \cap e) = 7$. Similar to (3).

$$\begin{aligned}
I(P, c \cap e) &= I(P, c \cap \underbrace{(e + (-x^3 - 2x^2 - y^2 + y)c)}_{\text{(Property (7))}}) \\
&= I(P, c \cap x^2(x^4 + 2x^3 + x^2 - xy + 3y)) \\
&= \overbrace{2 \underbrace{I(P, c \cap x)}_{=2 \text{ (Property (5))}} + I(P, c \cap (\underbrace{x^4 + 2x^3 + x^2 - xy + 3y}_{:= h_6}))}^{\text{(Property (6))}} \\
&= 4 + I(P, c \cap h_6).
\end{aligned}$$

Here

$$\begin{aligned}
&I(P, c \cap h_6) \\
&= I(P, (3c) \cap h_6) \\
&= I(P, (3c - yh_6) \cap h_6) \\
&= I(P, (-x^4 y - 2x^3 y \underbrace{-3x^3 - x^2 y + xy^2}) \cap (x^4 + 2x^3 + x^2 - xy + \underbrace{3y}_{})) \\
&= 3 \cdot 1 \\
&= 3
\end{aligned}$$

by Properties (5) and (7). Therefore, $I(P, c \cap e) = 4 + 3 = 7$.

(7) *Show that* $I(P, c \cap f) = 10$. Similar to (5). Let

$$q_7 = -x^6 - 3x^5 - x^3 y^2 - 3x^4 - 3x^2 y^2 - y^4 + 4x^2.$$

So

$$\begin{aligned}
& I(P, c \cap f) \\
&= I(P, c \cap \underbrace{(f + q_7 c)}_{\text{(Property (7))}}) \\
&= I(P, c \cap x^5(x^4 + 3x^3 + 3x^2 + x - 4) \\
&= \overbrace{5\underbrace{I(P, c \cap x)}_{=2} + \underbrace{I(P, c \cap (x^4 + 3x^3 + 3x^2 + x - 4))}_{=0 \text{ (Property (2))}}}^{\text{(Property (6))}} \\
&= 10.
\end{aligned}$$

□

Problem 3.18.

Give a proof of Property (8) that uses only Properties (1)-(7).

Recall Properties (1)-(8):

(1) $I(P, f \cap g)$ is a nonnegative integer for any f, g, and P such that f and g intersect properly at P. $I(P, f \cap g) = \infty$ if f and g do not intersect properly at P.

(2) $I(P, f \cap g) = 0$ if and only if $P \notin f \cap g$. $I(P, f \cap g)$ depends only on the components of f and g that pass through P.

(3) If t is an affine change of coordinates on $\mathbf{A}^2$, and $t(Q) = P$, then

$$I(P, f \cap g) = I(Q, f^t \cap g^t).$$

(4) $I(P, f \cap g) = I(P, g \cap f)$.

(5) $I(P, f \cap g) \geq m_P(f) m_P(g)$, with equality occurring if and only if f and g have not tangent lines in common at P.

(6) If $f = \prod f_i^{r_i}$, and $g = \prod g_j^{s_j}$, then

$$I(P, f \cap g) = \sum_{i,j} r_i s_j I(P, f_i \cap g_j).$$

(7) $I(P, f \cap g) = I(P, f \cap (g + af))$ for any $a \in k[x, y]$.

(8) If P is a simple point on f, then $I(P, f \cap g) = \mathrm{ord}_P^f(g)$.

Proof.

(1) Might assume that f is irreducible. There is nothing to prove if $\mathrm{ord}_P^f(g) = \infty$. Might assume that $n = \mathrm{ord}_P^f(g) < \infty$.

(2) Similar to the proof of Theorem 1 in §3.2, Property (3) implies that we might assume that $P = (0,0)$, that y is the tangent line, and that x is one line through P which is not tangent to f at P. Here x is a uniformizing parameter for $\mathscr{O}_P(f)$ (Theorem 1 in §3.2).

(3) By definition,
$$g = ux^n$$
for some unit in $\mathscr{O}_P(f)$. Write $u = \frac{a}{b}$ where $a, b \in k[x,y]$, $a(P) \neq 0$ and $b(P) \neq 0$. Hence,
$$bg = ax^n + cf$$
in $k[x,y]$ for some $c \in k[x,y]$.

(4) Therefore,
$$\begin{aligned}
I(P, f \cap g) &= I(P, f \cap bg) - I(P, f \cap b) && \text{(Property (6))} \\
&= I(P, f \cap bg) - 0 && \text{(Property (2))} \\
&= I(P, f \cap (ax^n + cf)) && \text{(Step (3))} \\
&= I(P, f \cap ax^n) && \text{(Property (7))} \\
&= I(P, f \cap a) + nI(P, f \cap x) && \text{(Property (6))} \\
&= 0 + nI(P, f \cap x) && \text{(Property (2))} \\
&= n. && \text{(Property (5))}
\end{aligned}$$

□

Problem 3.19.*

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

Proof.

(1) Note that $m_P(L) = 1$ and the only tangent line of L is itself.

(2) By Property (5),
$$\begin{aligned}
& I(P, f \cap L) > m_P(f) = m_P(f) m_P(L) \\
\iff & f \text{ and } L \text{ have one common tangent line at } P \\
\iff & L \text{ is tangent to a curve } f \text{ at } P. && \text{(By (1))}
\end{aligned}$$

□

Problem 3.20.

If P is a simple point on f, then $I(P, f \cap (g+h)) \geq \min\{I(P, f \cap g), I(P, f \cap h)\}$. Give an example to show that this may be false if P is not simple on f.

Proof.

(1)

$$\begin{aligned} I(P, f \cap (g+h)) &= \mathrm{ord}_P^f(g+h) && \text{(Property (8))} \\ &\geq \min\left\{\mathrm{ord}_P^f(g), \mathrm{ord}_P^f(h)\right\} && \text{(Problem 2.28)} \\ &= \min\{I(P, f \cap g), I(P, f \cap h)\}. && \text{(Property (8))} \end{aligned}$$

(2) Pick $P = (0,0)$, $f = (x^2+y^2)^3 - 4x^2y^2$, $g = x$ and $h = y$. By Property (5), $I(P, f \cap (g+h)) = 4$, $I(P, f \cap g) > 4$ and $I(P, f \cap h) > 4$. So

$$I(P, f \cap (g+h)) < \min\{I(P, f \cap g), I(P, f \cap h)\}$$

for such example.

□

Problem 3.21.

Let f be an affine plane curve. Let L be a line that is not a component of f. Suppose $L = \{(a+tb, c+td) : t \in k\}$. Define $g(t) = f(a+tb, c+td)$. Factor $g(t) = \prod(t-\lambda_i)^{e_i}$, λ_i distinct. Show that there is a natural one-to-one correspondence between the λ_i and the points $P_i \in L \cap f$. Show that under this correspondence, $I(P_i, L \cap f) = e_i$. In particular, $\sum I(P, L \cap f) \leq \deg(f)$.

Proof.

(1) *Show that there is a natural one-to-one correspondence between the λ_i and the points $P_i \in L \cap f$.*

$$\begin{aligned} P_i \in L \cap f &\iff P_i \in L \text{ and } P \in f \\ &\iff \exists \lambda \in k \text{ such that } 0 = f(P_i) = f(a+\lambda b, c+\lambda d) = g(\lambda) \\ &\iff \lambda \in k \text{ is a root of } g(t) = \prod(t-\lambda_i)^{e_i} \\ &\iff \lambda = \lambda_i \in k \text{ for some } i. \end{aligned}$$

(2) *Show that $I(P_i, L \cap f) = e_i$.* By Property (3), we may suppose $P_i = (0,0)$ and $L = y$. Write

$$f(x,y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots \in (k[x])[y]$$

where $f_j \in k[x]$. Note that $f_0(x) = f(x,0) = g(x)$. So

$$\begin{aligned} I(P_i, L \cap f) &= I(P_i, y \cap (f_0(x) + f_1(x)y + \cdots)) \\ &= I(P_i, y \cap f_0(x)) && \text{(Property (7))} \\ &= I(P_i, y \cap g(x)) \\ &= I\left(P_i, y \cap \prod (x - \lambda_i)^{e_i}\right) \\ &= \sum_j e_j I(P_j, y \cap (x - \lambda_j)) && \text{(Property (6))} \\ &= e_i I(P_i, y \cap x) && \text{(Property (2))} \\ &= e_i. && \text{(Property (5))} \end{aligned}$$

Here $\lambda_i = 0$ by the correspondence of (1).

(3) In particular,

$$\sum_i I(P_i, L \cap f) = \sum_i e_i = \deg(g(x)) = \deg(f(x,0)) \leq \deg(f(x,y)).$$

□

Problem 3.22. (Cusp)

Suppose P is a double point on a curve f, and suppose f has only one tangent L at P.

(a) *Show that $I(P, f \cap L) \geq 3$. The curve f is said to have an (ordinary) **cusp** at P if $I(P, f \cap L) = 3$.*

(b) *Suppose $P = (0,0)$, and $L = y$. Show that P is a cusp if and only if $\frac{\partial^3 f}{\partial x^3}(P) \neq 0$. Give some examples.*

(c) *Show that if P is a cusp on f, then f has only one component passing through P.*

Might assume that $\mathrm{char}(k) = 0$.

Proof of (a). Since $I(P, f \cap L) > m_P(f) = 2$ (Problem 3.19), $I(P, f \cap L) \geq 3$ (Property (1)). □

Proof of (b).

(1) By assumption,

$$f = y^2 + f_3 + f_4 + \cdots$$

where f_i is a form in $k[x,y]$.

(2) Hence, P is a cusp of f if and only if

$$\begin{aligned} 3 &= I(P, f \cap y) \\ &= I(P, (y^2 + f_3 + f_4 + \cdots) \cap y) \\ &= I(P, (f_3 + f_4 + \cdots) \cap y) \\ &\geq m_P(f_3 + f_4 + \cdots) m_P(y) \\ &\geq 3. \end{aligned}$$

Here the equality is occuring if and only if y is not a tangent line of $f_3 + f_4 + \cdots$ (Property (5)).

(3) Note that

$$\begin{aligned} & y \text{ is not a tangent line of } f_3 + f_4 + \cdots \\ \iff & y \nmid f_3 \\ \iff & \frac{\partial^3 f}{\partial x^3}(P) \neq 0. \qquad \text{(Problem 3.5)} \end{aligned}$$

(4) Examples: $y^2 = x^3$, $y^2 = -x^2y^2 + x^3$ and so on.

□

Proof of (c).

(1) Might assume $P = (0, 0)$ and $L = y$ by Property (3).

(2) Given $f = gh$. Write

$$\begin{aligned} f &= y^2 + \text{higher terms} \\ g &= g_r + \text{higher terms} \\ h &= h_s + \text{higher terms} \end{aligned}$$

where g_r (resp. h_s) is a form of degree r (resp. s) in $k[x, y]$. So $f = gh$ implies that

$$\begin{aligned} y^2 + \text{higher terms} &= (g_r + \text{higher terms})(h_s + \text{higher terms}) \\ &= (g_r h_s) + \text{higher terms}. \end{aligned}$$

Hence $y^2 = g_r h_s$. In particular, $2 = r + s$.

(3) If $y \mid g_r$ and $y \mid h_s$, then

$$\begin{aligned} I(P, g \cap L) > m_P(g) m_P(L) = r &\Longrightarrow I(P, g \cap L) \geq r + 1 \\ I(P, h \cap L) > m_P(h) m_P(L) = s &\Longrightarrow I(P, g \cap L) \geq s + 1. \end{aligned}$$

So,

$$\begin{aligned} 3 &= I(P, f \cap L) \\ &= I(P, g \cap L) + I(P, h \cap L) \\ &\geq (r+1) + (s+1) \\ &= 4, \end{aligned}$$

which is absurd. So we might assume that $g_r = 1$ and $h_s = y^2$. $f = gh$ implies that $g = 1 + g_1 + \cdots$ is not passing through P. Hence the conclusion is established.

□

Problem 3.23. (Hypercusp)

A point P on a curve f is called a ***hypercusp*** *if $m_P(f) > 1$, f has only one tangent line L at P, and $I(P, L \cap f) = m_P(f) + 1$. Generalize the results of the preceding problem to this case.*

Generalization.

(a) *$I(P, f \cap L) \geq m_P(f) + 1$.*

(b) *Suppose $P = (0, 0)$, $L = y$ and $m = m_P(f)$. Then P is a hypercusp if and only if $\frac{\partial^{m+1} f}{\partial x^{m+1}}(P) \neq 0$. Give some examples.*

(c) *If P is a hypercusp on f, then f has only one component passing through P.*

The proof is almost the same as Problem 3.22 by replacing 2 by $m_P(f)$. □

Problem 3.24.*

The object of this problem is to find a property of the local ring $\mathcal{O}_P(f)$ that determines whether or not P is an ordinary multiple point on f. Let f be an irreducible plane curve, $P = (0, 0)$, $\mathfrak{m} = \mathfrak{m}_P(f) > 1$. Let $m = m_P(f)$. For $g \in k[x, y]$ or $\in \Gamma(f)$, denote its residue in $\mathfrak{m}/\mathfrak{m}^2$ by $\overline{g}$.

(a) *Show that the map from $V = \{$forms of degree 1 in $k[x, y]\}$ to $\mathfrak{m}/\mathfrak{m}^2$ taking $ax + by$ to $\overline{ax + by}$ is an isomorphism of vector spaces (see Problem 3.13).*

(b) *Suppose P is an ordinary multiple point, with tangents $L_1, \ldots, L_m$. Show that $I(P, f \cap L_i) > m$ and $\overline{L_i} \neq \lambda \overline{L_j}$ for all $i \neq j$, and all $\lambda \in k$.*

(c) *Suppose there are* $g_1, \ldots, g_m \in k[x,y]$ *such that* $I(P, f \cap g_i) > m$ *and* $\overline{g_i} \neq \lambda \overline{g_j}$ *for all* $i \neq j$, *and all* $\lambda \in k$. *Show that* P *is an ordinary multiple point on* f. *(Hint: Write* $g_i = L_i +$ *higher terms* $\in k[x,y]$. $\overline{L_i} = \overline{g_i} \neq 0$, *and* L_i *is the tangent to* g_i, *so* L_i *is tangent to* f *by Property (5) of intersection numbers. Thus* f *has* m *tangents at* P.*)*

(d) *Show that* P *is an ordinary multiple point on* f *if and only if there are* $g_1, \ldots, g_m \in \mathfrak{m}$ *such that* $\overline{g_i} \neq \lambda \overline{g_j}$ *for all* $i \neq j$, $\lambda \in k$, *and*

$$\dim_k \mathscr{O}_P(f)/(g_i) > m.$$

Proof of (a).

(1) $\mathscr{B} = \{x, y\}$ is a basis for V as a k-vector space.

(2) $\mathscr{B}' = \{\overline{x}, \overline{y}\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$. as a k-vector space.

(3) By (1)(2), we can define a canonical isomorphism

$$\alpha : V \to \mathfrak{m}/\mathfrak{m}^2$$

by sending $\mathscr{B}$ to $\mathscr{B}'$, that is, $\alpha(x) = \overline{x}$ and $\alpha(y) = \overline{y}$.

□

Proof of (b).

(1) Write

$$f = \prod_{i=1}^{m} L_i + \text{higher terms}.$$

Problem 3.19 says that $I(P, f \cap L_i) > m_P(f) = m$.

(2) Since P is an ordinary multiple point on f, L_i and L_j are linearly independent in V in the sense of (a). Hence, $\alpha(L_i) = \overline{L_i}$ and $\alpha(L_j) = \overline{L_j}$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$ (since α is an isomorphism). The conclusion holds.

□

Proof of (c).

(1) Write $g_i = L_i +$ higher terms $\in k[x,y]$. Here g_i has no constant term since $P \in g_i$ by the defintion of intersection numbers.

(2) Pick $\lambda = 0 \in k$ and $j \neq i$. ($m > 1$ implies the existence of j.) So

$$\alpha(L_i) = \overline{L_i} = \overline{g_i} \neq \lambda \overline{g_j} = 0$$

or $L_i \neq 0$ (since α is an isomorphism).

(3) Hence, L_i is the tangent to g_i. So Property (5) implies that

$$I(P, f \cap g_i) \geq m_P(f) m_P(g_i) = m.$$

Note that L_i is the only tangent line of g_i. By Property (5), the assumption $I(P, f \cap g_i) > m$ implies that L_i is tangent to f.

(4) Note that $\overline{g_i} \neq \lambda \overline{g_j}$ for all $i \neq j$, and all $\lambda \in k$. So $\overline{L_i} \neq \lambda \overline{L_j}$ for all $i \neq j$, and all $\lambda \in k$. Since α is an isomorphism, all L_i are linearly independent and thus f has m tangents $L_1, \ldots, L_m$ at P. Therefore, P is an ordinary multiple point.

□

Proof of (d).

(1) Note that

$$\dim_k \mathscr{O}_P(f)/(g_i) = \dim_k \mathscr{O}_P(\mathbf{A}^2)/(f, g_i) = I(P, f \cap g_i)$$

(by Problem 2.44).

(2) ($\Longrightarrow$) Suppose that P is an ordinary multiple point, with tangents $L_1, \ldots, L_m$. By (b),

$$\dim_k \mathscr{O}_P(f)/(L_i) = I(P, f \cap L_i) > m$$

and $\overline{L_i} \neq \lambda \overline{L_j}$ for all $i \neq j$, and all $\lambda \in k$. Take

$$g_i = L_i + I(f) \in \Gamma(f) \subseteq \mathscr{O}_P(f).$$

Since $g_i \in \mathfrak{m}$ (by $L_i(P) = 0$) and $\overline{g_i} = \overline{L_i}$, the conclusion is proved.

(3) ($\Longleftarrow$) Suppose that there are $g_1, \ldots, g_m \in \mathfrak{m}$ such that $\overline{g_i} \neq \lambda \overline{g_j}$, and $\dim_k \mathscr{O}_P(f)/(g_i) > m$. For each $i = 1, \ldots, m$, we take $g_i' + I(f) = g_i \in \mathfrak{m}$ for some $g_i' \in k[x, y]$. Although g_i' is not uniquely determined by g_i, $\overline{g_i'} = \overline{g_i}$ and thus $\overline{g_i'} \neq \lambda \overline{g_j'}$. By (1),

$$\dim_k \mathscr{O}_P(f)/(g_i) = \dim_k \mathscr{O}_P(f)/(g_i') = I(P, f \cap g_i') > m$$

Hence, by (c) f has m tangents at P.

□

Chapter 4: Projective Varieties

4.1. Projective Space

Problem 4.1.

What points in $\mathbf{P}^2$ *do not belong to two of the three sets* U_1, U_2, U_3*?*

Proof.

(1) The point $[1:0:0]$ does not belong to U_2 and U_3.

(2) The point $[0:1:0]$ does not belong to U_3 and U_1.

(3) The point $[0:0:1]$ does not belong to U_1 and U_2.

□

Problem 4.2.*

Let $f \in k[x_1, \ldots, x_{n+1}]$ *(k infinite). Write* $f = \sum f_i$, f_i *a form of degree i. Let* $P \in \mathbf{P}^n(k)$*, and suppose* $f(x_1, \ldots, x_{n+1}) = 0$ *for every choice of homogeneous coordinates* $(x_1, \ldots, x_{n+1})$ *for P. Show that each* $f_i(x_1, \ldots, x_{n+1}) = 0$ *for all homogeneous coordinates for P. (Hint: consider*

$$g(\lambda) = f(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum \lambda^i f_i(x_1, \ldots, x_{n+1})$$

for fixed $(x_1, \ldots, x_{n+1})$*.)*

Proof.

(1) Consider

$$g(\lambda) = f(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum \lambda^i f_i(x_1, \ldots, x_{n+1})$$

for fixed $(x_1, \ldots, x_{n+1})$. $g(\lambda)$ is a polynomial in $k[\lambda]$.

(2) Since $g(\lambda) = f(\lambda x_1, \ldots, \lambda x_{n+1}) = 0$ for all $\lambda \in k - \{0\}$, $g(\lambda) = 0$ has infinitely many solutions in k. Similar to Problem 1.4, $g = 0 \in k[\lambda]$, that is, each $f_i(x_1, \ldots, x_{n+1}) = 0$ for all homogeneous coordinates for P.

□

Problem 4.3.

(a) *Show that the definitions of this section carry over without change to the case where k is an arbitrary field.*

(b) *If k_0 is a subfield of k, show that $\mathbf{P}^n(k_0)$ may be identified with a subset of $\mathbf{P}^n(k)$.*

Proof of (a). Note that a field is a commutative ring where $0 \neq 1$ and all nonzero elements are invertible. Hence the definitions in this section are well-defined for any field k. □

Proof of (b). Note that $0 \in k_0$ and $0 \in k$. So any point $P \in \mathbf{P}^n(k_0)$ is also in $\mathbf{P}^n(k)$ since $P \neq (0, \ldots, 0)$ and

$$\{(\lambda x_1, \ldots, \lambda x_{n+1}) : \lambda \in k_0\} \subseteq \{(\lambda x_1, \ldots, \lambda x_{n+1}) : \lambda \in k\}$$

as a subset. □

4.2. Projective Algebraic Sets

Problem 4.4.*

Let I be a homogeneous ideal in $k[x_1, \ldots, x_{n+1}]$. Show that I is prime if and only if the following condition is satisfied: for any forms $f, g \in k[x_1, \ldots, x_{n+1}]$, if $fg \in I$, then $f \in I$ or $g \in I$.

Proof.

(1) ($\Longrightarrow$) Trivial.

(2) ($\Longleftarrow$) Suppose that $f, g \in k[x_1, \ldots, x_{n+1}]$ and $fg \in I$. Write $f = \sum_{i=0}^{r} f_i$ (resp. $g = \sum_{j=0}^{s} g_j$), f_i a form of degree i (resp. g_j a form of degree j). Induction on the $\deg(fg) = r + s$.

(3) When $r + s = 0$, nothing to do.

(4) Assume that the result is true for smaller values of $r+s$. Then the highest homogeneous component $f_r g_s$ of fg is also in I since I is homogeneous. By assumption, $f_r \in I$ or $g_s \in I$, and might say that $f_r \in I$. Therefore,

$$(f - f_r)g \in I.$$

By the induction hypothesis, $f - f_r \in I$ or $g \in I$. Hence, $f = (f - f_r) + f_r \in I$ or $g \in I$.

(5) Therefore, (3)(4) implies that I is prime.

□

Problem 4.5.

If I is a homogeneous ideal, show that $\mathrm{rad}(I)$ *is also homogeneous.*

Proof.

(1) Given any $f = \sum_{i=0}^{r} f_i \in \mathrm{rad}(I)$, f_i a form of degree i. It suffices to show that each $f_i \in \mathrm{rad}(I)$. Note that $f^m \in I$ for some $m > 0$.

(2) The highest homogeneous component ${f_r}^m$ of f^m is also in I since I is homogeneous. Hence, $f_r \in \mathrm{rad}(I)$. Again note that $f - f_r \in \mathrm{rad}(I)$ and $\deg(f - f_r) < r$. Continue this process (or by induction), and we have $f_{r-1}, \ldots, f_0 \in \mathrm{rad}(I)$.

□

Problem 4.6.

State and prove the projective analogues of properties (1)-(10) of Chapter 1, Sections 2 and 3.

Statements.

(1) *If I is the homogeneous ideal in $k[x_1, \ldots, x_{n+1}]$ generated by a set of forms S, then $V(S) = V(I)$; so every algebraic set is equal to $V(I)$ for some homogeneous ideal I.*

(2) *If $\{I_\alpha\}$ is any collection of homogeneous ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$; so the intersection of any collection of algebraic sets is an algebraic set.*

(3) *If $I \subseteq J$, then $V(I) \supseteq V(J)$.*

(4) *$V(fg) = V(f) \cup V(g)$ for any forms f, g; $V(I) \cup V(J) = V(\{fg : f \in I, g \in J\})$; so any finite union of algebraic sets is an algebraic set.*

(5) *$V(0) = \mathbf{P}^n(k)$; $V(I) = \varnothing$ if I contains all forms of degree $\geq N$ for some N; $V(a_i x_j - a_j x_i) = \{[a_1 : \cdots : a_{n+1}]\}$ for $[a_1 : \cdots : a_{n+1}] \in \mathbf{P}^n(k)$. So any finite subset of $\mathbf{P}^n(k)$ is an algebraic set.*

(6) *If $X \subseteq Y$ are nonempty, then $I(X) \supseteq I(Y)$.*

(7) *$I(\varnothing) = k[x_1, \ldots, x_{n+1}]$; $I(\mathbf{P}^n(k)) = (0)$ if k is an infinite field;*

(8) *$I(V(S)) \supseteq S$ for any set S of forms; $V(I(X)) \supseteq X$ for any set X of points.*

(9) *$V(I(V(S))) = V(S)$ for any set S of forms, 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 homogeneous ideal of an algebraic set, $I = I(V(I))$.*

(10) *$I(X)$ is a radical ideal for any nonempty $X \subseteq \mathbf{P}^n(k)$.*

Proof. Proposition 1 and the projective Nullstellensatz give all. □

Problem 4.7.

Show that each irreducible component of a cone is also a cone.

Proof.

(1) Let V is an algebraic set in $\mathbf{P}^n$, and $C(V)$ be the cone over V. Might assume that $V \neq \varnothing$.

(2) *Show that V is irreducible if and only if $C(V)$ is irreducible.* V is irreducible if and only if $I_p(V) = I_a(C(V))$ is prime if and only if $C(V)$ is irreducible.

(3) Let $V = V_1 \cup \cdots \cup V_r$ be the decomposition of an algebraic set into irreducible components. Note that

$$C(V_1 \cup \cdots \cup V_r) = C(V_1) \cup \cdots \cup C(V_r)$$

(by the definition of the cone). Here each $C(V_i)$ is irreducible (by (2)). By Theorem 2 in §1.5, each irreducible component of $C(V)$ must be one of $C(V_i)$, which is also a cone.

□

Problem 4.8.

Let $V = \mathbf{P}^1$, $\Gamma_h(V) = k[x, y]$. Let $t = x/y \in k(V)$, and show that $k(V) = k(t)$. Show that there is a natural one-to-one correspondence between the points of $\mathbf{P}^1$ and the DVRs with quotient field $k(V)$ that contain k (see Problem 2.27); which DVR corresponds to the point at infinity?

Proof.

(1) *Show that* $k(V) = k(t)$. Given any $f/g \in k(V)$ where $f, g \in \Gamma_h(V)$ are of the same degree. Then

$$f(x,y)/g(x,y) = f(t,1)/g(t,1) \in k(t).$$

Conversely, given any $f/g \in k(t)$,

$$\frac{f(t)}{g(t)} = \frac{f(x/y)}{g(x/y)} = \frac{y^d f(x/y)}{y^d g(x/y)} \in k(V)$$

where $d = \max\{\deg(f), \deg(g)\}$.

(2) Note that $k = \overline{k}$. By Problem 2.27, the DVR's with quotient field $k(V) = k(t)$ are

$$\mathscr{O}_a(\mathbf{A}^1) \text{ where } a \in \mathbf{A}^1 = k \text{ and } \mathscr{O}_\infty(\mathbf{A}^1),$$

which correspond to

$$\mathbf{P}^1(k) = \{[a:1] : a \in k\} \cup \{[1:0]\}.$$

In particular, the DVR $\mathscr{O}_\infty(\mathbf{A}^1)$ corresponds to the point at infinity (= $[1:0]$).

□

Problem 4.9.*

Let I be a homogeneous ideal in $k[x_1, \ldots, x_{n+1}]$, and

$$\Gamma = k[x_1, \ldots, x_{n+1}]/I.$$

Show that the forms of degree d in Γ form a finite-dimensional vector space over k.

Proof.

(1) Write $R = k[x_1, \ldots, x_{n+1}]$. For R (resp. Γ), define $R_{(d)}$ (resp. $\Gamma_{(d)}$) to be the corresponding homogeneous component of degree d. Consider a natural homomorphism

$$\alpha : R_{(d)} \to R_{(d)}/I \cong \Gamma_{(d)}$$

by $\alpha(h) = \overline{h}$ for any form h of degree d.

(2) $\Gamma_{(d)}$ can be regarded as a subspace of $R_{(d)}$ since α is surjective. Since $R_{(d)}$ is finite-dimensional with $\dim R_{(d)} = \binom{d+n-1}{n-1}$, $\Gamma_{(d)}$ is finite-dimensional by linear algebra.

□

Problem 4.10.

Let $R = k[x, y, z]$, $f \in R$ an irreducible form of degree n, $V = V(f) \subseteq \mathbf{P}^2$, and $\Gamma = \Gamma_h(V)$.

(a) *Construct an exact sequence*

$$0 \to R \xrightarrow{\psi} R \xrightarrow{\varphi} \Gamma \to 0$$

where ψ is multiplication by f.

(b) *Show that*

$$\dim_k\{\textit{forms of degree } d \textit{ in } \Gamma\} = dn - \frac{n(n-3)}{2}$$

if $d > n$.

Proof of (a).

(1) ψ is defined by $\psi(g) = fg$ and φ is naturally defined by $\varphi(h) = \overline{h}$. ψ and φ are well-defined and homomorphisms of vector space.

(2) $\mathrm{im}(\psi) = \ker(\varphi) = (f) = I(f)$ (since f is irreducible). ψ is injective since $R = k[x, y, z]$ is a domain. φ is surjective trivially. Hence, the sequence of vector spaces over k is exact.

□

Proof of (b).

(1) The exact sequence

$$0 \to R \xrightarrow{\psi} R \xrightarrow{\varphi} \Gamma \to 0$$

induces the exact sequence

$$0 \to R_{(d-n)} \xrightarrow{\psi} R_{(d)} \xrightarrow{\varphi} \Gamma_{(d)} \to 0,$$

where $*_{(d)}$ (resp. $*_{(d-n)}$) denotes the corresponding homogeneous component of degree d (resp. $d - n$).

(2) By Problem 2.36,

$$\dim_k R_{(d-n)} = \binom{d-n+2}{2}, \qquad \dim_k R_{(d)} = \binom{d+2}{2}.$$

(3) Since $R_{(d)}$ is finite-dimensional, $\Gamma_{(d)}$ is also finite-dimensional (by regarding $\Gamma_{(d)}$ as a subspace of $R_{(d)}$). Proposition 7 in §2.9 shows that

$$\begin{aligned}\dim_k \Gamma_{(d)} &= \dim_k R_{(d)} - \dim_k R_{(d-n)} \\ &= \binom{d+2}{2} - \binom{d-n+2}{2} \\ &= dn - \frac{n^2}{2} + \frac{3n}{2}.\end{aligned}$$

□

Problem 4.11.* (Linear subvariety)

*A set $V \subseteq \mathbf{P}^n(k)$ is called a **linear subvariety** of $\mathbf{P}^n(k)$ if $V = V(h_1, \cdots, h_r)$, where each h_i is a form of degree 1.*

(a) *Show that if t is a projective change of coordinates, then $V^t = t^{-1}(V)$ is also a linear subvariety.*

(b) *Show that there is a projective change of coordinates t of $\mathbf{P}^n$ such that $V^t = V(x_{m+2}, \cdots, x_{n+1})$, so V is a variety.*

(c) *Show that the m that appears in part (b) is independent of the choice of t. It is called the **dimension** of V ($m = -1$ if $V = \varnothing$).*

Proof of (a).

(1) Say $t = (t_1, \ldots, t_{n+1})$ is a projective change of coordinates, and $V = V(h_1, \cdots, h_r)$, where each h_i is a form of degree 1.

(2) *Show that V is a variety and thus $I(V) = (h_1, \ldots, h_r)$ by the projective Nullstellensatz.* V is the set of all non-trivial solutions of the system of linear equations:

$$\begin{aligned} h_1 &= a_{1,1}x_1 + \cdots + a_{1,n+1}x_{n+1} = 0, \\ &\cdots \\ h_r &= a_{r,1}x_1 + \cdots + a_{r,n+1}x_{n+1} = 0. \end{aligned}$$

(Here we identify $[x_1 : \cdots : x_{n+1}] \in \mathbf{P}^n$.) Write $Ax = 0$ and thus $V = V(Ax = 0)$, where

$$A = \underbrace{\begin{pmatrix} a_{1,1} & \cdots & a_{1,n+1} \\ \vdots & \ddots & \vdots \\ a_{r,1} & \cdots & a_{r,n+1} \end{pmatrix}}_{\in \mathsf{M}_{r\times(n+1)}(k)}, \qquad x = \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix}}_{\in \mathsf{M}_{(n+1)\times 1}(k)}.$$

(3) The Gaussian elimination in linear algebra says that $(A|0)$ has the same solutions as its reduced row echelon form $(A'|0)$, that is, $V(Ax = 0) = V(A'x = 0)$.

(4) If $V(h_1, \ldots, h_r) = \varnothing$, nothing to do. If $V(h_1, \ldots, h_r) \neq \varnothing$, then

$$V(h_1, \ldots, h_r) = V(g_1, \ldots, g_{m+1})$$

where $m + 1 = \operatorname{rank}(A)$ is the number of nonzero rows in A' ($m + 1 \leq r, n + 1$) and $g_i = a'_{i,1}x_1 + \cdots + a'_{i,n+1}x_{n+1}$ for $1 \leq i \leq m + 1$. ($a'_{i,j}$ is the entry of the matrix A'.)

(5) Now given any $f + I(V) \in k[x_1, \ldots, x_{n+1}]/I(V)$, we replace the leading term x_{i_1} of g_1 by $x_{i_1} - g_1$ to get

$$f + I(V) = f(x_1, \cdots, \underbrace{x_{i_1} - g_1}_{i_1\text{th position}}, \cdots, x_{n+1}) + I(V) := f_1 + I(V)$$

where $f_1 \in k[x_1, \ldots, \widehat{x_{i_1}} \ldots, x_{n+1}]$. Continue this process to replace each leading term x_{i_j} of g_j by $x_{i_j} - g_j$ to get one by one to get

$$\begin{aligned} f + I(V) &= f_1 + I(V), f_1 \in k[x_1, \ldots, \widehat{x_{i_1}} \ldots, x_{n+1}]. \\ &\cdots \\ f_m + I(V) &= f_{m+1} + I(V), f_{m+1} \in k[x_1, \ldots, \widehat{x_{i_1}}, \ldots, \widehat{x_{i_{m+1}}} \ldots, x_{n+1}]. \end{aligned}$$

Hence, a routine shows that there is a ring isomorphism

$$\alpha : k[x_1, \ldots, x_{n+1}]/I(V) \to \underbrace{k[x_1, \ldots, \widehat{x_{i_1}}, \ldots, \widehat{x_{i_{m+1}}} \ldots, x_{n+1}]}_{\text{a domain}}$$

sending f to f_{m+1}. Therefore, V is a variety.

(6) As $I(V) = (h_1, \ldots, h_r)$, $I(V)^t = (h_1^t, \ldots, h_r^t)$ where each h_i^t is a form of degree 1. Thus $V^t = V(I(V)^t) = V(h_1^t, \ldots, h_r^t)$ is also a linear subvariety of $\mathbf{P}^n(k)$.

□

Proof of (b).

(1) Suppose $A \in \mathsf{M}_{r\times(n+1)}(k)$ is of rank $(n+1) - (m+1) = n - m$. Linear algebra says that there exist invertible matrices $B \in \mathsf{M}_{r\times r}(k)$ and $C \in \mathsf{M}_{(n+1)\times(n+1)}(k)$ such that $D = BAC$, where

$$D = BAC = \underbrace{\begin{pmatrix} O_1 & O_2 \\ O_3 & I_{n-m} \end{pmatrix}}_{\in \mathsf{M}_{r\times(n+1)}(k)}$$

in which $I_{n-m} \in \mathsf{M}_{(n-m)\times(n-m)}(k)$ is the identity matrix and O_1, O_2, and O_3 are zero matrices.

(2) Let t' be the linear map corresponding to the matrix C. So

$$\begin{aligned} V^{t'} &= V(Ax = 0)^{t'} \\ &= V(ACx = 0) \\ &= V(BACx = 0) && (B\text{: invertible}) \\ &= V(Dx = 0) \\ &= V(0, \cdots, 0, x_{m+2}, \cdots, x_{n+1}) && (V \neq \varnothing) \\ &= V(x_{m+2}, \cdots, x_{n+1}). \end{aligned}$$

□

Proof of (c). Linear algebra says that the rank of any matrix is uniquely determined. Therefore, $m = n - \operatorname{rank}(A)$ is uniquely determined. □

Problem 4.12.*

Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbf{P}^n$, $m \leq n$. Show that

$$H_1 \cap H_2 \cap \cdots \cap H_m \neq \varnothing.$$

Proof.

(1) Let
$$H_i : a_{i,1}x_1 + \cdots + a_{i,n+1}x_{n+1} = 0$$
for $i = 1, 2, \ldots, m$.

(2) View (1) as the system of linear equations. Let the coefficient matrix A be
$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n+1} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n+1} \end{pmatrix}.$$
Note that $\operatorname{rank}(A) \leq \min\{m, n+1\} = m$. The rank-nullity theorem shows that
$$\dim_k \ker(A) = (n+1) - \operatorname{rank}(A) \geq (n+1) - m \geq 1.$$
Hence, there is a nonzero solution of $\bigcap_{i=1}^m H_i$, or $\bigcap_{i=1}^m H_i \neq \varnothing \in \mathbf{P}^n$.

□

Problem 4.13.* (Line)

*Let $P = [a_1 : \cdots : a_{n+1}]$, $Q = [b_1 : \cdots : b_{n+1}]$ be distinct points of $\mathbf{P}^n$. The **line** L through P and Q is defined by*

$$L = \{[\lambda a_1 + \mu b_1 : \cdots : \lambda a_{n+1} + \mu b_{n+1}] : \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\}.$$

Prove the projective analogue of Problem 2.15.

(a) *Show that if L is the line through P and Q, and t is a projective change of coordinates, then $t(L)$ is the line through $t(P)$ and $t(Q)$.*

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

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

(d) *Let* $P, P' \in \mathbf{P}^2$*,* L_1*,* L_2 *two distinct lines through* P*,* L_1'*,* L_2' *distinct lines through* P'*. Show that there is a projective change of coordinates* t *of* $\mathbf{P}^2$ *such that* $t(P) = P'$ *and* $t(L_i) = L_i'$*,* $i = 1, 2$*.*

Proof of (a).

(1) Write $t = (t_1, \ldots, t_{n+1})$ as

$$t_i = \sum_j c_{ij} x_j.$$

Given any point $P_{\lambda,\mu} = [\lambda a_1 + \mu b_1 : \cdots : \lambda a_{n+1} + \mu b_{n+1}] \in L$ for some not all zeros $\lambda, \mu \in k$. (In particular, $P_{1,0} = P$ and $P_{0,1} = Q$.)

(2) As

$$\begin{aligned} t_i(P_{\lambda,\mu}) &= \sum_j c_{ij}(\lambda a_j + \mu b_j) \\ &= \lambda \sum_j c_{ij} a_j + \mu \sum_j c_{ij} b_j \\ &= \lambda t_i(P) + \mu t_i(Q), \end{aligned}$$

we have

$$\begin{aligned} t(L) = \{[\lambda t_1(P) + \mu t_1(Q) : \cdots : \lambda t_{n+1}(P) + \mu t_{n+1}(Q)] \\ : \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\}. \end{aligned}$$

Moreover, $t(P) \in t(L)$ as $(\lambda, \mu) = (1, 0)$, $t(Q) \in t(L)$ as $(\lambda, \mu) = (0, 1)$, and $t(P) \neq t(Q)$ (since $P \neq Q$ and t is a projective change of coordinates.) Therefore, $t(L)$ is the line through $t(P)$ and $t(Q)$.

□

Proof of (b).

(1) First, write L as the system of equations

$$x_i = \lambda a_i + \mu b_i$$

$(i = 1, \ldots, n+1)$ where $\lambda, \mu \in k, \lambda \neq 0$ or $\mu \neq 0$. Since $P \neq Q \in \mathbf{P}^n$, there exist $1 \leq \alpha, \beta \leq n$ such that $a_\alpha b_\beta - a_\beta b_\alpha \neq 0$. So we can solve λ and μ in terms of x_α and x_β by Cramer's rule, say

$$\lambda = \frac{x_\alpha b_\beta - x_\beta b_\alpha}{a_\alpha b_\beta - a_\beta b_\alpha}, \qquad \mu = \frac{a_\alpha x_\beta - a_\beta x_\alpha}{a_\alpha b_\beta - a_\beta b_\alpha}.$$

(2) Define

$$V = V\left(x_i = \frac{x_\alpha b_\beta - x_\beta b_\alpha}{a_\alpha b_\beta - a_\beta b_\alpha} a_i + \frac{a_\alpha x_\beta - a_\beta x_\alpha}{a_\alpha b_\beta - a_\beta b_\alpha} b_i : 1 \le i \le n+1\right)$$
$$= V\left(\begin{vmatrix} x_i & a_i & b_i \\ x_\alpha & a_\alpha & b_\alpha \\ x_\beta & a_\beta & b_\beta \end{vmatrix} = 0 : 1 \le i \le n+1\right).$$

By construction, $L = V$ is a linear subvariety in $\mathbf{P}^n$. (See Problem 4.11.)

(3) Might assume that $\alpha = n$ and $\beta = n+1$. View

$$\begin{vmatrix} x_i & a_i & b_i \\ x_\alpha & a_\alpha & b_\alpha \\ x_\beta & a_\beta & b_\beta \end{vmatrix} = 0, i = 1, \ldots, n+1$$

as the system of linear equations. Write A as the corresponding coefficient matrix. A is a reduced row echelon form of rank $(n+1) - 2 = n - 1$ So $\dim(V) = n - \operatorname{rank}(A) = n - (n-1) = 1$.

(4) Conversely, $\dim(V) = 1$ implies that $\operatorname{rank}(A'|0) = n - 1$. So all leading terms are all x_i except two x_α, x_β for some $\alpha \neq \beta$, might say $\alpha = n$ and $\beta = n+1$. Hence V is of the form

$$V = (x_i + a_i x_n + b_i x_{n+1} = 0)$$

for $1 \le i \le n-1$. So

$$V = \{[-a_1\lambda - b_1\mu : \ldots : -a_{n-1}\lambda - b_{n-1}\mu : \lambda : \mu] :$$
$$\lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\}$$

is a line passing two different points

$$P = [-a_1 : \ldots : -a_{n-1} : 1 : 0]$$
$$Q = [-b_1 : \ldots : -b_{n-1} : 0 : 1].$$

□

Proof of (c).

(1) By part (b), a line $L \subseteq \mathbf{P}^2$ is

$$V((a_2b_3 - b_2a_3)x + (a_3b_1 - a_1b_3)y + (a_1b_2 - a_2b_1)z = 0)$$
$$= V\left(\begin{vmatrix} x & a_1 & b_1 \\ y & a_2 & b_2 \\ z & a_3 & b_3 \end{vmatrix} = 0\right),$$

which is also a plane in $\mathbf{P}^2$.

(2) Conversely, given any plane

$$V = V(ax + by + cz = 0) \subseteq \mathbf{P}^2$$

where a, b, c are not all zero. Might assume that $a \neq 0$. (Other cases are similar.) So

$$V = \left\{ \left[-\frac{b}{a}\lambda - \frac{c}{a}\mu : \lambda : \mu \right] \in \mathbf{P}^2 : \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0 \right\}$$

is a line passing $P = \left[-\frac{b}{a} : 1 : 0\right] \in \mathbf{P}^2$ and $Q = \left[-\frac{c}{a} : 0 : 1\right] \in \mathbf{P}^2$.

□

Proof of (d).

(1) Take one point $P_i \in L_i$ (resp. $P_i' \in L_i'$) other than P (resp. P') for $i = 1, 2$. It is possible since every line is passing two distinct points.

(2) By Problem 4.15, $P_1 \notin L_2$ (resp. $P_1' \notin L_2'$) and $P_2 \notin L_1$ (resp. $P_2' \notin L_1'$).

(3) By Problem 4.14, there is a unique projective change of coordinates $t : \mathbf{P}^2 \to \mathbf{P}^2$ such that $t(P) = P'$, $t(P_1) = P_1'$ and $t(P_2) = P_2'$.

(4) Hence, the line $t(L_i)$ (by part (a)) and the line L_i' are both passing P' and P_i' for $i = 1, 2$. Since $P' \neq P_i'$ by construction, Problem 4.15 implies that $t(L_i) = L_i'$.

□

Problem 4.14.*

Let P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) be three points in $\mathbf{P}^2$ not lying on a line. Show that there is a projective change of coordinates $t : \mathbf{P}^2 \to \mathbf{P}^2$ such that $t(P_i) = Q_i$, $i = 1, 2, 3$. Extend this to $n + 1$ points in $\mathbf{P}^n$, not lying on a hyperplane.

Proof.

(1) Write

$$P_i = [a_{i1} : a_{i2} : a_{i3}] \in \mathbf{P}^2(k)$$
$$Q_i = [b_{i1} : b_{i2} : b_{i3}] \in \mathbf{P}^2(k)$$

for $i = 1, 2, 3$.

(2) Define

$$A = \begin{pmatrix} P_1 & P_2 & P_3 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$$
$$B = \begin{pmatrix} Q_1 & Q_2 & Q_3 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{21} & b_{31} \\ b_{12} & b_{22} & b_{32} \\ b_{13} & b_{23} & b_{33} \end{pmatrix}.$$

Note that A (resp. B) is depending on the representations of P_i (resp. Q_i) up to a nonzero constant in k.

(3) Here A (resp. B) is invertible since P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) are not lying on a line. Define $t : \mathbf{P}^2 \to \mathbf{P}^2$ by sending $P = [x : y : z] \in \mathbf{P}^2$ to

$$t(P) = BA^{-1}P = \begin{pmatrix} b_{11} & b_{21} & b_{31} \\ b_{12} & b_{22} & b_{32} \\ b_{13} & b_{23} & b_{33} \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Note that the matrix $BA^{-1} \in \mathsf{GL}_3(k)$ depends on the representations of P_i (resp. Q_i) up to a nonzero constant in k. Hence, t is a well-defined map from $\mathbf{P}^2$ to $\mathbf{P}^2$. Besides, t is a projective change of coordinates mapping P_i to Q_i $(i = 1, 2, 3)$.

(4) *Generalization. Let P_i (resp. Q_i) be $n+1$ points in $\mathbf{P}^n$ $(i = 1, \ldots, n+1)$ not lying on a hyperplane. Then there is a projective change of coordinates $t : \mathbf{P}^n \to \mathbf{P}^n$ such that $t(P_i) = Q_i$ $(i = 1, \ldots, n+1)$.* The proof is the same except replacing 2 by n.

□

Problem 4.15.*

Show that any two distinct lines in $\mathbf{P}^2$ intersect in one point.

Proof.

(1) Let

$$L_1 : a_1x + b_1y + c_1z = 0$$
$$L_2 : a_2x + b_2y + c_2z = 0$$

be two distinct lines in $\mathbf{P}^2$.

(2) View (1) as the system of linear equations. Let the coefficient matrix A be

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

Since L_1 and L_2 are distinct, $\operatorname{rank}(A) = 2$. The rank-nullity theorem shows that

$$\dim_k \ker(A) = 3 - \operatorname{rank}(A) = 1.$$

(3) Might take a basis $\{(x_0, y_0, z_0)\}$ for $\ker(A)$. Here $(x_0, y_0, z_0) \neq 0$ and any other nonzero solutions of $L_1 \cap L_2$ is of the form $(\lambda x_0, \lambda y_0, \lambda z_0)$ $(\lambda \neq 0)$. Therefore,

$$L_1 \cap L_2 = \{[x_0 : y_0 : z_0]\} \in \mathbf{P}^2.$$

□

Problem 4.16.*

Let L_1, L_2, L_3 (resp. M_1, M_2, M_3) be lines in $\mathbf{P}^2(k)$ that do not all pass through a point. Show that there is a projective change of coordinates: $t : \mathbf{P}^2 \to \mathbf{P}^2$ such that $t(L_i) = M_i$. (Hint: Let $P_{ij} = L_i \cap L_j$, $Q_{ij} = M_i \cap M_j$, $i \neq j$, and apply Problem 4.14.) Extend this to $n+1$ hyperplanes in $\mathbf{P}^n$, not passing through a point.

Proof.

(1) Let $P_{ij} = L_i \cap L_j$ (resp. $Q_{ij} = M_i \cap M_j$), $i \neq j$. P_{ij} (resp. Q_{ij}) is uniquely determined by L_i and L_j (resp. M_i and M_j) (Problem 4.15). Also, $P_{ij} \neq P_{i'j'}$ (resp. $Q_{ij} \neq Q_{i'j'}$) if $\{i, j\} \neq \{i', j'\}$ (as sets) by assumption.

(2) Problem 4.14 shows that there is a projective change of coordinates $t : \mathbf{P}^2 \to \mathbf{P}^2$ such that $t(P_{ij}) = Q_{ij}$, $i \neq j$. Similar to the argument in Problem 4.13(d), we conclude that $t(L_i) = M_i$.

(3) *Show that we can extend this to $n+1$ hyperplanes in $\mathbf{P}^n$, not passing through a point.* We cannot apply steps (1)(2) to the generalized case $\mathbf{P}^n$. Instead, we can apply the proof of Problem 4.14.

(4) Let E_i (resp. F_i) $(i = 1, \ldots, n+1)$ be $(n+1)$ hyperplanes in $\mathbf{P}^n$ that do not passing through a point. Write

$$E_i : a_{i,1}x_1 + \cdots + a_{i,n+1} = 0 \in \mathbf{P}^n(k)$$
$$F_i : b_{i,1}x_1 + \cdots + b_{i,n+1} = 0 \in \mathbf{P}^n(k)$$

for $i = 1, \ldots, n+1$.

(5) View E_i (resp. F_i) as the system of linear equations. Let the coefficient

matrix A (resp. B) be

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{n+1,1} \\ \vdots & \ddots & \vdots \\ a_{1,n+1} & \cdots & a_{n+1,n+1} \end{pmatrix}$$
$$B = \begin{pmatrix} b_{1,1} & \cdots & b_{n+1,1} \\ \vdots & \ddots & \vdots \\ b_{1,n+1} & \cdots & b_{n+1,n+1} \end{pmatrix}.$$

Note that A (resp. B) is depending on the representations of E_i (resp. F_i) up to a nonzero constant in k.

(6) Here A (resp. B) is invertible since E_i (resp. F_i) are not passing through a point. Define $t : \mathbf{P}^n \to \mathbf{P}^n$ by sending $P = [x_1 : \cdots : x_{n+1}] \in \mathbf{P}^n$ to

$$t(P) = BA^{-1}P$$
$$= \begin{pmatrix} b_{1,1} & \cdots & b_{n+1,1} \\ \vdots & \ddots & \vdots \\ b_{1,n+1} & \cdots & b_{n+1,n+1} \end{pmatrix} \begin{pmatrix} a_{1,1} & \cdots & a_{n+1,1} \\ \vdots & \ddots & \vdots \\ a_{1,n+1} & \cdots & a_{n+1,n+1} \end{pmatrix}^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix}.$$

Note that the matrix $BA^{-1} \in \mathsf{GL}_{n+1}(k)$ depends on the representations of E_i (resp. F_i) up to a nonzero constant in k. Hence, t is a well-defined map from $\mathbf{P}^n$ to $\mathbf{P}^n$. Besides, t is a projective change of coordinates mapping E_i to F_i $(i = 1, \ldots, n+1)$.

□

Note. It is the duality of Problem 4.14. See Problem 4.18 for more details.

Problem 4.17.*

Let z be a rational function on a projective variety V. Show that the pole set of z is an algebraic subset of V.

Proof.

(1) Similar to the proof of Proposition 2 in §2.4. For $g \in k[x_1, \ldots, x_{n+1}]$, denote the residue of g in $\Gamma_h(V)$ by $\overline{g}$.

(2) Let
$$J_z = \{g \in k[x_1, \ldots, x_{n+1}] : \overline{g}z \in \Gamma_h(V)\}.$$
J_z is an ideal in $k[x_1, \ldots, x_{n+1}]$ containing $I(V)$, and the points of $V(J_z)$ are exactly those points where z is not defined if J_z is homogeneous.

(3) *Show that J_z is homogeneous by the homogeneous property of $I(V)$.* Given any $g = g_r + g_{r+1} + \cdots \in J_z$, where g_i is a form of $k[x_1, \ldots, x_{n+1}]$. Write $z = a/b$ for some form $a, b \in \Gamma_h(V)$ of the same degree. So $\overline{g}z = \overline{g}a/b \in \Gamma_h(V)$. So there is $f = f_s + f_{s+1} + \cdots \in k[x_1, \ldots, x_{n+1}]$ (where f_i is a form of $k[x_1, \ldots, x_{n+1}]$) such that $ga - fb \in I(V)$. Since $I(V)$ is homogeneous, each form $g_i a - f_i b$ is in $I(V)$. So $\overline{g_i}z = \overline{f_i} \in \Gamma_h(V)$ for each i (since $\Gamma_h(V)$ is homogeneous), that is, $g_i \in J_z$ for each i.

□

Problem 4.18. (Duality)

Let $H = V(\sum a_i x_i)$ be a hyperplane in $\mathbf{P}^n$. Note that $(a_1, \ldots, a_{n+1})$ is determined by H up to a constant.

(a) *Show that assigning $[a_1 : \cdots : a_{n+1}] \in \mathbf{P}^n$ to H sets up a natural one-to-one correspondence between $\{$hyperplanes in $\mathbf{P}^n\}$ and $\mathbf{P}^n$. If $P \in \mathbf{P}^n$, let P^* be the corresponding hyperplane; if H is a hyperplane, H^* denotes the corresponding point.*

(b) *Show that $P^{**} = P$, $H^{**} = H$. Show that $P \in H$ if and only if $H^* \in P^*$.*

*This is the well-known **duality** of the projective space.*

Proof of (a).

(1) Define $\alpha : \{\text{hyperplanes}\} \to \mathbf{P}^n$ (resp. $\beta : \mathbf{P}^n \to \{\text{hyperplanes}\}$) by

$$\alpha : V\left(\sum a_i x_i\right) \mapsto [a_1 : \cdots : a_{n+1}],$$
$$\beta : [a_1 : \cdots : a_{n+1}] \mapsto V\left(\sum a_i x_i\right).$$

(2) As $H = V(\sum a_i x_i)$ is a hyperplane, the corresponding

$$\alpha(H) = [a_1 : \cdots : a_{n+1}] \in \mathbf{P}^n$$

and thus α is well-defined. Similarly, β is well-defined.

(3) Note that both $\alpha \circ \beta$ and $\beta \circ \alpha$ are identity maps. α (resp. β) is an isomorphism, that is, there is a natural one-to-one correspondence between

$$\{\text{hyperplanes in } \mathbf{P}^n\} \longleftrightarrow \mathbf{P}^n.$$

□

Proof of (b).

(1) We've showed that $P^{**} = P$, $H^{**} = H$ in (a). It is suffices to show that $P \in H$ iff $H^* \in P^*$.

(2) Write $H = V\left(\sum a_i x_i\right) \subseteq \mathbf{P}^n$ and $P = [b_1 : \cdots : b_{n+1}] \in \mathbf{P}^n$. Hence,

$$\begin{aligned} P \in H &\iff a_1 b_1 + \cdots + a_{n+1} b_{n+1} = 0 \\ &\iff b_1 a_1 + \cdots + b_{n+1} a_{n+1} = 0 \\ &\iff H^* \in P^*. \end{aligned}$$

□

4.3. Affine and Projective Varieties

Problem 4.19.*

If $I = (f)$ is the ideal of an affine hypersurface, show that $I^* = (f^*)$.

Proof.

(1) Note that I^* is the ideal in $k[x_1, \ldots, x_{n+1}]$ generated by $\{g^* : g \in I = (f)\}$. In particular, $f^* \in I^*$. Thus $(f^*) \subseteq I^*$.

(2) Conversely, given any $g = \sum a_i (h_i f)^* \in I^*$, where $a_i, h_i \in k[x_1, \ldots, x_{n+1}]$. Thus,

$$g = \sum_i a_i (h_i f)^* = \sum_i a_i h_i^* f^* = \left(\sum_i a_i h_i^*\right) f^* \in (f^*)$$

(by Proposition 5 in §2.6).

□

Problem 4.20.

Let $V = V(y - x^2, z - x^3) \subseteq \mathbf{A}^3$. Prove:

(a) *$I(V) = (y - x^2, z - x^3)$.*

(b) *$zw - xy \in I(V)^* \subseteq k[x, y, z, w]$, but $zw - xy \notin I((y - x^2)^*, (z - x^3)^*)$. So if $I(V) = (f_1, \ldots, f_r)$, it does not follow that $I(V)^* = (f_1^*, \ldots, f_r^*)$.*

Proof of (a). By Problems 1.11 and 2.8, V is an affine variety. Thus $I(V) = (y - x^2, z - x^3)$ is a prime ideal. □

Proof of (b).

(1) Since $z - xy = (z - x^3) - x(y - x^2) \in I(V)$, $zw - xy = (z - xy)^* \in I(V)^*$.

(2) Suppose $zw - xy \in I((y - x^2)^*, (z - x^3)^*) = I(yw - x^2, zw^2 - x^3)$. Write $zw - xy = f \cdot (yw - x^2) + g \cdot (zw^2 - x^3)$ for some $f, g \in k[x, y, z, w]$. Then $\deg_x(zw - xy) = 1$ but $\deg_x(f \cdot (yw - x^2) + g \cdot (zw^2 - x^3))$ cannot be 1, which is absurd.

□

Problem 4.21.

Show that if $V \subseteq W \subseteq \mathbf{P}^n$ are varieties, and V is a hypersurface, then $W = V$ or $W = \mathbf{P}^n$ (see Problem 1.39).

Proof.

(1) Write $V = V(f)$ for some irreducible form $f \in k[x_1, \ldots, x_{n+1}]$. So $I(V) = (f)$ by the projective Nullstellensatz.

(2) Note that $I(W)$ is a prime ideal such that

$$(f) \supseteq I(W) \supseteq (0).$$

By Problem 1.39, $I(W) = (f)$ or (0). Thus, $W = V$ or $W = \mathbf{P}^n$.

□

Problem 4.22.*

Suppose V is a variety in $\mathbf{P}^n$ and $V \supseteq H_\infty$. Show that $V = \mathbf{P}^n$ or $V = H_\infty$. If $V = \mathbf{P}^n$, $V_* = \mathbf{A}^n$, while if $V = H_\infty$, $V_* = \varnothing$.

Proof.

(1) Note that $H_\infty = V(x_{n+1})$ is a hypersurface. By Problem 4.21, $V = \mathbf{P}^n$ or $V = H_\infty$.

(2) If $V = \mathbf{P}^n$, then $I = I(V) = (0)$. So $V_* = V(I_*) = V(0) = \mathbf{A}^n$.

(3) If $V = H_\infty$, then $I = I(V) = (x_{n+1})$. So $V_* = V(I_*) = V(1) = \varnothing$.

□

Problem 4.23.*

Describe all subvarieties in $\mathbf{P}^1$ *and in* $\mathbf{P}^2$.

Proof.

(1) *Show that all subvarieties in* $\mathbf{P}^1$ *are* $\varnothing$, $\mathbf{P}^1$, *and single points.* (Also compare to Problem 1.8.)

   (a) $\varnothing$, single points and $\mathbf{P}^1$ are all varieties.

   (b) Let V be a nonempty subvariety in $\mathbf{P}^1$. Write $\{[a:b]\} = V(bx-ay) \subseteq V$ for some point $[a:b] \in \mathbf{P}^1$. So $V(bx-ay) \subseteq V \subseteq \mathbf{P}^1$.

   (c) Since $V(bx-ay)$ is a hypersurface and $bx-ay$ is irreducible, Problem 4.21 implies that $V = V(bx-ay)$ (a single point) or $V = \mathbf{P}^1$ itself.

(2) *Show that all subvarieties in* $\mathbf{P}^2$ *are* $\varnothing$, $\mathbf{P}^2$, *single points, and hypersurfaces* $V(f)$, *where* f *is an irreducible form.* Similar to Corollary 2 of Proposition 2 in §1.6.

   (a) Let V be a subvariety in $\mathbf{P}^2$. If V is finite or $I(V) = (0)$, V is of one required type.

   (b) Otherwise $I(V)$ contains a non-constant form f; since $I(V)$ is prime, we may assume f is irreducible.

   (c) Hence, $I(V) = (f)$; for if $g \in I(V)$, $g \notin (f)$, then $V \subseteq V(f,g)$ is finite by Problem 5.7, which is a projective analogue of Proposition 2 in §1.6.

□

Problem 4.24.*

Let $P = [0:1:0] \in \mathbf{P}^2(k)$. *Show that the lines through* P *consist of the following:*

(a) *The vertical lines* $L_\lambda = V(x-\lambda z) = \{[\lambda : t : 1] : t \in k\} \cup \{P\}$.

(b) *The line at infinity* $L_\infty = V(z) = \{[x:y:0] : x, y \in k, x \neq 0 \text{ or } y \neq 0\}$.

Proof.

(1) Let L be one line passing through P and $Q = [b_1 : b_2 : b_3] \neq P$. Thus,

$$\begin{aligned} L &= \{[\mu b_1 : \lambda + \mu b_2 : \mu b_3] : \lambda, \mu \in k, \lambda \neq 0 \text{ or } \mu \neq 0\} \\ &= \{[\mu b_1 : \lambda + \mu b_2 : \mu b_3] : \lambda, \mu \in k, \mu \neq 0\} \cup \{P\} \\ &= \{[b_1 : t + b_2 : b_3] : t \in k\} \cup \{P\} \qquad (t := \lambda/\mu) \end{aligned}$$

Consider two cases: $b_3 \neq 0$ and $b_3 = 0$.

(2) $b_3 \neq 0$. So

$$\begin{aligned} L &= \{[b_1 : t + b_2 : b_3] : t \in k\} \cup \{P\} \\ &= \left\{ \left[\frac{b_1}{b_3} : \frac{t}{b_3} + \frac{b_2}{b_3} : 1 \right] : t \in k \right\} \cup \{P\} \\ &= \{[\lambda : t : 1] : t \in k\} \cup \{P\} \qquad \left(\frac{b_1}{b_3} \mapsto \lambda, \frac{t + b_2}{b_3} \mapsto t \right) \\ &= L_\lambda. \end{aligned}$$

(3) $b_3 = 0$. So

$$\begin{aligned} L &= \{[b_1 : t + b_2 : 0] : t \in k\} \cup \{P\} \\ &= \{[x : y : 0] : y \in k\} \cup \{P\} \qquad (b_1 \mapsto x, t + b_2 \mapsto y) \\ &= \{[x : y : 0] : y \in k, x \neq 0\} \cup \{P\} \\ &= \{[x : y : 0] : y \in k, x \neq 0 \text{ or } y \neq 0\} \\ &= L_\infty. \end{aligned}$$

□

Problem 4.25.*

Let $P = [x : y : z] \in \mathbf{P}^2$.

(a) *Show that* $\{(a, b, c) \in \mathbf{A}^3 : ax + by + cz = 0\}$ *is a hyperplane in* $\mathbf{A}^3$.

(b) *Show that for any finite set of points in* $\mathbf{P}^2$*, there is a line not passing through any of them.*

Proof of (a).

(1) Let $V = \{(a, b, c) \in \mathbf{A}^3 : ax + by + cz = 0\}$.

(2) V is well-defined and the form $ax + by + cz$ is of degree one since not all a, b, c are zero. Hence V is a hyperplane (plane) in $\mathbf{A}^3$.

□

Proof of (b).

(1) Let S be any finite set of points in $\mathbf{P}^2(k)$. Write $S = (S \cap H_\infty) \cap (S - H_\infty)$.

(2) $S \cap H_\infty$ is a finite subset of $H_\infty = \mathbf{P}^1(k) \supseteq \mathbf{A}^1(k) = k$. Since $k = \overline{k}$ is infinite (Problem 1.6), there is one point $[\beta : 1 : 0] \in H_\infty - S$. Here $\beta \in k$ is uniquely determined.

(3) $S - H_\infty$ is finite too. Write $S - H_\infty = \{[\lambda_1 : \mu_1 : 1], \ldots, [\lambda_r : \mu_r : 1]\}$. Here λ_i and μ_i are all uniquely determined ($i = 1, \ldots, r$). Take any $\gamma \in k$ such that $\gamma \notin \{\lambda_1 - \beta\mu_1, \ldots, \lambda_r - \beta\mu_r\}$. (It is possible since k is infinite.)

(4) Let
$$L = V(x - \beta y - \gamma z)$$
be a line in $\mathbf{P}^2$. By construction, $L \cap S = \varnothing$.

□

4.4. Multiprojective Space

Problem 4.26.*

(a) *Define maps $\varphi_{i,j} : \mathbf{A}^{n+m} \to U_i \times U_j \subseteq \mathbf{P}^n \times \mathbf{P}^m$. Using $\varphi_{n+1,m+1}$, define the "biprojective closure" of an algebraic set in $\mathbf{A}^{n+m}$. Prove an analogue of Proposition 3 of §4.3.*

(b) *Generalize part (a) to maps*
$$\varphi : \mathbf{A}^{n_1} \times \cdots \times \mathbf{A}^{n_r} \times \mathbf{A}^m \to \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_r} \times \mathbf{A}^m.$$
Show that this sets up a correspondence between
$$\{\textit{nonempty affine varieties in } \mathbf{A}^{n_1+\cdots+n_r+m}\}$$
and
$$\{\textit{varieties in } \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_r} \times \mathbf{A}^m \textit{ that intersect } U_{n_1+1} \times \cdots \times U_{n_r+1} \times \mathbf{A}^m\}.$$
Show that this correspondence preserves function fields and local rings.

Proof of (a).

(1) Define maps $\varphi_{i,j} : \mathbf{A}^{n+m} \to U_i \times U_j \subseteq \mathbf{P}^n \times \mathbf{P}^m$ by
$$\varphi_{i,j} : (x_1, \ldots, x_n, y_1, \ldots, y_m) \mapsto [x_1 : \ldots : x_{i-1} : 1 : x_i : \ldots : x_n] \times [y_1 : \ldots : y_{j-1} : 1 : y_j : \ldots : y_m].$$
Actually, we can write $\varphi_{i,j}(x, y) = (\varphi_i(x), \varphi_j(y))$ for $x = (x_1, \ldots, x_n) \in \mathbf{A}^n$ and $y = (y_1, \ldots, y_m) \in \mathbf{A}^m$.

(2) Given any algebraic set V in $\mathbf{A}^{n+m}$. Let I^* be the bihomogeneous ideal in $k[x,y] = k[x_1,\dots,x_{n+1},y_1,\dots,y_{m+1}]$ generated by $\{f^* : f \in I\}$. Here

$$f^* = x_{n+1}^r y_{m+1}^s f\left(\frac{x_1}{x_{n+1}},\dots,\frac{x_n}{x_{n+1}},\frac{y_1}{y_{m+1}},\dots,\frac{y_m}{y_{m+1}}\right)$$

where r (resp. s) is the degree of f in x (resp. y). Define $V^* = V(I^*)$ as the "biprojective closure."

(3) Proposition 3 for multiprojective space.

(i) *If $V \subseteq \mathbf{A}^{n+m}$, $\varphi_{n+1,m+1}(V) = V^* \cap (U_{n+1} \times U_{m+1})$ and $(V^*)_* = V$.*

(ii) *If $V \subseteq W \subseteq \mathbf{A}^{n+m}$, then $V^* \subseteq W^* \subseteq \mathbf{P}^n \times \mathbf{P}^m$. If $V \subseteq W \subseteq \mathbf{P}^n \times \mathbf{P}^m$, then $V_* \subseteq W_* \subseteq \mathbf{A}^{n+m}$.*

(iii) *If V is irreducible in $\mathbf{A}^{n+m}$, then V^* is irreducible in $\mathbf{P}^n \times \mathbf{P}^m$.*

(iv) *If $V = \bigcup_i V_i$ is the irreducible decomposition of V in $\mathbf{A}^{n+m}$, then $V^* = \bigcup_i V_i^*$ is the irreducible decomposition of V^* in $\mathbf{P}^n \times \mathbf{P}^m$.*

(v) *If $V \subseteq \mathbf{A}^{n+m}$, then V^* is the smallest algebraic set in $\mathbf{P}^n \times \mathbf{P}^m$ that contains $\varphi_{n+1,m+1}(V)$.*

(vi) *If $V \subsetneq \mathbf{A}^{n+m}$, then no component of V^* lies in or contains $H_\infty \times H_\infty$.*

(vii) *If $V \subseteq \mathbf{P}^n \times \mathbf{P}^m$, and no component of V lies in or contains $(H_\infty \times \mathbf{P}^m) \cup (\mathbf{P}^n \times H_\infty)$, then $V_* \subsetneq \mathbf{A}^{n+m}$ and $(V_*)^* = V$.*

(4) *Proof of Proposition 3 for multiprojective space.*

(i) It follows from Proposition 5 in §2.6.

(ii) It is obvious.

(iii) If $V \subseteq \mathbf{A}^{n+m}$, $I = I(V)$, then a biform f belongs to I^* if and only if $f_* \in I$. If I is prime, it follows readily that I^* is also prime.

(iv) It follows from (ii)(iii)(v).

(v) Suppose W is an algebraic set in $\mathbf{P}^n \times \mathbf{P}^m$ which contains $\varphi_{n+1,m+1}(V)$. If $f \in I(W)$, then $f_* \in I(V)$, so $f = x_{n+1}^r y_{m+1}^s (f_*)^* \in I(V)^*$. Therefore $I(W) \subseteq I(V)^*$, so $W \supseteq V^*$, as desired.

(vi) We may assume V is irreducible. $V^* \not\subseteq H_\infty \times H_\infty$ by (i). If $V \subseteq H_\infty \times H_\infty$, then $I(V)^* \subseteq I(V^*) \subseteq I(H_\infty \times H_\infty) = (x_{n+1}, y_{m+1})$. Buf if $0 \neq f \in I(V)$, then $f^* \in I(V)^*$, but $f^* \notin (x_{n+1}, y_{m+1})$. So $V^* \not\supseteq H_\infty \times H_\infty$.

(vii) We may assume V is irreducible. Since $\varphi_{n+1,m+1}(V_*) \subseteq V$, it suffices to show that $V \subseteq (V_*)^*$, or that $I(V_*)^* \subseteq I(V)$. Let $f \in I(V_*)$. Then $f^N \in I(V)_*$ for some N (Nullstellensatz), so $x_{n+1}^t y_{m+1}^s (f^N)^* \in I(V)$ for some t, s (Proposition 5 in §2.6). But $I(V)$ is prime, and $x_{n+1}, y_{m+1} \notin I(V)$ since $V \not\subseteq (H_\infty \times \mathbf{P}^m) \cup (\mathbf{P}^n \times H_\infty)$, so $f^* \in I(V)$, as desired.

□

Proof of (b).

(1) Define maps $\varphi_{i_1,\dots,i_r} : \mathbf{A}^{n_1} \times \cdots \times \mathbf{A}^{n_r} \times \mathbf{A}^m \to U_{i_1} \times \cdots \times U_{i_r} \times \mathbf{A}^m$ by

$$\varphi_{i_1,\dots,i_r} : (\mathbf{x}_1, \dots, \mathbf{x}_r, \mathbf{y}) \mapsto (\varphi_{i_1}(\mathbf{x}_1), \cdots, \varphi_{i_r}(\mathbf{x}_r), \mathbf{y}),$$

where $\mathbf{x}_i = (x_{i,1}, \dots, x_{i,n_i}) \in \mathbf{A}^{n_i}$ and $\mathbf{y} = (y_1, \dots, y_m) \in \mathbf{A}^m$.

(2) Applying the same argument in (a), we have that there is a correspondence between

$$\{\text{nonempty affine varieties in } \mathbf{A}^{n_1+\cdots+n_r+m}\}$$

and

$$\{\text{varieties in } \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_r} \times \mathbf{A}^m \text{ that intersect } U_{n_1+1} \times \cdots \times U_{n_r+1} \times \mathbf{A}^m\}.$$

(3) Let V be a nonempty affine varieties in $\mathbf{A}^{n_1+\cdots+n_r+m}$. Let $V^* \subseteq \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_r} \times \mathbf{A}^m$ be the multiprojective closure of V intersecting $U_{n_1+1} \times \cdots \times U_{n_r+1} \times \mathbf{A}^m$.

(4) If $\overline{f} \in \Gamma(V^*)$ is a multi-form, we may define $\overline{f}_*$ as follows: take a multi-form $f \in k[\mathbf{x}_1, \dots, \mathbf{x}_r, \mathbf{y}]$ such whose $I(V^*)$-residue in $\overline{f}$, and let $\overline{f}_*$ to be $I(V)$-residue of f_* (one checks that this is independent of the choice of f).

(5) Define a natural isomorphism $\alpha : k(V^*) \to k(V)$ by $\alpha(f/g) = f_*/g_*$, where f, g are multi-forms of the same multi-degree on V^*.

(6) If $P \in V$, we may consider $P \in V^*$ (by means of $\varphi_{n_1+1,\dots,n_r+1}$) and then α induces an isomorphism of $\mathscr{O}_P(V^*)$ with $\mathscr{O}_P(V)$.

□

Problem 4.27.*

Show that the pole set of a rational function on a variety in any multispace is an algebraic subset.

Proof.

(1) Similar to Problem 4.17. Let V be a variety in one multispace $\mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_r} \times \mathbf{A}^m$. Let z be a rational function on V.

(2) Let
$$J_z = \{g \in k[\mathbf{x}_1, \ldots, \mathbf{x}_r, \mathbf{y}] : \overline{g}z \in \Gamma(V)\},$$
where $\mathbf{x}_i = [x_{i,1} : \ldots : x_{i,n_i+1}] \in \mathbf{P}^{n_i}$ for $1 \leq i \leq r$, $\mathbf{y} = (y_1, \ldots, y_m) \in \mathbf{A}^m$, and $\overline{g}$ is the residue of g in the multi-homogeneous coordinate ring $\Gamma(V)$.

(3) J_z is an ideal in $k[\mathbf{x}_1, \ldots, \mathbf{x}_r, \mathbf{y}]$ containing the multi-homogeneous ideal $I(V)$, and the points of $V(J_z)$ are exactly those points where z is not defined if J_z is multi-homogeneous.

(4) *Show that J_z is multi-homogeneous by the multi-homogeneous property of $I(V)$.* Induction on r and then apply the proof of Problem 4.17.

□

Problem 4.28.* (Segre embedding)

*For simplicity of notation, in this problem we let $x_0, \ldots, x_n$ be coordinates for $\mathbf{P}^n$, $y_0, \ldots, y_m$ coordinates for $\mathbf{P}^m$, and $t_{00}, t_{01}, \ldots, t_{0m}, t_{10}, \ldots, t_{nm}$ coordinates $\mathbf{P}^N$, where $N = (n+1)(m+1) - 1 = n + m + nm$. Define $S : \mathbf{P}^n \times \mathbf{P}^m \to \mathbf{P}^N$ by the formula: $S([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]) = [x_0y_0 : x_0y_1 : \ldots : x_ny_m]$. S is called the **Segre embedding** of $\mathbf{P}^n \times \mathbf{P}^m$ in $\mathbf{P}^{n+m+nm}$.*

(a) *Show that S is a well-defined, one-to-one mapping.*

(b) *Show that if W is an algebraic subset of $\mathbf{P}^N$, then $S^{-1}(W)$ is an algebraic subset of $\mathbf{P}^n \times \mathbf{P}^m$.*

(c) *Let $V = V(\{t_{ij}t_{k\ell} - t_{i\ell}t_{kj} : i, k = 0, \ldots, n; j, \ell = 0, \ldots, m\}) \subseteq \mathbf{P}^N$. Show that $S(\mathbf{P}^n \times \mathbf{P}^m) = V$. In fact, $S(U_i \times U_j) = V \cap U_{ij}$, where $U_{ij} = \{[t] : t_{ij} \neq 0\}$.*

(d) *Show that V is a variety.*

Proof of (a).

(1) *Show that S is well-defined.* Given any non-zero $\lambda, \mu \in k$.
$$\begin{aligned}
&S([\lambda x_0 : \ldots : \lambda x_n], [\mu y_0 : \ldots : \mu y_m]) \\
&= [(\lambda x_0)(\mu y_0) : (\lambda x_0)(\mu y_1) : \ldots : (\lambda x_n)(\mu y_m)] \\
&= [(\lambda\mu)x_0y_0 : (\lambda\mu)x_0y_1 : \ldots : (\lambda\mu)x_ny_m] \\
&= [x_0y_0 : x_0y_1 : \ldots : x_ny_m] \qquad (\lambda\mu \neq 0) \\
&= S([x_0 : \ldots : x_n], [y_0 : \ldots : y_m]).
\end{aligned}$$
So S is independent of the choices of $[x_0 : \ldots : x_n]$ and $[y_0 : \ldots : y_m]$. Since there is an index i (resp. j) such that $x_i \neq 0$ (resp. $y_j \neq 0$), $x_iy_j \neq 0$ and thus $\mathrm{im}(S) \subseteq \mathbf{P}^N$.

(2) *Show that S is one-to-one.* Given any $P = [x_0y_0 : x_0y_1 : \ldots : x_ny_m] \in \mathrm{im}(S) \subseteq \mathbf{P}^N$. Might assume that $x_0 = y_0 = 1$. So

$$\begin{aligned} P &= [x_0y_0 : x_0y_1 : \ldots : x_ny_m] \\ &= [1 : y_1 : y_2 : \ldots : y_m : x_1 : \ldots : x_2 : \ldots : x_n : \ldots x_ny_m]. \end{aligned}$$

By the expression of P, $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ are uniquely determined. Hence $[1 : x_1 : \ldots : x_n]$ and $[1 : y_1 : \ldots : y_m]$ are are uniquely determined by P. S is injective.

□

Proof of (b).

(1) $S^{-1}(W) = \{P \in \mathbf{P}^n \times \mathbf{P}^m : S(P) \in W\}$ is the inverse image of W under S. Write

$$W = V(h_1, \ldots, h_r)$$

where each $h_i \in k[t_{00}, \ldots, t_{nm}]$ is a form of degree d_i.

(2) Define the pullback $\widetilde{h_i} \in k[x_0, \ldots, x_n, y_0, \ldots, y_m]$ as

$$\widetilde{h_i}(x_0, \ldots, x_n, y_0, \ldots, y_m) = h_i(x_0y_0, \ldots, x_ny_m)$$

for each i. Clearly, $\widetilde{h_i}$ is a biform of bidegree (d_i, d_i).

(3) As

$$\begin{aligned} P \in S^{-1}(W) &\iff S(P) \in W \\ &\iff h_i(S(P)) = 0 \,\forall\, h_i \\ &\iff \widetilde{h_i}(P) = 0 \,\forall\, \widetilde{h_i} \\ &\iff P \in V(\widetilde{h_1}, \ldots, \widetilde{h_r}), \end{aligned}$$

$S^{-1}(W) = V(\widetilde{h_1}, \ldots, \widetilde{h_r})$ is algebraic.

□

Proof of (c).

(1) *Show that $\mathrm{im}(S) = V$ is algebraic.* $\mathrm{im}(S) \subseteq V$ by the construction of S. Conversely, take $P = [a_{ij}]_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}} \in V \subseteq \mathbf{P}^N$. So there is one entry $a_{k\ell} \neq 0$. So

$$\begin{aligned} P &= [a_{ij}]_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}} \\ &= [a_{ij}a_{k\ell}]_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}} \\ &= [a_{i\ell}a_{kj}]_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}} \\ &= S([a_{i\ell}]_{i=0,\ldots,n}, [a_{kj}]_{j=0,\ldots,m}) \end{aligned}$$

is in $\mathrm{im}(S)$.

(2) In the proof of (1), we have $S(U_i \times U_j) = V \cap U_{ij}$ where $U_{ij} = \{[t] : t_{ij} \neq 0\}$ (by setting $(k, \ell) \to (i, j)$).

□

Proof of (d).

(1) Write $V = V_1 \cup V_2$ where V_1, V_2 are algebraic sets in $\mathbf{P}^N$. By (b)(c),

$$\mathbf{P}^n \times \mathbf{P}^m = S^{-1}(V) = S^{-1}(V_1) \cup S^{-1}(V_2).$$

(2) Since $\mathbf{P}^n \times \mathbf{P}^m$ is irreducible (Problem 4.26), we might assume that $\mathbf{P}^n \times \mathbf{P}^m = S^{-1}(V_1)$. Note that $S(S^{-1}(W)) = W$ holds for any set $W \subseteq V$. Hence

$$V_1 = S(S^{-1}(V_1)) = S(\mathbf{P}^n \times \mathbf{P}^m) = V,$$

that is, V is irreducible.

□

Chapter 5: Projective Plane Curves

5.1. Definitions

Problem 5.1.*

Let f be a projective plane curve. Show that a point P is a multiple point of f if and only if $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$.

Proof.

(1) Let P be a point in f. Might assume $P \in U_3$. By dehomogenizing f with respect to z, $m_P(f) = m_P(f_*)$. Thus,

$$\begin{aligned} & m_P(f) = m_P(f_*) > 1 \\ \iff & f_*(P) = \frac{\partial f_*}{\partial x}(P) = \frac{\partial f_*}{\partial y}(P) = 0 \\ \iff & f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0. \qquad (f \text{ is a form}) \end{aligned}$$

(2) By Euler's Theorem in §1.1, $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$ implies that $\frac{\partial f}{\partial z}(P) = 0$.

□

Problem 5.2.

Show that the following curves are irreducible; find their multiple points, and the multiplicities and tangents at the multiple points.

(a) $xy^4 + yz^4 + xz^4$.

(b) $x^2y^3 + x^2z^3 + y^2z^3$.

(c) $y^2z - x(x - z)(x - \lambda z)$, $\lambda \in k$.

(d) $x^n + y^n + z^n$, $n > 0$.

Proof of (a).

(1) Let $f = xy^4 + yz^4 + xz^4$. It suffices to show that $f_* = x(y^4 + 1) + y$ is irreducible. View $f_* \in (k[y])[x]$ as a linear function in x. Since $y^4 + 1$ and y have no common factors in $k[x]$, f_* is irreducible in $(k[y])[x] = k[x, y]$.

(2) By solving the system of equations $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$, there is only one multiple point $[1:0:0]$ of f.

(3) Since $P = [1:0:0]$, we dehomogenize f w.r.t. x to get

$$m_P(f) = m_P(f_*) = m_{(0,0)}(yz^4 + y^4 + z^4) = 4.$$

P is an ordinary multiple point of 4 distinct tangents $y \pm (-1)^{\frac{1}{4}} z$, $y \pm (-1)^{\frac{3}{4}} z$.

□

Proof of (b).

(1) Let $f = x^2y^3 + x^2z^3 + y^2z^3$. It suffices to show that $f_* = x^2(y^3+1) + y^2$ is irreducible. View $f_* \in (k[y])[x]$ as a quadratic function in x. Note that $y^3 + 1$ and y^2 have no common factors in $k[x]$. We may write

$$f_*(x, y) = (a(y)x + b(y))(c(y)x + d(y))$$

if f_* were reducible. So

$$\begin{aligned} ac &= y^3 + 1 \\ ad + bc &= 0 \\ bd &= y^2. \end{aligned}$$

There is no solutions for $a, b, c, d \in k[y]$. Hence, f_* is irreducible in $(k[y])[x] = k[x, y]$.

(2) By solving the system of equations $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$, we have $P = [1:0:0], [0:1:0], [0:0:1]$.

(3) Suppose $P = [1:0:0]$. We dehomogenize f w.r.t. x to get

$$m_P(f) = m_P(f_*) = m_{(0,0)}(y^2z^3 + y^3 + z^3) = 3.$$

P is an ordinary multiple point of 3 distinct tangents $y + z$, $y + (-1)^{\frac{1}{3}} z$, $y - (-1)^{\frac{2}{3}} z$.

(4) Suppose $P = [0:1:0]$. We dehomogenize f w.r.t. y to get

$$m_P(f) = m_P(f_*) = m_{(0,0)}(x^2z^3 + z^3 + x^2) = 2.$$

x is the tangent to f at P of the multiplicity $= 2$.

(5) Suppose $P = [0:0:1]$. We dehomogenize f w.r.t. z to get

$$m_P(f) = m_P(f_*) = m_{(0,0)}(x^2y^3 + x^2 + y^2) = 2.$$

P is an ordinary multiple point of 2 distinct tangents $x \pm (-1)^{\frac{1}{2}} y$.

□

Proof of (c).

(1) Note that $y^2 - x(x-1)(x-\lambda)$ is irreducible (Problem 1.35). Hence, the homogenizing form $f = y^2z - x(x-z)(x-\lambda z)$ of $y^2 - x(x-1)(x-\lambda)$ w.r.t. z is also irreducible.

(2) By solving the system of equations $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$, we have

$$P = [0:0:1] \text{ if } \lambda = 0$$
$$P = [1:0:1] \text{ if } \lambda = 1$$

are all multiple points of f.

(3) Suppose $P = [0:0:1]$ with $\lambda = 0$. Then

$$m_P(f) = m_P(f_*) = m_{(0,0)}(y^2 - x^2(x-1)) = 2.$$

y is the tangent to f at P of the multiplicity $= 2$. (The projective closure of y is y.)

(4) Similarly, suppose $P = [1:0:1]$ with $\lambda = 1$. Then

$$\begin{aligned} m_P(f) &= m_P(f_*) \\ &= m_{(1,0)}(y^2 - x(x-1)^2) \\ &= m_{(0,0)}(y^2 - x^2(x+1)) \\ &= 2. \end{aligned}$$

y is the tangent to f at P of the multiplicity $= 2$.

□

Proof of (d).

(1) Let $f = x^n + y^n + z^n$. It suffices to show that $f_* = x^n + y^n + 1$ is irreducible. Write

$$f_* = x^n + (y^n + 1) \in (k[y])[x].$$

Note that $k[y]$ is a UFD and $y^n + 1$ is separable. Thus by the Eisenstein's criterion, f_* irreducible in $(k[y])[x] = k[x, y]$.

(2) By solving the system of equations $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$, there are no multiple points on f for $n \geq 1$.

□

Problem 5.3.

Find all points of intersection of the following pairs of curves, and the intersection numbers at these points:

(a) $y^2z - x(x-2z)(x+z)$ *and* $y^2 + x^2 - 2xz$.

(b) $(x^2+y^2)z + x^3 + y^3$ *and* $x^3 + y^3 - 2xyz$.

(c) $y^5 - x(y^2 - xz)^2$ *and* $y^4 + y^3z - x^2z^2$.

(d) $(x^2+y^2)^2 + 3x^2yz - y^3z$ *and* $(x^2+y^2)^3 - 4x^2y^2z^2$.

Proof of (a).

(1) Say $f = y^2z - x(x-2z)(x+z)$ and $g = y^2 + x^2 - 2xz$. By $f - zg = 0$, $x(x-2z)(x+2z) = 0$. So the intersection points in $\mathbf{P}^2$ are

$$\underbrace{[0:0:1]}_{x=0}, \underbrace{[2:0:1]}_{x-2z=0}, \underbrace{[-2, \pm\sqrt{-8}:1]}_{x+2z=0}.$$

(2) Suppose $P = [0:0:1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned} I(P, f \cap g) &= I((0,0), f_* \cap g_*) \\ &= I((0,0), (-x(x-2)(x+1) + y^2) \cap (y^2 + x^2 - 2x)) \\ &= 2 \end{aligned}$$

(since they have no common tangents).

(3) Suppose $P = [2:0:1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned} I(P, f \cap g) &= I(P, f_* \cap g_*) \\ &= I(P, (-x(x-2)(x+1) + y^2) \cap (y^2 + x^2 - 2x)) \\ &= I((0,0), (-x(x+2)(x+3) + y^2) \cap (y^2 + x^2 + 2x)) \\ &= 2. \end{aligned}$$

(4) Suppose $P = [-2, \pm\sqrt{-8}:1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned} I(P, f \cap g) &= I(P, f_* \cap g_*) \\ &= I(P, (-x(x-2)(x+1) + y^2) \cap (y^2 + x^2 - 2x)) \\ &= I((0,0), (-x^3 + 7x^2 + y^2 - 14x \pm 2\sqrt{-8}y) \cap \\ &\qquad (y^2 + x^2 - 6x \pm 2\sqrt{-8}y)) \\ &= 1. \end{aligned}$$

(Or by Bézout's theorem, each intersection point has the intersection number 1 in this case.)

□

Proof of (b).

(1) Say $f = (x^2+y^2)z + x^3 + y^3$ and $g = x^3 + y^3 - 2xyz$. By $f - g = 0$, $(x+y)^2 z = 0$. So the intersection points in $\mathbf{P}^2$ are

$$\underbrace{[0:0:1]}_{x+y=0}, \underbrace{[1:-1:0], [1:\omega:0], [1:1-\omega:0]}_{z=0}.$$

where $\omega = (-1)^{\frac{1}{3}} \in k$.

(2) Suppose $P = [0:0:1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned} I(P, f \cap g) &= I((0,0), f_* \cap g_*) \\ &= I((0,0), (x^3+y^3+x^2+y^2) \cap (x^3+y^3-2xy)) \\ &= 4. \end{aligned}$$

(3) Suppose $P = [1:-1:0]$. We dehomogenize f and g w.r.t. x to get

$$\begin{aligned} I(P, f \cap g) &= I(P, f_* \cap g_*) \\ &= I(P, (f_* - g_*) \cap g_*) \\ &= I(P, (y+1)^2 z \cap (1+y^3-2yz)) \\ &= I((0,0), y^2 z \cap (y^3 - 3y^2 - 2yz + 3y + 2z)) \\ &= 3. \end{aligned}$$

(4) Suppose $P = [1:\omega:0]$. Similar to (3), we dehomogenize f and g w.r.t. x to get

$$\begin{aligned} I(P, f \cap g) &= I(P, (y+1)^2 z \cap (1+y^3-2yz)) \\ &= I((0,0), (y^2 z + 2(1+\omega)yz + (1+\omega)^2 z) \cap \\ &\qquad (y^3 + 3\omega y^2 - 2yz + 3\omega^2 y - 2\omega z)) \\ &= I((0,0), (y^2 z + 2(1+\omega)yz + 3\omega z) \cap \\ &\qquad (y^3 + 3\omega y^2 - 2yz + 3\omega^2 y - 2\omega z)) \\ &= 1. \end{aligned}$$

(5) Suppose $P = [1:1-\omega:0]$. We dehomogenize f and g w.r.t. x to get

$$\begin{aligned} & I(P, f \cap g) \\ &= I(P, (y+1)^2 z \cap (1+y^3-2yz)) \\ &= I((0,0), (y^2 z + 2(2-\omega)yz + (2-\omega)^2 z) \cap \\ &\qquad (y^3 + 3(1-\omega)y^2 - 2yz + 3(1-\omega)^2 y - 2(1-\omega)z)) \\ &= I((0,0), (y^2 z + 2(2-\omega)yz + 3(1-\omega)z) \cap \\ &\qquad (y^3 + 3(1-\omega)y^2 - 2yz - 3\omega y - 2(1-\omega)z)) \\ &= 1. \end{aligned}$$

□

Proof of (c).

(1) Say $f = y^5 - x(y^2 - xz)^2$ and $g = y^4 + y^3 z - x^2 z^2$. If $y = 0$, the intersection points in $\mathbf{P}^2 - U_2$ are

$$[0 : 0 : 1], [1 : 0 : 0].$$

If $y \neq 0$, the intersection points in $2_3 \cong \mathbf{A}^2$ are the solutions of $f_* = 1 - x(1 - xz)^2$ and $g_* = 1 + z - x^2 z^2$:

$$\left[\frac{1}{2} : 1 : 2 \pm 2\sqrt{2}\right].$$

Note that there are only 4 different intersection points (Bézout's theorem).

(2) Suppose $P = [0 : 0 : 1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned}
& I(P, f \cap g) \\
&= I((0,0), f_* \cap g_*) \\
&= I((0,0), (y^5 - x(y^2 - x)^2) \cap (y^4 + y^3 - x^2)) \\
&= I((0,0), ((y^5 - x(y^2 - x)^2) - x(y^4 + y^3 - x^2)) \cap (y^4 + y^3 - x^2)) \\
&= I((0,0), y^2(y^2 - x)(2x - y) \cap (y^4 + y^3 - x^2)) \\
&= I((0,0), y^2 \cap (y^4 + y^3 - x^2)) \\
&\quad + I((0,0), (y^2 - x) \cap (y^4 + y^3 - x^2)) \\
&\quad + I((0,0), (2x - y) \cap (y^4 + y^3 - x^2)) \\
&= 4 + I((0,0), (y^2 - x) \cap (y^4 + y^3 - x^2)) + 2 \\
&= 9.
\end{aligned}$$

Here

$$\begin{aligned}
& I((0,0), (y^2 - x) \cap (y^4 + y^3 - x^2)) \\
&= I((0,0), (y^2 - x) \cap ((y^4 + y^3 - x^2) - x(y^2 - x))) \\
&= I((0,0), (y^2 - x) \cap (y^4 - xy^2 + y^3)) \\
&= 3.
\end{aligned}$$

(3) Suppose $P = [1:0:0]$. We dehomogenize f and g w.r.t. x to get

$$\begin{aligned}
&I(P, f \cap g)\\
&= I((0,0), f_* \cap g_*)\\
&= I((0,0), (y^5 - (y^2 - z)^2) \cap (y^4 + y^3 z - z^2))\\
&= I((0,0), ((y^5 - (y^2 - z)^2) - (y^4 + y^3 z - z^2)) \cap (y^4 + y^3 z - z^2))\\
&= I((0,0), y^2(y^2 - z)(y - 2) \cap (y^4 + y^3 z - z^2))\\
&= I((0,0), y^2 \cap (y^4 + y^3 z - z^2))\\
&\quad + I((0,0), (y^2 - z) \cap (y^4 + y^3 z - z^2))\\
&\quad + I((0,0), (y - 2) \cap (y^4 + y^3 z - z^2))\\
&= 4 + I((0,0), (y^2 - z) \cap (y^4 + y^3 z - z^2)) + 0\\
&= 4 + 5 + 0\\
&= 9.
\end{aligned}$$

Here

$$\begin{aligned}
&I((0,0), (y^2 - z) \cap (y^4 + y^3 z - z^2))\\
&= I((0,0), (y^2 - z) \cap ((y^4 + y^3 z - z^2) - z(y^2 - z)))\\
&= I((0,0), (y^2 - z) \cap y^2(y^2 + yz - z))\\
&= I((0,0), (y^2 - z) \cap y^2) + I((0,0), (y^2 - z) \cap (y^2 + yz - z))\\
&= 2 + I((0,0), (y^2 - z) \cap yz)\\
&= 2 + I((0,0), (y^2 - z) \cap y) + I((0,0), (y^2 - z) \cap z)\\
&= 2 + 1 + I((0,0), y^2 \cap z)\\
&= 2 + 1 + 2\\
&= 5.
\end{aligned}$$

(4) Suppose $P = \left[\frac{1}{2} : 1 : 2 + 2\sqrt{2}\right]$. We dehomogenize f and g w.r.t. y to get

$$\begin{aligned}
&I(P, f \cap g)\\
&= I(P, f_* \cap g_*)\\
&= I(P, (1 - x(1 - xz)^2) \cap (1 + z - x^2 z^2))\\
&= I\left((0,0), \left(-(6 + 2\sqrt{2})x - \sqrt{2}/2 \cdot z + \text{higher terms}\right) \bigcap \right.\\
&\qquad\qquad \left. (-(12 + 8\sqrt{2})x - \sqrt{2}z + \text{higher terms})\right)\\
&= 1.
\end{aligned}$$

Similarly, $I(P, f \cap g) = 1$ as $P = \left[\frac{1}{2} : 1 : 2 - 2\sqrt{2}\right]$.

□

Proof of (d).

(1) Say $f = (x^2+y^2)^2 + 3x^2yz - y^3z$ and $g = (x^2+y^2)^3 - 4x^2y^2z^2$. If $z = 0$, the intersection points in $\mathbf{P}^2 - U_3$ are

$$[1 : \pm\sqrt{-1} : 0].$$

If $z \neq 0$, the intersection points in $U_3 \cong \mathbf{A}^2$ are the solutions of $f_* = (x^2+y^2)^2 + 3x^2y - y^3$ and $g_* = (x^2+y^2)^3 - 4x^2y^2$:

$$[0:0:1], \left[\pm\frac{\sqrt{5+2\sqrt{5}}}{4} : \frac{-\sqrt{5}}{4} : 1\right], \left[\pm\frac{\sqrt{5-2\sqrt{5}}}{4} : \frac{\sqrt{5}}{4} : 1\right].$$

(To find these solutions, we might solve $f_*(r\cos\theta, r\sin\theta) = g_*(r\cos\theta, r\sin\theta) = 0$ over $k = \mathbb{C}$. As $r = 0$, nothing to do. As $r > 0$, we get $\theta = \frac{m\pi}{5}$ for all integers m.) Note that there are only 7 different intersection points (Bézout's theorem).

(2) Suppose $P = [1 : \sqrt{-1} : 0]$. We dehomogenize f and g w.r.t. x to get

$$\begin{aligned}
&I(P, f \cap g)\\
=&I(P, f_* \cap g_*)\\
=&I(P, ((1+y^2)^2 + 3yz - y^3z) \cap ((1+y^2)^3 - 4y^2z^2))\\
=&I(P, ((1+y^2)^2 + 3yz - y^3z) \cap (yz(y^4 - 2y^2 - 4yz - 3))\\
=&I(P, ((1+y^2)^2 + 3yz - y^3z) \cap y)\\
&+ I(P, ((1+y^2)^2 + 3yz - y^3z) \cap z)\\
&+ I(P, ((1+y^2)^2 + 3yz - y^3z) \cap (y^4 - 2y^2 - 4yz - 3))\\
=&2I(P, (1+y^2) \cap z)\\
&+ I(P, ((1+y^2)^2 + 3yz - y^3z) \cap (y^4 - 2y^2 - 4yz - 3))\\
=&3.
\end{aligned}$$

Here

$$I(P, (1+y^2) \cap z) = I((0,0), (y^2 + 2\sqrt{-1}y) \cap z) = 1$$

and

$$\begin{aligned}
&I(P, ((1+y^2)^2 + 3yz - y^3z) \cap (y^4 - 2y^2 - 4yz - 3))\\
=&I((0,0), (y^4 - y^3z + 4\sqrt{-1}y^3 - 3\sqrt{-1}y^2z - 4y^2 + 6yz + 4\sqrt{-1}z) \cap\\
&\qquad (y^4 + 4\sqrt{-1}y^3 - 8y^2 - 4yz - 8\sqrt{-1}y - 4\sqrt{-1}z))\\
=&1.
\end{aligned}$$

Similarly, $I(P, f \cap g) = 3$ if $P = [1 : -\sqrt{-1} : 0]$.

(3) Suppose $P = [0:0:1]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned}
I(P, f \cap g) &= I((0,0), f_* \cap g_*)\\
&= I((0,0), ((x^2+y^2)^2 + 3x^2y - y^3) \cap ((x^2+y^2)^3 - 4x^2y^2))\\
&= 14
\end{aligned}$$

(Example in §3.3).

(4) Suppose $P = \left[\frac{\sqrt{5+2\sqrt{5}}}{4} : \frac{-\sqrt{5}}{4} : 1\right]$. We dehomogenize f and g w.r.t. z to get

$$\begin{aligned}
&I(P, f \cap g) \\
&= I(P, f_* \cap g_*) \\
&= I(P, ((x^2+y^2)^2 + 3x^2y - y^3) \cap ((x^2+y^2)^3 - 4x^2y^2)) \\
&= I(P, ((x^2+y^2)^2 + 3x^2y - y^3) \cap y(-3x^4 - 2x^2y^2 + y^4 - 4x^2y)) \\
&= 4I(P, x \cap y) \\
&\quad + I(P, ((x^2+y^2)^2 + 3x^2y - y^3) \cap (-3x^4 - 2x^2y^2 + y^4 - 4x^2y)) \\
&= 1.
\end{aligned}$$

Here

$$I(P, x \cap y) = I\left((0,0), \left(x + \frac{\sqrt{5+2\sqrt{5}}}{4}\right) \bigcap \left(y + \frac{-\sqrt{5}}{4}\right)\right) = 0$$

and

$$\begin{aligned}
&I(P, ((x^2+y^2)^2 + 3x^2y - y^3) \cap (-3x^4 - 2x^2y^2 + y^4 - 4x^2y)) \\
&= I\left((0,0), \left(\frac{(5+2\sqrt{5})\sqrt{5+2\sqrt{5}}}{8}x - \frac{5+2\sqrt{5}}{8}y + \text{higher terms}\right) \bigcap \right. \\
&\qquad\qquad \left. \left(\frac{(-10+\sqrt{5})\sqrt{5+2\sqrt{5}}}{8}x - \frac{5+4\sqrt{5}}{8}y + \text{higher terms}\right)\right) \\
&= 1.
\end{aligned}$$

Similarly, $I(P, f \cap g) = 1$ for rest three cases.

□

Problem 5.4.*

Let P be a simple point on f. Show that the tangent line to f at P has the equation $\frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z = 0$.

Proof.

(1) Similar to Problem 5.1. Might assume $P = [x_0 : y_0 : 1] \in U_3$. By

dehomogenizing f with respect to z, the tangent line to f_* at P is

$$\begin{aligned} L : 0 &= \frac{\partial f}{\partial x}(P)(x - x_0) + \frac{\partial f}{\partial x}(P)(y - y_0) \\ &= \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial x}(P)y - \left(\frac{\partial f}{\partial x}(P)x_0 + \frac{\partial f}{\partial x}(P)y_0\right) \\ &= \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial x}(P)y + \frac{\partial f}{\partial z}(P). \end{aligned}$$

(The last equation is due to Euler's Theorem in §1.1.)

(2) Hence, the projective closure of L, say

$$L^* : 0 = \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial x}(P)y + \frac{\partial f}{\partial z}(P)z,$$

is the tangent line to f at P.

□

Problem 5.5.*

Let $P = [0 : 1 : 0]$, f a curve of degree n, $f = \sum f_i(x, z)y^{n-i}$, f_i a form of degree i. Show that $m_P(f)$ is the smallest m such that $f_m \neq 0$, and the factors of f_m determine the tangents to f at P.

Proof.

(1) By dehomogenizing f with respect to y, we have

$$m_P(f) = m_P(f_*) = m_{(0,0)}\left(\sum f_i(x, z)\right) = m$$

where m is the smallest integer such that $f_m \neq 0$.

(2) The factors of f_m determine the tangents to f_* at P. Note that each factor of f_m is a form. Therefore, these factors of f_m also determine the tangents to f at P.

□

Problem 5.6.*

For any f, $P \in f$, show that $m_P\left(\frac{\partial f}{\partial x}\right) \geq m_P(f) - 1$.

Proof.

(1) If $P = [1 : 0 : 0]$, by dehomogenizing f with respect to x we get

$$m_P\left(\frac{\partial f}{\partial x}\right) = m_P\left(\frac{\partial f_*}{\partial x}\right) = m_P(0) = \infty.$$

The result is established.

(2) Might assume $P \in U_3$. By dehomogenizing f with respect to z, it suffices to show that

$$m_P\left(\frac{\partial f_*}{\partial x}\right) \geq m_P(f_*) - 1.$$

(3) Write $m = m_P(f_*)$ and $f_* = g_m + g_{m+1} + \cdots \in k[x, y]$ where $g_i \neq 0$ is a form of degree m. Note that

$$\frac{\partial f_*}{\partial x} = \frac{\partial g_m}{\partial x} + \frac{\partial g_{m+1}}{\partial x} + \cdots.$$

So that $m_P\left(\frac{\partial f_*}{\partial x}\right) \geq m - 1 = m_P(f_*) - 1$.

□

Problem 5.7.*

Show that two plane curves with no common components intersect in a finite number of points.

Proof.

(1) Similar to Proposition 2 in §1.6. Let f and g be forms in $k[x, y, z]$ with no common components. In particular, $f \neq 0$ and $g \neq 0$.

(2) *Show that the conclusion is true for a line g.* Similar to Problem 1.12. Let $\alpha : \mathbf{P}^1 \to \mathbf{P}^2$ be the map

$$\alpha([\lambda : \mu]) = [\lambda a_1 + \mu b_1 : \lambda a_2 + \mu b_2 : \lambda a_3 + \mu b_3]$$

and $g = \mathrm{im}(\alpha)$ be a line. Note that the points of $V(f, g)$ correspond to the zero of

$$\widetilde{f}(\lambda, \mu) = f(\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2, \lambda a_3 + \mu b_3) = 0 \text{ in } \mathbf{P}^1.$$

$\widetilde{f}$ is a form in $k[\lambda, \mu]$ of degree $m := \deg(f)$ since f and g have no common components. Hence, $\widetilde{f}$ has exactly m zeros in $\mathbf{P}^1$ (with multiplicity). $V(f, g)$ has exactly m zeros (with multiplicity).

Note. It is the same as Problem 5.12(b).

(3) *Show that the conclusion is true for any f, g.* Note that f and g have no common factors in $k(x,y)[z]$. Since $k(x,y)[z]$ is a PID, $(f,g) = (1) \in k(x,y)[z]$. So $\alpha f + \beta g = 1$ for some $\alpha, \beta \in k(x,y)[z]$. Clearing denominators from α, β gives us

$$af + bg = d$$

where d is a non-zero polynomial in $k[x,y]$, $a = d\alpha \in k[x,y,z]$ and $b = d\beta \in k[x,y,z]$. Taking suitable homogeneous parts of a, b and d, we might assume a, b and d are all homogeneous.

(4) By Corollary to Proposition 5 in §2.6, d is a product of linear forms, say $d = L_1 \cdots L_r$. A common zero of f and g is also a zero of d, and therefore it is a zero of L_j for some j. So it suffices to show that $V = (f,g) = V(f,g,L_j)$ is finite for each j.

(5) (Reductio ad absurdum) If not, there were one j such that both $V(f,L_j)$ and $V(g,L_j)$ were infinite. By (2), $L_j \mid f$ and $L_j \mid g$. f and g have one common factor, which is absurd.

□

Problem 5.8.*

Let f be an irreducible curve.

(a) *Show that $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, or $\frac{\partial f}{\partial z} \neq 0$.*

(b) *Show that f has only a finite number of multiple points.*

Proof of (a). If $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, and $\frac{\partial f}{\partial z}$ are all zero, f is a constant, which is not a projective plane curve. □

Proof of (b).

(1) Let

$$V = V\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}\right)$$

be the set of the multiple points of f (Problem 5.1). Moreover, V is an algebraic set.

(2) Suppose $\frac{\partial f}{\partial x} \neq 0$ (since not all $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$ and $\frac{\partial f}{\partial z}$ are zero). It is nothing to do if $\frac{\partial f}{\partial x}$ is a nonzero constant. Suppose $\deg\left(\frac{\partial f}{\partial x}\right) \geq 1$. Since f is irreducible and $\deg\left(\frac{\partial f}{\partial x}\right) = \deg f - 1$, f and $\frac{\partial f}{\partial x}$ have no common factors. By Problem 5.7, $V\left(f, \frac{\partial f}{\partial x}\right)$ is a finite set. Hence, V is finite as a subset of a finite set $V\left(f, \frac{\partial f}{\partial x}\right)$.

□

Problem 5.9. (Conic)

(a) *Let f be an irreducible conic, $P = [0 : 1 : 0]$ a simple point on f, and $z = 0$ the tangent line to f at P. Show that $f = ayz - bx^2 - cxz - dz^2$, $a, b \neq 0$. Find a projective change of coordinates t so that $f^t = yz - x^2 - c'xz - d'z^2$. Find t' so that $(f^t)^{t'} = yz - x^2$. ($t' = (x, y + c'x + d'z, z)$.)*

(b) *Show that, up to projective equivalence, there is only one irreducible conic: $yz = x^2$. Any irreducible conic is nonsingular.*

Proof of (a).

(1) Given any conic

$$f = ayz - bx^2 - cxz - dz^2 + \alpha y^2 + \beta xy.$$

(2) $\alpha = 0$ since $P \in f$.

(3) *Show that $a \neq 0$ and $\beta = 0$.* We dehomogenize f w.r.t. y to get $f_* = -bx^2 - cxz - dz^2 + az + \beta x$. Thus, the tangent line of f_* at $(0, 0)$ is $az + \beta x$. So $a \neq 0$ and $\beta = 0$ since z is the tangent line to f at P.

(4) *Show that $b \neq 0$.* If $b = 0$, $f = ayz - cxz - dz^2 = z(ay - cx - dz)$ is reducible, which is absurd.

(5) Write

$$\begin{aligned} f &= ayz - bx^2 - cxz - dz^2 \\ &= (\sqrt{a}y)(\sqrt{a}z) - (\sqrt{b}x)^2 - \frac{c}{\sqrt{ab}}(\sqrt{b}x)(\sqrt{a}z) - \frac{d}{a}(\sqrt{a}z)^2. \end{aligned}$$

Apply a projective change of coordinates $t = \left(\frac{x}{\sqrt{b}}, \frac{y}{\sqrt{a}}, \frac{z}{\sqrt{a}}\right)$ to f:

$$f^t = yz - x^2 - c'xz - d'z^2,$$

where $c' = \frac{c}{\sqrt{ab}}$ and $d' = \frac{d}{a}$.

(6) Write

$$f^t = yz - x^2 - c'xz - d'z^2 = (y - c'x - d'z)z - x^2.$$

Apply a projective change of coordinates $t' = (x, y + c'x + d'z, z)$ to f^t:

$$(f^t)^{t'} = yz - x^2.$$

□

Proof of (b).

(1) Take one simple point $P_1 \in f$ and the corresponding tangent line L. (It is possible since Problem 5.8 and $|f| = \infty$.) Take $P_2 \in L - f$ and $P_3 \in f - L$. (It is possible since Problem 5.7 or 5.12 and both $|f|$ and $|L|$ are ∞.)

(2) Let $Q_1 = [0:1:0]$, $Q_2 = [1:0:0]$, $Q_3 = [0:0:1]$. Since P_1, P_2, P_3 (resp. Q_1, Q_2, Q_3) are not lying on a common line, there is a unique projective change of coordinates t such that $t(P_i) = Q_i$ $(i = 1, 2, 3)$ by Problem 4.14.

(3) Hence, f is projectively equivalent to an irreducible conic g such that $P = [0:1:0]$ is a simple point on g and $z = 0$ is the tangent line to g at P. By (a),
$$f \sim g \sim (yz - x^2).$$

(4) Nonsingularity is preserved under projectively equivalence. Might assume that $f = yz - x^2$. $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$ implies that $P = [0:0:0]$, which is not in $\mathbf{P}^2$. Hence f is nonsingular (Problem 5.1).

□

Problem 5.10. (Cubic with a cusp)

Let f be an irreducible cubic, $P = [0:0:1]$ a cusp on f, $y = 0$ the tangent line to f at P. Show that $f = ay^2z - bx^3 - cx^2y - dxy^2 - ey^3$. Find projective changes of coordinates

(i) *to make $a = b = 1$;*

(ii) *to make $c = 0$ (change x to $x - \frac{c}{3}y$);*

(iii) *to make $d = e = 0$ (z to $z + dx + ey$).*

Up to projective equivalence, there is only one irreducible cubic with a cusp: $y^2z = x^3$. It has no other singularities.

Proof.

(1) Given any cubic
$$\begin{aligned} f = {} & ay^2z - bx^3 - cx^2y - dxy^2 - ey^3 \\ & + \alpha_1 z^3 + \alpha_2 x^2 z + \alpha_3 z^2 x + \alpha_4 z^2 y + \alpha_5 xyz. \end{aligned}$$

(2) $\alpha_1 = 0$ since $P \in f$.

(3) *Show that* $b \neq 0$ *and* $\alpha_2 = \alpha_3 = 0$. Since $P = [0:0:1]$ is a cusp on f and $y = 0$ is the tangent line to f at P, $I(f \cap y) = 3$. So

$$\begin{aligned} 3 &= I(P, f \cap y) \\ &= I(P, (-bx^3 + \alpha_2 x^2 z + \alpha_3 z^2 x) \cap y) \\ &= I(P, (-bx^3 + \alpha_2 x^2 + \alpha_3 x) \cap y) \qquad \text{(Dehomogenize w.r.t. } z\text{)} \end{aligned}$$

if and only if $b \neq 0$ and $\alpha_2 = \alpha_3 = 0$.

(4) *Show that* $a \neq 0$ *and* $\alpha_4 = \alpha_5 = 0$. We dehomogenize f w.r.t. z to get

$$f_* = -bx^3 - cx^2 y - dxy^2 - ey^3 + ay^2 + \alpha_5 xy + \alpha_4 y.$$

Since $(0,0)$ is a double point, $\alpha_4 = 0$. Since f_* has only one tangent y on $(0,0)$,

$$ay^2 + \alpha_5 xy = y(ay + \alpha_5 x)$$

implies that $a \neq 0$ and $\alpha_5 = 0$.

(5) Therefore, $f = ay^2 z - bx^3 - cx^2 y - dxy^2 - ey^3$ with $a \neq 0$ and $b \neq 0$. Similar to Problem 5.9,

(i) Write

$$\begin{aligned} f &= ay^2 z - bx^3 - cx^2 y - dxy^2 - ey^3 \\ &= (\sqrt[3]{a}y)^2(\sqrt[3]{a}z) - (\sqrt[3]{b}x)^3 - \frac{c}{\sqrt[3]{ab^2}}(\sqrt[3]{b}x)^2(\sqrt[3]{a}y) \\ &\quad - \frac{d}{\sqrt[3]{a^2 b}}(\sqrt[3]{b}x)(\sqrt[3]{a}y)^2 - \frac{e}{a}(\sqrt[3]{a}y)^3. \end{aligned}$$

Apply a projective change of coordinates $t_1 = \left(\frac{x}{\sqrt[3]{b}}, \frac{y}{\sqrt[3]{a}}, \frac{z}{\sqrt[3]{a}}\right)$ to f:

$$f^{t_1} = y^2 z - x^3 - c_1 x^2 y - d_1 xy^2 - e_1 y^3,$$

where $c_1 = \frac{c}{\sqrt[3]{ab^2}}$ and $d_1 = \frac{d}{\sqrt[3]{a^2 b}}$ and $e_1 = \frac{e}{a}$.

(ii) Write

$$\begin{aligned} f^{t_1} &= y^2 z - x^3 - c_1 x^2 y - d_1 xy^2 - e_1 y^3 \\ &= y^2 z - \left(x + \frac{c_1}{3}y\right)^3 - \left(d_1 - \frac{c_1^2}{3}\right)\left(x + \frac{c_1}{3}y\right) y^2 \\ &\quad - \left(e_1 - \frac{c_1 d_1}{3} + \frac{2c_1^3}{27}\right) y^3. \end{aligned}$$

Apply a projective change of coordinates $t_2 = \left(x - \frac{c_1}{3}y, y, z\right)$ to f^{t_1}:

$$(f^{t_1})^{t_2} = y^2 z - x^3 - d_2 xy^2 - e_2 y^3$$

where $d_2 = d_1 - \frac{c_1^2}{3}$ and $e_2 = e_1 - \frac{c_1 d_1}{3} + \frac{2c_1^3}{27}$. (Compare to Cardano's formula.)

(iii) Write

$$\begin{aligned}(f^{t_1})^{t_2} &= y^2z - x^3 - d_2xy^2 - e_2y^3\\ &= y^2(z - d_2x - e_2y) - x^3.\end{aligned}$$

Apply a projective change of coordinates $t_3 = (x, y, z + d_2x + e_2y)$ to $(f^{t_1})^{t_2}$:

$$((f^{t_1})^{t_2})^{t_3} = y^2z - x^3.$$

(6) Given any irreducible cubic f with a cusp. Apply the proof of Problem 5.9(b), f is projectively equivalent to an irreducible cubic g such that $P = [0 : 0 : 1]$ is a cusp on g and $y = 0$ is the tangent line to g at P. By (5),

$$f \sim g \sim (y^2z - x^3).$$

Similar to Problem 5.9(b), $y^2z - x^3$ has no other singularities except one point $P = [0 : 0 : 1]$.

□

Problem 5.11. (Cubic with a node)

Up to projective equivalence, there is only one irreducible cubic with a node: $xyz = x^3 + y^3$. It has no other singularities.

Proof.

(1) *Let f be an irreducible cubic, $P = [0 : 0 : 1]$ a node on f, $x = 0$, $y = 0$ the tangent lines to f at P. Show that $f = ax^3 + by^3 - cxyz - dx^2y - exy^2$, $a \neq 0$, $b \neq 0$, $c \neq 0$.*

(a) Given any cubic

$$\begin{aligned}f = &ax^3 + by^3 - cxyz - dx^2y - exy^2\\ &+ \alpha_1z^3 + \alpha_2x^2z + \alpha_3y^2z + \alpha_4z^2x + \alpha_5z^2y.\end{aligned}$$

(b) $\alpha_1 = 0$ since $P \in f$.

(c) We dehomogenize f w.r.t. z to get

$$f_* = ax^3 + by^3 - cxy - dx^2y - exy^2 + \alpha_2x^2 + \alpha_3y^2 + \alpha_4x + \alpha_5y.$$

Since $(0, 0)$ is a double point, $\alpha_4 = \alpha_5 = 0$. Since f_* have only two tangents x, y on $(0, 0)$, $-cxy + \alpha_2x^2 + \alpha_3y^2$ implies that $c \neq 0$ and $\alpha_2 = \alpha_3 = 0$.

(d) Now $f = ax^3 + by^3 - cxyz - dx^2y - exy^2$ with $c \neq 0$. If $a = 0$ or $b = 0$, f is reducible, which is absurd. So $a \neq 0$ and $b \neq 0$.

(2) Hence,

$$f \sim (x^3 + y^3 - xyz - dx^2y - exy^2) \sim (x^3 + y^3 - xyz)$$

by $(x, y, z) \mapsto \left(\frac{1}{\sqrt[3]{a}}x, \frac{1}{\sqrt[3]{b}}y, \frac{\sqrt[3]{ab}}{c}z\right)$ and $(x, y, z) \mapsto (x, y, z - dx - ey)$.

(3) Given any irreducible cubic f with a node. Apply the proof of Problem 5.9(b), f is projectively equivalent to an irreducible cubic g such that $P = [0 : 0 : 1]$ is a node on g and x, y are the tangent lines to g at P. By (2),

$$f \sim g \sim (x^3 + y^3 - xyz).$$

Similar to Problem 5.9(b), $x^3 + y^3 - xyz$ has no other singularities except one point $P = [0 : 0 : 1]$.

□

Problem 5.12.*

(a) *Assume $P = [0 : 1 : 0] \notin f$, f a curve of degree n. Show that*

$$\sum_P I(P, f \cap x) = n.$$

(b) *Show that if f is a curve of degree n, L a line not contained in f, then*

$$\sum_P I(P, f \cap L) = n.$$

Proof of (a).

(1) Similar to Problem 5.7. The intersection points of f and x are the solutions of

$$f(0, y, z) = 0.$$

Write

$$f(0, y, z) = cy^n + \cdots$$

as a form in $k[y, z]$ of degree n.

(2) Note that $c \neq 0$ since $P = [0 : 1 : 0] \notin f$. By Corollary to Proposition 5 in §2.6,

$$f(0, y, z) = c\prod_i (y - \alpha_i z)^{r_i}$$

where $\alpha_i \in k$ and $\sum r_i = n$. So all intersection points are $P_i = [0 : \alpha_i : 1]$ with multiplicity r_i.

(3) Hence,

$$\begin{aligned}
&\sum_P I(P, f \cap x) \\
&= \sum_i I(P_i, f \cap x) \\
&= \sum_i I(P_i, f(0, y, z) \cap x) && \text{(Property (7) in §3.3)} \\
&= \sum_i \sum_j r_j I(P_i, (y - \alpha_j z) \cap x) && \text{(Property (6) in §3.3)} \\
&= \sum_i \sum_j r_j I((0, \alpha_i), (y - \alpha_j) \cap x) && \text{(Dehomogenize w.r.t. } z\text{)} \\
&= \sum_i \sum_j r_j I((0, 0), (y + \alpha_i - \alpha_j) \cap x) \\
&= \sum_i \sum_j r_j \delta_{ij} \\
&= \sum_i r_i \\
&= n.
\end{aligned}$$

□

Proof of (b).

(1) Take any point $Q_1 \notin f \cup L$ (since $\mathbf{P}^2$ is irreducible). Suppose L is a line passing Q_2 and Q_3, $Q_2 \neq Q_3$.

(2) By Problem 4.14, there is a projective change of coordinates $t : \mathbf{P}^2 \to \mathbf{P}^2$ such that $t(Q_1) = [0 : 1 : 0]$ and $t(L) = x$. In particular, $t(Q_1) = [0 : 1 : 0] \notin f^t$ (by the construction in (1)).

(3) Hence,

$$\sum_P I(P, f \cap L) = \sum_P I(P, f^t \cap L^t) = \sum_P I(P, f^t \cap x) = n.$$

□

Problem 5.13.

Prove that an irreducible cubic is either nonsingular or has at most one double point (a node or a cusp). (Hint: Use Problem 5.12, where L is a line through

two multiple points; or use Problems 5.10 and 5.11.)

Proof (Problem 5.12).

(1) (Reductio ad absurdum) Suppose there were a line L passing through two multiple points P, Q of an irreducible cubic f.

(2) Note that

$$\begin{aligned}\sum I(P, f \cap L) &\geq I(P, f \cap L) + I(Q, f \cap L) \\ &\geq m_P(f)m_P(L) + m_Q(f)m_Q(L) \\ &\geq 2 \cdot 1 + 2 \cdot 1 \\ &= 4.\end{aligned}$$

By Problem 5.12, $\sum I(P, f \cap L) = 3$, a contradiction. Hence f has at most one multiple point. In particular, f has at most one double point.

□

Proof (Problems 5.10 and 5.11).

(1) Suppose one irreducible cubic f has one multiple point P. It suffices to show that P is a cusp or a node, or it suffices to show that P is a double point.

(2) Up to projective equivalence, might assume that $P = [0 : 0 : 1]$. If $m_P(f) = m_P(f_*) = 3$, then f_* is a form in $k[x, y]$ of degree 3. Thus f is in $k[x, y] \hookrightarrow k[x, y, z]$, which is reducible. Hence P is a double point. By Problems 5.10 and 5.11, f has no other singularities.

□

Problem 5.14.*

Let $P_1, \ldots, P_n \in \mathbf{P}^2$. Show that there are an infinite number of lines passing through P_1, but not through $P_2, \ldots, P_n$. If P_1 is a simple point on f, we may take these lines transversal to f at P_1.

Proof.

(1) Might assume that all $P_1, \ldots, P_n$ are distinct. Write a line L_{ij} passing through P_i and P_j.

(2) (Reductio ad absurdum) Suppose there were finite number of lines passing through P_1, but not through $P_2, \ldots, P_n$, say $M_1, \ldots, M_r$. Hence, we can write $\mathbf{P}^2$ as

$$\mathbf{P}^2 = L_{12} \cup \cdots \cup L_{1n} \cup M_1 \cup \cdots \cup M_r,$$

contrary to the fact that $\mathbf{P}^2$ is irreducible.

□

Problem 5.15.*

Let C be an irreducible projective plane curve, $P_1, \ldots, P_n$ simple points on C, $m_1, \ldots, m_n$ integers. Show that there is a $z \in k(C)$ with $\mathrm{ord}_{P_i}(z) = m_i$ for $i = 1, \ldots, n$. (Hint: Take lines L_i as in Problem 5.14 for P_i, and a line L_0 not through any P_j, and let $z = \prod L_i^{m_i} L_0^{-\sum m_i}$.)

Proof.

(1) Take lines L_i not tangent to C at P_i as in Problem 5.14 for P_i. Since $\mathbf{P}^2 = V(0) \supsetneq V(C)$, we can pick a point P outside C. Take one line L_0 through P but not through any P_j as in Problem 5.14.

(2) Define $z = \prod L_i^{m_i} / L_0^{\sum m_i} \in k(C)$ since $\prod L_i^{m_i}$ and $L_0^{\sum m_i}$ are in $\Gamma(C)$ of the same degree $\sum m_i$. Note that $L_0(P_j) \neq 0$ for any P_j. So $\mathrm{ord}_{P_i}(z)$ is well-defined. Moreover,

$$\mathrm{ord}_{P_i}(z) = \sum_j m_j \mathrm{ord}_{P_i}(L_j) - \left(\sum m_j\right) \mathrm{ord}_{P_i}(L_0) = m_i$$

since L_j $(j \neq i)$ and L_0 are units in $k(C)$ and $L_i \ni P_i$ is not tangent to C.

□

Problem 5.16.*

Let f be an irreducible curve in $\mathbf{P}^2$. Suppose $I(P, f \cap z) = 1$, and $P \neq [1:0:0]$. Show that $\frac{\partial f}{\partial x}(P) \neq 0$. (Hint: If not, use Euler's Theorem to show that $\frac{\partial f}{\partial y}(P) = 0$; but z is not tangent to f at P.)

Proof.

(1) Might write $P = [\alpha : 1 : 0] \in \mathbf{P}^2$ since $z(P) = 0$ (by $I(P, f \cap z) > 0$) and $P \neq [1:0:0]$.

(2) Since $I(P, f \cap z) = 1$, $m_P(f) = 1$ and z is not tangent to f at P. Thus, P is a simple point of f. By Problem 5.4, the tangent line L to f at P is

$$\frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z = 0.$$

In particular, $P = [\alpha : 1 : 0] \in L$, that is,

$$\frac{\partial f}{\partial x}(P)\alpha + \frac{\partial f}{\partial y}(P) = 0.$$

(3) (Reductio ad absurdum) If $\frac{\partial f}{\partial x}(P) = 0$, $\frac{\partial f}{\partial y}(P) = 0$ by (2). Hence, the tangent line $L = z$, which is absurd.

□

5.2. Linear Systems of Curves

Problem 5.17.

Let P_1, P_2, P_3, P_4 are distinct points in $\mathbf{P}^2$. Let V be the linear system of conics passing through these points. Show that $\dim(V) = 2$ if P_1, P_2, P_3, P_4 lie on a line, and $\dim(V) = 1$ otherwise.

Proof.

(1) Let $V_i = V(2; P_1, \ldots, P_i)$. (So $V = V_4$.) By Theorem 1 in §5.2, we have

$$\dim V_4 \geq \frac{2(2+3)}{2} - \sum_{i=1}^{4} \frac{1(1+1)}{2} = 1,$$

$$\dim V_3 = \frac{2(2+3)}{2} - \sum_{i=1}^{3} \frac{1(1+1)}{2} = 2.$$

Also note that $V_4 \subseteq V_3$. Hence

$$\dim V_4 = 1 \text{ or } 2.$$

Therefore, it suffices to show that P_1, P_2, P_3, P_4 lie on a line if and only if

$$V_4 = V_3.$$

(2) The case P_1, P_2, P_3, P_4 lie on a line L. Take any conic $C \in V_3$. By Bézout's theorem or Problem 5.12, $L \mid C$. Hence $P_4 \in L \subseteq C$ and thus $C \in V_4$.

(3) The case P_1, P_2, P_3, P_4 are not collinear.

   (a) Suppose there are some three points, say P_1, P_2, P_3, are in a line L. Since $P_4 \notin L$ by assumption, the conic L^2 is in V_3 but not in V_4.

   (b) Suppose there are no three points lying on a line. Let L_{ij} be the line passing through P_i and P_j. Then the conic $L_{12}L_{13} \in V_3$ but not in V_4.

   By (a)(b), $V_4 \subsetneq V_3$ if P_1, P_2, P_3, P_4 are not collinear.

□

Problem 5.18.

Show that there is only one conic passing through the five points $[0:0:1]$, $[0:1:0]$, $[1:0:0]$, $[1:1:1]$, *and* $[1:2:3]$*; show that it is nonsingular.*

Proof.

(1) Let $C : ax^2 + bxy + cxz + dy^2 + eyz + fz^2$ be the conic passing these five points. That is,

$$\underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 6 & 9 \end{pmatrix}}_{\text{say } A \in \mathsf{M}_{5\times 6}(k)} \underbrace{\begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix}}_{\in \mathbf{P}^5(k)} = 0.$$

(2) The row echelon form A' of A is

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 0 \\ 0 & 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathsf{M}_{5\times 6}(k).$$

$\operatorname{rank}(A') = 5$ and thus there is a unique solution in $\mathbf{P}^5$, say $[0:3:-4:0:1:0] \in \mathbf{P}^5$. Hence,

$$C : 3xy - 4xz + yz = 0$$

is only one conic passing through these five points.

(3) By solving the system of equations $C(P) = \frac{\partial C}{\partial x}(P) = \frac{\partial C}{\partial y}(P) = \frac{\partial C}{\partial z}(P) = 0$, $P = [0:0:0]$, which is absurd. Hence C is nonsingular.

□

Problem 5.19.

Consider the nine points $[0:0:1]$, $[0:1:1]$, $[1:0:1]$, $[1:1:1]$, $[0:2:1]$, $[2:0:1]$, $[1:2:1]$, $[2:1:1]$, *and* $[2:2:1] \in \mathbf{P}^2$ *(Sketch). Show that there are an infinite number of cubics passing through these points.*

Proof.

(1) Let $C : a_1x^3 + a_2y^3 + a_3z^3 + a_4x^2y + a_5x^2z + a_6y^2x + a_7y^2z + a_8z^2x + a_9z^2y + a_{10}xyz$ be the cubic passing these five points. That is,

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 8 & 1 & 0 & 0 & 0 & 4 & 0 & 2 & 0 \\ 8 & 0 & 1 & 0 & 4 & 0 & 0 & 2 & 0 & 0 \\ 1 & 8 & 1 & 2 & 1 & 4 & 4 & 1 & 2 & 2 \\ 8 & 1 & 1 & 4 & 4 & 2 & 1 & 2 & 1 & 2 \\ 8 & 8 & 1 & 8 & 4 & 8 & 4 & 2 & 2 & 4 \end{pmatrix}}_{\text{say } A \in \mathsf{M}_{9\times 10}(k)} \underbrace{\begin{pmatrix} a_1 \\ \vdots \\ a_{10} \end{pmatrix}}_{\in \mathbf{P}^9(k)} = 0.$$

(2) The row echelon form A' of A is

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-1}{2} & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{-1}{2} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \frac{3}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathsf{M}_{9\times 10}(k).$$

$\operatorname{rank}(A') = 8 < 9$ and thus there are an infinite number of cubics passing through these points, say

$$C : \lambda x(x-z)(x-2z) + \mu y(y-z)(y-2z),$$

where $[\lambda : \mu] \in \mathbf{P}^2(k)$.

□

5.3. Bézout's Theorem

Problem 5.20.

Check your answers of Problem 5.3 with Bézout's theorem

Proof.

(1) $f = y^2z - x(x-2z)(x+z)$ and $g = y^2 + x^2 - 2xz$.

$$I([0:0:1], f \cap g) = 2,$$
$$I([2:0:1], f \cap g) = 2,$$
$$I([-2, \sqrt{-8}:1], f \cap g) = 1,$$
$$I([-2, -\sqrt{-8}:1], f \cap g) = 1.$$

Hence, $\sum_P I(P, f \cap g) = 2 + 2 + 1 + 1 = 6 = \deg(f)\deg(g)$.

(2) $f = (x^2 + y^2)z + x^3 + y^3$ and $g = x^3 + y^3 - 2xyz$.

$$I([0:0:1], f \cap g) = 4,$$
$$I([1:-1:0], f \cap g) = 3,$$
$$I([1:\sqrt[3]{-1}:0], f \cap g) = 1,$$
$$I([1:1-\sqrt[3]{-1}:0], f \cap g) = 1.$$

Hence, $\sum_P I(P, f \cap g) = 4 + 3 + 1 + 1 = 9 = \deg(f)\deg(g)$.

(3) $f = y^5 - x(y^2 - xz)^2$ and $g = y^4 + y^3z - x^2z^2$.

$$I([0:0:1], f \cap g) = 9,$$
$$I([1:0:0], f \cap g) = 9,$$
$$I\left(\left[\frac{1}{2}:1:2+2\sqrt{2}\right], f \cap g\right) = 1,$$
$$I\left(\left[\frac{1}{2}:1:2-2\sqrt{2}\right], f \cap g\right) = 1.$$

Hence, $\sum_P I(P, f \cap g) = 9 + 9 + 1 + 1 = 20 = \deg(f)\deg(g)$.

(4) $f = (x^2 + y^2)^2 + 3x^2yz - y^3z$ and $g = (x^2 + y^2)^3 - 4x^2y^2z^2$.

$$I([1:\sqrt{-1}:0], f \cap g) = 3,$$
$$I([1:-\sqrt{-1}:0], f \cap g) = 3,$$
$$I([0:0:1], f \cap g) = 14,$$
$$I\left(\left[\frac{\sqrt{5+2\sqrt{5}}}{4}:\frac{-\sqrt{5}}{4}:1\right], f \cap g\right) = 1,$$
$$I\left(\left[-\frac{\sqrt{5+2\sqrt{5}}}{4}:\frac{-\sqrt{5}}{4}:1\right], f \cap g\right) = 1,$$
$$I\left(\left[\frac{\sqrt{5-2\sqrt{5}}}{4}:\frac{\sqrt{5}}{4}:1\right], f \cap g\right) = 1,$$
$$I\left(\left[-\frac{\sqrt{5-2\sqrt{5}}}{4}:\frac{\sqrt{5}}{4}:1\right], f \cap g\right) = 1.$$

Hence, $\sum_P I(P, f \cap g) = 3 + 3 + 14 + 1 + 1 + 1 + 1 = 24 = \deg(f)\deg(g)$.

□

Problem 5.21.*

Show that every nonsingular projective plane curve is irreducible. Is this true for affine curves?

Proof.

(1) Let f be a nonsingular projective plane curve. (Reductio ad absurdum) Suppose $f = gh$ were reducible. Then g and h intersects in $\mathbf{P}^2$ (Bézout's theorem).

(2) *Show that each intersection point P is a singularity of f.* Note that $g(P) = h(P) = 0$ and the chain rule for derivatives. Thus,

$$\frac{\partial f}{\partial x_i}(P) = g(P)\frac{\partial h}{\partial x_i}(P) + \frac{\partial g}{\partial x_i}(P)h(P) = 0$$

for $i = 1, 2, 3$. P is a singularity of f (Problem 5.1).

(3) *Show that it is not true for affine curves.* $V(x^2 - x) \subseteq \mathbf{A}^2$ is nonsingular but not irreducible.

□

Problem 5.22.*

Let f be an irreducible curve of degree n. Assume $\frac{\partial f}{\partial x} \neq 0$. Apply Corollary 1 to f and $\frac{\partial f}{\partial x}$, and conclude that $\sum m_P(f)(m_P(f) - 1) \leq n(n-1)$. In particular, f has at most $\frac{n(n-1)}{2}$ multiple points. (See Problems 5.6, 5.8.)

Proof.

(1) There is nothing to do for $n = 1$. Might assume that $n > 1$.

(2) Since f and $\frac{\partial f}{\partial x}$ have no common component (Problem 5.8), Corollary 1 to Bézout's theorem gives us

$$\sum m_P(f)m_P\left(\frac{\partial f}{\partial x}\right) \leq \deg(f)\deg\left(\frac{\partial f}{\partial x}\right) \leq n(n-1).$$

By Problem 5.6, the conclusion is established.

(3) Then

$$\begin{aligned} n(n-1) &\geq \sum_P m_P(f)(m_P(f)-1) \\ &\geq \sum_{m_P(f)>1} 2(2-1) \\ &\geq \sum_{m_P(f)>1} 2 \\ &= 2 \cdot (\text{number of multiple points}). \end{aligned}$$

□

Problem 5.23. (Hessian matrix)

A problem about flexes (see Problem 3.12): Let f be a projective plane curve of degree n, and assume f contains no lines.

*Let $D_i f = \frac{\partial f}{\partial x_i}$ and $D_{ij} f = \frac{\partial^2 f}{\partial x_i x_j}$, forms of degree $n-1$ and $n-2$ respectively. Form a 3×3 matrix with the entry in the (i,j)th place being $D_{ij} f$ $(i,j = 1,2,3)$. Let H be the determinant of this matrix, a form of degree $3(n-2)$. This H is called the **Hessian** of f. Problems 5.22 and 6.47 show that $H \neq 0$, for f irreducible. The following theorem shows the relationship between flexes and the Hessian.*

Theorem. *(*$\mathrm{char}(k) = 0$*)*

(1) *$P \in H \cap f$ if and only if P is either a flex or a multiple point of f.*

(2) *$I(P, H \cap f) = 1$ if and only if P is an ordinary flex.*

Outline of proof.

(a) *Let t be a projective change of coordinates. Then the Hessian of f^t is $\det(t)^2(H^t)$. So we can assume $P = [0:0:1]$; write $f_*(x,y) = f(x,y,1)$ and $H_*(x,y) = H(x,y,1)$.*

(b) *$(n-1)D_j f = \sum_i x_i D_{ij} f$. (Use Euler's Theorem.)*

(c) *$I(P, f_* \cap H_*) = I(P, f_* \cap g)$ where*

$$g = (D_2 f_*)^2 (D_{11} f_*) + (D_1 f_*)^2 (D_{22} f_*) - 2(D_1 f_*)(D_2 f_*)(D_{12} f_*).$$

(Hint: Perform row and column operations on the matrix for H_*. Add x times the first row plus y times the second row to the third row, then apply part (b). Do the same with the columns. Then calculate the determinant.)

(d) *If P is a multiple point on f, then $I(P, f_* \cap g) > 1$.*

(e) *Suppose P is a simple point, $y = 0$ is the tangent line to f at P, so*

$$f_* = y + ax^2 + bxy + cy^2 + dx^3 + ex^2y + \cdots .$$

Then P is a flex if and only if $a = 0$, and P is an ordinary flex if and only if $a = 0$ and $d \neq 0$. A short calculation shows that

$$g = 2a + 6dx + (8ac - 2b^2 + 2e)y + \textit{higher terms},$$

which concludes the proof.

Corollary.

(1) *A nonsingular curve of degree > 2 always has a flex.*

(2) *A nonsingular cubic has nine flexes, all ordinary.*

Proof of (a).

(1) Write $t = (t_1, t_2, t_3)$ where $t_1, t_2, t_3 \in k[x, y, z]$.

(2) By the chain rule for differentiation,

$$\frac{\partial f^t}{\partial x_j} = \sum_{\beta=1}^{3} \frac{\partial f^t}{\partial t_\beta} \frac{\partial t_\beta}{\partial x_j}$$

and thus

$$\begin{aligned}
\frac{\partial^2 f^t}{\partial x_i \partial x_j} &= \frac{\partial}{\partial x_i}\left(\frac{\partial f^t}{\partial x_j}\right) \\
&= \frac{\partial}{\partial x_i}\left(\sum_{\beta=1}^{3} \frac{\partial f^t}{\partial t_\beta}\frac{\partial t_\beta}{\partial x_j}\right) \\
&= \sum_{\beta=1}^{3} \frac{\partial}{\partial x_i}\left(\frac{\partial f^t}{\partial t_\beta}\right) \cdot \frac{\partial t_\beta}{\partial x_j} + \frac{\partial f^t}{\partial t_\beta} \cdot \underbrace{\frac{\partial^2 t_\beta}{\partial x_i \partial x_j}}_{=0} \\
&= \sum_{\beta=1}^{3}\sum_{\alpha=1}^{3} \frac{\partial t_\alpha}{\partial x_i}\left(\frac{\partial f^t}{\partial t_\alpha \partial t_\beta}\right) \cdot \frac{\partial t_\beta}{\partial x_j} \\
&= \sum_{\alpha=1}^{3}\sum_{\beta=1}^{3} \frac{\partial t_\alpha}{\partial x_i}\left(\frac{\partial f^t}{\partial t_\alpha \partial t_\beta}\right) \frac{\partial t_\beta}{\partial x_j}.
\end{aligned}$$

(3) Hence, the Hessian of f^t is

$$\begin{aligned}
H(f^t) &= \det\left(\left(\frac{\partial^2 f^t}{\partial x_i \partial x_j}\right)_{i,j}\right) \\
&= \det\left(\left(\sum_{\alpha=1}^{3}\sum_{\beta=1}^{3}\frac{\partial t_\alpha}{\partial x_i}\left(\frac{\partial f^t}{\partial t_\alpha \partial t_\beta}\right)\frac{\partial t_\beta}{\partial x_j}\right)_{i,j}\right) \\
&= \det\left(\left(\frac{\partial t_\alpha}{\partial x_i}\right)^T_{\alpha,i}\left(\frac{\partial f^t}{\partial t_\alpha \partial t_\beta}\right)_{\alpha,\beta}\left(\frac{\partial t_\beta}{\partial x_j}\right)_{\beta,j}\right) \\
&= \det\left(\left(\frac{\partial t_\alpha}{\partial x_i}\right)^T_{\alpha,i}\right)\det\left(\left(\frac{\partial f^t}{\partial t_\alpha \partial t_\beta}\right)_{\alpha,\beta}\right)\det\left(\left(\frac{\partial t_\beta}{\partial x_j}\right)_{\beta,j}\right) \\
&= \det\left(t^T\right)\cdot H(f)^t \cdot \det(t) \\
&= \det(t)^2 H(f)^t.
\end{aligned}$$

(4) Note that t is invertible. So we can assume $P = [0:0:1]$.

□

Proof of (b). Since $D_j f$ is a form of degree $n-1$, the result is established by Euler's theorem in §1.1. □

Proof of (c).

(1) Note that

$$
\begin{aligned}
& z^2 H \\
&= z^2 \begin{vmatrix} D_{11}f & D_{12}f & D_{13}f \\ D_{21}f & D_{22}f & D_{23}f \\ D_{31}f & D_{32}f & D_{33}f \end{vmatrix} \\
&= z \begin{vmatrix} D_{11}f & D_{12}f & D_{13}f \\ D_{21}f & D_{22}f & D_{23}f \\ xD_{11}f + yD_{21}f + zD_{31}f & xD_{12}f + yD_{22}f + zD_{32}f & xD_{13}f + yD_{23}f + zD_{33}f \end{vmatrix} \\
&= z \begin{vmatrix} D_{11}f & D_{12}f & D_{13}f \\ D_{21}f & D_{22}f & D_{23}f \\ (n-1)D_1 f & (n-1)D_2 f & (n-1)D_3 f \end{vmatrix} \\
&= \begin{vmatrix} D_{11}f & D_{12}f & xD_{11}f + yD_{12}f + zD_{13}f \\ D_{21}f & D_{22}f & xD_{21}f + yD_{22}f + zD_{23}f \\ (n-1)D_1 f & (n-1)D_2 f & (n-1)xD_1 f + (n-1)yD_2 f + (n-1)zD_3 f \end{vmatrix} \\
&= \begin{vmatrix} D_{11}f & D_{12}f & (n-1)D_1 f \\ D_{21}f & D_{22}f & (n-1)D_2 f \\ (n-1)D_1 f & (n-1)D_2 f & n(n-1)f \end{vmatrix} \\
&= (n-1)^2 (D_1 f)(D_{21}f D_2 f - D_{22}f D_1 f) \\
&\quad - (n-1)^2 (D_2 f)(D_{11}f D_2 f - D_{12}f D_1 f) \\
&\quad + n(n-1)f(D_{11}f D_{22}f - D_{12}f D_{21}f) \\
&= (n-1)^2 (-(D_1 f)^2 D_{22}f - (D_2 f)^2 D_{11}f + 2(D_1 f)(D_2 f)(D_{12}f)) \\
&\quad + n(n-1)f(D_{11}f D_{22}f - D_{12}f D_{21}f).
\end{aligned}
$$

(2) Dehomogenize $z^2 H$ w.r.t. z:

$$H_* = -(n-1)^2 g + n(n-1) f_* [(D_{11}f_*)(D_{22}f_*) - (D_{12}f_*)^2].$$

Hence if $n > 1$, then

$$I(P, f_* \cap H_*) = I(P, f_* \cap (-(n-1)^2 g)) = I(P, f_* \cap g).$$

(If $n \leq 1$, then $I(P, f_* \cap H_*) = I(P, f_* \cap g) = \infty$.)

□

Proof of (d).

(1) Since $I(P, f_* \cap g) \geq m_P(f_*) m_P(g) \geq 2 m_P(g)$, it suffices to show that $m_P(g) > 0$ or $P \in g$.

(2) Problem 5.1 shows that

$$\begin{aligned} g(P) &= (D_1 f_*(P))^2 D_{22} f_*(P) \\ &\quad + (D_2 f_*(P))^2 D_{11} f_*(P) \\ &\quad - 2(D_1 f_*(P))(D_2 f_*(P))(D_{12} f_*(P)) \\ &= 0^2 \cdot D_{22} f_*(P) + 0^2 \cdot D_{11} f_*(P) - 2 \cdot 0 \cdot 0 \cdot D_{12} f_*(P) \\ &= 0. \end{aligned}$$

□

Proof of (e).

(1) Suppose P is a simple point of f, $y = 0$ is the tangent line to f at P. Write

$$f_* = y + ax^2 + bxy + cy^2 + dx^3 + ex^2y + \cdots .$$

Then P is a flex if and only if $a = 0$, and P is an ordinary flex if and only if $a = 0$ and $d \neq 0$ (Problem 3.12).

(2) A short calculation shows that

$$\begin{aligned} g &= (D_2 f_*)^2 (D_{11} f_*) + (D_1 f_*)^2 (D_{22} f_*) - 2(D_1 f_*)(D_2 f_*)(D_{12} f_*) \\ &= [2a + (6d + 4ab)x + (8ac + 2e)y] + 0 - 2[2abx + b^2 y] + \text{higher terms} \\ &= 2a + 6dx + (8ac - 2b^2 + 2e)y + \text{higher terms}. \end{aligned}$$

(3) Hence,

$$\begin{aligned} & P \in f_* \cap g \\ \iff & I(P, f_* \cap g) \geq 1 \\ \iff & I(P, (y + \cdots) \cap (2a + 6dx + (8ac - 2b^2 + 2e)y + \cdots)) \geq 1 \\ \iff & a = 0 \\ \iff & P \text{ is a flex} \end{aligned}$$

if P is a simple point of f.

(4) Also note that

$$\begin{aligned} & I(P, f_* \cap g) = 1 \\ \iff & I(P, (y + \cdots) \cap (2a + 6dx + (8ac - 2b^2 + 2e)y + \cdots)) = 1 \\ \iff & a = 0 \text{ and } d \neq 0 \\ \iff & P \text{ is an ordinary flex} \end{aligned}$$

if P is a simple point of f.

□

Proof of Theorem (1).

(1) ($\Longrightarrow$) Suppose $P \in H \cap f$ and P is not a multiple point of f. So P is a simple point of f. Note that

$$I(P, H \cap f) = I(P, H_* \cap f_*) = I(P, g \cap f_*) \geq 1.$$

So P is a flex by part (e).

(2) ($\Longleftarrow$) If P is a flex of f, then part (e) shows that

$$I(P, H \cap f) = I(P, H_* \cap f_*) = I(P, g \cap f_*) \geq 1.$$

If P is a multiple point of f, then part (d) shows that

$$I(P, H \cap f) = I(P, H_* \cap f_*) \geq 2.$$

In any case, $P \in H \cap f$.

□

Proof of Theorem (2).

(1) ($\Longrightarrow$) By the proof of Theorem (1), P is a simple point of f. Therefore, the conclusion is established by part (e).

(2) ($\Longleftarrow$) Part (e).

□

Proof of Corollary (1).

(1) Let f be a nonsingular curve of degree > 2. So $\deg(H) = 3(n-2) > 0$. $H \cap f \neq \varnothing$ (Bézout's theorem).

(2) Since f is nonsingular, every point in $H \cap f$ is a simple point. So every point in $H \cap f$ is a flex (Theorem (1)).

□

Proof of Corollary (2).

(1) *Show that every flex of a nonsingular cubic f is ordinary.* Given any flex $P \in f$ and the corresponding tangent line L to f at P. By definition,

$$\mathrm{ord}_P^f(L) = I(P, f \cap L) \geq 3.$$

Bézout's theorem or Problem 5.12 shows that

$$\sum_P I(P, f \cap L) = I(P, f \cap L) = 3.$$

That is, $\mathrm{ord}_P^f(L) = 3$ or P is an ordinary flex.

(2) Since f is nonsingular, we have

$$\begin{aligned} H \cap f &= \{\text{all flexes of } f\} && \text{(Theorem (1))} \\ &= \{\text{all ordinary flexes of } f\} && \text{((1))} \\ &= \{P \in f : I(P, H \cap f) = 1\}. && \text{(Theorem (2))} \end{aligned}$$

(3) Hence

$$\sum_P I(P, H \cap f) = \deg(H)\deg(f) = 3 \cdot 3 = 9$$

(Bézout's theorem) shows that there are exactly 9 (ordinary) flexes of f. (Also see Problem 5.37.)

□

Problem 5.24.

($\mathrm{char}(k) = 0$*)*

(a) *Let* $P := [0:1:0]$ *be a flex on an irreducible cubic* f*,* $z = 0$ *the tangent line to* f *at* $[0:1:0]$*. Show that* $f = zy^2 + byz^2 + cyxz +$ *terms in* x*,* z*. Find a projective change of coordinates (using* $y \mapsto y - \frac{b}{2}z - \frac{c}{2}x$*) to get* f *to the form* $zy^2 =$ *cubic in* x*,* z*.*

(b) *Show that any irreducible cubic is projectively equivalent to one of the following:* $y^2z = x^3$*,* $y^2z = x^2(x+z)$*, or* $y^2z = x(x-z)(x-\lambda z)$*,* $\lambda \in k$*,* $\neq 0, 1$*. (See Problems 5.10, 5.11.)*

Proof of (a).

(1) As $z = 0$ is the tangent line to f at $[0:1:0]$, we can write

$$f(x, 1, z) = z + ax^2 + bz^2 + cxz - \alpha_0 x^3 - \alpha_1 x^2 z - \alpha_2 x z^2 - \alpha_3 z^3.$$

By assumption,

$$I(P, f \cap z) = I(P, (ax^2 - \alpha_0 x^3) \cap z) \geq 3$$

implies that $a = 0$. Also, $\alpha_0 \neq 0$ since f is irreducible. Hence,

$$f(x, y, z) = zy^2 + byz^2 + cyxz - \underbrace{\alpha_0}_{\neq 0} x^3 - \alpha_1 x^2 z - \alpha_2 x z^2 - \alpha_3 z^3.$$

(2) So

$$\begin{aligned} f &\sim y^2 z - \underbrace{\alpha_0}_{:=\beta_0} x^3 - \underbrace{\left(\alpha_1 - \frac{c^2}{4}\right)}_{:=\beta_1} x^2 z - \underbrace{\left(\alpha_2 - \frac{bc}{2}\right)}_{:=\beta_2} x z^2 - \underbrace{\left(\alpha_3 - \frac{b^2}{4}\right)}_{:=\beta_3} z^3 \\ &= y^2 z - \beta_0 x^3 - \beta_1 x^2 z - \beta_2 x z^2 - \beta_3 z^3 \end{aligned}$$

by $y \mapsto y - \frac{b}{2}z - \frac{c}{2}x$. Hence f is of the form $zy^2 =$ cubic in x, z (up to projective equivalence).

□

Proof of (b).

(1) Since $\beta_0 \neq 0$ and $k = \overline{k}$, by $x \mapsto \beta_0^{-\frac{1}{3}} x$ we might write

$$f \sim y^2 z - x^3 - \beta_1 x^2 z - \beta_2 x z^2 - \beta_3 z^3.$$

(2) Since $k = \overline{k}$,

$$x^3 + \beta_1 x^2 z + \beta_2 x z^2 + \beta_3 z^3 = (x - \gamma_1 z)(x - \gamma_2 z)(x - \gamma_3 z)$$

for some $\gamma_1, \gamma_2, \gamma_3 \in k$. Consider the cases about $\gamma_1, \gamma_2, \gamma_3$.

(3) The case $\gamma_1 = \gamma_2 = \gamma_3$.

$$\begin{aligned} f &\sim y^2 z - (x - \gamma_1 z)(x - \gamma_2 z)(x - \gamma_3 z) \\ &\sim y^2 z - x^3. && (x \mapsto x + \gamma_1 z) \end{aligned}$$

(4) The case $\gamma_1 = \gamma_2 \neq \gamma_3$.

$$\begin{aligned} f &\sim y^2 z - (x - \gamma_1 z)(x - \gamma_2 z)(x - \gamma_3 z) \\ &\sim y^2 z - x^2(x + (\gamma_1 - \gamma_3)z) && (x \mapsto x + \gamma_1 z) \\ &\sim (\gamma_1 - \gamma_3)^{-1} y^2 z - x^2(x + z) && (z \mapsto (\gamma_1 - \gamma_3)^{-1} z) \\ &\sim y^2 z - x^2(x + z). && (y \mapsto (\gamma_1 - \gamma_3)^{\frac{1}{2}} y) \end{aligned}$$

(5) The case all $\gamma_1, \gamma_2, \gamma_3$ are different.

$$\begin{aligned} f &\sim y^2 z - (x - \gamma_1 z)(x - \gamma_2 z)(x - \gamma_3 z) \\ &\sim y^2 z - x(x - (\gamma_2 - \gamma_1)z)(x - (\gamma_3 - \gamma_1)z) && (x \mapsto x + \gamma_1 z) \\ &\sim (\gamma_2 - \gamma_1)^{-1} y^2 z - x^2(x - z)\left(x - \frac{\gamma_3 - \gamma_1}{\gamma_2 - \gamma_1} z\right) && (z \mapsto (\gamma_2 - \gamma_1)^{-1} z) \\ &\sim y^2 z - x^2(x - z)\left(x - \frac{\gamma_3 - \gamma_1}{\gamma_2 - \gamma_1} z\right) && (y \mapsto (\gamma_2 - \gamma_1)^{\frac{1}{2}} y) \\ &\sim y^2 z - x^2(x - z)\,(x - \lambda z)\,. && \left(\lambda := \frac{\gamma_3 - \gamma_1}{\gamma_2 - \gamma_1}, \lambda \neq 0, 1\right) \end{aligned}$$

□

5.4. Multiple Points

Problem 5.25.

Let f be a projective plane curve of degree n with no multiple components, and c simple components. Show that

$$\sum \frac{m_P(m_P-1)}{2} \leq \frac{(n-1)(n-2)}{2} + c - 1 \leq \frac{n(n-1)}{2}.$$

(Hint: Let $f = f_1 f_2$; consider separately the points on one f_i or on both.)

Proof.

(1) Write

$$f = f_1 \cdots f_c,$$

where each f_i is irreducible. By assumption, f_i and f_j have no common factor whenever $i \neq j$. By Bézout's theorem, we might consider separately the points on one f_i or on many components.

(2) Hence

$$\begin{aligned}
&\sum \frac{m_P(m_P-1)}{2} \\
\leq &\sum_{P \in f_1} \frac{m_P(m_P-1)}{2} + \sum_{P \notin f_1} \frac{m_P(m_P-1)}{2} \\
\leq &\underbrace{\frac{(d-1)(d-2)}{2}}_{\text{Theorem 2 in §5.4}} + \underbrace{\frac{(n-d-1)(n-d-2)}{2} + (c-1) - 1}_{\text{Mathematical induction}} \\
= &\frac{(n-1)(n-2)}{2} + c - 1 + \underbrace{1 - d(n-d)}_{\leq 0} \\
\leq &\frac{(n-1)(n-2)}{2} + c - 1
\end{aligned}$$

where $d = \deg(f_1) \geq 1$.

(3) Note that $c \leq n$. So

$$\frac{(n-1)(n-2)}{2} + c - 1 \leq \frac{(n-1)(n-2)}{2} + n - 1 = \frac{n(n-1)}{2}.$$

□

Problem 5.26.*

($\mathrm{char}(k) = 0$*) Let f be an irreducible curve of degree n in $\mathbf{P}^2$. Suppose $P \in \mathbf{P}^2$, with $m_P(f) = r \geq 0$. Then for all but a finite number of lines L through P, L intersects f in $n - r$ distinct points other than P. We outline a proof:*

(a) *We may assume $P = [0 : 1 : 0]$. If $L_\lambda = \{[\lambda : t : 1] : t \in k\} \cup \{P\}$, we need only consider the L_λ. Then $f = a_r(x, z)y^{n-r} + \cdots + a_n(x, z)$, $a_r \neq 0$. (See Problems 4.24, 5.5).*

(b) *Let $g_\lambda(t) = f(\lambda, t, 1)$. It is enough to show that for all but a finite number of λ, g_λ has $n - r$ distinct points.*

(c) *Show that g_λ has $n-r$ distinct roots if $a_r(\lambda, 1) \neq 0$, and $f \cap \frac{\partial f}{\partial y} \cap L_\lambda = \{P\}$ if $P \in f$ (see Problem 1.53).*

Proof of (a).

(1) Might assume $P = [0 : 1 : 0]$ (up to projective equivalence).

(2) By Problem 4.24, we might consider the lines $L_\lambda = \{[\lambda : t : 1] : t \in k\} \cup \{P\}$ except finitely one line L_∞.

(3) Write $f = a_r(x, z)y^{n-r} + \cdots + a_n(x, z)$, $a_r \neq 0$ (Problem 5.5).

□

Proof of (b). Let $g_\lambda(t) = f(\lambda, t, 1) = a_r(\lambda, 1)t^{n-r} + \cdots + a_n(\lambda, 1)$. It suffices to show that all but a finite number of λ, $g_\lambda(t)$ has $n - r$ distinct roots in k. □

Proof of (c).

(1) There are finitely number of $\lambda \in k$ such that $a_r(\lambda, 1) = 0$ since k is a field.

(2) $g_\lambda(t)$ is irreducible over $(k[\lambda])[t]$ since f is irreducible. Hence $a_r(\lambda, 1) \neq 0$ and $\mathrm{char}(k) = 0$ implies that $g_\lambda(t)$ has $n - r$ distinct roots in k (Problem 1.53).

(3) By (1)(2), the result is established.

(4) *Suppose $P \in f$. Show that $f \cap \frac{\partial f}{\partial y} \cap L_\lambda = \{P\}$ (for all but finitely number of λ).* Since $f \cap L_\lambda = \{P\}$, it suffices to show that $P \in \frac{\partial f}{\partial y}$.

   (a) It is nothing to do if P is a multiple point of f (Problem 5.1).

   (b) If P is a simple point of f, then the tangent line to f at P is $L = \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z$ (Problem 5.4). Since $P \in L$, $\frac{\partial f}{\partial y}(P) = 0$.

   In any case, $\frac{\partial f}{\partial y}(P) = 0$.

□

Problem 5.27.

Show that Problem 5.26 remains true if f is reducible, provided it has no multiple components.

Proof.

(1) Write $f = f_1 \cdots f_s$ where each f_i is irreducible and f_i, f_j have no common factor whenever $i \neq j$.

(2) Apply Problem 5.26 to each f_i to get that for all but a finite number of lines L_i through P, L_i intersects f_i in $n_i - r_i$ distinct points other than P, where $n_i = \deg(f_i)$ and $r_i = m_P(f_i)$. Collect these lines as $\mathscr{L}_i$.

(3) Since $f_i \cap f_j$ is finite whenever $i \neq j$ (Problem 5.7), there are finitely number of lines through P also passing through $f_i \cap f_j$ for any $i \neq j$. Collect these lines as $\mathscr{L}'$.

(4) Hence any line from
$$(\mathscr{L}_1 \cup \cdots \cup \mathscr{L}_s) - \mathscr{L}'$$
passes through P and intersects f in
$$\sum (n_i - r_i) = \sum n_i - \sum r_i = n - r$$
distinct points other than P (by part (2) and our construction). The result is established.

□

Problem 5.28. (Terrible point)

($\mathrm{char}(k) = p > 0$*)* $f = x^{p+1} - y^p z$, $P = [0 : 1 : 0]$. *Find $L \cap f$ for all lines L passing through P. Show that every line that is tangent to f at a simple point passes through P!*

Proof.

(1) The case $\mathrm{char}(k) = p > 0$ for Problem 4.24 shows that $L = L_\lambda = V(x - \lambda z)$ for any $\lambda \in k$ or $L = L_\infty = V(z)$. Note that $L_0 \cap f = \{P\}$ and $L_\infty \cap f = \{P\}$. It suffices to consider the case $L_\lambda \cap f$ for $\lambda \neq 0$.

(2) So

$$\begin{aligned} 0 &= x^{p+1} - y^p z \\ &= x^{p+1} - y^p(\lambda^{-1}x) && (x - \lambda z = 0) \\ &= x(x^p - \lambda^{-1}y^p) \\ &= x\left(x^p - \left(\lambda^{-\frac{1}{p}}y\right)^p\right) && (k = \overline{k}) \\ &= x\left(x - \lambda^{-\frac{1}{p}}y\right)^p. && (\mathrm{char}(k) = p > 0) \end{aligned}$$

Here $\lambda^{-\frac{1}{p}}$ is the unique p^{th} root of λ^{-1} (since $\mathrm{char}(k) = p$). Hence

$$L_\lambda \cap f = \left\{P, [\lambda^{-\frac{1}{p}} : 1 : \lambda^{-\frac{p+1}{p}}]\right\}.$$

(3) *Show that every line that is tangent to f at a simple point passes through P.* Let L be the tangent line to f at a simple point $Q = [a : b : c]$ passing through P. Problem 5.4 shows that

$$\begin{aligned} L &= \frac{\partial f}{\partial x}(Q)x + \frac{\partial f}{\partial y}(Q)y + \frac{\partial f}{\partial z}(Q)z \\ &= \frac{\partial f}{\partial x}(Q)x + \frac{\partial f}{\partial z}(Q)z. \end{aligned}$$

Here $\frac{\partial f}{\partial y} = -py^{p-1} = 0 \in k[x, y, z]$ since $\mathrm{char}(k) = p > 0$. So $P = [0 : 1 : 0] \in L$ for any tangent line to f at a simple point of f.

□

5.5. Max Noether's Fundamental Theorem

Problem 5.29.

Fix f, g, and P. Show that in cases (1) and (2) - but not (3) - of Proposition 1 the conditions on h are equivalent to Noether's conditions.

Recall Proposition 1 in §5.5:

(1) f and g meet transversally at P, and $P \in h$.

(2) P is a simple point on f, and $I(P, h \cap f) \geq I(P, g \cap f)$.

(3) f and g have distinct tangents at P, and $m_P(h) \geq m_P(f) + m_P(g) - 1$.

Proof.

(1) (Noether's condition $\Longrightarrow$ (1) of Proposition 1) Since $h_* = af_* + bg_*$ for some $a, b \in \mathscr{O}_P(\mathbf{P}^2)$,

$$\begin{aligned} I(P, h \cap f) &= I(P, h_* \cap f_*) \\ &= I(P, (af_* + bg_*) \cap f_*) \\ &= I(P, (bg_*) \cap f_*) \\ &= I(P, b \cap f_*) + I(P, g_* \cap f_*) \\ &\geq I(P, g_* \cap f_*) \\ &= 1. \end{aligned}$$

Hence $P \in h$.

(2) (Noether's condition $\Longrightarrow$ (2) of Proposition 1) As $h_* \in (f_*, g_*) \subseteq \mathscr{O}_P(\mathbf{P}^2)$, $(f_*, h_*) \subseteq (f_*, g_*)$. So

$$\begin{aligned} I(P, h \cap f) &= I(P, h_* \cap f_*) \\ &= \dim_k(\mathscr{O}_P(\mathbf{P}^2)/(f_*, h_*)) \\ &\geq \dim_k(\mathscr{O}_P(\mathbf{P}^2)/(f_*, g_*)) \\ &= I(P, g_* \cap f_*) \\ &= I(P, g \cap f). \end{aligned}$$

(3) (Noether's condition $\not\Longrightarrow$ (3) of Proposition 1) Consider $h = y^2z - x^3$, $f = y^2$, $g = x^3$ and $P = [0 : 0 : 1]$. Noether's condition holds for h_*, f_*, g_* at the point $P = [0 : 0 : 1]$, and f, g have distinct tangents at P. However,

$$\underbrace{m_P(h)}_{=2} < \underbrace{m_P(f)}_{=2} + \underbrace{m_P(g)}_{=3} - 1.$$

□

Problem 5.30.

Let f be an irreducible projective plane curve. Suppose $z \in k(f)$ is defined at every $P \in f$. Show that $z \in k$. (Hint: Write $z = \frac{h}{g}$, and use max Noether's fundamental theorem).
Proof.

(1) Write $z = \frac{h}{g}$ where h, g are forms of the same degree in $k[x, y, z]$ and $g(P) \neq 0$ for any $P \in V(f)$. Given any $P \in \mathbf{P}^2$ and consider two cases about $g(P)$.

(2) If $g(P) \neq 0$, then $h - zg = 0 \in \mathscr{O}_P(f) = \mathscr{O}_P(\mathbf{P}^2)/(f)\mathscr{O}_P(\mathbf{P}^2)$. So

$$h = \alpha f + zg \in \mathscr{O}_P(\mathbf{P}^2)$$

for some $\alpha \in \mathscr{O}_P(\mathbf{P}^2)$.

(3) If $g(P) = 0$, then $f(P) \neq 0$ and thus f is a unit in $\mathscr{O}_P(\mathbf{P}^2)$. Hence $h_* \in \mathscr{O}_P(\mathbf{P}^2) = (f_*, g_*)$ is always true.

(4) By (2)(3), Noether's conditions are satisfied at $P \in \mathbf{P}^2$. Hence there is an equation $h = af + bg$ with a, b forms of degree $\deg(h) - \deg(f)$, $\deg(h) - \deg(g)$ (Max Noether's fundamental theorem in §5.5). Note that $b \in k$ since $\deg(b) = \deg(h) - \deg(g) = 0$. Therefore,

$$z = h/g = \underbrace{(a/g)f}_{=0 \text{ in } k(f)} + b = b \in k.$$

□

5.6. Applications of Noether's Theorem

Problem 5.31.

If in Pascal's Theorem we let some adjacent vertices coincide (the side being a tangent), we get many new theorems:

(a) *State and sketch what happens if $P_1 = P_2$, $P_3 = P_4$, $P_5 = P_6$.*

(b) *Let $P_1 = P_2$, the other four distinct.*

(c) *From (b) deduce a rule for constructing the tangent to a given conic at a given point, using only a straight-edge.*

Proof of (a).

(1) Suppose a triangle $\triangle$ is inscribed in an irreducible conic. Then tangent lines to the conic at the vertices of $\triangle$ with the unique opposite sides meet in collinear points.

(2) See Pascal's theorem: degenerations for a sketch.

□

Proof of (b).

(1) Suppose a pentagon $P_1P_3P_4P_5P_6$ is inscribed in an irreducible conic. The tangent line to the conic at P_1 with any opposite side, and the rest opposite sides meet in collinear points.

(2) See Pascal's theorem: degenerations for a sketch.

□

Proof of (c).

(1) By (b), we can draw the collinear line L passing through two points Q_1, Q_2 whose are determined by opposite sides.

(2) The fifth unused side of the pentagon meets the collinear line L at Q_3. Hence the line passing through P_1 and Q_3 is the tangent line to the conic at P_1.

□

Problem 5.32. (Braikenridge-Maclaurin theorem)

Suppose the intersections of the opposite sides of a hexagon lie on a straight line. Show that the vertices lie on a conic.

Proof.

(1) Let C be three sides, C' the three opposite sides, L the line.

(2) Note that all points of $C' \cap L$ are simple points of C' (Corollary 2 to Bézout's theorem), and $C \bullet C' \geq L \bullet C'$. Max Noether's fundamental theorem shows that there is a conic Q such that $Q \bullet C' = C \bullet C' - L \bullet C'$ where Q contains the hexagon.

□

Problem 5.33.

Let C be an irreducible cubic, L a line such that $L \bullet C = P_1 + P_2 + P_3$, P_i distinct. Let L_i be the tangent line to C at P_i: $L_i \bullet C = 2P_i + Q_i$ for some Q_i. Show that Q_1, Q_2, Q_3 lie on a line. (L^2 is a conic!)

Proof.

(1) Similar to the proof of Proposition 2 in §5.6. Corollary 2 to Bézout's theorem shows that each P_i is simple. So all the points of $L^2 \cap C$ are simple points of C.

(2) Note that

$$\begin{aligned}(L_1L_2L_3) \bullet C &= L_1 \bullet C + L_2 \bullet C + L_3 \bullet C \\ &= (2P_1 + Q_1) + (2P_2 + Q_2) + (2P_3 + Q_3) \\ &= (2P_1 + 2P_2 + 2P_3) + (Q_1 + Q_2 + Q_3)\end{aligned}$$

and

$$L^2 \bullet C = 2(L \bullet C) = 2(P_1 + P_2 + P_3) = 2P_1 + 2P_2 + 2P_3.$$

So $(L_1L_2L_3) \bullet C \geq L^2 \bullet C$.

(3) By Corollary (2) to max Noether's fundamental theorem, there is a curve M such that $M \bullet C = Q_1 + Q_2 + Q_3$. Bézout's theorem shows that $\deg(M) = 1$ or M is a line. Therefore, M is a line passing Q_1, Q_2, Q_3.

□

Problem 5.34.

Show that a line through two flexes on a cubic passes through a third flex.

Proof.

(1) Let C be a cubic, L a line such that $L \bullet C = P_1 + P_2 + P_3$.

(2) *Let P_i be a simple point in C, L_i the tangent line to C at P_i. Show that P_i is a flex in C if and only if $L_i \bullet C = 3P_i$.*

$$\begin{aligned} & P_i \text{ is a flex in } C \\ \iff & I(P_i, L_i \cap C) = \operatorname{ord}_{P_i}^{C}(L_i) \geq 3 \\ \iff & I(P_i, L_i \cap C) = 3 \text{ and } L_i \cap C = \{P_i\} \\ \iff & L_i \bullet C = 3P_i. \qquad \text{(Bézout's theorem)} \end{aligned}$$

(3) Suppose P_1 and P_2 are flexes in C. $I(P_3, L_3 \cap C) > 1$ since L_3 is one tangent line to C at P_3. So $L_3 \bullet C = 2P_3 + P_3'$ for some $P_3' \in C$. Now it suffices to show that $P_3' = P_3$. (P_3 is simple since P_1 and P_2 are simple points by Corollary 2 to Bézout's theorem. So P_3 is a flex if $L_3 \bullet C = 3P_3$ by (2).)

(4) Consider $C' = L^3$ and $C'' = L_1L_2L_3$. So

$$\begin{aligned} C' \bullet C &= 3(L \bullet C) = 3(P_1 + P_2 + P_3) = 3P_1 + 3P_2 + 3P_3 \\ C'' \bullet C &= L_1 \bullet C + L_2 \bullet C + L_3 \bullet C = 3P_1 + 3P_2 + 2P_3 + P_3'. \end{aligned}$$

By Proposition 3 in §5.6, $P_3 = P_3'$.

□

Problem 5.35.

Let C be any irreducible cubic, or any cubic without multiple components, C° the set of simple points of $C, O \in C^\circ$. Show that the same definition as in the nonsingular case makes C° into an abelian group.

Proof.

(1) It suffices to show that $\varphi(C^\circ \times C^\circ) \subseteq C^\circ$.

(2) Let C be a any irreducible cubic. Given any $P_1, P_2 \in C^\circ$. Then there is a unique line L such that $L \bullet C = P_1 + P_2 + P_3$ for some $P_3 \in C$. (If $P_1 = P_2$, L is the tangent to C at P.) So it suffices to show that $P_3 \in C^\circ$.

(3) Might assume $P_3 \neq P_1, P_3 \neq P_2$. Bézout's theorem shows that

$$\sum_P I(P, L \cap C) = 3.$$

So $I(P_3, L \cap C) = 1$ whenever $P_1 = P_2$ or $P_1 \neq P_2$. Therefore, $P_3 \in C^\circ$ (Property (5) in §3.3).

□

Problem 5.36.

Let C be an irreducible cubic, O a simple point on C giving rise to the addition $\oplus$ on the set C° of simple points. Suppose another O' gives rise to an addition $\oplus'$. Define $\alpha : (C, O, \oplus) \to (C, O', \oplus')$ by $\alpha(P) = \varphi(\varphi(O, O'), P)$. Show that α is a group isomorphism. So the structure of the group is independent of the choice of O.

Proof.

(1) *Show that α is a group homomorphism, that is, $\alpha(P \oplus Q) = \alpha(P) \oplus' \alpha(Q)$ for all $P, Q \in C^\circ$.* The definition is well-defined (Problem 5.35).

(2) Similar to Proposition 4 in §5.6. Let

$$\begin{aligned} L_1 \bullet C &= P + Q + R', \\ M_1 \bullet C &= R' + O + R, && (R = P \oplus Q) \\ L_2 \bullet C &= O + O' + O'' \\ L_3 \bullet C &= R + O'' + T. && (T = \alpha(P \oplus Q)) \end{aligned}$$

Let

$$\begin{aligned} M_2 \bullet C &= P + O'' + P' && (P' = \alpha(P)) \\ M_3 \bullet C &= Q + O'' + Q' && (Q' = \alpha(Q)) \\ L_4 \bullet C &= P' + Q' + S \\ M_4 \bullet C &= S + O' + T'. && (T' = \alpha(P) \oplus' \alpha(Q)) \end{aligned}$$

Let $f = L_1L_2L_3L_4$, $f' = M_1M_2M_3M_4$. Apply Problem 5.42 on C° to get $T = T'$ or $\alpha(P \oplus Q) = \alpha(P) \oplus' \alpha(Q)$.

(3) Define $\beta : (C, O', \oplus') \to (C, O, \oplus)$ by $\beta(P) = \varphi(\varphi(O', O), P)$. β is a group homomorphism too. By step (1) in the proof of Problem 5.37(b), $\alpha \circ \beta = 1_{(C,O',\oplus')}$ and $\beta \circ \alpha = 1_{(C,O,\oplus)}$. Hence α is a group isomorphism.

□

Problem 5.37.

In Proposition 4, suppose O is a flex on C.

(a) *Show that the flexes form a subgroup of C; as an abelian group, this subgroup is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

(b) *Show that the flexes are exactly the elements of order three in the group. (i.e., exactly those elements P such that $P \oplus P \oplus P = O$).*

(c) *Show that a point P is of order two in the group if and only if the tangent to C at P passes through O.*

(d) *Let $C = y^2z - x(x - z)(x - \lambda z)$, $\lambda \neq 0, 1$, $O = [0 : 1 : 0]$. Find the points of order two.*

(e) *Show that the points of order two on a nonsingular cubic form a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(f) *Let C be a nonsingular cubic, $P \in C$. How many lines through P are tangent to C at some point $Q \neq P$? (The answer depends on whether P is a flex.)*

Proof of (a).

(1) *Let G be the set of all flexes of C. Show that G is a subgroup of C.* $G \neq \varnothing$ since $O \in G$. Given any two flexes $P, Q \in C$, we have

$$\begin{aligned} -P &= \varphi(O, P) \in G \\ P \oplus Q &= \varphi(O, \varphi(P, Q)) \in G \end{aligned}$$

by using Problem 5.34 three times. Thus G is a subgroup of C.

(2) *Show that $P \oplus P \oplus P = O$ for all flexes of C.* Let L be the tangent line to C at P. By step (2) in the proof of Problem 5.34, P is a flex in C if and only if $L \bullet C = 3P$. Hence $\varphi(P, P) = P$,

$$P \oplus P = \varphi(O, \varphi(P, P)) = \varphi(O, P) = -P.$$

(3) Note that $|G| = 9$ since a nonsingular cubic C has 9 nine ordinary flexes (Corollary (2) to Problem 5.23). So G is an abelian group of order 9 ((1)). So $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (the fundamental theorem of finite abelian groups and (2)).

□

Proof of (b).

(1) Let L be one line such that $L \bullet C = P_1 + P_2 + P_3$. Then L is uniquely determined by P_1 and P_2. (If $P_1 \neq P_2$, nothing to do. If $P_1 = P_2$, the tangent line is unique since $P_1 = P_2$ is simple.)

(2) Might assume $P \neq O$. (O is of order 1.) So

$$\begin{aligned}
& P \oplus P \oplus P = O \\
\iff & P \oplus P = -P \\
\iff & \varphi(O, \varphi(P, P)) = \varphi(O, P) \\
\iff & \varphi(O, \varphi(O, P)) = \varphi(P, P) && ((1)) \\
\iff & P = \varphi(P, P) \\
\iff & L \bullet C = 3P \text{ where } L \text{ is the tangent line to } C \text{ at } P \\
\iff & P \text{ is a flex in } C. && \text{(Problem 5.34)}
\end{aligned}$$

□

Proof of (c).

(1) $P \neq O$ since O is of order 1.

(2) So

$$\begin{aligned}
& P \oplus P = O \\
\iff & \varphi(O, \varphi(P, P)) = O \\
\iff & \varphi(O, O) = \varphi(P, P) && ((b)(1)) \\
\iff & O = \varphi(P, P) && (O\text{: flex}) \\
\iff & \text{The tangent line to } C \text{ at } P \text{ passing through } O.
\end{aligned}$$

□

Proof of (d).

(1) Problem 5.4 shows that the tangent line L to C at $P := [a : b : c] \in C$ is

$$L = \frac{\partial C}{\partial x}(P)x + \frac{\partial C}{\partial y}(P)y + \frac{\partial C}{\partial z}(P)z.$$

Might assume $P \neq O$. By (c), $O \in L$ and thus $\frac{\partial C}{\partial y}(P) = 2bc = 0$. $b = 0$ or $c = 0$.

(2) The case $b = 0$. $P \in C$ implies that $a(a - c)(a - \lambda c) = 0$. So $P = [0 : 0 : 1], [1 : 0 : 1], [\lambda : 0 : 1]$. It is easy to verify that $P \oplus P = O$ and $P \neq O$.

(3) The case $c = 0$. $P = [0 : 1 : 0] = O$.

(4) By (2)(3), the points of order two (including O) are

$$[0 : 0 : 1], [1 : 0 : 1], [\lambda : 0 : 1], [0 : 1 : 0].$$

□

Proof of (e).

(1) *Let H be the set of all points $P \in C$ with $P \oplus P = O$. Show that H is a subgroup of C.* $H \neq \varnothing$ since $O \in H$. Given any two $P, Q \in H$, we have

$$\begin{aligned}(-P) \oplus (-P) &= P \oplus P = O,\\ (P \oplus Q) \oplus (P \oplus Q) &= (P \oplus P) \oplus (Q \oplus Q) = O \oplus O = O.\end{aligned}$$

So H is a subgroup of C.

(2) Note that the nonsingularity is preserved under projectively equivalence. By Problems 5.21, 5.24, 5.10 and 5.11, it suffices to assume that $C = y^2z - x(x - z)(x - \lambda z)$.

(3) By (d) and the fundamental theorem of finite abelian groups, $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

□

Proof of (f).

(1) To find lines through P are tangent to C at some point $Q \in C$, it suffices to find $Q \in C$ satisfying $\varphi(Q, Q) = P$. Construct an abelian group $(C, P, \oplus)$ on C.

(2) The case $P \in C$ is a flex. (c)(e) implies that there are 4 lines through P are tangent to C at some point $Q \in C$. Since $\varphi(P, P) = P$, there are 3 lines through P are tangent to C at some point $Q \neq P$.

(3) The case $P \in C$ is not a flex. Construct another abelian group $(C, P', \oplus')$ on C where $P' \in C$ is any flex. (The existence of P' is guaranteed by (a).) By Problem 5.36, the map

$$\alpha : (C, P, \oplus) \to (C, P', \oplus')$$

defined by $\alpha(Q) = \varphi(\varphi(P, P'), Q)$ is an isomorphism. Here $\alpha^{-1}(Q') = \varphi(\varphi(P, P'), Q')$.

(4) By (2), there are 4 points $Q_i' \in C$ $(i = 1, 2, 3, 4)$ such that

$$Q_i' \oplus' Q_i' = P'.$$

Take α^{-1} on the both sides to get

$$Q_i \oplus Q_i = P,$$

where $Q_i := \alpha^{-1}(Q_i')$. Note that each $Q_i \neq P$ since P is not a flex. Therefore, there are 4 lines through P are tangent to C at some point $Q \in C$.

□

Problem 5.38.

Let C be a nonsingular cubic given by the equation

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

$O = [0 : 1 : 0]$. *Let $P_i = [x_i : y_i : 1]$, $i = 1, 2, 3$, and suppose $P_1 \oplus P_2 = P_3$. Let*

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2ax_1 + b}{2y_1} & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0. \end{cases}$$

Let $\mu = y_i - \lambda x_i$, $i = 1, 2$. Show that

$$\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2 \\ y_3 = -\lambda x_3 - \mu. \end{cases}$$

This gives an explicit method for calculating in the group.

Proof.

(1) Suppose $x_1 \neq x_2$. Let the line L_1 passing throught P_1 and P_2. Since $L_1 \subseteq U_3 = \{[x : y : z] : z \neq 0\}$, we dehomogenize C (resp. L_1) to get

$$C_* : y^2 = x^3 + ax^2 + bx + c,$$
$$(L_1)_* : y - y_1 = \lambda(x - x_1).$$

Here $\lambda = \frac{y_2-y_1}{x_2-x_1}$. Write $y = \lambda(x-x_1)+y_1 = \lambda x + \mu$ where $\mu = y_1 - \lambda x_1$. (μ is also equal to $y_2 - \lambda x_2$.) So

$$\begin{aligned}
&(\lambda x+\mu)^2 = x^3 + ax^2 + \text{lower terms}\\
\iff &x^3 + (a-\lambda^2)x^2 + \text{lower terms} = 0\\
\iff &x_1 + x_2 + x_3' = \lambda^2 - a \qquad \text{(Vieta's formulas)}\\
\iff &\alpha = \lambda^2 - a - x_1 - x_2, \beta = \lambda\alpha + \mu.
\end{aligned}$$

Here $P_3' = [\alpha : \beta : 1]$ is the third point on $L_1 \cap C$. ($L_1 \bullet C = P_1 + P_2 + P_3'$.)

(2) Suppose $P_1 = P_2$ and $y_1 \neq 0$. Write $C = y^2z - x^3 - ax^2z - bxz^2 - cz^3$. By Problem 5.4, the tangent line L_1 at $P_1 = P_2$ is

$$L_1 : y = \lambda x + \frac{bx_1 + 2c}{2y_1}z.$$

(Note that $\lambda = \frac{3x_1^2+2ax_1+b}{2y_1}$ and $P_1 \in C$.) In particular, $O \notin L_1$. By dehomogenizing C and replacing y by $\lambda x + \frac{bx_1+2c}{2y_1}$, we have

$$\begin{aligned}
&\left(\lambda x + \frac{bx_1+2c}{2y_1}\right)^2 = x^3 + ax^2 + \text{lower terms}\\
\iff &x^3 + (a-\lambda^2)x^2 + \text{lower terms} = 0\\
\iff &x_1 + x_2 + x_3' = \lambda^2 - a \qquad \text{(Vieta's formulas)}\\
\iff &\alpha = \lambda^2 - a - x_1 - x_2, \beta = \lambda\alpha + \mu.
\end{aligned}$$

Here $\mu = y_1 - \lambda x_1$ and $P_3' = [\alpha : \beta : 1]$ is the third point on $L_1 \cap C$. ($L_1 \bullet C = P_1 + P_2 + P_3'$.)

(3) In any case of (1) or (2), we let the line L_2 passing throught P_3' and O. $L_2 = x - \alpha z$. So

$$\begin{aligned}
&y^2z = \alpha^3z^3 + a\alpha^2z^3 + b\alpha z^3 + cz^3 = \beta^2 z\\
\iff &(y+\beta)(y-\beta)z = 0\\
\iff &P_3 = [\alpha : -\beta : 1] = [\lambda^2 - a - x_1 - x_2 : -\lambda x_3 - \mu : 1].
\end{aligned}$$

Here P_3 is the third point on $L_2 \cap C$. ($L_2 \bullet C = P_3' + O + P_3$.)

□

Problem 5.39.

(a) *Let $C = y^2z - x^3 - 4xz^2$, $O = P_0 = [0:1:0]$, $P_1 = [2:4:1]$, $P_2 = [0:0:1]$ and $P_3 = [2:-4:1]$. Show that $G = \{P_0, P_1, P_2, P_3\}$ form a subgroup of C that is cyclic of order 4.*

(b) *Let* $C = y^2z - x^3 + 43xz^2 - 166z^3$. *Let* $O = [0 : 1 : 0]$, $P = [3 : 8 : 1]$. *Show that* P *is an element of order* 7 *in* C.

Proof of (a).

(1) A direct calculation shows that

$$P_i \oplus P_j = P_{i+j}$$

for all $i, j \in \mathbb{Z}/4\mathbb{Z}$ (Problem 5.38). Hence G is a subgroup of C.

(2) Note that $G \xrightarrow{\sim} \mathbb{Z}/4\mathbb{Z}$ (by $P_i \mapsto i$) is an isomorphism. So G is a cyclic group of order 4.

□

Proof of (b).

(1) A direct calculation shows that $2P = P \oplus P = [-5 : -16 : 1]$, $4P = 2P \oplus 2P = [11 : 32 : 1]$, and $8P = 4P \oplus 4P = [3 : 8 : 1] = P$ (Problem 5.38).

(2) Since $8P = P$, $7P = O$. The order of P is 1 or 7 (since 7 is a prime integer). Note that $P \neq O$. Therefore, P is of order 7.

□

Problem 5.40. (Rational point)

Let k_0 *be a subfield of* k. *If* V *is an affine variety,* $V \subseteq \mathbf{A}^n(k)$, *a point* $P = (a_1, \ldots, a_n) \in V$ *is* ***rational*** *over* k_0, *if each* $a_i \in k_0$. *If* $V \subseteq \mathbf{P}^n(k)$ *is projective, a point* $P \in V$ *is rational over* k_0 *if for some homogeneous coordinates* $(a_1, \ldots, a_{n+1})$ *for* P, *each* $a_i \in k_0$.

A curve f *of degree* d *is said to be emphrational over* k_0 *if the corresponding point in* $\mathbf{P}^{\frac{d(d+3)}{2}}$ *is rational over* k_0.

Suppose a nonsingular cubic C *is rational over* k_0. *Let* $C(k_0)$ *be the set of points of* C *that are rational over* k_0.

(a) *If* $P, Q \in C(k_0)$, *show that* $\varphi(P, Q)$ *is in* $C(k_0)$.

(b) *If* $O \in C(k_0)$, *show that* $C(k_0)$ *forms a subgroup of* C.

(If $k_0 = \mathbb{Q}$, $k = \mathbb{C}$, *this has important applications to number theory.)*

Proof of (a).

(1) If $P \neq Q$, then the line L passing through $P = [a_1 : a_2 : a_3]$ and $Q = [b_1 : b_2 : b_3]$ is

$$L : \{[\lambda a_1 + \mu b_1 : \lambda a_2 + \mu b_2 : \lambda a_3 + \mu b_3] : [\lambda : \mu] \in \mathbf{P}^2(k)\}.$$

Hence

$$C \cap L = C(\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2, \lambda a_3 + \mu b_3) := \widetilde{C}(\lambda, \mu).$$

(2) Note that $\deg(\widetilde{C}) = 3$ since $C \neq 0$ is nonsingular (and thus is irreducible by Problem 5.21). By Problem 5.7 or Bézout's theorem, $\widetilde{C}$ has exactly 3 zeros in $\mathbf{P}^1(k)$.

(3) Note that $\widetilde{C} \in k_0[\lambda, \mu]$ since $C \in k_0[x, y, z]$ and $P, Q \in \mathbf{P}^2(k_0)$. Since $P, Q \in \mathbf{P}^2(k_0)$, we apply Vieta's formulas on $\widetilde{C}$ to get the third point $\varphi(P, Q) \in \mathbf{P}^2(k_0)$ too.

(4) If $P = Q$, then the line L tangent to C at P is $\frac{\partial C}{\partial x}(P)x + \frac{\partial C}{\partial y}(P)y + \frac{\partial C}{\partial z}(P)z = 0$ (Problem 5.4). Define

$$[b_1 : b_2 : b_3] = \begin{cases} [a_1 : a_2 : a_3 + 1] & \text{if } \frac{\partial C}{\partial z}(P) = 0 \\ \left[a_1 + \frac{\partial C}{\partial y}(P) : a_2 - \frac{\partial C}{\partial x}(P) : a_3\right] & \text{otherwise.} \end{cases}$$

Note that $L \in k_0[x, y, z]$ and $[b_1 : b_2 : b_3] \in \mathbf{P}^2(k_0)$. Hence L has the same form as (1). The rest proof is the same as (2)(3).

□

Proof of (b). Since $O \in C(k_0)$ and $\varphi(C(k_0) \times C(k_0)) \subseteq C(k_0)$, $C(k_0)$ is a subgroup of C (as Problem 5.35). □

Problem 5.41.

Let C be a nonsingular cubic, O a flex on C. Let $P_1, \ldots, P_{3m} \in C$. Show that $P_1 \oplus \cdots \oplus P_{3m} = O$ if and only if there is a curve f of degree m such that $f \bullet C = \sum_{i=1}^{3m} P_i$. (Hint: Use induction on m. Let $L \bullet C = P_1 + P_2 + Q$, $L' \bullet C = P_3 + P_4 + R$, $L'' \bullet C = Q + R + S$, and apply induction to $S, P_5, \ldots, P_{3m}$; use Noether's theorem.)

Proof.

(1) Induction on m.

(2) Base case.

$$\begin{aligned} P_1 \oplus P_2 \oplus P_3 = O &\iff P_1, P_2, P_3 \text{ are collinear} \\ &\iff \exists \text{ a line } L \text{ such that } L \bullet C = P_1 + P_2 + P_3. \end{aligned}$$

(3) Inductive step. Let $L \bullet C = P_1 + P_2 + Q$, $L' \bullet C = P_3 + P_4 + R$, $L'' \bullet C = Q + R + S$. By (2), $O = P_1 \oplus P_2 \oplus Q = P_3 \oplus P_4 \oplus R = Q \oplus R \oplus S$. Hence

$$S = P_1 \oplus P_2 \oplus P_3 \oplus P_4.$$

Hence

$$\begin{aligned}
& P_1 \oplus \cdots \oplus P_{3m} = O \\
\Longleftrightarrow\ & S \oplus P_5 \oplus P_6 \cdots \oplus P_{3m} = O \\
\Longleftrightarrow\ & \exists\ f' \text{ of degree } m-1 \text{ such that } f' \bullet C = S + \sum_{i=5}^{3m} P_i \\
\Longrightarrow\ & (LL'f') \bullet C \geq L'' \bullet C \\
\Longrightarrow\ & \exists\ f \text{ of degree } m \text{ such that } f \bullet C = \sum_{i=1}^{3m} P_i \\
\Longrightarrow\ & (L''f) \bullet C \geq (LL') \bullet C \\
\Longrightarrow\ & \exists\ f' \text{ of degree } m-1 \text{ such that } f' \bullet C = S + \sum_{i=5}^{3m} P_i.
\end{aligned}$$

(4) Since both the base case and the inductive step have been proved as true, by mathematical induction the statement holds for any m.

□

Problem 5.42.

Let C be a nonsingular cubic, f, f' curves of degree m such that $f \bullet C = \sum_{i=1}^{3m} P_i$, $f' \bullet C = \sum_{i=1}^{3m-1} P_i + Q$. Show that $P_{3m} = Q$.

Proof.

(1) Similar to Proposition 3 in §5.6.

(2) Let L be a line through P_{3m} that doesn't pass through Q; $L \bullet C = P_{3m} + R + S$. Then

$$\begin{aligned}
(Lf') \bullet C &= L \bullet C + f' \bullet C \\
&= (P_{3m} + R + S) + \left(\sum_{i=1}^{3m-1} P_i + Q \right) \\
&= \sum_{i=1}^{3m} P_i + Q + R + S \\
&= f \bullet C + Q + R + S,
\end{aligned}$$

so there is a line L' such that $L' \bullet C = Q + R + S$ (max Noether's fundamental theorem). But then $L' = L$ and so $P_{3m} = Q$.

□

Problem 5.43. (Sextatic point)

For which points P on a nonsingular cubic C does there exist a nonsingular conic that intersects C only at P?

Proof.

(1) *We say P a sextatic point of C if there is a nonsingular conic K that intersects C six times at P. Suppose O is a flex on C. Show that the followings are equivalent:*

   (i) *P is a sextatic point of C.*

   (ii) *$6P = O$ and $3P \neq O$.*

   (iii) *The tangent at P contains a flex of C not equal to P.*

   (iv) *P has order 2 or 6.*

(2) (ii) $\iff$ (iii) $\iff$ (iv) is followed by Problem 5.37. To prove (i) $\iff$ (ii), it suffices to show that

   $(*)$ *$6P = O \iff$ there is a conic K that intersects C six times at P, which is followed by Problem 5.41.*

   $(**)$ *$3P = 0 \iff K$ is reducible.*

(3) Note that

$$\begin{aligned} & K = L_1 L_2 \text{ for some lines } L_1, L_2 \\ \Longrightarrow\ & C \bullet K = C \bullet (L_1 L_2) = C \bullet L_1 + C \bullet L_2 = 6P \\ \Longrightarrow\ & C \bullet L_1 = C \bullet L_2 = 3P \\ \Longrightarrow\ & 3P = O. \qquad \text{(Problem 5.41)} \end{aligned}$$

and

$$\begin{aligned} & 3P = O \\ \Longrightarrow\ & C \bullet L = 3P \text{ for some line } L \qquad \text{(Problem 5.41)} \\ \Longrightarrow\ & C \bullet K = C \bullet L^2 = 6P \\ \Longrightarrow\ & K = L^2 \text{ is reducible (up to a nonzero constant).} \end{aligned}$$

Therefore, the statement $(**)$ is established (and thus part (a) holds).

(4) There are 27 sextatic points of C by Problem 5.37(a)(c)(e) and (iii). Note that $G = \{$ flex points $+$ sextatic points $\}$ is a subgroup of C with $|G| = 27 + 9 = 36$. So

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

□

Chapter 6: Varieties, Morphisms, and Rational Maps

6.1. The Zariski Topology

Problem 6.1.*

Let $Z \subseteq Y \subseteq X$, X a topological space. Give Y the induced topology. Show that the topology induced by Y on Z is the same as that induced by X on Z.

Proof.

(1) Take any open set U in Z whose topology is induced by Y. $U = Z \cap B$ for some open subset B in Y. Since Y is induced by X. $A = Y \cap A$ for some open subset A in X. Hence,

$$U = Z \cap B = Z \cap (Y \cap A) = Z \cap A,$$

that is, U is also an open set in Z whose topology is induced by X.

(2) Conversely, take any open set U in Z whose topology is induced by X. $U = Z \cap A$ for some open subset A in X. Hence

$$U = Z \cap A = Z \cap (Y \cap A),$$

where $Y \cap A$ is an open set in Y whose topology is induced by X. So U is also an open set in Z whose topology is induced by Y.

□

Problem 6.2.*

(a) *Let X be a topological space, $X = \bigcup_{\alpha \in \mathscr{A}} U_\alpha$, U_α open in X. Show that a subset W of X is closed if and only if each $W \cap U_\alpha$ is closed (in the induced topology) in U_α.*

(b) *Suppose similarly $Y = \bigcup_{\alpha \in \mathscr{A}} V_\alpha$, V_α open in Y, and suppose $f : X \to Y$ is a mapping such that $f(U_\alpha) \subseteq V_\alpha$. Show that f is continuous if and only if the restriction of f to each U_α is a continuous mapping from U_α to V_α.*

Proof of (a).

(1) *Show that a subset E of X is open if and only if each $E \cap U_\alpha$ is open (in the induced topology) in U_α.* One way is nothing to do. Conversely,

$$E = E \cap X = E \cap \left(\bigcup_{\alpha \in \mathscr{A}} U_\alpha \right) = \bigcup_{\alpha \in \mathscr{A}} (E \cap U_\alpha)$$

is a union of open sets, which is open again.

(2) Let $E = X - W$ be an open set in X. Note that

$$E \cap U_\alpha = (X - W) \cap U_\alpha = X \cap U_\alpha - W \cap U_\alpha = U_\alpha - W \cap U_\alpha.$$

Hence the conclusion holds.

(3) It motivates the local study of topologies.

□

Proof of (b).

(1) ($\Longrightarrow$) Suppose f is continuous. It suffices to show that $(f|_{U_\alpha})^{-1}(W)$ is closed in U_α for every closed set W in V_α. Write $W = W_\alpha \cap V_\alpha$ where W_α is closed in Y. Note that

$$\begin{aligned} (f|_{U_\alpha})^{-1}(W) &= f^{-1}(W) \cap U_\alpha \\ &= f^{-1}(W_\alpha \cap V_\alpha) \cap U_\alpha \\ &= f^{-1}(W_\alpha) \cap f^{-1}(V_\alpha) \cap U_\alpha \\ &= f^{-1}(W_\alpha) \cap U_\alpha. \qquad (f^{-1}(V_\alpha) \supseteq U_\alpha) \end{aligned}$$

Since $f^{-1}(W_\alpha)$ is closed in X, $(f|_{U_\alpha})^{-1}(W)$ is closed in U_α.

(2) ($\Longleftarrow$) Conversely, suppose $f|_{U_\alpha}$ is a continuous mapping from U_α to V_α. It suffices to show that $f^{-1}(W)$ is closed for every closed set W in Y. Note that $W \cap V_\alpha$ is closed in each V_α. By the continunity of $f|_{U_\alpha}$,

$$\begin{aligned} (f|_{U_\alpha})^{-1}(W \cap V_\alpha) &= f^{-1}(W \cap V_\alpha) \cap U_\alpha \\ &= f^{-1}(W) \cap f^{-1}(V_\alpha) \cap U_\alpha \\ &= f^{-1}(W) \cap U_\alpha \end{aligned}$$

is closed in U_α. Since $\alpha \in \mathscr{A}$ is arbitrary and $X = \bigcup_{\alpha \in \mathscr{A}} U_\alpha$, $f^{-1}(W)$ is closed in X by (a).

□

Problem 6.3.*

(a) *Let V be an affine variety, $f \in \Gamma(V)$. Considering f as a mapping from V to $k = \mathbf{A}^1$, show that f is continuous.*

(b) *Show that any polynomial map of affine varieties is continuous.*

Proof of (a).

(1) It is a special case of (b) since f itself is a polynomial map from V to $\mathbf{A}^1$.

(2) By Problem 6.6, it suffices to show that

$$f^{-1}(\lambda) = \{P \in V : f(P) = \lambda\}$$

is closed for any $\lambda \in k$. Note that $f^{-1}(\lambda) = V \cap V(f - \lambda = 0)$ is closed.

□

Proof of (b).

(1) Let $V \subseteq \mathbf{A}^n$, $W \subseteq \mathbf{A}^m$ be affine varieties. Let φ be a polynomial map from V to W.

(2) Problem 2.7 shows that $\varphi^{-1}(X)$ is closed for every closed subset X of W. Hence, φ is continuous.

□

Problem 6.4.*

Let $U_i \subseteq \mathbf{P}^n$, $\varphi_i : \mathbf{A}^n \to U_i$ as in Chapter 4. Give U_i the topology induced from $\mathbf{P}^n$.

(a) *Show that φ_i is a homeomorphism.*

(b) *Show that a set $W \subseteq \mathbf{P}^n$ is closed if and only if each $\varphi_i^{-1}(W)$ is closed in $\mathbf{A}^n$, $i = 1, \ldots, n+1$.*

(c) *Show that if $V \subseteq \mathbf{A}^n$ is an affine variety, then the projective closure V^* of V is the closure of $\varphi_{n+1}(V)$ in $\mathbf{P}^n$.*

Proof of (a).

(1) Note that φ_i is one-to-one and onto. It suffices to show that φ_i and φ_i^{-1} are continuous.

(2) *Show that φ_i is continuous.* Suppose $W \subseteq \mathbf{P}^n$ is closed in U_i. Let $\overline{W}$ be its closure in $\mathbf{P}^n$. $\overline{W} = V(I)$ for some homogeneous ideal I in $k[x_1, \ldots, x_{n+1}]$. Thus $\varphi_i^{-1}(W) = V(I_*)$ (w.r.t. x_i) is closed.

(3) *Show that φ_i^{-1} is continuous.* Suppose $V \subseteq \mathbf{A}^n$ is closed. Proposition 3 in §4.3 gives us $\varphi_i(V) = V^* \cap U_i$ is closed in U_i.

□

Proof of (b).

$$
\begin{aligned}
& W \subseteq \mathbf{P}^n \text{ is closed} \\
\Longleftrightarrow\ & W \text{ is closed in } U_i \text{ for each } i && \text{(Problem 6.2.)} \\
\Longleftrightarrow\ & \varphi_i^{-1}(W) \text{ is closed in } \mathbf{A}^n \text{ for each } i. && (\varphi_i \text{ is a homeomorphism})
\end{aligned}
$$

□

Proof of (c). By Proposition 3 in §4.3, the projective closure V^* of V is the smallest algebraic set in $\mathbf{P}^n$ containing $V = \varphi_{n+1}(V)$. That is the same as the definition of the closure of V. □

Problem 6.5.

Any infinite subset of an irreducible plane curve V is dense in V. Any one-to-one mapping from one irreducible plane curve onto another is a homeomorphism.

Proof.

(1) *Show that any infinite subset of an irreducible plane curve V is dense in V.* It is not true if V is reducible.

  (a) Let W be the closure of an infinite subset of a plane curve V. $W \subseteq V$.

  (b) By Corollary 2 to Proposition 2 in §1.6 or Problem 4.23, W is a finite union of points and irreducible plane curves. By Proposition 2 in §1.6 or Problem 5.7, each of these plane curves intersects V in finite number of points, or is equal to V.

  (c) Since W is infinite, $W = V$. That is, any infinite subset of an irreducible plane curve is dense in V.

(2) *Show that any one-to-one mapping from one irreducible plane curve onto another is a homeomorphism.*

  (a) Let $\varphi : f \to g$ be a bijective mapping. It suffices to show that φ is continuous.

(b) The closed sets in $V(g)$ are $V(g)$ itself and points (by the same argument in (1)). $\varphi^{-1}(V(g)) = V(f)$ is closed. Given any point $Q \in V(g)$, $\varphi^{-1}(Q) = P$ is closed for some point $P \in V(f)$ since φ is bijective. So, φ is continuous.

(c) Similarly, φ^{-1} is continuous too. Hence, φ is homeomorphic.

□

Problem 6.6.*

Let X be a topological space, $f : X \to \mathbf{A}^n$ a mapping. Then f is continuous if and only if for each hypersurface $V = V(f)$ of $\mathbf{A}^n$, $f^{-1}(V)$ is closed in X. A mapping $f : X \to k = \mathbf{A}^1$ is continuous if and only if $f^{-1}(\lambda)$ is closed for any $\lambda \in k$.

Proof.

(1) We give a stronger version of the statement. *Show that f is continuous iff $f^{-1}(V)$ is closed for each irreducible hypersurface $V = V(f) \subseteq \mathbf{A}^n$.* One way is nothing to do.

(2) Conversely, note that $f^{-1}(\mathbf{A}^n) = X$ and $f^{-1}(\varnothing) = \varnothing$ are closed. Now given any proper closed set V in $\mathbf{A}^n$, V is of the form

$$V = V(f_1, \ldots, f_r) = V(f_1) \cap \cdots \cap V(f_r),$$

where each f_i is irreducible polynomial. Hence,

$$f^{-1}(V) = f^{-1}(V(f_1)) \cap \cdots \cap f^{-1}(V(f_r))$$

is a union of closed sets in a topological space X, which is closed again.

(3) f is continuous iff $f^{-1}(V)$ is closed for each irreducible hypersurface $V = V(f) \subseteq \mathbf{A}^1$ (by (1)). Note that the irreducible hypersurface f in $\mathbf{A}^1$ is $f = x - \lambda$ for some $\lambda \in k$. So f is continuous iff

$$f^{-1}(V) = f^{-1}(x - \lambda) = f^{-1}(\lambda)$$

is closed for each $\lambda \in k$.

□

Problem 6.7.*

Let V be an affine variety, $f \in \Gamma(V)$.

(a) *Show that $V(f) = \{P \in V : f(P) = 0\}$ is a closed subset of V, and $V(f) \neq V$ unless $f = 0$.*

(b) *Suppose U is a dense subset of V and $f(P) = 0$ for all $P \in U$. Then $f = 0$.*

Proof of (a).

(1) Write $f = \widetilde{f} + I(V) \in \Gamma(V)$ for some $\widetilde{f} \in k[x_1, \ldots, x_n]$. Note that $f(P) = \widetilde{f}(P)$ is well-defined for any $P \in V$. Thus,

$$\begin{aligned} V(f) &= \{P \in V : f(P) = 0\} \\ &= \{P \in V : \widetilde{f}(P) = 0\} \\ &= V \cap \{P \in \mathbf{A}^n : \widetilde{f}(P) = 0\} \\ &= V \cap V(\widetilde{f}) \end{aligned}$$

is closed in V.

(2) Also,

$$\begin{aligned} V(f) = V &\iff V \cap V(\widetilde{f}) = V \\ &\iff V(\widetilde{f}) \supseteq V \\ &\iff \widetilde{f} \in I(V) \\ &\iff f = 0 \in \Gamma(V). \end{aligned}$$

□

Proof of (b).

(1) Since $V(f) \supseteq U$ (by assumption) and $V(f)$ is closed (by (a)), $V(f) \supseteq \overline{U}$ by the definition of the closure of U.

(2) Since U is dense in V, $\overline{U} = V$. Thus $V \supseteq V(f) \supseteq \overline{U} = V$ or $V(f) = V$. By (a), $f = 0$.

□

Problem 6.8.*

Let U be an open subset of a variety V, $z \in k(V)$. Suppose $z \in \mathscr{O}_P(V)$ for all $P \in U$. Show that $U_z = \{P \in U : z(P) \neq 0\}$ is open, and that the mapping from U to $k = \mathbf{A}^1$ defined by $P \mapsto z(P)$ is continuous.

Proof.

(1) *Show that U_z is open.* By Problem 6.1, it suffices to show that U_z is open in U, or show that

$$W_z := U - U_z = \{P \in U : z(P) = 0\}$$

is closed in U.

(2) Write $z = f/g$ where $f, g \in \Gamma(V)$, $g(P) \neq 0$ for all $P \in V$. $z(P) = 0$ if and only if $f(P) = 0$ on V. Hence,

$$W_z = \{P \in U : f(P) = 0\} = U \cap \{P \in V : f(P) = 0\}$$

is closed in U (Problem 6.7(a)).

(3) *Show that the mapping $\varphi : U \to k = \mathbf{A}^1$ defined by $\varphi : P \mapsto z(P)$ is continuous.* By Problem 6.6, it suffices to show that $\varphi^{-1}(\lambda)$ is closed in U for any $\lambda \in k$.

(4) Note that $z - \lambda \in \mathscr{O}_P(V)$ for all $P \in V$. Hence,

$$\varphi^{-1}(\lambda) = \{P \in U : z(P) = \lambda\} = \{P \in U : (z - \lambda)(P) = 0\} = W_{z-\lambda}$$

is closed in U by (2).

□

6.2. Varieties

Problem 6.9.

Let $X = \mathbf{A}^2 - \{(0,0)\}$, an open subvariety of $\mathbf{A}^2$. Show that $\Gamma(X) = \Gamma(\mathbf{A}^2) = k[x, y]$.

Proof.

(1) Let $z = f/g \in \Gamma(X)$ be a regular function on X. So $f = 0$ (nothing to do) or $g(P) \neq 0$ for all $P \in X = \mathbf{A}^2 - \{(0,0)\}$.

(2) As $V(g)$ is contained in a finite set $\{(0,0)\}$, g is a nonzero constant. Therefore, $z \in k[x, y] = \Gamma(\mathbf{A}^2)$ (Problem 1.4).

□

Problem 6.10.*

Let U be an open subvariety of a variety X, Y a closed subvariety of U. Let $\overline{Y}$ be the closure of Y in X. Show that

(a) *$\overline{Y}$ is a closed subvariety of X.*

(b) *Y is an open subvariety of $\overline{Y}$.*

Proof of (a).

(1) It suffices to show that $\overline{Y}$ is irreducible if Y is irreducible (since $\overline{Y}$ is closed in X already).

(2) (Reductio ad absurdum) If $\overline{Y}$ were reducible, there are two closed sets Y_1 and Y_2 such that $\overline{Y} \subseteq Y_1 \cup Y_2$ and $\overline{Y} \not\subseteq Y_1, Y_2$.

(3) *Show that $Y \subseteq \overline{Y} \subseteq Y_1 \cup Y_2$ and $Y \not\subseteq Y_1, Y_2$ if $\overline{Y}$ were reducible.* If not, might assume that $Y \subseteq Y_1$. Take closure to get $\overline{Y} \subseteq \overline{Y_1} = Y_1$ (since Y_1 is closed), contrary to the assumption.

(4) Therefore, Y is reducible, a contradiction.

□

Proof of (b).

(1) It suffices to show that $Y = \overline{Y} \cap X$.

(2) $Y \subseteq \overline{Y} \cap X$ is trivial.

(3) Conversely, write $Y = \widetilde{Y} \cap X$ for some closed set $\widetilde{Y}$ in X. $\widetilde{Y} \supseteq \overline{Y}$ since $\overline{Y}$ is the smallest closed set containing Y. So $Y = \widetilde{Y} \cap X \supseteq \overline{Y} \cap X$.

□

Problem 6.11. (Noetherian topological space)

(a) *Show that every family of closed subsets of a variety has a minimal member.*

(b) *Show that if a variety is a union of a collection of open subsets, it is a union of a finite number of these subsets. (All varieties are **quasi-compact**.)*

Proof of (a).

(1) Similar to the proof of Proposition 1 in §6.2, we may assume that X is an affine variety in $\mathbf{A}^N$.

(2) By Problem 1.38, there is a natural one-to-one correspondence between closed subsets of X and radical ideals in $k[x_1, \ldots, x_N]/I(X)$.

(3) Note that $I(X)$ is finitely generated (by the Hilbert basis theorem in §1.4). By Problem 1.22, $k[x_1, \ldots, x_N]/I(X)$ is Noetherian. Hence, Lemma in §1.5 shows that every family of closed subsets of X has a minimal member.

□

Proof of (b).

(1) Let $\{U_\alpha\}$ be an open covering of X. Let Σ be the family of closed sets being finite intersections of complements of members of $\{U_\alpha\}$, say

$$\bigcap_{\text{finite } \alpha} (X - U_\alpha) = X - \bigcup_{\text{finite } \alpha} U_\alpha.$$

By (a), Σ has a minimal member S. Now it suffices to show that $S = \varnothing$.

(2) By the minimality of S, $S \cap (X - U_\alpha) = S$ for all α. So $S \subseteq X - U_\alpha$, or $X - S \supseteq U_\alpha$ for all α. Hence,

$$X \supseteq X - S \supseteq \bigcup_{\text{all } \alpha} U_\alpha \supseteq X.$$

(3) Besides, we can show that X is a Noetherian topological space if every open subset of X is quasi-compact.

□

Problem 6.12.*

Let X be a variety, $z \in k(X)$. Show that the pole set of z is closed. If $z \in \mathcal{O}_P(X)$, there is a neighborhood U of z such that $z \in \Gamma(U)$; so $\mathcal{O}_P(X)$ is the union of all $\Gamma(U)$, where U runs through all neighborhoods of P.

Proof.

(1) Similar to the proof of Proposition 1 in §6.2, we may assume that X is an affine variety in $\mathbf{A}^N$.

(2) Proposition 2 in §2.4 shows that the pole set $V(J_z) \subseteq X$ of z is algebraic or closed.

(3) Given $z \in \mathcal{O}_P(X)$ ($P \notin V(J_z)$), there is an open neighborhood $U := X - V(J_z)$ of z such that $z \in \Gamma(U)$. So

$$\mathcal{O}_P(X) = \bigcup_U \Gamma(U)$$

where U runs through all neighborhoods of P.

□

6.3. Morphisms of Varieties

Problem 6.13.*

Let R be a domain with quotient field K, $f \neq 0$ in R. Let

$$R[1/f] = \{a/f^n : a \in R, n \in \mathbb{Z}\},$$

a subring of K.

(a) *Show that if $\varphi : R \to S$ is any ring homomorphism such that $\varphi(f)$ is a unit in S, then φ extends uniquely to a ring homomorphism from $R[1/f]$ to S.*

(b) *Show that the ring homomorphism from $R[x]/(xf-1)$ to $R[1/f]$ that takes x to $1/f$ is an isomorphism.*

Proof of (a).

(1) Suppose $\psi : R[1/f] \to S$ is a ring homomorphism such that $\psi = \varphi$ on R.

(2) To see ψ is uniquely determined, it suffices to show that $\psi(1/f)$ is uniquely determined (since ψ is a homomorphism).

(3) By $1 = f/f$, we have $\psi(1) = \psi(f)\psi(1/f)$. $\varphi(1) = \varphi(f)\psi(1/f)$ since $\psi = \varphi$ on R. Since $\varphi(1) = 1$ and $\varphi(f)$ is a unit in S, $\psi(1/f) = \varphi(f)^{-1}$ is uniquely determined.

(4) Lastly, it is easy to check $\psi(a/f^n) = \varphi(a)\varphi(f)^{-n}$ is a ring homomorphism.

□

Proof of (b).

(1) Define a ring homomorphism $\varphi : R \hookrightarrow R[x] \to S := R[x]/(xf-1)$ by

$$\varphi : r \mapsto r \mapsto \overline{r} = r + (xf - 1).$$

(2) Note that $\varphi(f) = \overline{f}$ is a unit in S since $\overline{x}\overline{f} = \overline{1}$ in S. By (a), φ extends uniquely to a ring homomorphism from $R[1/f]$ to S. In particular, $\varphi(1/f) = \varphi(f)^{-1} = \overline{x}$.

(3) *Show that φ is surjective.* Note that $\varphi(r) = \overline{r}$ for any $r \in R$ and $\varphi(1/f) = \overline{x}$. So, φ is surjective since φ is a ring homomorphism.

(4) *Show that φ is injective.* Suppose $\varphi(r/f^n) = 0$ for some $r/f^n \in R[1/f]$. May assume that $n > 0$. Write

$$rx^n = (xf - 1)g(x)$$

for some $g(x) \in R[x]$. It suffices to show that $g(x) = 0$. (Reductio ad absurdum) If $g(x) \neq 0$, then $r \neq 0$ and $\deg(g) = n - 1$. Take $x = 0$ in $rx^n = (xf - 1)g(x)$ to get $g(0) = 0$. So $g = xg_1$ for some $g_1 \in R[x]$ if $n > 1$. Hence,

$$rx^{n-1} = (xf - 1)g_1(x)$$

where $\deg g_1 = n-2$ if $n > 1$. Continue this process to get $g(x) = cx^{n-1} \in R[x]$ for some nonzero $c \in R$. So $rx = cfx - c$, which is absurd.

□

Problem 6.14.*

Let X, Y be varieties, $f : X \to Y$ a mapping. Let $X = \bigcup_\alpha U_\alpha$, $Y = \bigcup_\alpha V_\alpha$, with U_α, V_α open subvarieties, and suppose $f(U_\alpha) \subseteq V_\alpha$ for all α.

(a) *Show that f is a morphism if and only if each restriction $f_\alpha : U_\alpha \to V_\alpha$ of f is a morphism.*

(b) *If each U_α, V_α is affine, f is a morphism if and only if each $\widetilde{f}(\Gamma(V_\alpha)) \subseteq \Gamma(U_\alpha)$.*

Proof of (a).

(1) Problem 6.2 shows that f is continuous if and only if each restriction $f_\alpha : U_\alpha \to V_\alpha$ of f is continuous.

(2) Suppose $f : X \to Y$ is a morphism. The diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle i_X}\uparrow & & \uparrow{\scriptstyle i_Y} \\ U_\alpha & \xrightarrow{f_\alpha} & V_\alpha \end{array}$$

is commutative. By Problem 6.15(a), two inclusion maps i_X and i_Y are morphisms. By Problem 6.15(b), $f \circ i_X$ is a morphism. So it suffices to show that f_α is a morphism if $i_Y \circ f_\alpha$ is a morphism.

(3) Given a rational function $g \in \Gamma(V, \mathscr{O}_{V_\alpha})$ on an open set V of V_α. So $g \circ i_Y$ is a rational function in $\Gamma(V, \mathscr{O}_Y)$ on an open set V of Y (Problem 6.1).

Therefore, given any $y \in V$ we have

$$\begin{aligned}(\widetilde{f_\alpha}(g))(y) &= (g \circ f_\alpha)(y) \\ &= g(f_\alpha(y)) \\ &= g(i_Y(f_\alpha(y))) \\ &= (\widetilde{i_Y \circ f_\alpha}(g))(y).\end{aligned}$$

Hence $\widetilde{f_\alpha}$ pulls back g to a rational function $\widetilde{f_\alpha}(g)$ on U_α. Therefore, f_α is a morphism if f is a morphism.

(4) Suppose $f_\alpha : U_\alpha \to V_\alpha$ of f is a morphism for all α. Given a rational function $g \in \Gamma(V, \mathscr{O}_Y)$ on an open set V of Y. g is a rational function in $\Gamma(V \cap V_\alpha, \mathscr{O}_{V_\alpha})$ on an open set $V \cap V_\alpha$ of $V_\alpha \subseteq Y$ for all α. Therefore,

$$\widetilde{f_\alpha}(g) = g \circ f_\alpha \in \Gamma(f_\alpha^{-1}(V \cap V_\alpha), \mathscr{O}_{U_\alpha}) = \Gamma(f_\alpha^{-1}(V), \mathscr{O}_{U_\alpha})$$

for all α. So each restriction $g \circ f_\alpha = (g \circ f)|_{U_\alpha}$ is a rational function on U_α. Hence, $\widetilde{f}(g) = g \circ f$ is a rational function on $X = \bigcup_\alpha U_\alpha$.

□

Proof of (b).

(1) Part (a) and Proposition 2 in §6.2 show that f is a morphism if and only if each $\widetilde{f_\alpha}(\Gamma(V_\alpha)) \subseteq \Gamma(U_\alpha)$.

(2) Since f and f_α are the same on U_α, $\widetilde{f_\alpha} = \widetilde{f}$ on $\Gamma(V_\alpha)$.

□

Problem 6.15.*

(a) *If Y is an open or closed subvariety of X, the inclusion $i : Y \to X$ is a morphism.*

(b) *The composition of morphisms is a morphism.*

Proof of (a).

(1) The inclusion map is continuous in any topological space. ($i^{-1}(U) = U \cap Y$ is open in Y for every open set U of X.)

(2) For every open set U of X, if $f \in \Gamma(U, \mathscr{O}_X)$, then $\widetilde{i}(f)$ is a rational function defined on $U \cap Y = i^{-1}(U)$. Thus, $\widetilde{i}(f) = f \circ i \in \Gamma(i^{-1}(U), \mathscr{O}_Y)$. (The ring $\Gamma(i^{-1}(U), \mathscr{O}_Y)$ is well-defined since Y is a variety.)

□

Proof of (b).

(1) Given two morphisms $X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z$. The composition continuous functions $\psi \circ \varphi$ is continuous in any topological space.

(2) For every open set U of Z, if $f \in \Gamma(U, \mathscr{O}_Z)$, then $\widetilde{\psi}(f) = f \circ \psi \in \Gamma(\psi^{-1}(U), \mathscr{O}_Y)$. Note that $\psi^{-1}(U)$ is open since ψ is continuous. So

$$\widetilde{\varphi}(\widetilde{\psi}(f)) = f \circ \psi \circ \varphi \in \Gamma(\varphi^{-1}(\psi^{-1}(U)), \mathscr{O}_X).$$

Problem 2.6 gives that $\widetilde{\varphi} \circ \widetilde{\psi} = \widetilde{\psi \circ \varphi}$. Besides, $\varphi^{-1} \circ \psi^{-1} = (\psi \circ \varphi)^{-1}$. Therefore, $\widetilde{\psi \circ \varphi}$ pulls back rational functions to rational functions on every open set.

□

Problem 6.17.

(a) *Show that $\mathbf{A}^2 - \{(0,0)\}$ is not an affine variety (see Problem 6.9).*

(b) *The union of two open affine subvarieties of a variety may not be affine.*

Note that $\mathbf{A}^1 - \{0\}$ is an affine variety which is isomorphic to $V(1-xy) \subseteq \mathbf{A}^2$ (Proposition 5 in §6.3).

Proof of (a).

(1) (Reductio ad absurdum) Suppose $X := \mathbf{A}^2 - \{(0,0)\}$ were an affine variety. By Problem 6.15(a), the inclusion map $i : X \hookrightarrow \mathbf{A}^2$ is a morphism. By Proposition 2 in §6.2, $\widetilde{i} : \Gamma(\mathbf{A}^2) \hookrightarrow \Gamma(X)$ is a ring homomorphism.

(2) Problems 6.9 shows that $\Gamma(\mathbf{A}^2) = \Gamma(X) = k[x,y]$. Hence $\widetilde{i}$ is an isomorphism, so i is an isomorphism. However, i is not surjective on the point $(0,0)$, which is absurd.

□

Proof of (b).

(1) Write $\mathbf{A}^2 - \{(0,0)\} = (\mathbf{A}^2 - V(x)) \bigcup (\mathbf{A}^2 - V(y))$. It suffices to show that $\mathbf{A}^2 - V(x)$ is an affine variety.

(2) Note that $\mathbf{A}^2 - V(x)$ is isomorphic to a closed subvariety $V(1-xz)$ of $\mathbf{A}^3$.

□

Problem 6.18.

Show that the natural map π from $\mathbf{A}^{n+1} - \{(0, \ldots, 0)\}$ to $\mathbf{P}^n$ is a morphism of varieties, and that a subset U of $\mathbf{P}^n$ is open if and only if $\pi^{-1}(U)$ is open.

Proof.

(1) *Show that π is the morphism by Problem 6.14.* Write

$$X := \mathbf{A}^{n+1} - \{(0, \ldots, 0)\} = \bigcup_{i=1}^{n+1} U_i$$

where $U_i = \{(a_1, \ldots, a_{n+1}) \in X : a_i \neq 0\}$ are open subvarieties in X. Similarly, write

$$Y := \mathbf{P}^n = \bigcup_{i=1}^{n+1} V_i$$

where $V_i = \{[a_1 : \ldots : a_{n+1}] \in Y : a_i \neq 0\}$ are open subvarieties. Hence $\pi(U_i) = V_i$ for all i.

(2) Now it suffices to show $\pi|_{U_i} : U_i \to V_i$ is a morphism for all i (Problem 6.14). Given any closed subset $V(f) \cap V_i$ of V_i, where $f \in k[x_1, \ldots, x_{n+1}]$. $(\pi|_{U_i})^{-1}(V(f) \cap V_i) = V(f) \cap U_i$ is also closed in U_i. Hence $\pi|_{U_i}$ is continuous. Also, $\pi|_{U_i}$ pulls back rational functions to a rational functions.

(3) *Show that $U \subseteq \mathbf{P}^n$ is open if and only if $\pi^{-1}(U)$ is open.* $\pi^{-1}(U)$ is open if U is open since π is continuous. It suffices to show that $\pi(E)$ is open if E is open in X.

(4) Let $\widetilde{E}$ be the union of all the lines through the origin that meet E, that is, $\widetilde{E} = \pi^{-1}(\pi(E))$. Note that

$$\widetilde{E} = \bigcup_{a \in k - \{0\}} (aE)$$

is open in X since each aE is open in X. (Write $E = X - V(f_1, \ldots, f_r)$. Then $aE = X - V(g_1, \ldots, g_r)$, where

$$g_i(x_1, \ldots, x_{n+1}) := f_i(a^{-1}x_1, \ldots, a^{-1}x_{n+1}) \in k[x_1, \ldots, x_{n+1}]$$

for each i.) By the continuity of π, $\pi(E)$ is open since $\widetilde{E} = \pi^{-1}(\pi(E))$ is open.

□

Problem 6.21.

Any variety is the union of a finite number of open affine subvarieties.

Proof.

(1) Propositions 4 and 3 in §6.2 give all.

(2) *Proof of Proposition 3 in §6.2.* By Problem 6.4, $V_i = \varphi_i^{-1}(V)$ is a closed subvariety of $\mathbf{A}^{n+1}$. Since $\varphi : \varphi_i^{-1}(V) \to V \cap U_i$ is an isomorphism, $V \cap U_i$ is an open affine subvariety. Therefore, $V = \bigcup_{i=1}^{n+1}(V \cap U_i)$ is the union of a finite number of open affine subvarieties.

□

6.4. Products and Graphs

Problem 6.26.*

(a) *Let $f : X \to Y$ be a morphism of varieties such that $f(X)$ is dense in Y. Show that the homomorphism $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one*

(b) *If X and Y are affine, show that $f(X)$ is dense in Y if and only if $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one. Is this true if Y is not affine?*

Proof of (a).

(1) Given $\varphi \in \Gamma(Y)$ such that $\widetilde{f}(\varphi) = \varphi \circ f = 0$.

(2) So $\varphi = 0$ on $f(X)$. Since $f(X)$ is dense in Y, $\varphi = 0$ on Y by Problem 6.7(b). Hence $\widetilde{f}$ is injective.

□

Proof of (b).

(1) *If X and Y are affine, show that $f(X)$ is dense in Y if and only if $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one.* One direction is followed by (a).

(2) If $f(X)$ is not dense in $Y \subseteq \mathbf{A}^N$, then there is one open set $O = \bigcup_{i=1}^{r} V_{\varphi_i}$ such that
$$O \cap Y = \bigcup (V_{\varphi_i} \cap Y) \neq \varnothing$$
and
$$O \cap f(X) = \bigcup (V_{\varphi_i} \cap f(X)) = \varnothing.$$

(Note that Y is affine.) Hence $V_{\varphi_i} \cap Y \neq \varnothing$ for some $i = i_0$ and $V_{\varphi_i} \cap f(X) = \varnothing$ for all i. Take $\varphi = \varphi_{i_0}$. So there is $\varphi \in \Gamma(Y)$ such that $\widetilde{f}(\varphi) = 0$ and $\varphi \neq 0$. So $\widetilde{f}$ is not injective. Hence part (1) is established.

(3) *If Y is not affine, then $\widetilde{f} : \Gamma(Y) \to \Gamma(X)$ is one-to-one $\not\Longrightarrow$ $f(X)$ is dense in Y.* Let $f : \mathbf{P}^1 \to \mathbf{P}^2$ be a morphism as in Problem 6.25. Hence the image of f is not dense in $\mathbf{P}^2$ (since $f(\mathbf{P}^1) \cap \{z \neq 0\} = \varnothing$).

(4) Note that $\Gamma(\mathbf{P}^n(k)) = k$ for any projective n-space over k (since $k = \overline{k}$.) Therefore, the k-homomorphism

$$\widetilde{f} : \underbrace{\Gamma(\mathbf{P}^2)}_{=k} \to \underbrace{\Gamma(\mathbf{P}^1)}_{=k}$$

is an isomorphism (and thus $\widetilde{f}$ is injective).

□

Problem 6.29. (Algebraic group)

*Let V be a variety, and suppose V is also a group, i.e., there are mappings $\varphi : V \times V \to V$ (multiplication or addition), and $\psi : V \to V$ (inverse) satisfying the group axioms. If φ and ψ are morphisms, V is said to be an **algebraic group**. Show that each of the following is an algebraic group:*

(a) *$\mathbf{A}^1 = k$, with the usual addition on k; this group is often denoted $\mathbb{G}_a$.*

(b) *$\mathbf{A}^1 - \{(0)\} = k - \{0\}$, with the usual multiplication on k; this is denoted $\mathbb{G}_m$.*

(c) *$\mathbf{A}^n(k)$ with addition; likewise $\mathsf{M}_n(k) = \{n$ by n matrices$\}$ under addition may be identified with $A^{n^2}(k)$.*

(d) *$\mathsf{GL}_n(k) = \{$invertible $n \times n$ matrices$\}$ is an affine open subvariety of $\mathsf{M}_n(k)$, and a group under multiplication.*

(e) *C a nonsingular plane cubic, $O \in C$, $\oplus$ the resulting addition (see Problem 5.38).*

Proof of (a).

(1) $\mathbf{A}^1 = k$ is an affine variety.

(2) k is an abelian group under addition with 0 as the additive identity.

(3) $\varphi : (a, b) \mapsto a + b$ is continuous (by identifying $\mathbf{A}^1 \times \mathbf{A}^1$ to $\mathbf{A}^2$) and pulls back rational functions to a rational functions.

(4) $\psi : a \mapsto -a$ is continuous and pulls back rational functions to a rational functions.

□

Proof of (b).

(1) $\mathbf{A}^1 - \{0\}$ is an affine variety which is isomorphic to $V(1-xy) \subseteq \mathbf{A}^2$. It is the same as Proposition 5 in §6.3.

(2) k is an abelian group under multiplication with 1 as the multiplicative identity.

(3) $\varphi : (a, b) \mapsto ab$ is continuous (by identifying $\mathbf{A}^1 \times \mathbf{A}^1$ to $\mathbf{A}^2$) and pulls back rational functions to a rational functions.

(4) $\psi : a \mapsto a^{-1}$ is continuous and pulls back rational functions to a rational functions.

□

Proof of (c).

(1) $\mathbf{A}^n = k^n$ is an affine variety (or apply Proposition 6 in §6.4).

(2) k^n is a direct sum of n copies of abelian groups k under addition.

(3) By Proposition 7 in §6.4 and (a), both φ and ψ are morphisms.

□

Proof of (d).

(1) Similar to (b). $\mathsf{GL}_n(k)$ is an affine open subvariety of $\mathsf{M}_n(k)$ which is isomorphic to $V(1 - \det(x_{ij})y) \subseteq \mathbf{A}^{n^2+1}$ (where $(x_{ij}) \in \mathsf{M}_n(k)$).

(2) $\mathsf{GL}_n(k)$ is a group under multiplication with I_n as the multiplicative identity.

(3) Similar to (b). Both φ and ψ are morphisms.

□

Proof of (e).

(1) Similar to Problem 5.10, we might assume that $C = y^2z - x^3 - ax^2z - bxz^2 - cz^3$ and $O = [0 : 1 : 0] \in C$. C is an affine variety in $\mathbf{P}^2$.

(2) By Proposition 4 in §5.6, C is an abelian group with the addition $\oplus$. Now we can use Problem 5.38 to compute $P \oplus Q$ for any $P, Q \in C$.

(3) Define the addition φ as in Problem 5.38. Let

$$U_1 = \{x_1 \neq x_2\},$$
$$U_2 = \{x_1 = x_2, y_1 \neq 0\},$$
$$U_3 = \{x_1 = x_2, y_1 = 0, z_1 \neq 0\}$$

be an open covering of $C \times C$ (Proposition 7 in §6.4). It suffices to show that φ is a morphism on each U_α ($\alpha = 1, 2, 3$) (Problem 6.14). Since φ is a polynomial map on each U_α, φ is continuous on each U_α. Also, φ pulls back rational functions to a rational functions on each U_α. Hence φ is a morphism.

(4) Define the inverse ψ as $\psi(O) = O$ and $\psi([x : y : 1]) = [x : -y : 1]$ (Problem 5.38). ψ is continuous and pulls back rational functions to a rational functions. So ψ is a morphism.

□

6.5. Algebraic Function Fields and Dimension of Varieties

Problem 6.31.* (Theorem of the primitive element)

Let K be a field of a characteristic zero, L a finite (algebraic) extension of K. Then there is a $z \in L$ such that $L = K(z)$.

Outline of Proof.

(1) *Suppose $L = K(x, y)$. Let f and g be monic irreducible polynomials in $K[t]$ such that $f(x) = 0$, $g(y) = 0$. Let L' be a field in which $f = \prod_{i=1}^{n}(t - x_i)$, $g = \prod_{j=1}^{m}(t - y_j)$, $x = x_1$, $y = y_1$, $L' \supseteq L$ (see Problems 1.52, 1.53).*

(2) *Choose $\lambda \neq 0$ in K so that $\lambda x + y \neq \lambda x_i + y_j$ for all $i \neq 1, j \neq 1$. Let $z = \lambda x + y$, $K' = K(z)$. Set $h(t) = g(z - \lambda t) \in K'[t]$. Then $h(x) = 0$, $h(x_i) \neq 0$ if $i \neq 1$. Therefore $(h, f) = (t - x) \in K'[t]$. Then $x \in K'$, so $y \in K'$, so $L = K'$.*

(3) *If $L = K(x_1, \ldots, x_n)$, use induction on n to find $\lambda_1, \ldots, \lambda_n \in K$ such that $L = K(\sum \lambda_i x_i)$.*

Proof.

(1) Suppose $L = K(x, y)$. Let f and g be monic irreducible polynomials in $K[t]$ such that $f(x) = 0$, $g(y) = 0$. Let L' be a splitting field of L in which $f = \prod_{i=1}^{n}(t - x_i)$, $g = \prod_{j=1}^{m}(t - y_j)$, $x = x_1$, $y = y_1$, $L' \supseteq L$ (Problems 1.52). Note that the x_i (resp. y_j) are distinct by the irreducibility of f (resp. g) (Problem 1.53).

(2) Choose $\lambda \neq 0$ in K so that $\lambda x + y \neq \lambda x_i + y_j$ for all $i \neq 1, j \neq 1$. (Note that $\mathbb{Q} \hookrightarrow K$ since $\text{char}(K) = 0$. Hence, such one λ exists since K contains an infinite set $\mathbb{Q}$.) Let $z = \lambda x + y$ and $K' = K(z)$.

(3) *Show that* $L = K'$. $K' = K(z) \subseteq L$ since $z \in L$. Conversely, it suffices to show that $x \in K'$. Define $h(t) = g(z - \lambda t) \in K'[t]$. Then $h(x) = 0$ and $h(x_i) \neq 0$ if $i \neq 1$ by the construction of λ. Therefore $(h, f) = (t - x) \in K'[t]$. Then $x \in K'$, so $y \in K'$, so $L = K'$.

(4) If $L = K(x_1, \ldots, x_n)$ is a finite (algebraic) extension of K, use induction on n to find $\lambda_1, \ldots, \lambda_n \in K$ such that

$$\begin{aligned} L &= K(x_1, \ldots, x_{n-1})(x_n) \\ &= K(\lambda_1 x_1 + \cdots + \lambda_{n-1} x_{n-1})(x_n) && \text{(Induction hypothesis)} \\ &= K(\lambda_1 x_1 + \cdots + \lambda_n x_n) && \text{(Base step)} \end{aligned}$$

where $\lambda_1 := 1$.

□

Problem 6.32.*

Let $L = K(x_1, \ldots, x_n)$ as in Problem 6.31. Suppose $k \subseteq K$ is an algebraically closed subfield, and $V \subsetneq \mathbf{A}^n(k)$ is an algebraic set. Show that $L = K(\sum \lambda_i x_i)$ for some $(\lambda_1, \ldots, \lambda_n) \in \mathbf{A}^n - V$.

Proof.

(1) Since $V \subsetneq \mathbf{A}^n$, there is one index $1 \leq i \leq n$ such that the projection map $\pi_i : V \to \mathbf{A}^1$ defined by $\pi_i(a_1, \ldots, a_n) = a_i$ satisfies $\pi_i(V) \subsetneq \mathbf{A}^1$ (Problem 2.10). Here $\pi_i(V)$ is a finite subset of $\mathbf{A}^1$ (Problem 1.8).

(2) In the proof of Problem 6.31, we also take $\lambda_i \notin \pi_i(V)$. It is possible since k is infinite. Therefore, $(\lambda_1, \ldots, \lambda_n) \in \mathbf{A}^n - V$.

□

Problem 6.33. (Transcendence degree)

The notion of transcendence degree is analogous to the idea of the dimension of a vector space. If $k \subseteq K$, we say that $x_1, \ldots, x_n \in K$ are ***algebraically independent*** *if there is no nonzero polynomial $f \in k[x_1, \ldots, x_n]$ such that $f(x_1, \ldots, x_n) = 0$. By methods entirely analogous to those for bases of vector spaces, one can prove:*

(a) *Let $x_1, \ldots, x_n \in K$, K a finitely generated extension of k. Then $x_1, \ldots, x_n$ is a minimal set such that K is algebraic over $k(x_1, \ldots, x_n)$ if and only if $x_1, \ldots, x_n$ is a maximal set of algebraically independent elements of K. Such $\{x_1, \ldots, x_n\}$ is called a* ***transcendence basis*** *of K over k.*

(b) *Any algebraically independent set may be completed to a transcendence basis. Any set $\{x_1, \ldots, x_n\}$ such that K is algebraic over $k(x_1, \ldots, x_n)$ contains a transcendence basis.*

(c) $\mathrm{tr.deg}_k K$ *is the number of elements in any transcendence basis of K over k.*

Proof of (a).

(1) *Let $S = \{s_1, \ldots, s_n\} \subseteq K$. Show that the following statements are equivalent:*

(i) *S is algebraically independent over k.*

(ii) *For each i, s_i is transcendental over $k(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$.*

(iii) *For each i, s_i is transcendental over $k(s_1, \ldots, s_{i-1})$.*

(Lemma 19.7 in the textbook: *Patrick Morandi, Field and Galois Theory.*) The result is established if we can show that (i) $\iff$ (ii).

(2) ((i) $\implies$ (ii)) Suppose there are $a_j \in k(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ such that

$$s_i^m + \cdots + a_1 s_i + a_0 = 0.$$

Clearing denominators, might assume $a_j \in k[s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n]$. ($a_m = 1$.) Then

$$f = \sum_j a_j(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n) s_i^j \in k[s_1, \ldots, s_n]$$

has a root $(s_1, \ldots, s_n) \in \mathbf{A}^n(k)$. Since S is algebraically independent over k, $f = 0$. So $a_j = 0$. So s_i is transcendental over $k(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$.

(3) ((ii) $\implies$ (iii)) Clearly.

(4) ((iii) $\implies$ (i)) Suppose S were not algebraically independent over k. Choose m minimal such that there exists a nonzero $f \in k[x_1, \ldots, x_m]$ having a root $(s_1, \ldots, s_m) \in \mathbf{A}^n$. Write $f = \sum_j a_j x_m^j$ where $a_j \in k[x_1, \ldots, x_{m-1}]$. So

$$\sum_j a_j(s_1, \ldots, s_{m-1}) s_m^j = 0.$$

Since s_m is not algebraic over $k(s_1, \ldots, s_{i-1})$ by assumption, all $a_j(s_1, \ldots, s_{m-1}) = 0$ in k. By the minimality of m, all $a_j = 0$ in $k[x_1, \ldots, x_{m-1}]$. So $f = 0$, which is absurd.

□

Proof of (b).

(1) *Show that any algebraically independent set may be completed to a transcendence basis.* Let A be any algebraically independent subset of K. We claim we can find a transcendence basis $\mathscr{B}$ such that $A \subseteq \mathscr{B} \subseteq K$.

(2) (Zorn's lemma) Let

$$\Sigma = \{S \text{ is algebraically independent} : A \subseteq S \subseteq K\}.$$

Order Σ by inclusion. Σ is non empty since $A \in \Sigma$. To apply Zorn's lemma we must show that every chain in Σ has an upper bound in Σ.

(3) Let (S_α) be a chain in Σ, so that for each pair of indices α, β we have either $S_\alpha \subseteq S_\beta$, or $S_\beta \subseteq S_\alpha$. Let $B = \bigcup_\alpha S_\alpha$. Clearly, $B \in \Sigma$ since $A \subseteq B \subseteq K$ and polynomials only involve finitely many variables. By Zorn's lemma, Σ has a maximal element $\mathscr{B}$.

(4) *Show that K is algebraic over $k(\mathscr{B})$.* (Reductio ad absurdum) Suppose there were an element $s \in K$ transcendental over $k(\mathscr{B})$. Then $\mathscr{B} \cup \{s\}$ is algebraically independent, which contradicts the maximality of $\mathscr{B}$.

(5) *Show that any set $A = \{x_1, \ldots, x_n\}$ such that K is algebraic over $k(x_1, \ldots, x_n)$ contains a transcendence basis.* If A is algebraically independent, nothing to do. If A is algebraically dependent, then there is some x_i such that x_i algebraic over $k(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. So K is algebraic over $k(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Continue this process, we can find a minimal subset $\mathscr{B}$ of A such that K is algebraic over $k(x_1, \ldots, x_r)$ (with suitable relabeling). Here $\mathscr{B} \subseteq A$ is a transcendence basis.

□

Proof of (c).

(1) It suffices to show that $\text{tr. deg}_k K$ is well-defined. *Let K be a field extension of k. If S and T are transcendence bases for K/k, then $|S| = |T|$.* (Theorem 19.15 in the textbook: *Patrick Morandi, Field and Galois Theory.*)

(2) Suppose $S = \{s_1, \ldots, s_n\}$ is finite. In the proof of (b), $K/k(S - \{s_1\})$ is not algebraic. Since $K/k(T)$ is algebraic, some $t \in T$, say $t_1 \in T$ (by relabeling), must be transcendental over $k(S - \{s_1\})$. By the proof of (a),

$$S_1 := \{t_1, s_2, \ldots, s_n\}$$

is algebraically independent. Note that s_1 is algebraic over $k(S_1)$, or else $\{t_1, s_1, \ldots, s_n\}$ is algebraically independent, contrary to the assumption of S. Therefore, $K/k(S_1)$ is algebraic.

(3) Continue this process to replace each element in S to get $S_n = \{t_1, \ldots, t_n\} \subseteq T$. So $|S| \leq |T|$. Similarly, $|T| \leq |S|$. Therefore, $|S| = |T|$ if S is finite.

(4) Suppose S (and thus T) are infinite. Since t is algebraic over $k(S)$ for each $t \in T$, there is a corresponding finite subset $S_t \subseteq S$ such that t is algebraic over $k(S_t)$.

(5) Let

$$S' = \bigcup_{t \in T} S_t.$$

Then each $t \in T$ is algebraic over $k(S')$. Since $K/k(T)$ is algebraic, $K/k(S')$ is algebraic. Thus $S' = S$ since $S' \subseteq S$ and S is a transcendental basis for K/k.

(6) Hence,

$$|S| = |S'| = \left| \bigcup_{t \in T} S_t \right| \leq |T \times \mathbb{N}| = |T|,$$

where the last equality holds since $|T| = \infty$. Similarly, $|T| \leq |S|$. Therefore, $|S| = |T|$ if S is infinite.

□

Problem 6.34.

Show that $\dim \mathbf{A}^n = \dim \mathbf{P}^n = n$.

Proof.

(1) By Proposition 10 in §6.5,

$$\dim \mathbf{P}^n = \dim \mathbf{A}^n$$

since $\mathbf{P}^n$ is the projective closure of $\mathbf{A}^n$.

(2) A direct calculation shows

$$\dim \mathbf{A}^n = \text{tr. deg}_k\, k(\mathbf{A}^n) = \text{tr. deg}_k\, k(x_1, \ldots, x_n) = n.$$

□

6.6. Rational Maps

Chapter 7: Resolution of Singularities

7.1. Rational Maps of Curves

Problem 7.1.

Show that any curve has only a finite number of multiple points.

Proof.

(1) Write $C = f_1^{\alpha_1} \cdots f_r^{\alpha_r}$ where each f_i is irreducible and α_i is positive integer. Define $D = f_1 \cdots f_r$. Hence $\mathscr{O}_P(C) = \mathscr{O}_P(D)$ and thus

$$\{\text{simple points of } C\} = \{\text{simple points of } D\}.$$

(2) Note that the simple points of D agrees with our original definition. Hence D has only a finite number of multiple points (Problem 5.25). Therefore C has only a finite number of multiple points.

□

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

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

7.4. Quadratic Transformations

7.5. Nonsingular Models of Curves

Chapter 8: Riemann-Roch Theorem

8.1. Divisors

Problem 8.1.

Let $X = C = \mathbf{P}^1$, $k(X) = k(t)$, where $t = \frac{x_1}{x_2}$, x_1, x_2 homogeneous coordinates on $\mathbf{P}^1$.

(a) *Calculate* $\operatorname{div}(t)$.

(b) *Calculate* $\operatorname{div}\left(\frac{f}{g}\right)$, *$f$, g in $k[t]$.*

(c) *Prove Proposition 1 in §8.1 directly in this case.*

Proof of (a).

(1) By definition,

$$\operatorname{div}(t) = \operatorname{ord}_{[0:1]}(x_1) \cdot [0:1] - \operatorname{ord}_{[1:0]}(x_2) \cdot [1:0] = [0:1] - [1:0].$$

(2) Note that $\deg(\operatorname{div}(t)) = 1 - 1 = 0$.

□

Proof of (b).

(1) Write

$$f = \prod_i (t - \lambda_i)^{\alpha_i} \text{ and } g = \prod_i (t - \lambda_i)^{\beta_i}$$

where $\lambda_i \in k$ and α_i, β_i are nonnegative integers (since $k = \overline{k}$).

(2) Hence

$$\operatorname{ord}_{[\lambda:1]}\left(\frac{f}{g}\right) = \begin{cases} \alpha_i - \beta_i & \text{if } \lambda_i = \lambda \\ 0 & \text{otherwise} \end{cases}$$

(3) It remains to find $\operatorname{ord}_{[1:0]}\left(\frac{f}{g}\right)$. Write

$$\begin{aligned} \frac{f}{g} &= \prod_i (t - \lambda_i)^{\alpha_i - \beta_i} \\ &= \prod_i \left(\frac{x_1}{x_2} - \lambda_i\right)^{\alpha_i - \beta_i} \\ &= \left(\frac{x_2}{x_1}\right)^{-\sum_i (\alpha_i - \beta_i)} \prod_i \left(1 - \lambda_i \frac{x_2}{x_1}\right)^{\alpha_i - \beta_i}. \end{aligned}$$

So

$$\mathrm{ord}_{[1:0]}\left(\frac{f}{g}\right) = -\sum_i(\alpha_i - \beta_i).$$

(4)

$$\mathrm{div}\left(\frac{f}{g}\right) = \sum_i(\alpha_i - \beta_i)\cdot[\lambda_i : 1] - \left(\sum_i(\alpha_i - \beta_i)\right)\cdot[1:0].$$

□

Proof of (c). It suffices to show that $\deg\left(\mathrm{div}\left(\frac{f}{g}\right)\right) = 0$. In fact,

$$\deg\left(\mathrm{div}\left(\frac{f}{g}\right)\right) = \sum_i(\alpha_i - \beta_i) - \left(\sum_i(\alpha_i - \beta_i)\right) = 0.$$

□

Problem 8.2.

Let $X = C = V(y^2z - x(x-z)(x-\lambda z)) \subseteq \mathbf{P}^2$, $\lambda \in k$, $\lambda \neq 0, 1$. *Let* $\overline{x} = \frac{x}{z}$, $\overline{y} = \frac{y}{z} \in K$; $K = k(\overline{x}, \overline{y})$. *Calculate* $\mathrm{div}(\overline{x})$ *and* $\mathrm{div}(\overline{y})$.

Proof.

(1) Note that $V(x) \cap C = \{[0:1:0], [0:0:1]\}$ and $V(z) \cap C = \{[0:1:0]\}$. Hence

$$\begin{aligned}\mathrm{div}\left(\frac{x}{z}\right) = {} & \mathrm{ord}_{[0:1:0]}(x)[0:1:0] + \mathrm{ord}_{[0:0:1]}(x)[0:0:1] \\ & - \mathrm{ord}_{[0:1:0]}(z)[0:1:0].\end{aligned}$$

(2) Since

$$\begin{aligned}
\mathrm{ord}_{[0:1:0]}(x) &= I((0,0), x \cap C_*) \\
&= I((0,0), x \cap (z - x(x-z)(x-\lambda z))) \\
&= I((0,0), x \cap z) \\
&= 1, \\
\mathrm{ord}_{[0:0:1]}(x) &= I((0,0), x \cap C_*) \\
&= I((0,0), x \cap (y^2 - x(x-1)(x-\lambda))) \\
&= I((0,0), x \cap y^2) \\
&= 2, \\
\mathrm{ord}_{[0:1:0]}(z) &= I((0,0), z \cap C_*) \\
&= I((0,0), z \cap (z - x(x-z)(x-\lambda z))) \\
&= I((0,0), z \cap x^3) \\
&= 3,
\end{aligned}$$

we have

$$\begin{aligned}
\mathrm{div}\left(\frac{x}{z}\right) &= [0:1:0] + 2[0:0:1] - 3[0:1:0] \\
&= 2[0:0:1] - 2[0:1:0].
\end{aligned}$$

(3) Note that $V(y) \cap C = \{[0:0:1], [1:0:1], [\lambda:0:1]\}$. Hence

$$\begin{aligned}
\mathrm{div}\left(\frac{y}{z}\right) = &\,\mathrm{ord}_{[0:0:1]}(y)[0:0:1] + \mathrm{ord}_{[1:0:1]}(y)[1:0:1] \\
&+ \mathrm{ord}_{[\lambda:0:1]}(y)[\lambda:0:1] - \mathrm{ord}_{[0:1:0]}(z)[0:1:0].
\end{aligned}$$

(4) Since

$$\begin{aligned}
\mathrm{ord}_{[0:0:1]}(y) &= I((0,0), y \cap C_*) \\
&= I((0,0), y \cap (y^2 - x(x-1)(x-\lambda))) \\
&= I((0,0), y \cap x(x-1)(x-\lambda)) \\
&= 1, \\
\mathrm{ord}_{[1:0:1]}(y) &= I((1,0), y \cap C_*) \\
&= I((1,0), y \cap x(x-1)(x-\lambda)) \\
&= I((0,0), y \cap x(x+1)(x+1-\lambda)) \\
&= 1, \\
\mathrm{ord}_{[\lambda:0:1]}(y) &= I((\lambda,0), y \cap C_*) \\
&= I((\lambda,0), y \cap x(x-1)(x-\lambda)) \\
&= I((0,0), y \cap x(x-1+\lambda)(x+\lambda)) \\
&= 1,
\end{aligned}$$

we have

$$\operatorname{div}\left(\frac{y}{z}\right) = [0:0:1] + [1:0:1] + [\lambda:0:1] - 3[0:1:0].$$

□

Problem 8.3.

Let $C = X$ be a nonsingular cubic.

(a) *Let $P, Q \in C$. Show that $P \equiv Q$ if and only if $P = Q$. (Hint: Lines are adjoints of degree 1.)*

(b) *Let $P, Q, R, S \in C$. Show that $P + Q \equiv R + S$ if and only if the line through P and Q intersects the line through R and S in a point on C (if $P = Q$ use the tangent line).*

(c) *Let P_0 be a fixed point on C, thus defining an addition $\oplus$ on C (§5.6). Show that $P \oplus Q = R$ if and only if $P + Q \equiv R + P_0$. Use this to give another proof of Proposition 4 of §5.6.*

Proof of (a).

(1) One direction is trivial by taking $z \in k - \{0\}$ in the definition of linearly equivalence. For the opposite direction, we need the residue theorem in §8.1.

(2) Take $E = 0$ (since C is nonsingular), $D = P$, $D' = Q$, and $G = L$ be any line passing throught D, that is,

$$\operatorname{div}(L) = P + E + A = P + A$$

for some effective divisor A. The existence of A is guaranteed by Bézout theorem. Note that we can write $A = P' + P''$ where P' and P'' are points in C.

(3) By residue theorem in §8.1, there is an adjoint L' of degree 1 such that

$$\operatorname{div}(L') = Q + E + A = Q + A.$$

Therefore,

$$P = \varphi(P', P'') = Q.$$

□

Proof of (b).

(1) Let L (resp. L') be a line passing through P, Q (resp. R, S). So

$$\begin{aligned}\operatorname{div}(L) &= P + Q + \varphi(P, Q)\\ \operatorname{div}(L') &= R + S + \varphi(R, S).\end{aligned}$$

Hence

$$P + Q + \varphi(P, Q) \equiv R + S + \varphi(R, S)$$

(by Proposition 2(5) in §8.1).

(2) Therefore,

$$\begin{aligned}& P + Q \equiv R + S\\ \iff & \varphi(P, Q) \equiv \varphi(R, S) && \text{(Proposition 2(4))}\\ \iff & \varphi(P, Q) = \varphi(R, S) && ((a))\\ \iff & \text{the line through } P \text{ and } Q \text{ intersects}\\ & \quad \text{the line through } R \text{ and } S \text{ in a point on } C.\end{aligned}$$

□

Proof of (c).

(1) By taking $S = P_0$ in (b), we have $P \oplus Q = R \iff P + Q \equiv R + P_0$.

(2) $P + Q \equiv R + P_0$ implies that $R \in C$. That is, $\oplus$ defines an addition on C. $P \oplus Q = Q \oplus P$ since $P + Q = Q + P \equiv R + P_0$. P_0 is the identity since $P + P_0 \equiv P + P_0$ is always true for any $P \in C$. Hence the rest is to prove the associativity.

(3) Suppose $P, Q, R \in C$. Hence

$$\begin{aligned}& (\underbrace{P \oplus Q}_{:=S}) \oplus R := T\\ \iff & S + R \equiv T + P_0 \text{ and } P + Q \equiv S + P_0\\ \implies & P + Q + R \equiv T + 2P_0 && \text{(Proposition 2(4))}\end{aligned}$$

and

$$\begin{aligned}& P \oplus (\underbrace{Q \oplus R}_{:=S'}) := T'\\ \iff & P + S' \equiv T' + P_0 \text{ and } Q + R \equiv S' + P_0\\ \implies & P + Q + R \equiv T' + 2P_0. && \text{(Proposition 2(4))}\end{aligned}$$

Proposition 2(1) in §8.1 implies that $T + 2P_0 \equiv T' + 2P_0$. Hence $T \equiv T'$ (Proposition 2(4)). Therefore $T = T'$ by (a).

□

Problem 8.4.

Let C be a cubic with a node. Show that for any two simple points P, Q on C, $P \equiv Q$.

Proof.

(1) Let E be the node of C. Consider a line L passing through P and E. So

$$\operatorname{div}(L) = P + E + \varphi(P, E).$$

Since P is simple, $\varphi(P, E) = E$ (Problems 5.35, 5.11). So

$$\operatorname{div}(L) = P + 2E.$$

(2) Similarly, if L' is a line passing through Q and E, then

$$\operatorname{div}(L') = Q + 2E.$$

(3) Hence $\operatorname{div}(L') + P + 2E = \operatorname{div}(L) + Q + 2E$ or $\operatorname{div}(L') + P = \operatorname{div}(L) + Q$ (Proposition 2(4) in §8.1). Therefore $P \equiv Q$ (Proposition 2(5) in §8.1).

(4) Note that the conclusion also holds for an irreducible cubic with a cusp.

□

Problem 8.5.

Let C be a nonsingular quartic, $P_1, P_2, P_3 \in C$. Let $D = P_1 + P_2 + P_3$. Let L and L' be lines such that $L \bullet C = P_1 + P_2 + P_4 + P_5$, $L' \bullet C = P_1 + P_3 + P_6 + P_7$. Suppose these seven points are distinct. Show that D is not linearly equivalent to any other effective divisor. (Hint: Apply the residue theorem to the conic LL'.) Investigate in a similar way other divisors of small degree on quartics with various types of multiple points.

Proof.

(1) Suppose D' is linearly equivalent to D. Let $G = LL'$ be a conic. Note that

$$\operatorname{div}(G) = D + P_1 + P_4 + P_5 + P_6 + P_7.$$

By the residue theorem, there is an adjoint G' of degree 2 such that

$$\operatorname{div}(G') = D' + P_1 + P_4 + P_5 + P_6 + P_7.$$

In particular, $G \cap G' \supseteq \{P_1, P_4, P_5, P_6, P_7\}$.

(2) (Reductio ad absurdum) If G, G' were distinct, then by Bézout's theorem we might write

$$G = L \cup L', \qquad G' = L \cup L''$$

for some distinct line $L'' \neq L'$. (The case $G' = L' \cup L''$ with $L'' \neq L$ is similar.)

(3) So

$$G \cap G' = L \cup (\underbrace{L' \cap L''}_{\{\text{single point}\}}).$$

Hence there are four points on L, contrary to the fact that any four points of $\{P_1, P_4, P_5, P_6, P_7\}$ are not collinear. (If so, then all five points are on the same line L and thus $L \mid C$, contrary to the irreducibility of C.) Therefore $G = G'$. So $\operatorname{div}(G) = \operatorname{div}(G')$ or $D = D'$.

(4) *Let C be a nonsingular quartic, $P_1, P_2 \in C$. Let $D = P_1 + P_2$. Let L and L' be lines such that $L \bullet C = P_1 + P_3 + P_4 + P_5$, $L' \bullet C = P_2 + P_6 + 2P_7$. Suppose these 7 points are distinct. Then D is not linearly equivalent to any other effective divisor.* The proof is similar to (1)(2)(3). (Omit to discuss the rest case $\deg(D) = 1$.)

□

Problem 8.6. (Divisor class group)

*Let $D(X)$ be the group of divisors on X, $D_0(X)$ the subgroup consisting of divisors of degree zero, and $P(X)$ the subgroup of $D_0(X)$ consisting of divisors of rational functions. Let $C_0(X) = D_0(X)/P(X)$ be the quotient group. It is the **divisor class group** on X.*

(a) *If $X = \mathbf{P}^1$, then $C_0(X) = 0$.*

(b) *Let $X = C$ be a nonsingular cubic. Pick $P_0 \in C$, defining $\oplus$ on C. Show that the map from C to $C_0(X)$ that sends P to the residue class of the divisor $P - P_0$ is an isomorphism from $(C, \oplus)$ onto $C_0(X)$.*

Proof of (a).

(1) Given a divisor

$$D = \sum_{P \in X} n_P P \in D_0(X)$$

where $n_P \in \mathbb{Z}$ and $\sum_P n_P = 0$.

(2) Note that $\sum_P n_P = 0$. We can define a rational function $z \in k(X)$ by

$$z = \prod_{P=[a_P:b_P]\in X} (b_P x - a_P y)^{n_P}.$$

Hence $\operatorname{div}(z) = D \in P(X)$. Therefore $C_0(X) = D_0(X)/P(X) = 0$.

□

Proof of (b).

(1) Define $\alpha : (C, \oplus) \to C_0(X)$ by $P \mapsto [P - P_0]$.

(2) *Show that α is a group homomorphism.* If $P \oplus Q = R$, then

$$\begin{aligned} & P \oplus Q = R \\ \iff & [P + Q] = [R + P_0] && \text{(Problem 8.3(c))} \\ \iff & [P - P_0] + [Q - P_0] = [R - P_0] && \text{(Proposition 2)} \\ \iff & \alpha(P) + \alpha(Q) = \alpha(R) = \alpha(P \oplus Q). \end{aligned}$$

(3) *Show that α is injective.*

$$\begin{aligned} \alpha(P) = 0 \iff & [P - P_0] = 0 \\ \iff & [P] = [P_0] && \text{(Proposition 2)} \\ \iff & P = P_0. && \text{(Problem 8.3(a))} \end{aligned}$$

(4) *Show that α is surjective.* Given $[D] \in C_0(X)$ and we want to find a point $P \in C$ such that $\alpha(P) = [D]$. Write

$$D = (P_1 + \cdots + P_r) - (Q_1 + \cdots + Q_r)$$

for some $P_i, Q_i \in C$. So

$$\begin{aligned} [D] &= [P_1 - P_0] + \cdots + [P_r - P_0] - [Q_1 - P_0] - \cdots - [Q_r - P_0] \\ &= \alpha(P_1) + \cdots + \alpha(P_r) - \alpha(Q_1) - \cdots - \alpha(Q_r) \\ &= \alpha(P_1) + \cdots + \alpha(P_r) + \alpha(Q_1') + \cdots + \alpha(Q_r') \\ &= \alpha(P_1 \oplus \cdots \oplus P_r \oplus Q_1' \oplus \cdots \oplus Q_r'). \end{aligned}$$

where Q_i' is the inverse of Q_i in $(C, \oplus)$. Hence there is a point $P := P_1 \oplus \cdots \oplus P_r \oplus Q_1' \oplus \cdots \oplus Q_r' \in C$ such that $\alpha(P) = [D]$.

□

Problem 8.7.

When do two curves g, h have the same divisor (C and X are fixed)?

Proof.

(1) Define $z = \frac{g}{h} \in k(X)$. It is well-defined since g and h has the same degree.

(2) Hence
$$\operatorname{div}(z) = \operatorname{div}(g) - \operatorname{div}(h) = 0.$$
By Corollary 1 to Proposition 1 in §8.1, $z \in k$. Hence $g = \lambda h$ for some $\lambda \in k$ if g, h have the same divisor.

□

8.2. The Vector Spaces $\mathscr{L}(D)$

Problem 8.8.*

If $D \leq D'$, then $\ell(D') \leq \ell(D) + \deg(D' - D)$, i.e., $\deg(D) - \ell(D) \leq \deg(D') - \ell(D')$.

Proof. Note that D' is obtained from D by adding $\deg(D' - D)$ points and $\ell(D + P) \leq \ell(D) + 1$ (Proposition 3(1) in §8.2). Hence the conclusion is established by induction on $\deg(D' - D)$. □

Problem 8.11.*

Let D be a divisor. Show that $\ell(D) > 0$ if and only if D is linearly equivalent to an effective divisor.

Proof.

$$\begin{aligned}
& f \in \mathscr{L}(D) \text{ is nonzero} \\
\Longrightarrow\ & D' := \operatorname{div}(f) + D \geq 0 \\
\Longrightarrow\ & D \equiv D' \text{ where } D' \text{ is effective} \\
\Longrightarrow\ & D' = \operatorname{div}(f) + D \geq 0 \text{ for some nonzero } f \in K \\
& \qquad \text{(Here we take } f \in k - \{0\} \text{ if } \operatorname{div}(f) = 0.\text{)} \\
\Longrightarrow\ & f \in \mathscr{L}(D) \text{ is nonzero.}
\end{aligned}$$

□

Problem 8.12.

Show that $\deg(D) = 0$ *and* $\ell(D) > 0$ *are true if and only if* $D \equiv 0$.

Proof.

$$\begin{aligned}
&\ell(D) > 0 \text{ and } \deg(D) = 0 \\
\iff &D \equiv D' \text{ and } \deg(D) = 0 \text{ for some effective devisor } D' \quad \text{(Problem 8.11)} \\
\iff &D \equiv D' \text{ and } \deg(D') = 0 \text{ for some effective devisor } D' \quad \text{(Prop. 2(3))} \\
\iff &D \equiv 0.
\end{aligned}$$

□

Problem 8.13.*

Suppose $\ell(D) > 0$*, and let* $f \neq 0$*,* $f \in \mathscr{L}(D)$*. Show that* $f \notin \mathscr{L}(D - P)$ *for all but a finite number of* P*. So* $\ell(D-P) = \ell(D)-1$ *for all but a finite number of* P*.*

Proof.

(1) By Problem 8.11, we might assume that $D = \sum_P n_P P$ is effective (with $n_P \geq 0$).

(2) Let $S = \{P \in X : f \in \mathscr{L}(D - P)\}$. For each $P \in S$, we have

$$\operatorname{ord}_P(f) + n_P - 1 \geq 0.$$

Since D is effective, $\operatorname{ord}_P(f) > 0$ for all $P \in S$. Since $\operatorname{ord}_P(f)$ is nonzero for finitely many points, S is finite.

(3) By Proposition 3,

$$\ell(D - P) \leq \ell(D) \leq \ell(D - P) + 1.$$

By (2), $\ell(D - P) \neq \ell(D)$ for all but a finite number of P. Hence $\ell(D) = \ell(D - P) + 1$ for all but a finite number of P.

□

8.3. Riemann's Theorem

Problem 8.14.

Calculate the genus of each of the following curves:

(a) $x^2y^2 - z^2(x^2 + y^2)$.

(b) $(x^3 + y^3)z^2 + x^3y^2 - x^2y^3$.

(c)

(d) $(x^2 - z^2)^2 - 2y^3z - 3y^2z^2$.

Proof of (a).

(1) Let $C = x^2y^2 - z^2(x^2 + y^2)$. By solving $C(P) = \frac{\partial C}{\partial x}(P) = \frac{\partial C}{\partial y}(P) = \frac{\partial C}{\partial z}(P) = 0$, we have $P = [0 : 0 : 1], [0 : 1 : 0], [1 : 0 : 0]$.

(2) Note that

$$\begin{aligned} & m_{[0:0:1]}(C) \\ &= m_{(0,0)}(C_*) && \text{(Dehomogenize } C \text{ w.r.t. } z) \\ &= m_{(0,0)}(x^2y^2 - (x^2 + y^2)) \\ &= 2. \end{aligned}$$

Similarly, $m_{[0:1:0]}(C) = m_{[1:0:0]}(C) = 2$. Proposition 5 in §8.3 shows that

$$g = \frac{(4-1)(4-2)}{2} - 3 \cdot \frac{2(2-1)}{2} = 0.$$

□

Proof of (b).

(1) Let $C = (x^3+y^3)z^2+x^3y^2-x^2y^3$. By solving $C(P) = \frac{\partial C}{\partial x}(P) = \frac{\partial C}{\partial y}(P) = \frac{\partial C}{\partial z}(P) = 0$, we have $P = [0 : 0 : 1], [0 : 1 : 0], [1 : 0 : 0]$.

(2) Note that

$$\begin{aligned} & m_{[0:0:1]}(C) \\ &= m_{(0,0)}(C_*) && \text{(Dehomogenize } C \text{ w.r.t. } z) \\ &= m_{(0,0)}(x^3 + y^3 + x^3y^2 - x^2y^3) \\ &= 3, \\ & m_{[0:1:0]}(C) \\ &= m_{(0,0)}(C_*) && \text{(Dehomogenize } C \text{ w.r.t. } y) \\ &= m_{(0,0)}(x^3z^2 + x^3 - x^2 + z^2) \\ &= 2. \end{aligned}$$

Similarly, $m_{[1:0:0]}(C) = 2$. Proposition 5 in §8.3 shows that

$$g = \frac{(5-1)(5-2)}{2} - \frac{3(3-1)}{2} - 2 \cdot \frac{2(2-1)}{2} = 1.$$

□

Proof of (c).

(1)

□

Proof of (d).

(1) Let $C = (x^2 - z^2)^2 - 2y^3 z - 3y^2 z^2$. By solving $C(P) = \frac{\partial C}{\partial x}(P) = \frac{\partial C}{\partial y}(P) = \frac{\partial C}{\partial z}(P) = 0$, we have $P = [\pm 1 : 0 : 1], [0 : -1 : 1]$.

(2) Note that

$$\begin{aligned}
&m_{[\pm 1:0:1]}(C) \\
&= m_{(\pm 1,0)}(C_*) && \text{(Dehomogenize } C \text{ w.r.t. } z) \\
&= m_{(\pm 1,0)}((x^2-1)^2 - 2y^3 - 3y^2) \\
&= m_{(0,0)}(x^4 \pm 4x^3 - 2y^3 + 4x^2 - 3y^2) \\
&= 2, \\
&m_{[0:-1:1]}(C) \\
&= m_{(0,-1)}(C_*) && \text{(Dehomogenize } C \text{ w.r.t. } z) \\
&= m_{(0,-1)}((x^2-1)^2 - 2y^3 - 3y^2) \\
&= m_{(0,0)}(x^4 - 2y^3 - 2x^2 + 3y^2) \\
&= 2.
\end{aligned}$$

Proposition 5 in §8.3 shows that

$$g = \frac{(4-1)(4-2)}{2} - 3 \cdot \frac{2(2-1)}{2} = 0.$$

□

8.4. Derivations and Differentials

8.5. Canonical Divisors

8.6. Riemann-Roch Theorem