Chapter 1, Geometry, Algebra, and Algorithms

§1. Polynomials and Affine Space.

Proposition 1.1.5. Let k be an infinite field, and $f \in k[x_1, \ldots, x_n]$. Then $f = 0$ in $k[x_1, \ldots, x_n]$ if and only if the function $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$ of $k^n \to k$ is the zero function.

Proof.($\Rightarrow$): The zero polynomial is the polynomial all of whose coefficients are zero; so if f is the zero polynomial the associated function mapping $k^n \to k$ is certainly the zero function.

($\Leftarrow$): Let (1.1.5.n) be the statement listed above as Proposition 1.1.5 with n variables. (1.1.5.0) is true and says that the constant zero is the zero polynomial. For some $n > 0$ suppose (1.1.5.$n-1$) is true. Let $f \in k[x_1, \ldots, x_n] = k[x_1, \ldots, x_{n-1}][x_n]$ induce the zero function $: k^n \to k$. For the inductive step we must show f is the zero polynomial. If f is not the zero polynomial of $k[x_1, \ldots, x_n]$, one of the "coefficients", say $c(x_1, \ldots, x_{n-1})$, of f regarded as an element of $k[x_1, \ldots, x_{n-1}][x_n]$ is not the zero polynomial in $k[x_1, \ldots, x_{n-1}]$. (1.1.5.$n-1$) then insures that there exist $\zeta_1, \ldots, \zeta_{n-1} \in k$ such that $c(\zeta_1, \ldots, \zeta_{n-1}) \neq 0$. In this case not all the coefficients of the polynomial $h(x_n) = f(\zeta_1, \ldots, \zeta_{n-1}, x_n) \in k[x_n]$ vanish; so $h[x_n]$ is not the zero polynomial (in $k[x_n]$). h has at most a finite number of roots in k; so (since k is infinite) there is a $\zeta_n \in k$ with $0 \neq h(\zeta_n) = f(\zeta_1, \ldots, \zeta_n)$. Thus if f is not the zero polynomial, then $(\xi_1, \ldots, \xi_n) \mapsto f(\xi_1, \ldots, \xi_n)$ is not the zero function; so zero function implies zero polynomial. Summing up, the only f in $k[x_1, \ldots, x_n]$ which vanishes on k^n is the zero polynomial. This proves (1.1.5.n)and by induction, Proposition 1.1.5 is true. ∎

Note. A variant on this argument runs as follows: Assume f is the zero function on k^n. Let $g(x_1, \ldots, x_{n-1})$ be the product of the coefficients of $f \in k[x_1, \ldots, x_{n-1}][x_n]$. If g is not the zero polynomial in $k[x_1, \ldots, x_{n-1}]$, (1.1.5.$n-1$) states that we can choose $\zeta_1, \ldots, \zeta_{n-1}$ so that $g(\zeta_1, \ldots, \zeta_{n-1}) \neq 0$. With this choice of $\zeta_1, \ldots, \zeta_{n-1}$, none of the coefficients vanishes when evaluated at $(\zeta_1, \ldots, \zeta_{n-1}) \in k^{n-1}$, and (1.1.5.1) used on $f(\zeta_1, \ldots, \zeta_{n-1}, x_n) \in k[x_n]$ then enables us to choose ζ_n so that $f(\zeta_1, \ldots, \zeta_n) \neq 0$. This, however, contradicts the assumption that f is the zero function on k^n. It must be that g is the zero polynomial in $k[x_1, \ldots, x_{n-1}]$ and in consequence f is the zero polynomial in $k[x_1, \ldots, x_n]$.

---

§1.1.2.

(a) Consider the polynomial $g(x,y) = x^2y + y^2x \in \mathbf{Z}_2[x,y]$. Show that $g(x,y) = 0$ for every $(x,y) \in \mathbf{Z}_2^2$, and explain why this does not contradict Proposition 1.1.5.

(b) Find a nonzero polynomial in $\mathbf{Z}_2[x,y,z]$ which vanishes at every point of $\mathbf{Z}_2^3$. Try to find one involving three variables.

(c) Find a nonzero polynomial in $\mathbf{Z}_2[x_1, \ldots, x_n]$ which vanishes at every point of $\mathbf{Z}_2^n$. Can you find one in which all of the $x_1, \ldots, x_n$ appear?

Solution. $x_1x_2 \cdots x_n(x_1 + x_2 + \cdots + x_n + n \mod 2)$ will do the trick.

---

§1.1.6].

Inside of $\mathbf{C}^n$ we have the subset $\mathbf{Z}^n$ which consists of those points all of whose coordinates are integers.

- -

a. Prove that if $f \in \mathbf{C}[x_1, \ldots, x_n]$ vanishes at every point of $\mathbf{Z}^n$, then f is the zero polynomial.

Solution. The proof is by induction. If $n = 1$, and the polynomial $f(x_1)$ vanishes on the integers $\mathbf{Z}$, then f is the zero polynomial because any nonzero polynomial in one variable can have at most a finite number of roots. Suppose $f \in \mathbf{C}[x_1, \ldots, x_n] = \mathbf{C}[x_1, \ldots, x_{n-1}][x_n]$ and vanishes on $\mathbf{Z}^n$. Suppose f is not the zero polynomial and $c(x_1, \ldots, x_{n-1})$ is one of the coefficients of f regarded as an element of $\mathbf{C}[x_1, \ldots, x_{n-1}][x_n]$ which is not identically zero. Then the inductive hypothesis guarantees that there are integers $n_1, \ldots, n_{n-1}$ such that $c(n_1, \ldots, n_{n-1}) \neq 0$. It follows that the polynomial $g(x_n) = f(n_1, \ldots, n_{n-1}, x_n) \in \mathbf{C}[x_n]$ is not the zero polynomial. By the "basis step" where $n = 1$ it follows that g cannot vanish on the integers $\mathbf{Z}$. There is thus an integer n_n such that $0 \neq g(n_n) = f(n_1, \ldots, n_{n-1}, n_n)$; so f doesn't vanish on $\mathbf{Z}^n$. ∎

- -

b. Let $f \in \mathbf{C}[x_1, \ldots, x_n]$, and let M be the largest power of any variable that appears in f. Let $\mathbf{Z}^n_{M+1}$ be the set of points of $\mathbf{Z}^n$, all accordinates of which lie between 1 and $M+1$. Prove that if f vanishes at all points of $\mathbf{Z}^n_{M+1}$, then f is the zero polynomial.

Solution. By induction: (Case $n = 1$.) If $f \in \mathbf{C}[x_1]$, $\deg f \leq M$, and f vanishes on the $M+1$ points $1, 2, \ldots, M+1$, then f is identically zero, because a nonzero polynomial of degree $\leq M$ can have at most M roots and this f has $M+1$ roots; so it must be the zero polynomial.

(Inductive step.) Write

$$f(x_1, \ldots, x_n) = a_M(x_1, \ldots, x_{n-1})x_n^M + a_{M-1}(x_1, \ldots, x_{n-1})x_n^{M-1} + \cdots + a_0(x_1, \ldots, x_{n-1}). \tag{1.1.6.b.1}$$

Now for every choice of integers $1 \leq b_i \leq M+1$, $1 \leq i \leq n-1$, the polynomial $x_n \mapsto f(b_1, \ldots, b_{n-1}, x_n)$ has $M+1$ roots and is consequently the zero polynomial according to the case where $n = 1$ above. This means that each of the polynomials $a_m, \ldots, a_0$ vanish on $\mathbf{Z}^{n-1}_{M+1}$ and each is then the zero polynomial by the inductive step. It follows from (1.1.6.b.1) that f is the zero polynomial.