

# Solutions to the book: *Fulton, Algebraic Curves*

Meng-Gen Tsai  
plover@gmail.com

May 27, 2021

## Contents

|                                                             |          |
|-------------------------------------------------------------|----------|
| <b>Chapter 1: Affine Algebraic Sets</b>                     | <b>6</b> |
| 1.1. Algebraic Preliminaries . . . . .                      | 6        |
| Problem 1.1.* . . . . .                                     | 6        |
| Problem 1.2.* . . . . .                                     | 7        |
| Problem 1.3.* . . . . .                                     | 8        |
| Problem 1.4.* . . . . .                                     | 9        |
| Problem 1.5.* . . . . .                                     | 10       |
| Problem 1.6.* . . . . .                                     | 10       |
| Problem 1.7.* . . . . .                                     | 11       |
| 1.2. Affine Space and Algebraic Sets . . . . .              | 13       |
| Problem 1.8.* . . . . .                                     | 13       |
| Problem 1.9. . . . .                                        | 14       |
| Problem 1.10. . . . .                                       | 14       |
| Problem 1.11. . . . .                                       | 14       |
| Problem 1.12. . . . .                                       | 15       |
| Problem 1.13. . . . .                                       | 16       |
| Problem 1.14.* . . . . .                                    | 18       |
| Problem 1.15.* . . . . .                                    | 20       |
| 1.3. The Ideal of a Set of Points . . . . .                 | 20       |
| Problem 1.16.* . . . . .                                    | 20       |
| Problem 1.17.* . . . . .                                    | 21       |
| Problem 1.18.* . . . . .                                    | 22       |
| Problem 1.19. . . . .                                       | 23       |
| Problem 1.20.* . . . . .                                    | 24       |
| Problem 1.21.* . . . . .                                    | 24       |
| 1.4. The Hilbert Basis Theorem . . . . .                    | 25       |
| Problem 1.22.* (Correspondence theorem for rings) . . . . . | 25       |
| 1.5. Irreducible Components of an Algebraic Set . . . . .   | 28       |
| Problem 1.23. . . . .                                       | 28       |

|                                                      |           |
|------------------------------------------------------|-----------|
| Problem 1.24.                                        | 29        |
| Problem 1.25.                                        | 29        |
| Problem 1.26.                                        | 30        |
| Problem 1.27.                                        | 31        |
| Problem 1.28.                                        | 32        |
| Problem 1.29.*                                       | 32        |
| 1.6. Algebraic Subsets of the Plane                  | 33        |
| Problem 1.30.                                        | 33        |
| Problem 1.31.                                        | 33        |
| 1.7. Hilbert's Nullstellensatz                       | 35        |
| Problem 1.32.                                        | 35        |
| Problem 1.33.                                        | 36        |
| Problem 1.34.                                        | 38        |
| Problem 1.35.                                        | 38        |
| Problem 1.36.                                        | 39        |
| Problem 1.37.*                                       | 40        |
| Problem 1.38.*                                       | 41        |
| Problem 1.39.                                        | 41        |
| Problem 1.40.                                        | 42        |
| 1.8. Modules; Finiteness Conditions                  | 44        |
| Problem 1.41.*                                       | 44        |
| Problem 1.42.                                        | 44        |
| Problem 1.43.*                                       | 45        |
| Problem 1.44.*                                       | 45        |
| Problem 1.45.*                                       | 46        |
| 1.9. Integral Elements                               | 47        |
| Problem 1.46.* (Transitivity of integral extensions) | 47        |
| Problem 1.47.*                                       | 48        |
| Problem 1.48.*                                       | 49        |
| Problem 1.49.*                                       | 49        |
| Problem 1.50.*                                       | 50        |
| 1.10. Field Extensions                               | 51        |
| Problem 1.51.*                                       | 51        |
| Problem 1.52.* (Splitting fields)                    | 53        |
| Problem 1.53.*                                       | 53        |
| Problem 1.54.*                                       | 54        |
| <b>Chapter 2: Affine Varieties</b>                   | <b>56</b> |
| 2.1. Coordinate Rings                                | 56        |
| Problem 2.1.*                                        | 56        |
| Problem 2.2.*                                        | 56        |
| Problem 2.3.*                                        | 57        |
| Problem 2.4.*                                        | 58        |
| Problem 2.5.                                         | 58        |
| 2.2. Polynomial Maps                                 | 59        |
| Problem 2.6.*                                        | 59        |

|      |                                                           |     |
|------|-----------------------------------------------------------|-----|
|      | Problem 2.7.* . . . . .                                   | 60  |
|      | Problem 2.8. . . . .                                      | 61  |
|      | Problem 2.9.* . . . . .                                   | 62  |
|      | Problem 2.10.* . . . . .                                  | 63  |
|      | Problem 2.11. . . . .                                     | 63  |
|      | Problem 2.12. . . . .                                     | 65  |
|      | Problem 2.13. . . . .                                     | 66  |
| 2.3. | Coordinate Changes . . . . .                              | 67  |
|      | Problem 2.14.* (Linear subvariety) . . . . .              | 67  |
|      | Problem 2.15.* (Line) . . . . .                           | 70  |
|      | Problem 2.16. . . . .                                     | 73  |
| 2.4. | Rational Functions and Local Rings . . . . .              | 74  |
|      | Problem 2.17. . . . .                                     | 74  |
|      | Problem 2.18. . . . .                                     | 75  |
|      | Problem 2.19. . . . .                                     | 76  |
|      | Problem 2.20. (Quadric surface) . . . . .                 | 76  |
|      | Problem 2.21.* . . . . .                                  | 78  |
|      | Problem 2.22.* . . . . .                                  | 78  |
| 2.5. | Discrete Valuation Rings . . . . .                        | 79  |
|      | Problem 2.23.* . . . . .                                  | 79  |
|      | Problem 2.24.* . . . . .                                  | 79  |
|      | Problem 2.25. ( $p$ -adic integers) . . . . .             | 81  |
|      | Problem 2.26.* . . . . .                                  | 82  |
|      | Problem 2.27. . . . .                                     | 83  |
|      | Problem 2.28.* . . . . .                                  | 84  |
|      | Problem 2.29.* . . . . .                                  | 86  |
|      | Problem 2.30.* . . . . .                                  | 87  |
|      | Problem 2.31. (Formal power series) . . . . .             | 88  |
|      | Problem 2.32. (Power series expansion) . . . . .          | 90  |
| 2.6. | Forms . . . . .                                           | 93  |
|      | Problem 2.33. . . . .                                     | 93  |
|      | Problem 2.34. . . . .                                     | 94  |
|      | Problem 2.35.* . . . . .                                  | 95  |
|      | Problem 2.36. . . . .                                     | 96  |
| 2.7. | Direct Products of Rings . . . . .                        | 97  |
|      | Problem 2.37. . . . .                                     | 97  |
|      | Problem 2.38.* . . . . .                                  | 97  |
| 2.8. | Operations with Ideals . . . . .                          | 97  |
|      | Problem 2.39.* . . . . .                                  | 97  |
|      | Problem 2.40.* (Chinese remainder theorem) . . . . .      | 99  |
|      | Problem 2.41.* . . . . .                                  | 101 |
|      | Problem 2.42.* (Isomorphism theorems for rings) . . . . . | 103 |
|      | Problem 2.43.* . . . . .                                  | 104 |
|      | Problem 2.44.* . . . . .                                  | 104 |
|      | Problem 2.45.* . . . . .                                  | 105 |
|      | Problem 2.46.* . . . . .                                  | 105 |

|                                                             |            |
|-------------------------------------------------------------|------------|
| 2.9. Ideals with a Finite Number of Zeros . . . . .         | 106        |
| Problem 2.47. . . . .                                       | 106        |
| 2.10. Quotient Modules and Exact Sequences . . . . .        | 107        |
| Problem 2.48.* . . . .                                      | 107        |
| Problem 2.49.* . . . .                                      | 107        |
| Problem 2.50.* . . . .                                      | 110        |
| Problem 2.51. . . . .                                       | 111        |
| Problem 2.52.* (Isomorphism theorems for modules) . . . . . | 112        |
| Problem 2.53.* . . . .                                      | 113        |
| 2.11. Free Modules . . . . .                                | 114        |
| Problem 2.54. . . . .                                       | 114        |
| Problem 2.55. . . . .                                       | 115        |
| Problem 2.56. . . . .                                       | 115        |
| <b>Chapter 3: Local Properties of Plane Curves</b>          | <b>117</b> |
| 3.1. Multiple Points and Tangent Lines . . . . .            | 117        |
| Problem 3.1. . . . .                                        | 117        |
| Problem 3.2. . . . .                                        | 118        |
| Problem 3.3. . . . .                                        | 121        |
| Problem 3.4. . . . .                                        | 121        |
| Problem 3.5. . . . .                                        | 122        |
| Problem 3.6. . . . .                                        | 123        |
| Problem 3.7. . . . .                                        | 123        |
| Problem 3.8. . . . .                                        | 127        |
| Problem 3.9. . . . .                                        | 129        |
| Problem 3.10. . . . .                                       | 130        |
| Problem 3.11. (Tangent space) . . . . .                     | 131        |
| 3.2. Multiplicities and Local Rings . . . . .               | 132        |
| Problem 3.12. (Flex) . . . . .                              | 132        |
| Problem 3.13.* . . . .                                      | 133        |
| Problem 3.14. . . . .                                       | 134        |
| Problem 3.15. . . . .                                       | 134        |
| Problem 3.16. . . . .                                       | 136        |
| 3.3. Intersection Numbers . . . . .                         | 137        |
| Problem 3.17. . . . .                                       | 137        |
| Problem 3.18. . . . .                                       | 140        |
| Problem 3.19.* . . . .                                      | 141        |
| Problem 3.20. . . . .                                       | 142        |
| Problem 3.22. (Cusp) . . . . .                              | 142        |
| Problem 3.23. (Hypercusps) . . . . .                        | 144        |
| <b>Chapter 4: Projective Varieties</b>                      | <b>145</b> |
| 4.1. Projective Space . . . . .                             | 145        |
| Problem 4.1. . . . .                                        | 145        |
| Problem 4.2.* . . . .                                       | 145        |
| Problem 4.3. . . . .                                        | 146        |

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| 4.2. Projective Algebraic Sets . . . . .                            | 146        |
| Problem 4.4.* . . . . .                                             | 146        |
| Problem 4.5. . . . .                                                | 147        |
| 4.3. Affine and Projective Varieties . . . . .                      | 147        |
| 4.4. Multiprojective Space . . . . .                                | 147        |
| <b>Chapter 5: Projective Plane Curves</b>                           | <b>148</b> |
| 5.1. Definitions . . . . .                                          | 148        |
| 5.2. Linear Systems of Curves . . . . .                             | 148        |
| 5.3. Bézout's Theorem . . . . .                                     | 148        |
| 5.4. Multiple Points . . . . .                                      | 148        |
| 5.5. Max Noether's Fundamental Theorem . . . . .                    | 148        |
| 5.6. Applications of Noether's Theorem . . . . .                    | 148        |
| <b>Chapter 6: Varieties, Morphisms, and Rational Maps</b>           | <b>149</b> |
| 6.1. The Zariski Topology . . . . .                                 | 149        |
| 6.2. Varieties . . . . .                                            | 149        |
| 6.3. Morphisms of Varieties . . . . .                               | 149        |
| 6.4. Products and Graphs . . . . .                                  | 149        |
| 6.5. Algebraic Function Fields and Dimension of Varieties . . . . . | 149        |
| 6.6. Rational Maps . . . . .                                        | 149        |
| <b>Chapter 7: Resolution of Singularities</b>                       | <b>150</b> |
| 7.1. Rational Maps of Curves . . . . .                              | 150        |
| 7.2. Blowing up a Point in $\mathbf{A}^2$ . . . . .                 | 150        |
| 7.3. Blowing up a Point in $\mathbf{P}^2$ . . . . .                 | 150        |
| 7.4. Quadratic Transformations . . . . .                            | 150        |
| 7.5. Nonsingular Models of Curves . . . . .                         | 150        |
| <b>Chapter 8: Riemann-Roch Theorem</b>                              | <b>151</b> |
| 8.1. Divisors . . . . .                                             | 151        |
| 8.2. The Vector Spaces $L(D)$ . . . . .                             | 151        |
| 8.3. Riemann's Theorem . . . . .                                    | 151        |
| 8.4. Derivations and Differentials . . . . .                        | 151        |
| 8.5. Canonical Divisors . . . . .                                   | 151        |
| 8.6. Riemann-Roch Theorem . . . . .                                 | 151        |

# Chapter 1: Affine Algebraic Sets

## 1.1. Algebraic Preliminaries

### Problem 1.1.\*

Let  $R$  be a domain.

- (a) If  $f, g$  are forms of degree  $r, s$  respectively in  $R[x_1, \dots, x_n]$ , show that  $fg$  is a form of degree  $r + s$ .
- (b) Show that any factor of a form in  $R[x_1, \dots, x_n]$  is also a form.

*Proof of (a).*

- (1) Write

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

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

- (2) Hence,

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

where  $(k) = (i_1 + j_1, \dots, i_n + j_n)$  with  $(i_1 + j_1) + \dots + (i_n + j_n) = r + s$ . 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  $f \in R[x_1, \dots, x_n]$ , and write  $f = gh$ . It suffices to show that  $g$  is a form as well. (So does  $h$ .)
- (2) Write

$$g = g_0 + \dots + g_r, \quad h = h_0 + \dots + h_s$$

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,  $R[x_1, \dots, x_n]$  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

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

where all  $p_1, \dots, p_n, q_1, \dots, q_m$  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

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

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

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

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

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

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

- (4) Conversely, we can apply the argument in (3) to  $i' = 1, \dots, n'$  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,  $f \in k[x_1, \dots, x_n]$ . Suppose  $f(a_1, \dots, a_n) = 0$  for all  $a_1, \dots, a_n \in k$ . Show that  $f = 0$ . (Hint: Write

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

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

*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  $f \in k[x_1, \dots, x_n]$  we can write

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

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

□

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

**Problem 1.5.\***

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

*Proof (Due to Euclid).*

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

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

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

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

and  $k[x]$  is a UFD.

- (2) However,  $f$  would divide the difference

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

contrary to  $\deg f_i \geq 1$ .

□

**Problem 1.6.\***

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

*Proof (Due to Euclid).*

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

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

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

□

**Problem 1.7.\***

Let  $k$  be a field,  $f \in k[x_1, \dots, x_n]$ ,  $a_1, \dots, a_n \in k$ .

(a) Show that

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

(b) If  $f(a_1, \dots, a_n) = 0$ , show that  $f = \sum_{i=1}^n (x_i - a_i)g_i$  for some (not unique)  $g_i$  in  $k[x_1, \dots, x_n]$ .

*Proof of (a).*

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

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

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,  $r \in k[x_1, \dots, x_{n-1}]$  is a constant in  $(k[x_1, \dots, x_{n-1}])[x_n]$ . 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  $f_{i_n} \in k[x_1, \dots, x_{n-1}]$ .

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

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

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

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

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

(4) Or use the induction on  $n$ .

□

*Proof of (b).*

(1) Write

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

by (a).

(2) As  $f(a_1, \dots, a_n) = 0$ ,  $\lambda_{(i)} = 0$  if all  $i_1, \dots, i_n$  are zero, that is, 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

$$f_{(i)} = (x_k - a_k) \underbrace{(\lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_k - a_k)^{i_k-1} \cdots (x_n - a_n)^{i_n})}_{:= g_{(i)} \in k[x_1, \dots, x_n]}.$$

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  $g_1 \in k[x_1, \dots, x_n]$ .

(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  $a_1, \dots, a_m \in k$ . Hence,

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

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  $I = (f_1, \dots, f_m)$ . Note that

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

Now apply the same argument to get the same conclusion.

- (2) Suppose  $k = \bar{k}$ .  $\mathbf{A}^1(k)$  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  $V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\} \subseteq \mathbf{A}^n(k)$  (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  $(r, \theta)$  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)  $S \neq \emptyset$  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  $(0, \frac{\pi}{2}) \in L - Y$ .

□

*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)  $S \neq \emptyset$  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)  $S \neq \emptyset$  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 the disk is called a **cycloid**. The parametrized curve  $\alpha : \mathbb{R} \rightarrow \mathbb{R}^2$  is

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

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

#### Problem 1.14.\*

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

*Proof.*

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

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

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

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

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

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

is infinite.

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

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

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

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

(b) If  $f_n$  is constant in  $k[x_1, \dots, x_{n-1}]$ , then  $f_n$  is nonzero (since  $m > 0$ ) or  $V(f_n) = \emptyset$ . If  $f_n$  is nonconstant in  $k[x_1, \dots, x_{n-1}]$ , 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  $P = (a_1, \dots, a_{n-1}) \in \mathbf{A}^{n-1}(k) - V(f_n)$ ,

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

defines a polynomial in  $k[x_n]$  of degree  $m > 0$ . Since  $k = \bar{k}$ ,  $g_P$  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  $k \neq \bar{k}$ . For example,  $V(x^2 + y^2 + 1) = \emptyset$  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

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

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

*Proof.*

(1) Write

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

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

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

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

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

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

Here we regard  $k$  as a subring of  $k[y_1, \dots, y_m]$ . 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  $x_1, \dots, x_n$ . 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  $f \in k[x_1, \dots, x_n]$  such that  $f(Q) = 0$  for all  $Q \in V$ , but  $f(P) = 1$ . (Hint:  $I(V) \neq I(V \cup \{P\})$ .)
- (b) Let  $P_1, \dots, P_r$  be distinct points in  $\mathbf{A}^n(k)$ , not in an algebraic set  $V$ . Show that there are polynomials  $f_1, \dots, f_r \in I(V)$  such that  $f_i(P_j) = 0$  if  $i \neq j$ , and  $f_i(P_i) = 1$ . (Hint: Apply (a) to the union of  $V$  and all but one point.)
- (c) With  $P_1, \dots, P_r$  and  $V$  as in (b), and  $a_{ij} \in k$  for  $1 \leq i, j \leq r$ , show that there are  $g_i \in I(V)$  with  $g_i(P_j) = a_{ij}$  for all  $i$  and  $j$ . (Hint: Consider  $\sum_j a_{ij} f_j$ .)

*Proof of (a).*

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

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

□

*Proof of (b).*

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

$$W = V \cup \{P_1, \dots, P_r\}$$

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

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

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

□

*Proof of (c).*

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

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

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

- (3) Also,

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

□

### **Problem 1.18.\***

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

- (a)  $0 \in \text{rad}(I)$  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  $\text{rad}(\text{rad}(I)) = \text{rad}(I)$ . It suffices to show  $\text{rad}(\text{rad}(I)) \subseteq \text{rad}(I)$ . Given any  $a \in \text{rad}(\text{rad}(I))$ . By definition  $a^n \in \text{rad}(I)$  for some positive integer  $n$ . Again by definition  $(a^n)^m = a^{nm} \in I$  for some positive integer  $m$ . As  $nm$  is a positive integer,  $a \in \text{rad}(I)$ .

- (4) Show that every prime ideal  $\mathfrak{p}$  is radical. Given any  $a \in \text{rad}(\mathfrak{p})$ , 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,  $I(\emptyset) = (1) \neq (x^2 + 1)$ .

□

**Problem 1.20.\***

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

*Proof.*

- (1) Show that  $V(I) = V(\text{rad}(I))$ . Since  $I \subseteq \text{rad}(I)$ , it suffices to show that  $V(I) \subseteq V(\text{rad}(I))$ . Given any  $P \in V(I)$ . For any  $f \in \text{rad}(I)$ ,  $f^n \in I$  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  $P \in V(\text{rad}(I))$ .

- (2) By Properties (6)(8) in §1.3,

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

□

*Note.*

- (1) By the Hilbert's Nullstellensatz,  $I(V(I)) = \text{rad}(I)$  if  $k = \bar{k}$ .  
 (2) Take  $I = (x^2 + 1)$  as an ideal in  $\mathbb{R}[x]$ . Note that  $I(V(I)) = I(\emptyset) = (1)$  and  $\text{rad}(I) = I = (x^2 + 1)$ . So the equality in  $\text{rad}(I) \subsetneq I(V(I))$  might not hold if  $k \neq \bar{k}$ . (See Problem 1.19.)

**Problem 1.21.\***

Show that  $I = (x_1 - a_1, \dots, x_n - a_n) \subseteq k[x_1, \dots, x_n]$  is a maximal ideal, and that the natural homomorphism from  $k$  to  $k[x_1, \dots, x_n]/I$  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  $\lambda \neq 0$ ,  $J = k[x_1, \dots, x_n]$  is not a proper ideal containing  $I$ .

- (2) Let  $\varphi : k \rightarrow k[x_1, \dots, x_n]/I$  be the natural homomorphism. (That is,  $\varphi : \lambda \rightarrow \lambda + I \in k[x_1, \dots, x_n]/I$ .)
- (3) Show that  $\varphi$  is surjective. Given any  $f + I \in k[x_1, \dots, x_n]/I$ . By Problem 1.7(a),

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

So

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

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

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

- (4) Show that  $\varphi$  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),  $\varphi : k \rightarrow k[x_1, \dots, x_n]/(x_1 - a_1, \dots, x_n - a_n)$  is an isomorphism.

□

## 1.4. The Hilbert Basis Theorem

### Problem 1.22.\* (Correspondence theorem for rings)

Let  $I$  be an ideal in a ring  $R$ ,  $\pi : R \rightarrow R/I$  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  $\{\text{ideals of } R/I\}$  and  $\{\text{ideals of } R \text{ that contain } I\}$ .
- (b) Show that  $J'$  is a radical ideal if and only if  $J$  is radical. Similarly for prime and maximal ideals.

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

*Proof of (a).*

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

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

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

$\pi$  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

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

$\pi$  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  $a_1, \dots, a_m$ . It suffices to show that  $J'$  is generated by

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

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  $a_1 + I, \dots, a_m + I$ .

- (2) *Show 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  $k[x_1, \dots, x_n]/I$  is Noetherian.* By the corollary to the Hilbert basis theorem,  $k[x_1, \dots, x_n]$  is Noetherian. By (2), the ring  $k[x_1, \dots, x_n]/I$  is Noetherian.

□

## 1.5. Irreducible Components of an Algebraic Set

### Problem 1.23.

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

*Proof.*

- (1) Let  $R$  be any Noetherian ring. Let  $\mathcal{S}$  be any collection of ideals containing  $R$  itself. Then the only maximal member of  $\mathcal{S}$  is  $R$ , which is not a maximal ideal.  
(2) Or let  $R$  be any Noetherian ring and  $R$  is not a field. ( $R = k[x_1, \dots, x_n]$  where  $k$  is a field for example.) Let  $\mathcal{S} = \{(0)\}$ . Then the only maximal member of  $\mathcal{S}$  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  $\{\text{proper ideals that contain } I\}$ .)

*Proof.*

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

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

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

- (2) Show that  $\mathfrak{m}$  is maximal. Since  $\mathfrak{m} \in \mathcal{S}$ ,  $\mathfrak{m}$  is a proper ideal in  $R$ . Suppose  $\mathfrak{m}' \supsetneq \mathfrak{m}$  is a proper ideal containing  $\mathfrak{m}$ . As  $\mathfrak{m}$  contains  $I$ ,  $\mathfrak{m}'$  also contains  $I$  or  $\mathfrak{m}' \in \mathcal{S}$ . 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,

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

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

$$f_2(x)g(x) = 1, \quad f_1(x)g(x) = 0, \quad f_0(x)g(x) = x^2(x - 1)^2.$$

Hence,

$$f_2(x)y^2 + f_1(x)y + f_0(x) = uf, \quad g(x) = u^{-1},$$

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  $f_1, f_2 \in k[x_1, \dots, x_n]$  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,  $(f_1 f_2)(a_1, \dots, a_n) = 0$  for any  $a_1, \dots, a_n \in k$ . As  $k$  is infinite,  $f_1 f_2 = 0$  by Problem 1.4. Since  $k[x_1, \dots, x_n]$  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).*  $I(V(x^2 + y^2 + 1)) = I(\emptyset) = (1)$  since  $x^2 + y^2 + 1 \geq 1$  is never zero for any  $x, y \in \mathbb{R}$ .  $\square$

*Proof of (b).*

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

$$f_i(x, y) = (x - a_i)^2 + (y - b_i)^2.$$

By the property of  $\mathbb{R}$ ,  $V_i = V(f_i)$ .

- (4) Define  $f = f_1 \cdots f_m \in \mathbb{R}[x, y]$ . Hence,

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

$\square$

### Problem 1.31.

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

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

*Proof of (a).*

(1) Note that

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

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

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

□

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

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

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

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

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

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

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,  $I(V) = \text{rad}(I)$ . 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  $\alpha : \mathbb{C}[x, y, z]/I \rightarrow \mathbb{C}[t]$  by

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

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

- (b) *Show that  $\alpha$  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  $\alpha$  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

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

So

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

is generated by  $\mathcal{B} = \{\bar{1}, \bar{x}, \bar{y}, \bar{xy}\}$ .

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

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

□

**Problem 1.37.\***

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

*Proof.*

- (1) Show that every element in  $K[x]/(f)$  is generated by  $\mathcal{B} = \{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$ . Given any  $\bar{g} \in K[x]/(f)$  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  $\mathcal{B}$ .

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

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in (f)$$

for  $a_1, \dots, a_{n-1} \in K$ . We can regard any linear combination of  $\{1, x, \dots, x^{n-1}\}$  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,  $a_0 = a_1 = \dots = a_{n-1} = 0 \in K$  and

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



□

**Problem 1.38.\***

Let  $R = k[x_1, \dots, x_n]$ ,  $k$  algebraically closed,  $V = V(I)$ . Show that there is a natural one-to-one correspondence between algebraic subsets of  $V$  and radical ideals in  $k[x_1, \dots, x_n]/I$ , 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,

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

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

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

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

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

□

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

$$f = g^m,$$

and

$$I(V(f)) = (g).$$

- (2) (Reductio ad absurdum) Suppose that there were an irreducible algebraic set  $W$  such that  $V \subsetneq W \subsetneq \mathbf{A}^n$ . Then by Corollary 3 to the Hilbert's Nullstellensatz again,

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

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

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

□

#### Problem 1.40.

Let  $I = (x^2 - y^3, y^2 - z^3) \subseteq k[x, y, z]$ . Define  $\alpha : k[x, y, z] \rightarrow k[t]$  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  $a + xb + yc + xzd$ , 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  $\bar{f} \in k[x, y, z]/I$  where  $f \in k[x, y, z]$ . Regard  $f \in (k[y, z])[x]$ , By the division-with-remainder property of  $(k[y, z])[x]$ ,

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

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

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

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

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

- (3) By  $\bar{r}_0 = \overline{yc + a}$  and  $\bar{r}_1 = \overline{yd + b}$ ,

$$\begin{aligned} \bar{f} &= \bar{r} \\ &= \overline{xr_1} + \bar{r}_0 \\ &= \overline{x(yd + b)} + (\overline{yc + a}) \\ &= \bar{a} + \bar{b} \cdot \bar{x} + \bar{c} \cdot \bar{y} + \bar{d} \cdot \overline{xy}. \end{aligned}$$

□

*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  $\alpha$  is a ring homomorphism. Therefore,

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

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

- (3) Therefore,

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

is injective.

□

## 1.8. Modules; Finiteness Conditions

### Problem 1.41.\*

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

*Proof.*

- (1) Write  $S = \sum Rs_i$  for some  $s_1, \dots, s_n \in S$  since  $S$  is module-finite over  $R$ .
- (2) Show that  $\sum Rs_i = R[s_1, \dots, s_n]$ .  $\sum Rs_i \subseteq R[s_1, \dots, s_n]$  is trivial. Conversely, take any  $v \in R[s_1, \dots, s_n]$ . Write

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

$\in R \quad \in S = \sum Rs_i$

Here each term  $a_{(j)} s_1^{j_1} \cdots s_n^{j_n}$  is in  $\sum Rs_i$ . As  $\sum Rs_i$  is an  $R$ -module,

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

□

*Note.* The converse is not true (by Problem 1.42).

### Problem 1.42.

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

*Proof.*

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

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

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

□

**Problem 1.43.\***

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

*Proof.*

- (1)  $L = K[v_1, \dots, v_n]$  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,  $L = K[v_1, \dots, v_n] = K(v_1, \dots, v_n)$  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  $L = K[v_1, \dots, v_m]$  where  $v_1, \dots, v_m \in L = K(x)$ . Let  $b \in K[x]$  be a common denominator of ring generators  $v_1, \dots, v_m$ . (So that all  $bv_i \in K[x]$ .) Therefore, for any  $z \in L = K[v_1, \dots, v_m]$ , there is an integer  $n > 0$  such that  $b^n z \in K[x]$ .
- (2) Consider  $z = 1/c \in K(x)$ , where  $c \in K[x]$  doesn't divide  $b$ . The existence of  $c$  is guaranteed by Problem 1.5. Hence, for any integer  $n > 0$

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

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

□

**Problem 1.45.\***

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

- (a) If  $S = \sum Rv_i$ ,  $T = \sum Sw_j$ , show that  $T = \sum Rv_iw_j$ .
- (b) If  $S = R[v_1, \dots, v_n]$ ,  $T = S[w_1, \dots, w_m]$ , show that  $T = R[v_1, \dots, v_n, w_1, \dots, w_m]$ .
- (c) If  $R, S, T$  are fields, and  $S = R(v_1, \dots, v_n)$ ,  $T = S(w_1, \dots, w_m)$ , show that  $T = R(v_1, \dots, v_n, w_1, \dots, w_m)$ .

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

*Proof of (a).*

- (1) Show that  $T \subseteq \sum Rv_iw_j$ . Given any  $t \in T = \sum Sw_j$ . There are some  $s_j \in S$  such that  $t = \sum_j s_j w_j$ . 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,

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

- (2) Show that  $T \supseteq \sum Rv_iw_j$ . Take any  $\sum r_{ij} v_i w_j \in \sum Rv_iw_j$ .

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

□

*Proof of (b).*

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

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

□

*Proof of (c).*

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

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

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

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

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

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

(2) Hence,

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

□

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

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

By Proposition 3,

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

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

- (3) Again by the transitive relation of the module-finiteness (Problem 1.45),  $R[a_1, \dots, a_n, z]$  is module-finite over  $R$ . Hence,  $R[a_1, \dots, a_n, z]$  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  $S = R[v_1, \dots, v_m]$  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

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

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  $S = R[v_1, \dots, v_m]$  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  $\alpha_1, \dots, \alpha_m \in k$ . 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  $z^n + a_1z^{n-1} + \cdots + a_n = 0$ , write  $z = f/g$ ,  $f, g$  relatively prime.  
Then  $f^n + a_1f^{n-1}g + \cdots + a_ng^n = 0$ , 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  $z^n + a_1z^{n-1} + \cdots + a_n = 0$  for some  $a_1, \dots, a_n \in K[x]$  and  $a_n \neq 0$  (since  $z \neq 0$ ).
- (3) Write  $z = f/g$ ,  $f, g$  relatively prime in  $K[x]$ . Then

$$f^n + a_1f^{n-1}g + \cdots + a_ng^n = 0 \in K[x].$$

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  $v^n + a_1v^{n-1} + \cdots + a_n = 0$ , 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  $a_1, \dots, a_n \in K$  and  $a_n \neq 0$ . So

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

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  $a_1, \dots, a_n \in K$  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  $\bar{x}$  is the residue of  $x$  in  $L$ , then  $f(\bar{x}) = 0$ .
- (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  $f = (x - \bar{x})f_1$ ,  $f_1 \in L[x]$ .

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

□

*Proof of (b).*

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

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

where  $a_i \in K$ .  $\text{im}(\alpha) = K(y)$  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,  $\alpha$  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),  $\bar{x} \in L$  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

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

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  $\bar{a} = a + (p(x)) \in L'$ .
- (3) By Problem 1.51(a),  $\bar{x}$  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  $\bar{x}$  of  $f(x)$ , say  $f(x) = (x - \bar{x})f_1(x)$  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  $(x - \bar{x})^2$  divides  $f$ , then  $g(\bar{x}) = 0$ .)

*Proof.*

- (1) Since  $f \in K[x]$  is irreducible over  $K$ ,  $\gcd(f, f_x)$  is 1 or  $f$ . As  $\text{char}(K) = 0$ ,  $\deg(f_x) = \deg(f) - 1$ . 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  $\bar{x}$  were a multiple root of  $f$ , then  $f(\bar{x}) = f_x(\bar{x}) = 0$ . By (1),

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

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  $v_1, \dots, v_n$  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

$$v^n + a_1v^{n-1} + \dots + a_n = 0$$

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

- (2) Hence,

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

$av$  is integral over  $R$ .

□

*Proof of (b).*

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

$$\{w_1, \dots, w_n\}$$

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

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

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  $\alpha_1, \dots, \alpha_n \in K$ . Since  $\{w_1, \dots, w_n\}$  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  $\{a_1 w_1, \dots, a_n w_n\}$  is linearly independent.

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

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

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

□

## Chapter 2: Affine Varieties

### 2.1. Coordinate Rings

#### Problem 2.1.\*

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

*Proof.*

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

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

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

- (2)  $\alpha$  is a ring homomorphism by construction in (1).  
 (3) Show that  $\ker(\alpha) = I(V)$ . In fact, given any  $f \in k[x_1, \dots, x_n]$ , we have  $\alpha(f) = 0$  (sending all  $a \in V$  to  $0 \in k$ ) if and only if  $f(a) = 0$  for all  $a \in V$  if and only if  $f \in I(V)$ .  
 (4) Hence,

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

as a ring isomorphism.

□

#### Problem 2.2.\*

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

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



**Problem 2.3.\***

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

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

*Proof of (a).*

- (1) Given any polynomial function  $f \in \mathcal{F}(V, k)$  on  $V$ . There is a polynomial  $g \in k[x_1, \dots, x_n]$  such that  $f(P) = g(P)$  for all  $P \in V \supseteq W$ ; thus  $f(P) = g(P)$  for all  $P \in W$ , or  $f|_W$  is a polynomial function on  $W$ .
- (2) The map  $\alpha : \{\text{polynomial functions in } \mathcal{F}(V, k)\} \rightarrow \{\text{polynomial functions in } \mathcal{F}(W, k)\}$  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  $\mathcal{F}(V, k)$  (resp. in  $\mathcal{F}(W, k)$ ) by Problem 2.1. The map

$$\alpha : \Gamma(V) \rightarrow \Gamma(W)$$

is defined by

$$\alpha(f + I(V)) = f + I(W).$$

It is well-defined by (a).

- (2) Show that  $\alpha$  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  $\alpha$  is a surjective homomorphism,

$$\begin{aligned} \ker(\alpha) &= \Gamma(V)/\Gamma(W) \\ &= (k[x_1, \dots, x_n]/I(V))/(k[x_1, \dots, x_n]/I(W)) \\ &= I(W)/I(V) \\ &= I_V(W). \end{aligned}$$

□

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

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

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

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

(by Problem 1.24).

- (2) (ii)  $\implies$  (iii).  $\dim_k(\Gamma(V)) = \dim_k(k) = 1 < \infty$ .
- (3) (iii)  $\implies$  (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  $y$ :  $f = y^n + a_1(x)y^{n-1} + \dots + a_n(x)$ , 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  $\bar{1}, \bar{y}, \dots, \bar{y}^{n-1}$  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  $\alpha : k[x] \rightarrow \Gamma(V) = k[x, y]/(f)$  by

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

- (2) *Show that  $\alpha$  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,  $\alpha$  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  $r_1, \dots, r_n \in k[x]$ . Hence

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

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

□

## 2.2. Polynomial Maps

### Problem 2.6.\*

Let  $\varphi : V \rightarrow W$ ,  $\psi : W \rightarrow Z$ . 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  $f \in \mathcal{F}(Z, k)$ . 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  $\varphi$  (resp.  $\psi$ ) is a polynomial map, there are polynomials  $t_1, \dots, t_m \in k[x_1, \dots, x_n]$  (resp.  $s_1, \dots, s_r \in k[x_1, \dots, x_m]$ ) such that

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

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

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

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

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

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

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

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

□

### Problem 2.7.\*

If  $\varphi : V \rightarrow W$  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  $\varphi$ , show that  $X$  is irreducible. This gives a useful test for irreducibility.

*Proof.*

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

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

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

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

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

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  $V(xz - y^2, yz - x^3, z^2 - x^2y) \subseteq \mathbf{A}^3(\mathbb{C})$  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  $k = \bar{k}$  is infinite (by Problem 1.29).
- (2) Define a mapping  $\varphi$  from  $\mathbf{A}^1(k)$  to  $Y$  by  $\varphi(t) = (t, t^2, t^3) \in Y$ .  $\varphi$  is a polynomial map. Also,  $\varphi$  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

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

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

- (a) Show that  $\tilde{\varphi}(I_W(W')) \subseteq I_V(V')$  (see Problems 2.3).
- (b) Show that the restriction of  $\varphi$  gives a polynomial map from  $V'$  to  $W'$ .

*Proof of (a).*

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

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

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

□

*Proof of (b).*

(1) Similar to Problem 2.3.

(2) Since  $\varphi$  is a polynomial map, there are polynomials  $t_1, \dots, t_m \in k[x_1, \dots, x_n]$  such that

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

for all  $P \in V$ . So that  $\varphi|_{V'} : V' \rightarrow \varphi(V') \subseteq W'$  is also a polynomial map which is equipped with the same polynomials  $t_1, \dots, t_m$  such that

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

for all  $P \in V' \subseteq V$ . (Note that both  $V'$  and  $W'$  are affine varieties.)

□

**Problem 2.10.\***

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

*Proof.*

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

(2) Clearly,

$$\text{pr}(P) = (t_1(P), \dots, t_r(P))$$

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

□

**Problem 2.11.**

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

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

the **graph** of  $f$ . Show that  $G(f)$  is an affine variety, and that the map  $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, f(a_1, \dots, a_n))$  defines an isomorphism of  $V$  with  $G(f)$ . (Projection gives the inverse.)

*Proof.*

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

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

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

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

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

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

$$\begin{aligned} g &= \sum_i g_i x_{n+1}^i = \sum_i g_i (\underbrace{(x_{n+1} - f) + f}_{\in J})^i, \\ h &= \sum_j h_j x_{n+1}^j = \sum_j h_j (\underbrace{(x_{n+1} - f) + f}_{\in J})^j \end{aligned}$$

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

- (3) Hence

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

or

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

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

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

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

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

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



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

□

**Problem 2.12.**

- (a) Let  $\varphi : \mathbf{A}^1 \rightarrow V = V(y^2 - x^3) \subseteq \mathbf{A}^2$  be defined by  $\varphi(t) = (t^2, t^3)$ . Show that although  $\varphi$  is a one-to-one, onto polynomial map,  $\varphi$  is not an isomorphism. (Hint:  $\tilde{\varphi}(\Gamma(V)) = k[t^2, t^3] \subsetneq k[t] = \Gamma(\mathbf{A}^1)$ .)
- (b) Let  $\varphi : \mathbf{A}^1 \rightarrow V = V(y^2 - x^2(x+1))$  be defined by  $\varphi(t) = (t^2 - 1, t(t^2 - 1))$ . Show that  $\varphi$  is one-to-one and onto, except that  $\varphi(\pm 1) = (0, 0)$ .

*Proof of (a).*

- (1) Similar to Problem 2.8(a),  $\varphi$  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  $\varphi$  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  $\varphi$  is not an isomorphism. It suffices to show that  $\tilde{\varphi}(\Gamma(V)) \subsetneq \Gamma(\mathbf{A}^1)$  by Proposition 1. For any  $f \in \Gamma(V)$ ,

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

Hence,

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

(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

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

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

- (2) By (1),  $\varphi$  is surjective and  $\varphi(\pm 1) = (0, 0)$ .
- (3) Show that  $\varphi$  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,  $\bar{\alpha} : \Gamma(V) \rightarrow k[t]$  induced by the homomorphism  $\alpha$  of that problem.

- (a) What is the polynomial map  $f$  from  $\mathbf{A}^1$  to  $V$  such that  $\tilde{f} = \bar{\alpha}$ ?
- (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,

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

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

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

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

□

*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  $\tilde{f}(\Gamma(V)) \subsetneq \Gamma(\mathbf{A}^1)$  by Proposition 1. For any  $g \in \Gamma(V)$ ,

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

Hence,

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

(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  $V = V(f_1, \dots, f_r)$  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  $V \neq \emptyset$ , show that there is an affine change of coordinates  $t$  of  $\mathbf{A}^n$  such that  $V^t = V(x_{m+1}, \dots, x_n)$ . (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  $V(x_{m+1}, \dots, x_n)^t = V(x_{s+1}, \dots, x_n)$ ,  $m < s$ ; show that  $t_{m+1}, \dots, t_n$  would be dependent.)

*Proof of (a).*

- (1) Say  $t = (t_1, \dots, t_n)$  is an affine change of coordinates, and  $V = V(f_1, \dots, f_r)$  for some polynomials  $f_i$  of degree 1.
- (2)  $V(f_1, \dots, f_r)$  is the set of all solutions of the system of linear equations:

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

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

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

- (3) Linear algebra says that Gaussian elimination transforms  $(A|b)$  into its reduced row echelon form  $(A'|b')$ . Therefore,  $V(Ax = b) = V(A'x = b')$ .
- (4) If  $V(f_1, \dots, f_r) = \emptyset$ , nothing to do. If  $V(f_1, \dots, f_r) \neq \emptyset$ , then

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

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

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

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

where  $f_1 \in k[x_1, \dots, \widehat{x_{i_1}} \dots, x_n]$ . 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

$$f + I(V) = f_1 + I(V) \text{ where } f_1 \in k[x_1, \dots, \widehat{x_{i_1}} \dots, x_n].$$

...

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

Hence, a routine shows that there is a ring isomorphism

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

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

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

□

*Proof of (b).*

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

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

in which  $I_{n-m} \in M_{(n-m) \times (n-m)}(k)$  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

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

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

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

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

□

*Proof of (c).*

- (1) Linear algebra says that the rank of any matrix is the maximal number of its linearly independent rows, which 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  $P = (a_1, \dots, a_n)$ ,  $Q = (b_1, \dots, b_n)$  be distinct points of  $\mathbf{A}^n$ . The **line** through  $P$  and  $Q$  is defined to be  $\{(a_1 + t(b_1 - a_1), \dots, a_n + t(b_n - a_n)) : t \in k\}$ .

- (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  $t = (t_1, \dots, t_n)$  as

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

Take any point  $\alpha_s = (a_1 + s(b_1 - a_1), \dots, a_n + s(b_n - a_n)) \in L$  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

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

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  $a_j \neq b_j$  for some  $1 \leq j \leq n$  since  $P \neq Q$ . Write

$$L = V \left( x_i = a_i + \frac{x_j - a_j}{b_j - a_j} (b_i - a_i) \right)$$

for  $1 \leq i \leq n$  and  $i \neq j$ . 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  $\text{rank}(A'|b') = n - 1$ . 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

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

is a line passing

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

with  $P \neq Q$  (since they are different in the  $j$ th 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  $(-\frac{c}{a}, 0)$  and  $(-\frac{c+b}{a}, 1)$ .

□

*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

$$\begin{aligned} L_1^t &= (L_1^{t'})^{t'} = x \\ L_2^t &= (L_2^{t'})^{t'} = y. \end{aligned}$$

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

$$\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} a_1x + b_1y + c_1 \\ a_2x + b_2y + c_2 \end{pmatrix}$$

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  $\gamma : [0, 1] \rightarrow X$  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  $S := \{P_1, \dots, P_m\} \subseteq \mathbb{C}^n$ .
- (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  $\mathcal{C} := \{L_{P_i} : P_i \in S\}$  (resp.  $\mathcal{C}' := \{L'_{P_i} : P_i \in S\}$ ) is a collection of finitely many lines.
- (3) Consider a unit sphere  $\mathbb{S}^{2n-1}(P)$  centered at  $P$ .

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

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  $L \cap S = \emptyset$ .

- (4) Similarly, we take a line  $L'$  passing  $Q$  and some point in  $\mathbb{S}^{2n-1}(Q)$  where  $L' \cap S = \emptyset$  and  $L' \cap L \neq \emptyset$ . (There are only two points in  $\mathbb{S}^{2n-1}(Q)$  such that  $L' \cap L = \emptyset$ . 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 contained in  $L$ ) and then to  $Q$  (on a segment contained 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  $V = (f_1, \dots, f_r)$  and  $L = \{(a_1 + t(b_1 - a_1), \dots, a_n + t(b_n - a_n)) : t \in k\}$  where  $P = (a_1, \dots, a_n)$  and  $Q = (b_1, \dots, b_n)$ . Then

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

Here  $f_i(a_1 + t(b_1 - a_1), \dots, a_n + t(b_n - a_n))$  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  $\bar{x}, \bar{y}$  the residues of  $x, y$  in  $\Gamma(V)$ ; let  $z = \bar{y}/\bar{x} \in k(V)$ . 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

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

(b) By (a),  $\{(0, 0)\}$  contains 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  $\bar{f}, \bar{g} \in \Gamma(V)$  such that  $z = \bar{y}/\bar{x} = \bar{f}/\bar{g}$  where  $\bar{g}(0, 0) \neq 0$ . So

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

which is absurd.

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

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

□

### Problem 2.18.

Let  $\mathcal{O}_P(V)$  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  $\mathcal{O}_P(V)$  and the subvarieties of  $V$  that pass through  $P$ . (Hint: If  $I$  is prime in  $\mathcal{O}_P(V)$ ,  $I \cap \Gamma(V)$  is prime in  $\Gamma(V)$ , and  $I$  is generated by  $I \cap \Gamma(V)$ ; use Problem 2.2.)

*Proof.*

(1) Write  $P = (a_1, \dots, a_n)$  and  $\mathfrak{m} := (x_1 - a_1, \dots, x_n - a_n)$ . It suffices to show that there is a natural one-to-one correspondence between the prime ideals in  $\mathcal{O}_P(V)$  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  $\mathcal{O}_P(V)$ ,  $\mathfrak{p} \cap \Gamma(V)$  is prime in  $\Gamma(V)$  since  $\Gamma(V)$  is a subring of  $\mathcal{O}_P(V)$ . Note that  $\mathfrak{p} \subseteq \mathfrak{m}_P(V)$  and thus

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

- (3) Conversely, if  $\mathfrak{q}$  is prime in  $\Gamma(V)$  which is contained in  $\mathfrak{m}$  then we need to show that  $\mathfrak{p} := \mathfrak{q}\mathcal{O}_P(V)$  is prime in  $\mathcal{O}_P(V)$ .
- (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  $\frac{a}{b} = a \cdot \frac{1}{b} \in \mathfrak{q}\mathcal{O}_P(V) = \mathfrak{p}$ . 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  $f : U \rightarrow k$  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,  $f : U \rightarrow k$  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  $\bar{x}, \bar{y}, \bar{z}, \bar{w}$  be the residues of  $x, y, z, w$  in  $\Gamma(V)$ . Then

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

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

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

- (2) Show that  $f$  is not defined at the origin  $O = (0, 0, 0, 0)$ . (Reductio ad absurdum) Suppose  $f = \bar{x}/\bar{y} = \bar{a}/\bar{b}$  with  $\bar{b}(O) \neq 0$ . So  $b\bar{x} - \bar{a}\bar{y} = 0$ , 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  $f = \bar{a}/\bar{b}$ , where  $\bar{a}, \bar{b} \in \Gamma(V)$ , and  $\bar{b}(P) \neq 0$  for every  $P$  where  $f$  is defined. (Reductio ad absurdum) Consider the polynomial

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

$\beta$  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  $f = \bar{x}/\bar{y} = \bar{a}/\bar{b}$  where  $\bar{b}(P) \neq 0$ . 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  $\varphi : V \rightarrow W$  be a polynomial map of affine varieties,  $\tilde{\varphi} : \Gamma(W) \rightarrow \Gamma(V)$  the induced map on coordinate rings. Suppose  $P \in V$ ,  $\varphi(P) = Q$ . Show that  $\tilde{\varphi}$  extends uniquely to a ring homomorphism (also written  $\tilde{\varphi}$ ) from  $\mathcal{O}_Q(W)$  to  $\mathcal{O}_P(V)$ . (Note that  $\tilde{\varphi}$  may not extend to all of  $k(W)$ .) Show that  $\tilde{\varphi}(\mathfrak{m}_Q(W)) \subseteq \mathfrak{m}_P(V)$ .

*Proof.*

- (1) Define  $\tilde{\varphi} : \mathcal{O}_Q(W) \rightarrow \mathcal{O}_P(V)$  by

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

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

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

- (2) Note that  $\tilde{\varphi}$  may not extend to all of  $k(W)$  since  $\tilde{\varphi} : k(W) \rightarrow k(V)$  might not be well-defined if  $\tilde{\varphi}(b) = 0$  for all  $b \in \Gamma(W)$ .
- (3) Show that  $\tilde{\varphi}(\mathfrak{m}_Q(W)) \subseteq \mathfrak{m}_P(V)$ . Take any  $a/b \in \mathfrak{m}_Q(W)$  with  $a(Q) = 0$  and  $b(Q) \neq 0$ . As

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

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

□

**Problem 2.22.\***

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

*Proof.*

- (1) Since  $\tilde{t} : \Gamma(\mathbf{A}^n) \rightarrow \Gamma(\mathbf{A}^n)$  is a ring isomorphism, it extends uniquely to a ring isomorphism (also written  $\tilde{t}$ ) from  $\mathcal{O}_Q(\mathbf{A}^n)$  to  $\mathcal{O}_P(\mathbf{A}^n)$  by Problem 2.21.
- (2) Note that  $\mathcal{O}_Q(V) \hookrightarrow \mathcal{O}_Q(\mathbf{A}^n)$ ,  $\mathcal{O}_P(V^t) \hookrightarrow \mathcal{O}_P(\mathbf{A}^n)$ , and  $\tilde{t}(\mathcal{O}_Q(V)) = \mathcal{O}_P(V^t)$ ,  $\tilde{t} : \mathcal{O}_Q(V) \rightarrow \mathcal{O}_P(V^t)$  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  $ut^n = va^mt^m$ . 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  $\mathcal{O}_a(V)$  is a DVR with uniformizing parameter  $t = x - a$ .
- (b) Show that  $\mathcal{O}_\infty = \{f/g \in k(x) : \deg(g) \geq \deg(f)\}$  is also a DVR, with uniformizing parameter  $t = 1/x$ .

*Proof of (a).*

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

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

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

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

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

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

□

*Proof of (b).*

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

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

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,  $\mathcal{O}_\infty$  is a subring of  $k(x)$ .

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

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

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



□

*Note.*

- (1) The quotient field of  $\mathcal{O}_\infty$  is  $K = k(V) = k(x)$ .
- (2) The set of units in  $\mathcal{O}_\infty(V)$  is  $\{f/g \in k(x) : \deg(g) = \deg(f)\}$ .
- (3) The maximal ideal of  $\mathcal{O}_\infty(V)$  is  $\{f/g \in k(x) : \deg(g) > \deg(f)\}$ .

**Problem 2.25. ( $p$ -adic integers)**

Let  $p \in \mathbb{Z}$  be a prime number. Show that

$$\{r \in \mathbb{Q} : r = a/b, a, b \in \mathbb{Z}, p \text{ doesn't divide } b\}$$

is a DVR with quotient field  $\mathbb{Q}$ .

*Proof.*

- (1) Let

$$\mathbb{Z}_p = \{r \in \mathbb{Q} : r = a/b, a, b \in \mathbb{Z}, p \nmid b\}$$

be the set of all  $p$ -adic integers.

- (2) Show that  $\mathbb{Z}_p$  is a subring of  $\mathbb{Q}$ . Clearly,  $1 = 1/1 \in \mathbb{Z}_p$  (since  $p \nmid 1$ ). Also, given any  $r = a/b, s = c/d \in \mathbb{Z}_p$ . So

$$\begin{aligned} r - s &= a/b - c/d = \frac{ad - bc}{bd} \in \mathbb{Z}_p \\ rs &= a/b \cdot c/d = \frac{ac}{bd} \in \mathbb{Z}_p \end{aligned}$$

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

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

Here  $\text{ord}_p : \mathbb{Z} \rightarrow \mathbb{Z}_{\geq 0}$  is defined by  $\text{ord}_p(a) = n$  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  $(\text{ord}_p(a), \text{ord}_p(c)) = (0, 1)$  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  $\mathcal{O}_a(V)$  and  $\mathcal{O}_\infty$  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  $S = \emptyset$ , 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,  $R \supseteq \mathcal{O}_a(V)$  and  $\mathfrak{m}$  contains  $(x - a)\mathcal{O}_a(V)$ , which is the maximal ideal of  $\mathcal{O}_a(V)$ . By Problem 2.26,  $R = \mathcal{O}_a(V)$ .

- (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  $f/g \in \mathcal{O}_\infty$ , 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,  $R \supseteq \mathcal{O}_\infty$  and  $\mathfrak{m}$  contains the maximal ideal  $x^{-1}\mathcal{O}_\infty$  of  $\mathcal{O}_\infty$ . By Problem 2.26,  $R = \mathcal{O}_\infty$ .

- (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  $\varphi$  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  $\text{ord} : K \rightarrow \mathbb{Z} \cup \{\infty\}$  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  $\varphi$ , 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,

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

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)  $R \neq \emptyset$  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  $\varphi$  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  $\varphi$ ). 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  $\text{ord}(\cdot)$  on  $K$  defines an order function  $\varphi$  on  $K$ . By Problem 2.29, it suffices to show that

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

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

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

□

**Problem 2.29.\***

Let  $R$  be a DVR with quotient field  $K$ ,  $\text{ord}$  the order function on  $K$ .

- (a) If  $\text{ord}(a) < \text{ord}(b)$ , show that  $\text{ord}(a+b) = \text{ord}(a)$ .
- (b) If  $a_1, \dots, a_n \in K$ , and for some  $i$ ,  $\text{ord}(a_i) < \text{ord}(a_j)$  (all  $j \neq i$ ), then  $a_1 + \dots + a_n \neq 0$ .

*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  $\text{ord}(a) < \text{ord}(b)$ ,  $n < m$ . Hence,

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

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

- (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. ( $i = 1, \dots, n$ .) Since  $\text{ord}(a_1) < \text{ord}(a_j)$  (all  $j \neq 1$ ),  $m_1 < m_j$ . Hence,

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

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

- (3) By (1)(2),

$$\text{ord}(a_1 + \dots + a_n) = \text{ord}(a_1) < \infty,$$

or  $a_1 + \dots + a_n \neq 0$  (since  $\text{ord}$  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  $k \rightarrow R \rightarrow R/\mathfrak{m}$  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  $\lambda_0, \lambda_1, \dots, \lambda_n \in k$  and  $z_n \in R$  such that

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

(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

$$\mathfrak{m} = \{z \in K : \text{ord}(z) > 0\}.$$

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

$$\text{ord}(\lambda_i t^i) = \begin{cases} \infty & (\lambda_i = 0) \\ i & (\lambda_i \neq 0) \end{cases}$$

since every nonzero element in  $k$  is a unit in  $k \subseteq R$ . Also,  $\text{ord}(z_n t^{n+1}) = \infty$  if  $z_n = 0$ ;  $\text{ord}(z_n t^{n+1}) \geq n+1$  if  $z_n \neq 0$ .

(3) Suppose  $i_0$  is the smallest integer such that  $\lambda_{i_0} \neq 0$ , then  $\text{ord}(\lambda_{i_0} t^{i_0}) = i_0 < \text{ord}(\lambda_j t^j)$  if  $i_0 \neq j$  and  $\text{ord}(\lambda_{i_0} t^{i_0}) = i_0 < n+1 \leq \text{ord}(z_n t^{n+1})$ . 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  $(a_0, a_1, \dots)$  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  $b_1, b_2, \dots$  by induction, and  $(b_0, b_1, \dots)$  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  $\lambda_0, \lambda_1, \dots$  are determined as in Problem 2.30(b).

- (a) Show that the map  $z \rightarrow \sum \lambda_i x^i$  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  $\alpha : R \rightarrow k[[x]]$  by

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

where  $\lambda_i$  are determined as in Problem 2.30(b).

- (2) Show that  $\alpha$  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,  $\alpha$  is well-defined. Also,  $0 = 0 + 0t + 0t^2 + \cdots + 0t^n + 0t^{n+1}$  implies that  $\alpha$  is one-to-one.

(3) *Show that  $\alpha$  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  $i = 0, 1, \dots, n$ . 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  $\alpha$  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

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

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  $i = 0, 1, \dots, n$ . 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  $\alpha$  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),  $\alpha$  is a ring homomorphism.

□

*Proof of (b).*

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

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

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

(2)  $\beta$  is well-defined since:

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

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

(3) Also,  $\beta$  is a ring homomorphism since  $\alpha$  is a ring homomorphism.

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

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

In fact,

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

□

*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

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

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

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

**Problem 2.34.**

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

*Proof.*

(1) Suppose  $f + g = rs \in k[x_1, \dots, x_n]$ . Proposition 5 implies that

$$(f + g)^* = (rs)^* \implies x_{n+1}f + g = r^*s^*.$$

Note that  $\deg_{x_{n+1}}(x_{n+1}f + g) = 1$ . So  $\deg_{x_{n+1}}(r^*) = 0$  or  $\deg_{x_{n+1}}(s^*) = 0$ . Might assume  $\deg_{x_{n+1}}(r^*) = 0$ . (The case  $\deg_{x_{n+1}}(s^*) = 0$  is similar.)

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

□

**Problem 2.35.\***

- (a) Show that there are  $d + 1$  monomials of degree  $d$  in  $R[x, y]$ , and  $1 + 2 + \cdots + (d + 1) = \frac{(d+1)(d+2)}{2}$  monomials of degree  $d$  in  $R[x, y, z]$ .
- (b) Let  $V(d, n) = \{\text{forms of degree } d \text{ in } k[x_1, \dots, x_n]\}$ ,  $k$  a field. Show that  $V(d, n)$  is a vector space over  $k$ , and that the monomials of degree  $d$  form a basis. So  $\dim V(d, 1) = 1$ ;  $\dim V(d, 2) = d + 1$ ;  $\dim V(d, 3) = \frac{(d+1)(d+2)}{2}$ .
- (c) Let  $\ell_1, \ell_2, \dots$  and  $m_1, m_2, \dots$  be sequences of nonzero linear forms in  $k[x, y]$ , and assume no  $\ell_i = \lambda m_j$ ,  $\lambda \in k$ . Let  $A_{ij} = \ell_1 \ell_2 \cdots \ell_i m_1 m_2 \cdots m_j$ ,  $i, j \geq 0$  ( $A_{00} = 1$ ). Show that  $\{A_{ij} : i + j = d\}$  forms a basis for  $V(d, 2)$ .

*Proof of (a).*

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

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

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

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

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

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

□

*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  $k[x_1, \dots, x_n]$  since  $k[x_1, \dots, x_n]$  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

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

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

- (4) Similar to (a),

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

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  $\mathcal{B}' := \{A_{ij} : i + j = d\}$  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

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

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

- (3) Since

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

$\mathcal{B}'$  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  $\times R_i$ ? Is the map from  $R_i$  to  $\times R_i$  taking  $a_i$  to  $(0, \dots, a_i, \dots, 0)$  a ring homomorphism?

*Proof.*

- (1)  $(0, \dots, 0)$  is the additive identity in  $\times R_i$ .
- (2)  $(1, \dots, 1)$  is the multiplicative identity in  $\times R_i$ .
- (3) The map  $\alpha : R_i \rightarrow \times R_i$  taking  $a_i$  to  $(0, \dots, a_i, \dots, 0)$  is not a ring homomorphism since

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

or  $\alpha$  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  $\dim(\times R_i) = \sum \dim(R_i)$ .

*Proof.*

- (1) In the terminology of linear algebra,  $\times R_i$  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  $1 \leq k \leq N$ . Hence

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

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

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

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

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

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

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

□

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

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

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  $I_1 \cdots I_N = I_1 \cap \dots \cap I_N$ . Induction on  $N$ .

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

- (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  $I \subseteq \text{rad}(J)$ . Show that  $I^n \subseteq J$  for some  $n$ .

*Proof.*

- (1) Let  $I$  be generated by  $x_1, \dots, x_m \in I$ . As  $I \subseteq \text{rad}(J)$ , 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,

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

□

**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  $\text{rad}(I)$  is finitely generated, then for some integer  $N$  we have  $(\text{rad}(I))^N \subseteq I$ . 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  $I, J \subseteq S = k[x_1, \dots, x_n]$  are ideals and  $k$  is algebraically closed, then  $Z(I) = Z(J)$  iff  $I^N \subseteq J$  and  $J^N \subseteq I$  for some  $N$ .

*Proof.*

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

- (a) For each  $i$ , there exists an integer  $n_i > 0$  such that  $x_i^{n_i} \in I$  (since  $\text{rad}(I)$  is radical).  
(b) Let  $N = n_1 + \dots + n_m$ . Given any  $x = \sum_{i=1}^m r_i x_i \in \text{rad}(I)$ , so

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

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

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

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

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

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

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

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

- (3) Show that if  $I, J \subseteq S = k[x_1, \dots, x_n]$  are ideals and  $k$  is algebraically closed, then  $Z(I) = Z(J)$  iff  $I^N \subseteq J$  and  $J^N \subseteq I$  for some  $N$ . Note that  $S$  is Noetherian and we can apply part (2). By the Nullstellensatz,  $Z(I) = Z(J)$  iff  $\text{rad}(I) = \text{rad}(J)$  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  $\alpha : R/I \rightarrow R/J$  by  $\alpha(r + I) = r + J$ .
- (2) Show that  $\alpha$  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  $\alpha$  is a surjective homomorphism.
- (a)  $\alpha$  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)  $\alpha$  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)  $\alpha$  is multiplicative identity preserving.  $\alpha(1 + I) = 1 + J$ .

- (d)  $\alpha$  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  $\alpha : R/I \rightarrow S/IS$  by  $\alpha(r + I) = r + IS$ . Note that  $I \subseteq IS$  as a subset in  $S$ . Apply the same argument in (a),  $\alpha$  is well-defined and  $\alpha$  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  $P = (0, \dots, 0) \in \mathbf{A}^n$ ,  $\mathcal{O} = \mathcal{O}_P(\mathbf{A}^n)$ ,  $\mathfrak{m} = \mathfrak{m}_P(\mathbf{A}^n)$ . Let  $I = (x_1, \dots, x_n) \subseteq k[x_1, \dots, x_n]$  be the ideal generated by  $x_1, \dots, x_n$ . Show that  $I\mathcal{O} = \mathfrak{m}$ , so  $I^r\mathcal{O} = \mathfrak{m}^r$  for all  $r$ .

*Proof.*

- (1) By the definition

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

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

- (2) By Problem 2.39(b),

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

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

□

**Problem 2.44.\***

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

*Proof.*



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

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

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

- (2) Note that  $V$  is a subvariety of  $\mathbf{A}^n$ . So  $\varphi : \Gamma(\mathbf{A}^n) \rightarrow \Gamma(V)$  is a ring homomorphism by Problem 2.3 and then  $\varphi$  extends uniquely to a ring homomorphism by using the similar argument in Problem 2.21.
- (3)  $\varphi$  is surjective since  $\mathcal{O}_P(\mathbf{A}^n) \hookrightarrow \mathcal{O}_P(V)$  and  $\varphi(J\mathcal{O}_P(\mathbf{A}^n)) = J'\mathcal{O}_P(V)$ .  $\varphi$  is injective since  $\varphi(J\mathcal{O}_P(\mathbf{A}^n)) = J'\mathcal{O}_P(V)$ . Hence  $\varphi : \mathcal{O}_P(\mathbf{A}^n)/J \rightarrow \mathcal{O}_P(V)/J'$  is isomorphic. In particular,  $\mathcal{O}_P(\mathbf{A}^n)/I\mathcal{O}_P(\mathbf{A}^n) \cong \mathcal{O}_P(V)$  (by taking  $J = I$  and noting that  $J' = I' = 0$ ).

□

**Problem 2.45.\***

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

*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,

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

□

**Problem 2.46.\***

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

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

*Proof.*

(1) The set

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

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  $\mathcal{B}$  is an independent set. Therefore,  $\mathcal{B}$  is a basis for  $k[x, y]/I^n$ .

(2) Hence,

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

□

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

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

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

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

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

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

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

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

which is isomorphic to a direct product of local rings.

□

## 2.10. Quotient Modules and Exact Sequences

### Problem 2.48.\*

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

$$0 \rightarrow \ker(\varphi) \rightarrow M \xrightarrow{\varphi} \text{im}(\varphi) \rightarrow 0$$

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

$$0 \rightarrow \ker(\varphi) \xrightarrow{i} M \xrightarrow{\varphi} \text{im}(\varphi) \rightarrow 0$$

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

□

### Problem 2.49.\*

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

- (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*

$$0 \rightarrow N/P \rightarrow M/P \rightarrow M/N \rightarrow 0$$

*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:*

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

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

$$0 \rightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^n \rightarrow 0.$$

*Proof of (a).*

- (1) Define  $\bar{\varphi} : M/N \rightarrow M'$  by

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

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

- (2)  $\bar{\varphi}$  is a homomorphism of  $R$ -modules since  $\varphi$  is a homomorphism of  $R$ -modules.
- (3)  $\bar{\varphi} \circ \pi = \varphi$  by construction.
- (4) Suppose there is a homomorphism  $\psi : M/N \rightarrow M'$  such that  $\psi \circ \pi = \varphi$ . For any  $m + N \in M/N$ , we have

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

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

□

*Proof of (b).*

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

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

- (a) *Show that  $\pi$  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)  $\pi$  is a module homomorphism since  $M/N$  is a module.
- (c)  $\pi$  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  $0 \rightarrow N/P \rightarrow M/P \rightarrow M/N \rightarrow 0$  is exact, it suffices to show that  $\ker(\pi) = \text{im}(i) = N/P$  (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),

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

is exact.

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

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

□

*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

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

□

*Proof of (e).*

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

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

$$0 \rightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^n \rightarrow 0.$$

□

**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  $\text{ord}(z) = n$  if  $(z) = \mathfrak{m}^n$ , and hence that  $\text{ord}(z) = \dim_k(R/(z))$ .

*Proof of (a).*

- (1) By Problem 2.49(e),

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

is exact.

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

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

□

*Proof of (b).*

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

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

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

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

- (2)  $\varphi$  is well-defined by the uniqueness of the expression of  $z$  in Problem 2.30(b).  $\varphi$  is a  $k$ -module homomorphism and  $\varphi$  is surjective (since  $k \subseteq R$ ).  $\varphi$  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  $(z) = (t^n) = \mathfrak{m}^n$ ,  $\text{ord}(z) = n$  by Problem 2.28. (Here  $\text{ord}(z) \geq n$  by  $z \in (t^n)$  and  $n \geq \text{ord}(z)$  by  $t^n \in (z)$ .)

- (3) Hence,

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

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

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

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

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

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

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

Hence,

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

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

□

**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  $\varphi : N \rightarrow M/P$  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,  $\varphi$  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,  $T : V \rightarrow V$  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  $\bar{T} : V/W \rightarrow T(V)/T(W)$  by

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

- (2) Show that  $\bar{T}$  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)  $\bar{T}$  is a linear map since  $T$  is a linear map.
- (4)  $\bar{T}$  is surjective by construction. Also,  $\bar{T}$  is injective since  $T$  is injective. Therefore,  $\bar{T} : V/W \xrightarrow{\sim} T(V)/T(W)$  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  $m_1, \dots, m_n$  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  $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$ , where  $\bar{x}$  is the residue of  $x$ .

*Proof.*

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

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

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

$$\mathcal{B} := \{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}.$$

- (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,

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

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

□

**Problem 2.56.**

Show that a subset  $X$  of a module  $M$  generates  $M$  if and only if the homomorphism  $M_X \rightarrow M$  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  $\delta_{xy}$  is the Kronecker delta. Hence, the homomorphism  $\alpha : M_X \rightarrow M$  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  $\alpha : M_X \rightarrow M$  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  $\varphi : F \rightarrow M$  by

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

$\varphi$  is well-defined.  $\varphi$  is a module homomorphism.  $\varphi$  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)

$$\begin{aligned}\frac{\partial c}{\partial x} &= -3x^2 = 0 \\ \frac{\partial c}{\partial y} &= 2y = 0\end{aligned}$$

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)

$$\begin{aligned}\frac{\partial d}{\partial x} &= -3x^2 - 2x = 0 \\ \frac{\partial d}{\partial y} &= 2y = 0\end{aligned}$$

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

(3)

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

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

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

implies that

$$\begin{aligned}6(x + y)^2 &= 0 \\ -4(x - y) &= 0\end{aligned}$$

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

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

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

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

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

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

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

$$10x \pm y$$

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

□

### 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.**

( $\text{char}(k) = 0$ ) 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  $\ell_i$  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  $(r, \theta)$  satisfy the equation  $r = -\sin(3\theta)$ . Find the polar equation for the curve  $f$ .
- (b) If  $n$  is an odd integer  $\geq 1$ , 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  $\sin(n\theta) = \operatorname{im}(e^{in\theta})$  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

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

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  $k = 0, 1, \dots, n-1$ . All  $\ell_k$  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  $k = 0, 1, \dots, n-1$ .

□

*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  $c \in \mathbb{C}$ ),  $\alpha_{n+1}$  and  $\alpha_n$  have no common factors in  $\mathbb{C}[x, y]$ .  
By Problem 2.34,  $\alpha$  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

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

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  $\beta_{2n}$  and  $\beta_{2n+2}$  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

$$\begin{aligned} r_p s_q &= - \left( \sum_{k=0}^{\frac{n-2}{2}} (-1)^k \binom{n}{2k+1} x^{n-2k-1} y^{2k+1} \right)^2 \\ r_p s_{q+1} + r_{p+1} s_q &= 0 \\ r_{p+1} s_{q+1} &= (x^2 + y^2)^{n+1} = (x + iy)^{n+1} (x - iy)^{n+1}. \end{aligned}$$

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),  $\beta$  is irreducible over  $\mathbb{C}$ .

□

### Problem 3.8.

Let  $t : \mathbf{A}^2 \rightarrow \mathbf{A}^2$  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,

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

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

- (2) Define

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

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,

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

is not invertible. □

### Problem 3.9.

Let  $f \in k[x_1, \dots, x_n]$  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  $P = (0, \dots, 0)$ . Write  $f = f_m + f_{m+1} + \dots + f_n$ , where  $f_i$  is a form in  $k[x_1, \dots, x_n]$  of degree  $i$ ,  $f_m \neq 0$ . We define  $m$  to be the multiplicity of  $f$  at  $P = (0, \dots, 0)$ , write  $m = m_P(f)$ .
- (2) To extend these definitions to a point  $P = (a_1, \dots, a_n) \neq (0, \dots, 0)$ , let  $t$  be the translation that takes  $(0, \dots, 0)$  to  $P$ , i.e.,

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

Then

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

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

□

*Proof of (b).*

- (1) Let  $P = (0, \dots, 0)$ . Write  $f = f_m + f_{m+1} + \dots + f_n$ , where  $f_i$  is a form in  $k[x_1, \dots, x_n]$  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  $P = (a_1, \dots, a_n) \neq (0, \dots, 0)$  is  $g_1$  where

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

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

□

*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  $\text{char}(k) = 0$ , 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. Let

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

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

- (2) 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  $f = x_2^2 - x_1^3 \in k[x_1, \dots, x_n]$ . The set of the multiple (singular) points of  $f$  is

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

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

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

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

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

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

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

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

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

(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  $\text{ord}_P^f(L) \geq 3$ , where  $L$  is the tangent to  $f$  at  $P$ . The flex is called **ordinary** if  $\text{ord}_P(L) = 3$ , 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  $\text{ord}_P^f(y)$ , 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

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

$P$  is a higher flex.

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

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

Here  $x$  is a uniformizing parameter for  $\mathcal{O}_P(f)$  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,  $\text{ord}_P^f(y) \geq 2$ . By Problem 2.29(a),

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

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

(2) In general,

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

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

$$0 \rightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^{n+1} \rightarrow \mathcal{O}/\mathfrak{m}^n \rightarrow 0,$$

it suffices to show that

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

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,

$$\begin{aligned} \dim_k(\mathcal{O}/\mathfrak{m}^n) &= \dim_k(k[x, y]/(I^n, f)) \\ &= \dim_k(k[x, y]/I^n) \\ &= \frac{n(n+1)}{2}. \end{aligned} \quad (\text{Problem 2.46})$$

So

$$\dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_k(\mathcal{O}/\mathfrak{m}^{n+1}) - \dim_k(\mathcal{O}/\mathfrak{m}^n) = n + 1.$$

(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  $\mathcal{O} = \mathcal{O}_P(V)$ . By Problem 1.40(a), every element of  $\mathcal{O}$  is of the form

$$\bar{a} + \bar{x}\bar{b} + \bar{y}\bar{c} + \bar{x}\bar{y}\bar{d}$$

for some  $a, b, c, d \in k[z]$ .

(3) By (1)(2),  $\{\bar{1}\}$  (resp.  $\{\bar{1}, \bar{z}, \bar{y}, \bar{z}\}$ ) is a basis for  $\mathcal{O}/\mathfrak{m}$  (resp.  $\mathcal{O}/\mathfrak{m}^2$ ). Hence,  $\dim_k(\mathcal{O}/\mathfrak{m}) = 1$  (resp.  $\dim_k(\mathcal{O}/\mathfrak{m}^2) = 4$ ). Therefore,

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathcal{O}/\mathfrak{m}^2) - \dim_k(\mathcal{O}/\mathfrak{m}) = 3$$

by Proposition 7 in §2.10.

(4) By Theorem I.5.1 in *Robin Hartshorne, Algebraic Geometry*,

$$3 = \dim_k(\mathfrak{m}/\mathfrak{m}^2) + \text{rank} J = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

Here the Jacobian matrix of  $V$  at  $P$

$$J = \left[ \frac{\partial f_i}{\partial x_j}(P) \right] = \begin{bmatrix} 2x & -3y^2 & 0 \\ 0 & 2y & -3z^2 \end{bmatrix}_{P=(0,0,0)} = 0$$

has rank zero.

□

**Problem 3.15.**

(a) Let  $\mathcal{O} = \mathcal{O}_P(\mathbf{A}^2)$  for some  $P \in \mathbf{A}^2$ ,  $\mathfrak{m} = \mathfrak{m}_P(\mathbf{A}^2)$ . Calculate  $\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n)$ .

(b) Let  $\mathcal{O} = \mathcal{O}_P(\mathbf{A}^r(k))$ . 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

$$\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[x, y]/(x, y)^n) = \frac{n(n+1)}{2}.$$

□

*Proof of (b).*

(1) Might assume that  $P = (0, \dots, 0)$ . Similar to (a),

$$\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n) = \dim_k(k[x_1, \dots, x_r]/(x_1, \dots, x_r)^n).$$

(2) Since

$$\mathcal{B} = \{x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r} : i_1 + \cdots + i_r < n\}$$

is a basis for  $k[x_1, \dots, x_r]/(x_1, \dots, x_r)^n$ ,

$$\dim_k(k[x_1, \dots, x_r]/(x_1, \dots, x_r)^n) = |\mathcal{B}|.$$

(3) By the stars and bars (combinatorics) method (as Problem 2.35(b)),

$$\begin{aligned} |\mathcal{B}| &= |\{(i_1, \dots, i_r) : i_1 + \cdots + i_r \leq n\}| \\ &\quad - |\{(i_1, \dots, i_r) : i_1 + \cdots + i_r = n\}| \\ &= |\{(i_1, \dots, i_r, j) : i_1 + \cdots + i_r + j = n\}| \\ &\quad - |\{(i_1, \dots, i_r) : i_1 + \cdots + i_r = n\}| \\ &= \binom{n+r}{r} - \binom{n+r-1}{r-1} \\ &= \binom{n+r-1}{r} \\ &= \frac{1}{r!} (n+r-1)(n+r-2) \cdots (n+1)(n). \end{aligned}$$

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

$$\begin{aligned} \dim_k(k[x_1, \dots, x_r]/(x_1, \dots, x_r)^n) &= \sum_{i=0}^{n-1} \dim_k V(i, r) \\ &= \sum_{i=0}^{n-1} \binom{i+r-1}{r-1} \\ &= \binom{n+r-1}{r} \end{aligned}$$

by the Pascal's identity.

□

**Problem 3.16.**

Let  $f \in k[x_1, \dots, x_r]$  define a hypersurface in  $\mathbf{A}^r$ . Write  $f = f_m + f_{m+1} + \dots$ , and let  $m = m_P(f)$  where  $P = (0, \dots, 0)$ . Suppose  $f$  is irreducible, and let  $\mathcal{O} = \mathcal{O}_P(V(f))$ ,  $\mathfrak{m}$  its maximal ideal. Show that  $\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n)$  is a polynomial of degree  $r-1$  for sufficiently large  $n$ , and that the leading coefficient of  $\chi$  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,

$$\mathfrak{m}^n = I^n \mathcal{O}$$

where  $I = (x_1, \dots, x_r) \subseteq k[x_1, \dots, x_r]$ . Since  $V(I^n) = \{P\}$ ,

$$k[x_1, \dots, x_r]/(I^n, f) \cong \mathcal{O}_P(\mathbf{A}^r)/(I^n, f) \mathcal{O}_P(\mathbf{A}^r) \cong \mathcal{O}/I^n \mathcal{O} \cong \mathcal{O}/\mathfrak{m}^n$$

(Corollary 2 to Proposition 6 in §2.9 and Problem 2.44).

- (2) So we are reduced to calculating the dimension of  $k[x_1, \dots, x_r]/(I^n, f)$ . As  $n \geq m = m_P(f)$ , there is a natural ring homomorphism

$$\varphi : k[x_1, \dots, x_r]/I^n \rightarrow k[x_1, \dots, x_r]/(I^n, f)$$

and a  $k$ -linear map

$$\psi : k[x_1, \dots, x_r]/I^{n-m} \rightarrow k[x_1, \dots, x_r]/I^n$$

defined by  $\bar{g} \mapsto \overline{fg}$ . It is easy to verify that the sequence

$$0 \rightarrow k[x_1, \dots, x_r]/I^{n-m} \xrightarrow{\psi} k[x_1, \dots, x_r]/I^n \xrightarrow{\varphi} k[x_1, \dots, x_r]/(I^n, f) \rightarrow 0$$

is exact.

- (3) By Problem 3.15,

$$\begin{aligned} & \dim_k(k[x_1, \dots, x_r]/(I^n, f)) \\ &= \binom{n+r-1}{r} - \binom{n-m+r-1}{r} \\ &= \frac{1}{r!} ((n+r-1) \cdots n - (n-m+r-1) \cdots (n-m)) \\ &= \frac{1}{r!} (n^{r-1}(rm) + \cdots) \\ &= \frac{m}{(r-1)!} n^{r-1} + \cdots. \end{aligned}$$

Therefore,  $\chi(n) = \dim_k(\mathcal{O}/\mathfrak{m}^n)$  is a polynomial of degree  $r-1$  for  $n \geq m$ , and that the leading coefficient of  $\chi$  is  $\frac{m_P(f)}{(r-1)!}$ .



(4) It is reasonable to define the multiplicity of a Noetherian local ring  $\mathcal{O}$  by

$$(d!) \cdot (\text{leading coefficient of } \chi(n))$$

for sufficiently large  $n$ , where  $d$  is the dimension (or Krull dimension) of  $\mathcal{O}$ . (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,

$$I(P, a \cap b) = m_P(a)m_P(b) = 1 \cdot 1 = 1$$

$$I(P, a \cap d) = m_P(a)m_P(d) = 1 \cdot 2 = 2$$

$$I(P, b \cap c) = m_P(b)m_P(c) = 1 \cdot 2 = 2$$

$$I(P, b \cap d) = m_P(b)m_P(d) = 1 \cdot 2 = 2$$

$$I(P, b \cap e) = m_P(b)m_P(e) = 1 \cdot 3 = 3$$

$$I(P, c \cap d) = m_P(c)m_P(d) = 2 \cdot 2 = 4$$

$$I(P, d \cap e) = m_P(d)m_P(e) = 2 \cdot 3 = 6$$

$$I(P, d \cap f) = m_P(d)m_P(f) = 2 \cdot 4 = 8$$

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

$$\begin{aligned}
I(P, a \cap f) &= I(P, a \cap \underbrace{(f + q_4a)}_{\text{(Property (7))}}) \\
&= I(P, a \cap y^3(y^3 + 3y^2 + 3y - 3)) \\
&\quad \text{(Property (6))} \\
&= \underbrace{3I(P, a \cap y)}_{=2 \text{ (by (3))}} + \underbrace{I(P, a \cap (y^3 + 3y^2 + 3y - 3))}_{=0 \text{ (Property (2))}} \\
&= 6.
\end{aligned}$$

(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

$$\begin{aligned}
& I(P, b \cap f) \\
&= I(P, b \cap \underbrace{(f + q_5 b)}_{\text{(Property (7))}}) \\
&= I(P, b \cap x^3(x^6 + 3x^5 - 5x^3 - 4x^2 + 3x + 3)) \\
&\quad \text{(Property (6))} \\
&= \underbrace{3I(P, b \cap x)}_{=2} + \underbrace{I(P, b \cap (x^6 + 3x^5 - 5x^3 - 4x^2 + 3x + 3))}_{=0 \text{ (Property (2))}} \\
&= 6.
\end{aligned}$$

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).

$$\begin{aligned}
I(P, c \cap e) &= I(P, c \cap \underbrace{(e + (-x^3 - 2x^2 - y^2 + y)c)}_{\text{(Property (7))}}) \\
&= I(P, c \cap x^2(x^4 + 2x^3 + x^2 - xy + 3y)) \\
&\quad \text{(Property (6))} \\
&= 2 \underbrace{I(P, c \cap x)}_{=2 \text{ (Property (5))}} + I(P, c \cap \underbrace{(x^4 + 2x^3 + x^2 - xy + 3y)}_{:=h_6}) \\
&= 4 + I(P, c \cap h_6).
\end{aligned}$$

Here

$$\begin{aligned}
& I(P, c \cap h_6) \\
&= I(P, (3c) \cap h_6) \\
&= I(P, (3c - yh_6) \cap h_6) \\
&= I(P, (-x^4y - 2x^3y - \underbrace{3x^3 - x^2y + xy^2}_{\text{}}) \cap (x^4 + 2x^3 + x^2 - xy + \underbrace{3y}_{\text{}})) \\
&= 3 \cdot 1 \\
&= 3
\end{aligned}$$

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

$$q_7 = -x^6 - 3x^5 - x^3y^2 - 3x^4 - 3x^2y^2 - y^4 + 4x^2.$$

So

$$\begin{aligned}
& I(P, c \cap f) \\
&= I(P, c \cap \underbrace{(f + q_7 c)}_{\text{(Property (7))}}) \\
&= I(P, c \cap x^5(x^4 + 3x^3 + 3x^2 + x - 4)) \\
&\quad \text{(Property (6))} \\
&= \underbrace{5 I(P, c \cap x)}_{=2} + \underbrace{I(P, c \cap (x^4 + 3x^3 + 3x^2 + x - 4))}_{=0 \text{ (Property (2))}} \\
&= 10.
\end{aligned}$$

□

**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  $I(P, f \cap g) = \text{ord}_P^f(g)$ .

*Proof.*

- (1) Might assume that  $f$  is irreducible. There is nothing to prove if  $\text{ord}_P^f(g) = \infty$ . Might assume that  $n = \text{ord}_P^f(g) < \infty$ .
- (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  $\mathcal{O}_P(f)$  (Theorem 1 in §3.2).
- (3) By definition,

$$g = ux^n$$

for some unit in  $\mathcal{O}_P(f)$ . 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),

$$\begin{aligned}
 I(P, f \cap L) &> m_P(f) = m_P(f)m_P(L) \\
 \iff f \text{ and } L &\text{ have one common tangent line at } P \\
 \iff L \text{ is tangent} &\text{ to a curve } f \text{ at } P. && \text{(By (1))}
 \end{aligned}$$

□

**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)

$$\begin{aligned} I(P, f \cap (g+h)) &= \text{ord}_P^f(g+h) && \text{(Property (8))} \\ &\geq \min\{\text{ord}_P^f(g), \text{ord}_P^f(h)\} && \text{(Problem 2.28)} \\ &= \min\{I(P, f \cap g), I(P, f \cap h)\}. && \text{(Property (8))} \end{aligned}$$

- (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 3.22. (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  $\text{char}(k) = 0$ .

*Proof of (a).*

- (1) By Property (5),

$$I(P, f \cap L) \geq m_P(f)m_P(L) = 2 \cdot 1 = 2.$$

Here  $m_P(f) = 2$  since  $P$  is a double point on a curve  $f$ .

- (2) The equality does not hold since  $f$  has one tangent  $L$  (Property (5)).  
Therefore,  $I(P, f \cap L) \geq 3$  since  $I(P, f \cap L)$  is an integer (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 occurring if and only if  $y$  is not a tangent line of  $f_3 + f_4 + \cdots$  (Property (5)).

- (3) Note that

$$\begin{aligned} &y \text{ is not a tangent line of } f_3 + f_4 + \cdots \\ \iff &y \nmid f_3 \\ \iff &\frac{\partial^3 f}{\partial x^3}(P) \neq 0. \end{aligned} \quad (\text{Problem 3.5})$$

- (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

$$\begin{aligned} f &= y^2 + f_3 + f_4 + \cdots \\ g &= g_r + g_{r+1} + \cdots \\ h &= h_s + h_{s+1} + \cdots \end{aligned}$$

where  $f_\alpha, g_\beta, h_\gamma$  is a form in  $k[x, y]$ . So  $f = gh$  implies that

$$\begin{aligned} y^2 + f_3 + f_4 + \cdots &= (g_r + g_{r+1} + \cdots)(h_s + h_{s+1} + \cdots) \\ &= (g_r h_s) + (g_r h_{s+1} + g_{r+1} h_s) + \cdots \end{aligned}$$

Hence  $y^2 = g_r h_s$ . In particular,  $2 = r + s$ .

(3) If  $y \mid g_r$  and  $y \mid h_s$ , then

$$\begin{aligned} I(P, g \cap L) > m_P(g)m_P(L) = r &\implies I(P, g \cap L) \geq r + 1 \\ I(P, h \cap L) > m_P(h)m_P(L) = s &\implies I(P, h \cap L) \geq s + 1. \end{aligned}$$

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  $g = 1 + g_1 + \dots$  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  $m_P(f)$ . □



## 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  $f \in k[x_1, \dots, x_{n+1}]$  ( $k$  infinite). Write  $f = \sum f_i$ ,  $f_i$  a form of degree  $i$ . Let  $P \in \mathbf{P}^n(k)$ , and suppose  $f(x_1, \dots, x_{n+1}) = 0$  for every choice of homogeneous coordinates  $(x_1, \dots, x_{n+1})$  for  $P$ . Show that each  $f_i(x_1, \dots, x_{n+1}) = 0$  for all homogeneous coordinates for  $P$ . (Hint: consider

$$g(\lambda) = f(\lambda x_1, \dots, \lambda x_{n+1}) = \sum \lambda^i f_i(x_1, \dots, x_{n+1})$$

for fixed  $(x_1, \dots, x_{n+1})$ .)

*Proof.*

- (1) Consider

$$g(\lambda) = f(\lambda x_1, \dots, \lambda x_{n+1}) = \sum \lambda^i f_i(x_1, \dots, x_{n+1})$$

for fixed  $(x_1, \dots, x_{n+1})$ .  $g(\lambda)$  is a polynomial in  $k[\lambda]$ .

- (2) Since  $g(\lambda) = f(\lambda x_1, \dots, \lambda x_{n+1}) = 0$  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  $f_i(x_1, \dots, x_{n+1}) = 0$  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  $k$ .  $\square$

*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  $P \neq (0, \dots, 0)$  and

$$\{(\lambda x_1, \dots, \lambda x_{n+1}) : \lambda \in k_0\} \subseteq \{(\lambda x_1, \dots, \lambda x_{n+1}) : \lambda \in k\}$$

as a subset.  $\square$

**4.2. Projective Algebraic Sets****Problem 4.4.\***

*Let  $I$  be a homogeneous ideal in  $k[x_1, \dots, x_{n+1}]$ . Show that  $I$  is prime if and only if the following condition is satisfied: for any forms  $f, g \in k[x_1, \dots, x_{n+1}]$ , if  $fg \in I$ , then  $f \in I$  or  $g \in I$ .*

*Proof.*

- (1)  $(\implies)$  Trivial.
- (2)  $(\impliedby)$  Suppose that  $f, g \in k[x_1, \dots, x_{n+1}]$  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  $\text{rad}(I)$  is also homogeneous.*

*Proof.*

- (1) Given any  $f = \sum_{i=0}^r f_i \in \text{rad}(I)$ ,  $f_i$  a form of degree  $i$ . It suffices to show that each  $f_i \in \text{rad}(I)$ . 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,  $f_r \in \text{rad}(I)$ . Again note that  $f - f_r \in \text{rad}(I)$  and  $\deg(f - f_r) < r$ . Continue this process (or by induction), and we have  $f_{r-1}, \dots, f_0 \in \text{rad}(I)$ .

□

### 4.3. Affine and Projective Varieties

### 4.4. Multiprojective Space

## Chapter 5: Projective Plane Curves

### 5.1. Definitions

### 5.2. Linear Systems of Curves

### 5.3. Bézout's Theorem

### 5.4. Multiple Points

### 5.5. Max Noether's Fundamental Theorem

### 5.6. Applications of Noether's Theorem

## Chapter 6: Varieties, Morphisms, and Rational Maps

### 6.1. The Zariski Topology

### 6.2. Varieties

### 6.3. Morphisms of Varieties

### 6.4. Products and Graphs

### 6.5. Algebraic Function Fields and Dimension of Varieties

### 6.6. Rational Maps

## Chapter 7: Resolution of Singularities

### 7.1. Rational Maps of Curves

### 7.2. Blowing up a Point in $A^2$

### 7.3. Blowing up a Point in $P^2$

### 7.4. Quadratic Transformations

### 7.5. Nonsingular Models of Curves

## Chapter 8: Riemann-Roch Theorem

### 8.1. Divisors

### 8.2. The Vector Spaces $L(D)$

### 8.3. Riemann's Theorem

### 8.4. Derivations and Differentials

### 8.5. Canonical Divisors

### 8.6. Riemann-Roch Theorem