Das Umkehrproblem der Galoistheorie

Bachelorarbeit

Paul Ziegler

Betreuer

Prof. Richard Pink

Frühlingsemester 2008

Departement Mathematik

ETH Zürich

Inhaltsverzeichnis

1 Einleitung

Sei p prim, $s \in \mathbb{N}$ und $q = p^s$. Es sei $\mathbb{F}_q$ der Körper mit q Elementen. Sei k eine Körpererweiterung von $\mathbb{F}_q$ und $\bar{k}$ ein algebraischer Abschluss von k. Für Polynome $f(X) \in k[X]$ der Form $f(X) = \sum_{i=0}^{n} a_i X^{q^i}$ gilt $f(x+y) = f(x) + f(y)$ für alle x, y in $\bar{k}$ und $f(\lambda x) = \lambda f(x)$ für alle $\lambda \in \mathbb{F}_q$ und alle $x \in \bar{k}$. Deshalb nennen wir solche Polynome $\mathbb{F}_q$-linear. Die Nullstellenmenge V von f in $\bar{k}$ ist ein $\mathbb{F}_q$-Vektorraum. Aus $f' = a_0$ folgt, dass f separabel ist genau dann wenn $a_0 \neq 0$. In diesem Fall ist $|V| = q^n$, deshalb hat V Dimension n. Es sei $\mathrm{Gal}(f)$ die Galoisgruppe von f. Da diese $\mathbb{F}_q$-linear auf V operiert, kann man $\mathrm{Gal}(f)$ wie folgt als Untergruppe der $\mathrm{GL}_n(\mathbb{F}_q)$ auffassen: Sei $\Phi : V \to \mathbb{F}_q^n$ ein Vektorraumisomorphismus. Dann ist die Abbildung

$$\begin{aligned} \mathrm{Gal}(f) &\to \mathrm{GL}_n(\mathbb{F}_q) \\ \sigma &\mapsto \Phi \circ \sigma|_V \circ \Phi^{-1} \end{aligned}$$

injektiv, weil V den Zerfällungskörper von f über $\mathbb{F}_q$ erzeugt. Dies hängt aber von der Wahl einer Basis von V ab, deshalb ist diese Einbettung nur bis auf Konjugation bestimmt. Das Ziel dieser Arbeit ist zu zeigen, dass es für den Funktionenkörper $k = \mathbb{F}_q(T)$, für jedes $n \geq 1$ und jede Primpotenz q separable $\mathbb{F}_q$-lineare Polynome f und g mit $\mathrm{Gal}(f) = \mathrm{GL}_n(\mathbb{F}_q)$ und $\mathrm{Gal}(g) = \mathrm{SL}_n(\mathbb{F}_q)$ gibt. Wir werden auch zeigen, wie man solche Polynome explizit berechnen kann.

Diese Arbeit behandelt also einen Spezialfall des allgemeinen Umkehrproblems der Galoistheorie. Dabei handelt es sich um die Frage, wann es zu einem Körper k und einer Gruppe G eine Galoiserweiterung ℓ/k gibt, deren Galoisgruppe G ist.

Im ersten Abschnitt wird zunächst untersucht, welche Gruppen als Galoisgruppen von $\mathbb{F}_q$-linearen Polynomen über $\mathbb{F}_q$ auftreten. In den nächsten beiden Abschnitten werden einige Hilfmittel eingeführt, die dann im vierten Abschnitt verwendet werden, um zu untersuchen, welche Gruppen als Galoisgruppen von $\mathbb{F}_q$-linearen Polynomen über einer endlichen Erweiterung von $\mathbb{F}_q$ auftreten. Im fünften Abschnitt wird beschrieben, wie sich die Galoisgruppe eines $\mathbb{F}_q$-linearen Polynoms mit Koeffizienten in einem Ring verhält, wenn diese Koeffizienten modulo ein Primideal reduziert werden. Mit den Resultaten aus den ersten fünf Abschnitten kann dann in den nächsten beiden Abschnitten die Existenz der gesuchten Polynome bewiesen werden. Im neunten Abschnitt wird schliesslich ein Erzeugendensystem der $\mathrm{GL}_n(\mathbb{F}_q)$ erarbeit, mit dessen Hilfe, wie im letzen Abschnitt gezeigt wird, sich $\mathbb{F}_q$-lineare Polynome mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$ explizit angeben lassen.

2 Der Fall $k = \mathbb{F}_q$

Wir untersuchen zunächst den Fall $k = \mathbb{F}_q$. Dann ist der Zerfällungskörper von f eine endliche Körpererweiterung von $\mathbb{F}_q$. Deshalb ist $\mathrm{Gal}(f)$ zyklisch und wird vom Frobeniusautomorphismus $\tau : x \mapsto x^q$ erzeugt. Für $\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$

bezeichne $\mu_\sigma(X) \in \mathbb{F}_q[X]$ das Minimalpolynom von σ und $\chi_\sigma(X) \in \mathbb{F}_q[X]$ das charakteristische Polynom von σ.

Lemma 2.1. *Es sei $f(X) = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_q[X]$ separabel. Dann ist $\mu_\tau(X) = \chi_\tau(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$.*

Beweis. Es seien $\mu_\tau(X) = X^m + \sum_{i=0}^{m-1} b_i X^i$ und $\tilde{f}(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{F}_q[X]$. Für alle $x \in V = \ker f$ gilt

$$f(x) = \tau^n(x) + \sum_{i=0}^{n-1} a_i \tau^i(x) = \tilde{f}(\tau)(x) = 0.$$

Daraus folgt $\mu_\tau | \tilde{f}$. Da für die q^n verschiedenen Elemente x von V gilt

$$\tau^m(x) + \sum_{i=0}^{m-1} b_i \tau^i(x) = x^{q^m} + \sum_{i=0}^{m-1} b_i x^{q^i} = 0,$$

folgt $m = \deg \mu_\tau \geq n$. Da $\tilde{f}$ und μ_τ normiert sind, muss also $\tilde{f} = \mu_\tau$ sein. Da χ_τ ebenfalls normiert ist, folgt aus $\mu_\tau | \chi_\tau$ und $\deg \chi_\tau = n = \deg \mu_\tau$ auch $\mu_\tau = \chi_\tau$.□

Lemma 2.2. *Es seien $\sigma, \tau \in \mathrm{GL}_n(\mathbb{F}_q)$ mit $\mu_\sigma = \chi_\sigma = \mu_\tau = \chi_\tau$. Dann sind σ und τ konjugiert.*

Beweis. Da das charakteristische Polynom und das Minimalpolynom von σ übereinstimmen, besteht die Jordannormalform von σ aus genau einem Block für jeden Eigenwert von σ. Das Gleiche gilt für τ. Also haben σ und τ die gleiche Jordannormalform, woraus die Behauptung folgt. □

Satz 2.3. *Es treten bis auf Konjugation genau diejenigen Elemente der Gruppe $\mathrm{GL}_n(\mathbb{F}_q)$ als Bild des Frobeniusautomorphismus unter der Einbettung $\mathrm{Gal}(f) \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$ für separable $\mathbb{F}_q$-lineare Polynome $f \in \mathbb{F}_q[X]$ auf, deren charakteristisches Polynom und Minimalpolynom übereinstimmen.*

Beweis. Es sei $f(X) = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i}$ separabel und τ sei der Frobeniusautomorphismus $x \mapsto x^q$. Aus Lemma 2.1 folgt, dass das charakteristische Polynom und das Minimalpolynom von τ übereinstimmen.

Sei andererseits $\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$ mit $\mu_\sigma(X) = \chi_\sigma(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$. Dann ist $a_0 = \pm \det(\sigma) \neq 0$. Deshalb ist $f(X) = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_q[X]$ separabel und es gilt $\mathrm{Gal}(f) = \langle \tau \rangle$ für den Frobeniusautomorphismus τ. Aus Lemma 2.1 folgt $\mu_\tau = \chi_\tau = \mu_\sigma = \chi_\sigma$. Aus Lemma 2.2 folgt damit, dass σ und τ konjugiert sind. □

3 Die Mooresche Determinante

Die Resultate in diesem Abschnitt sind dem Buch "Basic Structures of Function Field Arithmetic" von David Goss entnommen ([1], Abschnitt 1.4).

Es sei nun k eine beliebige Körpererweiterung von $\mathbb{F}_q$.

Definition 3.1. *Für $v_1, \ldots, v_n \in k$ ist die Mooresche Determinante definiert als*

$$\Delta(v_1, \ldots, v_n) = \det \begin{bmatrix} v_1 & \ldots & v_n \\ v_1^q & \ldots & v_n^q \\ \vdots & & \vdots \\ v_1^{q^{n-1}} & \ldots & v_n^{q^{n-1}} \end{bmatrix}.$$

Lemma 3.2. *Für $v_1, \ldots, v_n \in k$ gilt: $\{v_1, \ldots, v_n\}$ ist linear unabhängig über $\mathbb{F}_q$ genau dann, wenn $\Delta(v_1, \ldots, v_n) \neq 0$ ist.*

Beweis. Sei $\Delta(v_1, \ldots, v_n) \neq 0$. Seien a_i in $\mathbb{F}_q$ mit $\sum_{i=1}^n a_i v_i = 0$ gegeben. Sei $\tau : k \to k, x \mapsto x^q$ der Frobeniusautomorphismus. Da τ eine $\mathbb{F}_q$-lineare Abbildung ist, folgt

$$\sum_{i=1}^n a_i \begin{bmatrix} v_i \\ \tau(v_i) \\ \vdots \\ \tau^{n-1}(v_i) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Da $\Delta(v_1, \ldots, v_n)$ nicht 0 ist, folgt daraus, dass alle a_i gleich 0 sind. Also ist $\{v_1, \ldots, v_n\}$ linear unabhängig.

Sei nun $\{v_1, \ldots, v_n\}$ eine linear unabhängige Menge über $\mathbb{F}_q$. Wir zeigen $\Delta(v_1, \ldots, v_n) \neq 0$ mit Induktion nach n. Für $n = 1$ ist $\Delta(v_1) = v_1 \neq 0$. Wir nehmen nun widerspruchsweise an, dass die Behauptung für $n = t$ stimmt und dass $\Delta(v_1, \ldots, v_{t+1}) = 0$ ist. Es gibt also $a_1, \ldots, a_{t+1}$ in k, nicht alle 0, so dass gilt

$$\begin{gathered} a_1 v_1 + \ldots + a_{t+1} v_{t+1} = 0 \\ a_1 v_1^q + \ldots + a_{t+1} v_{t+1}^q = 0 \\ \vdots \\ a_1 v_1^{q^t} + \cdots + a_{t+1} v_{t+1}^{q^t} = 0. \end{gathered}$$

Wir können annehmen, dass $a_1 = 1$ ist. Indem wir τ auf die i-te Gleichung anwenden und diese danach von der $(i+1)$-ten Gleichung abziehen, erhalten wir dann

$$\begin{gathered} (a_2 - a_2^q) v_2^q + \cdots + (a_{t+1} - a_{t+1}^q) v_{t+1}^q = 0 \\ \vdots \\ (a_2 - a_2^q) v_2^{q^t} + \cdots + (a_{t+1} - a_{t+1}^q) v_{t+1}^{q^t} = 0. \end{gathered}$$

Da $\tau : k \to k$ ein Isomorphismus von $\mathbb{F}_q$-Vektorräumen ist, ist die Menge $\{v_2^q, \ldots, v_{t+1}^q\}$ linear unabhängig über $\mathbb{F}_q$. Aus der Induktionsannahme folgt daher, dass $\Delta(v_2^q, \ldots, v_{t+1}^q)$ nicht 0 ist. Dies impliziert $a_i - a_i^q = 0$ für alle $i \in \{2, \ldots, t+1\}$, also liegen alle a_i in $\mathbb{F}_q$. Daraus folgt aber, dass $\{v_1, \ldots, v_{t+1}\}$ über $\mathbb{F}_q$ linear abhängig ist. Dies ist ein Widerspruch, also ist die Behauptung bewiesen. □

Lemma 3.3. *Sei $V \subset k$ ein $\mathbb{F}_q$-Vektorraum und $(v_1, \ldots, v_n)$ eine Basis von V. Für*

$$f(X) = \prod_{v \in V} (X - v) \in k[X]$$

gilt:

(i) $f(X) = \frac{\Delta(v_1, \ldots, v_n, X)}{\Delta(v_1, \ldots, v_n)}$.

(ii) Das Polynom f ist $\mathbb{F}_q$-linear.

Beweis. (i)Aus Lemma 3.2 folgt, dass X eine Nullstelle von $\Delta(v_1, \ldots, v_n, X)$ ist genau dann, wenn $X \in V$ ist. Also ist $f(X) = c\Delta(v_1, \ldots, v_n, X)$ für ein $c \neq 0$. Indem man die Mooresche Determinante $\Delta(v_1, \ldots, v_n, X)$ nach der letzten Spalte entwickelt, sieht man, dass der Koeffizient von X^{q^n} in $\Delta(v_1, \ldots, v_n, X)$ gerade $\Delta(v_1, \ldots, v_n)$ ist. Da f normiert ist, folgt daraus $c = 1/\Delta(v_1, \ldots, v_n)$.

(ii) Dies sieht man, indem man die Darstellung aus (i) verwendet und die Mooresche Determinante nach der letzten Spalte entwickelt. □

Lemma 3.4. *Sei $V \subset k$ ein $\mathbb{F}_q$-Vektorraum und $(v_1, \ldots, v_n)$ eine Basis von V. Dann gilt*

$$\prod_{v \in V \setminus \{0\}} v = (-1)^n \Delta(v_1, \ldots, v_n)^{q-1}.$$

Beweis. Es sei

$$f(X) = \prod_{v \in V} (X - v) = \frac{\Delta(v_1, \ldots, v_n, X)}{\Delta(v_1, \ldots, v_n)}$$

wie in Lemma 3.3.

Der Koeffizient von X in $\prod_{v \in V}(X - v)$ ist $(-1)^{|V|-1} \prod_{v \in V \setminus \{0\}} v$. Da gilt $|V|-1 = q^n - 1$, ist $(-1)^{|V|-1} = 1$, falls die Charakteristik nicht 2 ist. In Charakteristik 2 ist $-1 = 1$, also gilt immer $(-1)^{|V|-1} = 1$. Indem man $\Delta(v_1, \ldots, v_n, X)$ nach der letzten Spalte entwickelt, sieht man, dass $(-1)^n \Delta(v_1^q, \ldots, v_n^q)$ der Koeffizient von X in $\Delta(v_1, \ldots, v_n, X)$ ist. Also folgt

$$\begin{aligned} \prod_{v \in V \setminus \{0\}} v &= (-1)^n \frac{\Delta(v_1^q, \ldots, v_n^q)}{\Delta(v_1, \ldots, v_n)} \\ &= (-1)^n \frac{\Delta(v_1, \ldots, v_n)^q}{\Delta(v_1, \ldots, v_n)} = (-1)^n \Delta(v_1, \ldots, v_n)^{q-1}. \quad \square \end{aligned}$$

4 Gruppenringe

Für einen Ring R und eine endliche Gruppe G sei $R[G]$ definiert als die Menge aller formalen Linearkombinationen der Form

$$\sum_{g \in G} x_g [g]$$

mit Koeffizienten $x_g \in R$. Auf $R[G]$ wird eine Addition und eine Multiplikation durch

$$\sum_{g\in G} x_g[g] + \sum_{g\in G} y_g[g] = \sum_{g\in G}(x_g + y_g)[g]$$

und

$$\left(\sum_{g\in G} x_g[g]\right)\left(\sum_{g\in G} y_g[g]\right) = \sum_{g\in G}\left(\sum_{\substack{h,h'\in G\\ hh'=g}} x_h y_{h'}\right)[g]$$

definiert. Dadurch wird $R[G]$ zu einem Ring, der Gruppenring genannt wird. Er ist genau dann kommutativ, wenn G abelsch ist. Ist R unitär, so ist auch $R[G]$ unitär.

Ist M ein Modul über dem Gruppenring $R[G]$, so erhält man eine R-lineare Aktion von links von G auf M, indem man die Aktion von $R[G]$ auf G einschränkt. Hat man umgekehrt eine R-lineare Aktion von G auf M, so rechnet man leicht nach, dass M mittels

$$R[G] \times M \to M$$
$$\left(\sum_{g\in G} x_g[g], x\right) \mapsto \sum_{g\in G} x_g(gx)$$

zu einem $R[G]$-Modul wird. Eine Struktur von M als $R[G]$-Modul anzugeben ist also äquivalent dazu, eine R-lineare Aktion von G auf M anzugeben.

Seien M, N zwei Mengen auf denen G von links operiert. Eine Abbildung $\varphi : N \to M$ heisst G-äquivariant, falls für alle $g \in G$ und für alle $x \in N$ gilt $\varphi(gx) = g\varphi(x)$.

Da die Multiplikation in $R[G]$ als R-lineare Fortsetzung der Multiplikation in G definiert ist, gilt, wie man leicht überprüft, das folgende Lemma:

Lemma 4.1. *Sei R ein Ring und G eine endliche Gruppe. Seien N, M zwei $R[G]$-Moduln. Für eine Abbildung $\varphi : N \to M$ sind äquivalent:*

(i) Die Abbildung φ ist ein Homomorphismus von $R[G]$-Moduln.

(ii) Die Abbildung φ ist R-linear und G-äquivariant.

Nun sei k ein Körper und G weiterhin eine endliche Gruppe. Wir betrachten einen $k[G]$-Modul V. Dann ist V insbesondere ein k-Vektorraum. Es sei V^* der duale Vektorraum von V. Mittels

$$(gv^*)(v) = v^*(g^{-1}v) \text{ für } g \in G, v \in V, v^* \in V^*$$

operiert G k-linear von links auf V^*. Diese Darstellung wird die kontragrediente Darstellung genannt. Durch sie wird V^* ebenfalls zu einem $k[G]$-Modul.

Zu $A \in \mathrm{GL}_n(k)$ bezeichne A^T die transponierte Matrix. Das folgende Lemma lässt sich mit Standardargumenten der Linearen Algebra beweisen. Deshalb lassen wir den Beweis weg.

Lemma 4.2. *Sei G eine endliche Gruppe. Seien V, W zwei endlich erzeugte $k[G]$-Moduln und $\varphi : V \to W$ ein Homomorphismus von $k[G]$-Moduln. Dann ist die duale Abbildung $\varphi^* : W^* \to V^*$ definiert durch*

$$\varphi^*(w^*) = w^* \circ \varphi \text{ für } w^* \in W^*$$

ein Homomorphismus von $k[G]$-Moduln. Es gilt

(i) Es seien $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_m)$ Basen von V beziehungsweise W über k. Die zugehörigen Dualbasen von V^* beziehungsweise W^* über k seien $(v_1^*, \ldots, v_n^*)$ und $(w_1^*, \ldots, w_m^*)$. Ist A die Matrixdarstellung von φ bezüglich $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_m)$, so ist A^T die Matrixdarstellung von φ^* bezüglich den Dualbasen $(w_1^*, \ldots, w_m^*)$ und $(v_1^*, \ldots, v_n^*)$.

(ii) φ ist injektiv genau dann, wenn φ^* surjektiv ist.

(iii) φ ist surjektiv genau dann, wenn φ^* injektiv ist.

Satz 4.3. *Sei G eine endliche zyklische Gruppe und $d \in \mathbb{N}$. Dann sind für einen endlichen $k[G]$-Modul V die folgenden Aussagen äquivalent:*

(i) Es gibt einen injektiven Homomorphismus $V \hookrightarrow k[G]^{\oplus d}$ von $k[G]$-Moduln.

(ii) Es gibt einen surjektiven Homomorphismus $\left(k[G]^{\oplus d}\right)^* \twoheadrightarrow V^*$ von $k[G]$-Moduln.

(iii) V^* wird von d Elementen erzeugt.

(iv) V wird von d Elementen erzeugt.

Beweis. (i) $\iff$ (ii): Zu jedem Homomorphismus $i : V \to k[G]^{\oplus d}$ von $k[G]$-Moduln erhält man den dualen Homomorphismus $i^* : (k[G]^{\oplus d})^* \to V^*$ wie in Lemma 4.2. Umgekehrt gibt es zu jedem Homomorphismus $i^* : (k[G]^{\oplus d})^* \to V^*$ von $k[G]$-Moduln einen eindeutigen Homomorphismus $i : V \to k[G]^{\oplus d}$ von $k[G]$-Moduln, so dass i^* der duale Homomorphismus von i ist. Damit folgt die Äquivalenz von (i) und (ii) aus Lemma 4.2 (ii).

(ii) $\iff$ (iii): Da $k[G]^{\oplus d}$ frei ist, gilt $k[G]^{\oplus d} \cong \left(k[G]^{\oplus d}\right)^*$. Dies impliziert die Äquivalenz von (ii) und (iii).

(iii) $\iff$ (iv): Sei γ ein Erzeuger von G. Seien φ und φ^* die Elemente von $\mathrm{GL}(V)$ beziehungsweise von $\mathrm{GL}(V^*)$ welche durch $\varphi(v) = \gamma v$ für $v \in V$ und $\varphi^*(v^*) = \gamma^{-1} v^*$ für $v^* \in V^*$ gegeben sind. Für $v \in V$ und $v^* \in V^*$ gilt

$$(\varphi^* v^*)(v) = (\gamma^{-1} v^*)(v) = v^*(\gamma v) = v^*(\varphi(v)).$$

Also ist φ^* die zu φ duale Abbildung.

Da γ ein Erzeuger von G ist, folgt aus der Normalformentheorie für Endomorphismen von endlichdimensionalen Vektorräumen, dass die kleinste Anzahl von Elementen, die V als $k[G]$-Modul erzeugen, die Anzahl der Blöcke in der Jordannormalform von φ ist. Das Gleiche gilt für V^* mit dem Erzeuger γ^{-1}

von G und der Abbildung φ^*. Es sei A die Matrix von φ bezüglich einer Basis von V. Dann ist gemäss Lemma 4.2 A^T die Darstellung von A^* bezüglich der zugehörigen Dualbasis. Da A und A^T ähnlich sind, haben sie die gleiche Jordannormalform. Dies impliziert (iii) $\iff$ (iv). $\square$

Bemerkung 4.4. *Die Äquivalenz von (iii) und (iv) in Satz 4.3 gilt im Allgemeinen nicht, wenn G nicht zyklisch ist.*

Man betrachte zum Beispiel die Gruppe

$$G = \left\{ \left. \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \right| a, b \in \mathbb{R} \right\} \subset \mathrm{GL}_3(\mathbb{R}).$$

Sie operiert auf kanonische Weise auf dem $\mathbb{R}$-Vektorraum $\mathbb{R}^3$.

Es sei $V = \mathbb{R}[G] \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$. Dann ist für alle $a, b \in \mathbb{R}$

$$\begin{bmatrix} a \\ b \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \in V.$$

Da V ein Vektorraum ist, folgt $V = \mathbb{R}^3$. Also wird $\mathbb{R}^3$ als $\mathbb{R}[G]$-Modul von einem Element erzeugt.

Mit der kontragredienten Darstellung operiert G auf $(\mathbb{R}^3)^*$ wie

$$G^T = \left\{ \left. \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{bmatrix} \right| a, b \in \mathbb{R} \right\}$$

auf dem $\mathbb{R}^3$. Es sei $v = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \mathbb{R}^3$ und $W = \mathbb{R}[G^T]v$. Für $a, b \in \mathbb{R}$ gilt

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ y \\ ax + by + z \end{bmatrix}.$$

Daraus folgt, dass für alle $\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} \in W$ gilt $\frac{x'}{y'} = \frac{x}{y}$. Deshalb kann W nicht der ganze $\mathbb{R}^3$ sein. Also wird $(\mathbb{R}^3)^*$ über $\mathbb{R}[G]$ nicht von einem Element erzeugt. Deshalb ist die Äquivalenz von (iii) und (iv) in diesem Fall nicht erfüllt.

Sei nun ℓ/k eine endliche Galoiserweiterung. Die Galoisgruppe $\mathrm{Gal}(\ell/k)$ operiert k-linear auf ℓ. Dadurch wird ℓ zum $k[\mathrm{Gal}(\ell/k)]$-Modul. Da ℓ/k galois ist, können wir die Struktur dieses Moduls bestimmen:

Lemma 4.5. *Sei ℓ/k eine endliche Galoiserweiterung. Dann sind $k[\mathrm{Gal}(\ell/k)]$ und ℓ als $k[\mathrm{Gal}(\ell/k)]$-Moduln isomorph, das heisst ℓ ist ein freier $k[\mathrm{Gal}(\ell/k)]$-Modul vom Rang 1.*

Beweis. Da ℓ/k eine endliche Galoiserweiterung ist, gibt es eine Normalbasis von ℓ über k, das heisst es gibt ein Element y aus ℓ für welches $(\sigma(y))_{\sigma \in \mathrm{Gal}(\ell/k)}$

eine Basis von ℓ über k ist. Für ein solches y sei

$$\begin{aligned}\Phi : k[\mathrm{Gal}(\ell/k)] &\to \ell \\ \sum_{\sigma\in\mathrm{Gal}(\ell/k)} x_\sigma[\sigma] &\mapsto \sum_{\sigma\in\mathrm{Gal}(\ell/k)} x_\sigma\sigma(y).\end{aligned}$$

Da $(\sigma(y))_{\sigma\in\mathrm{Gal}(\ell/k)}$ eine Basis ist, ist diese Abbildung bijektiv. Aus der Definition von Φ folgt, dass Φ sowohl k-linear als auch $\mathrm{Gal}(\ell/k)$-äquivariant ist. Also folgt aus Lemma 4.1, dass Φ ein Isomorphismus von $k[\mathrm{Gal}(\ell/k)]$-Moduln ist. □

Lemma 4.6. *Es seien $\ell/k/f$ ein Turm von Körpererweiterungen, so dass ℓ/k eine endliche Galoiserweiterung ist und k/f Grad d hat. Dann ist ℓ ein freier Modul von Grad d über $f[\mathrm{Gal}(\ell/k)]$.*

Beweis. Wegen Lemma 4.5 ist ℓ als $k[\mathrm{Gal}(\ell/k)]$-Modul isomorph zu $k[\mathrm{Gal}(\ell/k)]$, also sind diese Moduln auch als $f[\mathrm{Gal}(\ell/k)]$-Moduln isomorph.

Deshalb genügt es zu zeigen, dass $k[\mathrm{Gal}(\ell/k)]$ frei vom Grad d über dem Ring $f[\mathrm{Gal}(\ell/k)]$ ist. Dies folgt aus der Tatsache, dass k frei vom Grad d über f ist: Sei $(v_1,\dots,v_d)$ eine Basis von k über f und e das Einselement in $\mathrm{Gal}(\ell/k)$. Dann folgt die Behauptung aus

Behauptung 1. *Das Tupel $(v_1[e],\dots,v_d[e])$ ist eine Basis von $k[\mathrm{Gal}(\ell/k)]$ über $f[\mathrm{Gal}(\ell/k)]$.*

Da für $x_\sigma \in k$ mit $x_\sigma = \sum_{k=1}^d a_k^\sigma v_k$ für $a_k^\sigma \in f$ gilt

$$\sum_{\sigma\in\mathrm{Gal}(\ell/k)} x_\sigma[\sigma] = \sum_{\sigma\in\mathrm{Gal}(\ell/k)} \left(\sum_{k=1}^d a_k^\sigma v_k\right)[\sigma] = \sum_{k=1}^d \left(\sum_{\sigma\in\mathrm{Gal}(\ell/k)} a_k^\sigma[\sigma]\right) v_k[e],$$

ist $(v_1[e],\dots,v_d[e])$ ein Erzeugendensystem von $k[\mathrm{Gal}(\ell/k)]$ über $f[\mathrm{Gal}(\ell/k)]$. Da $(v_1,\dots,v_d)$ über f linear unabhängig ist, ist $(v_1[e],\dots,v_d[e])$ über f linear unabhängig, also auch über $f[\mathrm{Gal}(\ell/k)]$. □

5 Der Fall einer endlichen Körpererweiterung von $\mathbb{F}_q$

Wir untersuchen nun die Frage, welche Untergruppen der $\mathrm{GL}_n(\mathbb{F}_q)$ sich als Galoisgruppe eines $\mathbb{F}_q$-linearen Polynoms f über einer endlichen Körpererweiterung k von $\mathbb{F}_q$ realisieren lassen. Der Zerfällungskörper ℓ ist dann eine endliche Erweiterung von k. Da für solche Erweiterungen die Galoisgruppe $\mathrm{Gal}(\ell/k)$ zyklisch ist, lassen sich nur zyklische Untergruppen der $\mathrm{GL}_n(\mathbb{F}_q)$ realisieren. Wir zeigen nun, dass es für jedes $A \in \mathrm{GL}_n(\mathbb{F}_q)$ eine endliche Körpererweiterung k von $\mathbb{F}_q$ und ein $\mathbb{F}_q$-lineares Polynom $f \in k[X]$ gibt, dessen Galoisgruppe bis auf Konjugation die von A erzeugte zyklische Gruppe ist. Der folgende Satz und sein Beweis stammen von Pink.

Satz 5.1. *Sei $A \in \mathrm{GL}_n(\mathbb{F}_q)$ für ein $n \in \mathbb{N}$. Sei d_0 die minimale Anzahl von Erzeugern des $\mathbb{F}_q[\langle A \rangle]$-Moduls $\mathbb{F}_q^n$. Dann gibt es für jede endliche Körpererweiterung k von $\mathbb{F}_q$ mit $[k : \mathbb{F}_q] \geq d_0$ ein separables und $\mathbb{F}_q$-lineares Polynom $f \in k[X]$ für welches gilt: Das Bild des Frobeniusautomorphismus unter der Einbettung $\mathrm{Gal}(f) \hookrightarrow \mathrm{GL}_n(\mathbb{F}_q)$ ist bis auf Konjugation A.*

Beweis. Sei $d \geq d_0$ und k eine Körpererweiterung von $\mathbb{F}_q$ vom Grad d, das heisst $k = \mathbb{F}_{q^d}$ ist ein Körper mit q^d Elementen. Sei $m \in \mathbb{N}$ die Ordnung von A in $\mathrm{GL}_n(\mathbb{F}_q)$. Dann gibt es einen Turm $\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d}/\mathbb{F}_q$ von endlichen Körpern. Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})$ ist zyklisch mit Ordnung m und wird vom Frobeniusautomorphismus $\tau : x \mapsto x^{q^d}$ erzeugt. Die Zuweisung $A \mapsto \tau$ induziert einen Isomorphismus zwischen $\langle A \rangle$ und $\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})$ und wir identifizieren diese beiden Gruppen über diesen Isomorphismus. Dann ist $\mathbb{F}_q^n$ ein $\mathbb{F}_q[\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})]$-Modul.

Aus Satz 4.3 folgt die Existenz einer Einbettung $\mathbb{F}_q^n \hookrightarrow \mathbb{F}_q[\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})]^{\oplus d}$. Aus Lemma 4.6 folgt die Existenz eines Isomorphismus $\mathbb{F}_q[\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})]^{\oplus d} \to \mathbb{F}_{q^{md}}$ von $\mathbb{F}_q[\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})]$-Moduln. Daraus erhalten wir eine Einbettung $\mathbb{F}_q^n \hookrightarrow \mathbb{F}_{q^{md}}$, das heisst es gibt einen $\mathbb{F}_q$-Vektorraum $V \subset \mathbb{F}_{q^{md}}$ und einen Isomorphismus $\Phi : \mathbb{F}_q^n \to V$ von $\mathbb{F}_q[\mathrm{Gal}(\mathbb{F}_{q^{md}}/\mathbb{F}_{q^d})]$-Moduln. Aus Lemma 3.3 folgt, dass $f(X) := \prod_{v \in V}(X - v) \in \mathbb{F}_{q^{md}}[X]$ ein $\mathbb{F}_q$-lineares Polynom ist. Da V unter τ invariant ist, sind auch die Koeffizienten von f unter τ invariant. Deshalb liegt f in $\mathbb{F}_{q^d}[X]$.

Wir betten $\mathrm{Gal}(f)$ mittels Φ in $\mathrm{GL}_n(\mathbb{F}_q)$ ein: Sei

$$\begin{aligned} \Psi : \mathrm{Gal}(f) &\to \mathrm{GL}_n(\mathbb{F}_q) \\ \sigma &\mapsto \Phi^{-1} \circ \sigma \circ \Phi. \end{aligned}$$

Dann folgt für $x \in \mathbb{F}_q^n$

$$\Psi(\tau)(x) = \Phi^{-1}(\tau(\Phi(x))) = \Phi^{-1}(\Phi(A(x))) = A(x),$$

da Φ ein Modulisomorphismus ist. Also ist $\Psi(\tau) = A$. □

6 Verhalten der Galoisgruppe bei Koeffizientenreduktion

In diesem Abschnitt untersuchen wir das Verhalten der Galoisgruppe eines $\mathbb{F}_q$-linearen Polynoms mit Koeffizienten in einem Ring, wenn diese Koeffizienten modulo ein Primideal reduziert werden. Wir werden zeigen, dass die Galoisgruppe des reduzierten Polynoms bis auf Konjugation eine Untergruppe der Galoisgruppe des ursprünglichen Polynoms ist. Der hier dargestellte Beweis ist eine Abwandlung des Beweises der analogen Aussage über allgemeine Polynome, der im Buch “Algebra 1” von B. L. van der Waerden gegeben wird ([2], Paragraph 66).

Es sei R ein faktorieller Ring, das heisst ein Integritätsbereich mit eindeutiger Primfaktorzerlegung, und K der Quotientenkörper von R. Für ein Polynom $f \in R[T]$ sei $I(f)$ der grösste gemeinsame Teiler der Koeffizienten von f. Das Lemma von Gauss besagt $I(fg) = I(f)I(g)$ für Polynome $f, g \in R[T]$.

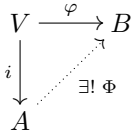
Lemma 6.1. *Es seien $h \in R[T]$ und $f, g \in K[T]$ mit $I(h) = 1$ und $h = fg$. Dann gilt $f, g \in R[T]$.*

Beweis. Da K der Quotientenkörper von R ist, gibt es $a, b \in R$, so dass $af, bg \in R[T]$. Man kann a, b so wählen, dass gilt $I(af) = I(bg) = 1$. Dann gilt $ab = I(abh) = I(abfg) = I(af)I(bg) = 1$. Also sind a und b Einheiten, daraus folgt die Behauptung. □

Im folgenden bezeichnen wir eine kommutative, assoziative und unitäre $\mathbb{F}_q$-Algebra einfach als Algebra.

Definition 6.2. *Es sei V ein $\mathbb{F}_q$-Vektorraum. Die symmetrische Algebra $\mathrm{S}(V)$ über V ist ein Paar (A, i) bestehend aus einer Algebra A und einer linearen Abbildung $i : V \to A$, welches die folgende universelle Eigenschaft besitzt:*

Zu jeder linearen Abbildung $\varphi : V \to B$ von V in eine Algebra B gibt es einen eindeutigen Algebrahomomorphismus $\Phi : A \to B$ mit $\Phi \circ i = \varphi$.



Durch diese universelle Eigenschaft wird $\mathrm{S}(V)$ bis auf eindeutige Isomorphie charakterisiert, und man kann zeigen, dass $\mathrm{S}(V)$ für jedes V existiert. Für einen endlichdimensionalen $\mathbb{F}_q$-Vektorraum V kann man $\mathrm{S}(V)$ wie folgt konstruieren:

Lemma 6.3. *Sei V ein $\mathbb{F}_q$-Vektorraum mit Basis $(v_1, \ldots, v_n)$. Wir betrachen $v_1, \ldots, v_n$ als Variablen über $\mathbb{F}_q$. Es sei $i : V \to \mathbb{F}_q[v_1, \ldots, v_n]$ die durch $v_i \mapsto v_i$ für $1 \leq i \leq n$ eindeutig definierte lineare Abbildung. Dann ist $\mathrm{S}(V) = (\mathbb{F}_q[v_1, \ldots, v_n], i)$.*

Beweis. Es sei B eine Algebra und $\varphi : V \to B$ linear. Es sei $\Phi : \mathbb{F}_q[v_1, \ldots, v_n] \to B$ die Abbildung, die man aus $\Phi|_{\mathbb{F}_q} = \mathrm{id}$ und $\Phi(v_1^{k_1} \cdots v_n^{k_n}) = \varphi(v_1)^{k_1} \cdots \varphi(v_n)^{k_n}$ durch $\mathbb{F}_q$-lineare Fortsetzung erhält. Dann gilt $\Phi \circ i = \varphi$, und Φ ist durch diese Eigenschaft eindeutig bestimmt. Man prüft leicht nach, dass Φ ein Algebrahomomorphismus ist. □

Aus der universellen Eigenschaft von $\mathrm{S}(V) = (A, i)$ folgt, dass i injektiv sein muss. Daher lassen wir im Folgenden den Homomorphismus i weg und fassen stattdessen V einfach als Untervektorraum von $\mathrm{S}(V)$ auf.

Sei V ein Vektorraum und $\sigma \in \mathrm{GL}(V)$. Aus der universellen Eigenschaft von $\mathrm{S}(V)$ erhalten wir einen eindeutigen Algebraisomorphismus $\rho(\sigma) : \mathrm{S}(V) \to \mathrm{S}(V)$, für den gilt $\rho(\sigma)|_V = \sigma$. Aus der Eindeutigkeitsaussage in der universellen Eigenschaft folgt, dass $\rho(id_V) = id_{\mathrm{S}(V)}$ ist und dass für $\sigma, \tau \in \mathrm{GL}(V)$ gilt $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$. Die $\mathrm{GL}(V)$ operiert also mittels ρ von links auf $\mathrm{S}(V)$.

Definition 6.4. *Es sei* $\mathrm{S}(V)^{\mathrm{GL}(V)}$ *die Menge der Elemente von* $\mathrm{S}(V)$*, die unter dieser Operation der* $\mathrm{GL}(V)$ *invariant sind.*

Die Menge $\mathrm{S}(V)^{\mathrm{GL}(V)}$ ist eine Unteralgebra von $\mathrm{S}(V)$. Für einen endlichdimensionalen Vektorraum V lässt sie sich wie folgt bestimmen:

Satz 6.5 (Dickson). *Für einen Vektorraum* V *der Dimension* n *sei*

$$f(X) = \prod_{v \in V} (X - v) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} c_i X^{q^i} \in \mathrm{S}(V)[X].$$

Die $c_i \in \mathrm{S}(V)$ *werden die* Dickson-Invarianten *von* V *genannt. Sie sind algebraisch unabhängig und es gilt*

$$\mathrm{S}(V)^{\mathrm{GL}(V)} = \mathbb{F}_q[c_0, \ldots, c_{n-1}].$$

Beweis. Siehe [3]. □

Es sei nun K eine Körpererweiterung von $\mathbb{F}_q$ und $R \subset K$ ein faktorieller Ring mit Quotientenkörper K. Weiter sei $f(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} a_i X^{q^i} \in R[X]$ ein separables $\mathbb{F}_q$-lineares Polynom mit Kern V in einem algebraischen Abschluss $\bar{K}$ von K. Es sei $L \subset \bar{K}$ der Zerfällungskörper von f in $\bar{K}$.

Für jedes $v \in V \setminus \{0\}$ führen wir eine neue Variable U_v ein. Wir definieren nun eine Aktion der $\mathrm{GL}_n(\mathbb{F}_q)$ von links auf dem Polynomring $L[T, (U_v)_{v \in V \setminus \{0\}}]$. Um Verwirrung mit der Aktion der Galoisgruppe von f zu vermeiden, schreiben wir diese Aktion als $(\sigma, x) \mapsto {}^{\sigma}x$. Sie sei definiert durch ${}^{\sigma}U_v = U_{\sigma(v)}$ für alle $v \in V \setminus \{0\}$, wobei L und T festgelassen werden.

Für eine Menge M sei $\mathscr{S}_M$ die symmetrische Gruppe auf M. Wie in Satz 6.5 seien $c_0, \ldots, c_{n-1}$ die Dickson-Invarianten von V.

Wir betrachten nun die Polynome

$$G = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{V \setminus \{0\}} \sigma(v) U_v \right) \in \mathrm{S}(V)[T, (U_v)_{v \in V \setminus \{0\}}],$$

$$g = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{v \in V \setminus \{0\}} \sigma(v) U_v \right) \in L[T, (U_v)_{v \in V \setminus \{0\}}]$$

und

$$g_\tau = \prod_{\sigma \in \mathrm{Gal}(f)} \left(T - \sum_{v \in V \setminus \{0\}} \sigma(\tau(v)) U_v \right) \in L[T, (U_v)_{v \in V \setminus \{0\}}]$$

für $\tau \in \mathrm{GL}(V)$.

Die Inklusion $V \hookrightarrow L$ lässt sich eindeutig zu einem Algebrahomomorphismus $\Theta : \mathrm{S}(V) \to L$ fortsetzen. Wir setzen Θ mittels $\Theta(T) = T$ und $\Theta(U_v) = U_v$ für alle $v \in V \setminus \{0\}$ zu einem Homomorphismus

$$\Theta : \mathrm{S}(V)[T, (U_v)_{v \in V \setminus \{0\}}] \to L[T, (U_v)_{v \in V \setminus \{0\}}]$$

fort. Aus der Definition von G und g folgt, dass gilt $\Theta(G) = g$.

Lemma 6.6. *Es gilt:*

(i) $G \in \mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v \in V \setminus \{0\}}]$.

(ii) $\Theta(c_i) = a_i$ *für alle* $0 \leq i \leq n-1$.

(iii) $\Theta(\mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v \in V \setminus \{0\}}]) \subset R[T, (U_v)_{v \in V \setminus \{0\}}]$.

(iv) $g \in R[T, (U_v)_{v \in V \setminus \{0\}}]$.

Beweis. (i) Wir setzen die Aktion der $\mathrm{GL}(V)$ auf $\mathrm{S}(V)$ mittels $\sigma T = T$ und $\sigma U_v = U_v$ für alle $\sigma \in \mathrm{GL}(V)$ und alle $v \in V \setminus \{0\}$ auf $\mathrm{S}(V)[T, (U_v)_{v \in V \setminus \{0\}}]$ fort. Dann gilt für alle $\tau \in \mathrm{GL}(V)$

$$\tau G = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{V \setminus \{0\}} \tau(\sigma(v)) U_v \right) = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{V \setminus \{0\}} \sigma(v) U_v \right) = G.$$

Also liegen die Koeffizienten von H in $\mathrm{S}(V)^{\mathrm{GL}(V)}$. Aus Satz 6.5 folgt damit die Behauptung.

(ii)Es gilt in $L[X]$

$$X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} \Theta(c_i) X^{q^i} = \Theta\Big(\prod_{v \in V} (X - v)\Big)$$

$$= \prod_{v \in V} (X - \Theta(v)) = \prod_{v \in V} (X - v) = f(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} a_i X^{q^i}.$$

Daraus folgt $\Theta(c_i) = a_i$ für alle $0 \leq i \leq n-1$.

(iii) Dies folgt aus (ii), da die a_i in R liegen.

(iv) Es gilt $\Theta(G) = g$. Aus (i) und (iii) folgt damit $g \in R[T, (U_v)_{v \in V \setminus \{0\}}]$.$\square$

Für eine Gruppe G, die auf einer Menge M operiert, bezeichne $\mathrm{Stab}_G(x)$ den Stabilisator von $x \in M$.

Lemma 6.7. *Es gilt:*

(i) $g = \prod_{[\tau] \in \mathrm{Gal}(f) \setminus \mathrm{GL}(V)} g_\tau$.

(ii) Für alle $\tau \in \mathrm{GL}(V)$ *ist* $g_\tau \in R[T, (U_v)_{v \in V \setminus \{0\}}]$.

(iii) Die g_τ *sind irreduzibel über* K.

(iv) Für alle $\tau \in \mathrm{GL}(V)$ *ist* $\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(g_\tau) = \tau^{-1}\,\mathrm{Gal}(f)\tau$.

Beweis. (i) Diese Darstellung folgt direkt aus der Definition von g und der g_τ.

(ii) Da die Koeffizienten von g_τ invariant unter allen $\sigma \in \mathrm{Gal}(f)$ sind, ist $g_\tau \in K[T, (U_v)_{v\in V\setminus\{0\}}]$. Da $g, g_\tau \in K((U_v)_{v\in V\setminus\{0\}})[T]$ normiert sind mit $g_\tau | g$ folgt deshalb (ii) aus Lemma 6.1 angewandt auf den faktoriellen Ring $R[(U_v)_{v\in V\setminus\{0\}}]$ und seinen Quotientenkörper $K((U_v)_{v\in V\setminus\{0\}})$.

(iii) Wir setzen die natürliche Aktion von $\mathrm{Gal}(f)$ von L auf $L[T, (U_v)_{v\in V\setminus\{0\}}]$ fort, indem die Variablen festgelassen werden. Es sei $r \in K[T, (U_v)_{v\in V\setminus\{0\}}]$ der irreduzible Faktor von g, welcher über L den Faktor $T - \sum_{v\in V\setminus\{0\}} \tau(v)U_v$ enthält. Für alle $\sigma \in \mathrm{Gal}(f)$ gilt dann

$$T - \sum_{v\in V\setminus\{0\}} \sigma(\tau(v))U_v = \sigma\left(T - \sum_{v\in V\setminus\{0\}} \tau(v)U_v\right) \;\Big|\; \sigma(r) = r.$$

Da die Faktoren $T - \sum_{v\in V\setminus\{0\}} \sigma(\tau(v))U_v$ paarweise verschieden sind, gilt also $g_\tau | r$. Aus $g_\tau \in K[T, (U_v)_{v\in V\setminus\{0\}}]$ folgt $g_\tau = r$. Also ist g_τ irreduzibel.

(iv) Für alle $\rho, \tau \in \mathrm{GL}(V)$ gilt

$$\begin{aligned} {}^\rho g_\tau &= \prod_{\sigma\in\mathrm{Gal}(f)} \left(T - \sum_{v\in V\setminus\{0\}} \sigma(\tau(v))U_{\rho(v)}\right) \\ &= \prod_{\sigma\in\mathrm{Gal}(f)} \left(T - \sum_{v\in V\setminus\{0\}} \sigma(\tau(\rho^{-1}(v)))U_v\right) = g_{\tau\rho^{-1}} \end{aligned}$$

Für $\tau, \tau' \in \mathrm{GL}(V)$ gilt

$$g_\tau = g_{\tau'} \iff \mathrm{Gal}(f)\tau = \mathrm{Gal}(f)\tau' \iff \tau'\tau^{-1} \in \mathrm{Gal}(f).$$

Daraus folgt für alle $\rho, \tau \in \mathrm{GL}(V)$

$${}^\rho g_\tau = g_\tau \iff g_{\tau\rho^{-1}} = g_\tau \iff \tau\rho\tau^{-1} \in \mathrm{Gal}(f) \iff \rho \in \tau^{-1}\,\mathrm{Gal}(f)\tau. \quad \square$$

Satz 6.8. *Sei* R *eine faktorielle* $\mathbb{F}_q$*-Algebra mit Quotientenkörper* K*. Sei* $\mathfrak{p}$ *ein maximales Ideal von* R *mit Restklassenkörper* $k = R/\mathfrak{p} \supset \mathbb{F}_q$*. Sei* $f \in R[X]$ *ein separables* $\mathbb{F}_q$*-lineares Polynom der Form* $f(X) = X^{q^n} + \sum_{i=0}^{n-1} (-1)^{n-i} a_i X^{q^i}$ *mit* $a_0 \notin \mathfrak{p}$*. Sei* $\bar{f} = f \bmod \mathfrak{p}$*. Betrachtet man* $\mathrm{Gal}(f)$ *und* $\mathrm{Gal}(\bar{f})$ *als Untergruppen der* $\mathrm{GL}_n(\mathbb{F}_q)$*, so enthält* $\mathrm{Gal}(f)$ *ein Konjugiertes von* $\mathrm{Gal}(\bar{f})$*.*

Beweis. Aus $a_0 \notin \mathfrak{p}$ folgt $a_0 \bmod \mathfrak{p} \neq 0$, also ist $\bar{f}$ separabel. Es sei $V = \ker(f)$ und $\bar{V} = \ker(\bar{f})$. Da f normiert ist, ist auch $\bar{f}$ normiert, also hat $\bar{f}$ Grad q^n. Deshalb ist $n = \dim V = \dim \bar{V}$. Dann erhalten wir mit Lemma 6.6 die folgenden

Polynome:

$$g = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{v \in V \setminus \{0\}} \sigma(v) U_v \right) \in R[T, (U_v)_{v \in V \setminus \{0\}}]$$

$$\bar{g} = \prod_{\sigma \in \mathrm{GL}(\bar{V})} \left(T - \sum_{\bar{v} \in \bar{V} \setminus \{0\}} \sigma(\bar{v}) U_{\bar{v}} \right) \in k[T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}]$$

Wir wählen einen Isomorphismus $\Phi : V \to \bar{V}$. Wir definieren den Homomorphismus

$$\pi : R[T, (U_v)_{v \in V \setminus \{0\}}] \to k[T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}]$$

mittels $\pi(x) = x \bmod \mathfrak{p}$ für alle $x \in R$ und $\pi(U_v) = U_{\Phi(v)}$ für alle $v \in V \setminus \{0\}$ und $\pi(T) = T$. Dann gilt

Behauptung 1. $\pi(g) = \bar{g}$.

Beweis. Es seien $c_0, \ldots, c_{n-1}$ die Dickson-Invarianten von V und $\bar{c}_0, \ldots, \bar{c}_{n-1}$ die Dickson-Invarianten von $\bar{V}$. Mit Lemma 6.6 erhalten wir die Polynome

$$G = \prod_{\sigma \in \mathrm{GL}(V)} \left(T - \sum_{v \in V \setminus \{0\}} \sigma(v) U_v \right) \in \mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v \in V \setminus \{0\}}]$$

und

$$\bar{G} = \prod_{\sigma \in \mathrm{GL}(\bar{V})} \left(T - \sum_{\bar{v} \in \bar{V} \setminus \{0\}} \sigma(\bar{v}) U_{\bar{v}} \right) \in \mathbb{F}_q[\bar{c}_0, \ldots, \bar{c}_{n-1}][T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}].$$

Wir definieren den Isomorphismus

$$\Psi : \mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v \in V \setminus \{0\}}] \to \mathbb{F}_q[\bar{c}_0, \ldots, \bar{c}_{n-1}][T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}]$$

mittels $\Psi(c_i) = \bar{c}_i$ für alle $0 \leq i \leq n-1$, $\Psi(U_v) = U_{\Phi(v)}$ für alle $v \in V \setminus \{0\}$ und $\Psi(T) = T$. Mit Lemma 6.6 erhalten wir Abbildungen

$$\Theta : \mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v \in V \setminus \{0\}}] \to R[T, (U_v)_{v \in V \setminus \{0\}}]$$

und

$$\bar{\Theta} : \mathbb{F}_q[\bar{c}_0, \ldots, \bar{c}_{n-1}][T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}] \to k[T, (U_{\bar{v}})_{\bar{v} \in \bar{V} \setminus \{0\}}]$$

für die gilt $\Theta(G) = g$ und $\bar{\Theta}(\bar{G}) = \bar{g}$.

Wir erhalten also das folgende Diagramm:

$$\begin{array}{ccc} \mathbb{F}_q[c_0,\ldots,c_{n-1}][T,(U_v)_{v\in V\setminus\{0\}}] & \xrightarrow{\Theta} & R[T,(U_v)_{v\in V\setminus\{0\}}] \\ \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{F}_q[\bar{c}_0,\ldots,\bar{c}_{n-1}][T,(U_{\bar{v}})_{\bar{v}\in \bar{V}\setminus\{0\}}] & \xrightarrow{\bar{\Theta}} & k[T,(U_{\bar{v}})_{\bar{v}\in \bar{V}\setminus\{0\}}] \end{array}$$

Es gilt nun

Behauptung 2.

(i) Das Diagramm ist kommutativ.

(ii) $\Psi(G) = \bar{G}$.

Aus Behauptung 2 folgt direkt Behauptung 1:

$$\pi(g) = \pi(\Theta(G)) = \bar{\Theta}(\Psi(G)) = \bar{\Theta}(\bar{G}) = \bar{g}.$$

Wir beweisen noch die Behauptung 2:

(i) Aus Lemma 6.6 folgt:

$$\begin{array}{ll} \Theta(c_i) = a_i & \text{für alle } 0 \le i \le n-1 \\ \bar{\Theta}(\bar{c}_i) = a_i \bmod \mathfrak{p} & \text{für alle } 0 \le i \le n-1 \end{array}$$

Daraus folgt für alle $0 \le i \le n-1$

$$\pi(\Theta(c_i)) = \pi(a_i) = a_i \bmod \mathfrak{p} = \bar{\Theta}(\bar{c}_i) = \bar{\Theta}(\Psi(c_i)).$$

Ausserdem gilt

$$\pi(\Theta(T)) = \pi(T) = T = \bar{\Theta}(T) = \bar{\Theta}(\Psi(T))$$

und

$$\pi(\Theta(U_v)) = \pi(U_v) = U_{\Phi(v)} = \bar{\Theta}(U_{\Phi(v)}) = \bar{\Theta}(\Psi(U_v)).$$

Daraus folgt $\pi \circ \Theta = \bar{\Theta} \circ \Psi$, das heisst das Diagramm kommutiert.

(ii)Aufgrund der universellen Eigenschaft von $\mathrm{S}(V)$ induziert Φ einen eindeutigen Isomorphismus $\tilde{\Phi} : \mathrm{S}(V) \to \mathrm{S}(\bar{V})$ für den gilt $\tilde{\Phi}|_V = \Phi$. Wir setzen $\tilde{\Phi}$ mittels $\tilde{\Phi}(T) = T$ und $\tilde{\Phi}(U_v) = U_{\Phi(v)}$ zu einem Isomorphismus

$$\tilde{\Phi} : \mathrm{S}(V)[T,(U_v)_{v\in V\setminus\{0\}}] \to \mathrm{S}(\bar{V})[T,(U_{\bar{v}})_{\bar{v}\in \bar{V}\setminus\{0\}}]$$

fort.

In $\mathrm{S}(V)[X]$ gilt

$$\prod_{v\in V}(X-v) = X^{q^n} + \sum_{i=0}^{n-1}(-1)^{n-i}c_i X^{q^i}.$$

Wir setzen $\tilde{\Phi}$ mittels $\tilde{\Phi}(X) = X$ zu einem Isomorphismus $\tilde{\Phi} : \mathrm{S}(V)[X] \to \mathrm{S}(\bar{V})[X]$ fort. Dann gilt

$$X^{q^n} + \sum_{i=0}^{n-1}(-1)^{n-i}\tilde{\Phi}(c_i)X^{q^i} = \tilde{\Phi}(\prod_{v\in V}(X-v)) = \prod_{v\in V}(X-\tilde{\Phi}(v))$$
$$= \prod_{\bar{v}\in\bar{V}}(X-\bar{v}) = X^{q^n} + \sum_{i=0}^{n-1}(-1)^{n-i}\bar{c}_i X^{q^i}.$$

Durch Koeffizientenvergleich folgt aus dieser Gleichung, dass für alle $0 \leq i \leq n-1$ gilt $\tilde{\Phi}(c_i) = \bar{c}_i$. Deshalb ist die Einschränkung von $\tilde{\Phi}$ auf die Unteralgebra $\mathbb{F}_q[c_0, \ldots, c_{n-1}][T, (U_v)_{v\in V\setminus\{0\}}]$ gerade Ψ. Damit folgt nun (ii):

$$\begin{aligned}\Psi(G) = \tilde{\Phi}(G) &= \prod_{\sigma\in\mathrm{GL}(V)}\left(T - \sum_{v\in V\setminus\{0\}}\Phi(\sigma(v))U_{\Phi(v)}\right)\\ &= \prod_{\sigma\in\mathrm{GL}(V)}\left(T - \sum_{\bar{v}\in\bar{V}\setminus\{0\}}\Phi(\sigma(\Phi^{-1}(\bar{v})))U_{\bar{v}}\right)\\ &= \prod_{\sigma\in\mathrm{GL}(\bar{V})}\left(T - \sum_{\bar{v}\in\bar{V}\setminus\{0\}}\sigma(v)U_{\bar{v}}\right) = \bar{G}\end{aligned}$$

Damit ist Behauptung 2, also auch Behauptung 1, bewiesen. □

Aus Lemma 6.7 erhalten wir

$$g = \prod_{[\tau]\in\mathrm{Gal}(f)\setminus\mathrm{GL}(V)} g_\tau$$

und

$$\bar{g} = \prod_{[\tau]\in\mathrm{Gal}(\bar{f})\setminus\mathrm{GL}(\bar{V})} \bar{g}_\tau,$$

wobei für alle $\tau \in \mathrm{GL}(V)$

$$g_\tau = \prod_{\sigma\in\mathrm{Gal}(f)}\left(T - \sum_{v\in V\setminus\{0\}}\sigma(\tau(v))U_v\right)$$

irreduzibel ist und für alle $\tau \in \mathrm{GL}(\bar{V})$

$$\bar{g}_\tau = \prod_{\sigma\in\mathrm{Gal}(\bar{f})}\left(T - \sum_{\bar{v}\in\bar{V}\setminus\{0\}}\sigma(\tau(\bar{v}))U_{\bar{v}}\right)$$

irreduzibel ist.

Aus Behauptung 1 folgt damit

$$\prod_{[\tau]\in \mathrm{Gal}(\bar{f})\backslash \mathrm{GL}(\bar{V})} \bar{g}_\tau = \bar{g} = \pi(g) = \prod_{[\tau]\in \mathrm{Gal}(f)\backslash \mathrm{GL}(V)} \pi(g_\tau). \tag{1}$$

Da die $\bar{g}_\tau$ irreduzibel sind, gibt es ein $\tau \in \mathrm{GL}$ für welches gilt $\bar{g}_\tau | \pi(g_{id})$.

Behauptung 3. $\mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\bar{g}_\tau) \subset \mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\pi(g_{id}))$.

Beweis. Es sei $\sigma \in \mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\bar{g}_\tau)$. Aus $\bar{g}_\tau | \pi(g_{id})$ folgt

$$\bar{g}_\tau = {}^{\sigma}\bar{g}_\tau | {}^{\sigma}\pi(g_{id}).$$

Da für $[\tau], [\tau'] \in \mathrm{Gal}(\bar{f})\backslash \mathrm{GL}(\bar{V})$ mit $[\tau] \neq [\tau']$ gilt $\bar{g}_\tau \neq \bar{g}_{\tau'}$, folgt damit aus (1) ${}^{\sigma}\pi(g_{id}) = \pi(g_{id})$. □

Die Abbildung

$$\begin{aligned} \Gamma : \mathrm{GL}(V) &\to \mathrm{GL}(\bar{V}) \\ \sigma &\mapsto \Phi \circ \sigma \circ \Phi^{-1} \end{aligned}$$

ist ein Gruppenisomorphismus. Für $v \in V \setminus \{0\}$ und $\sigma \in \mathrm{GL}(V)$ gilt

$$\pi({}^{\sigma}U_v) = \pi(U_{\sigma(v)}) = U_{\Phi(\sigma(v))} = U_{\Gamma(\sigma)(\Phi(v))} = {}^{\Gamma(\sigma)}U_{\Phi(v)} = {}^{\Gamma(\sigma)}\pi(U_v).$$

Daraus folgt, dass für alle $h \in R[T, (U_v)_{v\in V\setminus\{0\}}]$ und alle $\sigma \in \mathrm{GL}(V)$ gilt

$$\pi({}^{\sigma}h) = {}^{\Gamma(\sigma)}\pi(h).$$

Behauptung 4. $\mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\pi(g_{id})) \subset \Gamma(\mathrm{Stab}_{\mathrm{GL}(V)}(g_{id}))$.

Beweis. Es sei $\sigma \in \mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\pi(g_{id}))$. Es sei $\tilde{\sigma} = \Gamma^{-1}(\sigma) \in \mathrm{GL}(V)$. Dann folgt

$$\pi(g_{id}) = {}^{\sigma}\pi(g_{id}) = {}^{\Gamma(\tilde{\sigma})}\pi(g_{id}) = \pi({}^{\tilde{\sigma}}g_{id}).$$

Da die $\bar{g}_\rho$ für $[\rho] \in \mathrm{Gal}(\bar{f})\backslash \mathrm{GL}_n(\mathbb{F}_q)$ paarweise verschieden sind, folgt aus (1), dass auch die $\pi(g_\rho)$ paarweise verschieden sind für $[\rho] \in \mathrm{Gal}(f)\backslash \mathrm{GL}_n(\mathbb{F}_q)$. Also ist $g_{id} = {}^{\tilde{\sigma}}g_{id}$, das heisst es gilt $\tilde{\sigma} \in \mathrm{Stab}_{\mathrm{GL}(V)}(g_{id})$. Also liegt $\sigma = \Gamma(\tilde{\sigma})$ in $\Gamma(\mathrm{Stab}_{\mathrm{GL}(V)}(g_{id}))$. □

Insgesamt folgt mit Lemma 6.7 und den Behauptungen 3 und 4

$$\begin{aligned} \tau^{-1}\,\mathrm{Gal}(\bar{f})\tau = \mathrm{Stab}_{\mathrm{GL}(\bar{V})}(\bar{g}_\tau) &\subset \mathrm{Stab}_{\mathrm{GL}(V)}(\pi(g_{id})) \\ &\subset \Gamma(\mathrm{Stab}_{\mathrm{GL}(V)}(g_{id})) = \Gamma(\mathrm{Gal}(f)). \end{aligned}$$

Daraus folgt, dass $\mathrm{Gal}(f)$ ein Konjugiertes von $\mathrm{Gal}(\bar{f})$ enthält, wenn wir $\mathrm{GL}(V)$ und $\mathrm{GL}(\bar{V})$ mittels einer Basisdarstellung mit $\mathrm{GL}_n(\mathbb{F}_q)$ identifizieren. □

7 Konstruktion des Polynoms mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$

Mithilfe von Satz 6.8 können wir erzwingen, dass $\mathrm{Gal}(f)$ gewisse Elemente (bis auf Konjugation) enhält, indem wir die Koeffizienten von f geschickt wählen. Um auf diese Weise $\mathrm{Gal}(f) = \mathrm{GL}_n(\mathbb{F}_q)$ zu erzwingen, benötigen wir eine Teilmenge $\{g_i \mid i \in I\}$ der $\mathrm{GL}_n(\mathbb{F}_q)$ mit der Eigenschaft, dass eine Untergruppe G der $\mathrm{GL}_n(\mathbb{F}_q)$, welche ein Konjugiertes jedes der g_i enhält, notwendigerweise die ganze $\mathrm{GL}_n(\mathbb{F}_q)$ ist. Ein solches Erzeugendensystem nennen wir gut. Ein gutes Erzeugendensystem erhalten wir mithilfe des folgenden Satzes:

Satz 7.1. *Sei G eine endliche Gruppe und H eine Untergruppe mit der Eigenschaft, dass die Konjugierten von H die ganze Gruppe G überdecken. Dann gilt $G = H$.*

Beweis. Angenommen, H ist eine echte Untergruppe von G. Sei $h = |H|$ und $m = (G : H) > 1$. Aus der Bahnengleichung folgt, dass die Anzahl der Konjugierten von H der Index des Normalisators $\mathrm{N}_G(H)$ von H ist. Da $H \subset \mathrm{N}_G(H)$ ist, hat H deswegen höchstens m Konjugierte. Da alle Konjugierten das Einselement gemeinsam haben, liegen in den Konjugierten also höchstens $m(h-1)+1 = mh - m + 1 < mh = |G|$ Elemente. Also können die Konjugierten von H nicht ganz G überdecken. Dies ist ein Widerspruch. □

Satz 7.2. *Es gibt ein gutes Erzeugendensystem für jede endliche Gruppe G.*

Beweis. Aus Satz 7.1 folgt, dass ein Repräsentantensystem der Konjugationsklassen ein gutes Erzeugendensystem von G ist. □

Lemma 7.3. *Für jede natürliche Zahl d gibt es unendlich viele irreduzible Polynome mit Grad mindestens d in $\mathbb{F}_q[T]$.*

Beweis. Für jede natürliche Zahl n ist $\mathbb{F}_{q^n}^*$ zyklisch, also gilt $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma_n)$ für einen Erzeuger γ_n von $\mathbb{F}_{q^n}^*$. Daraus folgt, dass das Minimalpolynom von γ_n über $\mathbb{F}_q$ ein irreduzibles Polynom vom Grad n ist. Daraus folgt die Behauptung. □

Satz 7.4. *Für alle q, n gibt es ein separables $\mathbb{F}_q$-lineares Polynom $f \in \mathbb{F}_q[T][X]$ mit $\mathrm{Gal}(f) = \mathrm{GL}_n(\mathbb{F}_q)$.*

Beweis. Es sei $\{g_1, \ldots, g_r\}$ ein gutes Erzeugendensystem der $\mathrm{GL}_n(\mathbb{F}_q)$, ein solches existiert gemäss Satz 7.2. Aus Lemma 7.3 folgt, dass es r verschiedene irreduzible Polynome $p_1, \ldots, p_r \in \mathbb{F}_q[T]$ mit Grad mindestens n gibt. Für $1 \leq i \leq r$ sei $\mathfrak{p}_i = (p_i)$. Die Ideale $\mathfrak{p}_i$ sind maximal und die Restklassenkörper $\mathbb{F}_q[T]/\mathfrak{p}_i$ sind Körpererweiterungen von $\mathbb{F}_q$ vom Grad $\deg(p_i) \geq n$. Aus Satz 5.1 folgt, dass es für jedes $1 \leq i \leq r$ ein normiertes, separables und $\mathbb{F}_q$-lineares Polynom $f_i \in (\mathbb{F}_q[T]/\mathfrak{p}_i)[X]$ gibt mit $\mathrm{Gal}(f_i) = \langle g_i \rangle$ bis auf Konjugation.

Nun sei $f_i(X) = X^{q^s} + \sum_{j=0}^{s-1} a_j^{(i)} X^{q^j} \in (\mathbb{F}_q[T]/\mathfrak{p}_i)[X]$ für $1 \leq i \leq r$. Für $0 \leq j \leq s-1$ folgt aus dem Chinesischen Restsatz, dass es ein Element $a_j \in \mathbb{F}_q[T]$

gibt, für welches gilt $a_j \equiv a_j^{(i)} \pmod{\mathfrak{p}_i}$ für alle $i \in \{1, \ldots, r\}$. Für $f(X) = X^{q^s} + \sum_{j=0}^{s-1} a_j X^{q^j} \in \mathbb{F}_q[T][X]$ gilt also $f \bmod \mathfrak{p}_i = f_i$ für $1 \leq i \leq r$. Der Ring $\mathbb{F}_q[T]$ ist faktoriell. Die Polynome f_i sind separabel, also gilt $a_0^{(i)} \neq 0$. Deshalb ist $a_0 \notin \mathfrak{p}_i$ für alle $i \in \{1, \ldots, r\}$. Aus Satz 6.8 folgt deshalb, dass $\mathrm{Gal}(f)$ für jedes $i \in \{1, \ldots, r\}$ eine zu $\langle g_i \rangle$ konjugierte Untergruppe enthält. Daraus folgt $\mathrm{Gal}(f) = \mathrm{GL}_n(\mathbb{F}_q)$. □

8 Konstruktion des Polynoms mit Galoisgruppe $\mathrm{SL}_n(\mathbb{F}_q)$

Nun wenden wir uns dem Problem zu, für gegebene q, n ein $\mathbb{F}_q$-lineares Polynom f mit Galoisgruppe $\mathrm{SL}_n(\mathbb{F}_q)$ zu konstruieren. Wir haben bereits gesehen, wie wir mithilfe eines guten Erzeugendensystems und Satz 6.8 eine untere Schranke für $\mathrm{Gal}(f)$ erhalten. Um die $\mathrm{SL}_n(\mathbb{F}_q)$ zu realisieren, brauchen wir also noch eine obere Schranke für $\mathrm{Gal}(f)$.

Es sei k eine Körpererweiterung von $\mathbb{F}_q$ und $\bar{k}$ ein algebraischer Abschluss von k. Wir betrachten ein separables $\mathbb{F}_q$-lineares Polynom

$$f(X) = X^{q^n} + \sum_{i=0}^{n-1} a_i X^{q^i} \in k[X]$$

und dazu das Polynom

$$g(X) = X^q - (-1)^n a_0 X \in k[X].$$

Es seien $V_f = \ker(f|_{\bar{k}})$, $V_g = \ker(g|_{\bar{k}})$ und $G = \mathrm{Gal}(k(V_f, V_g)/k)$ die Galoisgruppe des gemeinsamen Zerfällungskörpers von f und g. Dann operiert G von links auf $\bigwedge^n V_f$ mittels $\sigma(v_1 \wedge \ldots \wedge v_n) = \sigma(v_1) \wedge \ldots \wedge \sigma(v_n)$. Ausserdem operiert G von links auf V_g auf die kanonische Weise. Beide Aktionen sind k-linear.

Satz 8.1. *Die beiden $k[G]$-Moduln $\bigwedge^n V_f$ und V_g sind isomorph.*

Beweis. Da die Mooresche Determinante multilinear und alternierend ist, induziert

$$v_1 \wedge \ldots \wedge v_n \mapsto \Delta(v_1, \ldots, v_n)$$

für $v_1, \ldots, v_n \in V_g$ eine k-lineare Abbildung $\tilde{\Delta} : \bigwedge^n V_f \to \bar{k}$.

Wegen Lemma 3.4 gilt für linear unabhängige $v_1, \ldots, v_n \in V_f$

$$a_0 = \prod_{v \in V_f \setminus \{0\}} v = (-1)^n \Delta(v_1, \ldots, v_n)^{q-1}.$$

Also liegt das Bild von $\tilde{\Delta}$ in V_g.

Da f separabel ist, ist $a_0 \neq 0$. Daraus folgt $\tilde{\Delta} \neq 0$. Da $\bigwedge^n V_f$ und V_g eindimensionale Vektorräume sind, ist $\tilde{\Delta} : \bigwedge^n V_f \to V_g$ also ein Isomorphismus von k-Vektorräumen.

Für $\sigma \in G$ und $v_1, \ldots, v_n \in V_f$ gilt

$$\tilde{\Delta}(\sigma(v_1) \wedge \ldots \wedge \sigma(v_n)) = \sigma(\tilde{\Delta}(v_1 \wedge \ldots \wedge v_n)).$$

Also ist $\tilde{\Delta}$ ein Isomorphismus von $k[G]$-Moduln. □

Satz 8.2. *Es sind äquivalent:*

(i) $a_0 = (-1)^n$.

(ii) G *operiert trivial auf* V_g.

(iii) G *operiert trivial auf* $\bigwedge^n V_f$.

(iv) $\mathrm{Gal}(f) \subset \mathrm{SL}_n(\mathbb{F}_q)$.

Beweis. (i) $\iff$ (ii): Es gilt

$$G \text{ operiert trivial auf } V_g. \iff \mathrm{Gal}(g) \text{ operiert trivial auf } V_g. \iff$$
$$\mathrm{Gal}(g) = \{1\} \iff V_g = \mathbb{F}_q \iff g(X) = X^q - X \iff a_0 = (-1)^n.$$

(ii) $\iff$ (iii): Dies folgt aus Satz 8.1.

(iii) $\iff$ (iv): Dies folgt aus der Tatsache, dass für $v_1, \ldots, v_n \in V_f$ und $\sigma \in \mathrm{Gal}(f)$ gilt

$$\sigma(v_1 \wedge \ldots \wedge v_n) = \det(\sigma) v_1 \wedge \ldots \wedge v_n.$$ □

Satz 8.3. *Für alle* q, n *gibt es ein separables* $\mathbb{F}_q$*-lineares Polynom* $f \in \mathbb{F}_q[T][X]$ *mit* $\mathrm{Gal}(f) = \mathrm{SL}_n(\mathbb{F}_q)$.

Beweis. Es sei $\{g_1, \ldots, g_r\}$ ein gutes Erzeugendensystem der $\mathrm{SL}_n(\mathbb{F}_q)$, ein solches existiert gemäss Satz 7.2. Aus Lemma 7.3 folgt, dass es r verschiedene irreduzible Polynome $p_1, \ldots, p_r \in \mathbb{F}_q[T]$ mit Grad mindestens n gibt. Für $1 \leq i \leq r$ sei $\mathfrak{p}_i = (p_i)$. Die Ideale $\mathfrak{p}_i$ sind maximal und die Restklassenkörper $\mathbb{F}_q[T]/\mathfrak{p}_i$ sind Körpererweiterungen von $\mathbb{F}_q$ vom Grad $\deg(p_i) \geq n$. Aus Satz 5.1 folgt, dass es für jedes $1 \leq i \leq r$ ein normiertes, separables und $\mathbb{F}_q$-lineares Polynom $f_i \in (\mathbb{F}_q[T]/\mathfrak{p}_i)[X]$ gibt mit $\mathrm{Gal}(f_i) = \langle g_i \rangle$ bis auf Konjugation.

Nun sei $f_i(X) = X^{q^s} + \sum_{j=0}^{s-1} a_j^{(i)} X^{q^j} \in (\mathbb{F}_q[T]/\mathfrak{p}_i)[X]$ für $1 \leq i \leq r$. Aus Satz 8.2 folgt, dass $a_0^{(i)} = (-1)^n$ ist für alle $1 \leq i \leq r$. Für $1 \leq j \leq s-1$ folgt aus dem Chinesischen Restsatz, dass es ein Element $a_j \in \mathbb{F}_q(X)$ gibt, für das gilt $a_j \equiv a_j^{(i)} \pmod{\mathfrak{p}_i}$ für alle $i \in \{1, \ldots, r\}$. Es sei $a_0 = (-1)^n$. Für $f(X) = X^{q^s} + \sum_{j=0}^{s-1} a_j X^{q^j} \in \mathbb{F}_q[T][X]$ gilt also $f \bmod \mathfrak{p}_i = f_i$ für $1 \leq i \leq r$. Der Ring $\mathbb{F}_q[T]$ ist faktoriell. Die Polynome f_i sind separabel, also gilt $a_0^{(i)} \neq 0$. Deshalb ist $a_0 \notin \mathfrak{p}_i$ für alle $i \in \{1, \ldots, r\}$. Aus Satz 6.8 folgt deshalb, dass $\mathrm{Gal}(f)$ für jedes $i \in \{1, \ldots, r\}$ ein zu g_i konjugiertes Element enthält. Daraus folgt $\mathrm{SL}_n(\mathbb{F}_q) \subset \mathrm{Gal}(f)$. Da $a_0 = (-1)^n$ ist, folgt schliesslich aus Satz 8.2, dass gilt $\mathrm{Gal}(f) \subset \mathrm{SL}_n(\mathbb{F}_q)$. □

9 Die Erzeugung der $\mathrm{GL}_n(\mathbb{F}_q)$

Wir möchten nun solche Polynome f mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$ explizit berechnen können. Mit den in den Beweisen von Satz 7.4 und Satz 8.3 verwendeten Methoden ist dies aber nur mit sehr grossem Aufwand möglich. Deshalb hätten wir gerne ein gutes Erzeugendensystem für die $\mathrm{GL}_n(\mathbb{F}_q)$, das wesentlich kleiner ist als dasjenige, welches wir aus Satz 7.2 erhalten. Ausserdem wollen wir die Elemente dieses Erzeugendensystem mit Polynomen über $\mathbb{F}_q$ selbst, und nicht einer endlichen Erweiterung von $\mathbb{F}_q$, erzeugen können. Aus Satz 2.3 folgt, dass wir auf diese Weise genau diejenigen Elemente der $\mathrm{GL}_n(\mathbb{F}_q)$ (bis auf Konjugation) in $\mathrm{Gal}(f)$ erzwingen können, deren charakteristisches und Minimalpolynom übereinstimmen. Deshalb möchten wir, dass das charakteristische Polynom und das Minimalpolynom der Elemente des gesuchten guten Erzeugendensystems übereinstimmen. Die Resultate in diesem Abschnitt stammen von Pink.

Für $1 \leq i, j \leq n$ sei E_{ij} die Matrix mit Eintrag 1 in der i-ten Zeile und j-ten Spalte und 0 sonst. Es bezeichne I die Einheitsmatrix.

Lemma 9.1. *Die Elemente $I + \lambda E_{ij}$ für $1 \leq i, j \leq n$ und $\lambda \in \mathbb{F}_q^*$ erzeugen $\mathrm{SL}_n(\mathbb{F}_q)$.*

Beweis. Sei $\lambda \in \mathbb{F}_q^*$. Multiplikation von $A \in \mathrm{GL}_n(\mathbb{F}_q)$ mit der Matrix $I + \lambda E_{ij}$ von links/rechts addiert die i-te Zeile/Spalte von A zur j-ten Zeile/Spalte. Mit dem Gausseliminationsverfahren lässt sich jedes $A \in \mathrm{GL}_n(\mathbb{F}_q)$ durch eine Reihe solcher Umformungen in eine Matrix der Form

$$\tilde{A} = \begin{bmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

bringen. Da diese Umformungen die Determinante festlassen, gilt $\det \tilde{A} = \det A$. Für $A \in \mathrm{SL}_n(\mathbb{F}_q)$ folgt daraus $\lambda = \det \tilde{A} = 1$. Also ist A ein Produkt von gewissen $I + \lambda E_{ij}$. □

Durch Multiplikation operiert die zyklische Gruppe $\mathbb{F}_{q^n}^*$ linear auf dem n-dimensionalen $\mathbb{F}_q$-Vektorraum $\mathbb{F}_{q^n}$. Man erhält also eine Einbettung $\varphi_n : \mathbb{F}_{q^n}^* \to \mathrm{GL}_n(\mathbb{F}_q)$, welche aber von der Wahl einer $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^n}$ abhängt. Es sei γ_n ein Erzeuger der $\mathbb{F}_{q^n}^*$. Dann ist $s_n = \varphi_n(\gamma_n)$ ein Erzeuger von $\varphi_n(\mathbb{F}_{q^n}^*)$. Für $x \in \mathbb{F}_{q^n}$ sei $\mathrm{N}(x) = \det(\varphi_n(x))$ die Norm von x. Da die Determinante invariant unter Konjugation ist, hängt N nicht von der Wahl der Basis ab. Es bezeichne $(e_1, \ldots, e_n)$ die Standardbasis von $\mathbb{F}_q^n$.

Lemma 9.2. $\mathrm{N} : \mathbb{F}_{q^n}^* \to \mathbb{F}_q^*$ *ist surjektiv.*

Beweis. Für $x \in \mathbb{F}_{q^n}^*$ gilt

$$\mathrm{N}(x) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(x) = \prod_{i=0}^{n-1} x^{q^i} = x^{\sum_{i=0}^{n-1} q^i} = x^{\frac{q^n-1}{q-1}}.$$

Also kann N jeden Wert in $\mathbb{F}_q^*$ höchstens $\frac{q^n-1}{q-1}$-mal annehmen. Aus $|\mathbb{F}_{q^n}^*| = q^n - 1$ und $|\mathbb{F}_q^*| = q - 1$ folgt damit die Behauptung. □

Lemma 9.3. *Für $A \in \mathrm{GL}_n(\mathbb{F}_q)$ gilt: $\langle A \rangle$ operiert transitiv auf $\mathbb{F}_q^n \setminus \{0\}$ genau dann, wenn $\langle A^T \rangle$ transitiv auf $\mathbb{F}_q^n \setminus \{0\}$ operiert.*

Beweis. Angenommen, $\langle A \rangle$ operiert transitiv auf $\mathbb{F}_q^n \setminus \{0\}$. Da A und A^T ähnlich sind, gibt es ein $S \in \mathrm{GL}_n(\mathbb{F}_q)$, für welches gilt $A^T = S^{-1}AS$. Seien $v, w \in \mathbb{F}_q^n \setminus \{0\}$. Dann gibt es eine ganze Zahl k für die gilt $A^k Sv = Sw$. Dann gilt $(A^T)^k v = w$. Also operiert auch $\langle A^T \rangle$ transitiv auf $\mathbb{F}_q^n \setminus \{0\}$. Die umgekehrte Implikation folgt nun mit $(A^T)^T = A$ aus dem eben Gezeigten. □

Satz 9.4. *Es sei $h_1 = s_n$,*

$$h_2 = \begin{bmatrix} 1 & 0 \\ 0 & s_{n-1} \end{bmatrix}$$

und

$$h_3 = \begin{bmatrix} 1 & 1 & 0 & \dots & \\ 0 & 1 & 0 & \dots & \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ & & & & 1 \end{bmatrix}.$$

Dann ist $\{h_1, h_2, h_3\}$ ein gutes Erzeugendensystem der $\mathrm{GL}_n(\mathbb{F}_q)$.

Beweis. Es sei G eine Untergruppe der $\mathrm{GL}_n(\mathbb{F}_q)$, welche für $i \in \{1, 2, 3\}$ ein konjugiertes Element $\tilde{h}_i$ von h_i enhält. Wir wollen zeigen, dass gilt $G = \mathrm{GL}_n(\mathbb{F}_q)$. Es genügt zu zeigen, dass $\sigma G \sigma^{-1} = \mathrm{GL}_n(\mathbb{F}_q)$ für ein $\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$. Deshalb sei ohne Beschränkung der Allgemeinheit $\tilde{h}_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & s_{n-1} \end{smallmatrix}\right]$.

Da $\mathbb{F}_{q^n}^*$ transitiv auf $\mathbb{F}_{q^n} \setminus \{0\}$ operiert, operiert $\langle \tilde{h}_1 \rangle$, also auch G, transitiv auf $\mathbb{F}_q^n \setminus \{0\}$.

Behauptung 1. *Für jedes zu h_3 konjugierte Element h gibt es ein $g \in G$, so dass $g^{-1}hg$ die Form*

$$\begin{bmatrix} 1 & b_1 & \dots & b_{n-1} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & I \end{bmatrix}$$

für einen Zeilenvektor $b \in \mathbb{F}_q^{n-1} \setminus \{0\}$ hat.

Beweis. Ein konjugiertes Element h von h_3 anzugeben ist äquivalent dazu, $\mathrm{im}(h-I)$, $\ker(h-I)$ und den von $h-I$ induzierten Isomorphismus $\mathbb{F}_q^n / \ker(h-I) \to \mathrm{im}(h-I)$ anzugeben. Da G transitiv auf $\mathbb{F}_q^n \setminus \{0\}$ operiert, kann man h so mit einem Element g von G konjugieren, dass gilt $\mathrm{im}(ghg^{-1} - I) = \mathbb{F}_q e_1$: Es sei $v \in \mathrm{im}(h-I) \setminus \{0\}$. Dann gibt es ein $g \in G$ für welches $gv = e_1$ ist. Dann gilt $\mathrm{im}(ghg^{-1} - I) = \mathrm{im}(g(h-I)g^{-1}) = g\,\mathrm{im}(h-I) = \mathbb{F}_q e_1$. Dann gibt es ein $b \in \mathbb{F}_q^n \setminus \{0\}$ mit $ghg^{-1} = \left[\begin{smallmatrix} 1 & b \\ 0 & I \end{smallmatrix}\right]$. □

Behauptung 2. *Für alle Zeilenvektoren $b \in \mathbb{F}_q^{n-1}$ enthält G die Matrix $\left[\begin{smallmatrix} 1 & b \\ 0 & I \end{smallmatrix}\right]$.*

Beweis. Sei $b \in \mathbb{F}_q^{n-1} \backslash \{0\}$. Wegen Behauptung 1 gibt es $g \in G$ und $\tilde{b} \in \mathbb{F}_q^{n-1} \backslash \{0\}$ mit $g\tilde{h}_3 g^{-1} = \left[\begin{smallmatrix} 1 & \tilde{b} \\ 0 & I \end{smallmatrix}\right] \in G$. Da $\langle s_{n-1} \rangle$ transitiv auf $\mathbb{F}_q^{n-1} \setminus \{0\}$ operiert, folgt aus Lemma 9.3, dass auch $\langle s_{n-1}^T \rangle$ transitiv auf $\mathbb{F}_q^{n-1} \setminus \{0\}$ operiert. Also gibt es ein $k \in \mathbb{N}$ mit $(s_{n-1}^T)^k \tilde{b} = b$. Dann ist

$$\begin{aligned} \tilde{h}_2^{-k} g h_3 g^{-1} \tilde{h}_2^k &= \begin{bmatrix} 1 & 0 \\ 0 & s_{n-1}^{-k} \end{bmatrix} \begin{bmatrix} 1 & \tilde{b} \\ 0 & I \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & s_{n-1}^{k} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & s_{n-1}^{-k} \end{bmatrix} \begin{bmatrix} 1 & (s_{n-1}^T)^k \tilde{b} \\ 0 & s_{n-1}^{k} \end{bmatrix} = \begin{bmatrix} 1 & (s_{n-1}^T)^k \tilde{b} \\ 0 & I \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & I \end{bmatrix} \in G. \quad \square \end{aligned}$$

Behauptung 3. *Alle $\mathrm{GL}_n(\mathbb{F}_q)$-Konjugierten von h_3 liegen in G.*

Beweis. Dies folgt aus den Behauptungen 1 und 2. $\square$

Behauptung 4. $\mathrm{GL}_n(\mathbb{F}_q) = G$

Beweis. Für alle $1 \leq i, j \leq n$ und für alle $\lambda \in \mathbb{F}_q^*$ ist das Element $I + \lambda E_{ij}$ zu h_3 konjugiert. Aus Behauptung 3 folgt also, dass diese Elemente in G liegen. Aus Lemma 9.1 folgt deshalb $\mathrm{SL}_n(\mathbb{F}_q) \subset G$. Aus Lemma 9.2 folgt, dass $\det : \langle \tilde{h}_1 \rangle \to \mathbb{F}_q^*$ surjektiv ist, also ist auch $\det : G \to \mathbb{F}_q^*$ surjektiv. Zusammen mit $\mathrm{SL}_n(\mathbb{F}_q) \subset G$ impliziert dies $\mathrm{GL}_n(\mathbb{F}_q) \subset G$. $\square$

Die Menge $\{h_1, h_2, h_3\}$ hat aber noch nicht alle gewünschten Eigenschaften, da für $n > 2$ das Minimalpolynom und das charakteristische Polynom von h_3 nicht übereinstimmen. Deshalb modifizieren wir Satz 9.4 wie folgt:

Für $\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$ sei wie oben μ_σ das Minimalpolynom von σ und χ_σ das charakteristische Polynom von σ.

Satz 9.5. *h_1, h_2 und h_3 seien wie in Satz 9.4 definiert. Falls $n > 2$ sei*

$$h_3' = \begin{bmatrix} 1 & 1 & & \\ 0 & 1 & & \\ & & & \\ & & & s_{n-2} \end{bmatrix}.$$

Es seien $g_1 = h_1$ und $g_2 = h_2$ sowie $g_3 = h_3$ falls $n \leq 2$ und $g_3 = h_3'$ falls $n > 2$. Dann gilt:

(i)

$$\begin{aligned} \mu_{g_1}(X) &= \chi_{g_1}(X) = \mu_{\gamma_n}(X) \\ \mu_{g_2}(X) &= \chi_{g_2}(X) = (X-1)\mu_{\gamma_{n-1}}(X) \\ \mu_{g_3}(X) &= \chi_{g_3}(X) = \begin{cases} (X-1)^2 \mu_{\gamma_{n-2}}(X) & \text{falls } n > 2, \\ (X-1)^2 & \text{falls } n = 2, \\ (X-1) & \text{falls } n = 1 \end{cases} \end{aligned}$$

Insbesondere stimmen das charakteristische Polynom und das Minimalpolynom von g_i überein für $i = 1, 2, 3$.

(ii) $\{g_1, g_2, g_3\}$ *ist ein gutes Erzeugendensystem.*

Beweis. (i) Da für den Erzeuger γ_n von $\mathbb{F}_{q^n}^*$ gilt $\mathbb{F}_q(\gamma_n) = \mathbb{F}_{q^n}$ und $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, hat das Minimalpolynom von γ_n, welches auch das Minimalpolynom von s_n ist, Grad n. Deshalb ist $\mu_{g_1} = \chi_{g_1} = \mu_{\gamma_n}$. Aus dem gleichen Grund haben die Minimalpolynome von s_{n-1} und s_{n-2} Grad $n-1$ beziehungsweise $n-2$. Weil γ_{n-1} und γ_{n-2} nicht den Eigenwert 1 haben, ist daher $\mu_{g_2}(X) = \chi_{g_2}(X) = (X-1)\mu_{\gamma_{n-1}}(X)$ und $\mu_{h_3'}(X) = \chi_{h_3'}(X) = (X-1)^2\mu_{\gamma_{n-2}}(X)$ falls $n > 2$. Die Behauptung zu μ_{g_3} im Fall $n \leq 2$ ist klar.

(ii) Für $n \leq 2$ folgt dies sofort aus Satz 9.4. Deshalb sei nun $n > 2$ und G eine Untergruppe der $\mathrm{GL}_n(\mathbb{F}_q)$, welche ein konjugiertes Element von h_1, h_2 und h_3' enthält. Es gibt also ein $h \in \mathrm{GL}_n(\mathbb{F}_q)$ für welches $h^{-1}h_3'h$ in G liegt.

Behauptung 1. $h^{-1}h_3h \in G$

Beweis. Es sei

$$g = \begin{bmatrix} 1 & 0 & \\ 0 & 1 & \\ & & s_{n-2} \end{bmatrix}.$$

Damit gilt $h_3' = h_3g = gh_3$. Die Ordnung von h_3 ist p und diejenige von g ist $q^{n-2}-1$. Da $n > 2$ ist, sind p und $q^{n-2}-1$ teilerfremd. Also gibt es ganze Zahlen r und s so dass gilt $rp + s(q^{n-2}-1) = 1$. Es folgt $(h^{-1}h_3'h)^{1-rp} = h^{-1}h_3'^{1-rp}h = hh_3^{1-rp}g^{s(q^{n-2}-1)}h^{-1} = hh_3h^{-1} \in G$. □

Nun folgt $G = \mathrm{GL}_n(\mathbb{F}_q)$ aus Satz 9.4. □

10 Die Berechnung von $\mathbb{F}_q$-linearen Polynomen mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$

Wir zeigen nun, wie man Polynome mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$ explizit angeben kann.

Satz 10.1. *Zu* $q = p^k$ *und* $n \geq 1$ *seien* g_1, g_2, g_3 *wie in Satz 9.5 definiert. Für* $1 \leq i \leq 3$ *sei*

$$\mu_{g_i}(X) = X^n + \sum_{j=0}^{n-1} a_j^{(i)} X^i \in \mathbb{F}_q[X].$$

Für $0 \leq j \leq n-1$ *sei*

$$a_j = (1-T)a_j^{(1)} + Ta_j^{(2)} + T^{2q^n - 2q^j - 1}(T-1)a_j^{(3)}$$

Dann ist das $\mathbb{F}_q$*-lineare Polynom*

$$f(X) = X^{q^n} + \sum_{j=0}^{n-1} a_j X^{q^j} \in \mathbb{F}_q[T][X]$$

separabel und hat Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$.

Beweis. Es seien $\mathfrak{p}_1 = (T)$ und $\mathfrak{p}_2 = (T-1)$. Die $\mathfrak{p}_i$ sind maximale Ideale in $\mathbb{F}_q[T]$ mit $\mathbb{F}_q[T]/\mathfrak{p}_i \cong \mathbb{F}_q$. Es gilt

$$f(X) \bmod \mathfrak{p}_i = X^{q^n} + \sum_{j=0}^{n-1} a_j^{(i)} X^{q^j} \in \mathbb{F}_q[X]$$

für $i = 1, 2$. Die Galoisgruppen der Polynome f mod $\mathfrak{p}_i$ werden vom zugehörigen Frobeniusautomorphismus τ_i erzeugt. Für $i = 1, 2$ gilt $a_0^{(i)} = \pm \det(g_i) \neq 0$, also sind die Polynome f mod $\mathfrak{p}_i$ separabel. Aus $a_0 \bmod \mathfrak{p}_1 \neq 0$ folgt $a_0 \neq 0$, also ist auch f separabel. Aus Lemma 2.1 folgt $\mu_{\tau_i} = \chi_{\tau_i} = \mu_{g_i} = \chi_{\tau_i}$. Also folgt aus Lemma 2.2, dass τ_i und g_i konjugiert sind für $i = 1, 2$.

Der Ring $\mathbb{F}_q[T]$ ist faktoriell. Aus Satz 6.8 folgt daher, dass $\mathrm{Gal}(f)$ für $i = 1, 2$ ein Konjugiertes von τ_i enthält. Also enthält $\mathrm{Gal}(f)$ auch ein Konjugiertes von g_1 und g_2.

Nun betrachten wir das Polynom

$$g(X) = T^{-2q^n} f(T^2 X) \in \mathbb{F}_q(T)[X].$$

Es seien V_f und V_g die Zerfällungskörper von f und g in einem algebraischen Abschluss von $\mathbb{F}_q(T)$. Da gilt $V_f = T^2 V_g$, stimmen die Bilder der Galoisgruppen von f und g unter der Einbettung in die $\mathrm{GL}_n(\mathbb{F}_q)$ überein.

Es gilt

$$g(X) = X^{q^n} + \sum_{j=0}^{n-1} b_j X^{q^j}$$

mit

$$b_j = T^{2(q^j - q^n)} a_j = T^{2(q^j - q^n)}(1-T) a_j^{(1)} + T^{2(q^j - q^n)+1} a_j^{(2)} + (1 - T^{-1}) a_j^{(3)}$$

für alle $0 \leq j \leq n-1$. Das Ideal $\mathfrak{p}_3 := (T^{-1})$ im Ring $\mathbb{F}_q[T^{-1}]$ ist maximal und es gilt $\mathbb{F}_q[T^{-1}]/\mathfrak{p}_3 \cong \mathbb{F}_q$. Da für $0 \leq j < n$ gilt $2(q^j - q^n) < -1$, liegt g in $\mathbb{F}_q[T^{-1}][X]$ und es gilt

$$g \bmod \mathfrak{p}_3 = X^{q^n} + \sum_{i=0}^{n-1} a_j^{(3)} X^{q^i}.$$

Es gilt $a_0^{(3)} = \pm \det(g_3) \neq 0$, also ist g mod $\mathfrak{p}_3$ separabel. Aus Lemma 2.1 folgt $\mu_{\tau_3} = \chi_{\tau_3} = \mu_{g_3} = \chi_{\tau_3}$. Also folgt aus Lemma 2.2, dass τ_3 und g_3 konjugiert sind.

Der Ring $\mathbb{F}_q[T^{-1}]$ ist faktoriell und hat Quotientenkörper $\mathbb{F}_q(T)$. Aus Satz 6.8 folgt daher, dass $\mathrm{Gal}(g) = \mathrm{Gal}(f)$ ein Konjugiertes von τ_3 enthält. Also enthält $\mathrm{Gal}(f)$ auch ein Konjugiertes von g_3.

Da gemäss Satz 9.5 die Menge $\{g_1, g_2, g_3\}$ ein gutes Erzeugendensystem der $\mathrm{GL}_n(\mathbb{F}_q)$ ist, folgt $\mathrm{Gal}(f) = \mathrm{GL}_n(\mathbb{F}_q)$. □

Mithilfe von Satz 10.1 können wir nun Polynome mit Galoisgruppe $\mathrm{GL}_n(\mathbb{F}_q)$ explizit angeben. Dafür benötigen wir die Minimalpolynome von Erzeugern γ_n der zyklischen Gruppe $\mathbb{F}_{q^n}^*$. Diese können wie folgt gefunden werden:

Die Erzeuger γ_n von $\mathbb{F}_{q^n}^*$ sind charakterisiert durch $\gamma_n^{q^n-1} = 1$ und $\gamma_n^k \neq 1$ für alle $0 < k < q^n - 1$. Solche Elemente von $\mathbb{F}_{q^n}$ heissen primitive $(q^n - 1)$-te Einheitswurzeln. Es sei

$$\Phi_{q^n-1}(X) = \prod_{\gamma}(X - \gamma) \in \mathbb{F}_{q^n}[X],$$

wobei sich das Produkt über alle (q^n-1)-ten Einheitswurzeln γ in $\mathbb{F}_{q^n}$ erstreckt.

Die Möbiussche μ-Funktion $\mu : \mathbb{N} \setminus \{0\} \to \mathbb{Z}$ ist definiert durch

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ 0 & \text{falls } n \text{ nicht quadratfrei ist}, \\ (-1)^k & \text{falls } n = p_1 \dots p_k \text{ für } k \text{ verschiedene Primzahlen } p_1, \dots, p_k. \end{cases}$$

Satz 10.2. *Es gilt für alle $q = p^k$ und alle $n \in \mathbb{N}$:*

$$\Phi_{q^n-1}(X) = \prod_{d|q^n-1} (X^d - 1)^{\mu(\frac{q^n-1}{d})}$$

Beweis. Siehe [4], Satz 16.9, Seite 143. □

Die Minimalpolynome der γ_n sind nun gerade die irreduziblen Teiler von Φ_{q^n-1}. Mit diesen Hilfsmitteln können wir nun alles berechnen.

Sei zum Beispiel $n = 3$ und $q = 2$. Dann erhalten wir

$$\begin{aligned} \Phi_{q^{n-2}-1}(X) &= \Phi_1(X) = X + 1 \\ \Phi_{q^{n-1}-1}(X) &= \Phi_3(X) = (X-1)^{-1}(X^3 - 1) = X^2 + X + 1 \\ \Phi_{q^n-1}(X) &= \Phi_7(X) = (X-1)^{-1}(X^7 - 1) \\ &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\ &= (X^3 + X^2 + 1)(X^3 + X + 1), \end{aligned}$$

wobei $X + 1$, $X^2 + X + 1$, $X^3 + X^2 + 1$ und $X^3 + X + 1$ irreduzibel sind. Wir wählen Minimalpolynome $\mu_{\gamma_1}(X) = X + 1$, $\mu_{\gamma_2}(X) = X^2 + X + 1$ und $\mu_{\gamma_3}(X) = X^3 + X^2 + 1$. Daraus erhalten wir für die Minimalpolynome der g_i mit den Formeln aus Satz 9.5:

$$\begin{aligned} \mu_{g_1}(X) &= X^3 + X^2 + 1 \\ \mu_{g_2}(X) &= (X-1)(X^2 + X + 1) = X^3 + 1 \\ \mu_{g_3}(X) &= (X-1)^2(X+1) = X^3 + X^2 + X + 1 \end{aligned}$$

Mit der Formel aus Satz 10.1 erhalten wir das Polynom

$$f(X) = X^8 + (T^8 + T^7 + T + 1)X^4 + (T^{12} + T^{11})X^2 + (T^{14} + T^{13} + 1)X \in \mathbb{F}_2[T][X]$$

mit Galoisgruppe $\mathrm{GL}_3(\mathbb{F}_2)$.

Literatur

[1] David Goss. *Basic Structures of Function Field Arithmetic.* Springer, 1997.

[2] Bartel Leendert van der Warden. *Algebra 1.* Springer, 9. Auflage.

[3] Clarence Wilkersen. A primer on the Dickson invariants. *Contemp. Math.*, 19:421–434, 1983.

[4] Gisbert Wüstholz. *Algebra.* Vieweg, 2004.