Appendix B

Polynomials and Polynomial Functions

Consider an arbitrary (commutative) field K. The functions from K^n to K form a K-algebra $A := \mathrm{Map}(K^n, K)$. Let $K[T]$ be the polynomial algebra in the n-tuple $T = (T_1, \ldots, T_n)$ of indeterminates. Then

$$\begin{array}{rcl} \alpha\colon K[T] & \longrightarrow & A, \\ \varphi & \mapsto & \alpha(\varphi) \quad \text{with } \alpha(\varphi)(x_1, \ldots, x_n) := \varphi(x_1, \ldots, x_n) \end{array}$$

is a K-algebra homomorphism, called the "substitution homomorphism". Its image, $\alpha(K[T]) \subseteq A$, is the algebra of polynomial functions on K^n. We distinguish two fundamentally different cases—K is infinite, or K is finite.

B.1 Polynomial Functions over Infinite Fields

Let K be infinite. Then α is

- injective, i. e., different polynomials define different functions—the proof is the uniqueness proof of interpolation formulas, and is given below,
- not surjective, because $K[T]$ has the same cardinality as K, but A is strictly larger—the proof is elementary set theory.

The proof of injectivity relies on the following lemma:

Lemma 4 *Let K be a field with at least $d + 1$ elements, and let $\varphi \in K[T]$ be a polynomial of degree $\leq d$ with $\varphi(x) = 0$ for all $x \in K^n$. Then $\varphi = 0$.*

Proof. We prove this by induction on the dimension n. In the case $n = 1$ the polynomial φ has more than d roots, whence $\varphi = 0$ by elementary algebra.

Now let $n \geq 2$. Split the indeterminates into $X = (T_1, \ldots, T_{n-1})$ and $Y = T_n$. Then

$$\varphi = \sum_{i=0}^{d} \psi_i(X) \cdot Y^i \quad \text{where } \deg \psi_i \leq d - i \leq d.$$

Fix an arbitrary $x \in K^{n-1}$. Then $\varphi(x, y) = \sum_i \psi_i(x) \cdot y^i = 0$ for all $y \in K$. The assertion in the case $n = 1$ gives $\psi_0(x) = \ldots = \psi_d(x) = 0$. Since this holds for all x, induction gives $\psi_0 = \ldots = \psi_d = 0$. Hence $\varphi = 0$. $\diamond$

From this lemma we immediately get the following theorem:

Theorem 7 *Let K be an infinite field. Then the substitution homomorphism $\alpha \colon K[T] \longrightarrow A$ is injective.*

Now let $x_1, \ldots, x_d \in K^n$ be d distinct points, $x_i = (x_{i1}, \ldots, x_{in})$. We want to construct a polynomial that takes given (not necessarily distinct) values $a_1, \ldots, a_d$ at these points. To this end consider the polynomials

$$\psi_k := \prod_{i \in \{1,\ldots,d\} \setminus \{k\}} \prod_{j \in \{1,\ldots,n \,|\, x_{ij} \neq x_{kj}\}} (T_j - x_{ij}).$$

For $i \neq k$ at least one coordinate $x_{ij} \neq x_{kj}$, therefore $\psi_k(x_i) = 0$. On the other hand $\psi_k(x_k) \neq 0$. Hence for $\varphi_k := \psi_k / \psi_k(x_k)$ we conclude:

Lemma 5 *For each $k = 1, \ldots d$ there is a polynomial $\varphi_k \in K[T]$ with all partial degrees $\leq d - 1$ and*

$$\varphi_k(x_i) = \begin{cases} 1 & \text{for } i = k, \\ 0 & \text{for } i \text{ otherwise.} \end{cases}$$

Taking the linear combination $\varphi = \sum a_k \varphi_k$ we get:

Theorem 8 *Let $x_1, \ldots, x_d \in K^n$ be d distinct points, and $a_1, \ldots, a_d \in K$. Then there is a polynomial $\varphi \in K[T_1, \ldots, T_n]$ of partial degree $\leq d - 1$ in each T_i such that $\varphi(x_k) = a_k$ for $k = 1, \ldots d$.*

Note that the proof was constructive but didn't care about the most efficient algorithm.

B.2 Polynomial Functions over Finite Fields

Let K be finite with $\#K = q$ elements. Then α is

- not injective, because $K[T]$ is infinite, but $\#A = q^{q^n}$.

- surjective, because $F \in A$ is completely determined by the q^n pairs $(x, F(x))$, $x \in K^n$, that is by the graph of F; interpolation gives a polynomial $\varphi \in K[T]$ with $\varphi(x) = F(x)$ for all $x \in K^n$, i. e., $\alpha(\varphi) = F$. A proof follows directly from Theorem 8, however in the following we give an independent proof.

The polynomial

$$\varphi = \prod_{i=1}^{n} \left(-T_i^{q-1} + 1\right) \in K[T]$$

has partial degree $q - 1$ in each T_i.

Lemma 6 *The function $\alpha(\varphi)$ is the indicator function*

$$\varphi(x) = \begin{cases} 1 & \text{for } x = 0, \\ 0 & \text{for } x \in K^n \text{ otherwise.} \end{cases}$$

Proof. This is immediate from $a^{q-1} = 1$ for $a \in K^\times$. $\diamond$

Corollary 1 *For each $a \in K$ there is a polynomial $\varphi_a \in K[T]$ with all partial degrees $q - 1$ and*

$$\varphi_a(x) = \begin{cases} 1 & \text{for } x = a, \\ 0 & \text{for } x \in K^n \text{ otherwise.} \end{cases}$$

Proof. Take $\varphi_a = \varphi(T_1 - a_1, \ldots, T_n - a_n)$. $\diamond$

Now let $F\colon K^n \longrightarrow K$ be given. Then the polynomial

$$\varphi = \sum_{a \in K^n} F(a)\varphi_a \in K[T]$$

has all partial degrees $\leq q - 1$, and $\varphi(x) = F(x)$ for all $x \in K^n$. This proves the following theorem:

Theorem 9 *Let K be a finite field with q elements, and $n \in \mathbb{N}$. Then each function $F\colon K^n \longrightarrow K$ is given by a polynomial $\varphi \in K[T_1, \ldots, T_n]$ of partial degree $\leq q - 1$ in each T_i.*

Corollary 2 *Each function $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is given by a polynomial $\varphi \in \mathbb{F}_2[T_1, \ldots, T_n]$ that is linear in each T_i.*

Corollary 3 *The kernel of the substitution homomorphism α is the ideal $\mathfrak{a} = (T_1^q - T_1, \ldots, T_n^q - T_n) \trianglelefteq K[T]$.*

Proof. Clearly $\mathfrak{a} \subseteq \ker\alpha$. Because $\dim K[T]/\mathfrak{a} = q^n = \dim A$, and α is surjective, we have $\mathfrak{a} = \ker\alpha$. $\diamond$

Corollary 4 *Let $m, n \in \mathbb{N}$. Then each map $F : K^n \longrightarrow K^m$ is given by an m-tuple $(\varphi_1, \ldots, \varphi_m)$ of polynomials $\varphi_i \in K[T_1, \ldots, T_n]$ of partial degree $\leq q-1$ in each T_i.*

Corollary 5 *Each map $F : V \longrightarrow W$ between finite dimensional K-vectorspaces V and W is polynomial with partial degrees each $\leq q-1$.*