Solutions to the book:
Fulton, Algebraic Curves

Meng-Gen Tsai
plover@gmail.com

March 12, 2021

Contents

Chapter 1: Affine Algebraic Sets **4**
1.1. Algebraic Preliminaries 4
Problem 1.1.* 4
Problem 1.2.* 5
Problem 1.3.* 6
Problem 1.4.* 7
Problem 1.5.* 8
Problem 1.6.* 8
Problem PLACEHOLDER 9
1.2. Affine Space and Algebraic Sets 9
Problem 1.8.* 9
Problem 1.9. 10
Problem 1.10. 10
Problem 1.11. 11
Problem 1.15.* 11
1.3. The Ideal of a Set of Points 12
Problem 1.18.* 12
Problem PLACEHOLDER 13
1.4. The Hilbert Basis Theorem 13
1.5. Irreducible Components of an Algebraic Set 13
1.6. Algebraic Subsets of the Plane 13
1.7. Hilbert's Nullstellensatz 13
1.8. Modules; Finiteness Conditions 13
Problem 1.41.* 13
Problem 1.42. 14
Problem 1.43.* (WIP) 14
1.9. Integral Elements 15
1.10. Field Extensions 15

Chapter 2: Affine Varieties **16**
2.1. Coordinate Rings . . . 16
Problem 2.1.* . . . 16
Problem PLACEHOLDER . . . 16
2.2. Polynomial Maps . . . 17
2.3. Coordinate Changes . . . 17
2.4. Rational Functions and Local Rings . . . 17
2.5. Discrete Valuation Rings . . . 17
2.6. Forms . . . 17
2.7. Direct Products of Rings . . . 17
2.8. Operations with Ideals . . . 17
Problem 2.39.* . . . 17
Problem 2.41.* . . . 19
2.9. Ideals with a Finite Number of Zeros . . . 21
2.10. Quotient Modules and Exact Sequences . . . 21
Problem 2.51. . . . 21
2.11. Free Modules . . . 22

Chapter 3: Local Properties of Plane Curves **23**
3.1. Multiple Points and Tangent Lines . . . 23
Problem PLACEHOLDER . . . 23
3.2. Multiplicities and Local Rings . . . 23
3.3. Intersection Numbers . . . 23

Chapter 4: Projective Varieties **24**
4.1. Projective Space . . . 24
Problem PLACEHOLDER . . . 24
4.2. Projective Algebraic Sets . . . 24
4.3. Affine and Projective Varieties . . . 24
4.4. Multiprojective Space . . . 24

Chapter 5: Projective Plane Curves **25**
5.1. Definitions . . . 25
Problem PLACEHOLDER . . . 25
5.2. Linear Systems of Curves . . . 25
5.3. Bézout's Theorem . . . 25
5.4. Multiple Points . . . 25
5.5. Max Noether's Fundamental Theorem . . . 25
5.6. Applications of Noether's Theorem . . . 25

Chapter 6: Varieties, Morphisms, and Rational Maps **26**
6.1. The Zariski Topology . . . 26
6.2. Varieties . . . 26
6.3. Morphisms of Varieties . . . 26
6.4. Products and Graphs . . . 26
6.5. Algebraic Function Fields and Dimension of Varieties . . . 26

6.6. Rational Maps 26

Chapter 7: Resolution of Singularities **27**
7.1. Rational Maps of Curves 27
Problem PLACEHOLDER 27
7.2. Blowing up a Point in $\mathbf{A}^2$ 27
7.3. Blowing up a Point in $\mathbf{P}^2$ 27
7.4. Quadratic Transformations 27
7.5. Nonsingular Models of Curves 27

Chapter 8: Riemann-Roch Theorem **28**
8.1. Divisors 28
Problem PLACEHOLDER 28
8.1. The Vector Spaces $L(D)$ 28
8.1. Riemann's Theorem 28
8.1. Derivations and Differentials 28
8.1. Canonical Divisors 28
8.6. Riemann-Roch Theorem 28

Chapter 1: Affine Algebraic Sets

1.1. Algebraic Preliminaries

Problem 1.1.*

Let R be a domain.

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

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

Proof of (a).

(1) Write

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

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

(2) Hence,

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

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

□

Proof of (b).

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

(2) Write

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

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

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

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

□

Problem 1.2.*

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

Proof.

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

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

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

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

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

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

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

(b) a and b have no common factors,

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

Write

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

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

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

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

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

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

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

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

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

□

Problem 1.3.*

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

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

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

Proof of (a).

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

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

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

□

Proof of (b).

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

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

□

Problem 1.4.*

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

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

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

Proof.

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

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

□

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

Problem 1.5.*

Let k be any field. Show that there are an infinitely number of irreducible monic polynomials in $k[x]$. (Hint: Suppose $f_1, \ldots, f_n$ 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 PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

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 1.10.

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 1.15.*

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 1.18.*

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) $0 \in \operatorname{rad}(I)$ 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* $\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$. It suffices to show $\operatorname{rad}(\operatorname{rad}(I)) \subseteq \operatorname{rad}(I)$. Given any $a \in \operatorname{rad}(\operatorname{rad}(I))$. By definition $a^n \in \operatorname{rad}(I)$ 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, $a \in \operatorname{rad}(I)$.

(4) *Show that every prime ideal* $\mathfrak{p}$ *is radical.* Given any $a \in \operatorname{rad}(\mathfrak{p})$, 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

Problem 1.41.*

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

Proof.

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

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

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

that is, S is ring-finite over R.

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

□

Problem 1.42.

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

Proof.

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

(2) (Reductio ad absurdum) If $S = \sum Rs_i$ for some $s_1, \ldots, s_n \in S$ 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.* (WIP)

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

Proof.

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

(2)

□

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

□

Problem PLACEHOLDER

PLACEHOLDER

Proof.

(1) PLACEHOLDER

2.2. Polynomial Maps

2.3. Coordinate Changes

2.4. Rational Functions and Local Rings

2.5. Discrete Valuation Rings

2.6. Forms

2.7. Direct Products of Rings

2.8. Operations with Ideals

Problem 2.39.*

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

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

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

Proof of (a).

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

(2) *Show that* $(I_1 + I_2)J \subseteq I_1 J + I_2 J$. Given any

$$(x_1 + x_2)y \in (I_1 + I_2)J$$

where $x_i \in I_i$ and $y \in J$. It suffices to show that $(x_1 + x_2)y \in I_1 J + I_2 J$ (by (1)). In fact,

$$(x_1 + x_2)y = x_1 y + x_2 y \in I_1 J + I_2 J.$$

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

$$x_1 y_1 + x_2 y_2 \in I_1 J + I_2 J$$

where $x_i \in I_i$ and $y_i \in J$. It suffices to show that $x_1 y_1 + x_2 y_2 \in (I_1 + I_2)J$ (by (1)). In fact,

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

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

$\square$

Proof of (b).

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

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

$$x = x_1 \cdots x_n$$

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

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

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

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

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

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

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

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

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

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

□

Problem 2.41.*

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

Proof.

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

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

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

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

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

□

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

Proof.

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

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

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

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

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

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

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

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

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

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

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

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

(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 part (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.

□

2.9. Ideals with a Finite Number of Zeros

2.10. Quotient Modules and Exact Sequences

Problem 2.51.

Let

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

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

Proof (Proposition 7 in this section).

(1) For $i = 0, \ldots, n$, 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 $\sum(-1)^i \dim(V_i) = 0$.

□

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