Chapter 1: Affine Algebraic Sets

Author: Meng-Gen Tsai
Email: plover@gmail.com

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

$$F = GH = G_0 H_0 + \cdots + G_r H_s.$$

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

□

Problem 1.5*. *Let k be any field. Show that there are an infinitely number of irreducible monic polynomials in $k[X]$. (Hint: Suppose $F_1, \ldots, F_n$ were all of them, and factor $F_1 \cdots F_n + 1$ into irreducible factors.)*

Proof (Due to Euclid).

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

$$G = F_1 F_2 \cdots F_n + 1 \in k[X]$$

and there were an irreducible 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 $c_i F_i$ for $1 \leq i \leq n$ and $c_i \in k - \{0\}$; otherwise F would divide the difference $G - F_1 F_2 \cdots F_n = 1$. That is, $F \neq c_i F_i$ for $1 \leq i \leq n$ and $c_i \in k - \{0\}$, which is absurd.

□