Solutions to the book: *Fulton, Algebraic Curves*

Meng-Gen Tsai
plover@gmail.com

March 11, 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

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

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

(2) Hence,

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

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

□

Proof of (b).

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

(2) Write

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

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

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

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

□

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

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

(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.

□

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 $\deg r < \deg f$. Now as

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

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

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

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

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

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

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

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

□

Notes.

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

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

Problem 1.9.

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

Proof.

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

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

□

Problem 1.11.

Show that the following are algebraic sets:

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

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

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

Proof of (a).

(1) The twisted cubic curve
$$Y = \{(t, t^2, t^3) \in \mathbf{A}^3(k) : t \in k\} = V(x^2 - y) \cap V(x^3 - z)$$
is algebraic. We say that Y is given by the parametric representation $x = t$, $y = t^2$, $z = t^3$.

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

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

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

$\square$

Proof of (b). The circle

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

is algebraic. $\square$

Proof of (c). The circle

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

is algebraic again. $\square$

Problem 1.15.*

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

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

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

Proof.

(1) Write

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

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

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

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

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

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

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

(3) By construction, $V \times W \subseteq V(S)$. Conversely, given any $(a, b) \in V(S)$, we have $h(a, b) = 0$ for all $h \in S = S_V \cup S_W$ (by (2)). By construction, $f(a) = 0$ for all $f \in S_V$ since f only involve $x_1, \dots, x_n$. Hence, $a \in V$. Similarly, $b \in W$. Therefore, $(a, b) \in V \times W$.

$\square$

1.3. The Ideal of a Set of Points

Problem 1.18.*

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

Proof.

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

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

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

(2) *Show that* 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 PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

1.4. The Hilbert Basis Theorem

1.5. Irreducible Components of an Algebraic Set

1.6. Algebraic Subsets of the Plane

1.7. Hilbert's Nullstellensatz

1.8. Modules; Finiteness Conditions

1.9. Integral Elements

1.10. Field Extensions

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

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

2.2. Polynomial Maps

2.3. Coordinate Changes

2.4. Rational Functions and Local Rings

2.5. Discrete Valuation Rings

2.6. Forms

2.7. Direct Products of Rings

2.8. Operations with Ideals

2.9. Ideals with a Finite Number of Zeros

2.10. Quotient Modules and Exact Sequences

2.11. Free Modules

Chapter 3: Local Properties of Plane Curves

3.1. Multiple Points and Tangent Lines

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

3.2. Multiplicities and Local Rings

3.3. Intersection Numbers

Chapter 4: Projective Varieties

4.1. Projective Space

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

4.2. Projective Algebraic Sets

4.3. Affine and Projective Varieties

4.4. Multiprojective Space

Chapter 5: Projective Plane Curves

5.1. Definitions

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

5.2. Linear Systems of Curves

5.3. Bézout's Theorem

5.4. Multiple Points

5.5. Max Noether's Fundamental Theorem

5.6. Applications of Noether's Theorem

Chapter 6: Varieties, Morphisms, and Rational Maps

6.1. The Zariski Topology

6.2. Varieties

6.3. Morphisms of Varieties

6.4. Products and Graphs

6.5. Algebraic Function Fields and Dimension of Varieties

6.6. Rational Maps

Chapter 7: Resolution of Singularities

7.1. Rational Maps of Curves

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

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

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

7.4. Quadratic Transformations

7.5. Nonsingular Models of Curves

Chapter 8: Riemann-Roch Theorem

8.1. Divisors

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

8.2. The Vector Spaces $L(D)$

8.3. Riemann's Theorem

8.4. Derivations and Differentials

8.5. Canonical Divisors

8.6. Riemann-Roch Theorem