A Endliche Körper

A.1 Die Spur

In diesem Abschnitt werden endliche Erweiterungskörper K des endlichen Körpers $\mathbb{F}_q$ mit q Elementen betrachtet.

Hilfssatz 1 (i) *Die Abbildung*

$$\varphi\colon K \longrightarrow K, \quad \varphi(x) = x^q,$$

ist ein Automorphismus von K, insbesondere $\mathbb{F}_q$-linear. (Man nennt sie den Frobenius-*Automorphismus von K.)*

(ii) *Ein $x \in K$ ist genau dann Fixpunkt von φ, wenn $x \in \mathbb{F}_q$.*

Beweis. (i) Die binomische Formel liefert $(x+y)^q = x^q + y^q$, da q eine Potenz der Charakteristik des Körpers K ist. Die entsprechende multiplikative Relation $(xy)^q = x^q y^q$ ist trivial. Daher ist φ ein Ringhomomorphismus. Da K Körper ist, ist φ injektiv, da K endlich ist, auch surjektiv.

(ii) Das Polynom $T^q - T$ hat die q Elemente von $\mathbb{F}_q$ als Nullstellen. Das müssen daher alle sein. $\diamond$

Sei n die Dimension von K als $\mathbb{F}_q$-Vektorraum. Die **Spur** ist auf K definiert als

$$\mathrm{Tr}\colon K \longrightarrow K, \quad \mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}} = \sum_{i=0}^{n-1} x^{q^i},$$

also

$$\mathrm{Tr} = \varphi^0 + \varphi + \varphi^2 + \cdots + \varphi^{n-1} = \sum_{i=0}^{n-1} \varphi^i,$$

Anmerkung. Im allgemeinen ist bei einer separablen Körpererweiterung die Spur $\mathrm{Tr}(x)$ die Summe über alle zu x konjugierten Elemente, also aller Bilder unter relativen Automorphismen. Der Zusammenhang entsteht dadurch, dass die Automorphismengruppe von K über $\mathbb{F}_q$ vom Frobenius-Automorphismus φ erzeugt wird und die Ordnung n hat.

Hilfssatz 2 *Für die Spur gilt:*

(i) $\mathrm{Tr}(x) \in \mathbb{F}_q$ *für alle* $x \in K$.

(ii) $\mathrm{Tr}\colon K \longrightarrow \mathbb{F}_q$ *ist $\mathbb{F}_q$-linear.*

(iii) $\mathrm{Tr}(x) = nx$ *für alle* $x \in \mathbb{F}_q$.

Beweis. (i) folgt, weil offensichtlich $\mathrm{Tr}(x)^q = \mathrm{Tr}(x)$. (ii) und (ii) sind trivial. $\diamond$

Satz 1 (ARTINs Lemma von der Unabhängigkeit der Charaktere) *Sei G eine Halbgruppe, K ein Körper und X eine Menge von Homomorphismen $G \longrightarrow K^\times$ („Charaktere"). Dann ist X im K-Vektorraum K^G aller K-wertigen Abbildungen von G linear unabhängig.*

Beweis. Sei

$$a_1\chi_1 + \cdots + a_n\chi_n = 0$$

eine minimale lineare Relation mit verschiedenen $\chi_i \in X$. Dann sind alle $a_i \neq 0$ und, da $\chi_1 \neq 0$, jedenfalls $n \geq 2$. Sei $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$ gewählt. Dann gilt für alle $h \in G$:

$$[a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n](h) = a_1\chi_1(gh) + \cdots + a_n\chi_n(gh) = 0.$$

Also haben wir, zusammen mit der ursprünglichen, die beiden linearen Relationen

$$\begin{aligned} a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + \cdots + a_n\chi_n(g)\chi_n &= 0, \\ a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + \cdots + a_n\chi_1(g)\chi_n &= 0, \end{aligned}$$

deren Differenz eine nichttriviale kürzere lineare Relation ergibt; Widerspruch. ◇

Korollar 1 *Ist $K \supseteq \mathbb{F}_q$ eine endliche Körpererweiterung, so gibt es ein $x \in K$ mit $\mathrm{Tr}(x) \neq 0$.*

Beweis. Ist φ der FROBENIUS-Automorphismus, so ist $\mathrm{Tr} = \varphi^0 + \varphi^1 + \cdots + \varphi^{n-1}$, wobei n die Dimension von K über $\mathbb{F}_q$ ist, und die φ_i sind verschiedene Gruppenhomomorphismen $K^\times \longrightarrow K^\times$. Also sind sie linear unabhängig; insbesondere kann ihre Summe nicht 0 sein. ◇

Die **Spurform** von K ist die bilineare Abbildung

$$\mathrm{Tr}_2 \colon K \times K \longrightarrow \mathbb{F}_q, \quad \mathrm{Tr}_2(x, y) := \mathrm{Tr}(xy).$$

Korollar 2 *Die Spurform ist eine nichtausgeartete Bilinearform.*

Beweis. Sei $x \in K$ gewählt mit $\mathrm{Tr}(x) \neq 0$. Dann ist für $y \in K$, $y \neq 0$,

$$\mathrm{Tr}_2(y, \frac{x}{y}) = \mathrm{Tr}(y \cdot \frac{x}{y}) = \mathrm{Tr}(x) \neq 0,$$

also y nicht im Kern der Bilinearform. ◇

Da die Spurform somit eine Bijektion zwischen K und seinem dualen $\mathbb{F}_q$-Vektorraum herstellt, folgt weiter:

Korollar 3 *Für jede $\mathbb{F}_q$-Linearform $\alpha\colon K \longrightarrow \mathbb{F}_q$ gibt es genau ein $a \in K$ mit*

$$\alpha(x) = \mathrm{Tr}(ax) \quad \textit{für alle } x \in K.$$

Für $x_1, \ldots, x_n \in K$ betrachten wir die Matrix

$$W(x) := \left(x_j^{q^{i-1}}\right)_{1 \le i,j \le n} \in M_{n,n}(K).$$

Es ist

$$W(x)^t\, W(x) = G(x) := (\mathrm{Tr}(x_i x_j))$$

die GRAMsche Matrix bezüglich der Spurform, denn

$$\mathrm{Tr}(x_i x_j) = \sum_{k=1}^{n} x_i^{q^{k-1}} x_j^{q^{k-1}}.$$

Bekanntlich sind $x_1, \ldots, x_n$ genau dann über $\mathbb{F}_q$ linear unabhängig, wenn ihre GRAMsche Matrix invertierbar ist. Damit ist gezeigt:

Hilfssatz 3 *Die Elemente $x_1, \ldots, x_n \in K$ bilden genau dann eine Basis von K über $\mathbb{F}_q$, wenn $n = \mathrm{Dim}_{\mathbb{F}_q} K$ und die Matrix $W(x)$ invertierbar ist.*

A.2 q-Polynome

Eine besondere Rolle spielen bei endlichen Körpern die Polynome, die lineare Funktionen definieren: Die Abbildung

$$\Psi\colon \mathbb{F}_q[T] \longrightarrow \mathbb{F}_q[T], \quad f = \sum_{i=0}^{n} a_i T^i \mapsto F = \sum_{i=0}^{n} a_i T^{q^i}$$

ist $\mathbb{F}_q$-linear; ihre Bilder heißen q-Polynome. Insbesondere sind sie durch T teilbar.

Hilfssatz 4 *Für alle Polynome $f, g \in \mathbb{F}_q[T]$ gilt:*
(i) $\Psi(fg) = \Psi(f)\,(\Psi(g))$ *(Einsetzen eines Polynoms in ein Polynom),*
(ii) $g|f \iff \Psi(g)|\Psi(f)$.
(iii) $\mathrm{ggT}(\Psi(f), \Psi(g)) = \Psi(\mathrm{ggT}(f, g))$.

Beweis. (i) Ist $g = \sum_{j=0}^{n} b_j t^j$, so

$$\begin{aligned} fg &= \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j T^{i+j}, \\ \Psi(fg) &= \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j \left(T^{q^j}\right)^{q^i} \\ &= \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n} b_j T^{q^j}\right)^{q^i} = \Psi(f)\,(\Psi(g))\,. \end{aligned}$$

(ii) Sei $f = hg$. Mit dem Polynom $\bar{h} := \frac{1}{T}\Psi(h)$ gilt

$$\Psi(f) = \Psi(hg) = \Psi(h)\,(\Psi(g)) = \Psi(g)\bar{h}\,(\Psi(g))\,.$$

Sei umgekehrt $\Psi(g)|\Psi(f)$. Sei $f = hg + r$ die Division mit Rest r, wobei $\operatorname{Grad} r < \operatorname{Grad} g$ ist. Dann ist auch

$$\Psi(f) = \Psi(hg) + \Psi(r) = \Psi(g)\bar{h}\,(\Psi(g)) + \Psi(r)$$

eine Division mit Rest, denn $\operatorname{Grad}\Psi(r) < \operatorname{Grad}\Psi(g)$. Da diese eindeutig ist und $\Psi(g)|\Psi(f)$, muss $\Psi(r) = 0$, also auch $r = 0$ und $g|f$ sein.

(iii) Sei $h := \mathrm{ggT}(f, g)$. Dann gilt:

$$L = \psi(l)|\Psi(h) \Longleftrightarrow l|h \Longleftrightarrow l|f, g \Longleftrightarrow L|\Psi(f), \Psi(g).$$

Also ist $\Psi(h) = \mathrm{ggT}(\Psi(f), \Psi(g)$. $\diamond$

Da jedes q-Polynom F eine $\mathbb{F}_q$-lineare Abbildung $K \longrightarrow K$ definiert, ist seine Nullstellenmenge V_F ein $\mathbb{F}_q$-Untervektorraum von K mit $\varphi(V_F) = V_F$. Umgekehrt gilt:

Satz 2 *Sei $V \subseteq K$ ein h-dimensionaler $\mathbb{F}_q$-Untervektorraum mit $\varphi(V) = V$. Dann ist*

$$F = F_V := \prod_{v \in V} (T - v) \in K[T]$$

ein q-Polynom, $F = \Psi(f)$ mit $\operatorname{Grad} f = h$; insbesondere ist $F \in \mathbb{F}_q[T]$.

Beweis. Die Koeffizienten von F sind die elementarsymmetrischen Funktionen der $v \in V$, also unter dem FROBENIUS-Automorphismus invariant, also in $\mathbb{F}_q$. Sei $v_1, \ldots v_h$ eine Basis von V. Dann ist die Matrix $W(v) := \left(v_j^{q^{i-1}}\right) \in M_{h,h}(K)$ invertierbar. Also gibt es eine Lösung $a_0, \ldots, a_{h-1} \in K$ des Gleichungssystems

$$v_i^{q^h} + \sum_{j=0}^{h-1} a_j v_i^{q^j} = 0 \quad \text{für } i = 1, \ldots, n.$$

Damit sind $v_1, \ldots, v_h$ Nullstellen des Polynoms

$$G = T^{q^h} + \sum_{j=0}^{h-1} a_j T^{q^j}.$$

Wegen der Linearität sind alle $v \in V$ ebenfalls Nullstellen, und das sind q^h Stück, also sämtliche Nullstellen von G. Daher ist $G = F \in \mathbb{F}_q[T]$. $\diamond$

Korollar 1 *Für jedes $x \in K$ gibt es ein q-Polynom F mit $F(x) = 0$.*

Beweis. Die Potenzen x^{q^i} spannen einen Unterraum $V \subseteq K$ mit $\varphi(V) = V$ auf. Daher ist F_V ein q-Polynom mit x als Nullstelle. $\diamond$

Aus der Konstruktion ist klar, dass F den Leitkoeffizienten 1 hat und jedes andere q-Polynom G mit $G(x) = 0$ teilt. Es heißt daher auch das **q-Minimalpolynom** von x. Umgekehrt heißt x **q-primitive** Nullstelle eines q-Polynoms F, wenn F bis auf einen konstanten Faktor das q-Minimalpolynom von x ist.

Satz 3 *Sei $F = \Psi(f) \in \mathbb{F}_q[T]$ ein q-Polynom mit $f(0) \neq 0$. Dann hat F im algebraischen Abschluss von $\mathbb{F}_q$ eine q-primitive Nullstelle.*

Beweis. Sei $f = f_1^{e-1} \cdots f_r^{e_r}$ die Primzerlegung in $\mathbb{F}_q[T]$; die f_i seien verschieden und vom Grad m_i. Dann ist f vom Grad $m = e_1 m_1 + \cdots + e_r m_r$. Ist $f = a_0 + \cdots a_m T^m$, so $F = a_0 T + \cdots + a_m T^{q^m}$ und die Ableitung $F' = a_0 \neq 0$ konstant. Also sind alle q^m Nullstellen von F einfach.

Nun ist eine Nullstelle x von F genau dann q-primitiv, wenn x nicht Nullstelle eines q-Polynoms $G|F$ von kleinerem Grad ist. Ist $G = \Psi(g)$, so $g|f$, also $g|g_i := \frac{f}{f_i}$ für ein i. Die Nullstellen der $G_i := \Psi(g_i)$ sind also nicht q-primitiv für F. Also ist die Menge der q-primitiven Nullstellen gleich der Nullstellenmenge V_F weniger die Vereinigung der Nullstellenmengen V_{G_i}. Deren Anzahlen sind q^m bzw. q^{m-m_i}. Um das folgende Lemma 5 anwenden zu können, brauchen wir noch die Elementeanzahlen der Durchschnitte $\bigcap_{i \in I} V_{G_i}$ für alle Teilmengen $I \subseteq \{1, \ldots, r\}$. Eine solche gemeinsame Nullstellenmenge ist genau die Nullstellenmenge des

$$\mathrm{ggT}\{G_i \mid i \in I\} = \Psi(\mathrm{ggT}\{g_i \mid i \in I\}).$$

Dieses q-Polynom hat nur einfache Nullstellen und ist vom Grad

$$q^{m - \sum_{i \in I} m_i}.$$

Das ist also auch seine Nullstellenzahl. Also ist die Zahl der q-primitiven Nullstellen von F gleich

$$\begin{aligned} q^m - \sum_{i=1}^{m} q^{m-m_i} + \sum_{1 \leq i < j \leq r} q^{m-m_i-m_j} - \cdots &= q^m \cdot (1 - \frac{1}{q^{m_1}}) \cdots (1 - \frac{1}{q^{m_r}}) \\ &> 0; \end{aligned}$$

insbesondere gibt es q-primitive Nullstellen. $\diamond$

Hilfssatz 5 (DE MOIVRES Ein- und Ausschlussprinzip) *Sei M eine endliche Menge und $M_1, \ldots, M_n \subseteq M$ Teilmengen. Für $I \subseteq \{1, \ldots, n\}$ sei $M_I := \bigcap_{i \in I} M_i$. Dann ist*

$$\# \left(M - \bigcup_{i=1}^{n} M_i \right) = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{\#I} \# M_I.$$

Beweis. Induktion über n. Der Fall $n = 1$ ist trivial. Sei also jetzt $n \geq 2$. Sei $M' := M - M_1$ und $M_i' := M_i - M_1 \cap M_i$. Weiter sei für $J \subseteq \{2, \ldots, n\}$

$$M_J' := \bigcap_{j \in J} M_j' = \bigcap_{j \in J} M_j - M_1 \cap \bigcap_{j \in J} M_j = M_J - M_{J \cup \{1\}}.$$

Also ist

$$\begin{aligned} \# \left(M - \bigcup_{i=1}^{n} M_i \right) &= \# \left(M' - \bigcup_{i=2}^{n} M_i' \right) \\ &= \sum_{J \subseteq \{2,\ldots,n\}} (-1)^{\#J} \# M_J' \\ &= \sum_{J \subseteq \{2,\ldots,n\}} (-1)^{\#J} \left[\# M_J - M_{J \cup \{1\}} \right] \\ &= \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{\#I} \# M_I, \end{aligned}$$

wie behauptet. $\diamond$

Die Anzahl der q-primitiven Nullstellen aus dem Beweis von Satz 3 lässt sich noch anders beschreiben. Dazu sei für ein Polynom $f \in \mathbb{F}_q[T]$ definiert:

$$\begin{aligned} \Phi_q(f) &:= \{g \in \mathbb{F}_q[T] \mid \operatorname{Grad} g < \operatorname{Grad} f,\ \operatorname{ggT}(f, g) = 1\}, \\ \varphi_q(f) &:= \#\Phi_q(f). \end{aligned}$$

Das ist das „q-Analogon“ zur EULERschen φ-Funktion und hat folgende Eigenschaften:

Hilfssatz 6 (i) *Ist f konstant, so $\varphi_q(f) = 1$.*
(ii) *Sind f und g teilerfremd, so ist $\varphi_q(fg) = \varphi_q(f)\varphi_q(g)$.*
(iii) *Ist $f \in \mathbb{F}_q[T]$ irreduzibel vom Grad n, so ist $\varphi_q(f) = q^n - 1$.*
(iv) *... und $\varphi_q(f^e) = q^{en}(1 - \frac{1}{q^n})$.*
(v) *Ist $f = f_1^{e_1} \cdots f_r^{e_r}$ die Primzerlegung und $n_i = \operatorname{Grad} f_i$, so ist*

$$\varphi_q(f) = q^n \cdot (1 - \frac{1}{q^{n_1}}) \cdots (1 - \frac{1}{q^{n_r}}).$$

(vi) *Hat f in* (v) *nur einfache Nullstellen, so ist*

$$\varphi_q(f) = (q^{n_1} - 1) \cdots (q^{n_r} - 1).$$

Beweis. (i) Nur das Nullpolynom wird gezählt.

(ii) Die Abbildung

$$\Phi_q(fg) \longrightarrow \Phi_q(f) \times \Phi_q(g), \quad h \mapsto (h \bmod f, h \bmod g),$$

ist wohldefiniert, denn ist h zu fg teilerfremd, so auch zu f und g. Nach dem chinesischen Restsatz ist sie bijektiv.

(iii) Es sind alle Polynome von kleinerem Grad zu f teilerfremd außer dem Nullpolynom.

(iv) Die Polynome vom Grad $< en$, die nicht in $\Phi_q(f^e)$ liegen, sind genau die hf mit $\operatorname{Grad} h < en - n$. Also ist $\varphi_q(f^e) = q^{en} - q^{en-n}$.

(v) folgt aus (iv) und (ii), denn $n = e_1 n_1 + \cdots e_r n_r$, und (vi) ist ein Spezialfall davon. $\diamond$

Korollar 1 *Sei $f \in \mathbb{F}_q[T]$ mit $f(0) \neq 0$ und $F = \Psi(f)$ das zugehörige q-Polynom. Dann ist die Anzahl der q-primitiven Nullstellen von F genau gleich $\varphi_q(f)$.*

Beweis. Das war gerade die Formel am Ende des Beweises von Satz 3. $\diamond$

A.3 Normalbasen

Für einen Erweiterungskörper K von $\mathbb{F}_q$ der Dimension n heißt eine Basis der Gestalt x, x^q, …, $x^{q^{n-1}}$ **Normalbasis** von K über $\mathbb{F}_q$, und zwar die von x erzeugte.

Bezüglich einer Normalbasis ist das Potenzieren mit q, also der Frobenius-Automorphismus sehr einfach auszudrücken; dadurch wird das explizite Rechnen in K in manchen Situationen sehr effizient.

Satz 4 *Sei K ein Erweiterungskörper von $\mathbb{F}_q$. Dann gilt:*

(i) *$x \in K$ erzeugt genau dann eine Normalbasis, wenn x q-primitive Nullstelle von $T^{q^n} - T$ ist.*

(ii) (Hensel) *Es gibt eine Normalbasis von K über $\mathbb{F}_q$.*

(iii) *Es gibt genau*

$$\frac{\varphi_q(T^n - 1)}{n}$$

verschiedene Normalbasen von K über $\mathbb{F}_q$.

(iv) *Die bezüglich der Spurform zu einer Normalbasis duale Basis ist ebenfalls Normalbasis.*

Beweis. (i) K ist die Nullstellenmenge des q-Polynoms $F = T^{q^n} - T \in \mathbb{F}_q[T]$. Sei x eine q-primitive Nullstelle von F. Dann ist K der kleinste Unterraum

von K, der x, x^q, ..., $x^{q^{n-1}}$ enthält. Also wird K von diesen Elementen aufgespannt. Da es n Stück sind, müssen sie linear unabhängig sein.

Erzeugt umgekehrt x eine Normalbasis, so sind die n Elemente x, x^q, ..., $x^{q^{n-1}}$ linear unabhängig, und alle Linearkombinationen von ihnen sind Nullstellen von $T^{q^n} - T$. Also ist dieses das q-Minimalpolynom von x.

(ii) (ORE) Nach Satz 3 hat $T^{q^n} - T$ eine primitive Nullstelle. Alle q^n Nullstellen dieses Polynoms liegen aber in K. Die Behauptung folgt aus (i).

(iii) Jeweils n der q-primitiven Nullstellen erzeugen dieselbe Normalbasis, und die Anzahl der q-primitiven Nullstellen ist $\varphi_q(T^n - 1)$.

(iv) Sei $x, x^q, \ldots, x^{q^{n-1}}$ eine beliebige Normalbasis. Die duale Basis besteht aus den eindeutig bestimmten $y_0, \ldots, y_{n-1} \in K$ mit $\mathrm{Tr}(y_i \cdot x^{q^j}) = \delta_{ij}$. Da die Spur unter dem FROBENIUS-Automorphismus invariant ist, folgt

$$\mathrm{Tr}(y_i^q \cdot x^{q^{j+1}}) = \delta_{ij} = \mathrm{Tr}(y_{i+1} \cdot x^{q^{j+1}}),$$

wobei $y_n := y_0$ gesetzt ist. Daher ist $y_{i+1} = y_i^q$ für alle i, also $y_i = y_0^{q^i}$ für alle i. $\diamond$

Bemerkungen

1. Das Polynom $f = \varphi(T^n - 1)$ hat die Ableitung $f' = n \cdot T^{n-1}$. Alle Nulstellen x von f sind $\neq 0$. Also ist für eine solche

   $$f'(x) = n \cdot x^{n-1} = 0 \Leftrightarrow p|n,$$

   wobei p die Charakteristik von F_q ist. Ist also p kein Teiler von n, so

   $$\varphi_q(T^n - 1) = (q^{n_1} - 1) \cdots (q^{n_r} - 1),$$

   und es sind „nur“ noch die Grade n_i der Primteiler dieses Polynoms zu bestimmen.

2. Ist $q = 2$ und n ungerade, so ist

   $$\varphi_2(T^n - 1) = (2^{n_1} - 1) \cdots (2^{n_r} - 1),$$

   ungerade. Es kann also nicht jede Normalbasis von ihrer dualen Basis verschieden sein – sonst müsste die Gesamtzahl gerade sein. Damit ist gezeigt:

Satz 5 (MACWILLIAMS/SLOANE) *Ist n ungerade, so hat der Körper $\mathbb{F}_{2^n}$ eine zu sich selbst duale Normalbasis.*

Anmerkung. Es ist bekannt, dass $\mathbb{F}_{2^n}$ für gerades n genau dann eine selbstduale Normalbasis hat, wenn $n \equiv 2 \pmod 4$.

A.4 Potenzabbildungen

In diesem Abschnitt werden für den Körper $K = \mathbb{F}_{2^n}$ mit 2^n Elementen die Abbildungen

$$f_s \colon K \longrightarrow K, \quad f_s(x) = x^s, \quad \text{für } s \in \mathbb{Z}$$

untersucht; für $s \leq 0$ wird $f_s(0) = 0$ gesetzt.

Bemerkungen

1. Auf $K^\times$ ist $f_0 = f_{2^n-1} = 1$ konstant.
2. Auf $K^\times$ ist $f_{2^n-2}(x) = x^{-1}$, also f_{2^n-2} die Inversionsabbildung.
3. $f_{2^k} = \varphi^k$ mit dem FROBENIUS-Automorphismus φ.
4. Wie sieht die algebraische Normalform von f_0 aus? Wir kennen sie schon aus Abschnitt 1.3: Bezüglich einer geeigneten Basis von K über $\mathbb{F}_2$ mit 1 als erstem Basisvektor sind alle Komponenten 0 bis auf die erste, die die algebraische Normalform

   $$\sum_{I \subseteq \{1,\ldots,n\}} T^I$$

   hat. Insbesondere ist $\operatorname{Grad} f_0 = n$.
5. Für alle $s, t \in \mathbb{Z}$ gilt $f_s f_t = f_{s+t}$, denn $x^s x^t = x^{s+t}$ für alle $x \neq 0$.
6. Insbesondere ist $f_{s+2^n-1} = f_s f_{2^n-1} = f_s$ für alle $s \in \mathbb{Z}$. Die Zuordnung $\mathbb{Z} \longrightarrow K^K$, $s \mapsto f_s$, hat also die Periode $2^n - 1$.
7. $\operatorname{Grad} f_{s+t} \leq \operatorname{Grad} f_s + \operatorname{Grad} f_t$; allgemeiner gilt sogar für $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ beliebig und $\gamma : \mathbb{F}_2^q \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ bilinear, dass $\operatorname{Grad} \gamma \circ (f, g) \leq \operatorname{Grad} f + \operatorname{Grad} g$.
8. Für alle $s, t \in \mathbb{Z}$ gilt $f_s \circ f_t = f_{st}$, denn $(x^t)^s = x^{st}$ für alle $x \neq 0$.
9. f_{st} ist genau dann bijektiv, wenn f_s und f_t bijektiv sind. Sind nämlich f_s und f_t bijektiv, so auch $f_{st} = f_s \circ f_t$. Ist f_s nicht bijektiv, so nicht surjektiv, also $f_s \circ f_t$ nicht surjektiv. Ist f_t nicht bijektiv, so nicht injektiv, also $f_s \circ f_t$ nicht injektiv.
10. Ist $s = 2^k t$ mit ungeradem t, so ist $\operatorname{Grad} f_s = \operatorname{Grad} f_t$. Es ist nämlich $f_s = f_{2^k} \circ f_t = \varphi^k \circ f_t$, und φ^k ist als Automorphismus von K linear über dem Grundkörper $\mathbb{F}_2$.

Insbesondere hat f_s dem ersten Anschein zum Trotz im allgemeinen *nicht* den algebraischen Grad s. Man erhält relativ leicht eine obere Schranke. Dazu sei $s \geq 1$ und $s = \sum_{i \in I_s} 2^i$ die Binärdarstellung. Dann heißt

$$\mathrm{wt}(s) := \# I_s$$

das HAMMING-**Gewicht** von s.

Hilfssatz 7 *Sei $s \geq 1$. Dann hat die Potenzabbildung $f_s : K \longrightarrow K$ den algebraischen Grad* $\operatorname{Grad} f_s \leq \mathrm{wt}(s)$.

Beweis. Falls $\mathrm{wt}(s) = 1$, ist $s = 2^k$ für ein k, also $f_s = \varphi^k$ linear und nicht 0, also vom Grad 1.

Für einen Induktionsbeweis wird jetzt $\mathrm{wt}(s) \geq 2$ angenommen. Dann ist $f_s = f_t \varphi^k$, wobei k das größte Element von I_s und $t = s - 2^k$ ist. Mit Bemerkung 7 folgt

$$\operatorname{Grad} f_s \leq \operatorname{Grad} f_t + 1 \leq \mathrm{wt}(t) + 1 = \mathrm{wt}(s)$$

nach Induktionsvoraussetzung. $\diamond$

Um in Hilfssatz 7 die Gleichheit zu beweisen, wird ausgenutzt, dass f_s für $s \leq 2^n - 1$ das Produkt von $\mathrm{wt}(s)$ verschiedenen Automorphismen von K ist. Betrachtet wird also eine Abbildung

$$f = \sigma_1 \cdots \sigma_m$$

mit paarweise verschiedenen $\sigma_i \in \operatorname{Aut} K$ für $i = 1, \ldots, m$. Zunächst zwei Hilfssätze:

Hilfssatz 8 *Seien $\sigma_1, \ldots, \sigma_r \in \operatorname{Aut} K$, $a, u \in K$. Dann ist*

$$\Delta_u(a\sigma_1 \cdots \sigma_r)(x) = a \cdot \sum_{i=1}^{r} \sigma_i(u) \prod_{j \neq i} \sigma_j(x) + h(x)$$

mit $h \colon K \longrightarrow K$ vom Grad $< r$.

Beweis. Das folgt aus der Formel

$$\Delta_u(a\sigma_1 \cdots \sigma_r)(x) = a \cdot \sigma_1(x+u) \cdots \sigma_r(x+u) - a \cdot \sigma_1(x) \cdots \sigma_r(x)$$

mit dem Distributivgesetz. $\diamond$

Hilfssatz 9 *Für $x, u_1, \ldots, u_r \in K$ und $f = \sigma_1 \cdots \sigma_m$ gilt:*

$$\Delta_{u_1 \ldots u_r} f(x) = \sum_{I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, m\}} \left[\sum_{\pi \in \mathcal{S}_r} \prod_{j=1}^{r} \sigma_{\pi(i_j)}(u_j) \right] \prod_{k \notin I} \sigma_k(x) + h(x)$$

mit $h \colon K \longrightarrow K$ vom Grad $< m - r$.

Beweis. Der Induktionsanfang $r = 0$ ist trivial: Auf der rechten Seite gibt es nur einen Summanden, nämlich für $I = \emptyset$, und der ist $\sigma_1(x) \cdots \sigma_m(x)$

Für den Schluss von r auf $r+1$ wird mit Hilfssatz 8 berechnet

$$\begin{aligned}
\Delta_{u_0 \ldots u_r} f(x) &= \Delta_{u_0}(\Delta_{u_1 \ldots u_r} f)(x) \\
&= \sum_{I=\{i_1,\ldots,i_r\}} \left[\sum_{\pi \in \mathcal{S}_r} \prod_{j=1}^{r} \sigma_{\pi(i_j)}(u_j) \right] \left[\sum_{k \notin I} \sigma_k(u_0) \cdot \prod_{l \notin I \cup \{k\}} \sigma_l(x) \right] \\
&\quad + \Delta_{u_0} h(x) \\
&= \sum_{J=\{i_0,\ldots,i_r\}} \left[\sum_{\pi \in \mathcal{S}_{r+1}} \prod_{j=0}^{r} \sigma_{\pi(i_j)}(u_j) \right] \prod_{l \notin J} \sigma_l(x) + \tilde{h}(x)
\end{aligned}$$

mit $\tilde{h}$ vom algebraischen Grad $< m - r - 1$. $\diamond$

Speziell im Fall $r = m$, also $I = \{1, \ldots, m\}$, folgt

Korollar 1 *Sind die σ_i paarweise verschieden, so ist die Differenzenfunktion*

$$\Delta_{u_1 \ldots u_m} f(x) = \sum_{\pi \in \mathcal{S}_m} \prod_{j=1}^{m} \sigma_{\pi(j)}(u_j)$$

konstant $\neq 0$.

Beweis. Es ist

$$\begin{aligned}
\Delta_{u_1 \ldots u_m} f(x) &= \sum_{\pi \in \mathcal{S}_m} \left[\prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) \right] \sigma_{\pi(m)}(u_m) \\
&= \sum_{k=1}^{m} \left[\sum_{\pi \in \mathcal{S}_m, \pi(m)=k} \prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) \right] \sigma_k(u_m).
\end{aligned}$$

Wäre das 0 für alle $u_m \in K$, so wäre wegen der linearen Unabhängigkeit der Charaktere, Satz 1,

$$\sum_{\pi \in \mathcal{S}_m, \pi(m)=k} \prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) = 0$$

für alle k und $u_1, \ldots, u_{m-1} \in K$. Mit Induktion würde schließlich folgen $\sigma_1(u_1) = \cdots = \sigma_m(u_1) = 0$ für alle $u_1 \in K$, Widerspruch. $\diamond$

Korollar 2 *Sind $\sigma_1, \ldots, \sigma_m$ paarweise verschiedene Automorphismen von K, so ist* $\operatorname{Grad} \sigma_1 \cdots \sigma_m = m$.

Damit ist gezeigt:

Satz 6 *Die Potenzabbildung* $f_s\colon K \longrightarrow K$ *hat für* $1 \le s \le 2^n - 1 = \#K - 1$ *den algebraischen Grad* $\mathrm{wt}(s)$.

Korollar 1 *Die* (2^k+1)*-te Potenz* $f_{2^k+1}\colon K \longrightarrow K$ *hat den algebraischen Grad* 2, *wenn* $n = \operatorname{Dim} K \ge k+1$.

Insbesondere sind f_3, f_5, f_9, f_{17} quadratische Abbildungen, wenn $n \ge 2, 3, 4, 5$ ist, und $f_{-1} = f_{2^n-2}$ hat den Grad $n-1$.

Als nächstes wird untersucht, wann f_s bijektiv ist. Es ist $K^\times$ eine Gruppe der Ordnung $2^n - 1$ und $f_s\colon K^\times \longrightarrow K^\times$ ein Gruppenhomomorphismus. In seinem Kern liegen genau die Elemente $x \in K$ mit $x^s = 1$, also $\operatorname{Ord} x | s$, also $\operatorname{Ord} x | \operatorname{ggT}(s, 2^n - 1)$. Damit ist gezeigt:

Satz 7 *Ist* K *ein endlicher Körper der Charakteristik* 2 *und Dimension* n *über* $\mathbb{F}_2$, *so ist die Potenzabbildung* $f_s\colon K \longrightarrow K$, *genau dann bijektiv, wenn* s *zu* $2^n - 1$ *teilerfremd ist.*

Korollar 1 (i) f_3 *ist genau dann bijektiv, wenn* n *ungerade ist.*
(ii) f_5 *ist genau dann bijektiv, wenn* n *kein Vielfaches von* 4 *ist.*
(iii) f_7 *ist genau dann bijektiv, wenn* n *kein Vielfaches von* 3 *ist.*

Beweis. Das folgt, weil $p = 3, 5, 7$ Primzahl ist und $p | 2^n - 1$ genau dann, wenn $2^n \equiv 1 \pmod{p}$. Und 2 hat mod $3, 5, 7$ die multiplikative Ordnung $2, 4, 3$. $\diamond$

A.5 Quadratische Gleichungen in Charakteristik 2

Sei weiterhin $K = \mathbb{F}_{2^n}$ der Körper mit 2^n Elementen. Wir wollen die Nullstellen des quadratischen Polynoms

$$f = aT^2 + bT + c \in K[T] \quad \text{mit } a \neq 0$$

bestimmen.

Der Fall $b = 0$ ist sehr einfach. Es ist

$$a \cdot f = (aT)^2 + ac = g(aT) \quad \text{mit } g = T^2 + ac \in K[T].$$

Da ac in K ein Quadrat ist, $ac = d^2$, ist

$$g = (T+d)^2 = h(T+d) \quad \text{mit } h = T^2 \in K[T],$$

und f hat genau die eine Nullstelle $\frac{d}{a}$. Zur expliziten Berechnung muss die Quadratwurzel aus ac gezogen werden.

Sei nun $b \neq 0$. Dann ist

$$\frac{a}{b^2} \cdot f = (\frac{a}{b}\,T)^2 + \frac{a}{b}\,T + \frac{ac}{b^2} = g(\frac{a}{b}\,T) \quad \text{mit } g = T^2 + T + d,\ d = \frac{ac}{b^2} \in K.$$

Betrachten wir also die Nullstellen eines solchen Polynoms g. Da die Ableitung konstant 1 ist, hat g in K entweder keine Nullstelle oder zwei verschiedene (einfache) Nullstellen. Sei u eine Nullstelle von g im algebraischen Abschluss von K. Dann ist $u+1$ die andere, und $u(u+1) = d$, also $d = u^2+u$.

Hilfssatz 10 *$g = T^2 + T + d \in K[T]$ hat genau dann eine Nullstelle u in K, wenn $\mathrm{Tr}(d) = 0$. Ist das der Fall, so $g = h(T + u)$ mit $h = T^2 + T$.*

Beweis. „$\Longrightarrow$“: Ist $u \in K$, so ist $\mathrm{Tr}(d) = \mathrm{Tr}(u^2) + \mathrm{Tr}(u) = 0$.

„$\Longleftarrow$“: Sei umgekehrt $\mathrm{Tr}(d) = 0$. Dann ist

$$\begin{aligned} 0 &= \mathrm{Tr}(d) = d + d^2 + \cdots + d^{2^{n-1}} \\ &= (u^2 + u) + (u^4 + u^2) + \cdots + (u^{2^n} + u^{2^{n-1}}) \\ &= u + u^{2^n}, \end{aligned}$$

also $u^{2^n} = u$ und somit $u \in K$.

Der Zusatz ist trivial. $\diamond$

Anmerkung. Der Hilfssatz ist ein Spezialfall des sogenannten Theorem 90 von Hilbert, additive Form. Zur expliziten Bestimmung der Nullstelle hilft er leider gar nicht. Immerhin führt er die Auflösung auf die Auflösung der Gleichung $u^2 + u = ac/b^2$ nach u zurück.

Korollar 1 *$g = T^2+T+d \in K[T]$ ist genau dann irreduzibel, wenn $\mathrm{Tr}(d) = 1$. Ist das der Fall, so $g = h(T+r)$ mit $h = T^2+T+e$, wobei e ein beliebiges Element von K mit Spur $\mathrm{Tr}(e) = 1$ ist und $r \in K$ mit $r^2 + r = d + e$.*

Beweis. g ist in $K[T]$ genau dann irreduzibel, wenn es kein Nullstelle in K hat. Der Zusatz folgt, weil $d + e$ die Spur 0 hat, also von der Form $r^2 + r$ ist. $\diamond$

Damit ist gezeigt:

Satz 8 (Nullstellen) *Sei K ein endlicher Körper der Charakteristik 2 und $f = aT^2 + bT + c \in K[T]$ vom Grad 2. Dann gilt:*

(i) *f hat genau eine Nullstelle in $K \iff b = 0$.*

(ii) *f hat genau zwei Nullstellen in $K \iff b \neq 0$ und $\mathrm{Tr}(\frac{ac}{b^2}) = 0$.*

(iii) *f hat keine Nullstelle in $K \iff b \neq 0$ und $\mathrm{Tr}(\frac{ac}{b^2}) = 1$.*

Satz 9 (Normalform) *Sei K ein endlicher Körper der Charakteristik 2 und $f = aT^2 + bT + c \in K[T]$ vom Grad 2. Dann gibt es ein $e \in K^\times$ und eine affine Transformation $\alpha : K \longrightarrow K$, $\alpha(x) = rx + s$ mit $r \in K^\times$ und $s \in K$, so dass*

$$e \cdot f \circ \alpha = T^2, \quad T^2 + T \quad \text{oder } T^2 + T + d,$$

wobei $d \in K$ ein beliebiges Element mit Spur $\mathrm{Tr}(d) = 1$ ist. Im Fall $n = \mathrm{Dim}\, K$ ungerade ist $e = 1$ wählbar.

Anmerkung. Eine Verallgemeinerung auf einen beliebigen endlichen Grundkörper $\mathbb{F}_q$ statt $\mathbb{F}_2$ und Polynome $T^q - T - d$ ist der Satz von Artin-Schreier, der die zyklischen Körpererweiterungen vom Grad q charakterisiert.

A.6 Elliptische Kurven

Sei K ein Körper und $f \in K[X, Y]$ ein Polynom in zwei Unbestimmten vom Grad $n \geq 1$. Sei $L \supseteq K$ ein Erweiterungskörper. Dann heißt

$$C(L) := \{(x, y) \in L^2 \mid f(x, y) = 0\}$$

die Menge der L-wertigen Punkte der (affinen) ebenen algebraischen Kurve C zu f.

> [Die „Kurve“ C selbst ist die Zuordnung $C : \mathrm{Alg}_K \longrightarrow$ Meng; in der Sprache der Kategorientheorie ist das ein Funktor, in der Sprache der Algebraischen Geometrie speziell ein Schema.]

Eine solche affine Kurve lässt sich zu einer projektiven Kurve erweitern. Dazu betrachtet man die homogenisierte Form von f,

$$F = Z^n \cdot f(\frac{X}{Z}, \frac{Y}{Z}) \in K[X, Y, Z],$$

die ein homogenes Polynom vom Grad n ist, und die projektive Ebene $\mathbb{P}^2$ über K mit

$$\mathbb{P}^2(L) = \{(x : y : z) \mid x, y, z \in L, \text{nicht alle } 0\},$$

wobei die „homogenen Koordinaten“ $(x : y : z)$ die Bahnen von $L^3 - \{0\}$ unter der Operation

$$(x, y, z) \overset{\lambda \in L^\times}{\mapsto} (\lambda x, \lambda y, \lambda z)$$

der multiplikativen Gruppe $L^\times$ repräsentieren. Damit ist

$$\bar{C}(L) = \{(x : y : z) \in \mathbb{P}^2(L) \mid F(x, y, z) = 0\}$$

die Menge der L-wertigen Punkte der (projektiven) ebenen algebraischen Kurve zu F.

„Punkte im Endlichen“ sind die $(x : y : z)$ mit $z \neq 0$, also die $(x : y : 1)$. Es gilt

$$F(x, y, 1) = 0 \Longleftrightarrow f(x, y) = 0,$$

die Punkte der projektiven Kurve im Endlichen sind also (bei kanonischer Identifizierung) die Punkte der affinen Kurve. Die übrigen Punkte von $\mathbb{P}^2$, also die $(x : y : 0)$, heißen „Punkte im Unendlichen“.

Elliptische Kurven sind die Kurven zu den Polynomen

$$f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in K[X, Y]$$

in der affinen Version bzw.

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X, Y, Z]$$

in der projektiven Version.

> [Außerdem verlangt man, dass die elliptische Kurve keine Singularitäten hat; d. h., es gibt in keinem Erweiterungskörper von K eine gemeinsame Nullstelle des Polynoms und aller seiner partiellen Ableitungen.]

Durch lineare Koordinatentransformation lässt sich f

- im Fall $\operatorname{char} K \neq 2, 3$ auf die Normalform

$$Y^2 - X^3 - aX - b \in K[X, Y]$$

- im Fall $\operatorname{char} K = 3$ auf die Normalform

$$Y^2 - X^3 - aX^2 - bX - c \in K[X, Y]$$

bringen (ohne Beweis – **Übungsaufgabe**). Zur Anwendung auf BOOLEsche Abbildungen interessiert der Fall $\operatorname{char} K = 2$. Hier sind zwei Fälle zu unterscheiden, der **gewöhnliche Fall** mit $a_1 \neq 0$ und der **supersinguläre Fall** mit $a_1 = 0$.

Im *gewöhnlichen Fall* geht f nach der Transformation $X \mapsto \frac{X}{a_1} - \frac{a_3}{a_1}$ und anschließender Umbenennung der Koeffizienten über in

$$Y^2 + XY - X^3 - b_2X^2 - b_4X - b_6,$$

nach der weiteren Transformation $Y \mapsto Y + b_4$ in die Normalform

$$Y^2 + XY - X^3 - aX^2 - b.$$

Zu einer andere Version der Normalform kommt man durch die weitere Transformation $Y \mapsto Y + sX$; zunächst erhält man

$$Y^2 + s^2X^2 + XY + sX^2 - X^3 - aX^2 - b.$$

Ist nun $\operatorname{Tr} a = 0$, so kann man nach Hilfssatz 10 ein s wählen mit $s^2 + s = a$, also erhält man die Gestalt $Y^2 + XY - X^3 - b$, die man durch $Y \mapsto Y + t$ mit $t^2 = b$ noch in die alternative Normalform

$$(E_a^+) \qquad\qquad Y^2 + XY - X^3 - aX$$

umformen kann. Ist dagegen $\operatorname{Tr} a = 1$, so $\operatorname{Tr}(a+\tau) = 0$ für ein fest gewähltes $\tau \in K$ mit $\operatorname{Tr} \tau = 1$; also kann man s wählen mit $s^2 + s = a + \tau$ und erhält die Gestalt $Y^2 + XY - X^3 - \tau X^2 - b$, die durch $Y \mapsto Y + t$ wie oben in die Normalform

$$(E_a^-) \qquad Y^2 + XY - X^3 - \tau X^2 - aX$$

umgewandelt wird. In beiden Fällen ist $a \neq 0$, da sonst 0 Singularität der Kurve ist: $\frac{\partial f}{\partial X} = Y - X - a$, $\frac{\partial f}{\partial Y} = X$ in beiden Fällen.

Damit sind die gewöhnlichen elliptischen Kurven im Fall $\operatorname{char} K = 2$ in zwei Scharen klassifiziert, die jeweils durch $a \in K^\times$ parametrisiert werden.

Im *supersingulären Fall* ist notwendig $a_3 \neq 0$, da es sonst wegen $\frac{\partial f}{\partial Y} = 0$ (konstant) Singularitäten gäbe, und durch die Transformation $X \mapsto X - a_2$ kommt man zur Normalform

$$(\text{SuSi}) \qquad Y^2 + aY - X^3 - bX - c$$

mit $a \in K^\times$. Dieser Fall interessiert im folgenden nicht weiter. Zusammengefasst haben wir:

Satz 10 (Normalformen elliptischer Kurven) *Sei K ein endlicher Körper der Charakteristik 2 und $f \in K[X,Y]$ das definierende Polynom einer (affinen) elliptischen Kurve über K. Dann lässt sich f durch affine Koordinatentransformationen auf eine der der drei Normalformen (E_a^+), (E_a^+) oder* (SuSi) *bringen.*

Die Aufgabe, die Anzahl der K-wertigen Punkte einer elliptischen Kurve für einen endlichen Körper K zu bestimmen oder abzuschätzen, gehört zu den ganz prominenten mathematischen Problemen. Ein tiefliegendes Ergebnis ist z. B. der Satz von Hasse:

Satz 11 (Hasse) *Sei K ein endlicher Körper mit q Elementen, E eine über K definierte (projektive) elliptische Kurve und $N = \#E(K)$ die Anzahl ihrer K-wertigen Punkte. Dann gilt:*

$$N = q + 1 + s \quad \textit{mit} \quad |s| \leq 2 \cdot \sqrt{q}.$$

(D. h., N weicht nicht zu stark von q ab.)

Der Beweis wird hier nicht wiedergegeben (siehe [131]); er beruht auf der Untersuchung der Zeta-Funktion der elliptischen Kurve.

Im Fall $q = 2^n$ wird die Formel zu

$$N = 2^n + 1 + s \quad \text{mit} \quad |s| \leq 2^{\frac{n}{2}+1}.$$

Für die gewöhnlichen elliptischen Kurven in Charakteristik 2 kommt man mit dem Versuch einer direkten Zählung der Punkte zu einer interessanten Formel. Diese Kurven werden in der projektiven Version durch die Polynome

$$\begin{array}{rll} & Y^2Z + XYZ & -X^3 - aXZ^2 \\ \text{bzw.} & Y^2Z + XYZ & -X^3 - \tau X^2 Z - aXZ^2 \end{array}$$

definiert. Vertauscht man X und Z (das bedeutet geometrisch, eine andere Gerade als „unendlich fern“ zu interpretieren), so werden diese Normalformen zu

$$\begin{array}{ll} (F_a^+) & XY^2 + XYZ - aX^2Z - Z^3 \\ (F_a^-) & XY^2 + XYZ - aX^2Z - \tau XZ^2 - Z^3 \end{array}$$

mit $a \in K^\times$ beliebig.

Zählen wir in dieser Version die K-wertigen Punkte $(x : y : z)$ der zugehörigen elliptischen Kurve für $K = \mathbb{F}_{2^n}$:

Im „Unendlichen“, also für $z = 0$, heißt die Bedingung $xy^2 = 0$, also $x = 0$ oder $y = 0$, also gibt es genau zwei solche Punkte: $(1 : 0 : 0)$ und $(0 : 1 : 0)$.

Im „Endlichen“ können wir $z = 1$ setzen und erhalten für (F_a^+) die Bedingung

$$(x : y : 1) \in E(K) \Longleftrightarrow xy^2 + xy = ax^2 + 1 \Longleftrightarrow y^2 + y = ax + \frac{1}{x},$$

denn mit $x = 0$ gibt es keine Lösung.

- Ist $x \in K^\times$ ein Wert mit $\mathrm{Tr}(ax + \frac{1}{x}) = 0$, so gibt es genau zwei Werte von y, so dass die Bedingung erfüllt ist.
- Ist $x \in K^\times$ ein Wert mit $\mathrm{Tr}(ax + \frac{1}{x}) \neq 0$, also $= 1$, so ist die Bedingung nicht erfüllbar.

Setzt man

$$N_a^+ := \#\{x \in K^\times \mid \mathrm{Tr}(ax + \frac{1}{x}) = 0\},$$

so ist gezeigt:

Satz 12 *Die für $a \in K^\times$ durch (F_a^+) definierte elliptische Kurve über $K = \mathbb{F}_{2^n}$ hat genau*

$$2N_a^+ + 2$$

K-wertige Punkte.

Die gleiche Überlegung für (F_a^-) ergibt die Bedingung

$$(x:y:1) \in E(K) \Longleftrightarrow xy^2 + xy = ax^2 + 1 + \tau x \Longleftrightarrow y^2 + y = ax + \frac{1}{x} + \tau.$$

Hier gibt es keine Möglichkeit für y, wenn $\mathrm{Tr}(ax + \frac{1}{x}) = 0$, und genau zwei, wenn $\mathrm{Tr}(ax + \frac{1}{x}) = 1$. Mit

$$N_a^- := \#\{x \in K^\times \mid \mathrm{Tr}(ax + \frac{1}{x}) = 1\}$$

folgt also:

Korollar 1 *Die für $a \in K^\times$ durch (F_a^-) definierte elliptische Kurve über $K = \mathbb{F}_{2^n}$ hat genau*

$$2N_a^- + 2$$

K-wertige Punkte.

Hilfssatz 11 *N_a^+ ist ungerade, N_a^- gerade für jedes $a \in K^\times$.*

Beweis. Da $N_a^+ + N_a^- = 2^n - 1$, genügt es, die erste Aussage zu beweisen. Es gibt genau ein $b \in K^\times$ mit $b^2 = a^{-1}$; für dieses ist $ab = b^{-1}$, also $\mathrm{Tr}(ab + b^{-1}) = 0$. Alle anderen Lösungen von $\mathrm{Tr}(ax + x^{-1}) = 0$ kommen paarweise vor: Ist $x \in K^\times - \{b\}$ eine solche, so ist auch $y = a^{-1}x^{-1}$ eine, denn $\mathrm{Tr}(ay + y^{-1}) = \mathrm{Tr}(x^{-1} + ax) = 0$, und $y \neq x$. $\diamond$

Korollar 2 *Sei E eine gewöhnliche elliptische Kurve über $K = \mathbb{F}_{2^n}$ mit $n \geq 2$ und $N = 2^n + 1 + s$ die Anzahl ihrer K-wertigen Punkte. Dann ist s ungerade, und zwar $s = 2N_a^+ + 1 - 2^n \equiv 3 \pmod 4$ im Fall (F_a^+), $s = 2N_a^- + 1 - 2^n \equiv 1 \pmod 4$ im Fall (F_a^-).*

Beweis. $2^n + 1 + s = N = 2N_a^\pm + 2$, und für $n \geq 2$ ist 2^n durch 4 teilbar. $\diamond$

Die relevanten Zahlen $N_a^\pm$ kann man durch Exponential-Summen, sogenannte Kloosterman-Summen, ausdrücken: Die reellwertige Funktion

$$\kappa\colon K^\times \longrightarrow \mathbb{R}$$

sei definiert durch

$$\kappa(u) := \sum_{x \in K^\times} (-1)^{\mathrm{Tr}(ux + x^{-1})}.$$

Klar, dass

$$\kappa(u) = N_u^+ - N_u^- = 2N_u^+ - 2^n + 1 = s,$$

wobei $2^n + 1 + s$ die Anzahl der Punkte der gewöhnlichen elliptischen Kurve vom Typ (F_u^+) ist. Also gilt für $n \geq 2$:

Korollar 3 (i) $\kappa(u) \equiv 3 \pmod 4$ *für alle* $u \in K^\times$.
(ii) $|\kappa(u)| \leq 2^{\frac{n}{2}+1}$ *für alle* $u \in K^\times$.

An dieser Stelle wird ein weiteres tiefliegendes Ergebnis aus der Theorie der elliptischen Kurven ohne Beweis verwendet – siehe [137]:

Satz 13 (Honda) *Für jede ungerade Zahl* $s \in \mathbb{Z}$ *mit* $|s| \leq 2^{\frac{n}{2}+1}$ *gibt es eine gewöhnliche elliptische Kurve über* $K = \mathbb{F}_{2^n}$*, die genau* $2^n + 1 + s$ K*-wertige Punkte hat.*

Klar im Fall $n \geq 2$, dass $s \equiv 3 \pmod 4$ genau dann, wenn die Kurve vom Typ (F_a^+) ist. Daraus folgt unmittelbar:

Hauptsatz 1 (Lachaud/Wolfmann) *Die* Kloosterman*-Funktion* κ *nimmt für* $n \geq 2$ *genau die Werte* $s \in \mathbb{Z}$ *mit* $|s| \leq 2^{\frac{n}{2}+1}$ *und* $s \equiv 3 \pmod 4$ *an.*