Math. Ann. 272, 549–565 (1985)

Mathematische Annalen

Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$

G. Malle und B. H. Matzat

Mathematisches Institut II, Universität Karlsruhe (TH), Englerstraße 2, D-7500 Karlsruhe 1, Bundesrepublik Deutschland

Einleitung

Lange Zeit war es ungewiß, ob es Polynome mit rationalen Koeffizienten gibt, deren Nullstellen über $\mathbb{Q}$ Körper mit den Galoisgruppen $\mathrm{PSL}_2(\mathbb{F}_p)$, $p \geqq 7$, erzeugen. Ein erstes solches Polynom für $p=7$ wurde 1968 in Karlsruhe mit dem Computer gefunden, nämlich $f(X)=X^7-7X+3$ [18]. Ein weiteres solches trinomisches Polynom wurde später in [4] angegeben.

Mit Hilfe der Shimuraschen Theorie der kanonischen Systeme von Modellen konnte Shih 1974 in [16] zeigen, daß die Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$, für die p kein quadratischer Rest modulo 2, 3 oder 7 ist, als Galoisgruppen über $\mathbb{Q}(t)$ und $\mathbb{Q}$ vorkommen. Der Beweis ist allerdings nicht konstruktiv und gestattet daher nicht die Berechnung von zugehörigen Polynomen. Auf der Tagung Algebraische Zahlentheorie in Oberwolfach 1977 hat der zweite Autor einen konstruktiven Beweis für die Existenz von Galoiserweiterungen mit den Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ mit $p \not\equiv \pm 1 \bmod(24)$ vorgeführt und ein Polynom achten Grades mit der Gruppe $\mathrm{PSL}_2(\mathbb{F}_7)$ über $\mathbb{Q}(t)$ vorgestellt, das dann nach dem Hilbertschen Irreduzibilitätssatz eine einparametrige Schar von Polynomen mit der Gruppe $\mathrm{PSL}_2(\mathbb{F}_7)$ über $\mathbb{Q}$ liefert. Dieses Resultat und die dazugehörigen Überlegungen bildeten den Grundstock zu der Arbeit [11]. Später fand LaMacchia eine zweiparametrige Schar von Polynomen vom Grad 7 mit der Gruppe $\mathrm{PSL}_2(\mathbb{F}_7)$ über $\mathbb{Q}$, die das Trinkssche Polynom als Spezialisierung besitzt [6].

In dieser Arbeit werden weitere Realisierungen der Gruppen $\mathrm{PGL}_2(\mathbb{F}_p)$ und $\mathrm{PSL}_2(\mathbb{F}_p)$ für $p \not\equiv \pm 1 \bmod(24)$ als Galoisgruppen über $\mathbb{Q}(t)$ vorgestellt, die mit den konstruktiven Methoden aus [11] gewonnen wurden. Diese ermöglichen nun auch die Berechnung von Polynomen mit den Gruppen $\mathrm{PSL}_2(\mathbb{F}_7)$ vom Grad 7, $\mathrm{PSL}_2(\mathbb{F}_{11})$ vom Grad 11 und $\mathrm{PSL}_2(\mathbb{F}_{13})$ vom Grad 14 jeweils über $\mathbb{Q}(t)$. Das für die $\mathrm{PSL}_2(\mathbb{F}_7)$ konstruierte Polynom stellt sich als Spezialisierung des von LaMacchia gefundenen Polynoms heraus. Polynome mit den Galoisgruppen $\mathrm{PSL}_2(\mathbb{F}_{11})$ und $\mathrm{PSL}_2(\mathbb{F}_{13})$ über $\mathbb{Q}$ waren bisher noch nicht gefunden worden. In der klassischen Literatur existieren allerdings Polynome mit den Gruppen $\mathrm{PSL}_2(\mathbb{F}_{11})$ über $\mathbb{Q}(\sqrt{-11}, t)$ und $\mathrm{PSL}_2(\mathbb{F}_{13})$ über $\mathbb{Q}(\sqrt{13}, t)$ (s. [5, II, 5., Abschn. 3,

(6)] bzw. [5, II, 5., Abschn. 2, (33)]); weiter ist in [7] ein Polynom mit der Gruppe $\mathrm{PSL}_2(\mathbb{F}_{11})$ über $\mathbb{Q}(\sqrt{5}, t)$ vorgestellt worden.

1. Existenzsätze

Es sei G eine endliche Gruppe der Ordnung $|G| = n$. Die Menge der s-Tupel $(\sigma_1, \ldots, \sigma_s)$ von Elementen aus G, für die σ_j Element einer festen Konjugiertenklasse C_j von G ist, nennt man eine *Klassenstruktur von G:*

$$\mathfrak{C} = (C_1, \ldots, C_s) := \{(\sigma_1, \ldots, \sigma_s) | \sigma_j \in C_j\}.$$

Die Konjugiertenklassen der v-ten Potenzen der Elemente von C_j bezeichnen wir mit C_j^v und den Restklassenring $\mathbb{Z}/n\mathbb{Z}$ mit Z_n, dann heißt

$$\mathfrak{C}^* = (C_1, \ldots, C_s)^* := \bigcup_{v \in Z_n^\times} (C_1^v, \ldots, C_s^v)$$

die von $\mathfrak{C}$ aufgespannte (feine) *Verzweigungsstruktur von G.*

Auf der *Menge der $\mathfrak{C}$-Erzeugendensysteme von G*

$$\Sigma(\mathfrak{C}) := \{(\sigma_1, \ldots, \sigma_s) \in \mathfrak{C} | \langle \sigma_1, \ldots, \sigma_s \rangle = G, \sigma_1, \ldots \sigma_s = 1\}$$

operiert G durch Konjugation

$$G \ni \tau : \Sigma(\mathfrak{C}) \to \Sigma(\mathfrak{C}), (\sigma_1, \ldots, \sigma_s) \mapsto (\sigma_1^\tau, \ldots, \sigma_s^\tau).$$

Die Anzahl der hierdurch entstehenden Bahnen auf $\Sigma(\mathfrak{C})$ heiße *Klassenzahl von $\mathfrak{C}$-Erzeugendensystemen von G modulo* $\mathrm{Inn}(G)$ und werde mit

$$l^i(\mathfrak{C}) := |\Sigma(\mathfrak{C})/\mathrm{Inn}(G)|$$

bezeichnet. Analog seien für die von $\mathfrak{C}$ aufgespannte Verzweigungsstruktur $\mathfrak{C}^*$ die Menge $\Sigma(\mathfrak{C}^*)$ und die Klassenzahl $l^i(\mathfrak{C}^*)$ gebildet. Mit diesen Bezeichnungen gilt:

Satz A. *Es seien G eine endliche Gruppe mit trivialem Zentrum und $\mathfrak{C}^*$ eine Verzweigungsstruktur von G mit $l^i(\mathfrak{C}^*) = 1$. Dann gibt es eine reguläre Körpererweiterung $N/\mathbb{Q}(t)$ mit einer zu G isomorphen Galoisgruppe und der Verzweigungsstruktur $\mathfrak{C}^*$.*

Dabei besitzt $N/\mathbb{Q}(t)$ die Verzweigungsstruktur $\mathfrak{C}^*$, wenn in der durch Konstantenerweiterung mit einer algebraisch abgeschlossenen Hülle $\bar{\mathbb{Q}}$ von $\mathbb{Q}$ aus $N/\mathbb{Q}(t)$ entstehenden Galoiserweiterung $\bar{\mathbb{Q}}N/\bar{\mathbb{Q}}(t)$ mit der Galoisgruppe G genau s Primdivisoren $\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_s$ von $\bar{\mathbb{Q}}(t)/\bar{\mathbb{Q}}$ verzweigt sind und es Erzeugende σ_j von Trägheitsgruppen gewisser Primteiler $\bar{\mathfrak{P}}_j$ von $\bar{\mathfrak{p}}_j$ in $\bar{N} := \bar{\mathbb{Q}}N$ über $\bar{\mathbb{Q}}$ gibt mit $(\sigma_1, \ldots, \sigma_s) \in \Sigma(\mathfrak{C}^*)$. Dieser Satz ist als Spezialfall in Satz 5.2 von [11] enthalten, siehe auch [12, Satz 1 mit Folgerung 1.b)].

Von jetzt an seien $\tilde{G} = \mathrm{PGL}_2(\mathbb{F}_p)$ und $G = \mathrm{PSL}_2(\mathbb{F}_p) < \tilde{G}$. In [11, Lemma 7.1] wurde gezeigt, daß die Gruppe $\tilde{G}$ für $p \not\equiv \pm 1 \bmod(24)$ Verzweigungsstrukturen $\tilde{\mathfrak{C}}^*$ besitzt mit $l^i(\tilde{\mathfrak{C}}^*) = 1$, nämlich $\tilde{\mathfrak{C}}_2^* = (\tilde{C}_2, \tilde{C}_4, C_p)^*$ im Falle $\left(\frac{2}{p}\right) = -1$ und

$\tilde{\mathfrak{C}}_3^* = (\tilde{C}_2, \tilde{C}_6, C_p)^*$ im Falle $\left(\frac{3}{p}\right) = -1$; dabei bedeuten C_n bzw. $\tilde{C}_n$ die Klasse der Elemente der Ordnung n in G bzw. in $\tilde{G}\backslash G$. Nach Satz A existieren dann Galoiserweiterungen $N/\mathbb{Q}(t)$ mit der Gruppe $\tilde{G}$ und der Verzweigungsstruktur $\tilde{\mathfrak{C}}_2^*$ bzw. $\tilde{\mathfrak{C}}_3^*$. Dabei ist der Fixkörper $K = N^G$ von G ein rationaler Funktionenkörper über $\mathbb{Q}$ (s. [11, Satz 7.3]), und N/K ist eine Galoiserweiterung mit der Gruppe G und der Verzweigungsstruktur $\mathfrak{C}_2^* = (C_2, C_p, C_p^w)$ im Falle $\left(\frac{2}{p}\right) = -1$ bzw. $\mathfrak{C}_3^* = (C_3, C_p, C_p^w)$ im Falle $\left(\frac{3}{p}\right) = -1$, wobei w eine Primitivwurzel modulo p bedeutet. (Für diese Verzweigungsstrukturen gelten dann $l^i(\mathfrak{C}_2^*) = l^i(\mathfrak{C}_3^*) = 2$, aber $\tilde{l}^i(\mathfrak{C}_2^*) = \tilde{l}^i(\mathfrak{C}_3^*) = 1$ im Sinne von [12, Satz 2 mit Folgerung 2] wegen $\mathrm{Aut}(\mathfrak{C}_2^*) = \mathrm{Aut}(\mathfrak{C}_3^*) = \langle(23)\rangle$.)

Alle übrigen dreigliedrigen Verzweigungsstrukturen $\mathfrak{C}^*$ von G mit $\tilde{l}^i(\mathfrak{C}^*) = 1$ erhält man, wie in [9] gezeigt wurde, auf die eben beschriebene Weise aus einer Verzweigungsstruktur $\tilde{\mathfrak{C}}^*$ von $\tilde{G}$, die der Menge

$$\tilde{\mathscr{C}} = \{(C_2, \tilde{C}_4, \tilde{C}_6)^*, (\tilde{C}_2, C_4, \tilde{C}_6)^*, (\tilde{C}_2, \tilde{C}_4, C_6)^*\}$$

angehört. Da $\tilde{G}$ je eine Klasse von Elementen der Ordnung 4 und 6 enthält, von denen für $p \not\equiv \pm 1 \bmod(24)$ mindestens eine nicht in G liegt, sowie je eine Klasse von Involutionen C_2 in G bzw. $\tilde{C}_2$ in $\tilde{G}\backslash G$, besitzt $\tilde{G}$ für $p \not\equiv \pm 1 \bmod(24)$ genau eine Verzweigungsstruktur $\tilde{\mathfrak{C}}^*$ in $\tilde{\mathscr{C}}$.

Lemma 1. *Es seien $p \geqq 5$ und $p \not\equiv \pm 1 \bmod(24)$. Dann gilt für die eindeutig bestimmte Verzweigungsstruktur $\tilde{\mathfrak{C}}^* \in \tilde{\mathscr{C}}$ der Gruppe $\tilde{G} = \mathrm{PGL}_2(\mathbb{F}_p)$*

$$l^i(\tilde{\mathfrak{C}}^*) = 1 .$$

Beweis. Zunächst stellt man fest, daß hier $\tilde{\mathfrak{C}}^* = \tilde{\mathfrak{C}}$ ist. Die Menge $\Sigma(\tilde{\mathfrak{C}})$ erhält man, indem man aus der Menge

$$\bar{\Sigma}(\tilde{\mathfrak{C}}) = \{(\sigma_1, \sigma_2, \sigma_3) \in \tilde{\mathfrak{C}} | \sigma_1\sigma_2\sigma_3 = \iota\}$$

die Erzeugendensysteme von $\tilde{G}$ heraussucht.

Im Fall $p \equiv 1 \bmod(6)$ stellen wir daher die Gruppe $\tilde{G}$ dar als Faktorgruppe von $H := \mathrm{GL}_2(\mathbb{F}_p)$ nach deren Zentrum und die Elemente σ_j als Kongruenzklassen nach $\mathbf{Z}(H)$:

$$\sigma_j = \begin{bmatrix} a_j & b_j \\ c_j & d_j \end{bmatrix} := \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \cdot \mathbf{Z}(H), \qquad j = 1, 2, 3 .$$

Wegen $p \equiv 1 \bmod(6)$ existiert in $\mathbb{F}_p$ eine sechste Einheitswurzel z. In der Klasse $[(\sigma_1, \sigma_2, \sigma_3)]$ von $(\sigma_1, \sigma_2, \sigma_3)$ in $\bar{\Sigma}(\tilde{\mathfrak{C}})/\mathrm{Inn}(G)$ gibt es also einen Repräsentanten mit $a_3 = 1$, $b_3 = c_3 = 0$ und $d_3 = z$. Wären nun $b_1 = 0$ oder $c_1 = 0$, so würden σ_1 und σ_3 nicht $\tilde{G}$ erzeugen. Deshalb ist $b_1 c_1 \neq 0$, woraus wegen $\sigma_1^2 = \iota$ folgt $d_1 = -a_1$. Damit sind

$$\sigma_2^{-1} = \sigma_3\sigma_1 = \begin{bmatrix} a_1 & b_1 \\ zc_1 & -za_1 \end{bmatrix}, \qquad \sigma_2^{-2} = \begin{bmatrix} a_1^2 + zb_1c_1 & (1-z)a_1b_1 \\ (z-z^2)a_1c_1 & z^2a_1^2 + zb_1c_1 \end{bmatrix}.$$

Weil σ_2 die Ordnung $o(\sigma_2)=4$ hat, sind $\sigma_2^{-2} \neq \iota$ und $a_1 \neq 0$. Also gilt wegen $o(\sigma_2^{-2})=2$ zunächst

$$(z^2+1)a_1^2+2zb_1c_1=0,$$

woraus wegen $z^2-z+1=0$ folgt $b_1=-\dfrac{a_1^2}{2c_1}$. Nach Konjugation mit $\begin{bmatrix} a_1 & 0 \\ 0 & c_1 \end{bmatrix} \in \mathbf{C}_{\tilde{G}}(\sigma_3)$ (Zentralisator von σ_3 in $\tilde{G}$) stellt man fest, daß es somit in $\bar{\Sigma}(\tilde{\mathbb{C}})/\mathrm{Inn}(G)$ höchstens eine Klasse von Erzeugendensystemen gibt, nämlich $[(\sigma_1,\sigma_2,\sigma_3)]$ mit

$$\sigma_1=\begin{bmatrix} 1 & -\frac{1}{2} \\ 1 & -1 \end{bmatrix}, \quad \sigma_2=\begin{bmatrix} z & -\frac{1}{2} \\ z & -1 \end{bmatrix}, \quad \sigma_3=\begin{bmatrix} 1 & 0 \\ 0 & z \end{bmatrix}.$$

Im Fall $p \equiv -1 \bmod(6)$ stellen wir $\tilde{G}$ dar als Faktorgruppe der zu $\mathrm{GL}_2(\mathbb{F}_p)$ isomorphen Gruppe

$$\tilde{H}=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q) \,\middle|\, q=p^2, c=b^p, d=a^p\right\}$$

nach dem Zentrum $\mathbf{Z}(\tilde{H})$ und die Elemente σ_j als Kongruenzklassen von $\tilde{H}$ nach $\mathbf{Z}(\tilde{H})$:

$$\sigma_j=\begin{bmatrix} a_j & b_j \\ b_j^p & a_j^p \end{bmatrix}=\begin{pmatrix} a_j & b_j \\ b_j^p & a_j^p \end{pmatrix} \cdot \mathbf{Z}(\tilde{H}).$$

$\mathbb{F}_q$ enthält eine sechste Einheitswurzel z, und es ist $z^p=z^{-1}$. In jeder Klasse $[(\sigma_1,\sigma_2,\sigma_3)] \in \bar{\Sigma}(\tilde{\mathbb{C}})/\mathrm{Inn}(G)$ gibt es also einen Repräsentanten $(\sigma_1,\sigma_2,\sigma_3)$ mit $a_3=z$ und $b_3=0$. Da σ_1 und σ_3 die Gruppe $\tilde{G}$ erzeugen sollen, ist $b_1 \neq 0$, woraus wegen $o(\sigma_1)=2$ folgt $a_1^p=-a_1$. Damit sind

$$\sigma_2^{-1}=\sigma_3\sigma_1=\begin{bmatrix} za_1 & zb_1 \\ z^{-1}b_1^p & -z^{-1}a_1 \end{bmatrix}, \quad \sigma_2^{-2}=\begin{bmatrix} z^2a_1^2+b_1^{p+1} & (z^2-1)a_1b_1 \\ (1-z^{-2})a_1b_1^p & z^{-2}a_1^2+b_1^{p+1} \end{bmatrix}.$$

Auf Grund von $o(\sigma_2)=4$ sind $a_1 \neq 0$ und die Spur von σ_2^{-2} gleich Null, wegen $(z^2+z^{-2})=-1$ ist also

$$a_1^2=2b_1^{p+1}.$$

Bezeichnet man eine feste Nullstelle des Polynoms $2Y^2-1$ in $\mathbb{F}_q$ mit y, so gilt

$$\sigma_1=\begin{bmatrix} 1 & \frac{b_1}{a_1} \\ \frac{a_1}{2b_1} & -1 \end{bmatrix}=\begin{bmatrix} 1 & \pm yb_1^{1-p} \\ \pm yb_1^{p-1} & -1 \end{bmatrix}.$$

Durch Konjugation mit

$$\begin{bmatrix} b_1^{-1} & 0 \\ 0 & b_1^{-p} \end{bmatrix} \in \mathbf{C}_{\tilde{G}}(\sigma_3) \quad \text{bzw.} \quad \begin{bmatrix} b_1^{-1}x & 0 \\ 0 & b_1^{-p}x^p \end{bmatrix} \in \mathbf{C}_{\tilde{G}}(\sigma_3),$$

wobei x eine primitive $2(p-1)$-te Einheitswurzel in $\mathbb{F}_q$ ist, ergibt sich, daß $\bar{\Sigma}(\tilde{\mathfrak{C}})/\mathrm{Inn}(G)$ auch im Fall $p \equiv -1 \bmod(6)$ höchstens eine Klasse von Erzeugendensystemen enthält, nämlich $[(\sigma_1, \sigma_2, \sigma_3)]$ mit

$$\sigma_1 = \begin{bmatrix} 1 & y \\ y & -1 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} z^{-1} & yz \\ yz^{-1} & -z \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} z & 0 \\ 0 & z^{-1} \end{bmatrix}.$$

Es bleibt zu zeigen, daß in beiden Fällen $(\sigma_1, \sigma_2, \sigma_3)$ ein Erzeugendensystem von G ist. Dazu fassen wir $\tilde{G}$ als Untergruppe von $\mathrm{PSL}_2(\mathbb{F}_q)$, $q = p^2$, auf. Für diese Gruppe hat Macbeath in [8] untersucht, welche Untergruppen von $(\sigma_1, \sigma_2, \sigma_3) \in \bar{\Sigma}(\tilde{\mathfrak{C}})$ erzeugt werden können. Offenbar ist $U = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ keine affine Gruppe, also ist $(\sigma_1, \sigma_2, \sigma_3)$ nach [8, Satz 2] kein singuläres Tripel. Weiter ist $(\sigma_1, \sigma_2, \sigma_3)$ nicht exzeptionell wegen $o(\sigma_1) = 2$, $o(\sigma_2) = 4$ und $o(\sigma_3) = 6$ [8, Abschn. 8]. Folglich ist U eine projektive Untergruppe von $\mathrm{PSL}_2(\mathbb{F}_q)$ nach [8, Satz 4]. Wegen $U \leqq \mathrm{PGL}_2(\mathbb{F}_p)$ und $U \neq \mathrm{PSL}_2(\mathbb{F}_p)$ für $p \not\equiv \pm 1 \bmod(24)$ ist $U = \mathrm{PGL}_2(\mathbb{F}_p)$. Hieraus ergibt sich schließlich $l^i(\tilde{\mathfrak{C}}) = l^i(\tilde{\mathfrak{C}}^*) = 1$. □

Aus diesem Lemma und Satz A ergibt sich nun:

Satz 1. *Für $p \not\equiv \pm 1 \bmod(24)$ lassen sich die Gruppen $\mathrm{PGL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}(u)$ realisieren. Genauer existieren Galoiserweiterungen über $\mathbb{Q}(u)$ mit zu $\mathrm{PGL}_2(\mathbb{F}_p)$ isomorphen Galoisgruppen und den Verzweigungsstrukturen*

$$\begin{aligned} &(C_2, \tilde{C}_4, \tilde{C}_6)^* \quad \text{für} \quad p \equiv \pm\ 5 \bmod(24), \\ &(\tilde{C}_2, C_4, \tilde{C}_6)^* \quad \text{für} \quad p \equiv \pm\ 7 \bmod(24), \\ &(\tilde{C}_2, \tilde{C}_4, C_6)^* \quad \text{für} \quad p \equiv \pm 11 \bmod(24). \end{aligned}$$

Ist $N/\mathbb{Q}(u)$ eine Galoiserweiterung mit der Gruppe $\tilde{G} \cong \mathrm{PGL}_2(\mathbb{F}_p)$ und ist K der Fixkörper der Untergruppe $G \cong \mathrm{PSL}_2(\mathbb{F}_p)$ von $\tilde{G}$, so ist $\bar{K}/\mathbb{Q}(u)$, $\bar{K} := \mathbb{Q}K$, eine zyklische Erweiterung mit höchstens drei verzweigten Primdivisoren. Folglich gilt für das Geschlecht $g(\bar{K}) = g(K) = 0$. Da die in $\bar{K}/\mathbb{Q}(u)$ verzweigten Primdivisoren auf Grund der verschiedenen Verzweigungsordnungen jeweils schon über $\mathbb{Q}(u)$ definiert sind, besitzt K Primdivisoren vom Grad 1, und $K/\mathbb{Q}$ ist ein rationaler Funktionenkörper: $K = \mathbb{Q}(t)$. Hieraus ergibt sich der erste Teil von

Satz 2. *Für $p \not\equiv \pm 1 \bmod(24)$ lassen sich die Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}(t)$ realisieren. Genauer existieren Galoiserweiterungen über $\mathbb{Q}(t)$ mit zu $\mathrm{PSL}_2(\mathbb{F}_p)$ isomorphen Galoisgruppen und den Verzweigungsstrukturen*

$$\begin{aligned} &(C_2, C_2, C_2, C_3)^* \quad \text{für} \quad p \equiv \pm\ 5 \bmod(24), \\ &(C_3, C_4, C_4)^* \quad \text{für} \quad p \equiv \pm\ 7 \bmod(24), \\ &(C_2, C_6, C_6)^* \quad \text{für} \quad p \equiv \pm 11 \bmod(24). \end{aligned}$$

Beweis. Es sind nur noch die Verzweigungsstrukturen von $\bar{N}/\mathbb{Q}(t)$ zu bestimmen. Da in $\mathbb{Q}(t)/\mathbb{Q}(u)$ genau diejenigen der drei in $\bar{N}/\mathbb{Q}(u)$ verzweigten Primdivisoren $\bar{\mathfrak{q}}_1$, $\bar{\mathfrak{q}}_2$, $\bar{\mathfrak{q}}_3$ unverzweigt sind, deren Primteiler $\bar{\mathfrak{P}}_j$ in $\bar{N}/\mathbb{Q}(t)$ Trägheitsgruppen besitzen, die Untergruppen von G sind, ergibt sich im Fall $p \equiv \pm 5 \bmod(24)$ in $\mathbb{Q}(t)/\mathbb{Q}(u)$

$$\bar{\mathfrak{q}}_1 = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2, \ \bar{\mathfrak{q}}_2 = \bar{\mathfrak{p}}_3^2, \ \bar{\mathfrak{q}}_3 = \bar{\mathfrak{p}}_4^2.$$

Die Trägheitsgruppen von $\mathfrak{P}_2/\bar{\mathfrak{p}}_3$ bzw. $\mathfrak{P}_3/\bar{\mathfrak{p}}_4$ werden durch Elemente aus $\tilde{C}_4^2 = C_2$ bzw. $\tilde{C}_6^2 = C_3$ erzeugt, also ist $(C_2, C_2, C_2, C_3)^*$ die Verzweigungsstruktur von $\bar{N}/\mathbb{Q}(t)$. Die übrigen Fälle beweist man analog. □

Zusatz 1. *Die in Satz 2 angegebenen Galoisrealisierungen der Gruppen* $\mathrm{PSL}_2(\mathbb{F}_p)$ *für* $p \not\equiv \pm 1 \bmod(24)$ *sind* GAR-*Realisierungen von* $\mathrm{PSL}_2(\mathbb{F}_p)$ *über* $\mathbb{Q}(t)$.

Beweis. Nach Konstruktion sind die Galoisrealisierungen von $G = \mathrm{PSL}_2(\mathbb{F}_p)$ in Satz 2 gemäß der Definition in [13] GA-Realisierungen von G über $\mathbb{Q}(t)$. Da die in $\mathbb{Q}(t)/\mathbb{Q}(u)$ verzweigten Primdivisoren den Grad 1 besitzen und $\mathrm{Out}(G) \cong Z_2$ ist, sind diese GA-Realisierungen nach der Anmerkung zu der Bemerkung 4 in [13] sogar GAR-Realisierungen von G über $\mathbb{Q}(t)$. □

Zusatz 2. *Für die beiden dreigliedrigen Verzweigungsstrukturen* $\mathfrak{C}_4^* = (C_3, C_4, C_4)^*$ *und* $\mathfrak{C}_6^* = (C_2, C_6, C_6)^*$ *der Gruppen* $\mathrm{PSL}_2(\mathbb{F}_p)$ *aus Satz 2 gelten mit* $\mathrm{Aut}(\mathfrak{C}_4^*) = \mathrm{Aut}(\mathfrak{C}_6^*) = \langle(23)\rangle$

$$l^i(\mathfrak{C}_4^*) = 2, \tilde{l}^i(\mathfrak{C}_4^*) = 1 \quad \textit{für} \quad p \equiv \pm\ 7 \bmod(24),$$
$$l^i(\mathfrak{C}_6^*) = 2, \tilde{l}^i(\mathfrak{C}_6^*) = 1 \quad \textit{für} \quad p \equiv \pm 11 \bmod(24).$$

Beweisskizze. Die Berechnung von $l^i(\mathfrak{C}^*)$ für $\mathfrak{C}^* \in \{\mathfrak{C}_4^*, \mathfrak{C}_6^*\}$ kann man nach dem Muster von Lemma 1 durchführen. Hieraus ergibt sich mit den in [12, Beispiel M_{12}] vorgeführten Überlegungen (s. auch [14, Satz 5.2]), daß die Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ für $p \equiv \pm 7 \bmod(24)$ im Falle $\tilde{l}^i(\mathfrak{C}_4^*) = 2$ wegen $\Sigma(C_2, C_4, C_3) = \emptyset$ Elemente der Ordnung 6 und für $p \equiv \pm 11 \bmod(24)$ im Falle $\tilde{l}^i(\mathfrak{C}_6^*) = 2$ Elemente der Ordnung 4 besäßen. Also sind $\tilde{l}^i(\mathfrak{C}_4^*) = 1$ und $\tilde{l}^i(\mathfrak{C}_6^*) = 1$ für die jeweiligen Kongruenzklassen von p modulo 24. □

Ein ausführlicher Beweis des Zusatzes befindet sich in [9, Bemerkungen 6.2 und 6.3]. Die Existenz einer Galoiserweiterung $N/\mathbb{Q}(t)$ mit der Gruppe $\mathrm{PSL}_2(\mathbb{F}_7)$ und der Verzweigungsstruktur $\mathfrak{C}_4^*$ wurde bereits in [11, Kommentar nach Satz 10.2] festgestellt.

2. Polynome mit der Galoisgruppe $\mathrm{PSL}_2(\mathbb{F}_7)$

Nach Satz 2 existiert eine Galoiserweiterung $N/\mathbb{Q}(t)$ mit der Gruppe $G = \mathrm{PSL}_2(\mathbb{F}_7)$ und der Verzweigungsstruktur $\mathfrak{C}_4^* = (C_3, C_4, C_4)^*$. In diesem Abschnitt wird ein Polynom siebten Grades $f(t, X) \in \mathbb{Q}(t)[X]$ berechnet, dessen Nullstellen N über $\mathbb{Q}(t)$ erzeugen. L sei ein durch eine Nullstelle von $f(t, X)$ über $\mathbb{Q}(t)$ erzeugter *Stammkörper von* $f(t, X)$. Das Verhalten der in $L/\mathbb{Q}(t)$ verzweigten Primdivisoren ergibt sich aus dem folgenden Satz, dessen Beweis eine einfache Übungsaufgabe in der Verzweigungstheorie darstellt:

Satz B. *$L = K(\theta)$ sei eine separable Körpererweiterung von K, $f(X) \in K[X]$ das Minimalpolynom von θ über K und N/K der Zerfällungskörper von $f(X)$ mit der Galoisgruppe $G = \mathrm{Gal}(f)$. Weiter seien $\mathfrak{p}$ ein Primdivisor von K, $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in N und die zugehörige Restklassenkörpererweiterung separabel.*

Zerfällt die Menge der Nullstellen $\{\theta_1, \ldots, \theta_n\}$ von $f(X)$ unter der Operation der Zerlegungsgruppe $G_Z(\mathfrak{P}/\mathfrak{p})$ von $\mathfrak{P}/\mathfrak{p}$ in r Transitivitätsgebiete $\mathbb{T}_1, \ldots, \mathbb{T}_r$ und $\mathbb{T}_j$ unter

der Operation der Trägheitsgruppe $G_T(\mathfrak{P}/\mathfrak{p})$ in f_j Transitivitätsgebiete der Längen e_j, so zerfällt $\mathfrak{p}$ in L/K in der Form

$$\mathfrak{p}=\prod_{j=1}^{r}\mathfrak{P}_j^{e_j} \quad \textit{mit} \quad \partial(\mathfrak{P}_j/\mathfrak{p})=f_j;$$

dabei bedeutet $\partial(\mathfrak{P}_j/\mathfrak{p})$ den Relativgrad von $\mathfrak{P}_j/\mathfrak{p}$.

Wegen $\mathfrak{C}_4^*=(C_3, C_4, C_4)^*$ sind in $\bar{L}:=\mathbb{Q}L$ über $\mathbb{Q}(t)$ drei Primdivisoren $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_3$ vom Restklassengrad 1 mit den Verzweigungsordnungen $e_1=3$, $e_2=e_3=4$ verzweigt. Da die Elemente der Ordnung 3 in $G\leqq S_7$ Permutationen vom Typ (3, 3, 1) und die Elemente der Ordnung 4 Permutationen vom Typ (4, 2, 1) sind, gilt nach Satz B in $\bar{L}/\mathbb{Q}(t)$:

$$\bar{\mathfrak{p}}_1=\mathfrak{P}_{1,1}^3\mathfrak{P}_{1,2}^3\mathfrak{P}_{1,3},\ \mathfrak{P}_i=\mathfrak{P}_{i,1}^4\mathfrak{P}_{i,2}^2\mathfrak{P}_{i,3} \quad \text{für} \quad i=2,3$$

mit $\partial(\mathfrak{P}_{i,j}/\bar{\mathfrak{p}}_i)=1$. Aus der Hurwitzschen Relativgeschlechtsformel bekommt man für die Geschlechter von $\bar{L}$ und L

$$g(L)=g(\bar{L})=1-7+\tfrac{1}{2}\partial(\mathfrak{D}_{L/\mathbb{Q}(t)})=0,$$

wobei $\partial(\mathfrak{D}_{\bar{L}/\mathbb{Q}(t)})=12$ den Grad der Differente $\mathfrak{D}_{\bar{L}/\mathbb{Q}(t)}$ von $\bar{L}/\mathbb{Q}(t)$ bezeichnet.

Offenbar ist $\bar{\mathfrak{p}}_1$ über $\mathbb{Q}(t)$ definiert im Gegensatz zu $\bar{\mathfrak{p}}_2$ und $\bar{\mathfrak{p}}_3$, da $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q}(t))$ nach dem Zusatz 2 die Primdivisoren $\bar{\mathfrak{p}}_2$ und $\bar{\mathfrak{p}}_3$ permutiert. Folglich sind in $L/\mathbb{Q}(t)$ zwei Primdivisoren $\mathfrak{p}_1$ vom Grad 1 mit der Verzweigungsordnung 3 und $\mathfrak{q}$ vom Grad 2 mit der Verzweigungsordnung 4 verzweigt. Die erzeugende Funktion t sei so gewählt, daß eine Divisorgleichung $\mathfrak{q}\mathfrak{p}_1^{-2}=(t^2-\pi)$ mit $\pi\in\mathbb{Q}$ gilt; hierdurch ist t bis auf rationale Vielfache bestimmt. Da die Gruppen Z_3 sowie deren Normalisatoren vom Typ S_3 in G jeweils 3 Transitivitätsgebiete der Längen $3-3-1$ besitzen, gilt in $L/\mathbb{Q}(t)$ nach Satz B

$$\mathfrak{p}_1=\mathfrak{P}_{1,1}^3\mathfrak{P}_{1,2}^3\mathfrak{P}_{1,3}.$$

Wegen $g(L)=0$ gibt es eine $L/\mathbb{Q}(t)$ erzeugende Funktion x mit dem Divisor $(x)=\mathfrak{P}_{1,2}\mathfrak{P}_{1,1}^{-1}$, die durch $(x+1)=\mathfrak{P}_{1,3}\mathfrak{P}_{1,1}^{-1}$ eindeutig bestimmt ist.

Nun sei $k(t)$ der Zerlegungskörper von $\bar{\mathfrak{p}}_2/\mathfrak{q}$ mit $(k:\mathbb{Q})=2$. Dann zerfällt $\mathfrak{q}$ in $k(t)/\mathbb{Q}(t)$ in $\tilde{\mathfrak{p}}_2$ und $\tilde{\mathfrak{p}}_3$, und $\tilde{\mathfrak{p}}_1$ sei der einzige Primteiler von $\mathfrak{p}_1$ in $k(t)$. Damit gelten die Divisorgleichungen

$$\frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1}=(t+\omega), \qquad \frac{\tilde{\mathfrak{p}}_3}{\tilde{\mathfrak{p}}_1}=(t-\omega) \quad \text{mit} \quad \omega^2=\pi\in\mathbb{Q}.$$

$\tilde{\mathfrak{p}}_2$ und $\tilde{\mathfrak{p}}_3$ zerfallen in $\tilde{L}:=kL$ über $k(t)$ weiter in

$$\tilde{\mathfrak{p}}_i=\tilde{\mathfrak{P}}_{i,1}^4\tilde{\mathfrak{P}}_{i,2}^2\tilde{\mathfrak{P}}_{i,3} \quad \text{für} \quad i=2,3.$$

Bezeichnet man nun die Primteiler von $\mathfrak{P}_{1,j}$ in $\tilde{L}$ mit $\tilde{\mathfrak{P}}_{1,j}$, so sind durch die Divisorgleichungen

$$\frac{\tilde{\mathfrak{P}}_{2,1}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\varrho), \qquad \frac{\tilde{\mathfrak{P}}_{2,2}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\sigma), \qquad \frac{\tilde{\mathfrak{P}}_{2,3}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\tau)$$

ϱ, σ und τ bestimmt. Da $\mathfrak{P}_{2,j}$ in $\tilde{L}/L$ zu $\mathfrak{P}_{3,j}$ konjugiert ist, gilt mit dem erzeugenden Automorphismus

$$\bar{}: k \to k,\ \alpha \mapsto \bar{\alpha}$$

von $k/\mathbb{Q}$:

$$\frac{\mathfrak{P}_{3,1}}{\mathfrak{P}_{1,1}} = (x+\bar{\varrho}), \quad \frac{\mathfrak{P}_{3,2}}{\mathfrak{P}_{1,1}} = (x+\bar{\sigma}), \quad \frac{\mathfrak{P}_{3,3}}{\mathfrak{P}_{1,1}} = (x+\bar{\tau}).$$

Damit erhält man

$$(t+\omega) = \frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1} = \frac{\mathfrak{P}_{2,1}^4 \mathfrak{P}_{2,2}^2 \mathfrak{P}_{2,3}}{\mathfrak{P}_{1,1}^3 \mathfrak{P}_{1,2}^3 \mathfrak{P}_{1,3}} = \left(\frac{(x+\varrho)^4 (x+\sigma)^2 (x+\tau)}{x^3(x+1)}\right)$$

und die dazu in $\tilde{L}/L$ konjugierte Divisorgleichung. Also existiert ein $\eta \in k^\times$ mit

$$x^3(x+1)(t+\omega) = \eta h(x) \tag{1}$$

für

$$h(x) := (x+\varrho)^4 (x+\sigma)^2 (x+\tau).$$

Durch Elimination von t aus (1) und der dazu in $\tilde{L}/L$ konjugierten Gleichung ergibt sich

$$2\omega x^3(x+1) = \eta h(x) - \bar{\eta}\bar{h}(x).$$

Da x über k transzendent ist, folgen hieraus $\eta = \bar{\eta}$ sowie die Polynomidentität

$$2\omega X^3(X+1) = \eta(h(X) - \bar{h}(X)). \tag{2}$$

Subtrahiert man von dem $X(X+1)$-fachen der nach X differenzierten Gleichung (2) die mit $(4X+3)$ multiplizierte Gleichung (2), so erhält man

$$(X+\varrho)^3 (X+\sigma) d(X) = (X+\bar{\varrho})^3 (X+\bar{\sigma}) \bar{d}(X)$$

mit

$$d(X) = \frac{X(X+1)h'(X) - (4X+3)h(X)}{(X+\varrho)^3 (X+\sigma)} \in k[X].$$

Auf Grund der Teilerfremdheit von $(X+\varrho)(X+\sigma)$ zu $(X+\bar{\varrho})(X+\bar{\sigma})$ spaltet sich diese Gleichung auf in

$$3(X+\varrho)^3 (X+\sigma) = \bar{d}(X) \tag{3}$$

und die dazu in $k[X]/\mathbb{Q}[X]$ konjugierte Gleichung. Durch Koeffizientenvergleich ergibt sich daraus das folgende nichtlineare Gleichungssystem aus den 4 Gleichungen

$$\begin{gathered}
9\varrho + 3\sigma + \bar{\varrho} - \bar{\sigma} - 2\bar{\tau} - 4 = 0, \\
9\varrho^2 + 9\varrho\sigma + 3\bar{\varrho}\bar{\sigma} + 2\bar{\varrho}\bar{\tau} - 2\bar{\sigma} - 3\bar{\tau} = 0, \\
3\varrho^3 + 9\varrho^2\sigma + 4\bar{\varrho}\bar{\sigma}\bar{\tau} + 2\bar{\varrho}\bar{\sigma} + \bar{\varrho}\bar{\tau} - \bar{\sigma}\bar{\tau} = 0, \\
\varrho^3\sigma + \bar{\varrho}\bar{\sigma}\bar{\tau} = 0
\end{gathered}$$

und den dazu in $k/\mathbb{Q}$ konjugierten Gleichungen. Unter Verwendung einer modularen Version des Buchbergerschen Verfahrens (s. [10, Abschn. 4, Beispiel 2]) stellt man fest, daß dieses Gleichungssystem aus 8 Gleichungen in 6 Unbekannten ein einziges Paar von Lösungen in einem quadratischen Erweiterungskörper von $\mathbb{Q}$ besitzt, dieses ist

$$\varrho = -1 \pm \sqrt{7}, \quad \sigma = -15 \mp 6\sqrt{7}, \quad \tau = -22 \pm 8\sqrt{7}.$$

Aus (1) folgt nun

$$t = \frac{\eta}{2} \frac{h(x) - \bar{h}(x)}{x^3(x+1)}. \tag{4}$$

Da t bisher nur bis auf rationale Vielfache festgelegt war und $\eta \in \mathbb{Q}$ ist, kann noch $\eta = 1$ gewählt werden, wodurch dann t eindeutig bestimmt ist. Setzt man die berechneten Werte für ϱ, σ, τ, $\bar{\varrho}$, $\bar{\sigma}$, $\bar{\tau}$ in (4) ein, so bekommt man schließlich das folgende Resultat:

Satz 3. *Der Zerfällungskörper N des Polynoms*

$$f(t, X) = X^7 - 56X^6 + 609X^5 + 1190X^4 + 6356X^3 + 4536X^2 - 6804X - 5832 - tX(X+1)^3$$

über $\mathbb{Q}(t)$ besitzt die Galoisgruppe $\mathrm{Gal}(N/\mathbb{Q}(t)) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ *und die Verzweigungsstruktur* $\mathfrak{C}_4^* = (C_3, C_4, C_4)^*$.

Nach dem Hilbertschen Irreduzibilitätssatz gibt es unendlich viele Spezialisierungen von t zu $\tau \in \mathbb{Q}$, so daß $f(\tau, X) \in \mathbb{Q}[X]$ eine zu $\mathrm{PSL}_2(\mathbb{F}_7)$ isomorphe Galoisgruppe besitzt. Eine unendliche Serie solcher Spezialisierungen wird in dem folgenden Zusatz angegeben:

Zusatz 3. *Spezialisiert man in dem Polynom $f(t, X)$ aus Satz 3 die Funktion t zu $\tau \in \mathbb{Z}$ mit*

$$\tau \equiv 1 \bmod(35),$$

so besitzt $f(\tau, X) \in \mathbb{Q}[X]$ eine zu $\mathrm{PSL}_2(\mathbb{F}_7)$ isomorphe Galoisgruppe.

Beweis. Offenbar ist die Galoisgruppe von $f(\tau, X)$ isomorph zu einer Untergruppe von $\mathrm{Gal}(f(t, X))$. Für $\tau \equiv 1 \bmod(35)$ besitzt $f(\tau, X)$ die folgende Primfaktorzerlegung modulo 5

$$f(\tau, X) \equiv (X+3)(X^2+4X+1)(X^4+2X^3+2X^2+X+1) \bmod(5)$$

und ist modulo 7 irreduzibel. Also enthält $\mathrm{Gal}(f(\tau, X))$ Elemente der Ordnungen 4 und 7, und es gilt daher $\mathrm{Gal}(f(\tau, X)) \cong \mathrm{PSL}_2(\mathbb{F}_7)$. □

Anmerkung. Das Polynom $f(t, X)$ aus Satz 3 kann aus dem Polynom $f_a(x)$ in [6] durch die Spezialisierung $a = -9$, $A = t$ und $x = -X$ erhalten werden.

3. Polynome mit der Galoisgruppe $\mathrm{PSL}_2(\mathbb{F}_{11})$

Nach Satz 2 gibt es eine Galoiserweiterung $N/\mathbb{Q}(t)$ mit der Gruppe $G = \mathrm{PSL}_2(\mathbb{F}_{11})$ und der Verzweigungsstruktur $\mathfrak{C}_6^* = (C_2, C_6, C_6)^*$. Für diesen Körper wird nun ein

erzeugendes Polynom $f(t,X)\in\mathbb{Q}(t)[X]$ elften Grades hergeleitet. Dazu sei $L/\mathbb{Q}(t)$ ein Stammkörper von $f(t,X)$. Da die Elemente der Ordnungen 2 bzw. 6 in der Permutationsdarstellung elften Grades von G die Permutationstypen (2, 2, 2, 2, 1, 1, 1) bzw. (6, 3, 2) besitzen, sind nach Satz B die drei in $\mathbb{Q}N/\mathbb{Q}(t)$ verzweigten Primdivisoren in $\bar{L}:=\mathbb{Q}L$ über $\mathbb{Q}(t)$ wie folgt verzweigt:

$$\bar{\mathfrak{p}}_1=\mathfrak{P}_{1,1}^2\mathfrak{P}_{1,2}^2\mathfrak{P}_{1,3}^2\mathfrak{P}_{1,4}^2\mathfrak{P}_{1,5}\mathfrak{P}_{1,6}\mathfrak{P}_{1,7},$$
$$\bar{\mathfrak{p}}_i=\mathfrak{P}_{i,1}^6\mathfrak{P}_{i,2}^3\mathfrak{P}_{i,3}^2 \quad \text{für} \quad i=2,3.$$

Damit ist der Differentengrad $\partial(\mathfrak{D}_{\bar{L}/\mathbb{Q}(t)})=20$, und aus der Hurwitzschen Relativgeschlechtsformel folgt

$$g(L)=g(\bar{L})=1-11+\tfrac{1}{2}\partial(\mathfrak{D}_{L/\mathbb{Q}(t)})=0.$$

Wie in Abschn. 2 sieht man, daß $\bar{\mathfrak{p}}_1$ über $\mathbb{Q}(t)$ definiert ist, während $\bar{\mathfrak{p}}_2$ und $\bar{\mathfrak{p}}_3$ die Primteiler eines Primdivisors $\mathfrak{q}$ von $\mathbb{Q}(t)$ vom Grad 2 sind. Des weiteren ist wieder eine erzeugende Funktion t von $\mathbb{Q}(t)$ durch $\mathfrak{q}\mathfrak{p}_1^{-2}=(t^2-\pi)$ mit $\pi\in\mathbb{Q}$ bis auf rationale Vielfache bestimmt. Der Zentralisator (und damit Normalisator) einer Z_2 in G ist eine Diedergruppe D_6 der Ordnung 12. Diese besitzt drei Transitivitätsgebiete der Längen $6-2-3$, da die Elemente der Ordnung 6 in G vom Permutationstyp (6, 3, 2) sind und die D_6 keine transitive Permutationsdarstellung auf 8 Symbolen besitzt. Nach Satz B gilt also für den von der Ordnung 2 in $L/\mathbb{Q}(t)$ verzweigten Primdivisor $\mathfrak{p}_1$ vom Grad 1:

$$\mathfrak{p}_1=\mathfrak{P}_{1,1}^2\mathfrak{P}_{1,2}^2\mathfrak{P}_{1,3} \quad \text{mit} \quad \partial(\mathfrak{P}_{1,1})=1,\ \partial(\mathfrak{P}_{1,j})=3 \quad \text{für} \quad j=2,3.$$

Dabei sind die Divisoren vom Grad 3 nicht notwendig Primdivisoren. Wegen $\partial(\mathfrak{P}_{1,1})=1$ ist $L/\mathbb{Q}$ ein rationaler Funktionenkörper und besitzt eine L über $\mathbb{Q}$ erzeugende Funktion x mit dem Nennerdivisor $\mathfrak{P}_{1,1}$. Der Primdivisor $\mathfrak{q}$ verzweigt sich in $L/\mathbb{Q}(t)$ nach Satz B in der Form

$$\mathfrak{q}=\mathfrak{Q}_1^6\mathfrak{Q}_2^3\mathfrak{Q}_3^2 \quad \text{mit} \quad \partial(\mathfrak{Q}_i/\mathfrak{q})=1.$$

Folglich kann man ein $x\in L$ unter den Funktionen mit dem Nenner $\mathfrak{P}_{1,1}$ festlegen durch die zusätzlichen Bedingungen

$$\frac{\mathfrak{Q}_1}{\mathfrak{P}_{1,1}^2}=(x^2+\xi), \qquad \frac{\mathfrak{Q}_2}{\mathfrak{P}_{1,1}^2}=(x^2+22x+\zeta).$$

(Der Ansatz $\mathfrak{Q}_2\mathfrak{P}_{1,1}^{-2}=(x^2+\zeta)$ führt in einem Zahlkörper k mit $(k:\mathbb{Q})\leqq 2$ nur zur trivialen Lösung $\zeta=0$!) Weiter gibt es Polynome

$$m(X)=X^3+\mu_2X^2+\mu_1X+\mu_0, \qquad n(X)=X^3+\nu_2X^2+\nu_1X+\nu_0$$

aus $\mathbb{Q}[X]$ mit

$$\frac{\mathfrak{P}_{1,2}}{\mathfrak{P}_{1,1}^3}=(m(x)), \qquad \frac{\mathfrak{P}_{1,3}}{\mathfrak{P}_{1,1}^3}=(n(x)).$$

$k(t)$ sei der Zerlegungskörper von $\bar{\mathfrak{p}}_2/\mathfrak{q}$. Sind $\tilde{\mathfrak{p}}_1$ der Primteiler von $\mathfrak{p}_1$ und $\tilde{\mathfrak{p}}_2, \tilde{\mathfrak{p}}_3$ die Primteiler von $\mathfrak{q}$ in $k(t)$, so gelten

$$\frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1}=(t+\omega), \qquad \frac{\tilde{\mathfrak{p}}_3}{\tilde{\mathfrak{p}}_1}=(t-\omega) \quad \text{mit} \quad \omega^2=\pi\in\mathbb{Q}.$$

Weiter zerfallen $\tilde{\mathfrak{p}}_2$ und $\tilde{\mathfrak{p}}_3$ in $\tilde{L}:=kL$ über $k(t)$ in

$$\tilde{\mathfrak{p}}_i=\tilde{\mathfrak{P}}_{i,1}^6\tilde{\mathfrak{P}}_{i,2}^3\tilde{\mathfrak{P}}_{i,3}^2 \quad \text{für} \quad i=2,3$$

mit $\mathfrak{Q}_j=\tilde{\mathfrak{P}}_{2,j}\tilde{\mathfrak{P}}_{3,j}$ für $j\in\{1,2,3\}$. Ist $\bar{}: k\to k$ wieder der erzeugende Automorphismus von $k/\mathbb{Q}$ und sind $\tilde{\mathfrak{P}}_{1,j}$ die Einbettungen von $\mathfrak{P}_{1,j}$ in die Divisorengruppe von $\tilde{L}/k$, so sind

$$\frac{\tilde{\mathfrak{P}}_{2,1}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\varrho), \quad \frac{\tilde{\mathfrak{P}}_{2,2}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\sigma), \quad \frac{\tilde{\mathfrak{P}}_{2,3}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\tau),$$
$$\frac{\tilde{\mathfrak{P}}_{3,1}}{\tilde{\mathfrak{P}}_{1,1}}=(x-\varrho), \quad \frac{\tilde{\mathfrak{P}}_{3,2}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\bar{\sigma}), \quad \frac{\tilde{\mathfrak{P}}_{3,3}}{\tilde{\mathfrak{P}}_{1,1}}=(x+\bar{\tau})$$

mit ϱ, σ, $\tau\in k$ und $\varrho^2=-\xi\in\mathbb{Q}$, $\sigma+\bar{\sigma}=22$. Damit gelten

$$(t+\omega)=\frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1}=\frac{\tilde{\mathfrak{P}}_{2,1}^6\tilde{\mathfrak{P}}_{2,2}^3\tilde{\mathfrak{P}}_{2,3}^2}{\tilde{\mathfrak{P}}_{1,1}^2\tilde{\mathfrak{P}}_{1,2}^2\tilde{\mathfrak{P}}_{1,3}}=\left(\frac{(x+\varrho)^6(x+\sigma)^3(x+\tau)^2}{m(x)^2n(x)}\right)$$

und die dazu in $\tilde{L}/L$ konjugierte Divisorgleichung. Folglich existiert ein $\eta\in k^\times$, so daß mit

$$g(x):=m(x)^2n(x), h(x):=(x+\varrho)^6(x+\sigma)^3(x+\tau)^2$$

gilt

$$g(x)(t+\omega)=\eta h(x). \tag{1}$$

Elimination von t aus (1) und der dazu in $\tilde{L}/L$ konjugierten Gleichung ergibt

$$2\omega g(x)=\eta h(x)-\bar{\eta}\bar{h}(x).$$

Da x über k transzendent ist, folgen hieraus wieder $\eta=\bar{\eta}$ und die Polynomidentität in $k[X]$:

$$2\omega g(X)=\eta(h(X)-\bar{h}(X)). \tag{2}$$

Subtrahiert man von dem $m(X)n(X)$-fachen der nach X differenzierten Gleichung (2) die mit $(2m'(X)n(X)+m(X)n'(X))$ multiplizierte Gleichung (2), so ergibt sich

$$(X+\varrho)^5(X+\sigma)^2(X+\tau)d(X)=(X-\varrho)^5(X+\bar{\sigma})^2(X+\bar{\tau})\bar{d}(X)$$

mit

$$d(X):=\frac{g(X)h'(X)-g'(X)h(X)}{m(X)(X+\varrho)^5(X+\sigma)^2(X+\tau)}\in k[X].$$

Da $(X+\varrho)(X+\sigma)(X+\tau)$ zu $(X-\varrho)(X+\bar{\sigma})(X+\bar{\tau})$ teilerfremd ist, spaltet sich diese Gleichung auf in

$$2(X+\varrho)^5(X+\sigma)^2(X+\tau)=\bar{d}(X) \tag{3}$$

und die dazu in $k[X]/\mathbb{Q}[X]$ konjugierte Gleichung. Durch Koeffizientenvergleich bei diesen beiden Polynomgleichungen erhält man unter Hinzufügung von $\sigma+\bar{\sigma}=22$ ein nichtlineares Gleichungssystem aus 17 Gleichungen in 11 Unbekannten. Dieses besitzt nur ein einziges Paar von Lösungen in einem Zahlkörper

$k/\mathbb{Q}$ mit $(k:\mathbb{Q}) \leqq 2$ (s. [10, Abschn. 4, Beispiel 6]). Diese Lösungen lauten mit $\theta = \pm\sqrt{33}$:

$$\mu_2 = 22, \quad \mu_1 = 165, \quad \mu_0 = 396,$$
$$\nu_2 = -22, \quad \nu_1 = -319, \quad \nu_0 = -924,$$
$$\varrho = \theta, \quad \sigma = 11 + \theta, \quad \tau = \tfrac{1}{2}(-33 - 9\theta).$$

Aus (1) ergibt sich

$$t = \frac{\eta}{2} \frac{h(x) + \bar{h}(x)}{m(x)^2 n(x)}. \tag{4}$$

Da t nur bis auf rationale Vielfache festgelegt war, kann noch $\eta = 1$ gesetzt werden, und man erhält durch Einsetzen der errechneten Werte für μ_i, ν_i, ϱ, σ, τ in (4) das Resultat:

Satz 4. *Der Zerfällungskörper N des Polynoms $f(t, X)$ mit*

$$\begin{aligned} 2f(t, X) = {} & 2X^{11} - 2541X^9 - 45254X^8 + 1026201X^7 + 51653448X^6 \\ & + 900904653X^5 + 8705450754X^4 + 50915146293X^3 \\ & + 180040201308X^2 + 355871173680X + 303064483392 \\ & - 2t(X^3 + 22X^2 + 165X + 396)^2 (X^3 - 22X^2 - 319X - 924) \end{aligned}$$

über $\mathbb{Q}(t)$ besitzt die Galoisgruppe $\mathrm{Gal}(N/\mathbb{Q}(t)) \cong \mathrm{PSL}_2(\mathbb{F}_{11})$ und die Verzweigungsstruktur $\mathfrak{C}_6^* = (C_2, C_6, C_6)^*$.

Zusatz 4. *Spezialisiert man in dem Polynom $f(t, X)$ aus Satz 4 die Funktion t zu $\tau \in \mathbb{Z}$ mit*

$$\tau \equiv -2 \bmod (595),$$

so besitzt $f(\tau, X) \in \mathbb{Q}[X]$ eine zu $\mathrm{PSL}_2(\mathbb{F}_{11})$ isomorphe Galoisgruppe.

Beweis. Für $\tau \equiv -2 \bmod (5 \cdot 7 \cdot 17)$ besitzt $f(\tau, X)$ die folgenden Primfaktorzerlegungen modulo 5 und 17

$$f(\tau, X) \equiv (X+4)(X^5 + 2X^4 + 4X^2 + 2)(X^5 + 4X^4 + 2X^3 + 4X^2 + 1) \bmod (5),$$
$$\begin{aligned} f(\tau, X) \equiv {} & (X^2 + 2X + 4)(X^3 + 7X + 15) \\ & \cdot (X^6 + 15X^5 + 8X^4 + 4X^3 + 10X^2 + 7X + 3) \bmod (17) \end{aligned}$$

und ist modulo 7 irreduzibel. Also enthält $\mathrm{Gal}(f(\tau, X))$ Elemente der Ordnungen 5, 6 und 11, und es ist daher $\mathrm{Gal}(f(\tau, X)) \cong \mathrm{PSL}_2(\mathbb{F}_{11})$. □

4. Polynome mit der Galoisgruppe $\mathrm{PSL}_2(\mathbb{F}_{13})$

Für die Verzweigungsstruktur $\mathfrak{C}_6^* := (C_2, C_6, C_6)^*$ von $G := \mathrm{PSL}_2(\mathbb{F}_{13})$ existiert nach Satz 2 eine Galoiserweiterung $N/\mathbb{Q}(t)$ mit einer zu G isomorphen Galoisgruppe, deren Stammkörper vom Grad 14 über $\mathbb{Q}(t)$ das Geschlecht 0 besitzen. Weil diese Stammkörper mit den verzweigungstheoretischen Methoden nicht als rationale Funktionenkörper nachgewiesen werden können, führt das in den

letzten beiden Paragraphen angewendete Verfahren zur Berechnung eines Polynoms mit der Galoisgruppe G zu einem erheblich komplizierteren nichtlinearen Gleichungssystem. Daher wird dieses Mal entsprechend dem Vorgehen in [11, Abschn. 7] zuerst ein Polynom $f(u,X)\in\mathbb{Q}(u)[X]$ mit der Galoisgruppe $\tilde{G}:=\mathrm{PGL}_2(\mathbb{F}_{13})$ konstruiert, das anschließend zu einem Polynom $f(t,X)$, $u\in\mathbb{Q}(t)$, mit der Gruppe G spezialisiert werden kann.

Nach Satz 1 gibt es eine Galoiserweiterung $N/\mathbb{Q}(u)$ mit der Galoisgruppe $\tilde{G}$ und der Verzweigungsstruktur $\tilde{\mathfrak{C}}^*:=(\tilde{C}_2,\tilde{C}_4,C_6)^*$. Der Fixkörper von $G\leqq\tilde{G}$ in $N/\mathbb{Q}(u)$ ist nach Satz 2 ein rationaler Funktionenkörper $\mathbb{Q}(t)$, und $N/\mathbb{Q}(t)$ besitzt die Galoisgruppe G und die Verzweigungsstruktur $\mathfrak{C}_6^*$. $L/\mathbb{Q}(u)$ sei ein Stammkörper vom Grad 14 in $N/\mathbb{Q}(u)$. Dann sind in $L/\mathbb{Q}(u)$ drei Primdivisoren $\mathfrak{q}_1,\mathfrak{q}_2,\mathfrak{q}_3$ mit den Verzweigungsordnungen $e_1=2$, $e_2=4$ und $e_3=6$ verzweigt. Da die Elemente aus $\tilde{C}_2$ bzw. $\tilde{C}_4$ bzw. C_6 in der Permutationsdarstellung vom Grad 14 von $\tilde{G}$ die Permutationstypen (2, 2, 2, 2, 2, 2, 2) bzw. (4, 4, 4, 1, 1) bzw. (6, 6, 1, 1) besitzen, sind die Primdivisoren $\mathfrak{q}_i$ nach Satz B in $L/\mathbb{Q}(u)$ folgendermaßen verzweigt:

$$\mathfrak{q}_1=\mathfrak{Q}_1^2,\qquad \mathfrak{q}_2=\mathfrak{Q}_{2,1}^4\mathfrak{Q}_{2,2},\qquad \mathfrak{q}_3=\mathfrak{Q}_{3,1}^6\mathfrak{Q}_{3,2}$$

mit $\partial(\mathfrak{Q}_1)=7$, $\partial(\mathfrak{Q}_{2,1})=3$, $\partial(\mathfrak{Q}_{2,2})=\partial(\mathfrak{Q}_{3,1})=\partial(\mathfrak{Q}_{3,2})=2$, wobei die Divisoren $\mathfrak{Q}_1$ und $\mathfrak{Q}_{i,j}$ keine Primdivisoren zu sein brauchen. Aus der Hurwitzschen Relativgeschlechtsformel ergibt sich somit

$$g(L)=1-14+\tfrac{1}{2}\partial(\mathfrak{D}_{L/\mathbb{Q}(u)})=0,$$

und $L/\mathbb{Q}$ ist ein rationaler Funktionenkörper, da $\mathfrak{Q}_1$ ein Divisor ungeraden Grades von L ist. Eine erzeugende Funktion $\tilde{u}$ von $\mathbb{Q}(u)$ wird bestimmt durch

$$\frac{\mathfrak{q}_1}{\mathfrak{q}_3}=(\tilde{u}),\qquad \frac{\mathfrak{q}_2}{\mathfrak{q}_3}=(\tilde{u}-1).$$

Da keiner der als Teiler von $\mathfrak{q}_1$, $\mathfrak{q}_2$ und $\mathfrak{q}_3$ auftretenden Divisoren $\mathfrak{Q}_1$ und $\mathfrak{Q}_{i,j}$ den Grad 1 besitzt, ist es nicht so ohne weiteres möglich, eine $L/\mathbb{Q}$ erzeugende Funktion durch Divisorgleichungen festzulegen. Dies wird durch eine geeignete Konstantenerweiterung erleichtert.

$\mathfrak{Q}_{3,1}$ zerfällt in $\mathbb{Q}L$ in zwei Primdivisoren $\tilde{\mathfrak{Q}}_\infty$ und $\tilde{\mathfrak{Q}}_0$. $\tilde{L}$ sei der Zerlegungskörper von $\tilde{\mathfrak{Q}}_\infty/\mathfrak{Q}_{3,1}$, und k sei der Konstantenkörper von $\tilde{L}$ mit $(k:\mathbb{Q})\leqq 2$. Weiter seien $\tilde{\mathfrak{q}}_i$ die Primteiler von $\mathfrak{q}_i$ in $k(u)$, $\tilde{\mathfrak{Q}}_\infty$ und $\tilde{\mathfrak{Q}}_0$ die Primteiler von $\mathfrak{Q}_{3,1}$ in $\tilde{L}$ sowie $\tilde{\mathfrak{Q}}_1$ bzw. $\tilde{\mathfrak{Q}}_{i,j}$ die in $\tilde{L}$ eingebetteten Divisoren $\mathfrak{Q}_1$ bzw. $\mathfrak{Q}_{i,j}$ von L. Dann wird $\tilde{L}/k$ erzeugt durch eine Funktion $\tilde{x}$, die durch die Divisorgleichungen

$$\frac{\tilde{\mathfrak{Q}}_0}{\tilde{\mathfrak{Q}}_\infty}=(\tilde{x}),\qquad \frac{\tilde{\mathfrak{Q}}_{3,2}}{\tilde{\mathfrak{Q}}_\infty^2}=(\tilde{s}(\tilde{x}))$$

festgelegt ist, wobei $\tilde{s}(X)\in k[X]$ eine vorgegebene von 0 verschiedene Spur besitzt, also ist etwa $\tilde{s}(X)=X^2+130X+\tilde{\sigma}$. Dann gibt es weiter normierte Polynome

$$\tilde{p}(X)=\sum_{i=0}^{7}\tilde{\pi}_iX^i,\qquad \tilde{q}(X)=\sum_{i=0}^{3}\tilde{\omega}_iX^i,\qquad \tilde{r}(X)=\sum_{i=0}^{2}\tilde{\varrho}_iX^i$$

in $k[X]$ mit

$$\frac{\mathfrak{Q}_1}{\mathfrak{Q}_\infty^7}=(\tilde{p}(\tilde{x})),\quad \frac{\mathfrak{Q}_{2,1}}{\mathfrak{Q}_\infty^3}=(\tilde{q}(\tilde{x})),\quad \frac{\mathfrak{Q}_{2,2}}{\mathfrak{Q}_\infty^2}=(\tilde{r}(\tilde{x})).$$

Damit existieren $\eta, \tilde{\eta}\in k$ mit

$$\tilde{x}^6\tilde{s}(\tilde{x})\tilde{u}=\eta\tilde{p}(\tilde{x})^2,\quad \tilde{x}^6\tilde{s}(\tilde{x})(\tilde{u}-1)=\tilde{\eta}\tilde{q}(\tilde{x})^4\tilde{r}(\tilde{x}). \tag{1}$$

Elimination von $\tilde{u}$ liefert

$$\tilde{x}^6\tilde{s}(\tilde{x})=\eta\tilde{p}(\tilde{x})^2-\tilde{\eta}\tilde{q}(\tilde{x})^4\tilde{r}(\tilde{x}).$$

Da $\tilde{x}$ über k transzendent ist, folgen hieraus $\eta=\tilde{\eta}$ und die Polynomidentität

$$X^6\tilde{s}(X)=\eta(\tilde{p}(X)^2-\tilde{q}(X)^4\tilde{r}(X)) \tag{2}$$

in $k[X]$. Durch Multiplikation der Gleichung (2) mit $(X\tilde{s}'(X)+6\tilde{s}(X))$ und anschließender Subtraktion des $X\tilde{s}(X)$-fachen der nach X differenzierten Gleichung (2) erhält man

$$\tilde{p}(X)g(X)=\tilde{q}(X)^3h(X)$$

mit

$$\begin{aligned}g(X):&=2X\tilde{p}'(X)\tilde{s}(X)-X\tilde{p}(X)\tilde{s}'(X)-6\tilde{p}(X)\tilde{s}(X),\\ h(X):&=4X\tilde{q}'(X)\tilde{r}(X)\tilde{s}(X)+X\tilde{q}(X)\tilde{r}'(X)\tilde{s}(X)\\ &\quad -X\tilde{q}(X)\tilde{r}(X)\tilde{s}'(X)-6\tilde{q}(X)\tilde{r}(X)\tilde{s}(X).\end{aligned}$$

Aus der Teilerfremdheit von $\tilde{p}(X)$ und $\tilde{q}(X)$ in $k[X]$ folgen nun

$$6\tilde{p}(X)=h(X),\quad 6\tilde{q}(X)^3=g(X). \tag{3}$$

Das durch Koeffizientenvergleich in (3) entstehende nichtlineare Gleichungssystem von 16 Gleichungen in den 12 Unbekannten $\tilde{\pi}_i$, $\tilde{\omega}_i$, $\tilde{\varrho}_i$ und $\tilde{\sigma}$ besitzt nur ein einziges Lösungspaar in Zahlkörpern k mit $(k:\mathbb{Q})\leqq 2$, dieses wurde mit Hilfe des in [10, Abschn. 3] beschriebenen Verfahrens festgestellt. Die hierbei gefundenen Lösungen lauten mit $\theta=\sqrt{-39}$:

$$\begin{aligned}&\tilde{\omega}_2=\tfrac{1}{2}(247\pm 5\theta),\quad \tilde{\omega}_1=\tfrac{1}{4}(1703\pm 91\theta),\quad \tilde{\omega}_0=\tfrac{1}{4}(169\pm 13\theta),\\ &\tilde{\varrho}_1=\tfrac{1}{2}(325\pm 25\theta),\quad \tilde{\varrho}_0=\tfrac{1}{8}(65\pm 13\theta),\quad \tilde{\sigma}=13.\end{aligned}$$

Hierdurch sind nach (3) auch die Koeffizienten $\tilde{\pi}_i$ von $\tilde{p}(X)$ sowie nach (2)

$$\eta^{-1}=-2^9 13^{-4}(13+9\theta)$$

bestimmt. Damit erhält man als Minimalpolynom von $\tilde{x}$ über $k(u)$ nach (1)

$$\tilde{f}(\tilde{u},X)=\tilde{p}(X)^2-\eta^{-1}X^6\tilde{s}(X)\tilde{u}\in k(u)[X]$$

mit $\mathrm{Gal}(\tilde{f}(\tilde{u},X))\cong\tilde{G}$.

Um zu einem Polynom $f(u,X)\in\mathbb{Q}(u)[X]$ und $\mathrm{Gal}(f(u,X))\cong\tilde{G}$ zu gelangen, wählen wir eine $L/\mathbb{Q}$ erzeugende Funktion x, deren Nennerdivisor $\mathfrak{N}$ sei, mit

$$(x^2+39)=\frac{\mathfrak{Q}_{3,1}}{\mathfrak{N}^2}=\frac{\mathfrak{Q}_\infty\mathfrak{Q}_0}{\mathfrak{N}^2}=\frac{\mathfrak{Q}_\infty^2}{\mathfrak{N}^2}\cdot\frac{\mathfrak{Q}_0}{\mathfrak{Q}_\infty}=((x+\xi)^2\tilde{x}),$$

wobei $\mathfrak{N}$ die Einbettung von $\mathfrak{N}$ in $\tilde{L}$ ist und $\mathfrak{Q}_\infty \mathfrak{N}^{-1} = (x+\xi)$ gilt. Dies ist möglich, da $\mathfrak{Q}_{3,1}$ ein Primdivisor von $L/\mathbb{Q}$ ist, der in $\tilde{L}/L$ in $\mathfrak{Q}_\infty \mathfrak{Q}_0$ zerfällt. Wegen $\xi \in \{\theta, -\theta\}$ ist

$$\tilde{x} = \varepsilon \frac{x \pm \theta}{x \mp \theta}$$

mit $\varepsilon \in k^\times$, und es ist noch ε so zu bestimmen, daß für $\tilde{d}(X) \in \{\tilde{p}(X), \tilde{q}(X), \tilde{r}(X), \tilde{s}(X)\}$ die Polynome

$$d(X) := \frac{(X+\theta)^{\partial(d)}}{\tilde{d}(\varepsilon)} \tilde{d}\left(\varepsilon \frac{X+\theta}{X-\theta}\right).$$

Elemente von $\mathbb{Q}[X]$ sind. Für $\varepsilon = \dfrac{13+\theta}{4}$ erhält man

$$p(X) = X^7 + 50X^6 + 63X^5 + 5040X^4 + 783X^3 + 168426X^2 - 6831X + 1864404,$$
$$q(X) = X^3 - X^2 + 35X - 27, \quad r(X) = X^2 + 36, \quad 7s(X) = 7X^2 - 2X + 247.$$

Um die folgenden Ergebnisse einfacher zu gestalten, ersetzen wir in (1) neben $\tilde{x} = \dfrac{(13+\theta)(x+\theta)}{4(x-\theta)}$ noch $\tilde{u} = \dfrac{1}{u-1}$. Nach Satz 4.3.b) in [11] ist nunmehr die Galoisgruppe des durch

$$(u+27) f(u, X) = p(X)^2 (u-1) + 28(X^2+39)^6 s(X) = p(X)^2 u + 27 q(X)^4 r(X) \quad (4)$$

definierten Polynoms $f(u, X) \in \mathbb{Q}(u)[X]$ isomorph zu $\tilde{G}$, da $\tilde{G}$ eine vollständige Gruppe ist. Weiter folgt aus (4) die Polynomidentität

$$28(X^2+39)^6 s(X) = p(X)^2 + 27 q(X)^4 r(X). \quad (5)$$

Nach Satz 2 ist der Fixkörper von G in $N/\mathbb{Q}(u)$ ein rationaler Funktionenkörper $\mathbb{Q}(t)$. Da in $\mathbb{Q}(t)/\mathbb{Q}(u)$ die Primdivisoren $\mathfrak{q}_1 = \mathfrak{p}_0^2$ und $\mathfrak{q}_2 = \mathfrak{p}_1^2$ verzweigt sind, gibt es eine erzeugende Funktion t mit

$$(t)^2 = \left(\frac{\mathfrak{p}_1}{\mathfrak{p}_0}\right)^2 = \frac{\mathfrak{q}_2}{\mathfrak{q}_3} \frac{\mathfrak{q}_3}{\mathfrak{q}_1} = \left(\frac{\tilde{u}-1}{\tilde{u}}\right) = (u)$$

und ein $\lambda \in \mathbb{Q}^\times$ mit $\lambda t^2 = u$. Die Galoisgruppe von $f(\lambda t^2, X)$ ist dann isomorph zu $G \leqq A_{14}$, also erhält man die Quadratklasse von λ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ durch die Bedingung, daß die Diskriminante $D(f(\lambda t^2, X))$ ein Quadrat in $\mathbb{Q}$ ist. Dazu berechnet man zunächst $-D(f(u, X))$ als die $L/\mathbb{Q}(u)$-Norm von $f'(u, x)$. Aus (4) folgt unter Verwendung der durch Differentiation aus (5) entstehenden Gleichung

$$\begin{aligned}(u+27) f'(u, X) &= 2p(X)p'(X)u + 108 q(X)^3 q'(X) r(X) + 27 q(X)^4 r'(X) \\ &\equiv 27 \frac{q(X)^3}{p(X)} (-2p'(X) q(X) r(X) + 4p(X) q'(X) r(X) + p(X) q(X) r'(X)) \\ &\equiv 2^3 3^3 13 \frac{q(X)^3 (X^2+39)^5}{p(X)} \bmod (f(u, X)).\end{aligned}$$

Mit

$$\mathcal{N}(p(x))=2^{134}3^{39}13, \quad \mathcal{N}(q(x))=2^{66}3^{6}u^{3}, \quad \mathcal{N}(x^2+39)=2^{32}3^{12}(u-1)^2$$

ergibt sich also

$$(u+27)^{14}D(f(u,X))=-(u+27)^{14}\mathcal{N}(f'(u,x))=-2^{266}3^{81}13^{13}u^{9}(u-1)^{10}.$$

Danach ist λ quadratgleich zu -39. Aus (4) und $u=-39t^2$ erhält man das folgende Resultat:

Satz 5. a) *Der Zerfällungskörper N des durch*

$$(u+27)f(u,X)=(X^7+50X^6+63X^5+5040X^4+783X^3+168426X^2$$
$$-6831X+1864404)^2u+27(X^3-X^2+35X-27)^4(X^2+36)$$

definierten Polynoms $f(u,X)\in\mathbb{Q}(u)[X]$ über $\mathbb{Q}(u)$ besitzt die Galoisgruppe $\mathrm{Gal}(N/\mathbb{Q}(u))\cong\mathrm{PGL}_2(\mathbb{F}_{13})$ *und die Verzweigungsstruktur $\mathfrak{C}^*=(\tilde{C}_2,\tilde{C}_4,C_6)$.*

b) *N ist der Zerfällungskörper von*

$$f(-39t^2,X)\in\mathbb{Q}(t)[X]$$

über $\mathbb{Q}(t)$ mit der Galoisgruppe $\mathrm{Gal}(N/\mathbb{Q}(t))\cong\mathrm{PSL}_2(\mathbb{F}_{13})$ *und der Verzweigungsstruktur $\mathfrak{C}_6^*=(C_2,C_6,C_6)^*$.*

Zusatz 5. a) *Spezialisiert man in dem Polynom $f(u,X)$ aus Satz 5 die Funktion u zu $v\in\mathbb{Z}$ mit*

$$v\equiv -3 \bmod(85),$$

so besitzt $f(v,X)\in\mathbb{Q}[X]$ eine zu $\mathrm{PGL}_2(\mathbb{F}_{13})$ *isomorphe Galoisgruppe.*

b) *Für $\tau\in\mathbb{Z}$ mit*

$$\tau\equiv\pm 1 \bmod(77)$$

besitzt $f(-39\tau^2,X)\in\mathbb{Q}[X]$ eine zu $\mathrm{PSL}_2(\mathbb{F}_{13})$ *isomorphe Galoisgruppe.*

Beweis. $f(-3,X)$ ist modulo 5 irreduzibel und zerfällt modulo 17 in Primfaktoren der Grade 13 und 1. Also enthält $\mathrm{Gal}(f(-3,X))\leqq\mathrm{Gal}(f(u,X))$ Elemente der Ordnungen 14 und 13, somit ist $\mathrm{Gal}(f(-3,X))\cong\mathrm{PGL}_2(\mathbb{F}_{13})$. Die Aussage a) folgt nun hieraus, da die Kongruenzen für $v\equiv -3 \bmod(5\cdot 17)$ erhalten bleiben.

$f(-39,X)$ zerfällt modulo 7 in Primfaktoren der Grade 13 und 1 und modulo 11 in 2 Primfaktoren vom Grad 7. Daher enthält $\mathrm{Gal}(f(-39\tau^2,X))$ für $\tau\in\mathbb{Z}$ mit $\tau\equiv\pm 1 \bmod(7\cdot 11)$ Elemente der Ordnungen 13 und 7 und ist folglich isomorph zu $\mathrm{PSL}_2(\mathbb{F}_{13})$. □

Schlußbemerkung

Für einfache Gruppen $\mathrm{PSL}_n(\mathbb{F}_q)$, $q=p^f$, sind uns bisher noch die folgenden weiteren Galoisrealisierungen über $\mathbb{Q}(t)$ bekannt: $\mathrm{PSL}_2(\mathbb{F}_4)\cong A_5$, $\mathrm{PSL}_2(\mathbb{F}_9)\cong A_6$ und $\mathrm{PSL}_2(\mathbb{F}_8)$ ([11], Sätze 6.3 und 8.5) sowie $\mathrm{PSL}_3(\mathbb{F}_p)$ für $p\not\equiv 47, 143, 167 \bmod(168)$. Letzteres ergibt sich aus Resultaten von Thompson [17], dem ersten Autor ([9], Satz 9.9) sowie einer Mitteilung von Feit. Weiter hat Ribet nach-

gewiesen, daß die Gruppen $PSL_2(\mathbb{F}_{p^2})$ mit solchen Primzahlen $p \neq 47$, für die 144169 kein quadratischer Rest modulo p ist, als Galoisgruppen über $\mathbb{Q}$ vorkommen ([15], Abschn. 7).

Läßt man statt $\mathbb{Q}$ den maximal abelschen Erweiterungskörper $\mathbb{Q}^{ab}$ von $\mathbb{Q}$ als Konstantenkörper zu, so werden alle Gruppen $PSL_n(\mathbb{F}_q)$ als Galoisgruppen über $\mathbb{Q}^{ab}(t)$ realisierbar. Nach den Arbeiten von Belyi [2] und [3] (s. auch [19]) besitzen nämlich alle klassischen einfachen Gruppen Galoisrealisierungen über $\mathbb{Q}^{ab}(t)$.

Literatur

1. Aschbacher, M. eds.: Proceedings of the Rutgers group theory year, 1983–1984. Cambridge: Cambridge University Press 1984
2. Belyi, G.V.: On Galois extensions of a maximal cyclotomic field. Math. USSR Izv. **14**, 247–256 (1980)
3. Belyi, G.V.: On extensions of the maximal cyclotomic field having a given classical Galois group. J. reine angew. Math. **341**, 147–156 (1983)
4. Erbach, D.W., Fischer, J., McKay, J.: Polynomials with PSL(2, 7) as Galois group. J. Number Theory **11**, 69–75 (1979)
5. Fricke, R.: Lehrbuch der Algebra III. Braunschweig: Vieweg 1928
6. LaMacchia, S.E.: Polynomials with Galois group PSL(2, 7). Commun. Algebra **8**, 983–991 (1980)
7. LaMacchia, S.E.: Polynomials with Galois group PSL(2, 11). Commun. Algebra **9**, 613–625 (1981)
8. Macbeath, A.M.: Generators of the linear fractional groups. Proc. Symp. Pure Math. **12**, 14–32 (1969)
9. Malle, G.: Realisierung von Gruppen $PSL_2(\mathbb{F}_p)$ und $PSL_3(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$. Diplomarbeit, Math. Fak. Univ. Karlsruhe 1984
10. Malle, G., Trinks, W.: Zur Behandlung algebraischer Gleichungssysteme mit dem Computer. Erscheint demnächst
11. Matzat, B.H.: Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. J. reine angew. Math. **349**, 179–220 (1984)
12. Matzat, B.H.: Realisierung endlicher Gruppen als Galoisgruppen. Manuscripta Math. **51**, 253–265 (1985)
13. Matzat, B.H.: Zum Einbettungsproblem der algebraischen Zahlentheorie mit nicht abelschem Kern. Invent. Math. **80**, 365–374 (1985)
14. Matzat, B.H.: Topologische Automorphismen in der konstruktiven Galoistheorie. Erscheint demnächst
15. Ribet, K.A.: On l-adic representations attached to modular forms. Invent. Math. **28**, 245–275 (1975)
16. Shih, K.: On the construction of Galois extensions of function fields and number fields. Math. Ann. **207**, 99–120 (1974)
17. Thompson, J.G.: PSL_3 and Galois groups over $\mathbb{Q}$. [1], 309–319 (1984)
18. Trinks, W.: Arithmetisch ähnliche Zahlkörper. Diplomarbeit, Math. Fak. Univ. Karlsruhe 1969
19. Walter, J.H.: Classical groups as Galois groups. [1], 357–383 (1984)

Eingegangen am 2. Mai 1985