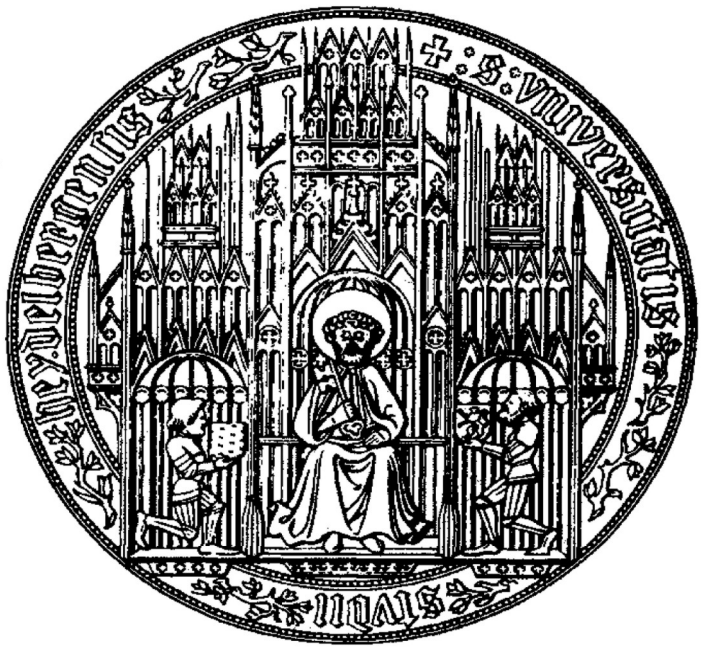
Galoisgruppen von relativen Frobenius-Moduln



Diplomarbeit

vorgelegt von
Florian Mirus

betreut von
Prof. Dr. B. Heinrich Matzat

16. Januar 2011

Fakultät für Mathematik und Informatik
der Universität Heidelberg

Vorwort

In der klassischen Galoistheorie, basierend auf den Ideen des französischen Mathematikers Évariste Galois (1811-1832), werden Symmetrien der Nullstellen von Polynomen untersucht. Dazu wird einem Polynom die sogenannte Galoisgruppe zugeordnet, die durch ihre Struktur viele Informationen über die Nullstellen des Polynoms enthält. Diese lässt sich in die symmetrische Gruppe einbetten. Dieser klassische Ansatz lässt sich auch auf andere Gebiete verallgemeinern. Die Galoistheorie für homogene lineare Differentialgleichungen hat ihren Ursprung im 19. Jahrhundert und wurde in der Mitte des 20. Jahrhunderts durch Kolchin (vgl. [Kol48]) auf ein solides Fundament gestellt. Auch hier wird jeder Gleichung die sogenannte Differential-Galoisgruppe, in diesem Fall eine lineare algebraische Gruppe, zugeordnet. Ein Differentialkörper ist dann ein Körper K mit einer Abbildung $\delta : K \longrightarrow K$, einer sogenannten Derivation. An die Stelle des Zerfällungskörpers tritt hier der Picard-Vessiot-Körper, der alle Lösungen der Differentialgleichung enthält. Den ersten praktisch anwendbaren Algorithmus zur Lösung (und damit zur Bestimmung der Galoisgruppe) solcher Gleichungen bis zum Grad 2 stellte Kovacic in seiner Arbeit [Kov86] vor. Lange Zeit beschränkte sich die Differential-Galoistheorie auf Gleichungen in Charakteristik 0. Um diese Theorie auf Gleichungen in positiver Charakteristik zu verallgemeinern geht man von einer Derivation δ zu einer Familie von Derivationen $(\delta^{(k)})_{k\in\mathbb{N}}$, einer sogenannten iterativen Derivation, über. Viele der ursprünglichen Aussagen lassen sich dann auf dieses Setting übertragen (vgl. [Mat01]).
Eine weitere Verallgemeinerung der klassischen Galoistheorie ist die Galoistheorie linearer Differenzengleichungen. Diese verhält sich recht analog zur Theorie der linearen Differentialgleichungen. Der Unterschied besteht darin, dass ein Differenzenkörper K anstatt einer Derivation δ einen Automorphismus (oder einen Endomorphismus) ϕ als zusätzliche Struktur trägt (vgl. [vdPM97]). Für Differenzengleichungen in Charakteristik 0 findet sich ein Analogon zum Kovacic-Algorithmus in der Dissertation von P.A. Hendriks (vgl. [Hen96]).

In dieser Arbeit befassen wir uns mit Differenzengleichungen in positiver Charakteristik. Die zugrundeliegenden Strukturen sind die sogenannten Frobenius-Moduln. Dies sind Moduln über einem Frobenius-Ring R zusammen mit dem Frobenius-Endomorphimus Φ. Die Motivation hierfür ist die Lösung bzw. Berechnung der Galoisgruppe von Differentialgleichungen über Frobenius-Moduln mit iterativen Derivationen ∇. Man kann zeigen, dass die Φ- bzw. ∇-Moduln als neutrale Tannaka-Kategorien äquivalent sind und dass ihre Galoisgruppen-Schemata bis auf einen Basiswechsel übereinstimmen (vgl. Kapitel 6 bzw. [Mat09b] und [Mat09a]). Der Vorteil die Moduln von der Differenzen-Seite zu betrachten besteht darin, dass man nur eine Gleichung statt einer Familie von Gleichungen untersuchen muss. Andererseits haben die Differenzengleichungen in positiver Charakteristik viele

Gemeinsamkeiten mit Differentialgleichungen in Charakteristik 0. Diese Gemeinsamkeiten begründen sich hauptsächlich durch die Analogie der Operator-Ringe (vgl. Kapitel 2 bzw. [Ore33]), aber auch dadurch, dass auch die Differential-Moduln in Charakteristik 0 eine neutrale Tannaka-Kategorie bilden (vgl. [vdPS03, Appendix B]).
Dies versetzt uns in die Lage den klassischen Kovacic-Algorithmus für Differentialgleichungen, bzw. dessen Analogon von Hendriks für Differenzengleichungen in Charakteristik 0 auf unsere Differenzengleichungen über Frobenius-Ringen zu übertragen. Dabei müssen natürlich einige Modifikationen vorgenommen werden. Dies sind unter anderem die Berechnung des $\mathbb{G}_a$-Anteils bei reduziblen Galoisgruppen (vgl. Abschnitt 5.1 Satz 5.2). Da die $\mathbb{G}_a$ in Charakteristik 0 keine nicht-trivialen algebraischen Untergruppen besitzt, tritt dieser Fall im klassischen Kovacic-Algorithmus nicht auf. Außerdem können in positiver Charakteristik auch nicht-zerfallende Tori als Galoisgruppe auftreten (vgl. Abschnitt 5.4 Satz 5.7). Die dritte Hauptmodifikation ist die Untersuchung der Zwischengruppen von $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$ (vgl. Satz 5.11). Auch dieser Fall tritt im klassischen Kovacic-Algorithmus nicht auf, da man die Galoisgruppe von Differentialgleichungen in Charakteristik 0 nach [SU93, Theorem 3.3.] in die $\mathrm{SL}_2(\mathbb{C})$ einbetten kann.
Die Arbeit ist folgendermaßen aufgebaut: In Kapitel 1 werden die wichtigsten Resultate über Frobenius-Moduln und Galoistheorie von Differenzengleichungen zusammengetragen und bewiesen. Kapitel 2 befasst sich mit Linearen Konstruktionen, die später im Algorithmus verwendet werden sollen, sowie der Theorie der Differenzen-Operatoren. In Kapitel 3 betrachten wir verschiedene Möglichkeiten zur Faktorisierung solcher Operatoren. In Kapitel 4 lösen wir Differenzengleichungen vom Grad 1, bzw. berechnen deren Galoisgruppe. In Kapitel 5 gehen wir zu Differenzengleichungen vom Grad 2 über und übertragen den Kovacic- bzw. Hendriks-Algorithmus auf unser Setting. Schließlich werden wir noch in Kapitel 6 einiges zur Berechenbarkeit der Galoisgruppe von Gleichungen beliebiger Ordnung sagen. Dieses letzte Kapitel, in dem wir weitgehend auf Beweise verzichten, befasst sich vor allem mit der Sprache der Tannaka-Kategorien und deren Anwendung auf Frobenius-Moduln.
Zum Abschluss sei allerdings noch erwähnt, dass das Thema aus zeitlichen Gründen im Rahmen dieser Diplomarbeit nicht abschließend behandelt werden konnte. Basierend auf den Ergebnissen der vorliegenden Arbeit gäbe es verschiedene Möglichkeiten das Thema zu vertiefen. Einerseits könnte man die Methoden aus den Kapiteln 4 und 5 für $\mathbb{F}_q(s,t)$ auf weitere Anwendungsbeispiele, wie zum Beispiel den Witt-Ring, übertragen. Andererseits könnte man auch versuchen, mit Hilfe der Faktorisierungsalgorithmen in Kapitel 3 einen Algorithmus zur Berechnung der Galoisgruppe für Gleichungen vom Grad 3 und höher zu entwickeln. Dafür wurden schon einige Grundlagen in den Sätzen 1.30, 1.36, sowie 2.30 (d) und (e) bewiesen, auf denen man wie in [SU93] aufbauen könnte, um einen solchen Algorithmus zumindest für Gleichungen vom Grad 3 zu entwickeln. Schließlich könnte man auch ausgehend von Kapitel 6 versuchen, einen allgemeinen Algorithmus zur Berechnung der Galoisgruppe von Differenzengleichungen beliebiger Ordnung zu finden. Wir haben in Kapitel 6 lediglich angedeutet, dass es aufgrund der Existenz eines entsprechenden Algorithmus für Differentialgleichungen in Charakteristik 0 (vgl. [Hru02]) nahe liegt, dass auch ein solcher Algorithmus für Differenzengleichungen in positiver Charakteristik existiert. Mit dem Beweis für die Existenz eines solchen Algorithmus wäre das Thema dann abschließend behandelt.

Inhaltsverzeichnis

Kapitel 1

Differenzen-Galoistheorie und Frobenius-Moduln

Wir wollen in diesem ersten Kapitel zunächst die grundlegenden Definitionen und Sätze über Frobenius-Ringe und Frobenius-Moduln zusammenstellen. Diese bilden die Grundlage für die Differenzengleichungen, die wir betrachten wollen. Dabei folgen wir hier hauptsächlich den Methoden und Resultaten von B. H. Matzat. Ausführlichere Abhandlungen über Frobenius-Moduln finden sich in [Mat03], [Mat09b] und [Mat09a].

1.1 Grundlegende Definitionen

Definition 1.1. Ein Integritätsbereich R mit $\mathrm{char}(R) > 0$ zusammen mit einem Endomorphismus $\phi \in \mathrm{End}(S)$ heißt **gewöhnlicher Frobenius-Ring**, falls eine natürliche Zahl $d \in \mathbb{N}$ existiert, so dass

$$\phi = \phi_q : R \longrightarrow R,\ x \longmapsto x^q$$

mit $q = p^d$ gilt. Das Paar (R, ϕ) heißt **relativer Frobenius-Ring**, falls ein ϕ-invariantes Primideal, ein sogenanntes ϕ**-Ideal** $Q \trianglelefteq R$, d.h. mit $\phi(Q) \subseteq Q$ existiert, so dass das Paar $(\bar{R} := R/Q, \bar{\phi})$, wobei $\bar{\phi}$ den induzierten Endomorphismus bezeichnet, einen gewöhnlichen Frobenius-Ring bildet. In diesem Fall heißt Q **definierendes Primideal**. Falls in Zukunft ein Frobenius-Ring nicht explizit als gewöhnlich bezeichnet wird, ist immer ein relativer Forbenius-Ring gemeint. Die Menge

$$R^\phi = \{r \in R \mid \phi(r) = r\}$$

heißt **Ring der Frobenius-Invarianten**.

Definition 1.2. Es sei (R, ϕ) ein Frobenius-Ring. Ein freier R-Modul M mit einem Endomorphismus $\Phi \in \mathrm{End}(M)$ heißt **Frobenius-Modul** über R, falls Φ eine ϕ-semilineare Abbildung ist, d.h. für alle $x, y \in M$ und alle $r \in R$ gilt

$$\Phi(x + y) = \Phi(x) + \Phi(y) \text{ und } \Phi(r \cdot x) = \phi(r) \cdot \Phi(x).$$

Die Menge

$$\mathrm{Sol}^\Phi(M) := \{x \in M \mid \Phi(x) = x\}$$

heißt **Lösungsraum** von (M, Φ).
Für einen Frobenius-Ring (E, ϕ_E) mit $E \geq R$ und $\phi_E|_R = \phi = \phi_R$ wird der Modul $M_E := E \otimes_R M$ zu einem Frobenius-Modul über E mit fortgesetzter Frobenius-Operation $\Phi_E = \phi_E \otimes \Phi$. Die Menge

$$\mathrm{Sol}_E^{\Phi}(M) := \mathrm{Sol}^{\Phi_E}(E \otimes_R M) = (E \otimes_R M)^{\Phi_E} = \{x \in E \otimes_R M \mid \Phi_E(x) = x\}$$

heißt **Lösungsraum** von M über E. Der Modul M heißt **trivial** über E, falls $\mathrm{Sol}_E^{\Phi}(M)$ eine E-Basis von M_E enthält. In diesem Fall heißt E **Lösungsring** des Frobenius-Moduls M.

Satz 1.3. *Es sei R ein gewöhnlicher Frobenius-Ring. Ferner sei (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R mit $\dim_F(M) := n$. Dann gelten:*
(a) Für jede Frobenius-Körpererweiterung (E, ϕ_E) von F ist der Lösungsraum $\mathrm{Sol}_E^{\Phi}(M)$ ein F^{ϕ}-Vektorraum der Dimension

$$\dim_{F^{\phi}}(\mathrm{Sol}_E^{\Phi}(M)) \leq \dim_E(E \otimes_F M) = n.$$

(b) Es existiert eine endliche Frobenius-Körpererweiterung E/F mit

$$\dim_{F^{\phi}}(\mathrm{Sol}_E^{\Phi}(M)) = n.$$

(c) Die minimale Frobenius-Körpererweiterung E/F mit $\dim_{F^{\phi}}(\mathrm{Sol}_E^{\Phi}(M)) = n$ ist (in einer gegeben algebraisch abgeschlossenen Hülle von F) eindeutig bestimmt und galoissch über F.

Beweis. Offensichtlich ist $\mathrm{Sol}_E^{\Phi}(M)$ ein F^{ϕ}-Vektorraum. Nehmen wir $\dim_{F^{\phi}}(\mathrm{Sol}_E^{\Phi}(M))$ echt größer n an, so existiert eine Menge Elemente $\{x_i \in \mathrm{Sol}_E^{\Phi}(M) \mid i = 1, \ldots, k\}$ mit k minimal, die linear unabhängig über F^{ϕ} aber linear abhängig über E ist. Daraus erhalten wir eine nicht-triviale Relation $x_1 = \sum_{i=2}^{k} a_i x_i$ mit $a_i \in E$, wobei wir ohne Einschränkung $a_1 \neq 0$ annehmen. Wendet man darauf ϕ an, so erhält man $x_1 = \sum_{i=2}^{k} \phi(a_i) x_i$. Subtraktion der beiden Gleichungen liefert eine nicht-triviale Relation der $x_2, \ldots, x_k$ über E. Dies steht im Widerspruch zur Annahme, dass k minimal gewählt war.
Um (b) zu zeigen, wählen wir eine Basis $B = \{b_1, \ldots, b_n\}$ von M. Durch $\Phi(b_j) = \sum_{i=1}^{n} d_{ij} b_i$ mit $d_{ij} \in F$ erhalten wir eine Darstellungsmatrix $D := D_B(\Phi) = (d_{ij})_{i,j=1}^{n} \in F^{n \times n}$ von Φ zur Basis B. Sei nun $B\boldsymbol{y} = \sum_{i=1}^{n} b_i y_i$ mit $\boldsymbol{y} = (y_1, \ldots, y_n)^{tr} \in E^n$ eine Lösung von M über E. Dann gilt

$$B\boldsymbol{y} = \Phi(B\boldsymbol{y}) = \Phi(B)\phi(\boldsymbol{y}) = B \cdot D \cdot \phi(\boldsymbol{y})$$

mit $\phi(\boldsymbol{y}) = (\phi(y_1), \ldots, \phi(y_n))^{tr}$. Diese Gleichung definiert ein System von algebraischen Gleichungen $\boldsymbol{y} - D\phi(\boldsymbol{y}) = 0$ für y_i über F. Nach dem Satz von Bézout hat dieses System höchstens q^n verschiedene Lösungen in einer algebraisch abgeschlossenen Hülle $\overline{F}$ von F.

Alle Lösungen sind einfach, da die Jaocbi-Matrix $\mathrm{J} = \left(\frac{\partial y_i}{\partial y_k}\right)_{i,k=1}^{n}$ die Einheitsmatrix ist, denn es gilt

$$\begin{aligned}\frac{\partial y_i}{\partial y_k} &= 1 \text{ , für } i = k \text{ und sonst}\\ \frac{\partial y_i}{\partial y_k} &= \frac{\partial(\sum_{j=1}^{n} d_{ij}\phi(y_j))}{\partial y_k} = \frac{\partial(\sum_{j=1}^{n} d_{ij} y_j^q)}{\partial y_k} = d_{ik}\cdot q\cdot y_k^{q-1} = d_{ik}\cdot p\cdot p^{d-1}\cdot y_k^{q-1} = 0.\end{aligned}$$

Der Körper E/F, der von diesen Lösungen erzeugt wird, hat die gewünschten Eigenschaften.
E ist minimal in $\overline{F}$ und hängt nicht von der Wahl der Basis ab. Da alle Nullstellen von $\boldsymbol{y} - D\phi(\boldsymbol{y}) = 0$ einfach sind, ist E/F separabel und normal, also galoissch. □

Anmerkung 1.4. Die Gleichung $\boldsymbol{y} - D\phi(\boldsymbol{y}) = 0$ aus dem Beweis zu Satz 1.3 ist äquivalent zu der Differenzengleichung (vgl. Definition 1.21) $\phi(\boldsymbol{y}) = A\boldsymbol{y}$ mit $A := D_B(\Phi)^{-1} \in \mathrm{GL}_n(F)$.

Korollar 1.5. *Unter den Voraussetzungen von Satz 1.3 existiert eine Matrix $Y = (y_{ij})_{i,j=1}^{n}$ in $\mathrm{GL}_n(E)$ mit $\phi_E(Y) = AY$ und E wird über F von den Einträgen von Y erzeugt, d.h. es gilt $E = F(y_{ij} \mid i,j = 1,\ldots,n)$.*

Definition 1.6. Eine Matrix $Y = (y_{ij})_{i,j=1}^{n} \in \mathrm{GL}_n(E)$ wie in Korollar 1.5 mit der Eigenschaft $\phi_E(Y) = AY$ heißt **Fundamental-Matrix** von (M,Φ).

Bemerkung 1.7. *Es sei R ein gewöhnlicher Frobenius-Ring mit Quotientenkörper $F := \mathrm{Quot}(R)$ und Lösungskörper E zum Frobenius-Modul (M,Φ) über F. Dann unterscheiden sich zwei Fundamental-Matrizen Y_1 und Y_2 von M nur durch Multiplikation mit einer Matrix $C \in \mathrm{GL}_n(F^\phi)$, d.h. es gilt*

$$Y_1 = Y_2 C.$$

Beweis. Die durch $C := Y_1^{-1}Y_2$ definierte Matrix existiert, da $Y_1, Y_2 \in \mathrm{GL}_n(E)$ liegen. Um zu zeigen, dass $C \in \mathrm{GL}_m(F^\phi)$ liegt, wenden wir ϕ auf C an und erhalten durch

$$\phi(C) = \phi(Y_1^{-1}Y_2) = \phi(Y_1)^{-1}\phi(Y_2) = Y_1^{-1}A^{-1}AY_2 = Y_1^{-1}Y_2 = C$$

die Behauptung. □

1.2 Lösungsringe für relative Frobenius-Moduln

Um die Existenz minimaler Lösungsringe von Frobenius-Moduln zu beweisen, benötigen wir einige grundlegende Kenntnisse über algebraische Funktionenkörper. Diese wollen wir nun kurz zusammentragen.
Wir bezeichnen mit $\mathbb{P}$ die Menge aller Primdivisoren bzw. Stellen eines algebraischen Funktionenkörpers F einer Variablen mit Konstantenkörper K. Mit $v_\mathfrak{p}$ bezeichnen wir die zu einer solchen Stelle $\mathfrak{p} \in \mathbb{P}$ gehörige Bewertung mit Bewertungsring

$$\begin{aligned}\mathcal{O}_\mathfrak{p} &= \{x \in F \mid v_\mathfrak{p}(x) \geq 0\} \text{ bzw. Bewertungsideal}\\ \mathfrak{p} &= \{x \in F \mid v_\mathfrak{p}(x) > 0\}\end{aligned}$$

und Restklassenkörper $R_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$.

Definition 1.8. Eine Primstelle $\mathfrak{p} \in \mathbb{P}$ eines algebraischen Funktionenkörpers F/K vom Grad $\deg(\mathfrak{p}) = [R_{\mathfrak{p}} : K] = 1$ heißt **rationale Stelle** bzw. **rationaler Punkt**.

Es sei R ein relativer Frobenius-Ring mit definierendem Bewertungsideal $Q \trianglelefteq R$. Wir setzen R als Integritätsbereich voraus. Damit bildet Q nach dem Erweiterungssatz von Chevalley (siehe [EP05] Theorem 3.1.1) ein Bewertungsideal in $\mathrm{Quot}(R)$. Dann wird die Vervollständigung (R_Q, ϕ) von R bezüglich Q ein Hensel'scher Integritätsbereich mit stetig fortgesetztem Frobenius-Endomorphismus. Wir bezeichnen mit $(R_Q^{\mathrm{ur}}, \phi^{\mathrm{ur}})$ die ganz abgeschlossene Hülle in einer maximal unverzweigten algebraischen Erweiterung von $\mathrm{Quot}(R_Q)$ mit der eindeutigen Fortsetzung ϕ^{ur} von ϕ, die mit dem gewöhnlichen Frobenius-Endomorphismus auf dem Restklassenring $R_Q^{\mathrm{ur}}/(Q)$ verträglich ist. Also ist die Vervollständigung $(\hat{R}_Q^{\mathrm{ur}}, \hat{\phi})$ von R_Q^{ur} bezüglich $(Q) \trianglelefteq R_Q^{\mathrm{ur}}$ wieder ein Hensel'scher Integritätsbereich mit stetig fortgesetzter Frobenius-Operation. Daher erzeugt Q nicht nur ein Ideal in R, sondern auch in R_Q, R_Q^{ur} und $\hat{R}_Q^{\mathrm{ur}}$ und diese sind auch Bewertungsideale.

Satz 1.9. ***(Matzat)*** *Es sei (R, ϕ) ein relativer Frobenius-Integritätsbereich, dessen definierendes Ideal Q ein Bewertungsideal in $\mathrm{Quot}(R)$ bildet und (M, Φ) ein Frobenius-Modul über (R, ϕ). Dann besitzt M einen minimalen Lösungsring in $(\hat{R}_Q^{\mathrm{ur}}, \hat{\phi})$.*

Beweis. Wir nehmen an, dass $Q = (r)$ eine diskrete Bewertung induziert, da der nichtdiskrete Fall für unsere Anwendungen nicht relevant ist. Wir bezeichnen mit $D := D_B(\Phi) \in \mathrm{GL}_n(R)$ die Darstellungsmatrix von Φ bezüglich einer Basis B von M und deren Inverse mit $A := D^{-1}$. Die Restklassenmatrix $\overline{A} \mod r$ liegt in $\mathrm{GL}_n(\overline{R})$, wobei $\overline{R} := R/Q$ den Restklassenkörper bezeichnet. Durch die Surjektivität der Lang-Isogenie

$$\pi : \mathrm{GL}_n(\overline{R}^{sep}) \longrightarrow \mathrm{GL}_n(\overline{R}^{sep})$$

erhalten wir eine Matrix $\overline{D}_0 \in \mathrm{GL}_n(\overline{R}^{sep})$ mit $\overline{A} = \overline{\phi}(\overline{D}_0)\overline{D}_0^{-1}$. Genauer gesagt liegen die Einträge von $\overline{D}_0$ in einer endlichen Erweiterung $\overline{R}_0/\overline{R}$. Daher existiert eine unverzweigte Ringerweiterung mit geliftetem Frobenius-Endomorphismus $(\tilde{R}_0, \phi_{\tilde{R}_0})$ von endlichem Grad über (R, ϕ) und eine Matrix $D_0 \in \mathrm{GL}_n(\tilde{R}_0)$, so dass gilt

$$A = \phi_{\tilde{R}_0}(D_0)(I + rG_0)D_0^{-1} \text{ mit } G_0 \in \tilde{R}_0^{n\times n}.$$

Wir wollen nun die daraus resultierende Kongruenz $A \equiv \phi_{\tilde{R}_0}(D_0)D_0^{-1} \mod r$ noch weiter verfeinern, nämlich modulo höherer Potenzen von r. Der nächste Approximationsschritt mit $D_1 = I + rH_1$ und $\phi(r) = er$ würde zu einer Kongruenz der Form

$$\begin{aligned} I + rG_0 &\equiv \phi_{\tilde{R}_1}(D_1)(I + r^2G_1)D_1^{-1} \\ &\equiv (I + \phi_{\tilde{R}1}(rH_1))(I - rH_1) \\ &\equiv I + er\phi_{\tilde{R}_1}(H_1) - rH_1 \mod r^2. \end{aligned}$$

führen. Da die reduzierte Gleichung $\overline{G}_0 = \overline{e}\overline{\phi}_{\overline{R}_1}(\overline{H}_1) - \overline{H}_1$ eine Lösungsmatrix $\overline{H}_1$ über einer endlichen Erweiterung $\overline{R}_1/\overline{R}_0$ besitzt, existiert eine unverzweigte R-Ringerweiterung $(\tilde{R}_1, \phi_{\tilde{R}_1})$ von endlichem Grad über $(\tilde{R}_0, \phi_{\tilde{R}_0})$ und eine Matrix $D_1 = I + rH_1 \in \mathrm{GL}_n(\tilde{R}_1)$, so dass

$$A = \phi_{\tilde{R}_0}(D_0)\phi_{\tilde{R}_1}(D_1)(I + r^2G_1)D_1^{-1}D_0^{-1} \text{ mit } G_1 \in \tilde{R}_1^{n\times n}$$

gilt. Durch Induktion erhalten wir einen Turm von unverzweigten Ringerweiterungen $R \leq \tilde{R}_0 \leq \tilde{R}_1 \leq \cdots \leq \tilde{R}_l$ innerhalb von $\hat{R}_Q^{\mathrm{ur}}$ und Matrizen $D_l \in \mathrm{GL}_n(\tilde{R}_l)$ mit

$$A \equiv \phi_{\tilde{R}_0}(D_0) \cdots \phi_{\tilde{R}_l}(D_l) D_l^{-1} \cdots D_0^{-1} \mod r^{l+1}.$$

Da $D_l = I + r^l H_l \in \mathrm{GL}_n(\hat{R}_Q^{\mathrm{ur}})$ liegt, konvergiert das Produkt $D_0 \cdots D_l$ in $\mathrm{GL}_n(\hat{R}_Q^{\mathrm{ur}})$. Daher existiert eine Matrix $Y \in \mathrm{GL}_n(\hat{R}_Q^{\mathrm{ur}})$ mit $A = \phi(Y)Y^{-1}$, also nach Definition eine Fundamentalmatrix von (M, Φ).

□

Anmerkung 1.10. Ein minimaler Lösungsring wie in Satz 1.9 kann im Allgemeinen Nullteiler enthalten (siehe [vdPM97, Example 1.6]) und ist nur dann bis auf Isomorphie eindeutig bestimmt, wenn der Grundring ein algebraisch abgeschlossener Körper ist (vgl. [vdPM97, Theorem 1.8]).

Korollar 1.11. *Es sei (R, ϕ) ein Frobenius-Ring mit Quotientenkörper $F := \mathrm{Quot}(R)$. Ein Erweiterungskörper E/F ist Lösungskörper des Frobenius-Moduls (M, Φ) über F, falls die beiden folgenden Bedingungen erfüllt sind:*
(a) Es existiert eine Fundamentalmatrix $Y \in \mathrm{GL}_n(E)$.
(b) E/F wird von den Einträgen von Y erzeugt, d.h. $E = F(Y)$.

Definition 1.12. Es sei (R, ϕ) ein Frobenius-Ring und (M, Φ) ein Frobenius-Modul über R. Ein Frobenius-Ring (E, ϕ_E) mit $E \geq R$ und $\phi_E|_R = \phi$ heißt **Picard-Vessiot-Ring** oder kurz ein **PV-Ring**, falls die beiden folgenden Bedingungen erfüllt sind:

(*i*) E ist ein minimaler Lösungsring von M.

(*ii*) Die ϕ-Invarianten von E stimmen mit den ϕ-Invarianten von R überein, d.h. es gilt $E^\phi = R^\phi$.

Anmerkung 1.13. Ein minimaler Lösungsring existiert nach Satz 1.9, falls der zugrundeliegende Frobenius-Ring ein Integritätsbereich ist. Es können allerdings beim Übergang zu $(\hat{R}_Q^{\mathrm{ur}}, \hat{\phi})$ neue ϕ-Invarianten auftreten. Setzten wir aber die Existenz einer rationalen, für den Modul M regulären Stelle (vgl. Definition 1.8 bzw. [Mat09b, Chap. 5.2]) voraus, so kommen beim Übergang von R zu $(\hat{R}_Q^{\mathrm{ur}}, \hat{\phi})$ keine neuen ϕ-Invarianten hinzu und somit existiert in diesem Fall sogar ein PV-Ring. Dies ist in unseren Anwendungsbeispielen ($\mathbb{F}_q(s,t)$ rationaler Funktionenkörper) immer gewährleistet und daher wollen wir von nun an immer implizit die Existenz einer solchen Stelle voraussetzen, wenn wir die Existenz eines PV-Rings bzw. PV-Körpers benötigen.

Satz 1.14. *Es sei R ein relativer Frobenius-Ring. Ferner sei (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R mit $\dim_F(M) := n$. Dann gelten:*
(a) Für jede Frobenius-Körpererweiterung (E, ϕ_E) von F ist der Lösungsraum $\mathrm{Sol}_E^\Phi(M)$ ein E^ϕ-Vektorraum der Dimension

$$\dim_{E^\phi}(\mathrm{Sol}_E^\Phi(M)) \leq \dim_E(E \otimes_F M) = n.$$

(b) Es gilt Gleichheit, falls eine Fundamentalmatrix in $\mathrm{GL}_m(E)$ für (M, Φ) existiert.
(c) Zwei Fundamentalmatrizen Y_1, Y_2 unterscheiden sich nur durch Multiplikation mit einer Matrix $C \in \mathrm{GL}_n(F^\phi)$, d.h. es gilt $Y_1 = Y_2 C$.

Beweis. Die Beweise verlaufen völlig analog zu den Beweisen aus Abschnitt 1.1 mit einem gewöhnlichen Frobenius-Ring R. □

1.3 Die Galoisgruppe eines Frobenius-Modul

Definition 1.15. Es sei R ein Frobenius-Ring. Ferner sei (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R und E ein PV-Körper von M. Wir definieren durch

$$\mathrm{Aut}^{\Phi}(M) = \{\sigma \in \mathrm{Aut}(E/F) \,|\, \sigma(\phi(x)) = \phi(\sigma(x)) \text{ für alle } x \in E\}$$

die **Frobenius-Automorphismengruppe** des Frobenius-Moduls M.
Außerdem definieren wir das **Galoisgruppenschema** als Funktor von der Kategorie der F^{ϕ}-Algebren in die Kategorie der Gruppen

$$\begin{array}{rccc} \underline{\mathrm{Aut}}^{\Phi}(E/F): & F^{\phi}\text{-Alg} & \longrightarrow & \text{Gruppen} \\ & A & \longmapsto & \mathrm{Aut}^{\Phi}(E \otimes_{F^{\phi}} A / F \otimes_{F^{\phi}} A) \end{array}.$$

Dieser wird über F^{ϕ} durch die F^{ϕ}-Algebra $(E \otimes_F E)^{\phi_E \otimes \phi_E}$ dargestellt. Das zugehörige affine Gruppenschema bezeichnen wir mit $\mathcal{G}^{\Phi} = \underline{\mathrm{Gal}}^{\Phi}(E/F)$ und nennen dies das **Frobenius-Galoisgruppenschema**.

Anmerkung 1.16. In unseren Anwendungsbeispielen liegt die Gruppe der rationalen Punkte

$$\mathrm{Gal}^{\Phi}(E/F) := \mathcal{G}^{\Phi}_{F^{\phi}}(F^{\phi}) = \mathrm{Aut}^{\Phi}(E/F)$$

des Frobenius-Galoisgruppenschemas $\underline{\mathrm{Gal}}^{\Phi}(E/F) = \mathcal{G}^{\Phi}$ Zariski-dicht. Dies impliziert $F = E^{\mathrm{Gal}^{\Phi}(E/F)}$. Also wird $\mathrm{Gal}^{\Phi}(E/F)$ die **Φ-Galoisgruppe** von E/F und $\underline{\mathrm{Gal}}^{\Phi}(E/F)$ ist durch $\mathrm{Gal}^{\Phi}(E/F)$ eindeutig bestimmt. Daher können wir der Einfachheit halber ab sofort mit der Frobenius Galoisgruppe $\mathrm{Gal}^{\Phi}(M) := \mathrm{Gal}^{\Phi}(E/F)$ selbst arbeiten anstatt mit dem darunterliegenden Gruppenschema.

Bemerkung 1.17. *Es sei R ein Frobenius-Ring. Ferner sei (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R und E ein PV-Körper von M. Dann lässt sich die zugehörige Galoisgruppe $\mathrm{Gal}^{\Phi}(M)$ injektiv in die $\mathrm{GL}_n(F^{\phi})$ einbetten.*

Beweis. Da E ein Lösungskörper von M ist, existiert eine Fundamentalmatrix $Y \in \mathrm{GL}_n(E)$. Da alle $\sigma \in \mathrm{Gal}^{\Phi}(M)$ mit ϕ verträglich sind, ist auch $\sigma(Y)$ eine Fundamentalmatrix. Nach Satz 1.14 (c) existiert eine Matrix $C_\sigma \in \mathrm{GL}_n(F^{\phi})$ mit $\sigma(Y) = YC_\sigma$. Daher definiert die Abbildung

$$\Psi : \mathrm{Gal}^{\Phi}(M) \longrightarrow \mathrm{GL}_n(F^{\phi}),\ \sigma \longmapsto C_\sigma$$

eine lineare Darstellung. Es bleibt nur noch zu zeigen, dass Ψ injektiv ist. Dazu wählen wir ein $\gamma \in \mathrm{Kern}(\Psi)$, d.h. es gilt $\Psi(\gamma) = C_\gamma = \mathrm{id}$. Damit operiert γ trivial auf $F(Y)$, denn Y ist invariant unter γ. Da aber E als Lösungskörper von M durch die Einträge von Y über F erzeugt wird, operiert $\gamma = \mathrm{id}_E$ trivial auf E, d.h. Ψ ist injektiv. Damit erhalten wir die Behauptung $\mathrm{Gal}^{\Phi}(M) \simeq \mathrm{Bild}(\Psi) \leq \mathrm{GL}_n(F^{\phi})$. □

Satz 1.18. *Es sei R ein Frobenius-Ring und (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R, sowie E ein PV-Körper von M. Ferner sei $\mathcal{G}$ eine reduzierte zusammenhängende lineare Gruppe über F^{ϕ}. Falls eine Basis B von M mit $D := D_B(\Phi) \in \mathcal{G}(F)$ existiert, so gilt für die Galoisgruppe*

$$\mathrm{Gal}^{\Phi}(M) \leq \mathcal{G}(F^{\phi}).$$

Beweis. Die Abbildung

$$\pi : \mathcal{G}(F^{sep}) \longrightarrow \mathcal{G}(F^{sep}),\ (x_{ij})_{i,j=1}^{n} \longmapsto \phi(x_{ij})(x_{ij})^{-1}$$

ist surjektiv nach einem Satz von S. Lang (vgl. [Spr98, Theorem 4.4.17]). Daher existiert ein Element $Y \in \mathcal{G}(F^{sep})$ mit $\phi(Y)Y^{-1} = D^{-1}$. Nach Satz 1.14 ist $F(Y)$ ein Lösungskörper von M, d.h. für jedes $\sigma \in \mathrm{Gal}^{\Phi}(M)$ gilt $C_\sigma = Y^{-1}\sigma(Y) \in \mathcal{G}(E) \cap \mathrm{GL}_m(F^{\phi})$, also $C_\sigma \in \mathcal{G}(F^{\phi})$. □

Definition 1.19. Es sei R ein Frobenius-Ring. Ferner sei (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R mit PV-Körper E und Galoisgruppenschema $\underline{\mathrm{Aut}}^{\Phi}(E/F)$ gemäß Definition 1.15. Für eine R-Algebra S sei $\mathcal{H}/R$ ein Untergruppenfunktor des Funktors $\underline{\mathrm{Aut}}^{\Phi}(S/R)$, d.h. für jede R-Algebra L ist die Menge der L-rationalen Punkte $\mathcal{H}(L)$ eine Gruppe und operiert funktoriell auf $S_L := S \otimes_R L$. Ein Element $s \in S$ heißt **invariant**, falls das Element $s \otimes 1 \in S_L$ für alle L invariant unter $\mathcal{H}(L)$ ist. Wir bezeichnen den Invariantenring mit $S^{\mathcal{H}}$. Ein Element $\frac{r}{s} \in E_S := \mathrm{Quot}(S)$ heißt **invariant** unter $\mathcal{H}$, falls

$$h.(r \otimes 1) \cdot (s \otimes 1) = (r \otimes 1) \cdot h.(s \otimes 1) \in S_L = S \otimes_R L$$

für alle R-Algebren L und für jedes Element $h \in \mathcal{H}(L)$ gilt. Wir bezeichnen den Invariantenkörper mit $E_S^{\mathcal{H}}$. Es läßt sich leicht nachprüfen, dass diese Definition eines invarianten Elements $e \in E_S$ unabhängig von der Vertreterwahl $\frac{r}{s}$ ist.

Satz 1.20. *(Galoiskorrespondenz)*
Es sei R ein Frobenius-Ring und (M, Φ) ein Frobenius-Modul über dem Quotientenkörper $(F := \mathrm{Quot}(R), \phi)$ von R, E ein PV-Körper von M und $\mathcal{G}$ das zugehörige Galoisgruppen-Schema. Ferner bezeichnen wir mit

$$\mathcal{K} := \{(K, \phi_K)\ \textit{Frobenius-Körper}\ \mid F \leq K \leq E,\ \textit{mit } E/K\ \textit{separabel}\ \}$$

die Menge aller Frobenius-Zwischenkörper und mit

$$\mathcal{H} := \{H \leq \mathcal{G} \mid H\ \textit{reduziertes Untergruppen-Schema}\ \}$$

die Menge aller reduzierten Untergruppen-Schemata von $\mathcal{G}$. Dann gelten:
(a) Für jeden Körper $K \in \mathcal{K}$ ist $\underline{\mathrm{Gal}}^{\Phi}(E/K)$ ein reduziertes Untergruppen-Schema von G.
(b) Für jedes reduzierte Gruppen-Schema $H \in \mathcal{H}$ liegen die H-Invarianten E^H (vgl. Definition 1.19) in $\mathcal{K}$.
(c) Die beiden Abbildungen

$$\begin{array}{rccc} \alpha: & \mathcal{K} & \longrightarrow & \mathcal{H} \\ & K & \longmapsto & \underline{\mathrm{Gal}}^{\Phi}(E/K) \end{array}$$

und

$$\begin{array}{rccc} \beta: & \mathcal{H} & \longrightarrow & \mathcal{K} \\ & H & \longmapsto & E^H \end{array}$$

sind zueinander invers.

Beweis. Diese Galoiskorrespondenz folgt aus der allgemeinen Korrespondenz in [AM05, Theorem 3.9]. □

1.4 Differenzengleichungen über Frobenius-Körpern

Definition 1.21. Es sei (R, ϕ) ein relativer Frobenius-Ring mit definierendem Ideal Q und $F := \mathrm{Quot}(R)$ der Quotientenkörper von R. Eine Gleichung der Form $L(y) = 0$ mit

$$L(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i \phi^i(y) \text{ mit } a_i \in F$$

heißt **Differenzengleichung (oder ϕ-Gleichung) vom Grad n über F**. Eine Gleichung der Form

$$\phi(\boldsymbol{y}) = A\boldsymbol{y} \text{ mit } A \in \mathrm{GL}_n(F)$$

heißt **Matrix-Differenzengleichung vom Grad n über F**.

Anmerkung 1.22. Durch die Abbildung $y \to \boldsymbol{y} := (y, \phi(y), \phi^2(y), \ldots, \phi^{n-1}(y))^{tr}$ erhalten wir die zu L **assoziierte Matrixgleichung**

$$\phi(\boldsymbol{y}) = A_L \cdot \boldsymbol{y} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix} \cdot \boldsymbol{y}.$$

Diese induziert einen Frobenius-Modul M_L via $D_B(\Phi)^{-1} := A_L$ mit Lösungskörper E gemäß Satz 1.9, Galoisgruppe $G := \mathrm{Gal}(L) := \mathrm{Gal}^{\Phi}(M_L)$ und Lösungsraum $V := \mathrm{Sol}_E^{\Phi}(M_L)$.

Satz 1.23. *Es sei $L(y) = 0$ eine Differenzengleichung vom Grad n über einem Frobenius-Körper $(F := \mathrm{Quot}(R), \phi)$ mit zugehöriger Galoisgruppe $G := \mathrm{Gal}(L)$, wobei R ein relativer Frobenius-Ring mit definierendem Ideal Q ist. Dann sind äquivalent:*
(a) Es existieren $L_{n-m}(y), L_m(y)$ vom Grad $n-m$ bzw. m über F, so dass $L(y) = L_{n-m}(L_m(y))$ ist.
(b) Es existiert ein m-dimensionaler G-invarianter Untervektorraum $W \leq V = \mathrm{Sol}_E^{\Phi}(M_L)$, d.h. mit $\sigma(W) \subseteq W$ für alle $\sigma \in G$.

Um diesen Satz zu beweisen benötigen wir die folgende Definition sowie zwei kleine Lemmata.

Definition 1.24. Es sei (R, ϕ) ein Frobenius-Ring und $y_1, \ldots, y_r \in R$ Ringelemente. Die durch

$$\mathrm{M}(y_1, \ldots, y_r) := \begin{pmatrix} y_1 & \cdots & y_r \\ \phi(y_1) & \cdots & \phi(y_r) \\ \vdots & \ddots & \vdots \\ \phi^{r-1}(y_1) & \cdots & \phi^{r-1}(y_r) \end{pmatrix}$$

definierte Matrix heißt **Moore-Matrix** bezüglich ϕ. Ihre Determinante

$$\Delta_\phi(y_1, \ldots, y_r) := \det(\mathrm{M}(y_1, \ldots, y_r))$$

nennen wir die **Moore-Determinante**.

Lemma 1.25. *Es sei $\phi(y) = A \cdot y$ eine Matrix-Differenzengleichung vom Grad n über einem Frobenius-Körper F. Ferner sei M der zugehörige Frobenius-Modul und $v_1, \ldots, v_r \in V = \mathrm{Sol}_E^\Phi(M)$ Lösungen der Gleichung, d.h. es gilt $\phi(v_i) = A \cdot v_i$ für alle $i = 1, \ldots, r$. Dann sind die v_i genau dann linear abhängig über F, wenn sie linear abhängig über F^ϕ sind.*

Beweis. Falls die v_i linear abhängig über F^ϕ sind, sind sie offensichtlich auch linear abhängig über F. Also gehen wir davon aus, dass die v_i linear abhängig über F sind und wollen nun durch Induktion nach r beweisen, dass sie auch abhängig über F^ϕ sind. Für $r = 1$ ist die Aussage trivial. Sei also $r > 1$ und $v_1, \ldots, v_r$ linear abhängig über F, aber jede echte Teilmenge von $\{v_1, \ldots, v_r\}$ linear unabhängig. Wir können also ohne Einschränkung v_1 als F-Linearkombination der anderen v_i darstellen, d.h. es existieren $a_i \in F$ für $i = 2, \ldots r$, so dass $v_1 = \sum_{i=2}^{r} a_i v_i$ gilt. Damit erhalten wir die folgende Gleichungskette:

$$\begin{aligned} 0 &= \phi(v_1) - A \cdot v_1 = \phi\left(\sum_{i=2}^{r} a_i v_i\right) - A \cdot \left(\sum_{i=2}^{r} a_i v_i\right) \\ &= \sum_{i=2}^{r} \phi(a_i)\phi(v_i) - a_i \cdot A \cdot v_i = \sum_{i=2}^{r} \phi(a_i) \cdot A \cdot v_i - a_i \cdot A \cdot v_i \\ &= \sum_{i=2}^{r} (\phi(a_i) - a_i) \cdot A \cdot v_i. \end{aligned}$$

Da $v_2, \ldots, v_r$ linear unabhängig über F sind, muss also $\phi(a_i) = a_i$ und damit $a_i \in F^\phi$ für alle $i = 2, \ldots, r$ gelten. Also sind $v_1, \ldots, v_r$ linear abhängig über F^ϕ. □

Lemma 1.26. *Die Elemente $y_1, \ldots, y_n \in F$ eines Frobenius-Körpers F sind genau dann linear unabhängig über F^ϕ, wenn $\Delta_\phi(y_1, \ldots, y_n) = 0$ gilt.*

Beweis. Zunächst ist klar, dass $\Delta_\phi(y_1, \ldots, y_n) = 0$ genau dann gilt, wenn $y_1, \ldots, y_n$ linear unabhängig über F sind. Und dies ist nach Lemma 1.25 genau dann der Fall, wenn $L(y)$ mit $L(y_i) = 0$ für alle $i = 1, \ldots, n$ existiert. Also konstruieren wir eine solche Gleichung induktiv:

$$\begin{aligned} L_1(y) &:= \phi(y) - \frac{\phi(y_1)}{y_1} y, \\ L_2(y) &:= \phi(L_1(y)) - \frac{\phi(L_1(y_2))}{L_1(y_2)} L_1(y), \\ &\vdots \\ L_n(y) &:= \phi(L_{n-1}(y)) - \frac{\phi(L_{n-1}(y_n))}{L_{n-1}(y_n)} L_{n-1}(y). \end{aligned}$$

Alle y_i für $i = 1, \ldots, n$ sind Lösungen der Differenzengleichung $L(y) := L_n(y) = 0$, d.h. es gilt $L(y_i) = 0$. Betrachten wir die zu L assoziierte Matrix-Differenzengleichung $\phi(\boldsymbol{y}) = A_L \cdot \boldsymbol{y}$, so gilt ebenfalls $\phi(\boldsymbol{y}_i) = A_L \boldsymbol{y}_i$, d.h. die $\boldsymbol{y}_i$ liegen in $\mathrm{Sol}_E^\Phi(M_L)$. Die Behauptung folgt jetzt unter Verwendung von Lemma 1.25. □

Beweis zu Satz 1.23.
Wir setzen zunächst voraus, dass $L_{n-m}(y), L_m(y)$ mit $L(y) = L_{n-m}(L_m(y))$ existieren. Dann existiert nach Satz 1.9 ein Lösungskörper $\tilde{E} \leq E$ mit $W := \mathrm{Sol}^{\Phi}_{\tilde{E}}(M_{L_m})$. Damit gilt $\dim_{F^\phi}(W) = \dim_F(M_{L_m}) = m$ nach Satz 1.14. Für alle $w \in W$ und $\sigma \in G$ gilt dann

$$L_m(\sigma(w)) = \sigma(L_m(w)) = \sigma(0) = 0.$$

Also liegt für jedes Element $w \in W$ auch $\sigma(w) \in W$ für alle $\sigma \in G$, d.h. es gilt $\sigma(W) \subseteq W$ für alle $\sigma \in G$.
Sei nun umgekehrt ein G-invarianter Untervektorraum $W \leq V = \mathrm{Sol}^{\Phi}_E(M_L)$ der Dimension $\dim_{F^\phi}(W) = m < n$ gegeben. Dann wählen wir ein geeignetes Fundamentalsystem von Lösungen $\eta_1, \ldots, \eta_n$ von L, so dass jedes Element σ der Galoisgruppe G die folgende Gestalt hat:

$$\begin{pmatrix} B_1 & * \\ 0 & B_2 \end{pmatrix},$$

wobei B_1, B_2 Blockmatrizen der Größe m bzw. $n-m$ sind. Also wird der Untervektorraum W über F^ϕ von den Lösungen $\eta_1, \ldots, \eta_m$ erzeugt. Wir definieren die Differenzengleichung

$$L_m(y) := \frac{\Delta_\phi(y, \eta_1, \ldots, \eta_m)}{\Delta_\phi(\eta_1, \ldots, \eta_m)}.$$

Durch Laplace-Entwicklung nach der ersten Spalte der oberen Determinante ergibt sich für $L_m(y)$ folgende Gestalt:

$$\begin{aligned} L_m(y) = \phi^m(y) \quad &+ \underbrace{\frac{\det \begin{pmatrix} \eta_1 & \cdots & \eta_m \\ \vdots & \ddots & \vdots \\ \phi^{m-2}(\eta_1) & \cdots & \phi^{m-2}(\eta_m) \\ \phi^m(\eta_1) & \cdots & \phi^m(\eta_m) \end{pmatrix}}{\Delta_\phi(\eta_1, \ldots, \eta_m)}}_{:= a_{m-1}} \phi^{m-1}(y) \\ &+ \quad \cdots \\ &+ \underbrace{\frac{\Delta_\phi(\phi(\eta_1), \ldots, \phi(\eta_m))}{\Delta_\phi(\eta_1, \ldots, \eta_m)}}_{:= a_0} y. \end{aligned}$$

Da W ein G-invarianter Unterraum ist, werden die ersten m der η_i von G permutiert, d.h. für jedes $i \in \{1, \ldots, m\}$ existiert ein $j \in \{1, \ldots, m\}$ mit $\sigma(\eta_i) = \eta_j$ für alle $\sigma \in G$. Damit gilt aber $\sigma(a_i) = a_i$ für die Koeffizienten von $L_m(y)$, d.h. für jeden Index $1 \leq i \leq m$ liegt a_i in F. Da alle η_i für $i = 1, \ldots, m$ nach Lemma 1.26 Lösungen von $L_m(y)$ sind, ist W der Lösungsraum von L_m. Außerdem ist L_m nach Konstruktion minimal. Dies liefert $L(y) = L_{n-m}(L_m(y))$ und damit die Behauptung. □

1.5 Lösungen von Differenzengleichungen

Definition 1.27. Es sei (R, ϕ) ein relativer Frobenius-Ring mit definierendem Ideal Q und $F := \mathrm{Quot}(R)$ der Quotientenkörper von R. Ein Frobeniuskörper (K, ϕ_K) mit $K \geq F$ und

$\phi_K|_F = \phi_F$ heißt **ϕ-Liouville-Erweiterung**, falls ein Körperturm

$$F = K_0 \leq K_1 \leq \ldots \leq K_n = K$$

mit $K_i = K_{i-1}(t_i)$ für $i = 1, \ldots, n$ existiert und eine der folgenden Bedingungen erfüllt ist:

- $\phi(t_i) - t_i \in K_{i-1}$,
- $t_i \neq 0$ und $\frac{\phi(t_i)}{t_i} \in K_{i-1}$,
- t_i ist algebraisch über K_{i-1}.

Definition 1.28. Es sei $L(y) = 0$ eine Differenzengleichung vom Grad n über einem Frobenius-Körper $(F := \mathrm{Quot}(R), \phi)$ mit PV-Körper E und zugehöriger Galoisgruppe $G := \mathrm{Gal}(L)$, wobei R ein relativer Frobenius-Ring mit definierendem Ideal Q ist. Eine Lösung $\eta \in E$ mit $L(\eta) = 0$ heißt

- **rational**, falls $\eta \in F$ liegt.
- **ϕ-additiv**, falls $\phi(\eta) - \eta \in F$ liegt.
- **ϕ-exponentiell**, falls $\frac{\phi(\eta)}{\eta} \in F$ liegt.
- **algebraisch**, falls η algebraisch über F ist.
- **ϕ-Liouvillesch**, falls η in einem ϕ-Liouvilleschen Teilkörper $K \leq E$ liegt.

Bemerkung 1.29. *Es sei $L(y) = 0$ eine Differenzengleichung über einem Frobenius-Körper $(F := \mathrm{Quot}(R), \phi)$ mit PV-Körper E und zugehöriger Galoisgruppe $G := \mathrm{Gal}(L)$, wobei R ein relativer Frobenius-Ring mit definierendem Ideal Q ist. Weiter sei $\eta \in E \setminus F$ eine algebraische und ϕ-exponentielle Lösung, d.h. es gilt $\frac{\phi(\eta)}{\eta} = u \in F$ mit $u \neq 0$. Dann existiert eine natürliche Zahl $m \in \mathbb{N}$ mit $\eta^m = a \in F$.*

Beweis. Es sei $X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0$ das Minimalpolynom von η über F, d.h. die a_i liegen in F und es gilt

$$\eta^m + a_{m-1}\eta^{m-1} + \ldots + a_1\eta + a_0 = 0.$$

Wenden wir auf diese Gleichung ϕ an, so erhalten wir mit $\phi(\eta) = u\eta$ die Gleichung

$$u^m\eta^m + \phi(a_{m-1})u^{m-1}\eta^{m-1} + \ldots + \phi(a_1)u\eta + \phi(a_0) = 0.$$

Multiplizieren wir andererseits die erste Gleichung mit u^m, ergibt sich

$$u^m\eta^m + a_{m-1}u^m\eta^{m-1} + \ldots + a_1)u^m\eta + a_0u^m = 0.$$

Subtrahieren wir nun diese beiden neuen Gleichungen, erhalten wir

$$b_{m-1}u^{m-1}\eta^{m-1} + b_{m-2}u^{m-2}\eta^{m-2} + \ldots b_1u^m\eta + b_0 = 0$$

mit $b_{m-i} := (\phi(a_{m-i}) - a_{m-i}u^i)$ und damit eine Gleichung vom Grad echt kleiner als m die η annuliert. Da aber die erste Gleichung minimal gewählt war, müssen alle Koeffizienten in der letzten Gleichung gleich 0 sein. Da wir $u \neq 0$ vorausgesetzt haben, muss

$$b_{m-i} = (\phi(a_{m-i}) - a_{m-i}u^i) = 0 \quad \text{für alle } 1 \leq i \leq m$$

gelten. Schreiben wir dies um, ergibt sich

$$\phi(a_{m-i}) = u^i a_{m-i} \quad \text{für alle } 1 \leq i \leq m.$$

Also ist $a_{m-i} \in F$ eine rationale Lösung der Differenzengleichung $\phi(y) = u^i y$ und unterscheidet sich daher nur durch eine Konstante c_i von η^i, d.h. es gilt $\eta^i c_i = a_{m-i}$. Dies steht aber für alle Indizes $1 \leq i < m$ im Widerspruch zur Voraussetzung $\eta \in E \setminus F$. Es gelten also $a_{m-i} = 0$ für alle $1 \leq i < m$ und $\eta^m = a := \frac{a_0}{c_m}$, und damit ist die Aussage bewiesen. □

Satz 1.30. *Es sei $L(y) = 0$ eine Differenzengleichung vom Grad n über einem Frobenius-Körper $(F := \mathrm{Quot}(R), \phi)$ mit PV-Körper E und zugehöriger Galoisgruppe $G := \mathrm{Gal}(L)$, wobei R ein relativer Frobenius-Ring mit definierendem Ideal Q ist. Dann gelten:*
(a) L besitzt genau dann nur algebraische Lösungen, falls $\mathrm{Gal}(L)$ eine endliche Gruppe ist.
(b) Die Zusammenhangskomponente der Eins G° ist eine auflösbare algebraische Gruppe bzgl. der Zariski-Topologie, falls L nur ϕ-Liouvillesche Lösungen besitzt. Die Umkehrung gilt nur, falls F^ϕ algebraisch abgeschlossen ist.
(c) Falls L eine ϕ-Liouvillesche Lösung besitzt, so besitzt L eine Lösung $\eta \in E$, für die $\frac{\phi(\eta)}{\eta}$ algebraisch über F ist.

Beweis.
(a) Falls G eine endliche Gruppe ist, so ist E/F eine endliche Galoiserweiterung und alle Lösungen von L sind algebraisch. Die umgekehrte Richtung zeigen wir im nächsten Teil des Beweises.
(b) Wir gehen zunächst davon aus, dass F^ϕ algebraisch abgeschlossen ist und beweisen die Aussage durch einen Ringschluss der folgenden Aussagen:

1. G° ist auflösbar.
2. E ist eine ϕ-Liouville-Erweiterung von F.
3. E ist in einer ϕ-Liouville-Erweiterung M von F enthalten.

Die Voraussetzung, dass F^ϕ algebraisch abgeschlossen ist benötigen wir nur an einer Stelle, nämlich beim ersten Schritt von 1. nach 2. Wir bezeichnen mit $V := \mathrm{Sol}_E^\Phi(M_L) \subseteq E$ den Lösungsraum und mit $G = \mathrm{Gal}^\Phi(M_L) = \mathrm{Gal}^\Phi(E/F)$ die Galoisgruppe von L. Außerdem sei G° die Zusammenhangskomponente von G und $F_0 = E^{G^\circ} \geq E^G = F$ der Fixkörper von G°. Dann ist E ein PV-Körper von L über F_0 mit Galoisgruppe G°. Nach dem Satz von Lie-Kolchin (siehe [vdPS03, Theorem A.46]) besitzt V eine Basis $\eta_1, \ldots, \eta_n$ über F^ϕ, bezüglich der $G^\circ \subseteq \mathrm{GL}_n(F^\phi)$ nur aus oberen Dreiecksmatrizen besteht. Hier geht die Voraussetzung ein, dass F^ϕ algberaisch abgeschlossen ist, da der Satz von Lie-Kolchin nur über algebraisch abgeschlossenen Körpern gilt. Nun wollen wir die Behauptung durch Induktion nach n und der Dimension von G° zeigen. Dazu müssen wir zwei Fälle unterscheiden. Es sei zunächst $\eta_1 \notin F_0$. Dann existiert zu jedem $\sigma \in G^\circ$ eine ϕ-Invarariante $c_\sigma \in F^\phi$ mit

$\sigma(\eta_1) = c_\sigma \eta_1$, d.h. $\frac{\phi(\eta_1)}{\eta_1}$ ist G°-invariant und liegt damit in F_0. Nun ist aber E ein PV-Körper von L über $F_0(\eta_1)$ und die zugehörige Galoisgruppe ist eine echte Untergruppe von G°. Nach der Induktionsvoraussetzung ist damit $E \supseteq F_0(\eta_1)$ eine ϕ-Liouville-Erweiterung und damit auch $E \supseteq F$.
Als nächstes soll $\eta_1 \in F_0$ gelten. Dann hat die Gleichung $\hat{L}(y) := L(y \cdot \eta_1)$ über F_0 die Lösungen $1, \frac{\eta_2}{\eta_1}, \ldots, \frac{\eta_n}{\eta_1}$. Daher besitzt der zugehörige Operator (vgl. Kapitel 2) $P_{\hat{L}}$ den Rechtsfaktor $\phi - 1$. Daraus ergibt sich die Darstellung $P_{\hat{L}} = P_{\tilde{L}}(\phi - 1)$. Der Lösungsraum der zum Linksfaktor $P_{\tilde{L}}$ assoziierten Gleichung $\tilde{L}(y)$ liegt in E und wird von $\phi(\frac{\eta_2}{\eta_1}) - \frac{\eta_2}{\eta_1}, \ldots, \phi(\frac{\eta_n}{\eta_1}) - \frac{\eta_n}{\eta_1}$ erzeugt. Also liegt ein PV-Körper $\tilde{E}$ von $\tilde{L}$ in E und die zugehörige Galoisgruppe ist eine zusammenhängende auflösbare Gruppe. Nach Induktionsannahme ist damit die Erweiterung $F \subseteq \tilde{E}$ eine ϕ-Liouville-Erweiterung. Außerdem ist $E = \tilde{E}(t_2, \ldots, t_n)$ mit $t_i = \frac{\eta_i}{\eta_1}$ nach Definition eine ϕ-Liouville-Erweiterung, denn es gilt $\phi(t_i) - t_i \in \tilde{E}$ für $i = 2, \ldots, n$. Daher ist sowohl $E \supseteq \tilde{E}$ als auch $\tilde{E} \supseteq F$ und damit $E \supseteq F$ insgesamt eine ϕ-Liouville-Erweiterung.
Die Inklusion von 2. nach 3. ist trivial, also wollen wir direkt den letzten Teil des Ringschlusses, nämlich 3. nach 1. zeigen. Diese Richtung gilt allgemein und wir benötigen nicht mehr die Voraussetzung, dass F^ϕ algebraisch abgeschlossen ist. Dazu sei $M = F(t_1, \ldots, t_m)$ eine ϕ-Liouville-Erweiterung, die E enthält. Wir wollen durch Induktion nach m zeigen, dass die Zusammenhangskomponente G° auflösbar ist. Dazu zeigen wir, dass G eine Normalreihe mit abelschen oder endlichen Faktoren besitzt. Dies ist für $m = 0$ trivial, also nehmen wir $m > 0$ an und gehen davon aus, dass für jeden Index $< m$ eine solche Normalreihe existiert. $E(t_1) \subseteq M$ ist ein PV-Körper von L über $F(t_1)$. Also ist $\mathrm{Gal}^\Phi(E(t_1)/F(t_1)) =: H$ eine abgeschlossene Untergruppe von G. Der Invariantenkörper ist $E^H = E(t_1)^H \cap E = F(t_1) \cap E$. Da E auch ein PV-Körper von L über $F(t_1) \cap E$ ist, gilt für die Galoisgruppe $\mathrm{Gal}^\Phi(E/F(t_1) \cap E) = H$. Diese besitzt nach Induktionsannahme eine Normalreihe mit abelschen oder endlichen Faktoren und damit ist H° auflösbar. Falls $F(t_1) \cap E = F$ gilt, so folgt $H = G$ und die Aussage ist bewiesen. Andernfalls müssen wir die drei möglichen Fälle für t_1 durchgehen. Falls t_1 algebraisch über F ist, so ist die Erweiterung $F(t_1) \cap E$ algebraisch über F und liegt im Fixkörper E^{G°. Außerdem liegen alle Nullstellen des Minimalpolynoms von t_1 in $F(t_1)$ und damit lässt die Galoisgruppe $F(t_1) \cap E$ als Menge invariant. Daher ist H ein Normalteiler in G und es gilt $G/H \cong \mathrm{Aut}((F(t_1) \cap E)/F)$, also ist die Faktorgruppe endlich. Dies beweist einerseits die Rückrichtung von Teil (a) und andererseits gilt für die Zusammenhangskomponenten $H^\circ = G^\circ$.
Falls dagegen t_1 transzendent über F ist, so gilt $F(t_1) \cap E \neq F$. Liegt außerdem $\phi(t_1) - t_1 \in F$, so ist die Galoisgruppe $\mathrm{Gal}^\Phi(F(t_1)/F) = \mathbb{G}_a(F^\phi)$. Diese hat nur endliche abelsche algebraische Untergruppen von Primzahlpotenzordnung. Also ist die folgende Sequenz von Gruppen exakt

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}^\Phi(E/F(t_1) \cap E) & \longrightarrow & \mathrm{Gal}^\Phi(E/F) & \longrightarrow & \mathrm{Gal}^\Phi(F(t_1)/F) & \longrightarrow & 1 \\
 & & \| & & \| & & \| & & \\
1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & \mathbb{G}_a(F^\phi) & \longrightarrow & 1.
\end{array}$$

Da H° und $\mathbb{G}_a(F^\phi)$ auflösbar sind, ist auch G° auflösbar.
Ist schließlich t_1 transzendent und $\phi(t_1) = at_1$ mit $a \in F$, so gilt für die Galoisgruppe

$\mathrm{Gal}^\Phi(F(t_1)/F) = \mathbb{G}_m(F^\phi)$. Die einzigen nicht-trivialen algebraischen Untergruppen sind endliche zyklische Gruppen. Also ist $F(t_1) \cap E = F(t_1^d)$, mit $1 \leq d \in \mathbb{N}$. Wie oben erhalten wir damit eine exakte Sequenz von Gruppen

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}^\Phi(E/F(t_1^d)) & \longrightarrow & \mathrm{Gal}^\Phi(E/F) & \longrightarrow & \mathrm{Gal}^\Phi(F(t_1)/F) & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & \mathbb{G}_m(F^\phi) & \longrightarrow & 1. \end{array}$$

und die Behauptung, dass G° auflösbar ist.
(c) Es sei nun $F(t_1, \ldots, t_m)$ eine ϕ-Liouville-Erweiterung von F mit $\eta \in F(t_1, \ldots, t_m)$, so dass $L(\eta) = 0$ gilt. Wir wollen die Aussage durch Induktion nach m beweisen.
Es sei also zunächst $m = 1$ und t_1 algebraisch über F. Damit sind aber auch η und $\frac{\phi(\eta)}{\eta}$ algebraisch über F.
Falls dagegen t_1 transzendent über F mit $\phi(t_1) - t_1 = a \in F$ ist, so ist die Galoisgruppe $\mathrm{Gal}^\Phi(F(t_1)/F) = \mathbb{G}_a(F^\phi)$. Daher operieren alle $\sigma \in \mathrm{Gal}^\Phi(F(t_1)/F)$ durch $\sigma(t_1) = t_1 + f$ mit $f \in F^\phi$ und weiterhin sind sowohl $\sigma(\eta)$ als auch $\sigma(\eta) - \eta$ Lösungen von L. Also hat L bereits eine Lösung im Grundkörper F.
Ist schließlich t_1 transzendent über F und $\frac{\phi(t_1)}{t_1} = a \in F^\times$, so ist die Galoisgruppe $\mathrm{Gal}^\Phi(F(t_1)/F) = \mathbb{G}_m(F^\phi)$. Die Elemente $\sigma \in \mathrm{Gal}^\Phi(F(t_1)/F)$ operieren durch $\sigma(t_1) = ft_1$ mit $f \in F^{\phi^\times}$ auf $F(t_1)$. Außerdem sind für jedes $\sigma \in \mathrm{Gal}(F(t_1)/F)$ und jedes $f \in F^\phi$ die Elemente $\sigma(\eta) - d\eta$ Lösungen von L. Also muss $F(t_1)$ eine Lösung der Form $\eta = bt_1^d$ mit $b \in F^\times$ und $d \in \mathbb{Z}$ enthalten. Für diese Lösung gilt $\frac{\phi(\eta)}{\eta} = \frac{\phi(b)}{b} \left(\frac{\phi(t_1)}{t_1}\right)^d \in F$.
Es sei nun $0 \neq y \in F(t_1, \ldots, t_{n+1})$ eine Lösung von L. Nach Induktionsannahme besitzt die Gleichung L über dem algebraischen Abschluss $\overline{F(t)}$ mit $t := t_1$ einen Rechtsfaktor vom Grad 1, denn es existiert eine Lösung mit $\frac{\phi(y)}{y} = a \in \overline{F(t)}$. Ist t algebraisch über F, so sind wir fertig. Ist dagegen t transzendent über F, so betrachten wir einen PV-Körper $E(t)$ von L über $F(t)$. Weiterhin sei $E_{\overline{F(t)}}$ ein PV-Körper von L über $\overline{F(t)}$. Außerdem sei $V \subset E$ der Lösungsraum von L und $0 \neq y \in V$ mit $\frac{\phi(y)}{y}$ algebraisch über $F(t)$. Dann haben die Elemente $\sigma(y)$ für jedes $\sigma \in \mathrm{Gal}(E/F)$ diesselbe Eigenschaft. Wir wählen nun $\sigma_1, \ldots, \sigma_s \in \mathrm{Gal}(E/F)$ mit s maximal, so dass $\sigma_1(y), \ldots, \sigma_s(y)$ linear unabhängig über F^ϕ sind. Der Vektorraum $W =< \sigma_1(y), \ldots, \sigma_s(y) >_{F^\phi} \subset V$ ist also invariant unter $\mathrm{Gal}(E/F)$. Sei nun $\tilde{L} = \phi^s(y) + a_{s-1}\phi^{s-1} + \ldots + a_0\phi^0(y)$ die eindeutige Differenzengleichung über E, für die $\tilde{L}(\sigma_i(y)) = 0$ gilt. Da für jedes $\sigma \in \mathrm{Gal}(E/F)$ die Gleichung $\sigma(\tilde{L})$ denselben Lösungsraum W besitzt, gilt $\sigma(\tilde{L}) = \tilde{L}$ und damit, dass die Koeffizienten von $\tilde{L}$ in F liegen. Wir betrachten nun die ϕ-Liouville-Erweiterung $F(t, u_1, \ldots, u_s, \sigma_1(y), \ldots, \sigma_s(y)) \subset E_{\overline{F(t)}}$, wobei die $u_i = \frac{\sigma_i(\phi(y))}{\sigma_i(y)}$ algebraisch über $F(t)$ sind. Diese Erweiterung enthält einen PV-Körper von $\tilde{L}$ über F. Also gilt nach Teil (b) für die Galoisgruppe H von $\tilde{L}$ über F, dass H° auflösbar ist. Sei nun $0 \neq \eta \in W$ ein Eigenvektor von H°. Dann ist $\frac{\phi(\eta)}{\eta}$ invariant unter H° und damit algebraisch über F. Da aber der Vektorraum W ein Untervektorraum von V ist, muss η eine Lösung von L sein, d.h. es gilt $L(\eta) = 0$. □

Satz 1.31. *(C. Jordan)*
Es sei C ein algebraisch abgeschlossener Körper mit $\mathrm{char}(C) = 0$. *Dann existiert eine*

ganzzahlige Funktion $J(n)$, so dass jede endliche Untergruppe von $\mathrm{GL}_n(C)$ einen abelschen Normalteiler vom Index höchstens $J(n)$ besitzt.

Der Beweis dieses klassischen Satzes von Jordan findet sich unter anderem in [Bli17] und in einer moderneren Version in [CR62]. Blichtfeldt gibt als Schranke $J(n) < n!(6^{n-1})^{\pi(n+1)+1}$ an, wobei $\pi(x)$ die Anzahl der Primzahlen kleiner oder gleich x bezeichnet. Er gibt außerdem die Werte $J(2) = 12, J(3) = 360, J(4) = 25920$ an. Eine andere Schranke, nämlich $J(n) \leq (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$, wurde von Schur entdeckt. Ein moderner Beweis findet sich in [CR62]. Satz 1.31 bildet die Grundlage für den Kovacic-Algorithmus (vgl. [Kov86]) für Differentialgleichungen in Charakteristik 0, der als Vorlage für unseren Algorithmus dienen soll. Daher benötigen wir einen analogen Satz in positiver Charakteristik. Diesen erhalten wir durch die folgenden drei Resultate.

Satz 1.32. *(L.E. Dickson)*
Es sei F ein Körper mit $\mathrm{char}(F) = p > 0$ und G eine endliche Untergruppe von $\mathrm{GL}_n(F)$ mit $\mathrm{ggT}\{p, \#G\} = 1$. Dann ist G isomorph zu einer Untergruppe von $\mathrm{GL}_n(\mathbb{C})$.

Korollar 1.33. *(I. Schur)*
Es sei F ein Körper mit $\mathrm{char}(F) = p > 0$ und G eine endliche Untergruppe von $\mathrm{GL}_n(F)$, wobei G kein Element der Ordnung p enthält. Dann enthält G einen abelschen Normalteiler vom Index höchstens $J(n)$.

Satz 1.34. *(R. Brauer und W. Feit)*
Es sei F ein Körper mit $\mathrm{char}(F) = p > 0$ und G eine endliche Untergruppe von $\mathrm{GL}_n(F)$. Falls die p-Sylowgruppen von G höchstens Ordnung p^m haben, dann enthält G einen abelschen Normalteiler vom Index höchstens $f(m, n, p)$, wobei f eine ganzzahlige Funktion ist, die nur von m, n und p abhängt.

Für die Beweise der Sätze 1.32 und 1.33 verweisen wir auf [Weh73]. Ein ausführlicher Beweis zu Satz 1.34 findet sich in [BF66]. Dieser verwendet den ursprünglichen Satz 1.31 von Jordan. Zusammen mit den folgenden beiden Sätzen liefert Satz 1.34 die Grundlage für unseren Algorithmus.

Satz 1.35. *Es sei F ein Körper mit $\mathrm{char}(F) = p > 0$ und G eine Untergruppe von $\mathrm{GL}_n(F)$, die auf den Ursprungsgeraden in F^n, also auf $\mathbb{P}^n(F) = \mathbb{P}(F^{n-1})$ operiert. Falls G auf $\mathbb{P}^n(F)$ eine endliche Bahn besitzt und die Voraussetzungen von Satz 1.34 erfüllt, so hat G auch eine Bahn, deren Länge durch eine Funktion $I(m, n, p) := \max_{r \leq n}\{[\frac{n}{r}]f(m, r, p)\}$ in Abhängigkeit von $f(m, n, p)$ aus Satz 1.34 beschränkt ist.*

Beweis. Wir gehen ohne Einschränkung davon aus, dass G eine lineare algebraische Gruppe ist, denn wir können die Gruppe G durch ihren Zariski-Abschluss in $\mathrm{GL}_n(F)$ ersetzen. Außerdem setzen wir voraus, dass die Gerade $Fw \subset V := F^n$ eine endliche Bahn $\{Fw_1, \ldots, Fw_s\}$ unter G besitzt. Dann ist die Menge

$$H = \{h \in G \mid h(Fw_i) = Fw_i \text{ für alle } i\}$$

ein Normalteiler in G vom Index höchstens $s!$. Seien $\chi_1, \ldots \chi_t$ die verschiedenen Charaktere

$$\chi_i : G \longrightarrow F^{\times},$$

so dass der Vektorraum

$$V_{\chi_i} := \{v \in V \mid h(v) = \chi_i(h)v \text{ für alle } h \in H\}$$

nicht der Nullraum ist. Dann ist $\bigoplus_{i=1}^{t} V_{\chi_i}$ ein Untervektorraum von V. Da H ein Normalteiler von G ist, permutiert G die Räume V_{χ_i} und damit ist $\bigoplus_{i=1}^{t} V_{\chi_i}$ ein G-invarianter Unterraum von V. Es sei nun $H_1 \subset G$ der Stabilisator von V_{χ_1}. Dann ist der Index von H_1 in G höchstens t. Also gilt $[G : H_1] \leq [\frac{n}{r}]$, wobei r die Dimension von V_{χ_1} bezeichnet. Falls also $r = 1$ ist, so hat die Gerade V_{χ_1} eine G-Bahn der Länge höchstens n.
Wir nehmen nun an, dass $r > 1$ gilt. Dann induziert die Operation von H_1 auf V_{χ_1} eine Operation der endlichen Gruppe $H_1/H \subset \mathrm{PGL}_n(F) = \mathrm{PSL}_n(F)$ auf dem projektiven Raum $\mathbb{P}(V_{\chi_1}) = \mathbb{P}^{r-1}(F)$. Also operiert H auf V_{χ_1} durch seinen Charakter χ_1. Es sei $H_2 \subset \mathrm{SL}_r(F)$ das Urbild von H_1/H. Wendet man nun Satz 1.34 auf die endliche Gruppe H_2, erhalten wir einen abelschen Normalteiler $H_3 \subset H_2$ vom Index höchstens $f(m, r, p)$. Dieser ist der Stabilisator einer Geraden $L \subset V_{\chi_1}$. Die H_2-Bahn von L hat höchstens die Länge $[H_2 : H_3] \leq f(m, r, p)$. Die H_1-Bahn von L stimmt mit der H_2-Bahn überein. Letztendlich hat also die G-Bahn von L die Länge höchstens $[G : H_1]$ mal die Länge der H_1-Bahn von L. Also ist die Länge der G-Bahn von L beschränkt durch $[\frac{n}{r}]f(m, r, p)$. □

Satz 1.36. *Es sei $L(y) = 0$ eine Differenzengleichung vom Grad n über einem Frobenius-Körper $(F := \mathrm{Quot}(R), \phi)$ mit PV-Körper E und zugehöriger Galoisgruppe $G := \mathrm{Gal}(L)$, wobei R ein relativer Frobenius-Ring mit definierendem Ideal Q ist. Falls die Gleichung $L(y) = 0$ eine ϕ-Liouvillesche Lösung besitzt, so besitzt L eine Lösung $\eta \in E$ für die $\frac{\phi(\eta)}{\eta}$ algebraisch vom Grad höchstens $I(m, n, p)$ über F ist.*

Beweis. Es sei E ein PV-Körper von L über F und $V := \mathrm{Sol}_E^{\Phi}(M_L)$ der Lösungsvektorraum. Die Galoisgruppe G von L operiert auf diesem Lösungsraum. Nach Satz 1.30 (c) existiert eine Lösung $0 \neq \eta \in V$, so dass $u := \frac{\phi(\eta)}{\eta} \in E$ algebraisch über F ist. Mit $P_u(T) \in F(T)$ bezeichnen wir das zugehörige Minimalpolynom vom Grad d. Dann sind $\sigma(u)$ für jedes $\sigma \in G$ ebenfalls Nullstellen von P_u. Daraus ergibt sich, dass die Zusammenhangskomponente G° von G trivial auf u operiert, bzw. dass $u \in F^{G^\circ}$ gilt. Da F^{G°/F eine gewöhnliche Galoiserweiterung mit der endlichen Galoisgruppe G/G° ist, besteht die G-Bahn von u aus allen Nullstellen von P_u und hat die Länge d. Also hat die G-Bahn der Geraden $F^\phi\eta \subset V$ ebenfalls die Länge d.
Umgekehrt impliziert eine Gerade $F^\phi\eta$ in V mit endlicher G-Bahn ein Element $u := \frac{\phi(\eta)}{\eta} \in E$ mit endlicher G-Bahn. Also muss u algebraisch über F sein. Wie oben folgt, dass der Grad von u über F mit der Länge der G-Bahn von $F^\phi\eta$ übereinstimmt. Nun können wir Satz 1.35 anwenden und erhalten damit die Behauptung. □

Kapitel 2

Lineare Konstruktionen und Differenzen-Operatoren

Um die Galoisgruppe einer Differenzengleichung bzw. des zugehörigen Frobenius-Moduls zu berechnen, werden wir einige Konstruktionen aus der linearen Algebra benötigen. Diese wollen wir in diesem Abschnitt einführen und die für unsere Zwecke relevanten Eigenschaften beweisen. Im Folgenden sei R ein kommutativer Ring und M ein R-Modul.

2.1 Die symmetrische Algebra

Definition 2.1. Wir definieren die **d-te symmetrische Algebra** als Quotienten des d-fachen Tensorprodukts

$$\mathrm{T}^d(M) := \bigotimes_{i=1}^{d} M$$

über dem Ideal

$$I_{Sym} :=< m_1 \otimes \cdots \otimes m_d - m_{\pi(1)} \otimes \cdots \otimes m_{\pi(d)} \,|\, \pi \in \mathrm{S}_d > \trianglelefteq \mathrm{T}^d(M).$$

Diese bezeichnen wir mit

$$\mathrm{Sym}_d(M) := \mathrm{T}^d(M)/I_{Sym}.$$

Eine Restklasse in der symmetrischen Algebra bezeichnen wir mit der gewöhnlichen Produktschreibweise $m_1 \cdots m_d$.

Bemerkung 2.2. *Ist M ein freier R-Modul mit Basis $\{e_1, \ldots, e_n\}$, so ist die d-te symmetrische Algebra* $\mathrm{Sym}_d(M)$ *ein freier R-Modul der Dimension $\binom{n+d-1}{n-1}$ mit Basis*

$$\{e_{j_1}^{i_1} \cdots e_{j_d}^{i_d} \,|\, i_k \geq 0 \text{ und } \sum_{k=1}^{d} i_k = d, 1 \leq j_1 < \ldots < j_d \leq n\}.$$

Beweis. Es seien $m_1, \ldots, m_d \in M$ mit Basisdarstellung $m_i = \sum_{j=1}^{n} a_{ij} e_j$ gegeben. Dann gilt

$$\begin{aligned} m_1 \cdots m_d &= \sum_{j_1=1}^{n} a_{1j_1} e_{j_1} \cdots \sum_{j_d=1}^{n} a_{dj_d} e_{j_d} \\ &= \sum_{j_1=1}^{n} \cdots \sum_{j_d=1}^{n} a_{1j_1} \cdots a_{dj_d}\, e_{j_1} \cdots e_{j_d} \end{aligned}$$

Unter Verwendung der Rechenregel $e_1 \cdots e_d = e_{\pi(1)} \cdots e_{\pi(d)}$ mit $\pi \in \mathrm{S}_d$ erhält man daraus dann die Darstellung

$$m_1 \cdots m_d = \sum_{j_1=1}^{n} \cdots \sum_{j_d > j_{d-1}}^{n} a_{1j_1} \cdots a_{dj_d}\, e_{j_1}^{i_1} \cdots e_{j_d}^{i_d} \text{ mit } \sum_{k=1}^{d} i_k = d.$$

Für Produkte der Form $e_{j_1}^{i_1} \cdots e_{j_d}^{i_d}$ gibt es $\binom{n+d-1}{n-1}$ verschiedene Möglichkeiten und damit erhalten wir die Behauptung. □

Anmerkung 2.3. Man kann die Elemente der d-ten symmetrischen Algebra $\mathrm{Sym}_d(M)$ mit den homogenen Polynomen vom Grad d in $R[X_1, \ldots, X_n]$ identifizieren.

2.2 Die äußere Algebra

Definition 2.4. Wir definieren die **d-te äußere Algebra** als Quotienten des d-fachen Tensorprodukts $\mathrm{T}^d(M)$ über dem Ideal

$$I_{Ex} := < m_1 \otimes \cdots \otimes m_d \,|\, \text{ es existieren Indizes } 1 \le i < j \le d : m_i = m_j > \trianglelefteq \mathrm{T}^d(M).$$

Diese bezeichnen wir mit

$$\Lambda^d(M) := \mathrm{T}^d(M)/I_{Ex}.$$

Eine Restklasse in der äußeren Algebra bezeichnen wir mit $m_1 \wedge \cdots \wedge m_d$.

Bemerkung 2.5. *Für die äußere Algebra $\Lambda^d(M)$ gelten:*
(a) Für $\pi \in \mathrm{S}_d$ gilt $m_{\pi(1)} \wedge \cdots \wedge m_{\pi(d)} = \mathrm{sign}(\pi)\, m_1 \wedge \cdots \wedge m_d$.
(b) Ist M ein freier R-Modul mit Basis $\{e_1, \ldots, e_n\}$, so ist $\Lambda^d(M)$ ein freier R-Modul der Dimension $\binom{n}{d}$ mit Basis $B := \{e_{i_1} \wedge \cdots \wedge e_{i_d} \,|\, 1 \le i_1 < \ldots < i_d \le n\}$.

Beweis. Die erste Behauptung zeigen wir durch Induktion nach d. In der 2-ten äußeren Algebra gilt:

$$0 = (m + \tilde{m}) \wedge (m + \tilde{m}) = m \wedge \tilde{m} + \tilde{m} \wedge m$$

und damit $m \wedge \tilde{m} = -\tilde{m} \wedge m$. Der Induktionsschritt lässt sich auf den Induktionsanfang zurückführen, da sich jede Permutation als Produkt von Transpositionen schreiben lässt.
(b) Es seien $m_1, \ldots, m_d \in M$ mit Basisdarstellung $m_i = \sum_{j=1}^{n} a_{ij} e_j$ gegeben. Dann gilt:

$$\begin{aligned} m_1 \wedge \cdots \wedge m_d &= \left(\sum_{j=1}^{n} a_{1j} e_j \right) \wedge \cdots \wedge \left(\sum_{j=1}^{n} a_{dj} e_j \right) \\ &= \sum_{1 \le i_1 < \ldots < i_d \le n} \alpha_{i_1 \ldots i_d} \, (e_{i_1} \wedge \cdots \wedge e_{i_d}). \end{aligned}$$

Dabei werden im letzten Umrechnungsschritt alle äußeren Produkte 0 , in denen gleiche Elemente auftreten. Es sei

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dn} \end{pmatrix} \in R^{d \times n}$$

die Darstellungsmatrix der m_i bezüglich der Basis B. Dann erhalten wir die Ringelemente $\alpha_{i_1 \ldots i_d}$ als Determinante der Matrix $A_{i_1 \ldots i_d}$. Diese entsteht aus A durch Streichen der Spalten mit Indizes $i_1, \ldots, i_d$. Für äußere Produkte der Form $e_{i_1} \wedge \cdots \wedge e_{i_d}$ gibt es $\binom{n}{d}$ verschiedene Möglichkeiten und damit erhalten wir die Behauptung. □

Anmerkung 2.6. Zwar wird die äußere Algebra durch äußere Produkte der Form $m_1 \wedge \cdots \wedge m_d$ erzeugt, dennoch kann man im Allgemeinen nicht jedes Element $\mathfrak{a} \in \Lambda^d(M)$ als äußeres Produkt der obigen Form schreiben, z.B.

$$\mathfrak{a} = e_1 \wedge e_2 + e_3 \wedge e_4 \text{ in } \Lambda^2(\mathbb{R}^4).$$

Dies bringt uns zu folgender Definition:

Definition 2.7. Ein Element $\mathfrak{a} \in \Lambda^d(M)$ der äußeren Algebra heißt **zerlegbar**, falls es sich als äußeres Produkt der Form $\mathfrak{a} = m_1 \wedge \cdots \wedge m_d$ mit $m_i \in M$ schreiben lässt.

Satz 2.8. *Es sei M ein freier R-Modul mit Basis $B := \{e_1, \ldots, e_n\}$. Ein Element $\mathfrak{a} = \sum_{1 \le i_1 < \ldots < i_d \le n} \alpha_{i_1 \ldots i_d} (e_{i_1} \wedge \cdots \wedge e_{i_d}) \in \Lambda^d(M)$ der äußeren Algebra ist genau dann zerlegbar, falls das folgende Gleichungssystem*

$$\alpha_{i_1 \ldots i_d} = \det(A_{i_1 \ldots i_d})$$

lösbar ist. Dabei erhalten wir die Matrizen $A_{i_1 \ldots i_d}$ aus der Matrix

$$A := \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{d1} & \cdots & x_{dn} \end{pmatrix}$$

durch Streichen der Spalten mit Indizes $i_1, \ldots, i_d$.

Beweis. Wir erhalten die Behauptung durch analoge Überlegungen wie im Beweis zu Bemerkung 2.5. □

Satz 2.9. *Es sei M ein freier R-Modul und $N \le M$ ein d-dimensionaler Untermodul. Ein eindimensionaler Untermodul $P \le \Lambda^d(M)$ hat genau dann die Form $P = \Lambda^d(N)$, falls P von einem zerlegbaren Element der Form $P =< m_1 \wedge \cdots \wedge m_d >$ erzeugt wird.*

Beweis. Wir gehen zunächst davon aus, dass P in der Form $P = \Lambda^d(N)$ gegeben ist. Es sei $\{m_1, \ldots, m_d\}$ eine Basis von N. Dann bildet $m_1 \wedge \cdots \wedge m_d$ nach Bemerkung 2.5 (b) eine Basis von $\Lambda^d(N) = P$.
Es sei nun umgekehrt $P =< m_1 \wedge \cdots \wedge m_d >$ ein eindimensionaler Untermodul von $\Lambda^d(M)$. Wir definieren durch $N :=< m_1, \ldots, m_d >$ den von den m_i erzeugten Untermodul von M. Wieder nach Bemerkung 2.5 (b) gilt nun $P =< m_1 \wedge \cdots \wedge m_d >= \Lambda^d(N)$. □

2.3 Der Ring der Differenzen-Operatoren

Wir bezeichnen im Folgenden mit F den Quotientenkörper des relativen Frobenius-Rings R mit Endomorphismus ϕ. Um die Begriffe der Irreduzibilität und Faktorisierung von Differenzengleichungen einzuführen, definieren wir den Ring der Differenzen-Operatoren. Wir folgen dabei den Ideen von O. Ore in [Ore33], denn die vorliegenden Differenzen-Operatoren sind ein Spezialfall der von ihm entdeckten Schiefpolynome.

Definition 2.10. Wir definieren den (nicht-kommutativen) **Ring der Differenzen-Operatoren** durch

$$\mathfrak{D} := F\{\tau\} := \{\sum_{i=0}^{n} a_i \tau^i \mid a_i \in F, \tau a = \phi(a)\tau\}.$$

Zu einer Differenzengleichung

$$L(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i \phi^i(y) = 0 \text{ mit } a_i \in F$$

definieren wir den **assoziierten Differenzen-Operator**

$$P_L := \tau^n + \sum_{i=0}^{n-1} a_i \tau^i \text{ mit } a_i \in F.$$

Durch $\deg_\tau(P)$ definieren wir den **Grad** des Differenzen-Operators P.

Anmerkung 2.11. Die Menge der Differenzen-Operatoren wird mit der gewöhnlichen Addition und der Multiplikation via der Regel $\tau a = \phi(a)\tau$ zu einem nicht-kommutativen Ring, der gewisse Ähnlichkeit mit dem Ring der gewöhnlichen Polynome über F hat. Da die Multiplikation aber nicht kommutativ ist, muss man z.B. bei Division mit Rest auf die Reihenfolge achten.

Definition 2.12. Ein Differenzen-Operator $P \in \mathfrak{D}$ von Grad $\deg_\tau(P) = n$ heißt **reduzibel**, falls es Differenzen-Operatoren $P_1, P_2 \in \mathfrak{D}$ von Grad $0 < \deg_\tau(P_1), \deg_\tau(P_2) < n$ mit $P = P_1 P_2$ gibt. Andernfalls heißt P **irreduzibel**. Eine Differenzengleichung $L(y) = 0$ heißt **reduzibel** bzw. **irreduzibel**, falls der zugehörige Differenzen-Operator P_L reduzibel bzw. irreduzibel ist.

Definition 2.13. Es sei $P = Q_1 Q_2 \in \mathfrak{D}$ ein reduzibler Differenzen-Operator. Wir nennen Q_1 einen **Linksteiler** und Q_2 einen **Rechtsteiler** von P. Weiterhin schreiben wir für $P, Q, M \in \mathfrak{D}$

$$P \equiv Q \pmod{M} \text{ , falls ein } D_1 \in \mathfrak{D} \text{ existiert, so dass } P - Q = D_1 M, \text{ bzw.}$$
$$P \equiv Q \pmod{M} \text{ , falls ein } D_2 \in \mathfrak{D} \text{ existiert, so dass } P - Q = M D_2.$$

Definition 2.14. Es seien $P_1, P_2 \in \mathfrak{D}$ Differenzen-Operatoren. Wir nennen den normierten Differenzen-Operator $g \in \mathfrak{D}$ maximalen Grades, so dass Differenzen-Operatoren $Q_1, Q_2 \in \mathfrak{D}$ mit

$$P_1 = Q_1 g \quad \text{und} \quad P_2 = Q_2 g$$

existieren, den **größten gemeinsamen Rechtsteiler** von P_1 und P_2. Diesen bezeichnen wir ab jetzt mit $\mathrm{ggrT}(P_1, P_2) := g$.

Bemerkung 2.15. *Es seien $P_1, P_2 \in \mathfrak{D}$ Differenzen-Operatoren. Dann lässt sich der größte gemeinsame Rechtsteiler* $\mathrm{ggrT}(P_1, P_2)$ *durch wiederholte Division mit Rest von rechts, dem sogenannten Euklidischen Algorithmus für Schiefpolynome, in endlich vielen Schritten berechnen. Außerdem ist der* $\mathrm{ggrT}(P_1, P_2)$ *eindeutig bestimmt.*

Beweis. Es seien $P_1 = \sum_{i=0}^{n} a_i \tau^i$ und $P_2 = \sum_{j=0}^{m} b_j \tau^j$ und wir gehen ohne Einschränkung davon aus, dass $n \geq m$ ist. Dann hat der Operator

$$\begin{aligned} P &:= P_1 - a_n \phi^{n-m}(b_m^{-1}) \tau^{n-m} P_2 \\ &= \sum_{i=0}^{n} a_i \tau^i - (a_n \tau^{n-m} b_m^{-1} \sum_{j=0}^{m} b_j \tau^j) \\ &= \sum_{i=0}^{n} a_i \tau^i - a_n \tau^{n-m} (\tau^m + \sum_{j=0}^{m-1} b_j \tau^j) \\ &= \sum_{i=0}^{n-1} a_n \tau^i - \sum_{j=0}^{m-1} a_n \phi^{n-m}(b_j) \tau^{j+n-m}. \end{aligned}$$

höchstens Grad $n-1$, d.h. wir erhalten die Darstellung

$$P_1 = Q_1 P_2 + P_3 \text{ mit } \deg_\tau(Q_1) = n - m \text{ und } \deg_\tau(P_3) < \deg_\tau(P_2) = m.$$

Mit diesem Verfahren erhalten wir sukzessive eine Euklidische Schiefpolynomrestfolge mit abnehmenden Graden der Gestalt

$$\begin{aligned} P_1 &= Q_1 P_2 + P_3, \\ P_2 &= Q_2 P_3 + P_4, \\ &\vdots \\ P_{l-2} &= Q_{l-2} P_{l-1} + P_l, \\ P_{l-1} &= Q_{l-1} P_l. \end{aligned}$$

Wie beim gewöhnlichen Euklidischen Algorithmus setzen wir $\mathrm{ggrT}(P_1, P_2) = P_l$ und erhalten damit die Behauptung. □

Bemerkung 2.16. *Zu zwei Differenzen-Operatoren $P_1, P_2 \in \mathfrak{D}$ existieren Differenzen-Operatoren $Q_1, Q_2 \in \mathfrak{D}$ mit*

$$Q_1 P_1 + Q_2 P_2 = \mathrm{ggrT}(P_1, P_2).$$

Beweis. Wir erhalten die Operatoren Q_1 und Q_2 aus der Restfolge aus dem Beweis zu Satz 2.15 wie beim erweiterten Euklidischen Algorithmus für Polynome durch rückwärtiges Einsetzen. □

Definition 2.17. Zwei Differenzen-Operatoren $P_1, P_2 \in \mathfrak{D}$ heißen **teilerfremd**, falls $\mathrm{ggrT}(P_1, P_2) = 1$ gilt.

Anmerkung 2.18. Im Allgemeinen ist eine entsprechende Linksdivision nur dann möglich, wenn ϕ ein Automorphismus ist.

Definition 2.19. Es seien $P_1, P_2 \in \mathfrak{D}$ Differenzen-Operatoren. Wir nennen den normierten Differenzen-Operator $M \in \mathfrak{D}$ kleinsten Grades, so dass Differenzen-Operatoren $Q_1, Q_2 \in \mathfrak{D}$ mit

$$M = Q_1 P_1 = Q_2 P_2$$

existieren, das **kleinste gemeinsame Linksvielfache** von P_1 und P_2. Diesen bezeichnen wir ab jetzt mit $M =: \mathrm{kglV}(P_1, P_2)$.

Satz 2.20. *Es seien $P_1, P_2 \in \mathfrak{D}$ Differenzen-Operatoren mit Euklidischer Restfolge $(P_i)_{i=1}^n$ gegeben. Dann lässt sich das kleinste gemeinsame Linksvielfache folgendermaßen darstellen:*

$$\mathrm{kglV}(P_1, P_2) = a P_{n-1} P_n^{-1} P_{n-2} P_{n-1}^{-1} \cdots P_3 P_4^{-1} P_2 P_3^{-1} P_1,$$

wobei $a \in F$ so gewählt wird, dass die rechte Seite normiert ist.

Zum Beweis dieses Satzes benötigen wir das folgende Lemma.

Lemma 2.21. *Es seien $P, Q, M \in \mathfrak{D}$ Differenzen-Operatoren mit $P \equiv Q (\mathrm{mod}\, M)$. Dann existiert ein $k \in F$, so dass*

$$\mathrm{kglV}(P, M) = k \cdot \mathrm{kglV}(Q, M) Q^{-1} P.$$

Beweis. Existiert $L := \mathrm{kglV}(P, M)$, so existiert ein $M_1 \in \mathfrak{D}$ minimalen Grades mit $L = M_1 P$. Nach Voraussetzung existiert ein $Q_1 \in \mathfrak{D}$, so dass $P = Q + Q_1 M$ und damit

$$L = M_1 P = M_1 Q + M_1 Q_1 M$$

gilt. Da aber L nach Voraussetzung durch M rechtsteilbar ist, muss auch $M_1 Q$ rechtsteilbar durch M sein. Nach Definition nimmt also M_1 den niedrigsten Grad an, wenn $M_1 Q = \mathrm{kglV}(Q, M)$ gilt. Dies liefert die gewünschte Darstellung

$$\mathrm{kglV}(P, M) = k \cdot \mathrm{kglV}(Q, M) Q^{-1} P$$

mit normierendem Körperelement $k \in F$. □

Beweis. zu Satz 2.20
Um die gewünschte Darstellung für $\mathrm{kglV}(P_1, P_2)$ zu gewinnen, wenden wir wiederholt Lemma 2.21 an. Wir erhalten also:

$$\begin{aligned}
\mathrm{kglV}(P_1, P_2) &= a_1 \,\mathrm{kglV}(P_2, P_3) P_3^{-1} P_1 \\
&= a_2 \,\mathrm{kglV}(P_3, P_4) P_4^{-1} P_2 P_3^{-1} P_1 \\
&\vdots \\
&= a_{n-1} \,\mathrm{kglV}(P_n, P_{n-1}) P_n^{-1} P_{n-2} P_{n-1}^{-1} \cdots P_2 P_3^{-1} P_1 \\
&= a_n P_{n-1} P_n^{-1} P_{n-2} P_{n-1}^{-1} \cdots P_3 P_4^{-1} P_2 P_3^{-1} P_1.
\end{aligned}$$

Damit haben wir die gewünschte Darstellung konstruiert. Wir müssen allerdings noch zeigen, dass die rechte Seite tatsächlich im Ring $\mathfrak{D}$ der Differenzen-Operatoren liegt und dass sie durch P_1, P_2 rechtsteilbar ist. Dies wollen wir durch Induktion beweisen und setzen

$$\tilde{L}_i := P_{n-1}P_nP_{n-2}P_{n-1}^{-1}\cdots P_{i+1}P_{i+2}^{-1}P_i.$$

Dann ist $\tilde{L}_{n-1} = P_{n-1} \in \mathfrak{D}$ und durch P_n und P_{n-1} rechtsteilbar. Wir gehen nun davon aus, dass bereits gezeigt wurde, dass $\tilde{L}_{i+1} \in \mathfrak{D}$ liegt und durch P_{i+1} und P_{i+2} rechtsteilbar ist. Dann liegt aber $\tilde{L}_i = \tilde{L}_{i+1}P_{i+2}^{-1}P_i$ in $\mathfrak{D}$ und ist durch P_i rechtsteilbar. Wegen dem Euklidischen Algorithmus gilt außerdem, dass $P_i = Q_iP_{i+1} + P_{i+2}$ und damit $\tilde{L}_i = \tilde{L}_{i+1}P_{i+2}^{-1}Q_iP_{i+1} + \tilde{L}_{i+1}$. Da aber $\tilde{L}_{i+1}$ nach Induktionsannahme durch P_{i+1} rechtsteilbar ist, ist auch $\tilde{L}_i$ durch P_{i+1} rechtsteilbar und damit ist der Beweis erbracht. □

Definition 2.22. Es seien $P = \sum_{i=0}^{n} a_i\tau^i, Q = \sum_{j=0}^{m} b_j\tau^j \in \mathfrak{D}$ Differenzen-Operatoren. Bezeichnen wir mit $\delta_{PQ} := \deg_\tau(\mathrm{ggrT}(P,Q))$ den Grad des größten gemeinsamen Rechtsteilers von P und Q, so heißt der Differenzen-Operator

$$\mathfrak{T}_{P,Q} := a_n\phi^{n-\delta_{PQ}}(b_m)\,\mathrm{kglV}(P,Q)Q^{-1}$$

die **Transformierte** von P durch Q. Falls P und Q teilerfremd sind, so gilt $\deg_\tau(P) = \deg_\tau(\mathfrak{T}_{P,Q})$. Differenzen-Operatoren, die aus P durch Transformation mit einem teilerfremden Differenzen-Operator gewonnen werden, heißen **ähnlich** zu P.

Bemerkung 2.23. *Es seien $P = \sum_{i=0}^{n} a_i\tau^i, Q_1, Q_2 = \sum_{j=0}^{m} b_j\tau^j \in \mathfrak{D}$ Differenzen-Operatoren mit der Eigenschaft, dass das Produkt Q_1Q_2 durch P rechtsteilbar ist und für die die Kongruenz $Q_1 \equiv Q_2 (\mathrm{mod}\, P)$ erfüllt ist, so ist Q_1 durch $\mathfrak{T}_{P,Q_2}$ rechtsteilbar.*

Beweis. Das Produkt Q_1Q_2 ist sowohl durch Q_2 als auch durch P rechtsteilbar, also auch durch $\mathrm{kglV}(P,Q_2)$. Es existiert also ein Differenzen-Operator $H \in \mathfrak{D}$, so dass $Q_1Q_2 = Ha_n\phi^{n-\delta_{PQ_2}}(b_m)\,\mathrm{kglV}(P,Q_2)$ und damit gilt

$$Q_1 = Ha_n\phi^{n-\delta_{PQ_2}}(b_m)\,\mathrm{kglV}(P,Q_2)Q_2^{-1} = H\mathfrak{T}_{P,Q_2}.$$

□

Die folgende Bemerkung halten wir nur der Vollständigkeit halber fest. Für einen Beweis und weitere Informationen über Schiefpolynome verweisen wir auf [Ore33].

Bemerkung 2.24. *Es gelten:*
(a) Jeder zu einem irreduziblen Differenzen-Operator ähnliche Operator ist ebenfalls irreduzibel.
(b) Ist ein Produkt Q_1Q_2 von Differenzen-Operatoren durch einen irreduziblen Operator P rechtsteilbar und Q_2 ist nicht durch P rechtsteilbar, so ist Q_1 durch $\mathfrak{T}_{P,Q_2}$ rechtsteilbar.

Beweis. [Ore33, Observations zu Beginn von Chap. II] □

Definition 2.25. Es seien $P, Q \in \mathfrak{D}$ Differenzen-Operatoren. P heißt mit Q **austauschbar**, falls es einen zu P ähnlichen Differenzen-Operator P_1 gibt, so dass $P = \mathfrak{T}_{P_1,Q}$ gilt.

Satz 2.26. *Jeder normierte Differenzen-Operator besitzt eine Darstellung als Produkt irreduzibler Faktoren. Zwei verschiedene Zerlegungen des gleichen Differenzen-Operators haben die selbe Anzahl an Primfaktoren und diese sind paarweise ähnlich. Man erhält eine Darstellung aus der anderen durch Austausch der Faktoren.*

Beweis. Es gibt offensichtlich mindestens eine Zerlegung eines Differenzen-Operators $F \in \mathfrak{D}$ in irreduzible Faktoren. Es seien nun zwei verschiedene Zerlegungen

$$\begin{aligned} F &= P_r \cdots P_1 \\ &= Q_s \cdots Q_1 \end{aligned}$$

gegeben. Also teilt Q_1 das Produkt $P_r \cdots P_1$ von rechts. Wir unterscheiden zwei Fälle. Ist $P_1 = Q_1$, so kann dieser Faktor gekürzt werden. Andernfalls sei $k \in \{1, \ldots, r\}$ der minimale Index, so dass $P_k \cdots P_1$ durch Q_1 rechtsteilbar ist. Dann ist aber das Produkt $H := P_{k-1} \cdots P_1$ teilerfremd zu Q_1. Nach Bemerkung 2.23 ist dann P_k rechtsteilbar durch das zu Q_1 ähnliche Primpolynom $\tilde{Q}_1 = \mathfrak{T}_{Q_1,H}$. Da aber P_k ebenfalls irreduzibel ist, muss $P_k = \mathfrak{T}_{Q_1,H} = \tilde{Q}_1$ gelten. Also ist P_k austauschbar mit $H = P_{k-1} \cdots P_1$ und damit erhalten wir $P_k \cdots P_1 = \mathfrak{T}_{H,Q_1} Q_1$. Wir können also durch Austausch der Faktoren Q_1 kürzen. Nun können wir mit dem gekürzten Produkt und den übrigen Primfaktoren analog verfahren und erhalten damit die Behauptung. □

2.4 Konstruktionen mit Differenzen-Operatoren

In Abschnitt 2.1 haben wir lineare Konstruktionen für Frobenius- bzw. Differenzen-Moduln kennengelernt. In Kapitel 1 haben wir bereits gesehen, dass die Sprechweisen der Differenzen-Moduln und Differenzengleichungen die selben Sachverhalte beschreiben. Daher liegt es nahe, die o.g. linearen Konstruktionen auch für Differenzengleichungen bzw. Differenzen-Operatoren einzuführen.

Satz 2.27. *Es sei* $L(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i \phi^i(y) = 0$ *mit* $a_i \in F$ *eine lineare Differenzengleichung vom Grad* n *über* F *mit Lösungskörper* E *und einem Fundamentalsystem von Lösungen* $\{\eta_1, \ldots, \eta_n\}$. *Dann existiert eine Differenzengleichung* $\mathrm{Sym}_m(L)(y)$ *vom Grad höchstens* $\binom{n+m-1}{n-1}$, *deren Lösungsraum von* $\{\eta_1^{i_1} \cdots \eta_n^{i_n} \mid \sum_{j=1}^{n} i_j = m\}$ *aufgespannt wird.*

Beweis. Um die gewünschte Differenzengleichung zu konstruieren definieren wir $v := u^m$ mit $u \in \{\eta_1, \ldots, \eta_n\}$ beliebig. Auf dieses v wenden wir wiederholt ϕ an, bis sich eine lineare

Abhängigkeit ergibt, also

$$\begin{aligned} v &= u^m, \\ \phi(v) &= \phi(u)^m, \\ \phi^2(v) &= \phi^2(u)^m, \\ &\vdots \\ \phi^n(v) &= \phi^n(u)^m = (-1)^m \left(\sum_{i=0}^{n-1} a_i \phi^i(u) \right)^m \\ \phi^{n+1}(v) &= \phi(\phi^n(u)^m), \\ &\vdots \\ \phi^r(v) &= \sum_I c_{r,I} \cdot \varepsilon^I, \end{aligned}$$

wobei $\varepsilon^I = u^{i_0} \cdot \phi(u)^{i_1} \cdot \phi^2(u)^{i_2} \cdots \phi^{n-1}(u)^{i_{n-1}}$ und $I = \{(i_0, \ldots, i_{n-1}) \mid \text{ mit } \sum_{j=0}^{n-1} i_j = m\}$ gelten. Da es für solche Tupel in I höchstens $\binom{n+m-1}{n-1}$ verschiedene Möglichkeiten gibt, ergibt sich spätestens bei $r = \binom{n+m-1}{n-1}$ eine lineare Abhängigkeit über F. Diese liefert ein lineares Gleichungssystem und durch dessen Lösung eine Differenzengleichung $\mathrm{Sym}_m(L)$ für $v = u^m$ vom Grade höchstens $\binom{n+m-1}{n-1}$, deren Lösungsraum nach Konstruktion von $\{\eta_1^{i_1} \cdots \eta_n^{i_n} \mid \sum_{j=1}^{n} i_j = m\}$ aufgespannt wird. □

Definition 2.28. Es sei $L(y) = 0$ eine lineare Differenzengleichung vom Grad n. Wir nennen die in Satz 2.27 definierte Differenzengleichung $\mathrm{Sym}_m(L)$ die **m-te symmetrische Potenz** von L.

Anmerkung 2.29. Ist M_L der zu der Differenzengleichung L gehörige Frobenius-Modul, so ist der zu $\mathrm{Sym}_m(L)$ gehörige Frobenius-Modul $M_{\mathrm{Sym}_m(L)}$ ein Untermodul von $\mathrm{Sym}_m(M_L)$. Falls $\deg_\tau(P_L) = 2$ ist, gilt sogar Gleichheit.

Satz 2.30. *Es sei $L(y) = 0$ eine lineare Differenzengleichung vom Grad n über F mit PV-Körper E mit einem rationalen Punkt (vgl. Definition 1.8), Galoisgruppe G und Lösungsraum $V := \mathrm{Sol}_E^\Phi(M_L)$. Ferner sei $\mathrm{Sym}_m(V)$ die m-te symmetrische Algebra über V. Wir definieren die natürliche Abbildung*

$$\begin{array}{rccc} \Psi_m : & \mathrm{Sym}_m(V) & \longrightarrow & E \\ & v_1 v_2 \cdots v_m & \longmapsto & v_1 \cdot v_2 \cdot \ldots \cdot v_m \end{array},$$

mit $\mathrm{Bild}(\Psi_m) = \mathrm{Sol}_E^\Phi(M_{\mathrm{Sym}_m(L)})$. Dann gelten:
(a) Ψ_m ist ein G-Morphismus von G-Moduln.
(b) Falls alle Darstellungen von G komplett reduzibel sind, so ist der Lösungsraum von $\mathrm{Sym}_m(L)$ isomorph zu einem direkten Summanden von $\mathrm{Sym}_m(V)$.
(c) Falls $n = 2$, so ist Ψ_m injektiv und $\mathrm{Sym}_m(L)$ hat Grad $m + 1$.
(d) Falls $n = 3$ und Ψ_i für alle Indizes $i < m$ injektiv ist, so hat $\mathrm{Kern}(\Psi_m)$ höchstens Dimension 1 und $\mathrm{Sym}_m(L)$ hat entweder Ordnung $\frac{1}{2}(m+2)(m+1)$ oder $\frac{1}{2}(m+2)(m+1)-1$.

(e) Falls $n = 3$ und Ψ_i für alle Indizes $i < m - 1$ injektiv ist, so hat $\mathrm{Kern}(\Psi_m)$ *höchstens Dimension* 3 *und* $\mathrm{Sym}_m(L)$ *hat mindestens Ordnung* $\frac{1}{2}(m+2)(m+1) - 3$.

Beweis. Die Aussagen (a) und (b) sind klar. Nach Anmerkung 2.3 können wir die symmetrische Algebra $\mathrm{Sym}_2(V)$ als homogene Polynome vom Grad 2 über F^ϕ auffassen. Wir müssen also zeigen, dass, falls für zwei linear unabhängige Lösungen η_1, η_2 von L, für die $P(\eta_1, \eta_2) = 0$ mit einem Polynom $P \in F^\phi[X_1, X_2]$ homogen vom Grad 2 gilt, es sich bei P nur um das Nullpolynom handeln kann. Der Restklassenkörper des PV-Körpers E stimmt mit F^ϕ überein, da wir die Existenz eines rationalen Punktes vorausgesetzt hatten. Es gilt also

$$0 = \overline{P(\eta_1, \eta_2)} = P(\overline{\eta}_1, \overline{\eta}_2),$$

mit $\overline{\eta}_1, \overline{\eta}_2 \in F^\phi$. D.h. $\overline{\eta}_1 - c\overline{\eta}_2$ teilt P mit $c = \frac{\overline{\eta}_1}{\overline{\eta}_2}$. Mit dem Hensel'schen Lemma können wir diesen Faktor liften und erhalten damit, dass $\eta_1 - c\eta_2$ auch $P(\eta_1, \eta_2)$ teilt. Für den Grad von $Sym_m(L)$ gilt $\binom{2+m-1}{2-1} = \binom{m+1}{1} = m + 1$ und damit ist Behauptung (c) gezeigt. Wir nehmen nun an, dass $n = 3$ gilt und Ψ_i für alle Indizes $i < m$ injektiv ist. Es sei weiter $\{\eta_1, \eta_2, \eta_3\}$ eine Basis des Lösungsraums $V = \mathrm{Sol}_E^\Phi(M_L)$. Falls ein Polynom $P \in F^\phi[X_1, X_2, X_3]$ homogen vom Grad $i < m$ nicht das Nullpolynom ist, so gilt $P(\eta_1, \eta_2, \eta_3) \neq 0$ nach Voraussetzung. Es sei

$$W = \{Q \in F^\phi[X_1, X_2, X_3] \,|\, Q \text{ homogen vom Grad } m \text{ mit } Q(\eta_1, \eta_2, \eta_3) = 0\},$$

dann muss jedes Polynom $0 \neq Q \in W$ irreduzibel sein, denn sonst wäre $P(\eta_1, \eta_2, \eta_3) = 0$ für ein homogenes Polynom P vom Grad echt kleiner als m. Wir nehmen nun an, dass $\mathrm{Kern}(\Psi_m)$ mindestens Dimension 2 hat und wollen dies zu einem Widerspruch führen. Es existieren also zwei teilerfremde irreduzible Polynome Q_1, Q_2 homogen vom Grad m mit $0 = Q_1(\eta_1, \eta_2, \eta_3) = Q_2(\eta_1, \eta_2, \eta_3)$. Dann ist aber die Resultante $Q(\eta_1, \eta_2) = \mathrm{Res}_{\eta_3}(Q_1, Q_2)$ ein homogenes Polynom vom Grad m^2 in η_1 und η_2 mit $Q(\eta_1, \eta_2) = 0$. Jetzt können wir wie in Teil (c) vorgehen und einen nicht-trivialen Faktor finden und erhalten dadurch einen Widerspruch.
Wir gehen jetzt davon aus, dass $n = 3$ gilt und Ψ_i für alle Indizes $i < m - 1$ injektiv ist. Wieder sei $\{\eta_1, \eta_2, \eta_3\}$ eine Basis des Lösungsraums $V = \mathrm{Sol}_E^\Phi(M_L)$. Falls Ψ_{m-1} injektiv ist, so hat der Kern von Ψ_m höchstens Dimension 1 nach Teil (d). Nehmen wir nun an, dass Ψ_{m-1} nicht injektiv ist, so hat $\mathrm{Kern}(\Psi_{m-1})$ Dimension 1. Wir identifizieren die symmetrische Algebra wieder mit den homogenen Polynomen vom Grad $m-1$ nach Anmerkung 2.3. Sei $P \in F^\phi[X_1, X_2, X_3]$ ein homogenes Polynom vom Grad $m-1$, das Kern Ψ_{m-1} erzeugt. Wie wir in Teil (d) schon gesehen haben, muss dieses Polynom irreduzibel sein. Sei

$$W = \{Q \in F^\phi[X_1, X_2, X_3] \,|\, Q \text{ homogen vom Grad } m \text{ mit } Q(\eta_1, \eta_2, \eta_3) = 0\}$$

die Menge der homogenen Polynome vom Grad m mit Nullstelle (η_1, η_2, η_3). Falls ein Element $Q \in W$ nicht von P geteilt wird, so erhalten wir mit demselben Argument der Resultantenbildung aus Teil (d) einen Widerspruch. Also teilt P jedes Polynom aus W. Daher ist W ein Unterraum der homogenen Polynome vom Grad m und wird von den Elementen X_1P, X_2P, X_3P aufgespannt. Damit ist die Dimension von W höchstens 3, was die letzte Behauptung (e) beweist. □

Satz 2.31. *Es sei* $L(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i\phi^i(y) = 0$ *mit* $a_i \in F$ *eine lineare Differenzengleichung vom Grad* n *über* F *mit PV-Körper* E *und einem Fundamentalsystem von Lösungen* $\{\eta_1, \ldots, \eta_n\}$. *Dann existiert eine Differenzengleichung* $\Lambda^m(L)(y)$ *vom Grad höchstens* $\binom{n}{m}$, *deren Lösungsraum von* $\{\Delta_\phi(\eta_{i_1}, \ldots, \eta_{i_m}) \,|\, 1 \le i_1 < \ldots < i_m \le n\}$ *aufgespannt wird.*

Beweis. Dieser Beweis verläuft analog zum Beweis von Satz 2.27. Um die gewünschte Differenzengleichung zu konstruieren definieren wir $v := u \wedge \phi(u) \wedge \cdots \wedge \phi^{m-1}(u)$ mit $u \in \{\eta_1, \ldots, \eta_n\}$ beliebig. Auf dieses v wenden wir wiederholt ϕ an, bis sich eine lineare Abhängigkeit ergibt. Dabei operiert ϕ auf einem äußeren Produkt $u_1 \wedge \cdots \wedge u_m$ via $\phi(u_1 \wedge \cdots \wedge u_m) = \sum_{i=1}^{m} u_1 \wedge \cdots \wedge \phi(u_i) \wedge \cdots \wedge u_m$. Es gilt also

$$\begin{aligned}
v &= u \wedge \phi(u) \wedge \cdots \wedge \phi^{m-1}(u) \\
\phi(v) &= u \wedge \cdots \wedge \phi^{m-2}(u) \wedge \phi^m(u) \\
\phi^2(v) &= u \wedge \cdots \wedge \phi^{m-3}(u) \wedge \phi^{m-1}(u) \wedge \phi^m(u) + u \wedge \cdots \wedge \phi^{m-2}(u) \wedge \phi^{m+1}(u) \\
&\vdots \\
\phi^{n-m}(v) &= \sum_I \phi^{i_1}(u) \wedge \cdots \phi^{i_m}(u) + u \wedge \cdots \wedge \phi^{m-2}(u) \wedge \phi^n(u) \\
&= \sum_I \phi^{i_1}(u) \wedge \cdots \phi^{i_m}(u) + u \wedge \cdots \wedge \phi^{m-2}(u) \wedge -\sum_{i=0}^{n-1} a_i\phi^i(y) \\
&\vdots \\
\phi^r(v) &= \sum_I \alpha_I \varepsilon^I,
\end{aligned}$$

wobei $\varepsilon^I = \phi^{i_0}(u) \wedge \phi^{i_1}(u) \wedge \cdots \wedge \phi^{i_{m-1}}(u)$ und $I = \{(i_0, \ldots, i_{m-1}) \,|\, \text{mit } \sum_{j=0}^{m-1} i_j = m\}$ sind. Da es für solche Tupel in I höchstens $\binom{n}{m}$ verschiedene Möglichkeiten gibt, ergibt sich spätestens bei $r = \binom{n}{m}$ eine lineare Abhängigkeit über F. Diese liefert ein lineares Gleichungssystem und durch dessen Lösung eine Differenzengleichung $\Lambda^m(L)$ für $v = u \wedge \cdots \wedge \phi^{m-1}(u)$ vom Grade höchstens $\binom{n}{m}$, deren Lösungsraum nach Konstruktion von $\{\Delta_\phi(\eta_{i_1}, \ldots, \eta_{i_m}) \,|\, 1 \le i_1 < \ldots < i_m \le n\}$ aufgespannt wird. □

Definition 2.32. Es sei $L(y) = 0$ eine lineare Differenzengleichung vom Grad n. Wir nennen die in Satz 2.31 definierte Differenzengleichung $\Lambda^m(L)$ die **m-te äußere Potenz** von L.

Anmerkung 2.33. Ist M_L der zu der Differenzengleichung L gehörige Frobenius-Modul, so ist der zu $\Lambda^m(L)$ gehörige Frobenius-Modul $M_{\Lambda^m(L)}$ ein Untermodul von $\Lambda^m(M_L)$.

Satz 2.34. *Es seien* $L_1(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i\phi^i(y) = 0$ *und* $L_2(y) := \phi^m(y) + \sum_{i=0}^{m-1} b_i\phi^i(y) = 0$ *mit* $a_i, b_i \in F$ *zwei lineare Differenzengleichungen vom Grad* n *bzw.* m *über* F *mit gemeinsamem PV-Körper* E *und zwei Fundamentalsystemen von Lösungen* $\{\eta_1, \ldots, \eta_n\}$ *bzw.* $\{\mu_1, \ldots, \mu_m\}$. *Dann existiert eine Differenzengleichung* $(L_1 \otimes L_2)(y)$ *vom Grad höchstens* $n \cdot m$, *deren Lösungsraum von* $\{\eta_i \cdot \mu_j \,|\, 1 \le i \le n, 1 \le j \le m\}$ *aufgespannt wird.*

Beweis. Die Konstruktion dieser Differenzengleichung verläuft analog zu den Konstruktionen in den Beweisen der Sätzen 2.27 und 2.31. □

Definition 2.35. Es seien $L_1(y) = 0$ und $L_2(y) = 0$ zwei lineare Differenzengleichungen vom Grad n bzw. m. Wir nennen die in Satz 2.34 definierte Differenzengleichung $(L_1 \otimes L_2)(y)$ den **Tensor-Operator** von L_1 und L_2.

Satz 2.36. *Es sei* $L(y) := \phi^n(y) + \sum_{i=0}^{n-1} a_i \phi^i(y) = 0$ *mit* $a_i \in F$ *eine lineare Differenzengleichung vom Grad* n *über* F *mit Lösungskörper* E *und einem Fundamentalsystem von Lösungen* $\{\eta_1, \ldots, \eta_n\}$. *Dann wird der Lösungsraum der Gleichung* $L^\phi(y) := \phi^n(y) + \sum_{i=0}^{n-1} \phi(a_i)\phi^i(y)$ *von* $\{\phi(\eta_1), \ldots, \phi(\eta_n)\}$ *aufgespannt.*

Beweis. Wir wählen eine beliebige Lösung η aus dem Fundamentalsystem $\{\eta_1, \ldots, \eta_n\}$ aus. Wir setzen $\phi(\eta)$ in die Gleichung L^ϕ ein und erhalten

$$\begin{aligned} L^\phi(\phi(\eta)) &= \phi^n(\phi(\eta)) + \sum_{i=0}^{n-1} \phi(a_i)\phi^i(\phi(\eta)) = \phi(\phi^n(\eta) + \sum_{i=0}^{n-1} a_i \phi^i(\eta)) \\ &= \phi(L(\eta)) = \phi(0) = 0. \end{aligned}$$

Daher wird der Lösungsraum von $L^\phi(y) = 0$ von dem System $\{\phi(\eta_1), \ldots, \phi(\eta_n)\}$ aufgespannt und der Satz ist bewiesen. □

Kapitel 3

Faktorisierung von Differenzen-Operatoren

Bei der Berechnung der Galoisgruppe einer Differenzengleichung wird die Faktorisierung von Differenzen-Operatoren eine wichtige Rolle spielen. Dazu wollen wir zunächst ein Kriterium, ähnlich dem Eisenstein-Kriterium für gewöhnliche Polynome, für die Irreduzibilität solcher Operatoren beweisen. Dann wollen wir zwei Methoden zur Faktorisierung einführen, um letztendlich daraus einen möglichst effizienten Faktorisierungsalgorithmus zu erhalten.

3.1 Ein Eisenstein-Irreduzibilitäts-Kriterium

Dieses Irreduzibilitäts-Kriterium für Differenzen-Operatoren geht auf eine Arbeit von Kovacic [Kov72] zurück, in der er dieses Kriterium allgemeiner für Schiefpolynome entwickelt. Wir wollen seine Ideen auf den Spezialfall unserer Differenzen-Operatoren übertragen. Wie im Kapitel 2 bezeichnen wir mit (R, ϕ) einen relativen Frobenius-Ring mit Quotientenkörper F. Ferner bezeichnen wir mit $\mathfrak{D}_R = R[\tau, \phi]$ den Ring der Differenzen-Operatoren über R.

Definition 3.1. Ein Differenzen-Operator $L = \sum_{i=0}^{n} a_i \tau^i \in \mathfrak{D}_R$ heißt **(ϕ-)primitiv**, falls für das (ϕ-)Ideal $I_L := (a_i \mid 0 \leq i \leq n) \trianglelefteq R$ gilt: $I_L = R$.

Anmerkung 3.2. Für jeden Differenzen-Operator $L \in \mathfrak{D}_R$ existiert ein Ringelement c_L und ein primitiver Differenzen-Operator $L^* \in \mathfrak{D}_R$, so dass $L = c_L L^*$. Dabei sind c_L und L^* bis auf (Links-) Multiplikation mit Einheiten eindeutig.

Bemerkung 3.3. *Es sei $\mathfrak{P} \trianglelefteq R$ ein ϕ-Primideal und der lokale Ring $R_{\mathfrak{P}}$ ein diskreter Bewertungsring. Falls ein Differenzen-Operator $L \in \mathfrak{D}_R$ ϕ-primitiv über $R_{\mathfrak{P}}$ ist, so ist L primitiv über $R_{\mathfrak{P}}$.*

Beweis. Es sei $L = \sum_{i=0}^{n} a_i \tau^i$. Dann existiert ein Ringelement $c_L \in R$ und ein primitiver Differenzen-Operator L^*, so dass $L = c_L L^*$ gilt. Wir unterscheiden nun zwei Fälle. Liegt c_L nicht in $\mathfrak{P}R_{\mathfrak{P}}$, so ist c_L eine Einheit in $R_{\mathfrak{P}}$ und damit ist L primitiv.
Liegt aber c_L in $\mathfrak{P}R_{\mathfrak{P}}$, so gilt für das ϕ-Ideal I_L:

$$I_L \trianglelefteq (c_L)_\phi \subsetneq \mathfrak{P}R_P,$$

wobei $(c_L)_\phi$, das von c_L erzeugte ϕ-Hauptideal bezeichnet. Dies steht aber im Widerspruch zur Voraussetzung, dass L ein ϕ-primitiver Differenzen-Operator über $R_\mathfrak{P}$ ist, d.h. $I_L = R_\mathfrak{P}$. □

Bemerkung 3.4. *Es sei R ein diskreter Bewertungsring mit der Eigenschaft, dass jedes echte ϕ-Ideal in einem ϕ-Primideal enthalten ist. Dann ist für ϕ-primitive (über R) Differenzen-Operatoren $M, N \in \mathfrak{D}_R$ auch das Produkt $L = MN$ ein ϕ-primitiver Operator.*

Beweis. Die beiden Differenzen-Operatoren M, N seien in der Darstellung $M = \sum_{i=0}^{m} a_i\tau^i, N = \sum_{j=0}^{n} b_j\tau^j$ gegeben. Dann gilt für das Produkt

$$\begin{aligned} L &= MN = \sum_{i=0}^{m} a_i\tau^i \sum_{j=0}^{n} b_j\tau^j = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i\tau^i b_j\tau^j \\ &= \sum_{i=0}^{m}\sum_{j=0}^{n} a_i\phi^i(b_j)\tau^{i+j} = \sum_{l=0}^{m+n} c_l\tau^l. \end{aligned}$$

Wir wollen nun annehmen, dass L nicht ϕ-primitiv über R ist und dies zu einem Widerspruch führen. Dazu sei $\mathfrak{P} \trianglelefteq R$ ein ϕ-Primideal, dass alle Koeffizienten c_l für $0 \le l \le m+n$ enthält, also $I_L \subseteq \mathfrak{P}$. Da M und N aber ϕ-primitiv sind, existieren maximale Indizes $0 \le r \le m$ bzw. $0 \le s \le n$, so dass a_r und b_s nicht in $\mathfrak{P}$ liegen. Dann gilt für den $(r+s)$-ten Produktkoeffizienten

$$c_{r+s} = \sum_{i=0}^{r} \sum_{j+i=r+s} a_i\phi^i(b_j).$$

Für die Indizes gilt $r+s = j+i \le j+r$ und damit $s \le j$, wobei Gleichheit im Falle von $i = r$ auftritt. Daraus erhalten wir, dass $a_r\phi^r(b_s) \equiv 0 \bmod \mathfrak{P}$, wobei aber nach Voraussetzung $a_r \notin \mathfrak{P}$ gilt. Da $\mathfrak{P}$ ein Primideal ist, muss also $\phi^r(b_s)$ in $\mathfrak{P}$ liegen und damit auch $b_s \in \mathfrak{P}$. Dies steht im Widerspruch zur Annahme, dass $b_s \notin \mathfrak{P}$ gilt. □

Bemerkung 3.5. *Es sei R ein diskreter Bewertungsring mit Quotientenkörper F. Ist ein Differenzen-Operator $L \in \mathfrak{D}_R$ reduzibel über F, so existieren Ringelemente $P, Q \in R$ und Differenzen-Operatoren $M, N \in \mathfrak{D}_R$, primitiv über R, so dass $QL = PMN$ gilt.*

Beweis. Es sei die Faktorisierung $L = \tilde{M}\tilde{N}$ mit $\tilde{M}, \tilde{N} \in \mathfrak{D}_F$, wobei $\tilde{M} = \sum_{i=0}^{m} a_i\tau^i$ gegeben. Wir wählen nun ein Element $f \in F$, so dass $N := f\tilde{N}$ in $\mathfrak{D}_R$ liegt und primitiv über R ist. Weiterhin wählen wir Ringelemente $P, Q \in R$ mit $PQ \neq 0$, so dass

$$M := \frac{Q}{P}\sum_{k=0}^{m}\sum_{i=k}^{m} a_i\phi^k(\frac{1}{f})\tau^k$$

in $\mathfrak{D}_R$ liegt und primitiv über R ist. Dann gilt für das Produkt

$$\begin{aligned} QMN &= P\frac{Q}{P}(\sum_{k=0}^{m}\sum_{i=k}^{m} a_i\phi^k(\frac{1}{f})\tau^k)f\tilde{N} \\ &= Q(\sum_{k=0}^{m}\sum_{i=k}^{m} a_i\tau^k)\frac{1}{f}f\tilde{N} \\ &= Q\tilde{M}\tilde{N} = QL \end{aligned}$$

und damit ist die Behauptung bewiesen. □

Korollar 3.6. *Es sei R ein ϕ-Integritätsbereich mit Quotientenkörper F und $\mathfrak{P} \trianglelefteq R$ ein ϕ-Primideal. Ferner sei der lokale Ring $R_\mathfrak{P}$ ein diskreter Bewertungsring. Ist dann ein Differenzen-Operator $L \in \mathfrak{D}_{R_\mathfrak{P}}$ reduzibel über F, so ist L reduzibel über $R_\mathfrak{P}$.*

Beweis. Da L reduzibel über F ist, existieren nach Bemerkung 3.5 Ringelemente $P, Q \in R_\mathfrak{P}$ mit $PQ \neq 0$ und Differenzen-Operatoren $M, N \in \mathfrak{D}_{R_\mathfrak{P}}$, primitiv über $R_\mathfrak{P}$, so dass $QL = PMN$ gilt. Ferner existiert ein Ringelement $c_L \in R_\mathfrak{P}$ und ein Differenzen-Operator $L^* \in \mathfrak{D}_{R_\mathfrak{P}}$, primitiv über $R_\mathfrak{P}$, so dass $L = c_L L^*$ gilt. Für jedes echte ϕ-Ideal $I \trianglelefteq R_\mathfrak{P}$ gilt $I \trianglelefteq \mathfrak{P}R_\mathfrak{P}$ und $\mathfrak{P}R_\mathfrak{P}$ ist ϕ-Ideal. Dann ist das Produkt MN nach Bemerkung 3.4 ϕ-primitiv und darüber hinaus nach Bemerkung 3.3 primitiv über $R_\mathfrak{P}$. Es existiert also eine Einheit $u \in R_\mathfrak{P}$, so dass $P = Qc_L u$ gilt. Daraus ergibt sich für

$$L = Q^{-1}PMN = (c_L u P^{-1})PMN = c_L uMN$$

und damit ist L reduzibel über $R_\mathfrak{P}$. □

Satz 3.7. *(Eisenstein-Kriterium)*
Es sei R ein ϕ-Integritätsbereich mit Quotientenkörper F, $\mathfrak{P} \trianglelefteq R$ ein ϕ-Primideal und der lokale Ring $R_\mathfrak{P}$ sei ein diskreter Bewertungsring. Dann ist ein Differenzen-Operator $L = \sum_{i=0}^{l} c_i\tau^i \in \mathfrak{D}_R$ mit $c_i \in \mathfrak{P}$ für $1 \leq i \leq l$, $c_0 \notin \mathfrak{P}$ und $c_l \notin \mathfrak{P}^2$ irreduzibel über F.

Beweis. Da L reduzibel über F ist, existieren nach Folgerung 3.6 Differenzen-Operatoren $M = \sum_{i=0}^{m} a_i\tau^i, N = \sum_{j=0}^{n} b_j\tau^j \in \mathfrak{D}_{R_\mathfrak{P}}$ mit

$$L = MN = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i\phi^i(b_j)\tau^{i+j}$$

und $c_{m+n} = a_m\phi^m(b_n)$. Wir unterscheiden zwei Fälle. Wir nehmen zunächst an, dass $a_m \in \mathfrak{P}R_\mathfrak{P}$ und $\phi^m(b_n) \notin \mathfrak{P}R_\mathfrak{P}$ gilt. Sei nun $0 \leq r \leq m$ der minimale Index, so dass $a_i\mathfrak{P}R_\mathfrak{P}$ für alle $i \geq r$ gilt. Da $c_0 = a_0 b_0$ nicht in $\mathfrak{P}$ liegt, muss $r > 0$ sein. Also liegt c_{n+r-1} in $\mathfrak{P}$. Außerdem hat dieser Koeffizient die Darstellung

$$c_{n+r-1} = \sum_{i=0}^{m}\sum_{j+i=n+r-1} a_i\phi^i(b_j),$$

wobei für die Indizes $n+r-1 = j+i \leq n+i$ und damit $r-1 \leq i$ gilt. Es tritt Gleichheit auf, falls $j = n$ ist. Dies liefert die Kongruenz $0 \equiv a_{r-1}\phi^{r-1}(b_n) \bmod \mathfrak{P}R_{\mathfrak{P}}$, wobei $a_{r-1} \notin \mathfrak{P}R_{\mathfrak{P}}$ gilt. Dies induziert aber, dass $\phi^{r-1}(b_n)$ und damit auch $\phi^m(b_n)$ in $\mathfrak{P}R_{\mathfrak{P}}$ liegt, was im Widerspruch zur Annahme steht.
Jetzt gelte andererseits $a_m \notin \mathfrak{P}R_{\mathfrak{P}}$ und $\phi^m(b_n) \in \mathfrak{P}R_{\mathfrak{P}}$. Sei $0 \leq s \leq n$ der minimale Index, so dass $\phi^m(b_j) \in \mathfrak{P}R_{\mathfrak{P}}$ für alle $j \geq s$. Da $\phi^m(c_0) = \phi^m(a_0)\phi^m(b_0)$ nicht in $\mathfrak{P}$ liegt, muss $s > 0$ sein und damit $c_{m+s-1} \in \mathfrak{P}$ liegen. Dieser Koeffizient besitzt die folgende Darstellung

$$c_{m+s-1} = \sum_{i=0}^{m} \sum_{j+i=m+s-1} a_i\phi^i(b_j),$$

wobei für die Indizes $m+s-1 = j+i \leq j+m$ und damit $s-1 \leq j$ gilt. Gleichheit tritt auf, falls $i = m$ ist. Dies liefert die Kongruenz $0 \equiv a_m\phi^m(b_{s-1}) \bmod \mathfrak{P}R_{\mathfrak{P}}$, wobei $\phi^m(b_{s-1})$ nicht in $\mathfrak{P}R_{\mathfrak{P}}$ liegt. Also muss $a_m \in \mathfrak{P}R_{\mathfrak{P}}$ gelten, was im Widerspruch zur Annahme steht. Wir haben beide Fälle zum Widerspruch geführt, folglich muss L irreduzibel über F sein. □

3.2 Der Eigenring und Reduzibilität

In diesem Abschnitt bezeichnet wieder R einen relativen Frobenius-Ring mit Quotientenkörper F und $\mathfrak{D} = \mathfrak{D}_F = F[\tau, \phi]$ den Ring der Differenzen-Operatoren über F.

Definition 3.8. Es sei $L \in \mathfrak{D}$ ein Differenzen-Operator. Wir definieren die **Idealisierung** des Ideals $\mathfrak{D}L$ durch

$$I(L) := \{u \in \mathfrak{D} \mid Lu \in \mathfrak{D}L\}.$$

Der dadurch erhaltene Quotient

$$\begin{aligned} \mathrm{E}(L) &:= I(L)/\mathfrak{D}L \\ &\cong \{u \in \mathfrak{D} \mid \text{ es existiert ein } \tilde{u} \in \mathfrak{D} : Lu = \tilde{u}L \text{ und } \deg_\tau(u) < \deg_\tau(L)\} \end{aligned}$$

heißt der **Eigenring** von L.

Anmerkung 3.9. Die Idealisierung $I(L)$ ist die größte Unteralgebra von $\mathfrak{D}$, so dass $\mathfrak{D}L$ ein zweiseitiges Ideal darin bildet. Außerdem ist der Eigenring $\mathrm{E}(L)$ eine assoziative Algebra über F^ϕ.

Bemerkung 3.10. *Es sei $L \in \mathfrak{D}$ ein Differenzen-Operator. Dann ist der Eigenring $\mathrm{E}(L)$ eine F^ϕ-Unteralgebra von $\mathrm{End}(\mathfrak{D}/\mathfrak{D}L)$.*

Beweis. Die F^ϕ-lineare Abbildung

$$\begin{array}{rccc} \Psi: & \mathrm{E}(L) & \longrightarrow & \mathrm{End}(\mathfrak{D}/\mathfrak{D}L) \\ & u & \longmapsto & \psi_u: \begin{array}{ccc} \mathfrak{D}/\mathfrak{D}L & \longrightarrow & \mathfrak{D}/\mathfrak{D}L \\ f & \longmapsto & fu \end{array} \end{array}$$

ist offensichtlich injektiv. □

Satz 3.11. *Es sei $L \in \mathfrak{D}$ ein Differenzen-Operator. Existieren im Eigenring $\mathrm{E}(L)$ nichttriviale Nullteiler $u, v \in I(L)\backslash\mathfrak{D}L$, d.h. $u \cdot v \in \mathfrak{D}L$ bzw. $u \cdot v = 0$ in $\mathrm{E}(L)$, so ist L reduzibel über F, d.h. es existieren Differenzen-Operatoren $L_1, L_2 \in \mathfrak{D}\backslash F$ mit $L = L_1L_2$.*

Beweis. Wir gehen davon aus, dass im Eigenring $\mathrm{E}(L)$ nicht-triviale Nullteiler u und v mit $u \cdot v \in \mathfrak{D}L$ existieren. Wir wollen zeigen, dass $L_2 := \mathrm{ggrT}(L, u) \neq 1$ und dass L rechtsteilbar durch L_2 ist. Die zweite Behauptung ist klar, da $L_2 = \mathrm{ggrT}(L, u)$ ist. Also nehmen wir an, dass $L_2 = 1$ gilt und wollen dies zu einem Widerspruch führen. Dann existieren Differenzen-Operatoren $Q_1, Q_2 \in \mathfrak{D}$ mit $Q_1 L + Q_2 u = 1$. Multiplizieren wir diese Gleichung von rechts mit v, so erhalten wir

$$Q_1 \underbrace{Lv}_{\in \mathfrak{D}L} + Q_2 \underbrace{uv}_{\in \mathfrak{D}L} = v$$

und damit, dass v in $\mathfrak{D}L$ liegt. Dies steht im Widerspruch zu unserer Annahme, also gilt $L_2 \neq 1$. Da $\deg_\tau(u)$ und $\deg_\tau(v)$ ohne Einschränkung kleiner sind als $\deg_\tau(L)$, erhalten wir die Faktorisierung $L = L_1 L_2$ und damit ist der Satz bewiesen. □

Algorithmus 3.12. (Eigenring-Faktorisierungsalgorithmus)
Eingabe: Ein Differenzen-Operator $L \in \mathfrak{D}$.

1. Finde nicht-triviale Nullteiler u, v im Eigenring $\mathrm{E}(L)$ mit $u \cdot v \in \mathfrak{D}L$. Falls keine Nullteiler gefunden wurden, beende den Algorithmus mit der Nachricht, dass keine Faktorisierung gefunden wurde.
2. Berechne $L_2 := \mathrm{ggrT}(L, u)$.
3. Teile L von rechts durch L_2. Dies liefert Faktorisierung $L = L_1 L_2$.
4. Starte bei Schritt 1 für L_1 und L_2 bis eine vollständige Faktorisierung gefunden wurde oder keine weitere Faktorisierung mehr möglich ist.

Mit Satz 3.11 haben wir jetzt eine Möglichkeit gefunden einen Differenzen-Operator L zu faktorisieren. Es könnte jedoch sein, dass wir keine Nullteiler im Eigenring $\mathrm{E}(L)$ finden aber L trotzdem nicht irreduzibel ist. Für diesen Fall können wir das Eisenstein-Irreduzibilitäts-Kriterium anwenden. Falls wir damit auch nicht entscheiden können, ob L irreduzibel ist, benötigen wir einen anderen Algorithmus. Dieser sollte die Irreduzibilität von L garantieren, falls keine Rechtsfaktoren von L gefunden werden.

3.3 Die Beke-Faktorisierungsmethode

Diese Faktorisierungsmethode geht auf einen Algorithmus von Beke [Bek94] zur Faktorisierung von Differentialgleichungen aus dem Jahr 1894 zurück. Da Differential-Operatoren sehr ähnlich zu unseren Differenzen-Operatoren sind, wollen wir diesen Algorithmus auf unser Setting übertragen. Der Beke-Algorithmus liefert entweder eine vollständige Faktorisierung des Differenzen-Operators L oder die Irreduzibilität, falls keine Faktoren gefunden werden. Im Laufe der Zeit wurde dieser Algorithmus hinsichtlich Effizienz wesentlich verbessert. Dennoch ist er nicht laufzeit-optimal. Dies liegt darin begründet, dass man viele Operatoren bzw. Moduln von hohen Graden konstruieren muss. Daher wollen wir diesen Algorithmus erst benutzen, wenn wir mit der Eigenring-Methode bzw. dem Eisenstein-Irreduzibilitäts-Kriterium keine weiteren Information erhalten, aber noch keine vollständige Faktorisierung gefunden haben.

Algorithmus 3.13. (Beke-Faktorisierungsalgorithmus)
Eingabe: Ein Differenzen-Operator $L \in \mathfrak{D}$ mit zugehörigem Frobenius-Modul M. Setze $d := 1$.

1. Falls $d = n$ gehe zu Schritt 6, sonst berechne die äußere Algebra $\Lambda^d(M)$.
2. Finde zerlegbare Elemente $\mathfrak{a}_i$ in $\Lambda^d(M)$ gemäss Satz 2.8. Wurden keine zerlegbaren Elemente gefunden, setze $d := d + 1$ und gehe zu Schritt 1.
3. $\mathfrak{a}_i = m_{i1} \wedge \cdots \wedge m_{id}$ liefert nach Satz 2.9 einen d-dimensionalen Untermodul $N_i \leq M$ mit Basis $\{m_{i1}, \ldots, m_{id}\}$.
4. Der zum Modul N_i gehörige Differenzen-Operator L_i vom Grad d ist ein Kandidat für einen Rechtsfaktor von L. Teile L von rechts durch L_i, um zu testen, welcher Kandidat in Frage kommt.
5. Wurde ein Faktor vom Grad d gefunden, faktorisiere diesen weiter. Sonst setze $d := d + 1$ und gehe zu Schritt 1.
6. Gib die gefundene Faktorisierung $L = L_r \cdots L_1$ aus oder, falls keine Faktorisierung gefunden wurde, eine Nachricht, dass L irreduzibel ist.

Mit Algorithmus 3.13 finden wir entweder eine vollständige Faktorisierung oder wir wissen, dass L irreduzibel ist. Man sieht aber, dass wir für jedes d die äußere Algebra vom Grad $\binom{n}{d}$ berechnen und darin zerlegbare Vektoren finden müssen. Dies ist nicht sonderlich effizient. Daher wollen wir den Beke-Algorithmus nur dann verwenden, wenn alle anderen Faktorisierungsmethoden kein Ergebnis geliefert haben.

3.4 Der kombinierte Faktorisierungsalgorithmus

Wir wollen nun aus den bekannten Faktorisierungsmethoden und Irreduzibilitätskriterien einen kombinierten, möglichst effizienten Algorithmus erhalten.

Algorithmus 3.14. (Faktorisierungsalgorithmus für Differenzen-Operatoren)
Eingabe: Ein Differenzen-Operator $L \in \mathfrak{D}$ mit zugehörigem Frobenius-Modul M.

1. Wende das Eisenstein-Irreduziblitäts-Kriterium auf L an. Falls L irreduzibel ist, gehe zu Schritt 5.
2. Faktorisiere L soweit wie möglich mit dem Eigenring-Algorithmus 3.12.
3. Wende auf die Faktoren das Eisenstein-Irreduzibilitäts-Kriterium an. Sind alle Faktoren irreduzibel sind, gehe zu Schritt 5.
4. Wende auf die gefundenen reduziblen Faktoren den Beke-Algorithmus 3.13 an.
5. Gib die gefundene Faktorisierung $L = L_r \cdots L_1$ aus oder, falls keine Faktorisierung gefunden wurde, eine Nachricht, dass L irreduzibel ist.

Kapitel 4

Berechnung der Galoisgruppe für Gleichungen vom Grad 1

In diesem Kapitel bezeichnen wir mit $R := \mathbb{F}_q[t, s]$ den Polynomring in zwei Variablen über einem endlichen Körper $\mathbb{F}_q$ mit einer Primzahlpotenz $q = p^d$. Dieser Ring wird zu einem relativen Frobenius-Ring mit definierendem Ideal $Q = (t)$ durch den Endomorphismus $\phi : R \longrightarrow R$ definiert durch $\phi|_{\mathbb{F}_q} = \phi_{p^m}$ und $\phi(t) = t$, $\phi(s) = s^{p^m}$, wobei $1 \leq m \leq d$ gilt. Ferner bezeichnen wir mit $F := \mathrm{Quot}(R) = \mathbb{F}_q(t, s)$ den Quotientenkörper von R. Dieser wird in natürlicher Weise ein Frobenius-Körper mit Frobenius-Invarianten $F^\phi = \mathbb{F}_{p^m}(t)$, falls d durch m teilbar ist, sonst gilt $F^\phi = \mathbb{F}_p(t)$.

4.1 Multiplikative Gleichungen

Wir betrachten die lineare Differenzengleichung $L(y) = \phi(y) + a_0 y$ vom Grad 1 und suchen Lösungen für $L(y) = 0$ bzw. $\phi(y) = a \cdot y$ mit $a := -a_0 \in F$. Nach Satz 1.18 kommen für die Galoisgruppe $G := \mathrm{Gal}(L)$ nur die $\mathbb{G}_{\mathrm{m}}(F^\phi) = (F^\phi)^\times$ oder endliche (zyklische) Untergruppen von $(F^\phi)^\times$ in Frage. Wir benötigen ein Entscheidungskriterium, ob die volle Gruppe $(F^\phi)^\times$ oder eine echte Untergruppe als Galoisgruppe auftritt. Zunächst wollen wir sehen, wann eine Differenzengleichung eine rationale Lösung, d.h. eine Lösung im Grundkörper F besitzt.

Satz 4.1. *Eine Differenzengleichung $\phi(y) = ay$ hat genau dann eine rationale Lösung $\eta \in F$ mit $\frac{\phi(\eta)}{\eta} = a$, falls die triviale Gruppe als Galoisgruppe auftritt.*

Beweis. Die Differenzengleichung $\phi(y) = ay$ hat genau dann die triviale Gruppe als Galoisgruppe, wenn eine Lösung η im Grundkörper F existiert, d.h. $\phi(\eta) = a\eta$. Schreiben wir diese Identität um, so erhalten wir $\frac{\phi(\eta)}{\eta} = a$. □

Falls also eine rationale Lösung $\eta \in F$ mit $\frac{\phi(\eta)}{\eta} = a$ existiert, so ist die Galoisgruppe G die triviale Gruppe.
Wir gehen nun davon aus, dass ein solches $\eta \in F$ existiert. Dann können wir sowohl η als auch a als Bruch teilerfremder Polynome darstellen, also $\eta = \frac{\eta_1(t)}{\eta_2(t)}$, $a = \frac{a_1(t)}{a_2(t)}$ mit $\eta_1(t), \eta_2(t) \in \mathbb{F}_q(s)[t]$ teilerfremd und $a_1(t), a_2(t) \in \mathbb{F}_q(s)[t]$ teilerfremd. Damit lässt sich

obige Gleichung umschreiben zu

$$a = \frac{a_1(t)}{a_2(t)} = \frac{\phi(\eta)}{\eta} = \frac{\phi(\eta_1(t))}{\phi(\eta_2(t))}\frac{\eta_2(t)}{\eta_1(t)}. \tag{4.2}$$

Für die weiteren Betrachtungen benötigen wir das folgende Lemma.

Lemma 4.3. *Sind die Polynome $f_1(t), f_2(t) \in \mathbb{F}_q(s)[t]$ teilerfremd, so sind auch deren ϕ-Bilder $\phi(f_1(t))$ und $\phi(f_2(t))$ teilerfremd.*

Beweis. Wir nehmen an, dass $\phi(f_1)$ und $\phi(f_2)$ nicht teilerfremd sind, d.h. es existiert ein nicht-trivialer größter gemeinsamer Teiler $1 \neq d := \mathrm{ggT}(\phi(f_1), \phi(f_2))$ mit $\phi(f_1) = d \cdot r_1$ und $\phi(f_2) = d \cdot r_2$. Da $\phi(f_1)$, $\phi(f_2) \in \mathrm{Bild}(\phi)$ liegen und $\phi(\mathbb{F}_q(s)[t])$ ein Hauptidealring ist, muss auch $d \in \mathrm{Bild}(\phi)$ liegen. Es existiert also ein Polynom $\tilde{d} \in \mathbb{F}_q(s)[t]$ mit $\phi(\tilde{d}) = d$. Entsprechend finden wir Polynome $\tilde{r}_1$, $\tilde{r}_2 \in \mathbb{F}_q(s)[t]$ mit $\phi(\tilde{r}_1) = r_1$ und $\phi(\tilde{r}_2) = r_2$. Damit erhalten wir die Zerlegungen $\tilde{d} \cdot \tilde{r}_1 = f_1$ und $\tilde{d} \cdot \tilde{r}_2 = f_2$. Da aber f_1 und f_2 als teilerfremd vorausgesetzt wurden, gilt $\tilde{d} = 1$ und wir erhalten durch $d = \phi(\tilde{d}) = \phi(1) = 1$ einen Widerspruch. □

Mit Lemma 4.3 sehen wir, dass eine rationale Lösung nur existieren kann, wenn die Eingabedaten, also $a = \frac{a_1}{a_2}$ eine spezielle Gestalt haben, z.B. müssen die Grade in t von a_1 und a_2 übereinstimmten, also $\deg_t(a_1) = \deg_t(a_2)$. Außerdem müssen die ϕ-Bilder der Primfaktoren des Zählers im Nenner vorkommen und umgekehrt. Falls ein Primfaktor gemeinsame Teiler mit seinem ϕ-Bild hat, kürzen sich diese und kommen in a nicht vor. Diese gemeinsamen Teiler kann man aber aus dem Restfaktor wieder berechnen. Also können wir aus der Form der obigen Gleichung (4.2) einen Algorithmus zur Bestimmung einer rationalen Lösung $\eta \in F$ ableiten. Dazu benötigen wir noch die folgende Definition:

Definition 4.4. Es sei R ein relativer Frobenius-Ring mit definierendem Ideal Q und Endomorphismus ϕ. Ein Element $r \in R$ heißt **periodisch**, falls eine natürliche Zahl $k \in \mathbb{N}$ mit $\phi^k(r) = r$ existiert. Wir nennen das Minimum solcher Zahlen k die **Länge der Periode**.

Bemerkung 4.5. *Es sei $R = \mathbb{F}_q[s,t]$ der relative Frobenius-Ring mit $q = p^m$ und definierendem Ideal $Q = (t)$ sowie dem Endomorphimus ϕ, wobei $\phi(x) = x^p$ für alle $x \in \mathbb{F}_q[s]$ gilt. Dann gelten:*
(a) Ein Element $f = \sum_{i=0}^{n} a_i(s)t^i \in R_Q = \mathbb{F}_q(s)[t]$ ist genau dann periodisch, falls alle $a_i(s)$ in $\mathbb{F}_q$ liegen, also nicht von s abhängen. Dabei ist die Länge der Periode höchstens m.
(b) Für zwei periodische Elemente $a_1, a_2 \in F$ mit Längen $k_1, k_2 \in \mathbb{N}$ sind auch die Summe und das Produkt von a_1 und a_2 periodisch von der Länge höchstens $\mathrm{kgV}\{k_1, k_2\}$.

Beweis. Es sei zunächst $f = \sum_{i=0}^{n} a_i(s)t^i$ ein periodisches Element in $\mathbb{F}_q(s)[t]$, d.h. es existiert eine natürliche Zahl $k \in \mathbb{N}$ mit $\phi^k(f) = f$. Wir rechnen die linke Seite der Gleichung direkt aus und erhalten

$$\phi^k(f) = \sum_{i=0}^{n} \phi(a_i(s))t^i = \sum_{i=0}^{n} a_i(s)^{p^k} t^i.$$

Durch Koeffizientenvergleich erhalten wir, dass $a_i(s) = a_i(s)^{p^k}$ gelten muss. Da ϕ injektiv ist, ist dies nur möglich, falls $a_i(s)$ nicht von s abhängt. Denn andernfalls würden die Grade in den s kontinuierlich wachsen.
Ist dagegen umgekehrt $f = \sum_{i=0}^{n} a_i t^i$ mit $a_i \in \mathbb{F}_q$ gegeben, so ist direkt ersichtlich, dass f periodisch sein muss. Außerdem wird f spätestens beim m-ten Schritt periodisch, denn für alle $x \in \mathbb{F}_q$ gilt $\phi^m(x) = x^{p^m} = x^q = x$. Dies beweist Teil (a).
Um Teil (b) zu beweisen, zeigen wir zunächst, dass für das periodische Element a_1 mit Länge k_1, also $\phi^{k_1}(a_1) = a_1$ für jede natürliche Zahl $n \in \mathbb{N}$ auch $\phi^{n \cdot k_1}(a_1) = a_1$ gelten muss. Dies erhalten wir durch direktes Ausrechnen:

$$\phi^{n \cdot k_1}(a_1) = \phi^{(n-1) \cdot k_1}(\phi^{k_1}(a_1)) = \phi^{(n-1) \cdot k_1}(a_1) = \cdots = \phi^{k_1}(a_1) = a_1.$$

Dies impliziert, dass für jedes ϕ-periodische Element a_1 mit Länge k_1 auch $\phi^k(a_1) = a_1$ gilt, wenn k von der Länge k_1 geteilt wird. Damit gilt also, dass für das Produkt $a_1 \cdot a_2$ bzw. die Summe $a_1 + a_2$ spätestens bei $\mathrm{kgV}\{k_1, k_2\}$-facher Anwendung von ϕ

$$\phi^{\mathrm{kgV}\{k_1,k_2\}}(a_1 \cdot a_2) = \phi^{g_1 k_1}(a_1) \cdot \phi^{g_2 k_2}(a_2) = a_1 \cdot a_2 \text{ bzw.}$$
$$\phi^{\mathrm{kgV}\{k_1,k_2\}}(a_1 + a_2) = \phi^{g_1 k_1}(a_1) + \phi^{g_2 k_2}(a_2) = a_1 + a_2$$

gilt. Damit sind sowohl das Produkt $a_1 \cdot a_2$ als auch die Summe $a_1 + a_2$ periodisch von der Länge höchstens $\mathrm{kgV}\{k_1, k_2\}$. □

Algorithmus 4.6. (zur Berechnung einer rationalen Lösung $\eta \in F$)
Eingabe: Eine Differenzengleichung ersten Grades $\phi(y) = ay$ mit $a = \frac{a_1(t)}{a_2(t)} \in \mathbb{F}_q(s,t)$

1. **if** $\deg_t(a_1) = \deg_t(a_2)$ **then**
   setze $\eta_1 = \eta_2 = 1$ und gehe zu Schritt 2
   else
   gehe zu Schritt 5.
   end if

2. Zerlege a_1 und a_2 in Primfaktoren p_{1j}, p_{2k} mit Vielfachheit v_{1j}, v_{2k} für $j = 1, \ldots, r$ bzw. $k = 1, \ldots s$. Dabei sind r bzw. s die Anzahl der Primfaktoren von a_1 bzw. a_2.

3. Gehe die Primfaktoren von a_1 durch
   for $j = 1$ to r **do**
   if p_{1j} nicht periodisch **then**
   if $p_{1j} \in \mathrm{Bild}(\phi)$ **then**
   setze $g := \phi^{-1}(p_{1j}), \eta_1 := \eta_1 \cdot g$.
   while $\phi^{-1}(g) \neq g$ **do**
   setze $g := \phi^{-1}(g), \eta_1 := \eta_1 \cdot g$.
   end while
   end if
   else
   for $h = 1$ to Periodenlänge von p_{1j} **do**
   if $\phi^h(p_{1j}^{v_{1j}}) \in (p_{2k})_{k=1}^{s}$ **then**
   $\eta_2 := \prod_{l=0}^{h-1} \phi^l(p_{1j}^{v_{ij}})$

end if
end for
end if
end for

4. Führe Schritt 3 für die Primfaktoren von a_2 durch und setze dann $\eta := \frac{\eta_1}{\eta_2}$
5. **if** $\frac{\phi(\eta)}{\eta} = a$ **then**
   Gib die rationale Lösung η aus.
   else
   Es gibt keine rationale Lösung.
   end if

Beispiel 4.7. Es sei $\phi(y) = ay$ mit

$$a = \frac{(t-s)^2(t-s^9)(t+s)}{(t^3-s)(t+s^3)}$$

eine Differenzengleichung über dem Frobenius-Körper $F = \mathbb{F}_9(s,t)$ mit dem Frobenius-Endomorphismus ϕ. Dabei operiert ϕ auf $\mathbb{F}_9(s)$ als 3-te Potenz und lässt das Ideal (t) invariant, d.h. $F^\phi = \mathbb{F}_3(t)$. Mit Hilfe von Algorithmus 4.6 finden wir eine rationale Lösung

$$\eta = \frac{(t^3-s)(t-s)(t-s^3)}{(t+s)}.$$

Zur Probe berechnen wir

$$\frac{\phi(\eta)}{\eta} = \frac{(t-s)^3(t-s^3)(t-s^9)(t+s)}{(t+s^3)(t^3-s)(t-s)(t-s^3)} = \frac{(t-s)^2(t-s^9)(t+s)}{(t^3-s)(t+s^3)} = a.$$

Satz 4.8. *Es sei $\phi(y) = ay$ mit $a \in F$ eine Differenzengleichung vom Grad 1 mit zugehöriger Galoisgruppe G. Diese ist genau dann eine endliche zyklische Gruppe, falls eine natürliche Zahl $n \in \mathbb{N}$ existiert, so dass die Gleichung $\phi(y) = a^n y$ triviale Galoisgruppe besitzt.*

Beweis. Es sei E ein PV-Körper unserer Differenzengleichung und $f \in E$ eine Lösung, d.h. $\phi(f) = af$. Die Galoisgruppe G ist nach Satz 1.30 (a) genau dann endlich, falls f algebraisch über F ist. Dann muss aber nach Bemerkung 1.29 eine natürliche Zahl $n \in \mathbb{N}$ und ein Körperelement $k \in F$ existieren, so dass $f^n = k$. Setzen wir dies in unsere Differenzengleichung ein, ergibt sich

$$\phi(k) = \phi(f^n) = \phi(f)^n = (af)^n = a^n f^n = a^n k,$$

d.h. die Gleichung $\phi(y) = a^n y$ hat eine Lösung k im Grundkörper F und damit triviale Galoisgruppe. □

Satz 4.9. *Es sei $\phi_{p^m}(y) = ay$ mit $a \in F = \mathbb{F}_q(s,t)$ eine Differenzengleichung vom Grad 1 mit zugehöriger Galoisgruppe G. Diese ist genau dann die volle multiplikative Gruppe $G = (F^\phi)^\times$, falls keine der potenzierten Gleichungen $\phi(y) = a^h y$ eine rationale Lösung besitzt, wobei h ein Teiler von $p-1$ (falls $F^\phi = \mathbb{F}_p(t)$) bzw. $p^m - 1$ (falls $F^\phi = \mathbb{F}_{p^m}(t)$) ist.*

Beweis. Als Galoisgruppe kommen nur endliche Untergruppen von $\mathbb{G}_{\mathrm{m}}(F^{\phi})$ oder $\mathbb{G}_{\mathrm{m}}(F^{\phi})$ selbst in Frage. Falls eine der potenzierten Gleichungen $\phi(y) = a^h y$ eine rationale Lösung besitzt, so ist die Galoisgruppe eine endliche zyklische Gruppe der Ordnung h nach Satz 4.8. Da die Frobeniusinvarianten F^{ϕ} durch $\mathbb{F}_p(t)$ bzw. $\mathbb{F}_{p^m}(t)$ gegeben sind, kann als endliche Galoisgruppe höchstens eine zyklische Gruppe der Ordnung $p-1$ bzw. p^m-1 auftreten. Falls keine der potenzierten Gleichungen eine rationale Lösung besitzt, muss also die volle $\mathbb{G}_{\mathrm{m}}(F^{\phi})$ als Galoisgruppe auftreten. □

Um zu entscheiden, ob die Galoisgruppe der Differenzengleichung $\phi(y) = ay$ endlich ist, genügt es also zu überprüfen, ob es eine natürliche Zahl $n \in \mathbb{N}$ gibt, so dass die potenzierte Gleichung $\phi(y) = a^n y$ die triviale Gruppe als Galoisgruppe besitzt. Dies ist aber äquvalent dazu, dass die potenzierte Gleichung eine rationale Lösung im Grundkörper F besitzt. Wie man feststellt, ob eine Gleichung eine solche Lösung besitzt haben wir schon in Satz 4.1 gesehen, die Berechnung erhalten wir mit Algorithmus 4.6. Zusammen mit Satz 4.8 und Satz 4.9 liefert dies einen Algorithmus zur Bestimmung der Galoisgruppe.

Algorithmus 4.10. (Zur Bestimmung der Galoisgruppe)
Eingabe: Eine Differenzengleichung ersten Grades $\phi(y) = ay$ mit $a = \frac{a_1(t)}{a_2(t)} \in \mathbb{F}_q(s,t)$. Man setze $b := p-1$ bzw. $b := p^m - 1$, $D := \{d_i \in \mathbb{N} \mid d_i \text{ teilt } b\}$ und $d := d_1$.

1. **if** $d = b$ **then**
   die Galoisgruppe ist die volle $(F^{\phi})^{\times}$
   else
   gehe zu Schritt 2.
   end if

2. Prüfe mit Algorithmus 4.6, ob die Gleichung $\phi(y) = a^d y$ eine rationale Lösung besitzt.
   if es existiert eine rationale Lösung η **then**
   die Gleichung $\phi(y) = ay$ hat eine zyklische Gruppe der Ordnung d als Galoisgruppe
   else
   setze $d := d_{i+1}$ und gehe zu Schritt 1.
   end if

Wir wollen Elemente, deren zugehörige Gleichung eine endliche Galoisgruppe besitzt, noch genauer charakterisieren. Dazu benötigen wir die folgenden Resultate.

Definition 4.11. Es sei $F := \mathrm{Quot}(R)$ ein Frobenius-Körper über dem relativen Frobenius-Ring (R, ϕ) mit definierendem Ideal Q und $\phi|_{R/Q} = \phi_p$. Ein Element $a = \frac{a_1}{a_2} \in F$ mit $a_i \in R$ heißt **gewöhnlich**, falls a in der Menge

$$F^{ord} := \{x \in F \mid \phi(x) = x^p\}$$

liegt. Ferner heißt a **multiplikativ transformierbar**, falls ein Element $f \in F$ existiert, so dass $\frac{\phi(f)}{f} a$ gewöhnlich ist. Das Element f nennen wir **Transformationselement**.

Bemerkung 4.12. *Für einen Frobenius-Körper F wie in Definition 4.11 ist die Menge F^{ord} ein Körper, der alle Einheitswurzeln von F enthält.*

Beweis. Offensichtlich liegen 0 und 1 in F^{ord}. Ferner ist F^{ord} abgeschlossen unter Addition und Multiplikation, da ϕ ein Endomorphismus und $char(F) = p$ ist. Außerdem gilt auch $\phi(x^{-1}) = (x^{-1})^p$ und $\phi(-x) = (-x)^p$ für jedes $x \in F^{ord}$ und damit ist F^{ord} ein Körper. Es sei nun $a \in F$ eine n-te Einheitswurzel, d.h. es gilt $a^n = 1$. Also liegt a in einem endlichen Körper $\mathbb{F}_{q^l}$. Da ϕ aber auf solchen endlichen Körpern als p-te Potenz operiert, gilt $a \in \mathbb{F}_{q^l} \subseteq F^{ord}$. Also enthält F^{ord} alle Einheitswurzeln von F, und damit ist die Aussage bewiesen. □

In der folgenden Bemerkung halten wir einige Eigenschaften multiplikativ transformierbarer Elemente fest.

Bemerkung 4.13. *Es sei $F := \mathrm{Quot}(R)$ ein Frobenius-Körper über einem relativen Frobenius-Ring mit definierendem Ideal Q. Dann gelten:*
(a) Ein Element $a \in F$ ist genau dann gewöhnlich bzw. multiplikativ transformierbar, falls die Galoisgruppe der Differenzengleichung $\phi(y) = ay$ eine endliche Untergruppe von $\mathbb{G}_m(F^\phi)$ ist.
(b) Für zwei gewöhnliche bzw. multiplikativ transformierbare Elemente $a_1, a_2 \in F$ sind sowohl das Produkt $a_1 \cdot a_2$ als auch die Quotient $\frac{a_1}{a_2}$ gewöhnlich bzw. multiplikativ transformierbar.

Beweis. Um Teil (a) zu beweisen, gehen wir zunächst davon aus, dass $a \in F$ multiplikativ transformierbar mit Transformationselement $f \in F$ ist. Wir können also auf die Differenzengleichung $\phi(y) = ay$ die Frobenius-Basiswechselmatrix (f) anwenden. Damit erhalten wir die äquivalente Gleichung $\phi(y) = \frac{\phi(f)}{f} ay$, wobei $\frac{\phi(f)}{f} a$ gewöhnlich ist. Dies ist aber eine Gleichung über dem gewöhnlichen Frobenius-Körper F^{ord} und hat daher eine endliche Gruppe als Galoisgruppe. Wir gehen nun umgekehrt davon aus, dass die Gleichung $\phi(y) = ay$ eine endliche Gruppe als Galoisgruppe besitzt. Um zu beweisen, dass a multiplikativ transformierbar ist, nehmen wir das Gegenteil an und wollen diese Annahme zu einem Widerspruch führen. Also gilt, dass für alle Elemente $f \in F$ das transformierte Element $\frac{\phi(f)}{f} a$ nicht gewöhnlich ist, also $\frac{\phi(f)}{f} a \in F \backslash F^{ord}$ gilt. Insbesondere gilt daher $\frac{\phi(f)}{f} a \neq 1$. Da F^{ord} nach Bemerkung 4.12 alle Einheitswurzeln von F enthält, muss auch für jede natürliche Zahl $k \in \mathbb{N}$ gelten, dass $(\frac{\phi(f)}{f} a)^k \neq 1$ ist. Daher kann für keine zu $\phi(y) = a^k y$ äquivalente Gleichung die triviale Gruppe als Galoisgruppe auftreten. Also muss aber die Galoisgruppe der Gleichung $\phi(y) = ay$ nach Satz 4.8 die volle $\mathbb{G}_\mathrm{m}(F^\phi)$ und damit eine unendliche Gruppe sein. Dies steht im Widerspruch zur Annahme.
Es seien nun zwei multiplikativ transformierbare Elemente $a_1, a_2 \in F$ mit Transformationselementen $f_1, f_2 \in F$ gegeben. Dann sind $a_1 \cdot a_2$ und $\frac{a_1}{a_2}$ multiplikativ transformierbar mit Transformationselementen $f_1 \cdot f_2$ bzw. $\frac{f_1}{f_2}$, denn $\frac{\phi(f_1 f_2)}{f_1 f_2} a_1 a_2 = \frac{\phi(f_1)}{f_1} a_1 \frac{\phi(f_2)}{f_2} a_2$ ist gewöhnlich. Die Aussage erhalten wir für den Quotienten entsprechend, und damit ist auch Teil (b) bewiesen. □

Anmerkung 4.14. Die Bemerkungen 4.12 und 4.13 gelten auch, falls ϕ als p^m-te Potenz operiert und für

$$F_m^{ord} := \{x \in F \mid \phi(x) = x^{p^m}\}.$$

Die Beweise verlaufen analog.

Anmerkung 4.15. Mit den Erkenntnissen aus Bemerkung 4.13 und Satz 4.8 können wir jedes Element a, dessen zugehörige Gleichung $\phi(y) = ay$ eine endliche Galoisgruppe besitzt, folgendermaßen darstellen:

$$a = \underbrace{\omega}_{\in \mathbb{F}_q(s)} \cdot \frac{p_1 p_2 \cdots p_r \cdots \phi^{e_{r+1}}(p_{r+1}) \cdots \phi^{e_x}(p_x)}{\phi^{e_1}(p_1) \cdots \phi^{e_r}(p_r) p_{r+1} \cdots p_x},$$

wobei der hintere Bruch durch einen Frobenius-Basiswechsel mit einem Transformationselement f entfernt werden kann, so dass nur noch das gewöhnliche Element ω übrig bleibt.

Beispiel 4.16. Wir wandeln Beispiel 4.7 leicht ab und betrachten die Differenzengleichung $\phi(y) = ay$ mit

$$a = s\frac{(t-s)^2(t-s^9)(t+s)}{(t^3+s)(t+s^3)}.$$

Für diese Gleichung finden wir keine rationale Lösung, aber die potenzierte Gleichung $\phi(y) = a^2 y$ hat die rationale Lösung

$$\eta = s\frac{(t^3-s)^2(t-s)^2(t-s^3)^2}{(t+s)^2}.$$

Zur Probe berechnen wir

$$\frac{\phi(\eta)}{\eta} = \frac{s^3(t-s)^6(t-s^3)^2(t-s^9)^2(t+s)^2}{s(t+s^3)^2(t^3-s)^2(t-s)^2(t-s^3)^2} = \frac{s^2(t-s)^4(t-s^9)^2(t+s)^2}{(t^3+s)^2(t+s^3)^2} = a^2.$$

Damit hat die Gleichung $\phi(y) = ay$ eine zyklische Gruppe der Ordnung 2, also $\mathbb{F}_3^\times$ als Galoisgruppe.

Beispiel 4.17. Es sei $\phi(y) = ay$ mit

$$a = \frac{(t+s^9)(t+s)^8}{(t^9+s)}$$

eine Differenzengleichung über dem Frobenius-Körper $F = \mathbb{F}_9(s,t)$ mit dem Frobenius-Endomorphismus ϕ. Dabei operiert ϕ auf $\mathbb{F}_9(s)$ als 9-te Potenz und lässt das Ideal (t) invariant, d.h. $F^\phi = \mathbb{F}_9(t)$. Mit Hilfe von Algorithmus 4.6 finden wir eine rationale Lösung $\eta = (t^9+s)(t+s)$, denn es gilt

$$\frac{\phi(\eta)}{\eta} = \frac{(t+s)^9(t+s^9)}{(t^9+s)(t+s)} = \frac{(t+s^9)(t+s)^8}{(t^9+s)} = a,$$

d.h. die Galoisgruppe der Differenzengleichung $\phi(y) = ay$ ist die triviale Gruppe.
Betrachten wir nun die Differenzengleichung $\phi(y) = (s \cdot a)y$, so finden wir mit Algorithmus 4.6 keine rationale Lösung. Aber die Gleichung $\phi(y) = (s \cdot a)^8 y$ hat die rationale Lösung $s \cdot \eta^8$, denn es gilt

$$\phi(s \cdot \eta^8) = s^9 \phi(\eta)^8 = (s \cdot a)^8 (s \cdot \eta^8)$$

und damit hat die Gleichung $\phi(y) = (s \cdot a)y$ eine zyklische Gruppe der Ordnung 8, also $\mathbb{F}_9^\times$ als Galoisgruppe.

4.2 Additive Gleichungen

In diesem Abschnitt betrachten wir $F = \mathbb{F}_q(s,t)$ als rationalen Funktionenkörper bezüglich t und beschränken uns auf den Spezialfall, dass ϕ auf $F^{ord} = \mathbb{F}_q(s)$ als p-te Potenz operiert. Wir betrachten die nicht-lineare Differenzengleichung $L(y) = \phi(y) - y - a$ vom Grad 1 und suchen Lösungen für $L(y) = 0$ bzw. $\phi(y) = y + a$ mit $a \in F$. Nach Satz 1.18 kommen für die Galoisgruppe $G := \mathrm{Gal}(L)$ nur die $\mathbb{G}_{\mathrm{a}}(F^\phi) = F^\phi$ oder endliche Untergruppen von $\mathbb{G}_{\mathrm{a}}(F^\phi)$ der Ordnung p^k für eine natürliche Zahl $k \in \mathbb{N}$ in Frage. Wir benötigen ein Entscheidungskriterium, ob die volle Gruppe $\mathbb{G}_{\mathrm{a}}(F^\phi)$ oder eine echte Untergruppe als Galoisgruppe auftritt. Zunächst wollen wir sehen, wann eine Differenzengleichung eine rationale Lösung, d.h. eine Lösung im Grundkörper F besitzt.

Satz 4.18. *Eine Differenzengleichung $\phi(y) = y + a$ hat genau dann eine rationale Lösung $\eta \in F$ mit $\phi(\eta) - \eta = a$, falls die triviale Gruppe als Galoisgruppe auftritt.*

Beweis. Die Differenzengleichung $\phi(y) = y + a$ hat genau dann die triviale Gruppe als Galoisgruppe, wenn eine Lösung η im Grundkörper F existiert, d.h. $\phi(\eta) = \eta + a$. Schreiben wir diese Identität um, so erhalten wir $\phi(\eta) - \eta = a$. □

Wir wollen nun analog zu Algorithmus 4.10 einen Algorithmus zur Berechnung einer rationalen Lösung von additiven Differenzengleichungen erster Ordnung entwickeln. Die Eingabedaten $a \in \mathbb{F}_q(s,t)$ sind als gekürzter Bruch der From $\frac{a_1(t)}{a_2(t)}$ gegeben. Um daraus eine additive Lösung zu erhalten, berechnen wir zunächst die Partialbruchzerlegung von a und verfahren dann mit den Summanden dieser Zerlegung wie mit den Primpolynomen des gekürzten Bruch im Algorithmus 4.10 für multiplikative Gleichungen.

Algorithmus 4.19. (zur Berechnung einer rationalen Lösung $\eta \in F$)
Eingabe: eine Differenzengleichung ersten Grades $\phi(y) = y + a$ mit $a = \frac{a_1(t)}{a_2(t)} \in \mathbb{F}_q(s,t)$

1. Setze $\eta = 0$.

2. Berechne die Partialbruchzerlegung von a. Dies liefert die Darstellung

$$a = \sum_{i=1}^{r} \frac{c_i}{P_i^{v_i}}$$

   mit Polynomen $c_i \in \mathbb{F}_q(s)[t]$, irreduzibeln Polynomen $P_i \in \mathbb{F}_q(s)[t]$ und $v_i = v_{\mathfrak{p}_{P_i}}$

3. Gehe die Summanden $S_i := \frac{c_i}{P_i^{v_i}}$ durch

   for $j = 1$ to r **do**
   if S_j nicht periodisch **then**
   if $S_j \in \mathrm{Bild}(\phi)$ **then**
   setze $g := \phi^{-1}(S_j), \eta := \eta_1 + g$.
   while $\phi^{-1}(g) \neq g$ **do**
   setze $g := \phi^{-1}(g), \eta := \eta_1 + g$.
   end while
   end if
   else

for $h = 1$ to Periodenlänge von S_j **do**
if $\phi^h(S_j^{v_{1j}}) = S_k$ für $j \neq k \in \{1, \ldots, r\}$ **then**
$\eta := \eta + \phi^h(S_j^{v_{1j}})$
end if
end for
end if
end for

4. **if** $\phi(\eta) - \eta = a$ **then**
Gib die rationale Lösung η aus.
else
Es gibt keine rationale Lösung.
end if

Beispiel 4.20. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Wir wenden Algorithmus 4.19 auf die additive Differenzengleichung $\phi(y) = y + a$ erster Ordnung mit $a = \frac{s-s^p}{t^2+s^pt+st+s^{p+1}}$ an. Durch Partialbruchzerlegung erhalten wir die folgende Darstellung

$$a = \frac{1}{t-s} - \frac{1}{t-s^p} = \frac{1}{t-s} - \phi\left(\frac{1}{t-s}\right).$$

Also erhalten wir $\eta = -\frac{1}{t-s}$ als rationale Lösung der Differenzengleichung und die triviale Gruppe als Galoisgruppe.

Definition 4.21. Ein Element $a \in F$ heißt **additiv transformierbar**, falls ein Element $f \in F$ existiert, so dass $a - (\phi(f) - f)$ gewöhnlich ist. Das Element f nennen wir **Transformationselement**.

Für die folgenden Beweise benötigen wir einige Resultate über rationale Funktionenkörper einer Variablen. Wie oben fassen wir $F = \mathbb{F}_q(s,t)$ als rationalen Funktionenkörper einer Variablen t über $K := \mathbb{F}_q(s)$ auf. Wir bezeichnen mit $\mathbb{P}_{F/K}$ die Menge der Stellen bzw. der Primdivisoren von F über K. Mit $v_\mathfrak{p}$ bezeichnen wir die zur Stelle $\mathfrak{p}$ gehörige Bewertung. Außerdem schreiben wir für ein Element $x \in F$

$$(x)_0 = \sum_{\substack{\mathfrak{p}\in\mathbb{P} \\ v_\mathfrak{p}(x)>0}} v_\mathfrak{p}(x)\mathfrak{p}$$

für den **Nulldivisor** von x und

$$(x)_\infty = \sum_{\substack{\mathfrak{p}\in\mathbb{P} \\ v_\mathfrak{p}(x)<0}} -v_\mathfrak{p}(x)\mathfrak{p}$$

für den **Poldivisor** von x. Ferner bezeichnen wir den Bewertungsring mit

$$\mathcal{O}_\mathfrak{p} = \{x \in F \mid v_\mathfrak{p}(x) \geq 0\} \text{ und das Bewertungsideal mit}$$
$$\mathfrak{p} = \{x \in F \mid v_\mathfrak{p}(x) > 0\}$$

und definieren den Restklassenkörper durch $R_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. Der Grad eines Primdivisors sei definiert durch

$$\deg(\mathfrak{p}) = [R_\mathfrak{p} : K].$$

Damit können wir den Grad eines beliebigen Divisors D durch

$$\deg(D) = \sum_{\mathfrak{p} \in \mathbb{P}_{F/K}} v_\mathfrak{p}(D) \deg(\mathfrak{p})$$

definieren.

Definition 4.22. Ein Element $a \in F$ heißt **additiv minimal**, falls

$$\deg((a)_\infty) \leq \deg\left((a - (\phi(f) - f))_\infty\right)$$

für alle Transformationselemente $f \in F$ ist. Entsprechend heißt a **multiplikativ minimal**, falls

$$\deg((a)_\infty) \leq \deg\left(\left(\frac{\phi(f)}{f} a\right)_\infty\right)$$

für alle Transformationselemente $f \in F$ ist. Wir bezeichnen mit

$$T_a := \deg((a)_\infty)$$

den **Transformationsindex** von a.

Anmerkung 4.23. Es sei $a \in F$ ein beliebiges Körperelement. Dann gelten:
(a) a ist genau dann gewöhnlich, wenn $T_a = 0$ gilt. In diesem Fall ist a sowohl additiv als auch multiplikativ minimal.
(b) Ist a nicht additiv transformierbar, so finden wir dennoch mit Algorithmus 4.19 ein Transformationselement f, so dass $\tilde{a} = a - (\phi(f) - f)$ additiv minimal ist.

Nach [Sti09, Theorem 1.2.2.] sind alle Primdivisoren eines rationalen Funktionenkörpers von der Form $\mathfrak{p}_\infty = \mathfrak{p}_{\frac{1}{t}}$ oder $\mathfrak{p}_{P(t)}$ mit einem irreduziblen Polynom $P(t) \in \mathbb{F}_q(s)[t]$. Wir wollen nun eine Operation des Endomorphismus ϕ auf den Stellen von F definieren. Für die unendliche Stelle definieren wir

$$\phi(\mathfrak{p}_{\frac{1}{t}}) := \mathfrak{p}_{\phi(\frac{1}{t})} = \mathfrak{p}_{\frac{1}{t}}$$

und damit bleibt $\mathfrak{p}_\infty$ invariant unter ϕ. Für ein irreduzibles Polynom $P(t) \in \mathbb{F}_q(s)[t]$, dessen ϕ-Bild $\phi(P(t))$ ebenfalls irreduzibel ist, definieren wir

$$\phi(\mathfrak{p}_P) := \mathfrak{p}_{\phi(P)}.$$

Falls $\phi(P(t))$ reduzibel ist, lässt sich die ϕ-Operation auf der Stelle $\mathfrak{p}_P$ nicht direkt definieren. Dann benötigen wir das folgende Lemma.

Lemma 4.24. *Es sei* $P(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{F}_q(s)[t]$ *ein irreduzibles Polynom. Das* ϕ*-Bild* $\phi(P(t)) = \sum_{i=0}^{n} a_i^p t^i$ *ist genau dann reduzibel, falls ein Polynom* $\tilde{P}(t) \in \mathbb{F}_q(s)[t]$ *mit* $\phi(P(t)) = \tilde{P}(t)^p$ *existiert. Dieses Polynom ist irreduzibel und es gilt* $P(t) = \sum_{j=0}^{m} b_j t^{jp}$ *und* $\tilde{P}(t) = \sum_{j=0}^{m} b_j t^j$*, also* $\tilde{P}(t^p) = P(t)$.

Beweis. Falls $\phi(P(t)) = \tilde{P}(t)^p$ ist, so ist klar, dass $\phi(P(t))$ reduzibel ist. Sei also umgekehrt $\phi(P(t))$ reduzibel in $\mathbb{F}_q(s,t)$. Wir wissen, dass $\mathbb{F}_q(s,t)/\mathbb{F}_q(s^p,t)$ eine inseparable Konstantenerweiterung ist. Außerdem bildet

$$\phi : \mathbb{F}_q(s,t) \longrightarrow \mathbb{F}_q(s^p,t)$$

Primpolynome auf Primpolynome ab. Daher ist $\phi(P(t))$ als Polynom in $\mathbb{F}_q(s^p,t)$ irreduzibel, da $P(t) \in \mathbb{F}_q(s,t)$ nach Voraussetzung irreduzibel ist. Aus der Algebra wissen wir in diesem Fall, dass $\phi(P(t))$ als Polynom in $\mathbb{F}_q(s^p,t)$ genau dann inseparabel ist, falls ein Polynom $\hat{P}(t) \in \mathbb{F}_q(s^p,t)$ mit $\hat{P}(t^p) = \phi(P(t))$ existiert. Dann ist $\phi(P(t))$ ein p-Polynom und es muss ein Polynom $\tilde{P}(t) \in \mathbb{F}_q(s,t)$ mit $\tilde{P}(t)^p = \phi(P(t))$ existieren. Damit gilt dann auch $\tilde{P}(t^p) = P(t)$. Wir nehmen nun an, dass $\tilde{P}(t) = h_1(t) \cdot h_2(t)$ reduzibel ist. Dann ist auch

$$P(t) = \tilde{P}(t^p) = h_1(t^p) \cdot h_2(t^p)$$

reduzibel, was im Widerspruch zur Voraussetzung steht, dass $P(t)$ irreduzibel ist. □

Damit können wir jetzt eine Operation von ϕ auf den Stellen $\mathbb{P}_{F/K}$ definieren.

Definition 4.25. Es sei der Frobeniuskörper $F = \mathbb{F}_q(s,t)$ ein rationaler Funktionenkörper einer Variablen t über $K := \mathbb{F}_q(s)$. Dann operiert ϕ auf den Stellen $\mathbb{P}_{F/K}$ folgendermaßen:

$$\begin{array}{rccc} \phi: & \mathbb{P}_{F/K} & \longrightarrow & \mathbb{P}_{F/K} \\ & \mathfrak{p} & \longmapsto & \phi(\mathfrak{p}) \end{array},$$

wobei wir $\phi(\mathfrak{p})$ wie folgt definieren:

$$\phi(\mathfrak{p}) := \begin{cases} \mathfrak{p} & \text{falls } \mathfrak{p} = \mathfrak{p}_\infty \\ \mathfrak{p}_{\phi(P(t))} & \text{falls } \mathfrak{p} = \mathfrak{p}_{P(t)} \text{ und } \phi(P(t)) \text{ irreduzibel} \\ \mathfrak{p}_{\tilde{P}(t)} & \text{falls } \mathfrak{p} = \mathfrak{p}_{P(t)} \text{ und } \phi(P(t)) = \tilde{P}(t)^p \text{ reduzibel} \end{cases}.$$

Ist $\phi(P((t)))$ irreduzibel, so nennen wir die zugehörige Stelle $\mathfrak{p}$ **separabel**. Ist dagegen $\phi(P((t))) = \tilde{P}(t)^p$ reduzibel, so nennen wir die zugehörige Stelle $\mathfrak{p}$ **rein inseparabel**.
Eine separable Stelle $\mathfrak{p} \in \mathbb{P}_{F/K}$ heißt **ϕ-periodisch**, falls eine natürliche Zahl $k \in \mathbb{N}$ mit $\phi^k(\mathfrak{p}) = \mathfrak{p}$ existiert. Falls sogar $\phi(\mathfrak{p}) = \mathfrak{p}$ gilt, so nennen wir $\mathfrak{p}$ eine **ϕ-invariante Stelle**.

Die beiden folgenden Lemmata sind technische Resultate, die wir für den Beweis des folgenden Satzes 4.28 zur Charakterisierung der Galoisgruppe additiver Differenzengleichungen vom Grad 1 benötigen.

Lemma 4.26. *Für eine Polstelle $\mathfrak{p}$ von $a \in F$ ist $\phi(\mathfrak{p})$ eine Polstelle von $\phi(a)$.*

Beweis. Es sei a in der Darstellung $a = \frac{a_1}{a_2}$ mit teilerfremden Polynomen $a_i \in \mathbb{F}_q(s)[t]$ gegeben. Nach Lemma 4.3 sind dann auch die $\phi(a_i)$ teilerfremde Polynome. Da t in F^ϕ liegt, bleibt der Grad der a_i unter ϕ invariant und die Aussage ist für die unendliche Stelle bewiesen. Für die anderen Stellen gehört $\mathfrak{p}$ zu einem irreduziblen Polynom, das a_2 teilt und $\phi(\mathfrak{p})$ zu einem irreduziblen Polynom, das $\phi(a_2)$ teilt. Da die ϕ-Bilder $\phi(a_i)$ nach Lemma 4.3 teilerfremde Polynome sind, muss $\phi(\mathfrak{p})$ also eine Polstelle von $\phi(a)$ sein und das Lemma ist bewiesen. □

Wegen Anmerkung 4.23 (b) können wir ab sofort ohne Einschränkung davon ausgehen, dass $a \in F$ additiv minimal ist. Andernfalls finden wir mit Algorithmus 4.19 ein Transformationselement f, so dass $\tilde{a} = a - (\phi(f) - f)$ additiv minimal ist und können ohne Einschränkung a durch $\tilde{a}$ ersetzen.

Lemma 4.27. *Es sei $a \in F$ ein additiv minimales Körperelement mit einer nicht ϕ-periodischen Polstelle $\mathfrak{p}$. Dann sind $\phi^k(\mathfrak{p})$ für alle natürlichen Zahlen mit $0 \leq k \leq n$ Polstellen von $\sum_{i=0}^{n} \phi^i(a)$.*

Beweis. Es sei a in der Darstellung $a = \frac{a_1}{a_2}$ als gekürzter Bruch mit teilerfremden Polynomen $a_1, a_2 \in \mathbb{F}_q(s)[t]$ gegeben. Nach Lemma 4.3 sind dann auch die ϕ-Bilder $\phi^k(a) = \frac{\phi^k(a_1)}{\phi^k(a_2)}$ für jede natürliche Zahl $k \in \mathbb{N}$ gekürzte Brüche. Wir wollen zunächst durch Induktion nach n zeigen, dass die Summe $\sum_{i=0}^{n} \phi^i(a)$ als Bruch in der Darstellung

$$\sum_{i=0}^{n} \phi^i(a) = \frac{\sum\limits_{j=0}^{n} \phi^j(a_1) \prod\limits_{\substack{l=0 \\ l \neq j}}^{n} \phi^l(a_2)}{\prod\limits_{k=0}^{n} \phi^k(a_2)}$$

gegeben ist. Es sei also zunächst $n = 1$. Dann ist $a_2\phi(a_2)$ der gemeinsame Nenner von

$$a + \phi(a) = \frac{a_1}{a_2} + \frac{\phi(a_1)}{\phi(a_2)}.$$

Damit erhalten wir für die Summe die Darstellung

$$a + \phi(a) = \frac{a_1\phi(a_2) + \phi(a_1)a_2}{a_2\phi(a_2)}.$$

Dies liefert den Induktionsanfang. Nun machen wir den Induktionsschritt von n nach $n+1$. Wir betrachten die Summe

$$\sum_{i=0}^{n+1} \phi^i(a) = \sum_{i=0}^{n} \phi^i(a) + \phi^{n+1}(a) = \frac{\sum\limits_{j=0}^{n} \phi^j(a_1) \prod\limits_{\substack{l=0 \\ l \neq j}}^{n} \phi^l(a_2)}{\prod\limits_{k=0}^{n} \phi^k(a_2)} + \frac{\phi^{n+1}(a_1)}{\phi^{n+1}(a_2)}.$$

Der gemeinsame Nenner dieser beiden Summanden ist

$$\prod_{k=0}^{n+1} \phi^k(a_2).$$

Dies liefert den Bruch

$$\sum_{i=0}^{n+1} \phi^i(a) = \frac{\sum\limits_{j=0}^{n+1} \phi^j(a_1) \prod\limits_{\substack{l=0 \\ l \neq j}}^{n+1} \phi^l(a_2)}{\prod\limits_{k=0}^{n+1} \phi^k(a_2)}.$$

Da $\mathbb{F}_q(s)[t]$ ein Euklidischer Ring ist, existiert ein größter gemeinsamer Teiler $\mathrm{ggT}\{\phi^k(a_2) \mid 0 \leq k \leq n\}$. Ist dieser trivial, so ist der Bruch

$$\sum_{i=0}^{n} \phi^i(a) = \frac{\sum\limits_{j=0}^{n} \phi^j(a_1) \prod\limits_{\substack{l=0 \\ l\neq j}}^{n} \phi^l(a_2)}{\prod\limits_{k=0}^{n} \phi^k(a_2)}.$$

sogar gekürzt. Nun konmmen wir zur eigentlichen Behauptung. Da $\mathfrak{p}$ eine nicht ϕ-periodische Polstelle von a ist, kann $\mathfrak{p}$ nicht die unendliche Stelle sein. Also gehört die Stelle $\mathfrak{p}$ zu einem irreduziblen Polynom $P \in \mathbb{F}_q(s,t)$, welches ein Teiler von a_2 ist. Aus Lemma 4.26 wissen wir, dass $\phi^k(\mathfrak{p})$ eine Polstelle von $\phi^k(a)$ für jede natürliche Zahl $1 \leq k \in \mathbb{N}$ ist. Da F/K Klassenzahl 1 hat, muss auch $\phi^k(P)$ ein Teiler von $\phi^k(a_2)$ für jede natürliche Zahl $1 \leq k \in \mathbb{N}$ sein. Da a additiv minimal ist, können sich in der Summe keine Polstellen wegkürzen. Denn dann könnte man ein nicht-triviales Transformationselement f finden und damit diese Polstelle aus a durch einen Frobenius-Basiswechsel $a - (\phi(f) - f)$ kürzen, was im Widerspruch zur additiven Minimalität von a stehen würde. Daher ist $\phi^k(P)$ für jede natürliche Zahl $1 \leq k \leq n$ ein Teiler von

$$\prod_{k=0}^{n} \phi^k(a_2),$$

also ist $\phi^k(\mathfrak{p})$ für jede natürliche Zahl $1 \leq k \leq n$ eine Polstelle der Summe $\sum\limits_{i=0}^{n} \phi^i(a)$, falls $\mathrm{ggT}\{\phi^k(a_2) \mid 0 \leq k \leq n\} = 1$ gilt. Andernfalls existieren gemeinsame Teiler der ϕ-Bilder von a_2. In der Darstellung der Summe als Bruch kürzen sich aber die mehrfachen Faktoren wieder heraus. Auch in diesem Fall ist $\phi^k(P)$ für jede natürliche Zahl $1 \leq k \leq n$ ein Teiler des Nenners von $\sum\limits_{i=0}^{n} \phi^i(a)$ und damit ist $\phi^k(\mathfrak{p})$ für jede natürliche Zahl $1 \leq k \leq n$ eine Polstelle der Summe. Und damit ist das Lemma bewiesen. □

Damit haben wir alle theoretischen Resultate, die für die Bestimmung der Galoisgruppe einer additiven Differenzengleichung erster Ordnung notwendig sind, zusammengetragen.

Satz 4.28. *Es sei $\phi(y) = y + a$ eine additive Differenzengleichung erster Ordnung mit $a \in F$ additiv minimal und Galoisgruppe G. Dann gelten:*
(a) Die Galoisgruppe G ist die triviale Gruppe, falls $a = 0$ ist.
(b) Die Galoisgruppe G ist eine endliche Gruppe der Ordnung p, falls a in der Darstellung $a = \tilde{a} \cdot t^k$ mit $\tilde{a} \in F^{ord} = \mathbb{F}_q(s)$ und $0 \leq k \in \mathbb{N}$ gegeben ist.
(c) Die Galoisgruppe G ist eine endliche Gruppe der Ordnung p^n mit $n \leq \deg(a) + 1$, falls $a \in \mathbb{F}_q(s)[t]$ liegt.
(d) Die Galoisgruppe G ist eine endliche Gruppe der Ordnung p^n mit $n \leq \deg(a_1) + \deg(a_2)(l-1) + 1$, falls $a = \frac{a_1(t)}{a_2(t)} \in \mathbb{F}_q(s,t)$ nur ϕ-periodische Polstellen besitzt und l die Periodenlänge von $a_2(t)$ bezeichnet.
(e) Die Galoisgruppe G ist die volle $\mathbb{G}_{\mathrm{a}}(F^{\phi}) = \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p(t))$, falls a mindestens eine nicht ϕ-periodische Polstelle $\mathfrak{q}$ besitzt.

Beweis. Die erste Aussage (a) folgt direkt aus Satz 4.18. Um (b) zu beweisen, wollen wir zunächst die triviale Gruppe als Galoisgruppe ausschließen. Wenn die Gleichung $\phi(y) = y + a$ mit $a = \tilde{a} \cdot t^k$ triviale Galoisgruppe hätte, so würde nach Satz 4.18 eine rationale Lösung $\eta \in F$ mit $\phi(\eta) - \eta = a$ existieren. Dies wäre aber ein Widerspruch zur additiven Minimalität von a, denn $a - (\phi(\eta) - \eta) = a - a = 0$. Also kann die triviale Gruppe nicht auftreten. Als nächstes betrachten wir die Differenzengleichung $\phi(y) = y + \tilde{a}$ erster Ordnung über dem gewöhnlichen Frobenius-Körper F^{ord}. Diese besitzt eine algebraische Lösung $\tilde{\eta}$ mit Minimalpolynom

$$g_{\tilde{\eta}} = X^p - X - \tilde{a}.$$

Da aber t^k für jede natürliche Zahl $0 \leq k \in \mathbb{N}$ invariant unter ϕ bleibt, ist $\frac{\tilde{\eta}}{t^k}$ eine Lösung von $\phi(y) = y + \tilde{a}$. Daher finden wir eine algebraische Lösung η der Gleichung $\phi(y) = y + a = y + \tilde{a}t^k$ mit Minimalpolynom

$$g_\eta = X^p - (t^k)^{p-1}X - (t^k)^p a.$$

Damit ist die Galoisgruppe von $\phi(y) = y + a$ eine endliche Gruppe der Ordnung p und Aussage (b) ist bewiesen.
Ist $a = \sum_{i=0}^{r} a_i t^i$ ein Polynom in $\mathbb{F}_q(s)[t]$, so erhalten wir durch Anwendung von (b) für jeden Term $a_i t^i$ mit $a_i \neq 0$ eine algebraische Lösung η_i mit Minimalpolynom

$$g_{\eta_i} = X^p - (t^i)^{p-1}X - (t^i)^p a_i.$$

Für $a_i = 0$ setzen wir $\eta_i = 0$. Durch $\eta := \sum_{i=0}^{r} \eta_i$ erhalten wir eine algebraische Lösung der Gleichung $\phi(y) = y + a$. Durch Resultantenbildung der Minimalpolynome g_{η_i} erhalten wir ein Polynom vom Grad p^m mit $m \leq \deg(a) + 1$. Das Minimalpolynom g_η vom Grad n ist ein Teiler dieses Polynoms und die Galoisgruppe ist eine Gruppe der Ordnung p^n mit $n \leq \deg(a) + 1$, was Aussage (c) beweist.
Um (d) zu zeigen sei a nun in der Darstellung $a = \frac{a_1}{a_2}$ mit teilerfremden Polynomen $a_i \in \mathbb{F}_q(s)[t]$ gegeben. Da a nur ϕ-periodische Polstellen besitzt, ist a_2 periodisch der Länge l und liegt nach Bemerkung 4.5 sogar in $\mathbb{F}_q[t]$. Mit dem ϕ-Invarianten Element

$$d := \prod_{i=0}^{l-1} \phi^i(a_2)$$

erhalten wir eine zu $\phi(y) = y + a$ äquivalente Gleichung, nämlich

$$\phi(yd) = (y + ad) = yd + ad = yd + \underbrace{a_1 \prod_{i=1}^{l-1} \phi^i(a_2)}_{:= \tilde{a}}$$

mit $\tilde{a} \in \mathbb{F}_q(s)[t]$. Die Galoisgruppe dieser Gleichung ist nach (c) eine endliche Gruppe der Ordnung p^n mit $n \leq \deg(a_1) + \deg(a_2)(l-1) + 1$. Damit ist auch die Galoisgruppe von $\phi(y) = y + a$ eine endliche Gruppe der Ordnung p^n.
Um schließlich (e) zu beweisen, sei nun η eine Lösung der Gleichung $\phi(y) = y + a$. Die

Galoisgruppe ist genau dann die volle $\mathbb{G}_{\mathrm{a}}(F^{\phi})$, falls η transzendent ist. Wir wollen also annehmen, dass η algebraisch ist und dies zu einem Widerspruch führen. Da η algebraisch über F ist, müssen auch die ϕ-Bilder $\phi^n(\eta)$ für $n \in \mathbb{N}$ algebraisch über F sein. Es gilt

$$\begin{aligned}\phi(\eta) &= \eta + a,\\ \phi^2(\eta) &= \phi(\eta + a) = \eta + a + \phi(a),\\ &\dots\\ \phi^n(\eta) &= \eta + \underbrace{\sum_{i=0}^{n-1} \phi^i(a)}_{:=\,\mu_n}.\end{aligned}$$

Als nächstes betrachten wir den Poldivisor von η

$$(\eta)_\infty = \sum_{\substack{\mathfrak{p}\in\mathbb{P}\\ v_{\mathfrak{p}}<0}} -v_{\mathfrak{p}}(\eta)\mathfrak{p}.$$

Da wir η als algebraisch vorausgesetzt haben, hat η nur endlich viele Polstellen. Außerdem hat auch jedes $\phi^n(\eta)$ für $n \in \mathbb{N}$ nur endlich viele Polstellen. Es sei

$$\mathfrak{P}_0 := \{\mathfrak{p} \in \mathbb{P}_{F/K} \mid v_{\mathfrak{p}}(\eta) < 0\}$$

die Menge aller Polstellen von η. Da für jedes $n \in \mathbb{N}$ auch $\phi^n(\eta)$ algebraisch ist, sind auch die Mengen

$$\mathfrak{P}_n := \{\mathfrak{p} \in \mathbb{P}_{F/K} \mid v_{\mathfrak{p}}(\phi^n(\eta)) < 0\}$$

aller Polstellen von $\phi^n(\eta)$ für alle natürlichen Zahlen $n \in \mathbb{N}$ endlich. Da ϕ ein injektiver Endomorphismus ist, werden beim Übergang von η zu $\phi^n(\eta)$ Polstellen auf Polstellen abgebildet. Da außer diesen auch keine neuen Polstellen auftreten können, gilt sogar

$$s := \#\mathfrak{P}_0 = \#\mathfrak{P}_n$$

für alle $n \in \mathbb{N}$. Jetzt wollen wir auch die Poldivisoren der ϕ-Bilder von η betrachten. Dazu untersuchen wir zunächst die Bewertungen

$$\begin{aligned}v_{\mathfrak{p}}(\phi^n(\eta)) &= v_{\mathfrak{p}}(\eta + \sum_{i=0}^{n-1} \phi^i(a))\\ &\geq \min\{v_{\mathfrak{p}}(\eta), v_{\mathfrak{p}}\left(\sum_{i=0}^{n-1} \phi^i(a)\right)\}\\ &= \min\{v_{\mathfrak{p}}(\eta), v_{\mathfrak{p}}(\mu_n)\}.\end{aligned}$$

Mit Lemma 4.27 ergibt sich, dass μ_n mindestens n verschiedene Polstellen, nämlich $\mathfrak{q}$, $\phi(\mathfrak{q})$, … , $\phi^{n-1}(\mathfrak{q})$ besitzt. Wir betrachten nun das algebraische Element $\phi^{2s+1}(\eta)$ mit s Polstellen. Nach obiger Rechnung gilt aber auch

$$v_{\mathfrak{p}}(\phi^{2s+1}(\eta)) \geq \min\{v_{\mathfrak{p}}(\eta), v_{\mathfrak{p}}(\mu_{2s+1})\},$$

wobei sogar Gleichheit gilt, falls $v_{\mathfrak{p}}(\eta) \neq v_{\mathfrak{p}}(\mu_{2s+1})$ ist. Das Element η besitzt genau s Polstellen, μ_{2s+1} nach Lemma 4.27 mindestens $2s+1$. Also hat $\phi^{2s+1}(\eta)$ einerseits nach Voraussetzung s Polstellen, aber andererseits nach obiger Rechnung mindestens $s+1$ Polstellen. Damit haben wir die Annahme, dass η algebraisch ist, zu einem Widerspruch geführt. Also muss η transzendent sein. □

Zum Abschluss des Kapitels führen wir noch einige Beispiele zur Berechnung der Galoisgruppe additiver Differenzengleichungen erster Ordnung vor. Dies erfolgt mit Hilfe von Algorithmus 4.19 und der Charakterisierung aus Satz 4.28.

Beispiel 4.29. Die Gleichung in Beispiel 4.20 hat die triviale Gruppe als Galoisgruppe, denn $a - (\phi(\eta) - \eta) = 0$.

Beispiel 4.30. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Wir wenden Algorithmus 4.19 auf die additive Differenzengleichung $\phi(y) = y + a$ erster Ordnung mit $a = \frac{st^3+s^{p+1}t^2+s^{p-1}t^2+s^{p+2}t+s^p-s}{t^2+s^pt+st+s^{p+1}}$ an. Durch Partialbruchzerlegung erhalten wir die folgende Darstellung

$$a = \frac{1}{t-s} - \frac{1}{t-s^p} + st = \frac{1}{t-s} - \phi\left(\frac{1}{t-s}\right) + st.$$

Also erhalten wir mit $f = -\frac{1}{t-s}$ als Transformationselement das additiv minimale Element $\tilde{a} = a - (\phi(f) - f) = st$ und damit als Galoisgruppe nach Satz 4.28 (b) eine endliche Gruppe der Ordnung p.

Beispiel 4.31. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Wir wenden Algorithmus 4.19 auf die additive Differenzengleichung $\phi(y) = y+a$ erster Ordnung mit $a = s - t$ an. Mit Algorithmus 4.19 finden wir kein Transformationselement, also ist a bereits additiv minimal. Wir berechnen das Minimalpolynom von η mit $\phi(\eta) = \eta + s - t$. Dazu schreiben wir η als Summe $\eta = \eta_1 + \eta_2$ mit $\phi(\eta_1) = \eta_1 + s$ und $\phi(\eta_1) = \eta_1 - t$. Die zugehörigen Minimalpolynome sind

$$g_{\eta_1}(X) = X^p - X - s \quad \text{bzw.}$$
$$g_{\eta_2}(X) = X^p - t^{p-1}X + t^p.$$

Dann erhalten wir das Minimalpolynom g_η als Teiler der Resultante

$$\mathrm{Res}_T(g_{\eta_1}(X-T), g_{\eta_2}(T)).$$

Dies ist ein Polynom vom Grad p^2. Daher erhalten wir als Galoisgruppe nach Satz 4.28 (c) eine endliche Gruppe der Ordnung höchstens p^2. Für den Spezialfall $p = 3$ und $q = p^2 = 9$ ergibt sich für die Resultante

$$\begin{aligned}\mathrm{Res}_T(g_{\eta_1}(T), g_{\eta_2}(X-T)) = 2X^9 &+ (t^6+t^4+t^2+1)X^3 \\ &+ (2t^6+2t^4+2t^2)X \\ &+ 2t^9 + t^7 + 2st^6 + t^5 + 2st^4 + t^3 + 2st^2 + s^3.\end{aligned}$$

Dies ist ein irreduzibles Polynom. Damit ist $g_\eta = \mathrm{Res}_T(g_{\eta_1}(T), g_{\eta_2}(X-T))$ das Minimalpolynom von η und die Galoisgruppe ist eine endliche Gruppe der Ordnung $3^2 = 9$.

Beispiel 4.32. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Wir wenden Algorithmus 4.19 auf die additive Differenzengleichung $\phi(y) = y + a$ erster Ordnung mit $a = \frac{1}{s-t}$ an. Mit Algorithmus 4.19 finden wir kein Transformationselement, also ist a bereits additiv minimal. Da die Fälle (a) bis (d) von Satz 4.28 nicht auftreten und a eine nicht ϕ-periodische Polstelle $\mathfrak{p} = \mathfrak{p}_{s-t}$ besitzt, ist die Galoisgruppe der Gleichung $\phi(y) = y + a$ die volle additive Gruppe $\mathbb{G}_\mathrm{a}(F^\phi)$.

Kapitel 5

Berechnung der Galoisgruppe für Gleichungen vom Grad 2

Wir betrachten in diesem Kapitel Differenzengleichungen zweiten Grades der Form $L(y) = \phi^2(y) + a\phi(y) + by = 0$. Diesen liegt wieder der relative Frobenius-Körper

$$F = \mathrm{Quot}(R) = \mathrm{Quot}(\mathbb{F}_q[s,t]) = \mathbb{F}_q(s,t)$$

mit Semi-Frobenius-Endomorphismus

$$\phi : R \longrightarrow R$$

zugrunde. Dieser Endomorphismus wird definiert durch $\phi|_{\mathbb{F}_q} = \phi_{p^m}$ und $\phi(t) = t$, $\phi(s) = s^{p^m}$ mit $1 \leq m \leq d$. Wir beschränken uns auf den Spezialfall $m = 1$, d.h. $\phi = \phi_p$ und $F^\phi = \mathbb{F}_p(t)$. Die Gleichung $L(y) = 0$ bzw. deren assoziierte Matrixgleichung

$$\phi(\boldsymbol{y}) = A_L \cdot \boldsymbol{y} \text{ mit } \boldsymbol{y} = (y, \phi(y))^{tr} \text{ und } A_L = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$$

induziert einen Frobenius-Modul M_L mit einem PV-Körper E. Ferner sei $G := \mathrm{Gal}(L)$ die Galoisgruppe und $V := \mathrm{Sol}_E^\phi(M_L)$ der Lösungsraum von L.
Um die möglichen Gruppen, die als Galoisgruppe einer multiplikativen Differenzengleichung erster Ordnung $\phi(y) = ay$ auftreten können, zu unterscheiden, haben wir die potenzierten Gleichungen $\phi(y) = a^d y$ für $d = 1, 2, \ldots$ bis zu einer gewissen Schranke b berechnet und daraus Rückschlüsse auf die Gruppe gezogen. Diese potenzierten Gleichungen sind aber nichts anderes als die d-te symmetrische Potenz der ursprünglichen Gleichung, denn für zwei Lösungen η_1, η_2 dieser Gleichung gilt

$$\phi(\eta_1\eta_2) = \phi(\eta_1)\phi(\eta_2) = (a\eta_1)(a\eta_2) = a^2(\eta_1\eta_2).$$

Wir haben also einen Zusammenhang zwischen Lösungen gewisser symmetrischer Potenzen und der Galoisgruppe einer Differenzengleichung erster Ordnung hergestellt. Ein solches Verfahren wollen wir auch für Gleichungen höherer Ordnungen anwenden. Dabei werden aber die Grade der symmetrischen Potenzen wachsen, d.h. es wird nicht nur darum gehen rationale Lösungen der symmetrischen Potenzen zu suchen, sondern diese zu faktorisieren. Beginnend mit der Faktorisierung der ursprünglichen Gleichung $L(y) = \phi^2(y) + a\phi(y) + by =$

0 (erste symmetrischen Potenz) lässt sich bestimmen, ob die Galoisgruppe in der Borel-Gruppe $\mathbb{B}_2(F^\phi)$ enthalten ist (Abschnitte 5.1 über reduzible Gruppen und 5.2 über zerfallende Tori). Bei der genauen Bestimmung der Gruppe werden dann auch die Ergebnisse aus Kapitel 4 über Differenzengleichungen erster Ordnung einfließen und auf die Faktoren bzw. den additiven Teil der assoziierten Matrix-Gleichung angewandt. Ist die ursprüngliche Gleichung irreduzibel, werden die höheren symmetrischen Potenzen bis zur Schranke aus Satz 1.36 betrachtet, um Rückschlüsse auf die Galoisgruppe zu ziehen (Abschnitte 5.3 über Diedergruppen, 5.4 über nicht-zerfallende Tori und 5.5 über irreduzible primitive Gruppen). Sind alle diese Operatoren irreduzibel, müssen nur noch durch die multiplikative Differenzengleichung $\phi(y) = by$ erster Ordnung die Zwischengruppen von $\mathrm{GL}_2(F^\phi)$ und $\mathrm{SL}_2(F^\phi)$ unterschieden werden (vgl. Abschnitt 5.6).

5.1 Reduzible Gruppen

Wir haben mit Satz 1.23 gesehen, dass die Galoisgruppe der Gleichung L genau dann reduzibel ist, wenn auch die Gleichung im Sinne von Definition 2.12 reduzibel ist. Dies liefert ein erstes Entscheidungskriterium für die Berechnung der Galoisgruppe einer Differenzengleichung zweiter Ordnung.

Satz 5.1. *Es sei $L(y) = 0$ eine Differenzengleichung zweiter Ordnung. Dann gelten:*
(a) Es existiert genau dann eine Lösung $0 \neq u \in E$ mit $\frac{\phi(u)}{u} := a_1 \in F$, so dass $\phi - a_1$ den Operator P_L von rechts teilt (d.h. er besitzt die Darstellung $P_L = (\phi - a_2)(\phi - a_1)$), wenn die Galoisgruppe G eine Untergruppe der Borelgruppe

$$\mathbb{B}_2(F^\phi) = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in (F^\phi)^\times, \gamma \in F^\phi \}$$

ist.
(b) Es existieren genau dann zwei linear unabhängige Lösungen $0 \neq u_1, u_2 \in E$ mit $\frac{\phi(u_i)}{u_i} := a_i \in F$, so dass $P_L = (\phi - a_2)(\phi - a_1)$ reduzibel ist, falls die Galoisgruppe G eine Untergruppe der Gruppe der Diagonalmatrizen

$$\mathbb{T}_2(F^\phi) = \{ \begin{pmatrix} \delta_1 & 0 \\ 0 & \delta_2 \end{pmatrix} \mid \delta_i \in (F^\phi)^\times \}$$

ist.

Beweis. Dieser Satz ist ein Spezialfall von Satz 1.23. Dieser besagt, dass eine Differenzengleichung genau dann reduzibel ist, wenn der Lösungsraum $V = \mathrm{Sol}_E^\Phi(M_L)$ einen G-invarianten Untervektorraum W besitzt. In Teil (a) korrespondiert die eindeutige Lösung u mit $\frac{\phi(u)}{u} := \tilde{a} \in F$ zu einem Rechtsfaktor vom Grad 1 und somit zu einem G-invarianten Unterraum W der Dimension 1. Daher muss die Galoisgruppe in der Borelgruppe $\mathbb{B}_2(F^\phi)$ enthalten sein. In Teil (b) korrespondiert jede der beiden linear unabhängigen Lösungen u_1, u_2 zu je einem Rechtsfaktor, d.h. die Gleichung ist komplett reduzibel. Dies impliziert, dass die Faktoren kommutieren und zwei G-invariante Untervektorräume W_1, W_2 existieren. Daher muss die Galoisgruppe in der Gruppe der Diagonalmatrizen $\mathbb{T}_2(F^\phi)$ enthalten sein. □

Mit Hilfe von Algorithmus 4.10 für Differenzengleichungen erster Ordnung angewendet auf $\tilde{a}$ bzw. a_i aus Satz 5.1 kann man weitere Einschränkungen machen und so die Galoisgruppe endgültig berechnen.

Wir betrachten zunächst den Fall aus Satz 5.1 (a). Dann ist der Operator $P_L = (\phi - a_2)(\phi - a_1)$ reduzibel, aber nicht komplett reduzibel, d.h. die Galoisgruppe G von L ist in der Gruppe der oberen Dreiecksmatrizen enthalten. Dies folgt einerseits unmittelbar aus Satz 1.23, andererseits können wir durch einen geschickten Frobenius-Basiswechsel die Darstellungsmatrix von Φ auf obere Dreiecksgestalt transformieren. Dies gelingt mit der folgenden Basiswechselmatrix:

$$T_1 = \begin{pmatrix} 1 - a_1 & 1 \\ -a_1 & 1 \end{pmatrix} \qquad T_1^{-1} = \begin{pmatrix} 1 & -1 \\ a_1 & 1 - a_1 \end{pmatrix}.$$

Die Darstellungsmatrix A_1 bezüglich der neuen Basis hat dann die folgende Gestalt:

$$\begin{aligned} A_1 = \phi(T_1) A_L T_1^{-1} &= \begin{pmatrix} 1 - \phi(a_1) & 1 \\ -\phi(a_1) & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ a_1 & 1 - a_1 \end{pmatrix} \\ &= \begin{pmatrix} a_1 - \phi(a_1)a_1 - b - aa_1 & 1 - a_1 - \phi(a_1) + \phi(a_1)a_1 + b - a + aa_1 \\ -\phi(a_1)a_1 - b - aa_1 & -\phi(a_1) + \phi(a_1)a_1 + b - a + aa_1 \end{pmatrix}. \end{aligned}$$

Da $\phi - a_1$ ein Rechtsfaktor von P_L ist, gelten:

$$b = a_1 a_2, \qquad a = -\phi(a_1) - a_2.$$

Aus diesen beiden Gleichungen erhält man außerdem

$$\phi(a_1) = \frac{-aa_1 - b}{a_1}.$$

Setzt man diese Gleichungen in die obige Matrix ein, ergibt sich

$$A_1 = \begin{pmatrix} a_1 & 1 + a_2 - a_1 \\ 0 & a_2 \end{pmatrix}.$$

Man sieht nun der Darstellungsmatrix A_1 direkt an, dass die Galoisgruppe von L in der Gruppe der oberen Dreiecksmatrizen enthalten sein muss. Die Gestalt der Diagonalelemente der Galoisgruppe hängt davon ab, welche Galoisgruppe die Faktoren von P_L haben. Wenn z.B. für die Differenzengleichung erster Ordnung $\phi(y) = a_1 y$ die Gruppe $H \leq \mathbb{G}_{\mathrm{m}}(F^\phi)$ als Galoisgruppe auftritt, so kann jedes Element dieser Gruppe im entsprechenden Matrixkoeffizienten stehen. So lassen sich die Diagonalelemente der Galoisgruppe mit Hilfe von Algorithmus 4.10 berechnen. Da aber die $\mathbb{G}_a(F^\phi)$ im Falle $\mathrm{char}(F) = p > 0$ nicht-triviale abgeschlossene Untergruppen besitzt, müssen wir bezüglich des Elements oberhalb der Diagonalen weitere Kriterien finden, um die Galoisgruppe zu bestimmen. Wir können jedoch die Möglichkeiten einschränken, indem wir die Diagonalelemente untersuchen.
Ist beispielsweise ein Diagonalelement beliebig aus der kompletten $\mathbb{G}_m(F^\phi)$ auswählbar, so

muss über der Diagonale die komplette $\mathbb{G}_a(F^\phi)$ stehen. Dies folgt daraus, dass die Matrizen

$$M_1 = \begin{pmatrix} \alpha & \gamma \\ 0 & 1 \end{pmatrix} \text{ mit } \alpha \in \mathbb{G}_m(F^\phi), \gamma \in H \lneq \mathbb{G}_a(F^\phi) \text{ beliebig und}$$
$$M_2 = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \text{ mit } \beta \in H \lneq \mathbb{G}_a(F^\phi) \text{ beliebig}$$

und damit auch die Konjugierte $M_1 \cdot M_2 \cdot M_1^{-1}$ in der Galoisgruppe G liegen. Diese hat die Gestalt

$$\begin{aligned} M_1 \cdot M_2 \cdot M_1^{-1} &= \begin{pmatrix} \alpha & \gamma \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{-1} & -\alpha^{-1}\gamma \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \in G \end{aligned}$$

und damit kann über der Diagonale jedes beliebige Element aus $\mathbb{G}_a(F^\phi)$ stehen. Das selbe Ergebnis erhalten wir durch analoge Überlegungen mit der Konjugationsmatrix

$$\tilde{M_1} = \begin{pmatrix} 1 & \gamma \\ 0 & \alpha \end{pmatrix} \text{ mit } \alpha \in \mathbb{G}_m(F^\phi) \text{ beliebig.}$$

Liegen dagegen beide Diagonalelemente in einer endlichen Untergruppe von $\mathbb{G}_m(F^\phi)$, d.h. beide Faktoren von P_L haben eine endliche Gruppe als Galoisgruppe, müssen wir mehrere Fälle unterscheiden. Dazu benötigen wir die Ergebnisse aus Bemerkung 4.13. Wir betrachten nun wieder die transformierte Darstellungsmatrix A_1. Durch einen erneuten Basiswechsel mit der Transformationsmatrix

$$T_2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \qquad T_2^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

erhalten wir dann

$$A_2 = \phi(T_2) A_1 T_2^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 + a_1 - a_1 \\ 0 & a_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 0 & a_2 \end{pmatrix}.$$

Sind nun sowohl a_1 als auch a_2 gewöhnlich, so ist die Galoisgruppe G von L endlich. Die Galoisgruppe G ist damit isomorph zu

$$\mathbb{B}_2(F^\phi)_{k,l,e,p} = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1, \gamma \in \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p) \},$$

denn die Gruppe $\mathbb{G}_{\mathrm{a}}(\mathbb{F}_p)$ hat nur die triviale Gruppe als Untergruppe und diese haben wir bereits ausgeschlossen durch die Annahme, dass G reduzibel aber nicht komplett reduzibel ist.
Sind dagegen die Elemente a_1 und a_2 multiplikativ transformierbar mit Transformationselementen f_1, f_2, so können wir auf A_2 die folgende Basiswechselmatrix anwenden

$$T_3 = \begin{pmatrix} f_1 & 0 \\ 0 & f_2 \end{pmatrix} \qquad T_3^{-1} = \begin{pmatrix} f_1^{-1} & 0 \\ 0 & f_2^{-1} \end{pmatrix}.$$

Dies liefert

$$A_3 = \phi(T_3)A_2T_3^{-1} = \begin{pmatrix} \phi(f_1) & \\ 0 & \phi(f_2) \end{pmatrix} \cdot \begin{pmatrix} a_1 & 1 \\ 0 & a_2 \end{pmatrix} \cdot \begin{pmatrix} f_1^{-1} & \\ 0 & f_2^{-1} \end{pmatrix}$$
$$= \begin{pmatrix} \tilde{a}_1 & \phi(f_1)f_2^{-1} \\ 0 & \tilde{a}_2 \end{pmatrix},$$

wobei $\tilde{\alpha}_1$ und $\tilde{\alpha}_2$ gewöhnlich sind. Dagegen ist $\phi(f_1)f_2^{-1}$ i.A. nicht gewöhnlich. Als Galoisgruppe tritt also eine Gruppe von der Form

$$\mathbb{B}_2(F^\phi)_{k,l,e,H} = \{\begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H \leq \mathbb{G}_\mathrm{a}(F^\phi)\}$$

auf. Nun muss man noch unterscheiden, welche Gruppe H für die Elemente über der Diagonale in Frage kommt. Es können die volle $\mathbb{G}_\mathrm{a}(\mathbb{F}_p(t))$, endliche Gruppen mit Primzahlpotenzordnung der Form $\mathbb{F}_p g_1 \oplus \mathbb{F}_p g_2 \oplus \ldots \oplus \mathbb{F}_p g_m$ mit $g_i \in F^\phi$ sowie, die $\mathbb{G}_\mathrm{a}(\mathbb{F}_p)$ auftreten. Um herauszufinden welche Gruppe die gesuchte Gruppe ist, betrachten wir eine Basis des Lösungsraums $V = \mathrm{Sol}_E^\Phi(M_L)$. Da sowohl $\tilde{a}_1$ also auch $\tilde{a}_2$ gewöhnlich sind, finden wir Lösungen η_1 und η_2 in einem algebraischen Abschluss von $F^{ord} = \mathbb{F}_q(s)$ mit $\phi(\eta_1) = \tilde{a}_1\eta_1$ und $\phi(\eta_2) = \tilde{a}_2\eta_2$. Die beiden entsprechenden Vektoren $\begin{pmatrix} \eta_1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \eta_2 \end{pmatrix}$ spannen allerdings noch nicht den Lösungsraum auf, denn für einen Lösungsvektor $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ gilt mit $c := \phi(f_1)f_2^{-1}$

$$\phi(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}) = \begin{pmatrix} \tilde{a}_1 & c \\ 0 & \tilde{a}_2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \tilde{a}_1 y_1 + cy_2 \\ \tilde{a}_2 y_2 \end{pmatrix}.$$

Also können wir als ersten Lösungsvektor einfach $\begin{pmatrix} \eta_1 \\ 0 \end{pmatrix}$ wählen. Für den zweiten setzen wir $y_2 = \eta_2$ und für y_1 wählen wir die formale Lösung

$$\eta := -\eta_1 \left(\sum_{i=0}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right),$$

denn es gilt

$$\phi(\eta) = \phi(-\eta_1 \left(\sum_{i=0}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right)) = -\phi(\eta_1) \cdot \phi \left(\sum_{i=0}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right)$$
$$= -\tilde{a}_1\eta_1 \left(\sum_{i=1}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right).$$

Andererseits gilt auch

$$\tilde{a}_1\eta = -\tilde{a}_1\eta_1 \left(\sum_{i=0}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right)) = -\tilde{a}_1\eta_1 \cdot \frac{c\eta_2}{\tilde{a}_1\eta_1} - \tilde{a}_1\eta_1 \left(\sum_{i=1}^{\infty} \phi^i \left(\frac{c\eta_2}{\tilde{a}_1\eta_1} \right) \right)$$
$$= -c\eta_2 + \phi(\eta)$$

und damit $\phi(\eta) = \tilde{a}_1\eta + c\eta_2$. Also wird der Lösungsraum V über F^ϕ von $\begin{pmatrix} \eta_1 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} \eta \\ \eta_2 \end{pmatrix}$ aufgespannt, d.h. es gilt

$$V = \mathrm{Sol}_E^\Phi(M_L) = < \begin{pmatrix} \eta_1 \\ 0 \end{pmatrix}, \begin{pmatrix} \eta \\ \eta_2 \end{pmatrix} >_{F^\phi} .$$

Da η_2 sowieso algebraisch über $\mathbb{F}_q(s)$ ist, hängt die Antwort auf die Frage, ob die Galoisgruppe endlich ist, nur noch von der formalen Lösung η ab. Ist η algebraisch über F, so ist G endlich. Andernfalls liegt eine unendliche Gruppe vor und es gilt

$$G = \mathbb{B}_2(F^\phi)_{k,l,e,H} = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H = \mathbb{G}_\mathrm{a}(F^\phi) \}.$$

Wir wollen nun genauer untersuchen, wann die obige formale Lösung η algebraisch (bzw. transzendent) und damit die Galoisgruppe endlich (bzw. unendlich) ist. Um die folgenden Rechnungen etwas zu vereinfachen ersetzen wir η ohne Einschränkung durch $\tilde{\eta} := \frac{\eta}{\eta_1}$. Damit gilt $\phi(\tilde{\eta}) = \tilde{\eta} + \frac{\eta_2}{\eta_1}c$ wegen $\phi(\eta) = \tilde{a}_1\eta + \eta_2 c$

Satz 5.2. *Es sei $L(y) = 0$ eine reduzible Differenzengleichung zweiter Ordnung, d.h. es gilt $P_L = (\phi - a_2)(\phi - a_1)$. Ferner seien die Elemente a_1 und a_2 multiplikativ transformierbar mit Transformationselementen f_1 bzw. f_2, d.h. es gilt $\frac{\phi(f_1)}{f_1}a_1 = \tilde{a}_1 \in \mathbb{F}_q$ bzw. $\frac{\phi(f_2)}{f_2}a_2 = \tilde{a}_2 \in \mathbb{F}_q$. Die Galoisgruppen G_i der Gleichungen $\phi(y) = \tilde{a}_i y$ seien endliche zyklische Untergruppen von $\mathbb{G}_\mathrm{m}(\mathbb{F}_p)$ mit $k := \#G_1$ bzw. $l := \#G_2$. Die Darstellungsmatrix A_L von Φ des zugehörigen Frobenius-Modul M_L lässt sich also durch einen Frobenius-Basiswechsel auf die folgende Gestalt transformieren:*

$$A := \begin{pmatrix} \tilde{a}_1 & c \\ 0 & \tilde{a}_2 \end{pmatrix} \quad \text{mit } c := \frac{\phi(f_1)}{f_2}.$$

Außerdem sei $f \in F$ ein Transformationselement, so dass $\tilde{c} = c - (\phi(f) - f)$ additiv minimal ist. Dann gelten:
(a) Ist $\tilde{c}$ ein Polynom in $\mathbb{F}_g(s)[t]$, so ist die Galoisgruppe

$$G = \mathbb{B}_2(F^\phi)_{k,l,e,H} = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H < \mathbb{G}_\mathrm{a}(F^\phi) \}.$$

(b) Ist $\tilde{c} \in F$ Körperlement mit ausschließlich ϕ-periodischen Polstellen, so ist die Galoisgruppe

$$G = \mathbb{B}_2(F^\phi)_{k,l,e,H} = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H < \mathbb{G}_\mathrm{a}(F^\phi) \}.$$

(c) Ist $\tilde{c}$ ein Körperelement mit mindestens einer nicht ϕ-periodischen Polstelle und (a) und (b) treten nicht auf, so ist die Galoisgruppe

$$G = \mathbb{B}_2(F^\phi)_{k,l,e,H} = \{ \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H = \mathbb{G}_\mathrm{a}(F^\phi) \}.$$

Beweis. Wir betrachten die additive Differenzengleichung $\phi(y) = y + \frac{\eta_2}{\eta_1}c$. Diese hat genau dann eine algebraische Lösung, falls die Gleichung $\phi(y) = y + c$ eine algebraische Lösung besitzt, da η_1, η_2 algebraisch über F^{ord} sind. Diese Gleichung hat aber genau dann eine algebraische Lösung bzw. eine endliche Galoisgruppe, falls die Gleichung $\phi(y) = y + \tilde{c}$ eine algebraische Lösung besitzt. Mit Satz 4.28 erhalten wir die entsprechenden Aussagen. Nun wollen wir noch für die Fälle (a) und (b) Aussagen über das Minimalpolynom von $\tilde{\eta}$ machen. Da η_1, η_2 algebraisch über $\mathbb{F}_q$ sind, existieren nach Bemerkung 1.29 natürliche Zahlen m_1, m_2 mit $\eta_i^{m_i} \in \mathbb{F}_q$ und $c = \frac{c_1}{c_2}$ mit $c_1 \in \mathbb{F}_q(s)[t]$ und $c_2 \in \mathbb{F}_q[t]$. Mit $k := \text{kgV}\{m_1, m_2\}$ gilt auch $\left(\frac{\eta_2}{\eta_1}\right)^k \in \mathbb{F}_q$. Wir erhalten mit

$$d := \prod_{i=0}^{l-1} \phi^i(c_2),$$

die Gleichung

$$\phi(\tilde{\eta}d) = \tilde{\eta}d + \frac{\eta_2}{\eta_1}cd$$

mit $cd = \sum_{j=0}^{h} b_i t^i \in \mathbb{F}_q(s)[t]$. Wie im Beweis zu Satz 4.28 erhalten wir für jeden Koeffizienten $b_j \neq 0$ eine algebraische Lösung θ_j mit $\phi(\theta_j) = \theta_j + b_j$ mit Minimalpolynom

$$g_{\theta_j} = X^p - X - b_j.$$

Damit gilt $\phi(\theta_j t^j) = \theta_j t^j + b_j t^j$ und daher ist $\bar{\theta}_j := \theta_j t^j$ eine algebraische Lösung der Gleichung $\phi(y) = y + b_j t^j$ mit Minimalpolynom

$$g_{\bar{\theta}_j} = X^p - (t^j)^{p-1}X - b_j(t^j)^p.$$

Da $\left(\frac{\eta_2}{\eta_1}\right)^k$ in $\mathbb{F}_q$ liegt, erhalten wir damit eine algebraische Lösung $\bar{\eta}_j$ mit $\phi(\bar{\eta}_j) = \bar{\eta}_j + \frac{\eta_2}{\eta_1}b_j t^j$ mit Minimalpolynom

$$g_{\bar{\eta}_j} = (X^p - (t^j)^{p-1}X)^k - \left(b_j(t^j)^p\frac{\eta_2}{\eta_1}\right)^k.$$

Damit lässt sich $\tilde{\eta}d$ schreiben als $\tilde{\eta}d = \sum_{j=0}^{h} \bar{\eta}_j$. Wir erhalten das Minimalpolynom $g_{\tilde{\eta}}$ als Teiler der Resultante der Polynome $g_{\bar{\eta}_j}$. Damit lassen sich wie in Satz 4.28 Abschätzungen für den Grad des Minimalpolynoms von $\tilde{\eta}$ und damit auch für die Elementanzahl des additiven Teils der Galoisgruppe machen. □

Zusammenfassend können also folgende Gruppen auftreten, falls die Galoisgruppe in der

Gruppe der oberen Dreiecksmatrizen enthalten ist:

$$\mathbb{B}_2(F^\phi) = \{\begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in \mathbb{G}_m(F^\phi), \gamma \in \mathbb{G}_a(F^\phi)\},$$

$$\mathbb{B}_2(F^\phi)_{l,\mathbb{G}_m} = \{\begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^l = 1, \delta \in \mathbb{G}_m(F^\phi), \gamma \in \mathbb{G}_a(F^\phi)\},$$

$$\mathbb{B}_2(F^\phi)_{\mathbb{G}_m,l} = \{\begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha \in \mathbb{G}_m(F^\phi), \delta^l = 1, \gamma \in \mathbb{G}_a(F^\phi)\},$$

$$\mathbb{B}_2(F^\phi)_{k,l,e,H} = \{\begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix} \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha}\delta^{g_\delta} = 1, \gamma \in H \leq \mathbb{G}_\mathrm{a}(F^\phi)\},$$

$$\mathbb{G}_a(F^\phi) \cong \{\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in \mathbb{G}_a(F^\phi)\},$$

$$H = \{\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in \mathbb{G}_a(\tilde{F}) \text{ mit } \mathbb{G}_\mathrm{a}(\mathbb{F}_p) \lneq H \lneq \mathbb{G}_a(F^\phi)\}$$

$$\mathbb{G}_\mathrm{a}(\mathbb{F}_p) = \{\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in \mathbb{G}_\mathrm{a}(\mathbb{F}_p)\}.$$

Dies sind alle möglichen Gruppen, die als Galoisgruppe einer reduziblen aber nicht komplett reduziblen Differenzengleichungen mit $\phi|_{\mathbb{F}_q(s)} = \phi_p$ auftreten können.

5.2 Zerfallende Tori

Definition 5.3. Eine algebraische Gruppe über einem Körper K heißt K**-Torus**, falls sie über dem algebraischen Abschluss $\bar{K}$ isomorph zu einem direkten Produkt $\mathbb{G}_\mathrm{m}(\bar{K})^d$ für eine natürliche Zahl $d \in \mathbb{N}$ ist. Für eine algebraische Erweiterung $\hat{K} \geq K$ heißt ein K-Torus $\hat{K}$**-zerfallend**, falls er über $\hat{K}$ isomorph zu einem direkten Produkt $\mathbb{G}_\mathrm{m}(\hat{K})^d$ für eine natürliche Zahl $d \in \mathbb{N}$ ist.

Es sei nun der Operator P_L komplett reduzibel, d.h. es gilt

$$P_L = (\phi - a_2)(\phi - a_1) = (\phi - a_1)(\phi - a_2) \text{ mit } a_1 \neq a_2,$$

so ist die Galoisgruppe nach Satz 5.1(b) in einem F^ϕ-zerfallenden Torus, also in der Gruppe der Diagonalmatrizen, enthalten. Da die beiden Faktoren kommutieren, also

$$(\phi - a_2)(\phi - a_1) = \phi^2 + (-\phi(a_2) - a_1)\phi + a_1a_2$$
$$(\phi - a_1)(\phi - a_2) = \phi^2 + (-\phi(a_1) - a_2)\phi + a_1a_2,$$

gilt, folgt durch Koeffizientenvergleich, dass $-\phi(a_2) - a_1 = -\phi(a_1) - a_2$ bzw.

$$a_1 - a_2 = \phi(a_1) - \phi(a_2) = \phi(a_1 - a_2)$$

gelten muss, d.h. die Differenz $a_1 - a_2$ ist ϕ-invariant. Daher können wir mit den Basiswechselmatrizen

$$T_4 = \begin{pmatrix} -a_2 & 1 \\ -a_1 & 1 \end{pmatrix} \qquad T_4^{-1} = \begin{pmatrix} \frac{1}{a_1-a_2} & \frac{-1}{a_1-a_2} \\ \frac{a_1}{a_1-a_2} & \frac{-a_2}{a_1-a_2} \end{pmatrix}$$

die Darstellungsmatrix

$$A_L = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$$

auf die folgende Gestalt bringen

$$\begin{aligned} D = \phi(T_4) A_L T_4^{-1} &= \begin{pmatrix} -a_2 & 1 \\ -a_1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \begin{pmatrix} \frac{1}{a_1-a_2} & \frac{-1}{a_1-a_2} \\ \frac{a_1}{a_1-a_2} & \frac{-a_2}{a_1-a_2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{-b-\phi(a_2)a_1-aa_1}{a_1-a_2} & \frac{b+\phi(a_2)a_2+aa_2}{a_1-a_2} \\ \frac{-b-\phi(a_1)a_1-aa_1}{a_1-a_2} & \frac{b+\phi(a_1)a_2-aa_2}{a_1-a_2} \end{pmatrix}. \end{aligned}$$

Wegen $b = a_1 a_2$, $a = -\phi(a_1) - a_2$ und $\phi(a_1) = \frac{-aa_1-b}{a_1}$ erhalten wir daraus

$$D = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$$

und damit muss die Galoisgruppe in einem F^ϕ-zerfallenden Torus enthalten sein. Wir können nun Algorithmus 4.10 für Differenzengleichungen erster Ordnung auf die Diagonalelemente a_1 und a_2 anwenden und erhalten damit eine Darstellungsmatrix, an der wir direkt die Galoisgruppe der Gleichung ablesen können. Damit kommen also die folgenden Gruppen als Galoisgruppe in Frage:

$$\mathbb{T}_2(F^\phi) = \{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in \mathbb{G}_m(F^\phi)\}, \tag{1}$$

$$\begin{aligned} \mathbb{T}_2(F^\phi)_{\mathbb{G}_m,l} &= \{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha \in \mathbb{G}_m(F^\phi), \delta^l = 1\} \\ &\cong \{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha^l = 1, \delta \in \mathbb{G}_m(F^\phi)\}, \end{aligned} \tag{2}$$

$$\begin{aligned} \mathbb{T}_2(F^\phi)_{\mathbb{G}_m} &= \{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in \mathbb{G}_m(F^\phi)\} \cong \{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^2 \end{pmatrix} \mid \alpha \in \mathbb{G}_m(F^\phi)\} \cong \dots \\ &\cong \mathbb{G}_m(F^\phi), \end{aligned} \tag{3}$$

$$H \leq \mathbb{T}_2(\mathbb{F}_p) \leq \mathrm{GL}_2(\mathbb{F}_p), \tag{4}$$

$$I \cong \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}. \tag{5}$$

Die Liste der obigen Gruppen entspricht den verschiedenen Möglichkeiten für die Galoisgruppen der Faktoren. Diese können mit Hilfe von Algorithmus 4.10 berechnet werden. Es tritt als Galoisgruppe also genau dann

(1) auf, falls für beide Faktoren die volle $\mathbb{G}_m(F^\phi)$ als Galoisgruppe auftritt. Dann sind weder a_1 noch a_2 multiplikativ transformierbar.

(2) auf, falls für einen Faktor die volle $\mathbb{G}_m(F^\phi)$ und für den anderen eine echte Untergruppe von $\mathbb{G}_m(F^\phi)$ als Galoisgruppe auftritt. Also ist ohne Einschränkung a_1 multiplikativ transformierbar und a_2 ist nicht multiplikativ transformierbar mit $a_2 = a_1 - \gamma$, wobei γ ein ϕ-invariantes Element ist.

(3) auf, falls beide Faktoren nicht multiplikativ transformierbar sind, aber $a_1 = a_2^{-1}$ oder $a_1 = a_2^2$ etc. gilt.

(4) auf, falls für beide Faktoren eine echte Untergruppe von $\mathbb{G}_m(F^\phi)$ als Galoisgruppe auftritt. In diesem Fall müssen sowohl a_1 als auch a_2 multiplikativ transformierbar sein. Wir wollen zeigen, dass beide sogar gewöhnlich sein müssen. Dazu nehmen wir ohne Einschränkung an, dass a_1 multiplikativ transformierbar, aber nicht gewöhnlich ist. Damit besitzt a_1 nach Anmerkung 4.15 die Darstellung

$$a_1 = \alpha \cdot \underbrace{\frac{p_1 p_2 \cdots p_r \cdots \phi^{e_{r+1}}(p_{r+1}) \cdots \phi^{e_x}(p_x)}{\phi^{e_1}(p_1) \cdots \phi^{e_r}(p_r) p_{r+1} \cdots p_x}}_{=:\,\tilde{a}_1}.$$

Außerdem muss $a_2 = a_1 - \gamma$ mit $\gamma \in F^\phi$ gelten. Mit der Darstellung

$$\gamma = \tilde{\gamma} \cdot \frac{q_1 \cdots q_r}{\hat{q}_1 \cdots \hat{q}_s},$$

wobei $\tilde{\gamma}$ in $\mathbb{F}_p$ und die $q_i, \hat{q}_i$ in $\mathbb{F}_p[t]$ liegen, erhalten wir für a_2 die folgende Darstellung:

$$a_2 = \frac{\tilde{\gamma} \cdot \text{Nenner}(\tilde{a}_1) \cdot q_1 \cdots q_r + \alpha \cdot \text{Zähler}(\tilde{a}_1) \cdot \hat{q}_1 \cdots \hat{q}_s}{\text{Nenner}(\tilde{a}_1) \cdot \hat{q}_1 \cdots \hat{q}_s}.$$

Da die $\hat{q}_i$ in F^ϕ liegen, muss $r = s$ und $q_i = \hat{q}_i$ für alle $i = 1, \ldots, r$ gelten, denn sonst kann a_2 nicht multiplikativ transformierbar sein. Daher gilt

$$a_2 = \frac{\tilde{\gamma} \cdot \text{Nenner}(\tilde{a}_1) + \alpha \cdot \text{Zähler}(\tilde{a}_1)}{\text{Nenner}(\tilde{a}_1)}.$$

Damit a_2 multiplikativ transformierbar ist, muss der Zähler die Gestalt $\delta \cdot \text{Zähler}(\tilde{a}_1)$ haben. Dies liefert $\tilde{\gamma} = (\alpha - \delta) \cdot a_1$. Da aber $\tilde{\gamma}$ in $\mathbb{F}_p$ liegen muss, aber a_1 nicht in $\mathbb{F}_p$ liegt, erhalten wir einen Widerspruch. Also müssen sowohl a_1 als auch a_2 gewöhnlich sein. Damit ist G eine Untergruppe $\mathbb{T}_2(\mathbb{F}_p) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Die Elementanzahl hängt von der Elementanzahl der Galoisgruppen von $\phi(y) = a_i y$ ab.

(5) auf, falls für beide Faktoren die triviale Gruppe als Galoisgruppe auftritt.

Ist L dagegen irreduzibel, müssen wir weitere Kriterien finden, um die Galoisgruppe zu bestimmen.

5.3 Diedergruppen

Wir gehen davon aus, dass die Differenzengleichung $L(y) = \phi^2(y) + a\phi(y) + by = 0$ irreduzibel ist. Nach Satz 1.36 wissen wir: Falls eine ϕ-Liouvillsche Lösung existiert, so existiert auch eine Lösung $\eta \in E$ mit $u := \frac{\phi(\eta)}{\eta}$ algebraisch vom Grad höchstens $I(m, n, p)$. Es sei nun $P_u(X) \in F[X]$ das Minimalpolynom von u. Dabei ist die Schranke $I(m, n, p)$ unabhängig von L. Die Konjugierten $\sigma(u)$ für $\sigma \in G$ sind ebenfalls Nullstellen von $P_u(X)$, denn es gilt

$$P_u(\sigma(u)) = \sigma(P_u(u)) = \sigma(0) = 0.$$

Außerdem gilt für die Konjugierten

$$\sigma(u) = \frac{\sigma(\phi(\eta))}{\sigma(\eta)} = \frac{\phi(\sigma(\eta))}{\sigma(\eta)} = \frac{\phi(\eta_2)}{\eta_2},$$

wobei $\eta_2 = \sigma(\eta)$ ebenfalls eine Lösung von L ist. Wir können also das Minimalpolynom $P_u(X)$ schreiben als

$$P_u(X) = \prod_{i=1}^{d}(X - \frac{\phi(\eta_i)}{\eta_i}),$$

wobei $\eta_1 := \eta$ und η_i für $i = 2, \ldots, d$ weitere Lösungen von L sind. Durch Ausmultiplizieren ergibt sich

$$P_u(X) = X^d \underbrace{- \sum_{i=1}^{d} \frac{\phi(\eta_i)}{\eta_i}}_{:= b_{d-1}} X^{d-1} + \ldots + \underbrace{(-1)^d \prod_{i=1}^{d} \frac{\phi(\eta_i)}{\eta_i}}_{:= b_0}.$$

Man sieht am niedrigsten Koeffizienten b_0, dass dieses Minimalpolynom nur dann in F liegen kann, falls die d-te symmetrische Potenz $\mathrm{Sym}_d(L)$ von L eine ϕ-exponentielle Lösung besitzt. Um die übrigen Koeffizienten zu berechnen, gehen wir folgendermaßen vor: Jeder Koeffizient b_{d-j} ist ein elementar symmetrisches Polynom in den $u_i = \frac{\phi(\eta_i)}{\eta_i}$. Dies liefert die folgende Darstellung:

$$\begin{aligned}\binom{d}{i} b_{d-i} &= \sum_{\pi \in S_d} \frac{\phi(\eta_{\pi(1)} \cdots \eta_{\pi(i)})}{\eta_{\pi(1)} \cdots \eta_{\pi(i)}} \\ &= \frac{\sum_{\pi \in S_d} \phi(\eta_{\pi(1)} \cdots \eta_{\pi(i)}) \eta_{\pi(i+1)} \cdots \eta_{\pi(d)}}{\eta_1 \cdots \eta_d},\end{aligned}$$

wobei S_d die Gruppe der Permutationen von d Elementen bezeichnet. Wie oben bereits erwähnt, ist $\phi - b_0$ mit $b_0 = \prod_{i=1}^{d} \frac{\phi(\eta_i)}{\eta_i}$ ein Rechtsfaktor der d-ten symmetrischen Potenz $\mathrm{Sym}_d(L)$. Außerdem ist für $i = 1, \ldots, m-1$ das Element $(\eta_1 \cdots \eta_d) b_{d-i}$ eine Lösung der Gleichung

$$L_i := \mathrm{Sym}_{d-i}(L) \otimes \mathrm{Sym}_i(L^\phi).$$

Diese muss also einen Rechtsfaktor vom Grad 1 haben, denn

$$\frac{\phi((\eta_1 \cdots \eta_d) b_{d-i})}{(\eta_1 \cdots \eta_d) b_{d-i}} = \frac{\phi(\eta_1 \cdots \eta_d)}{\eta_1 \cdots \eta_d} \cdot \frac{\phi(b_{d-i})}{b_{d-i}} = b_0 \cdot \frac{\phi(b_{d-i})}{b_{d-i}}$$

liegt in F. Also finden wir einen Rechtsfaktor $\phi - x$ vom Grad 1 von L_i mit $x = b_0 \cdot \frac{\phi(b_{d-i})}{b_{d-i}}$. Daraus erhalten wir den Koeffizienten b_{d-i} als rationale Lösung der Differenzengleichung ersten Grades $\phi(y) = \frac{x}{b_0} y$. Dies liefert einen Algorithmus zur Berechnung des Minimalpolynoms von u.

Zur Erinnerung (vgl. Kapitel 2): alle d-fachen Produkte von Lösungen von L sind Lösungen von $\mathrm{Sym}_d(L)$. Zusammen mit den Sätzen 1.35 und 1.36 ist nun klar, wie weiter vorzugehen ist. Wir berechnen die d-te symmetrische Potenz $\mathrm{Sym}_d(L)$ bis zur vorgegebenen Schranke

$d \leq I(m,n,p)$. Falls diese eine nicht-triviale ϕ-exponentielle Lösung besitzt, ist die Galoisgruppe eine echte Untergruppe von $\mathrm{GL}_2(F^\phi)$. Um welche Gruppe es sich handelt hängt vom Grad der minimalen symmetrischen Potenz $\mathrm{Sym}_d(L)$ ab, die eine ϕ-exponentielle Lösung besitzt. Hat dagegen keine der symmetrischen Potenzen $\mathrm{Sym}_d(L)$ für $d \leq I(m,n,p)$ eine ϕ-exponentielle Lösung, so kommen als Galoisgruppe nur noch die Gruppen $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$, sowie deren Zwischengruppen in Frage.

Satz 5.4. *Es sei $L(y) = 0$ eine irreduzible Differenzengleichung zweiter Ordnung mit Galoisgruppe $G \leq \mathrm{GL}_2(F^\phi)$. Diese ist in der unendlichen Diedergruppe*

$$D_\infty = \{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in F^\phi\} \cup \{\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta, \gamma \in F^\phi\}$$

enthalten, falls die zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ eine ϕ-exponentielle Lösung, d.h. einen Rechtsfaktor vom Grad 1 besitzt und P_L über der entsprechenden algebraischen Erweiterung in nicht-kommutierende Linearfaktoren zerfällt.

Beweis. Es sei E ein PV-Körper von L und $V := \mathrm{Sol}_E^\phi(M_L) = F^\phi\eta_1 + F^\phi\eta_2$ der Lösungsvektorraum mit Basis η_1, η_2. Nach Satz 2.30 (c) ist $\mathrm{Sym}_2(V)$ isomorph zu $\mathrm{Sol}_E^\phi(M_{\mathrm{Sym}_2(L)})$. Die Gerade $F^\phi\eta_1 \cdot \eta_2$ in $\mathrm{Sym}_2(V)$ ist also G-invariant, falls $\mathrm{Sym}_2(L)$ eine ϕ-exponentielle Lösung besitzt. Da D_∞ eine endliche G-Bahn besitzt, deren Länge höchstens 2 ist, folgt dann mit den Sätzen 1.35 und 1.36 die Behauptung. □

Die Galoisgruppe $\mathrm{Gal}(L)$ ist also in der Diedergruppe D_∞ enthalten, wenn die zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ eine rationale Lösung besitzt. Dann besitzt aber die ursprüngliche Gleichung L eine Lösung η, für die $u := \frac{\phi(\eta)}{\eta}$ algebraisch vom Grad 2 über F ist. Also zerfällt der zugehörige Operator P_L über der algebraischen Erweiterung $F(u)/F$ vom Grad 2 in Linearfaktoren, nämlich $P_L = (\phi - \tilde{u})(\phi - u)$. Um nun zu entscheiden, ob die volle unendliche Diedergruppe oder eine endliche Untergruppe als Galoisgruppe auftritt, müssen wir die Galoisgruppe der Differenzengleichung $\phi(y) = uy$ vom Grad 1 über dem Frobenius-Körper $F(u)$ bestimmen. Ist diese eine endliche Untergruppe der $\mathbb{G}_\mathrm{m}(F^\phi)$, so besitzt die Gleichung $\phi(y) = uy$ und damit auch unsere ursprüngliche Gleichung L nur algebraische Lösungen. In diesem Fall muss die Galoisgruppe eine endliche Untergruppe der Diedergruppe sein. Tritt dagegen die volle $\mathbb{G}_\mathrm{m}(F^\phi)$ als Galoisgruppe von $\phi(y) = uy$ auf, so muss die Galoisgruppe $\mathrm{Gal}(L)$ die volle Diedergruppe D_∞ sein.

5.4 Nicht-Zerfallende Tori

Satz 5.5. *Ein K-Torus $\mathbb{T}$ zerfällt über einer endlichen Galoiserweiterung $\hat{K}$ von K.*

Beweis. [Tit68, III Theorem 1.4.1] □

Satz 5.6. *Es sei $\mathbb{T} \leq \mathrm{GL}_n(F^\phi)$ ein F^ϕ-Torus. Dann existiert eine Körpererweiterung $K \geq F^\phi$ vom Grad höchstens $n!$, so dass $\mathbb{T}$ ein K-zerfallender Torus ist.*

Beweis. Nach [Tit68, III Theorem 1.6.4.] existiert ein Element $T \in \mathbb{T}$, das eine Untergruppe $H \leq \mathbb{T}$ erzeugt, die Zariski-dicht in $\mathbb{T}$ liegt. Es sei $p_T(X) \in F^\phi[X]$ das charakteristische Polynom mit $\deg(p_T) = n$ dieses Erzeugers. Nach [Mey76, Satz 6.5.4] existiert

eine Körpererweiterung $K \geq F^\phi$ vom Grad höchstens $n!$, über der dieses Polynom p_T in Linearfaktoren zerfällt. Also ist T über K diagonalisierbar, d.h. es existiert ein Element $A \in \mathrm{GL}_n(K)$ mit

$$ATA^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} =: D.$$

Die von $D = ATA^{-1}$ erzeugte Untergruppe liegt dicht in $\mathbb{T}$ und ist abgeschlossen. Daher ist jedes Element von $\mathbb{T}$ über K diagonalisierbar und damit ist $\mathbb{T}$ ein K-zerfallender Torus. □

Satz 5.7. *Es sei $L(y) = 0$ eine irreduzible Differenzengleichung zweiter Ordnung mit Galoisgruppe $G \leq \mathrm{GL}_2(F^\phi)$. Diese ist in einem nicht-zerfallenden Torus $\mathbb{T}$ enthalten, falls die zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ eine ϕ-exponentielle Lösung, d.h. einen Rechtsfaktor vom Grad 1 besitzt und P_L über der entsprechenden algebraischen Erweiterung in kommutierende Linearfaktoren zerfällt.*

Beweis. Besitzt die zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ eine ϕ-exponentielle Lösung, d.h. einen Rechtsfaktor vom Grad 1, so zerfällt P_L über einer algebraischen Erweiterung K vom Grad 2 in Linearfaktoren. Falls diese darüber hinaus kommutieren, ist die Galoisgruppe von L über K nach Satz 5.1 in einem zerfallenden Torus $\mathbb{T}$ enthalten. Da L irreduzibel über F ist, ist $\mathbb{T}$ nicht-zerfallend über F^ϕ. □

Wir berechnen also die zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ und suchen eine rationale Lösung. Existiert eine solche Lösung erhalten wir daraus wie oben das Minimalpolynom eines Elements u, so dass P_L über $F(u)$ in die Linearfaktoren $(\phi - \tilde{u})(\phi - u)$ zerfällt. Kommutieren diese Faktoren, so ist die Galoisgruppe $\mathrm{Gal}(L)$ in einem nicht-zerfallenden Torus $\mathbb{T}$ enthalten. Durch Berechnung der Galoisgruppen von $\phi(y) = uy$ bzw. $\phi(y) = \tilde{u}y$ erhalten wir die Struktur des Torus bzw. eine Darstellungsmatrix A von M_L über $F(u)$. Lösen wir das lineare Gleichungssystem $MAM^{-1} = B$ mit $B \in F$, so erhalten wir eine Darstellungsmatrix von M_L über F, an der wir die Struktur des Torus $\mathbb{T}$ über F^ϕ ablesen können. Wegen Satz 1.18 ist die Galoisgruppe in der kleinsten Gruppe, die B enthält, enthalten. Nicht-zerfallende Tori von höherer Dimension als 2 können wegen Satz 5.6 nicht auftreten.

5.5 Irreduzible primitive Gruppen

Falls die bisherigen Kriterien noch keine Ergebnisse geliefert haben, kommen als Galoisgruppe noch die irreduziblen primitiven Untergruppen von $\mathrm{GL}_2(F^\phi)$ und Gruppen H mit $\mathrm{SL}_2(F^\phi) \leq H \leq \mathrm{GL}_2(F^\phi)$ in Frage. Der folgende Satz liefert ein weiteres Entscheidungskriterium, welche dieser Gruppen als Galoisgruppe auftritt.

Satz 5.8. *Es sei $L(y) = 0$ eine irreduzible Differenzengleichung zweiter Ordnung mit Galoisgruppe $G \leq \mathrm{GL}_2(F^\phi)$, deren zweite symmetrische Potenz $\mathrm{Sym}_2(L)$ ebenfalls irreduzibel ist. Dann gelten:*
(a) Die vierte symmetrische Potenz $\mathrm{Sym}_4(L)$ besitzt genau dann eine ϕ-exponentielle Lösung, falls die Galoisgruppe G isomorph zur Tetraeder-Gruppe $A_4^{\mathrm{GL}_2(F^\phi)}$ ist.
(b) Es sei die vierte symmetrische Potenz $\mathrm{Sym}_4(L)$ irreduzibel. Dann besitzt die sechste

symmetrische Potenz $\mathrm{Sym}_6(L)$ *genau dann eine* ϕ*-exponentielle Lösung, falls die Galoisgruppe* G *isomorph zur Oktaeder-Gruppe* $S_4^{\mathrm{GL}_2(F^\phi)}$ *ist.*
(c) Es seien die vierte symmetrische Potenz $\mathrm{Sym}_4(L)$ *und die sechste symmetrische Potenz* $\mathrm{Sym}_6(L)$ *irreduzibel. Dann besitzt die zwölfte symmetrische Potenz* $\mathrm{Sym}_{12}(L)$ *genau dann eine* ϕ*-exponentielle Lösung, falls die Galoisgruppe* G *isomorph zur Ikosaeder-Gruppe* $A_5^{\mathrm{GL}_2(F^\phi)}$ *ist.*

Beweis. Die Gruppen-Operationen von A_4, S_4, A_5 auf $\mathbb{P}^1(F^\phi)$ haben minimale Bahnen der Länge $4, 6, 12$. Dies liefert mit analogen Argumenten wie im Beweis zu Satz 5.4 zusammen mit den Sätzen 1.35 und 1.36 die Behauptungen. □

Benutzt man die Zerlegung der Charaktere von $\mathrm{Sym}_m(V)$, wobei $V = \mathrm{Sol}_E^\Phi(M_L)$ den Lösungsvektorraum von L bezeichnet, in Verbindung mit Satz 2.30, so kann man Satz 5.8 zu folgendem Satz umformulieren.

Satz 5.9. *Es sei* $L(y) = 0$ *eine irreduzible Differenzengleichung zweiter Ordnung mit Galoisgruppe* $G \leq \mathrm{GL}_2(F^\phi)$*, deren zweite symmetrische Potenz* $\mathrm{Sym}_2(L)$ *ebenfalls irreduzibel ist. Dann gelten:*
(a) Die dritte symmetrische Potenz $\mathrm{Sym}_3(L)$ *ist genau dann reduzibel über* F*, falls die Galoisgruppe* G *isomorph zur Tetraeder-Gruppe* $A_4^{\mathrm{GL}_2(F^\phi)}$ *ist. In diesem Fall haben die Faktoren* $\mathrm{Sym}_3(L) = L_1L_2$ *beide Ordnung 2.*
(b) Es sei die dritte symmetrische Potenz $\mathrm{Sym}_3(L)$ *irreduzibel. Dann ist die vierte symmetrische Potenz* $\mathrm{Sym}_4(L)$ *genau dann reduzibel über* F*, falls die Galoisgruppe* G *isomorph zur Oktaeder-Gruppe* $S_4^{\mathrm{GL}_2(F^\phi)}$ *ist. In diesem Fall haben die Faktoren* $\mathrm{Sym}_4(L) = L_1L_2$ *Ordnung 3 bzw. 2.*
(c) Es seien die dritte symmetrische Potenz $\mathrm{Sym}_3(L)$ *und die vierte symmetrische Potenz* $\mathrm{Sym}_4(L)$ *irreduzibel. Dann ist die sechste symmetrische Potenz* $\mathrm{Sym}_6(L)$ *genau dann reduzibel über* F*, falls die Galoisgruppe* G *isomorph zur Ikosaeder-Gruppe* $A_5^{\mathrm{GL}_2(F^\phi)}$ *ist. In diesem Fall haben die Faktoren* $\mathrm{Sym}_6(L) = L_1L_2$ *Ordnung 4 bzw. 3.*

Der Vorteil an Satz 5.9 gegenüber Satz 5.8 ist, dass man die symmetrischen Potenzen nur bis Grad 6 anstatt bis Grad 12 berechnen muss. Dafür muss man diese faktorisieren und nicht nur einen Rechtsfaktor vom Grad 1 bestimmen. An dieser Stelle benötigen wir die Faktorisierungsalgorithmen aus Kapitel 3.

5.6 Zwischengruppen von $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$

Sind alle symmetrischen Potenzen $\mathrm{Sym}_d(L)$ für $d \leq I(m, n, p)$ der Differenzengleichung $L(y) = \phi^2(y) + a\phi(y) + by = 0$ irreduzibel, so kommen als Galoisgruppe nur noch Gruppen H mit $\mathrm{SL}_2(F^\phi) \leq H \leq \mathrm{GL}_2(F^\phi)$ in Frage. Solche Gruppen lassen sich für eine natürliche Zahl $m \in \mathbb{N}$ folgendermaßen charakterisieren:

$$H_m = \{A \in \mathrm{GL}_2(F^\phi) \mid \det(A)^m = 1\}.$$

Die spezielle lineare Gruppe $\mathrm{SL}_2(F^\phi)$ ist in jeder dieser Gruppen enthalten. Nach Satz 1.18 ist die Galoisgruppe G eine Untergruppe von H, falls es eine Matrix $T \in \mathrm{GL}_2(F)$ gibt, so dass

$$\phi(T) \cdot A_L \cdot T^{-1} \in H(F)$$

liegt. Dazu genügt es Matrizen der Form $D = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$ zu betrachten, denn man kann jede Matrix $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in \mathrm{GL}_2(F)$ schreiben als

$$T = S \cdot D \text{ mit } S = \begin{pmatrix} \frac{t_{11}}{\det(T)} & t_{12} \\ \frac{t_{21}}{\det(T)} & t_{22} \end{pmatrix} \in \mathrm{SL}_2(F) \text{ und } D = \begin{pmatrix} \det(T) & 0 \\ 0 & 1 \end{pmatrix}.$$

Falls also

$$\phi(T) \cdot A_L \cdot T^{-1} = \phi(S) \cdot \underbrace{\phi(D) \cdot A_L \cdot D^{-1}}_{:= B} \cdot S^{-1} \in H(F)$$

liegt, muss schon $B \in H(F)$ liegen.
Wir wollen nun untersuchen, in welchen Fällen eine Transformation der Form

$$\phi \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} \cdot A_L \cdot \begin{pmatrix} \frac{1}{f} & 0 \\ 0 & 1 \end{pmatrix} \in H(F) \tag{5.10}$$

möglich ist. Rechnen wir also (5.10) direkt aus, erhalten wir die Matrix

$$B := \begin{pmatrix} 0 & \phi(f) \\ -\frac{b}{f} & -a \end{pmatrix}.$$

Die Determinante dieser Matrix ist $\det(B) = \frac{\phi(f)}{f} b$. Um nun die Galoisgruppe G der Gleichung L zu bestimmen, müssen wir die Galoisgruppe der Differenzengleichung erster Ordnung $\phi(y) = by$ berechnen. Dazu verwenden wir Algorithmus 4.10. Besitzt diese Gleichung eine rationale Lösung $\eta \in F$, so erhalten wir mit $f := \eta^{-1}$ für die obige Determinante $\det(B) = 1$ und damit als Galoisgruppe die spezielle lineare Gruppe $\mathrm{SL}_2(F^\phi)$. Tritt dagegen eine endliche Untergruppe von $(F^\phi)^\times$, etwa mit Ordnung m, als Galoisgruppe von $\phi(y) = by$ auf, so besitzt die Gleichung $\phi(y) = b^m y$ eine rationale Lösung η. Mit $f := \eta^{-1}$ erhalten wir für die obige Determinante $\det(B)^m = \frac{\phi(f^m)}{f^m} b^m = 1$ und damit ist die Galoisgruppe G von L isomorph zur Gruppe

$$H_m = \{A \in \mathrm{GL}_2(F^\phi) \mid \det(A)^m = 1\}.$$

Andernfalls ist die Galoisgruppe der Gleichung $\phi(y) = by$ die volle multiplikative Gruppe $(F^\phi)^\times$ und als Galoisgruppe G bleibt nur noch die volle $\mathrm{GL}_2(F^\phi)$ übrig. Diese Erkenntnisse wollen wir im folgenden Satz festhalten.

Satz 5.11. *Es sei $L(y) = \phi^2(y) + a\phi(y) + by = 0$ eine irreduzible Differenzengleichung zweiter Ordnung mit Galoisgruppe $G \leq \mathrm{GL}_2(F^\phi)$. Außerdem seien alle symmetrischen Potenzen $\mathrm{Sym}_d(L)$ für $d \leq I(m,n,p)$ irreduzibel. Dann gelten:*
(a) Die Galoisgruppe G ist genau dann isomorph zur $\mathrm{SL}_2(F^\phi)$, falls für die Differenzengleichung $\phi(y) = by$ erster Ordnung die triviale Gruppe als Galoisgruppe auftritt.
(b) Die Galoisgruppe G ist genau dann isomorph zur Gruppe

$$H_m = \{A \in \mathrm{GL}_2(F^\phi) \mid \det(A)^m = 1\},$$

falls für die Differenzengleichung $\phi(y) = by$ erster Ordnung eine endliche zyklische Gruppe der Ordnung m als Galoisgruppe auftritt.
(c) Die Galoisgruppe G ist genau dann isomorph zur vollen Gruppe $\mathrm{GL}_2(F^\phi)$, falls für die Differenzengleichung $\phi(y) = by$ erster Ordnung die volle $\mathbb{G}_\mathrm{m}(F^\phi)$ als Galoisgruppe auftritt.

Damit endet der Algorithmus für Differenzengleichungen vom Grad 2.

5.7 Beispiele

Zum Abschluss des Kapitels wollen wir noch zu einigen Gleichungen zweiter Ordnung die Galoisgruppe bestimmen. Dabei soll veranschaulicht werden, wie sich die Ergebnisse der einzelnen Abschnitte auf die entsprechenden Beispiele anwenden lassen.

Beispiel 5.12. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - (t+1)\phi(y) + ty = 0$ bzw. der zugehörige Differenzen-Operator P_L ist komplett reduzibel mit der Zerlegung

$$P_L = (\phi - t)(\phi - 1) = (\phi - 1)(\phi - t).$$

Daher erhalten wir als Begleitmatrix

$$\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades die $\mathbb{G}_\mathrm{m}(\mathbb{F}_p(t))$ bzw. die triviale Gruppe als Galoisgruppe auftreten. Daher ergibt sich als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{G}_\mathrm{m}(\mathbb{F}_p(t))\}.$$

Beispiel 5.13. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - \frac{(t^2+1)}{t}\phi(y) + y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist komplett reduzibel mit der Zerlegung

$$P_L = (\phi - t)(\phi - \frac{1}{t}) = (\phi - \frac{1}{t})(\phi - t).$$

Daher erhalten wir als Begleitmatrix

$$\begin{pmatrix} t & 0 \\ 0 & \frac{1}{t} \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades die volle $\mathbb{G}_\mathrm{m}(F^\phi)$ als Galoisgruppe auftreten. Daher ergibt sich als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in \mathbb{G}_\mathrm{m}(\mathbb{F}_p(t))\}.$$

Beispiel 5.14. Es sei $F = \mathbb{F}_9(s,t) = \mathrm{Quot}(\mathbb{F}_9[s,t])$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_9(s)} = \phi_3$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_3(t)$. Ferner sei w ein Erzeuger der multiplikativen Gruppe $\mathbb{F}_9^\times$. Die Differenzengleichung $L(y) = \phi^2(y) + w^2\phi(y) + wy = 0$ bzw. der zugehörige Differenzen-Operator P_L ist reduzibel, aber nicht komplett reduzibel mit der Zerlegung

$$P_L = (\phi + w)(\phi + 1).$$

Daher erhalten wir als Begleitmatrix nach den oben beschriebenen Basiswechseln

$$\begin{pmatrix} 1 & w^2 \\ 0 & w^5 \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades die triviale Gruppe bzw. die $\mathbb{G}_\mathrm{m}(\mathbb{F}_3)$ als Galoisgruppe auftreten. Daher ergibt sich als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{\begin{pmatrix} 1 & \gamma \\ 0 & \alpha \end{pmatrix} \mid \alpha \in \mathbb{G}_\mathrm{m}(\mathbb{F}_3), \gamma \in \mathbb{G}_\mathrm{a}(\mathbb{F}_3)\}$$

eine zyklische Gruppe der Ordnung $6 = 2 \cdot 3$.

Beispiel 5.15. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + (\frac{s^{p^2}+t}{s^p+t})\phi(y) + (\frac{s^p+t}{s+t})y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist reduzibel, aber nicht komplett reduzibel mit der Zerlegung

$$P_L = (\phi - \frac{s^{p^2}+t}{s^p+t})(\phi - \frac{s^p+t}{s+t}).$$

Daher erhalten wir als Begleitmatrix nach den oben beschriebenen Basiswechseln zunächst

$$\begin{pmatrix} \frac{s^p+t}{s+t} & 1 \\ 0 & \frac{s^{p^2}+t}{s^p+t} \end{pmatrix}$$

und nach einem weiteren Basiswechsel mit Basiswechselmatrix

$$\begin{pmatrix} \frac{1}{s+t} & 0 \\ 0 & \frac{1}{s^p+t} \end{pmatrix}$$

schließlich

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades jeweils die triviale Gruppe als Galoisgruppe auftritt. Daher ergibt sich als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in \mathbb{G}_\mathrm{a}(\mathbb{F}_p)\}$$

eine zyklische Gruppe der Ordnung p.

Beispiel 5.16. Es sei $F = \mathbb{F}_9(s,t) = \mathrm{Quot}(\mathbb{F}_9[s,t])$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_9(s)} = \phi_3$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_3(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + (\frac{2s^{10}+2s^9t+2s^6+s^3t+2st+t^2}{s^4+s^3t+st+t^2})\phi(y) + (\frac{s^6+2s^3t+t^2}{s^2+2st+t^2})y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist reduzibel, aber nicht komplett reduzibel mit der Zerlegung

$$P_L = (\phi - \frac{s^3+t}{s+t})(\phi - \frac{s^3+t}{s+t}).$$

Daher erhalten wir als Begleitmatrix nach den oben beschriebenen Basiswechseln zunächst

$$\begin{pmatrix} \frac{s^3+t}{s+t} & 1 \\ 0 & \frac{s^3+t}{s+t} \end{pmatrix}$$

und nach einem weiteren Basiswechsel mit Basiswechselmatrix

$$\begin{pmatrix} \frac{1}{s+t} & 0 \\ 0 & \frac{1}{s+t} \end{pmatrix}$$

schließlich

$$\begin{pmatrix} 1 & \frac{s+t}{s^3+t} \\ 0 & 1 \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades jeweils die triviale Gruppe als Galoisgruppe auftritt. Da $c = \frac{s+t}{s^3+t}$ additiv minimal ist und eine nicht ϕ-periodische Polstelle besitzt, ergibt sich als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in \mathbb{G}_\mathrm{a}(\mathbb{F}_3(t))\}.$$

Beispiel 5.17. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - (\frac{s^p+s+t}{s-t})\phi(y) + (\frac{s^p-t}{s-t})y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist reduzibel, aber nicht komplett reduzibel mit der Zerlegung

$$P_L = (\phi - \frac{s^p-t}{s-t})(\phi - 1).$$

Daher erhalten wir als Begleitmatrix nach den oben beschriebenen Basiswechseln zunächst

$$\begin{pmatrix} 1 & 1 \\ 0 & \frac{s^p-t}{s-t} \end{pmatrix}$$

und nach einem weiteren Basiswechsel mit Basiswechselmatrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{s-t} \end{pmatrix}$$

schließlich

$$\begin{pmatrix} 1 & s-t \\ 0 & 1 \end{pmatrix},$$

wobei für die Faktoren als Differenzengleichungen ersten Grades jeweils die triviale Gruppe als Galoisgruppe auftritt. Da $c = s - t$ additiv minimal und ein Polynom in $\mathbb{F}_q(s)[t]$ ist, ergibt sich nach Satz 5.2 als Galoisgruppe von L

$$\mathrm{Gal}(L) = \{ \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in H < \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p(t)) \}$$

eine endliche Gruppe der Ordnung $\#H$. Um diese zu bestimmen, müssen wir das Minimalpolynom von η mit $\phi(\eta) = \eta + s - t$ bestimmen. Dazu schreiben wir η als Summe $\eta = \eta_1 + \eta_2$ mit $\phi(\eta_1) = \eta_1 + s$ und $\phi(\eta_1) = \eta_1 - t$. Die zugehörigen Minimalpolynome sind

$$\begin{aligned} g_{\eta_1}(X) &= X^p - X - s \quad \text{bzw.} \\ g_{\eta_2}(X) &= X^p - t^{p-1}X + t^p. \end{aligned}$$

Dann erhalten wir das Minimalpolynom g_η als Teiler der Resultante

$$\mathrm{Res}_T(g_{\eta_1}(X - T), g_{\eta_2}(T)).$$

Dies ist ein Polynom vom Grad p^2 und damit gilt für die Galoisgruppe

$$\mathrm{Gal}(L) = \{ \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \mid \gamma \in H < \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p(t)) \}$$

mit $\#H \leq p^2$. Daher ist G eine endliche Gruppe der Ordnung höchstens p^2. Wie in Beispiel 4.31 ist

$$g_\eta = \mathrm{Res}_T(g_{\eta_1}(X), g_{\eta_2}(X - T))$$

für den Spezialfall $p = 3$ und $q = 9$. In diesem Fall ist also die Galoisgruppe eine Gruppe der Ordnung $3^2 = 9$.

Beispiel 5.18. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + ty = 0$ ist irreduzibel. Die zweite symmetrische Potenz $\mathrm{Sym}_2(L) = -\frac{1}{t^2}\phi^3 - \frac{1}{t^2}\phi^2 + \phi + 1$ hat einen Rechtsfaktor vom Grad 1, nämlich $\phi + t$. Daher zerfällt P_L über $F(\sqrt{t})$ in die Faktoren

$$P_L = \phi^2 + t = (\phi + \sqrt{t})(\phi - \sqrt{t}) = (\phi - \sqrt{t})(\phi + \sqrt{t}).$$

Wir erhalten also als Galoisgruppe einen nicht-zerfallenden Torus. Über $F(\sqrt{t})$ hat die Darstellungsmatrix von Φ die folgende Gestalt:

$$A := \begin{pmatrix} \sqrt{t} & 0 \\ 0 & -\sqrt{t} \end{pmatrix}.$$

Mit der Konjugationsmatrix

$$M := \begin{pmatrix} \sqrt{t} & -\sqrt{t} \\ 1 & 1 \end{pmatrix}, \qquad M^{-1} = \begin{pmatrix} \frac{-1}{t\sqrt{t}} & -1 \\ \frac{1}{t\sqrt{t}} & -1 \end{pmatrix}$$

ergibt sich

$$M \cdot A \cdot M^{-1} = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}$$

und damit als Galoisgruppe

$$\mathrm{Gal}(L) \leq \{ \begin{pmatrix} \alpha & \beta t \\ \beta & \alpha \end{pmatrix} \in \mathrm{GL}_2(F^\phi) \mid \alpha, \beta \in \mathbb{G}_\mathrm{m}(\mathbb{F}_p(t)), \alpha^2 + \beta^2 t \neq 0 \}.$$

Beispiel 5.19. Es sei $F = \mathbb{F}_9(s,t) = \mathrm{Quot}(\mathbb{F}_9[s,t])$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_9(s)} = \phi_3$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_3(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - s^2t^2y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist irreduzibel. Die zweite symmetrische Potenz $\mathrm{Sym}_2(L) = \frac{2}{s^{12}t^4}\phi^3 + \frac{2}{s^4t^4}\phi^2 + \phi + 1$ hat einen Rechtsfaktor vom Grad 1, nämlich $\phi + st^2$. Daher zerfällt P_L über $F(\sqrt{s})$ in die Faktoren

$$P_L = \phi^2 - s^2t^2 = (\phi + \sqrt{s^3}t)(\phi - \sqrt{s}t).$$

Die beiden Faktoren haben über $F(\sqrt{s})$ die volle $\mathbb{G}_\mathrm{m}(F^\phi)$ als Galoisgruppe. Daher ist $\mathrm{Gal}(L)$ isomorph zur unendlichen Diedergruppe D_∞.

Beispiel 5.20. Es sei $F = \mathbb{F}_9(s,t) = \mathrm{Quot}(\mathbb{F}_9[s,t])$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_9(s)} = \phi_3$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_3(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - s^2y = 0$ bzw. der zugehörige Differenzen-Operator P_L ist irreduzibel. Die zweite symmetrische Potenz $\mathrm{Sym}_2(L) = \frac{2}{s^{12}}\phi^3 + \frac{2}{s^4}\phi^2 + \phi + 1$ hat einen Rechtsfaktor vom Grad 1, nämlich $\phi + s$. Daher zerfällt P_L über $F(\sqrt{s})$ in die Faktoren

$$P_L = \phi^2 - s^2 = (\phi + \sqrt{s^3})(\phi - \sqrt{s}).$$

Die beiden Faktoren haben über $F(\sqrt{s})$ eine endliche Untergruppe von $\mathbb{G}_\mathrm{m}(F^\phi)$ als Galoisgruppe, da man die Gleichung als gewöhnliche Gleichung betrachten kann. Daher ist $\mathrm{Gal}(L)$ isomorph zu einer endlichen Untergruppe der Diedergruppe D_∞.

Beispiel 5.21. Es sei $F = \mathbb{F}_9(s,t) = \mathrm{Quot}(\mathbb{F}_9[s,t])$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_9(s)} = \phi_3$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_3(t)$. Die Differenzengleichung $L(y) = \phi^2(y) - sy = 0$ bzw. der zugehörige Differenzen-Operator P_L ist irreduzibel. Die zweite symmetrische Potenz $\mathrm{Sym}_2(L) = \frac{2}{s^6}\phi^3 + \frac{2}{s^2}\phi^2 + \phi + 1$ ist ebenfalls irreduzibel. Die vierte symmetrische Potenz $\mathrm{Sym}_4(L) = \frac{2s^{12}+2}{s^120}\phi^5 + \frac{2s^4+2}{s^40}\phi^4 + \phi^3 + \phi^2 + \phi + 1$ hat dagegen einen Rechtsfaktor vom Grad 1, nämlich $\phi + s$. Daher ist $\mathrm{Gal}(L)$ isomorph zur Tetraedergruppe $A_4^{\mathrm{GL}_2(F^\phi)}$.

Beispiel 5.22. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + \frac{s^p+t}{s+t}y = 0$ ist irreduzibel. Alle symmetrischen Potenzen von P_L bis zum Grad 12 sind ebenfalls irreduzibel. Als Galoisgruppe kommen also nur Zwischengruppen H von $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$ in Frage, d.h. es gilt $\mathrm{SL}_2(F^\phi) \leq H \leq \mathrm{GL}_2(F^\phi)$. Die Galoisgruppe der Gleichung $\phi(y) = by$ ersten Grades mit $b = \frac{s^p+t}{s+t}$ ist die triviale Gruppe. Damit ist $\mathrm{SL}_2(\mathbb{F}_p(t))$ die Galoisgruppe von L.

Beispiel 5.23. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + s\frac{s^p+t}{s+t}y = 0$ ist irreduzibel. Alle symmetrischen Potenzen von P_L bis zum Grad 12 sind ebenfalls irreduzibel. Als Galoisgruppe kommen also nur Zwischengruppen H von $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$ in Frage, d.h. es gilt $\mathrm{SL}_2(F^\phi) \leq H \leq \mathrm{GL}_2(F^\phi)$. Die Galoisgruppe der Gleichung $\phi(y) = by$ ersten Grades mit $b = s\frac{s^p+t}{s+t}$ ist eine zyklische Gruppe der Ordnung $p-1$. Damit gilt für die Galoisgruppe

$$\mathrm{Gal}(L) = H_{p-1} = \{A \in \mathrm{GL}_2(F^\phi) \mid \det(A)^{p-1} = 1\}.$$

Beispiel 5.24. Es sei p eine Primzahl und $F = \mathbb{F}_q(s,t) = \mathrm{Quot}(\mathbb{F}_q[s,t])$ mit $q = p^n$ der Frobenius-Körper mit Endomorphismus $\phi|_{\mathbb{F}_q(s)} = \phi_p$ und $\phi(t) = t$, also $F^\phi = \mathbb{F}_p(t)$. Die Differenzengleichung $L(y) = \phi^2(y) + t\frac{s^p+t}{s+t}y = 0$ ist irreduzibel. Alle symmetrischen Potenzen von P_L bis zum Grad 12 sind ebenfalls irreduzibel. Als Galoisgruppe kommen also nur Zwischengruppen H von $\mathrm{SL}_2(F^\phi)$ und $\mathrm{GL}_2(F^\phi)$ in Frage. Die Galoisgruppe der Gleichung $\phi(y) = by$ ersten Grades mit $b = t\frac{s^p+t}{s+t}$ ist die volle $\mathbb{G}_\mathrm{m}(F^\phi)$. Daher tritt die volle $\mathrm{GL}_2(\mathbb{F}_p(t))$ als Galoisgruppe von L auf.

Kapitel 6

Allgemeine Berechenbarkeit

Nachdem wir für lineare Differenzengleichungen bis Grad 2 die Galoisgruppe berechnen können, wollen wir im abschließenden Kapitel noch einige Anmerkungen zur allgemeinen Berechenbarkeit der Galoisgruppe von linearen Differenzengleichungen vom Grad $n \in \mathbb{N}$ machen. Dazu benötigen wir die Sprache der Tannaka-Kategorien. Für die grundlegenden Definitionen und Sätze der Kategorien-Theorie verweisen wir an dieser Stelle auf [Lan71] und [DM82] sowie den Anhang von [vdPS03]. Schließlich werden wir sehen, wie sich diese Theorie auf unsere Gleichungen bzw. die zugrundeliegenden Frobenius-Moduln anwenden lassen.

6.1 Tannaka-Kategorien

Definition 6.1. Es sei $\mathfrak{C} = (\mathrm{Ob}(\mathfrak{C}), \mathrm{Mor}_{\mathfrak{C}}(A, B))$ ein Paar, das aus einer Klasse von Ojekten $\mathrm{Ob}(\mathfrak{C})$ sowie disjunkten Mengen $\mathrm{Mor}_{\mathfrak{C}}(A, B)$ von Morphismen für alle $A, B \in \mathrm{Ob}(\mathfrak{C})$ besteht. Ein solches Paar heißt **Kategorie**, falls die folgenden Bedingungen erfüllt sind:

(i) Es existiert ein Identitäsmorphismus $\mathrm{id}_A \in \mathrm{Mor}_{\mathfrak{C}}(A, A)$für alle $A \in \mathrm{Ob}(\mathfrak{C})$.

(ii) Es existiert eine Komposition von Morphismen, d.h. für alle $A, B, C \in \mathrm{Ob}(\mathfrak{C})$ existieren Abbildungen

$$\begin{array}{rccc} \circ: & \mathrm{Mor}_{\mathfrak{C}}(B,C) \times \mathrm{Mor}_{\mathfrak{C}}(A,B) & \longrightarrow & \mathrm{Mor}_{\mathfrak{C}}(A,C) \\ & (g, f) & \longmapsto & g \circ f \end{array},$$

so dass für alle $f \in \mathrm{Mor}_{\mathfrak{C}}(A, B), g \in \mathrm{Mor}_{\mathfrak{C}}(B, C), h \in \mathrm{Mor}_{\mathfrak{C}}(C, D)$ mit $A, B, C, D \in \mathrm{Ob}(\mathfrak{C})$ gilt:

- $(h \circ g) \circ f = h \circ (g \circ f)$
- $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.

Definition 6.2. Ein (kovarianter) **Funktor** $F : \mathfrak{A} \longrightarrow \mathfrak{C}$ von einer Kategorie $\mathfrak{A}$ in eine andere Kategorie $\mathfrak{C}$ ist eine Vorschrift,

(i) die jedem Objekt $A \in \mathfrak{A}$ ein Objekt $F(A) \in \mathfrak{C}$ zuordnet und

(*ii*) die jedem Morphismus $f \in \mathrm{Mor}_{\mathfrak{A}}(A_1, A_2)$ einen Morphismus $F(f) \in \mathrm{Mor}_{\mathfrak{C}}(F(A_1), F(A_2))$ zuordnet. Darüber hinaus soll $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ für alle $A \in \mathfrak{A}$ und $F(f \circ g) = F(f) \circ F(g)$ für alle Morphismen $g \in \mathrm{Mor}_{\mathfrak{A}}(A_1, A_2)$, $f \in \mathrm{Mor}_{\mathfrak{A}}(A_2, A_3)$ gelten.

Ist $G : \mathfrak{A}^\circ \longrightarrow \mathfrak{C}$ ein Funktor, so heißt der aus G resultierende Funktor $F : \mathfrak{A} \longrightarrow \mathfrak{C}$ **kontravariant**.

Definition 6.3. Eine Kategorie $\mathfrak{A}$ heißt **additive Kategorie**, falls die folgenden Bedingungen erfüllt sind:

(*i*) Für alle Objekte $A, B \in \mathfrak{A}$ trägt $\mathrm{Mor}_{\mathfrak{A}}(A, B)$ die Struktur einer abelschen Gruppe.

(*ii*) Die Komposition ist distributiv bezüglich der Addition, d.h. für alle Objekte A, B, C, D und Morphismen $f \in \mathrm{Mor}_{\mathfrak{A}}(A, B)$, $g, \tilde{g} \in \mathrm{Mor}_{\mathfrak{A}}(B, C)$, $h \in \mathrm{Mor}_{\mathfrak{A}}(C, D)$, also

$$A \xrightarrow{f} B \underset{\tilde{g}}{\overset{g}{\rightrightarrows}} C \xrightarrow{h} D$$

gilt $h \circ (g + \tilde{g}) \circ f = h \circ g \circ f + h \circ \tilde{g} \circ f$ in $\mathrm{Mor}_{\mathfrak{A}}(A, D)$.

(*iii*) Es existiert ein Nullobjekt $0 \in \mathfrak{A}$.

(*iv*) Für alle Objekte $A, B \in \mathfrak{A}$ existieren das Produkt $A \times B$ und das Koprodukt $A \coprod B$.

Bemerkung 6.4. *In additiven Kategorien ist der Nullhomomorphismus das neutrale Element in den Gruppen* $\mathrm{Mor}_{\mathfrak{A}}(A, B)$.

Definition 6.5. Eine additive Kategorie $\mathfrak{A}$ heißt **abelsche Kategorie**, die die folgenden Eigenschaften erfüllt.

(*i*) Für alle Morphismen existieren Kerne und Kokerne.

(*ii*) Zu je zwei Objekten $X_1, X_2 \in \mathfrak{A}$ existiert ein Objekt **direkte Summe** $X_1 \oplus X_2$ zusammen mit Morphismen

$$p_i : X_1 \oplus X_2 \longrightarrow X_i$$
$$q_i : X_i \longrightarrow X_1 \oplus X_2,$$

so dass $p_i \circ q_i = \mathrm{id}_{X_i}$ und $q_1 \circ p_1 + q_2 \circ p_2 = \mathrm{id}_{X_1 \oplus X_2}$ gilt.

(*iii*) Jeder Monomorphismus ist ein Kern und jeder Epimorphismus ist ein Kokern.

Definition 6.6. Eine Kategorie $\mathfrak{A}$ heißt **Tensorkategorie**, falls ein bis auf eindeutige Isomorphie eindeutig bestimmtes (Eins-) Objekt $I \in \mathfrak{A}$ und ein Funktor $\otimes : \mathfrak{A} \times \mathfrak{A} \longrightarrow \mathfrak{A}$ mit den folgenden Eigenschaften existiert, wobei A, B, C, D beliebige Objekte aus $\mathfrak{A}$ darstellen.

(*i*) Es existiert ein natürlicher Isomorphismus $\alpha_{A,B,C} : (A \otimes B) \otimes C \longrightarrow A \otimes (B \otimes C)$.

(*ii*) Es existieren zwei natürliche Isomorphismen $\lambda_A : I \otimes A \longrightarrow A$ und $\rho_A : A \otimes I \longrightarrow A$.

(*iii*) Die beiden folgenden Diagramme sollen für alle Objekte $A, B, C, D \in \mathfrak{A}$ kommutieren.

$$\begin{array}{ccccc}
((A \otimes B) \otimes C) \otimes D & \xrightarrow{\alpha_{A,B,C} \otimes D} & (A \otimes (B \otimes C)) \otimes D & \xrightarrow{\alpha_{A,B \otimes C,D}} & A \otimes ((B \otimes C) \otimes D) \\
\downarrow{\scriptstyle \alpha_{A \otimes B,C,D}} & & & & \downarrow{\scriptstyle A \otimes \alpha_{B,C,D}} \\
(A \otimes B) \otimes (C \otimes D) & & \xrightarrow[\alpha_{A,B,C \otimes D}]{} & & A \otimes (B \otimes (C \otimes D))
\end{array}$$

Dieses Diagramm stellt eine allgemeinere Assoziativität sicher, während das folgende Diagramm eine Art Kürzungsregel für das Einsobjekt darstellt.

$$\begin{array}{ccc}
(A \otimes I) \otimes B & \xrightarrow{\alpha_{A,I,B}} & A \otimes (I \otimes B) \\
& {\scriptstyle \rho_A \otimes B} \searrow \quad \swarrow {\scriptstyle A \otimes \lambda_B} & \\
& A \otimes B &
\end{array}$$

Definition 6.7. Es sei R ein kommutativer Ring mit 1. Die Menge

$$\mathrm{Spek}(R) := \{ P \trianglelefteq R \,|\, P \text{ ist Primideal } \}$$

der Primideale von R heißt das **Spektrum** von R.

Wir benötigen für den Hauptsatz über Tannaka-Kategorien den Begriff des affinen Schemas. Wir geben dabei der Einfachheit halber nicht die allgemeine Definition über die Strukturgarbe sondern lediglich die folgende etwas vereinfachte Version an.

Definition 6.8. Es sei K ein Körper und A eine K-Algebra. Das Paar $(\mathrm{Spek}(A), A)$ heißt **affines Schema** über K.
Ein Morphismus $\psi = (f, \varphi)$ von zwei affinen Schemata $(\mathrm{Spek}(A), A)$ und $(\mathrm{Spek}(B), B)$ besteht aus einem K-Algebra-Homomorphismus

$$\varphi : A \longrightarrow B$$

und der durch φ induzierten Abbildung

$$\begin{array}{rccc}
f: & \mathrm{Spek}(B) & \longrightarrow & \mathrm{Spek}(A) \\
& P & \longmapsto & \varphi^{-1}(P)
\end{array} .$$

Definition 6.9. Es sei K ein Körper und A eine K-Algebra. Ein affines K-Schema $G := (\mathrm{Spek}(A), A)$ mit einer Gruppenstruktur heißt **affines Gruppenschema** über K. Die Gruppenstruktur wird durch die Existenz von Morphismen $m : G \times_K G \longrightarrow G$, $i : G \longrightarrow G$

und $e : (\mathrm{Spek}(K), K) \longrightarrow G$ und die Kommutativität der folgenden Diagramme induziert:

$$\begin{array}{ccc} G \times_K G \times_K G & \xrightarrow{m \times \mathrm{id}_G} & G \times_K G \\ {\scriptstyle \mathrm{id}_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_K G & \xrightarrow[m]{} & G \end{array} \qquad \text{(Assoziativität)} \quad .$$

$$\begin{array}{ccc} G & \xrightarrow{p \times \mathrm{id}_G} & G \times_K G \\ {\scriptstyle \mathrm{id}_G \times p}\downarrow & \searrow^{\mathrm{id}_G} & \downarrow{\scriptstyle m} \\ G \times_K & \xrightarrow[m]{} & G \end{array} \qquad \text{(neutrales Element)}$$

$$\begin{array}{ccc} G & \xrightarrow{i \times \mathrm{id}_G} & G \times_K G \\ {\scriptstyle \mathrm{id}_G \times i}\downarrow & \searrow^{p} & \downarrow{\scriptstyle m} \\ G \times_K G & \xrightarrow[m]{} & G \end{array} \qquad \text{(inverses Element)}$$

Dabei ist $p : G \longrightarrow G$ definiert durch $p = e \circ \kappa$, wobei $\kappa : G \longrightarrow (\mathrm{Spek}(K), K)$ der durch die K-Algebra Inklusion $K \hookrightarrow A$ induzierte Morphismus ist.

Der duale Begriff zum affinen Schema $(\mathrm{Spek}(A), A)$ ist die K-Algebra, also definieren wir nun den dualen Begriff zum Gruppenschema $G := (\mathrm{Spek}(A), A)$.

Definition 6.10. Es sei K ein Körper. Eine kommutative K-Algebra A heißt **kommutative Hopf-Algebra**, falls K-Algebra-Homomorphismen $\Delta : A \longrightarrow A \otimes_K A$ (Komultiplikation), $\iota : A \longrightarrow A$ (Koinverse) und $\epsilon : A \longrightarrow K$ (Augmentation) existieren, durch welche die folgenden Diagramme kommutieren:

$$\begin{array}{ccc} A \otimes_K A \otimes_K A & \xleftarrow{\Delta \otimes \mathrm{id}_A} & A \otimes_K A \\ {\scriptstyle \mathrm{id}_A \otimes \Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ A \otimes_K A & \xleftarrow[\Delta]{} & A \end{array} \qquad \text{(Koassoziativität)} \; .$$

$$\begin{array}{ccc} A & \xleftarrow{p^* \otimes \mathrm{id}_A} & A \otimes_K A \\ {\scriptstyle \mathrm{id}_A \otimes p^*}\uparrow & \nwarrow^{\mathrm{id}_A} & \uparrow{\scriptstyle \Delta} \\ A \otimes_K A & \xleftarrow[\Delta]{} & A \end{array} \qquad \text{(Augmentation)}$$

$$\begin{array}{ccc} A & \xleftarrow{\iota \otimes \mathrm{id}_A} & A \otimes_K A \\ {\scriptstyle \mathrm{id}_A \otimes \iota}\uparrow & \nwarrow^{p^*} & \uparrow{\scriptstyle \Delta} \\ A \otimes_K A & \xleftarrow[\Delta]{} & A \end{array} \qquad \text{(Koinverse)}$$

Definition 6.11. Es sei K ein Körper, A eine K-Algebra und $G = (\mathrm{Spek}(A), A)$ ein affines Gruppenschema. Ein Paar (V, τ) bestehend aus einem K-Vektorraum V und einer K-linearen Abbildung $\tau : V \longrightarrow A \otimes_K V$ heißt eine **Darstellung** bzw. ein **G-Modul**, falls gelten:

(i) Die Abbildung

$$V \xrightarrow{\tau} A \otimes V \xrightarrow{\epsilon \otimes \mathrm{id}_V} K \otimes V \xrightarrow[\lambda \otimes v \mapsto \lambda v]{} V$$

ist die Identität.

(ii) Das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} A \otimes_K A \otimes_K V & & \xleftarrow{\Delta \otimes \mathrm{id}_V} & & A \otimes_K V \\ {\scriptstyle \mathrm{id}_A \otimes \tau}\uparrow & & & & \uparrow{\scriptstyle \tau} \\ A \otimes_K V & & \xleftarrow[\tau]{} & & A \end{array} .$$

Ein Morphismus $f : (V, \tau_1) \longrightarrow (W, \tau_2)$ zwischen zwei Darstellungen ist eine K-lineare Abbildung mit $\tau_2 \circ f = f \circ \tau_1$.

Definition 6.12. Es sei K ein Körper und G ein affines Gruppenschema über K. Alle endlichdimensionalen Darstellungen von G bilden eine Kategorie, die wir mit $\underline{\mathrm{Repr}}_G$ bezeichnen.

Man sieht direkt, dass $\underline{\mathrm{Repr}}_G$ viele Eigenschaften von $\underline{\mathrm{Vek}}_K$ erbt, beispielsweise ist $\underline{\mathrm{Repr}}_G$ eine abelsche Tensorkategorie mit dem durch $(V, \tau_1) \otimes (W, \tau_2) := (V \otimes W, \tau_1 \otimes \tau_2)$ definierten Tensorprodukt.
Wir bezeichnen ab sofort mit $\underline{\mathrm{Alg}}_K$ die Kategorie der K-Algebren und mit $\underline{\mathrm{Grp}}_K$ die Kategorie der affinen Gruppenschemata über K.

Definition 6.13. Es sei $G = (\mathrm{Spek}(A), A)$ ein affines Gruppenschema über einem Körper K. Dann ist

$$FG : \underline{\mathrm{Alg}}_K \longrightarrow \underline{\mathrm{Grp}}_K$$

ein Funktor. Dieser wird folgendermaßen definiert:
Für eine K-Algebra R ist

$$FG(R) := G(R)$$

die Menge der K-Algebra-Homomorphismen $\varphi : A \longrightarrow R$. Diese Menge erhält für zwei K-Algebra-Homomorphismen φ und ψ eine Gruppenstruktur durch

$$A \xrightarrow{\Delta} A \otimes_K A \xrightarrow{\varphi \otimes \psi} R \otimes_K R \xrightarrow{m} R ,$$

wobei die letzte Abbildung definiert ist durch

$$\begin{array}{rccc} m : & R \otimes_K R & \longrightarrow & R \\ & r_1 \otimes r_2 & \longmapsto & r_1 \cdot r_2 \end{array} .$$

Satz 6.14. *Es sei G ein affines Gruppenschema. Durch den folgenden Vergiss-Funktor*

$$\begin{array}{rccc} \omega: & \underline{\mathrm{Repr}}_G & \longrightarrow & \underline{\mathrm{Vek}}_K \\ & (V,\rho) & \longmapsto & V \end{array}$$

erhalten wir einen Funktor

$$\underline{\mathrm{Aut}}^{\otimes}(\omega) : \underline{\mathrm{Repr}}_G \longrightarrow \underline{\mathrm{Grp}}_K$$

folgendermaßen: Für eine K-Algebra R ist ein Element $\sigma \in G'(R) := \underline{\mathrm{Aut}}^{\otimes}(\omega)(R)$ durch eine Kollektion von Elementen $\{\sigma(X)\}_{X \in \underline{\mathrm{Repr}}_G}$ gegeben. Dabei ist jedes $\sigma(X)$ ein R-linearer Automorphismus von $R \otimes \omega(X)$ mit den folgenden Eigenschaften:

(i) $\sigma(1) = \mathrm{id}_{R\otimes\omega(1)} = \mathrm{id}_R$.

(ii) *Für jeden R-linearen Morphismus $f : X \longrightarrow Y$ kommutiert das folgende Diagramm*

$$\begin{array}{ccc} R \otimes_K \omega(X) & \xrightarrow{\sigma(X)} & R \otimes_K \omega(X) \\ {\scriptstyle \mathrm{id}_R \otimes \omega(f)}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_R \otimes \omega(f)} \\ R \otimes_K \omega(Y) & \xrightarrow[\sigma(Y)]{} & R \otimes_K \omega(Y) \end{array} .$$

(iii) $\sigma(X \otimes Y) = \sigma(X) \otimes \sigma(Y)$.

Satz 6.15. *(Tannaka)*
Es sei $G = (\mathrm{Spek}(A), A)$ ein affines Gruppenschema über einem Körper K und ω der oben definierte Funktor. Dann existiert ein Isomorphismus von Funktoren $FG \to \underline{\mathrm{Aut}}^{\otimes}(\omega)$.

Für einen ausführlichen Beweis dieses Satzes sei an dieser Stelle auf Appendix B in [vdPS03] verwiesen.

Definition 6.16. Es sei K ein Körper und $\mathfrak{C}$ eine Tensorkategorie. Diese heißt **neutrale Tannaka-Kategorie** über K, falls gelten:

(*i*) Es existieren interne $\underline{\mathrm{Hom}}$, d.h. für je zwei Objekte $X, Y \in \mathfrak{C}$ existiert ein $\underline{\mathrm{Hom}}(X,Y)$, so dass die beiden Funktoren

$$T \to \mathrm{Hom}(T \otimes X, Y) \text{ und } T \to \mathrm{Hom}(T, \underline{\mathrm{Hom}}(X,Y))$$

kanonisch isomorph sind.

(*ii*) Für $\underline{\mathrm{Hom}}(X,1) =: X^*$ ist der kanonische Morphismus $X \to (X^*)^*$ ein Isomorphismus.

(*iii*) Der kanonische Morphismus

$$\underline{\mathrm{Hom}}(X_1,Y_1) \otimes \underline{\mathrm{Hom}}(X_2,Y_2) \to \underline{\mathrm{Hom}}(X_1 \otimes X_2, Y_1 \otimes Y_2)$$

ist ein Isomorphismus.

(*iv*) $\mathfrak{C}$ ist eine abelsche Kategorie.

(*v*) Es gibt einen Isomorphimus zwischen End(1) und K.

(*vi*) Es ist ein K-linearer, exakter, treuer Funktor, der mit dem Tensorprodukt verträglich ist (ein sogenannter **Faserfunktor**) $\omega : \mathfrak{C} \longrightarrow \underline{\mathrm{Vek}}_K$ gegeben.

Satz 6.17. *(Tannaka)*
Eine neutrale Tannaka-Kategorie $\mathfrak{C}$ über einem Körper K mit Faserfunktor $\omega : \mathfrak{C} \longrightarrow \underline{\mathrm{Vek}}_K$ ist kanonisch isomorph zur Kategorie $\underline{\mathrm{Repr}}_G$, wobei G den Funktor $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ darstellt.

6.2 Anwendung auf Frobenius-Moduln

Satz 6.18. *Es sei R ein relativer Frobenius-Integritätsbereich. Die Kategorie der Frobenius-Moduln über R mit Faserfunktor gegeben durch einen PV-Ring E bildet eine neutrale Tannaka-Kategorie.*

Ein Beweis dieses Satzes findet sich beispielsweise in [Pap08, Theorem 3.3.15]. Die Kategorie der relativen Frobenius-Moduln mit Endomorphimus Φ ist darüber hinaus als Tannaka-Kategorie äquivalent zur Kategorie der Differential-Frobenius-Moduln mit einer iterativen Derivation ∇, falls die jeweiligen Konstanten übereinstimmen. Dies liefert insbesondere den in [Mat03] bewiesenen Zusammenhang zwischen den jeweiligen Galoisgruppen-Schemata

$$\underline{\mathrm{Gal}}^{\nabla}(R/F) = \mathrm{Spek}(C_S) \times_{S^{\phi}} \underline{\mathrm{Gal}}^{\Phi}(R/F),$$

wobei F den Quotientenkörper eines relativen Frobenius-Rings mit PV-Ring R und C_S die Differential-Konstanten bezeichnet. Damit sind diese bis auf einen C_S-Basiswechsel identisch. Daher erhalten wir durch die Berechnung der Differenzen-Galoisgruppe des Frobenius-Moduls die Differential-Galoisgruppe des entsprechenden iterativen Frobenius-Moduls, was unser ursprüngliches Ziel war.
Wir wollen nun eine Unterkategorie $\{\{M\}\}$ in der Kategorie der Frobenius-Moduln über einem relativen Frobenius-Körper F betrachten. Für einen fest gewählten Frobenius-Modul M über F bezeichnen wir für ganze Zahlen $m, n > 0$ den Modul

$$M_n^m := \underbrace{M \otimes \cdots \otimes M}_{n\text{-mal}} \otimes \underbrace{M^* \otimes \cdots \otimes M^*}_{m\text{-mal}},$$

wobei M^* der zu M duale Module ist. Für einen Modul N nennen wir einen Frobenius-Modul $\tilde{N}$ einen Submodul, falls er von der Form $\tilde{N} = N_1/N_2$ mit $N_2 \subset N_1 \subset N$ ist. Die Objekte der Kategorie $\{\{M\}\}$ sind definiert als Subquotienten von direkten Summen von Moduln der Form M_n^m. Hom hat dabei dieselbe Bedeutung wie in der ursprünglichen Kategorie der Frobenius-Moduln. Man sagt $\{\{M\}\}$ ist eine volle Unterkategorie von der Kategorie der relativen Frobenius-Moduln. Außerdem ist $\{\{M\}\}$ die kleinste Unterkategorie, die M enthält und unter allen Lineare-Algebra-Konstruktionen (z.B. direkte Summen, Tensorprodukte, usw.) abgeschlossen ist.

Satz 6.19. *Für einen Frobenius-Moduls M über einem relativen Frobenius-Integritätsbereich R mit PV-Ring E ist die oben definierte Kategorie $\{\{M\}\}$ eine neutrale Tannaka-Kategorie und damit äquivalent zu $\underline{\mathrm{Repr}}_G$, wobei G das Galoisgruppen-Schema des Frobenius-Moduls M bezeichnet.*

Dieser Satz liefert den Ansatz für die allgemeine Berechenbarkeit der Galoisgruppe eines relativen Frobenius-Moduls. Mit Hilfe der Konstruktionen aus der Linearen Algebra konnten wir in dieser Arbeit schrittweise die Galoisgruppe für Gleichungen bzw. Moduln der Ordnung 1 und 2 bestimmen. Theoretisch ist dies durch obigen Satz auch für Differenzengleichungen n-ten Grades bzw. die zugehörigen Frobenius-Moduln möglich. Sei also M nun ein solcher Frobenius-Modul mit PV-Körper E, Lösungsvektorraum $V := \mathrm{Sol}_E^{\Phi}(M)$, d.h. es gilt $n = \dim_{F^\phi}(V)$ und Galoisgruppe G. Nach Satz 1.23 stehen die Untermoduln von M in einer 1-1 Korrespondenz mit den G-invarianten Unterräumen von V. Diese Aussage lässt sich auch auf Moduln der Form $\bigoplus_{i=1}^{m} M_{b_i}^{a_i}$ aus der Kategorie $\{\{M\}\}$ und den Vektorraum $\bigoplus_{i=1}^{m} V_{b_i}^{a_i}$ übertragen. Wir definieren nun für einen Index $d \geq 1$ den Modul $M(d) := \bigoplus_{a\leq d, b\leq d} M_b^a$. Die Kenntnis der Untermoduln aller $M(d)$ liefert die Galoisgruppe, da man dann auch alle G-invarianten Unterräume von V kennt. Denn kennt man alle Untermoduln von $M(d)$, liefert dies eine algebraische Gruppe $G(d) \leq \mathrm{GL}(V)$ mit $G \subset G(d)$ für alle d. Nach Konstruktion gilt außerdem $G(d+1) \subset G(d)$. Um nun daraus einen Algorithmus zu entwickeln, ist ein Entscheidungskriterium notwendig, ob die Gruppe $G(d)$ und die Galoisgruppe G übereinstimmen. Dazu benötigt man eine von G unabhängige Schranke $B(n)$ für d, so dass die Folge $G(d)$ für $d \geq B(n)$ stationär wird. In diesem Fall gilt dann $G = G(d)$. Diese Schranke würde sicherstellen, dass der Algorithmus in endlicher Laufzeit terminiert. Beides lieferte Hrushovski mit seinem Algorithmus für Differentialgleichungen in Charakteristik 0 in [Hru02]. Einige der benötigten Schranken im Falle positiver Charakteristik konnten wir im Rahmen dieser Arbeit finden, z.B. Satz 1.36 oder Satz 5.6. Es liegt also nahe zu vermuten, dass sich der Hrushovski-Algorithmus auch auf Frobenius-Differenzengleichungen in positiver Charakteristik verallgemeinern lässt.

Literaturverzeichnis

[AM05] K. Amano and A. Masuoka. Picard-Vessiot extensions of artinian simple module algebras. *Journal of Algebra*, 285:743–767, 2005.

[BD79] F. Baldassarri and B. Dwork. On Second Order Linear Differential Equations with Algebraic Solutions. *American Journal of Mathematics*, 101:42–76, 1979.

[Bek94] E. Beke. Die Irreducibilität der homogenen linearen Differential-Gleichungen. *Mathematische Annalen*, 45:278–300, 1894.

[BF66] R. Brauer and W. Feit. An Analogue of Jordan's Theorem in characteristic p. *Annals of Mathematics*, 84(2):381–399, 1966.

[Bli17] H. F. Blichtfeldt. Finite Collineation Groups. *University of Chicago Press*, 1917.

[CR62] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* John Wiley and Sons, New York, 1962.

[DM82] P. Deligne and J. S. Milne. Tannakian Categories. In *Hodge Cycles, Motives and Shimura Varieties*, pages 101–229. Springer-Verlag Berlin Heidelberg New York, 1982.

[EP05] A. J. Engler and A. Prestel. *Valued Fields.* Springer, 2005.

[Gos99] D. Goss. *Basic Structures of Function Field Arithmetic.* Springer, 1999.

[GZ03] M. Giesbrecht and Y. Zhang. Factoring and Decomposing Ore Polynomials over $\mathbb{F}_q(t)$. *ACM International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 127–134, 2003.

[Hen96] P. A. Hendriks. An Algorithm determining the difference Galois group for second order linear difference equations. *To Appear in Journal of Symbolic Computation*, 1996.

[Hru02] E. Hrushovski. Computing the Galois Group of a Linear Differential Equation. In T. Crespo and Z. Hajto, editors, *Differential Galois Theory*, volume 58, pages 97–138. Banach Center Publications, 2002.

[Kol48] E.R. Kolchin. Algebraic Matrix Groups and the Picard-Vessiot Theory of homogeneous linear ordinaray differential equations. *Annals of Mathematics*, 49:1–42, 1948.

[Kov72] J. Kovacic. An Eisenstein criterium for noncommutative polynomials. *Proc. Amer. Math. Soc.*, 34, 1972.

[Kov86] J. Kovacic. An Algorithm for solving second order linear homogeneous differential equations. *Journal of Symbolic Computation*, 2, 1986.

[Lan71] S. Mac Lane. *Categories for the Working Mathematician*. Springer-Verlag, 1971.

[Mat01] B. H. Matzat. Differential Galois Theory in Positive Characteristic. IWR-Preprint 2001.

[Mat03] B. H. Matzat. Frobenius Modules and Galois Groups. In K. Miyake et al., editor, *Galois theory and modular forms*, pages 233–268. Kluwer, Dodrecht, 2003.

[Mat09a] B. H. Matzat. Frobenius Modules and Galois Representations. *Annales de l'institut Fourier*, 59(7):2805–2818, 2009.

[Mat09b] B. H. Matzat. From Frobenius Structures to Differential Equations. *DART II Proceedings, World Scientific Publisher*, 2009.

[Mey76] K. Meyberg. *Algebra*. Carl Hasner Verlag München Wien, 1976.

[Ore33] O. Ore. Theory of Non-Commutative Polynomials. *Annals of Mathematics*, 34(22):480–508, 1933.

[Pap08] M.A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Innventiones mathematicae*, 171:123–174, 2008.

[Spr98] T. A. Springer. *Linear Algebraic Groups*. Birkhäuser, second edition, 1998.

[Sti09] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, second edition, 2009.

[SU93] M. F. Singer and F. Ulmer. Galois Groups of Second and Third Order Linear Differential Equations. *Journal of Symbolic Computation*, 16:9–36, 1993.

[Tit68] J. Tits. *Lectures on Algebraic Groups*. Yale University, 1968. Lecture Notes.

[vdPM97] M. van der Put and M.Singer. *Galois Theory of Difference Equations*. Springer, 1997.

[vdPS03] M. van der Put and M. Singer. *Galois Theory of Linear Differential Equations*. Springer, 2003.

[Weh73] B. A. F. Wehrfritz. *Infinite Linear Groups*. Springer-Verlag, 1973.

Danksagung

Mein besonderer Dank geht an meinen Mentor Prof. Dr. B. Heinrich Matzat, der mir die Möglichkeit gab die Diplomarbeit über dieses interessante Thema zu verfassen. Er hatte stets ein offenes Ohr, wenn Fragen oder Probleme auftauchten. Für seine Betreuung, Geduld, Motivation und Unterstützung, besonders während der Entstehung dieser Diplomarbeit, bedanke ich mich ganz herzlich. Sein Stil und seine Vorlesungen, die ich seit Beginn des Studiums besuchte, hatten nachhaltigen Einfluss auf meine mathematische Enwicklung.

Weiterhin bedanke ich mich bei Dr. Andreas Maurischat für viele hilfreiche mathematische Diskussionen, geduldige Gespräche und das Korrektur-Lesen meiner Arbeit.

Ein weiteres Dankeschön geht an meinen guten Freund Felipe Garcia Lopez für zahllose mathematische Gespräche während des gesamten Studiums, aber noch mehr für viel Spaß außerhalb der Mathematik, der mir die nötige Ablenkung brachte.

Zum Schluss möchte ich mich noch bei meinen Eltern für ihren ständigen Zuspruch und ihre bedingungslose Unterstützung, nicht nur während des Studiums, bedanken. Der familiäre Rückhalt und ihr Glauben an mich haben mir auch in schwierigen Situationen geholfen, den richtigen Weg einzuschlagen.

Erklärung

Hiermit versichere ich, dass ich meine Arbeit selbstständig unter Anleitung verfasst habe, dass ich keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, und dass ich alle Stellen, die dem Wortlaut oder dem Sinne nach anderen Werken entlehnt sind, durch die Angabe der Quellen als Entlehnung kenntlich gemacht habe.

Heidelberg, den 16. Januar 2011