Solutions to Algebraic Curves

Meng-Gen Tsai
plover@gmail.com

March 9, 2021

Contents

Chapter 1: Affine Algebraic Sets

1.1. Algebraic Preliminaries

Problem 1.1.*

Let R be a domain.

(a) *If F, G are forms of degree r, s respectively in $R[X_1, \ldots, X_n]$, show that FG is a form of degree $r + s$.*

(b) *Show that any factor of a form in $R[X_1, \ldots, X_n]$ is also a form.*

Proof of (a).

(1) Write

$$F = \sum_{(i)} a_{(i)} X^{(i)},$$
$$G = \sum_{(j)} b_{(j)} X^{(j)},$$

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

(2) Hence,

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

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

□

Proof of (b).

(1) Given any form $F \in R[X_1, \ldots, X_n]$, and write $F = GH$. *It suffices to show that G (or H) is a form as well.*

(2) Write

$$G = G_0 + \cdots + G_r,$$
$$H = H_0 + \cdots + H_s$$

where $G_r \neq 0$ and $H_s \neq 0$. So

$$F = GH = G_0H_0 + \cdots + G_rH_s.$$

Since R is a domain, $R[X_1, \ldots, X_n]$ is a domain and thus $G_rH_s \neq 0$. The maximality of r and s implies that $\deg(F) = r + s$. Therefore, by the maximality of $r + s$, $F = G_rH_s$, or $G = G_r$, or G is a form.

□

Problem 1.5.*

Let k be any field. Show that there are an infinitely number of irreducible monic polynomials in $k[X]$. (Hint: Suppose $F_1, \ldots, F_n$ were all of them, and factor $F_1 \cdots F_n + 1$ into irreducible factors.)

Proof (Due to Euclid).

(1) If $F_1, F_2, \ldots, F_n$ were all irreducible monic polynomials, then we consider

$$G = F_1F_2 \cdots F_n + 1 \in k[X].$$

So there is an irreducible monic polynomial F dividing G since

$$\deg G = \deg F_1 + \deg F_2 + \cdots + \deg F_n \geq 1.$$

(2) F can not be any of F_i for all i; otherwise F would divide the difference $G - F_1F_2 \cdots F_n = 1$. That is, $F \neq F_i$ for all i, contrary to the assumption.

□

Problem 1.6.*

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

Proof (Due to Euclid).

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

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

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

□

1.2. Affine Space and Algebraic Sets

Problem 1.8.*

Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets, together with $\mathbb{A}^1(k)$ 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 $G \in I$,

   $$G = FQ + R$$

   for some $Q, R \in k[X]$ with $R = 0$ or $\deg R < \deg F$. Now as

   $$R = G - FQ \in I,$$

   $R = 0$ (otherwise contrary to the minimality of F), we have $G \in (F)$ for all $G \in I$.

(2) Let X be an algebraic subset of $\mathbb{A}^1(k)$, say $X = V(I)$ 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 $X = V(0) = \mathbb{A}^1(k)$.
   (b) If $F \neq 0$, then $F(X) = 0$ has finitely many roots in k, say $P_1, \dots, P_m \in k$. Hence,

   $$X = V(I) = V(F) = \{F(P) = 0 : P \in k\} = \{P_1, \dots, P_m\}$$

   is a finite subsets of X.

   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 $X = V(I)$ of $\mathbb{A}^1(k)$, we can write $I = (F_1, \cdots, F_m)$. Note that

$$V(I) = V(F_1) \cap \cdots \cap V(F_m).$$

Now apply the same argument to get the same conclusion.

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