2 Polynome über endlichen Körpern

Satz 1 *Sei K ein endlicher Körper mit q Elementen und $n \in \mathbb{N}$. Dann wird jede Funktion $F : K^n \longrightarrow K$ durch ein Polynom $\varphi \in K[T_1, \ldots, T_n]$ vom partiellen Grad $\leq q-1$ in jedem T_i beschrieben.*

Beweis. (Skizze) folgt unten. $\diamond$

Korollar 1 *Seien $m, n \in \mathbb{N}$. Dann wird jede Abbildung $F : K^n \longrightarrow K^m$ durch ein m-Tupel $(\varphi_1, \ldots, \varphi_m)$ von Polynomen $\varphi_i \in K[T_1, \ldots, T_n]$ vom partiellen Grad $\leq q-1$ in jedem T_i beschrieben.*

Korollar 2 *Jede Abbildung $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ wird durch ein m-Tupel von Polynomen $(\varphi_1, \ldots, \varphi_m)$ von Polynomen $\varphi_i \in \mathbb{F}_2[T_1, \ldots, T_n]$ beschrieben, deren sämtliche partiellen Grade ≤ 1 sind.*

Damit erhalten wir auch die **algebraische Normalform** einer Boolеschen Funktion $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$: Für eine Teilmenge $I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$ sei x^I das Monom

$$x^I = x_{i_1} \cdots x_{i_r}.$$

Dann lässt sich F eindeutig schreiben als

$$F(x_1, \ldots, x_n) = \prod_I a_I x^I \quad \text{mit } a_I = 0 \text{ oder } 1.$$

Insbesondere bilden die 2^n Monome x^I eine Basis des $\mathbb{F}_2$-Vektorraums $\mathrm{Abb}(\mathbb{F}_2^n, \mathbb{F}_2)$, und es gibt – wie auch anderweitig klar ist – 2^{2^n} solche Funktionen.

Beweisskizze für den Satz – ein etwas elementarerer, vollständiger Beweis im Fall $K = \mathbb{F}_2$ wird im Abschnitt „Die algebraische Normalform Boolescher Funktionen“ gegeben.

Sei zunächst K ein beliebiger (kommutativer) Körper. Dann ist $A := \mathrm{Abb}(K^n, K)$ eine K-Algebra. Sei $K[T]$ der Polynomring in dem n-Tupel $T = (T_1, \ldots, T_n)$ von Unbestimmten. Dann ist

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

ein K-Algebra-Homorphismus, der „Einsetzungs-Homomorphismus“. Sein Bild, $\mathrm{Bild}\,\alpha \subseteq A$, ist die Algebra der Polynomfunktionen. Es gibt zwei grundsätzlich unterschiedliche Fälle:

Fall 1: K ist unendlich. Dann ist α

- injektiv, d. h., unterschiedliche Polynome definieren unterschiedliche Funktionen – der Beweis ist der Eindeutigkeitsbeweis von Interpolationsformeln –,
- nicht surjektiv, denn $K[T]$ hat die gleiche Mächtigkeit wie K, dagegen hat A eine echt größere – der Beweis ist elementare Mengenlehre –.

Fall 2: K ist endlich. Dann ist α

- nicht injektiv, denn $K[T]$ ist unendlich, aber $\#A = q^{q^n}$,
- surjektiv, denn $F \in A$ wird vollständig beschrieben durch die q^n Paare $(x, F(x))$, $x \in K^n$, also durch den Graphen; mit Interpolation findet man ein Polynom $\varphi \in K[T]$ mit $\varphi(x) = F(x)$ für alle $x \in K^n$, d. h., $\alpha(\varphi) = F$.

Damit ist der erste Teil des Satzes bewiesen: *Jede Funktion $K^n \to K$ ist Polynomfunktion.*

Für den weiteren Beweisgang bestimmt man am besten $\operatorname{Kern}\alpha$. Sei $\mathfrak{a}$ das von den Polynomen $T_i^q - T_i$ erzeugte Ideal:

$$\mathfrak{a} = (T_1^q - T_1, \ldots, T_n^q - T_n) \trianglelefteq K[T].$$

Da die multiplikative Gruppe $K^\times$ die Ordnung $q-1$ hat, ist $a^q = a$ für alle $a \in K$. Also ist $\mathfrak{a} \subseteq \operatorname{Kern}\alpha$.

Nun hat der Restklassenring $K[T]/\mathfrak{a}$ offensichtlich ein vollständiges Repräsentantensystem aus den Restklassen derjenigen Polynome, die in allen T_i den Grad $\leq q-1$ haben, und die bilden einen K-Vektorraum der Dimension q^n, wie man durch Betrachtung der naheliegenden Basis sieht. Also ist

$$q^{q^n} = \#A = \#(K[T]/\operatorname{Kern}\alpha) \leq \#(K[T]/\mathfrak{a}) \leq q^{q^n}.$$

Da folglich überall in dieser Kette die Gleichheit gilt, ist $\operatorname{Kern}\alpha = \mathfrak{a}$, und $A \cong K[T]/\mathfrak{a}$ wird daher von den Polynomen mit allen partiellen Graden $\leq q-1$ ausgeschöpft. $\diamond$