Universität des Saarlandes
Naturwissenschaftlich-Technische Fakultät I
Mathematik

Masterarbeit

Die Geschlechter der Modulkurven zu dünn besetzten Drinfeld-Moduln des Rangs drei

Der lokale Fall

vorgelegt von
Marius Bohn

im Januar 2015

angefertigt am Lehrstuhl von Herrn Prof. Dr. Ernst-Ulrich Gekeler

Vorwort

Die vorliegende Masterarbeit mit dem Titel „Die Geschlechter der Modulkurven zu dünn besetzten Drinfeld-Moduln des Rangs drei- der lokale Fall“ zur Erlangung des Masterabschlusses in Mathematik ist am Lehrstuhl von Prof. Dr. Ernst-Ulrich Gekeler in Zusammenarbeit mit David Geis entstanden.

Dank. An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich bei der Anfertigung der vorliegenden Masterarbeit unterstützt haben. Zunächst danke ich Herrn Prof. Dr. Ernst-Ulrich Gekeler einerseits für das interessante und facettenreiche Thema und andererseits für die stete Hilfe, ständige Verfügbarkeit sowie die wertvollen Impulse und Anregungen.
Darüber hinaus gilt mein besonderer Dank David Geis für die gute Kooperation und die unermüdliche Einsatzbereitschaft bei der Bewältigung des Themenkomplexes, was erheblich zum Gelingen der vorliegenden Masterarbeit beitrug.
Außerdem danke ich Ruwen Hollenbach und Harald Brenner für das Korrekturlesen der Arbeit. Nicht zuletzt will ich auch meinen Eltern für den finanziellen und mentalen Rückhalt über mein gesamtes Studium hinweg danken. Diese Unterstützung lieferte erst die Rahmenbedingungen für den Erfolg meines Mathematikstudiums.

Saarbrücken, Januar 2015 — Marius Bohn

Ich versichere hiermit, die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet zu haben.

Saarbrücken, im Januar 2015

Inhaltsverzeichnis

Einführung

In den letzten Jahrzehnten rückte die Frage nach der Zahl der rationalen Punkte einer Kurve vom Geschlecht g über einem endlichen Körper $\mathbb{F}_q$ in den Fokus mathematischer Grundlagenforschung. Dies ist einerseits auf intrinsisches mathematisches Interesse zurückzuführen und andererseits ist diese Frage durch vielversprechende Anwendungen in der Kodierungstheorie und Kryptographie motiviert.
Unter einer „Kurve“ verstehen wir hierbei eine projektive, zusammenhängende, glatte algebraische Kurve. Bezeichnet $N_q(g)$ die maximale Zahl von rationalen Punkten einer Kurve vom Geschlecht g über einem endlichen Körper $\mathbb{F}_q$, so blieb die Hasse-Weil Schranke aus den 1940er Jahren

$$N_q(g) \leq q + 1 + \lfloor 2g\sqrt{q} \rfloor,$$

welche ursprünglich von Hasse für Kurven vom Geschlecht $g = 1$ und später von Weil auch für $g > 1$ gezeigt wurde, lange Zeit das einzige bedeutende Ergebnis (siehe etwa [HJ08] Theorem 9.2). Hierbei bezeichnet $\lfloor \cdot \rfloor$ die floor-Funktion, also die größte ganze Zahl, die kleiner gleich als das Argument ist. Goppa erweiterte schließlich den Anwendungsbereich dieses Forschungsgebietes durch die Begründung der algebraischen Kodierungstheorie (siehe [Gop88]). Zur Konstruktion von „guten“ Codes benötigt man Kurven mit vielen rationalen Punkten. 1981 konnte Ihara in [Iha81] mit einem einfachen und eleganten Argument zeigen, dass

$$N_q(g) \leq q + 1 + \lfloor \frac{\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g}{2} \rfloor$$

gilt. Für $g > \frac{q-\sqrt{q}}{2}$ ist diese Schranke schärfer als die Weil-Schranke. Nicht nur in diesem Zusammenhang ist es besonders interessant, die Zahl

$$A_q := \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

zu bestimmen. Offensichtlich ist $A_q \leq \lfloor 2\sqrt{q} \rfloor$ wegen der Hasse-Weil-Schranke. Die Arbeit von Ihara ([Iha81]) lieferte nun die asymptotische Schranke

$$A_q \leq \sqrt{2q + \frac{1}{4}} - \frac{1}{2}.$$

Drinfeld und Vladut zeigten, dass schon

$$A_q \leq \sqrt{q} - 1$$

gilt ([TM07] Theorem 3.2.1). Wir erhalten sogar Gleichheit, wenn q ein Quadrat ist, wie Ihara nachweisen konnte (siehe [Iha81]).
Mit der Zeit gab es immer mehr Veröffentlichungen, die sich mit der Konstruktion von Türmen von Kurven $X_i/\mathbb{F}_q$ beschäftigen, für welche die obere Schranke angenommen wird. Solche Serien von Kurven $(X_i)_{i \in \mathbb{N}}$ nennt man „asymptotisch optimal“. Einen guten Überblick über die Konstruktion und die Eigenschaften von solchen „asymptotisch optimalen“ Kurven kann man sich etwa in [TM07] ab Abschnitt 3.2.5 verschaffen. Die Kurven X_i kann man als die Reduktion von speziellen

Drinfeldschen Modulkurven identifizieren, bei welchen es äußerst schwierig ist, das Geschlecht exakt anzugeben oder auch nur abzuschätzen; einen Einstieg in die Konstruktion von Drinfeldschen Modulkurven findet man in [Gek91].
Ausgangspunkt der vorliegenden Masterarbeit sind die Erkenntnisse der neuesten Veröffentlichung von Ernst-Ulrich Gekeler [Gek14]. Die Arbeit von Ernst-Ulrich Gekeler liefert ein Konstruktionsverfahren für „asymptotisch optimale“ Türme von Kurven X_i vom Typ $X^{r,k}$ über dem Körper $\mathbb{F}_{q^r}$ mit q^r Elementen, welche $\limsup_{i\to\infty} \frac{X_i(\mathbb{F}_{q^r})}{g(X_i)} > 0$ erfüllen; es ist $N = \prod_{i=1}^{s} p_i^{r_i} \in A$. Hierbei haben die Galois-Überlagerungen $X^{r,k}(N)$ über $\mathbb{P}^1/\mathbb{F}_q(T)$ Galois-Gruppen vom Typ $G(N) = \{g \in \mathrm{GL}(r, \mathbb{F}_q[T]/(N))|\ \det(g) \in \mathbb{F}_q^*\}/Z$, wobei $Z \xrightarrow{\cong} \mathbb{F}_q^*$ die Gruppe der $\mathbb{F}_q$- wertigen Skalarmatrizen bezeichnet.
Die Geschlechter der Kurven $X^{r,k}(N)$ sind ohne größeren Aufwand zu berechnen, aber in der Regel nicht interessant genug. Verwendet man Untergruppen von $G(N)$ zur Konstruktion unserer Kurven, ist es deutlich attraktiver, leider aber auch mühsamer, das Geschlecht auszurechnen. Hier liegt der Ansatzpunkt der vorliegenden Masterarbeit. Es spielen dabei lediglich Kurven vom Rang $r \geq 3$ eine vielversprechende Rolle. Der Fall $r = 2$ liefert Kurven mit wohlbekannten Geschlechtern. Die Vorgehensweise zur Bestimmung der Geschlechter von diesen Modulkurven ist jedoch schon im GL(2)− Fall mustergültig für die Berechnung der Geschlechter von Kurven des Rangs $r \geq 3$; die Situation $r = 2$ wurde von Ernst-Ulrich Gekeler im Rahmen des Oberseminars zur Algebra und Zahlentheorie an der Universität des Saarlandes im November 2013 präsentiert.
Betrachten wir nun Kurven vom Rang drei, d.h. fixieren wir für die Kurven $X^{r,k}(N)$ die Parameter zu $r = 3$ und $k = 2$, so wird es uns gelingen, das Geschlecht der Kurve $X_0^{3,2}(N)$ zu bestimmen. Hierbei entsteht $X_0^{3,2}(N)$ durch das „Herausdividieren“ der parabolischen Untergruppe $P(N)$ aus $X^{3,2}(N)$. Die entsprechende Überlagerung der projektiven Geraden $X_0^{3,2}(N) \longrightarrow X(1) \cong \mathbb{P}^1(C_\infty)$ ist keine Galois-Überlagerung; somit kann die Riemann-Hurwitz-Formel zur Berechnung des Geschlechts nicht direkt angewendet werden. Stattdessen werden wir die Riemann-Hurwitz-Formel auf die galoisschen Überlagerungen $X^{3,2}(N) \longrightarrow X(1) \cong \mathbb{P}^1(C_\infty)$ und $X^{3,2}(N) \longrightarrow X_0^{3,2}(N)$ anwenden; über diesen Umweg wird es uns gelingen, das Geschlecht der Kurve $X_0^{3,2}(N)$ zu berechnen.
Das Hauptergebnis dieser Arbeit ist die Berechnung des Geschlechts $g(X_0^{3,2}(N))$ mit primärem Führer $\underline{N = p^r}$, wobei $p \in A = \mathbb{F}_q[T]$ ein Primpolynom ist.
Die Lösungsstrategie von Ernst-Ulrich Gekeler zur Bestimmung des Geschlechts von $X_0^{r,r-1}(T^n)$ können wir im Wesentlichen auf unsere Situation übertragen, weshalb eine Orientierung an dieser Vorgehensweise nahe lag. Im Unterschied zu den Rechnungen in der zugrunde liegenden Veröffentlichung ist der Grad d unseres Primpolynoms nicht mit $d = 1$ fixiert, sondern beliebig. Diese verallgemeinerte Annahme erfordert die Beachtung von mehr technischen Details. Insbesondere bei der Bestimmung der Verzweigungszahlen a_Q an den Spitzen $Q = \xi(\infty)$ treten hierbei in der Situation $d \equiv 0 \mod 2$ zusätzliche Beiträge auf, was eine umfassendere Untersuchung nötig macht.

Im *ersten Kapitel* mit dem Titel „Ausgangssituation“ führen wir zunächst alle Begriffe ein, die wir im weiteren Verlauf der Arbeit benötigen werden. Wir gehen hierbei kurz auf die $1-1$ Korrespondenz zwischen algebraischen Kurven und Funktionenkörpern ein. Wir definieren die Riemann-Hurwitz-Formel in der für uns passenden Form, also von der Perspektive algebraischer Kurven. Wir setzen allerdings beim Leser Grundkenntnisse zu Funktionenkörpern und zur Verzweigungstheorie algebraischer Kurven voraus. Daher werden wir in diesem Zusammenhang die meisten Begriffe nur informell definieren und an der gegebenen Stelle auf die entsprechende Literatur ([Sti09] und

[Har93]) verweisen. Wir führen in diesem Kapitel außerdem den für die gesamte Arbeit zugrunde liegenden lokalen Ring R und alle relevanten Gruppen vom GL(3)− Typ ein, sodass wir in den folgenden Kapiteln mit der Berechnung der Verzweigungszahlen beginnen können. Wir verwenden hierbei das, in der Arbeit von Ernst-Ulrich Gekeler ([Gek14]) festgehaltene, Resultat, dass Verzweigung höchstens an den Spitzen und elliptischen Punkten auftritt.

Das *zweite Kapitel* zur Spitzenverzweigung handelt von der Berechung der, zur Auswertung der Riemann-Hurwitz-Formel nötigen, Verzweigungszahlen a_Q an den Spitzen $\xi(\infty) = Q$. Dies ist der schwierigste und zugleich umfangreichste Teil der Masterarbeit. Die Berechnung der Verzweigungszahlen an den Spitzen (also den Punkten über $j = \infty$) kann auf ein Eigenwertproblem über dem lokalen Ring R zurückgeführt werden. Insbesondere in der Situation $d \equiv 0 \mod 2$, wobei d den Grad unseres Primpolynoms p bezeichnet, treten zusätzliche Komplikationen bei der Lösung des Eigenwertproblems auf.

Das *dritte Kapitel*, welches mit „Verzweigung an den elliptischen Punkten“ tituliert ist, beschäftigt sich mit der Bestimmung der Verzweigungszahlen an den elliptischen Punkten (also den Punkten über $j = 0$). Dies ist a priori durch eine vergleichbare Rechnung wie im zweiten Kapitel möglich. Es hat sich jedoch im Verlaufe der Arbeit herausgestellt, dass man mit gruppentheoretischen Überlegungen völlig auf Matrizenrechnungen verzichtet kann. Wir wollen uns hierbei darauf beschränken, die zweite, elegantere Vorgehensweise zu präsentieren und dem Leser die ermüdende Matrizenrechnung vorzuenthalten.

Im *vierten Kapitel* mit dem Titel „Berechnung des Geschlechts“ werden wir nun die Ergebnisse der beiden vorangehenden Kapitel benutzen, um die Riemann-Hurwitz-Formel auf die Galois-Überlagerung $X(p^r) \longrightarrow X_0(p^r)$ anzuwenden. Am Ende des Kapitels erhalten wir, nach einigen umfangreichen Äquivalenzumformungen durch Einsetzen aller Kardinalitäten und Verzweigungszahlen in Termen von der Zahl der Körperelemente q, dem Grad d unseres Primpolynoms p und dem Exponenten r, eine komplizierte, aber explizite, Formel für das Geschlecht $g(X_0(p^r))$. Dies ermöglicht eine computergestützte Auswertung der Formel zum Auffinden von interessanten Geschlechtern g, was eine Verbesserung der untere Schranke für die maximale Zahl $N_q(g)$ von rationalen Punkten einer Kurve über dem endlichen Köper $\mathbb{F}_{q^3}$ verspricht. Außerdem werden wir am Ende des Kapitels das asymptotische Verhalten der Geschlechtsformel $g_0(q, d, r)$ diskutieren. An dieser Stelle werden wir im lokalen Fall eine, lediglich von der Zahl der Körperelemente q abhängige, untere Schranke für den Grenzwert $\limsup_{r\to\infty} \frac{|\{P\in\overline{X_0(p^r)}\}|P \text{ ist rational über } \mathbb{F}_{q^3}\}|}{g(\overline{X_0(p^r)})}$ angeben; hierbei bezeichnet $\overline{X_0(p^r)}$ eine, bezüglich einer Primstelle $\mathfrak{q} \neq \mathfrak{p}$ reduzierte, Kurve mit gleichem Geschlecht.

Im *fünften Kapitel* geben wir abschließend noch die globale Formel für das Geschlecht der Kurve $X_0(N)$ an; hier ist also N von der allgemeinen Form $N = \prod_{i=1}^{s} p_i^{r_i}$. Die Formel wurde mit Hilfe des Computeralgebrasystems GAP (Groups, Algorithms, Programming) implementiert. Wir werden aber bei den meisten Ergebnissen nur Beweisskizzen angeben. Die globale Formel wird detailliert in der Masterarbeit von David Geis [Gei15] entwickelt.

Literatur
Wie bereits erwähnt, basiert die vorliegende Masterarbeit zum einen hinsichtlich des thematischen Hintergrundes und zum anderen bezüglich der Lösungsstrategie bei der betrachteten Problemstellung hauptsächlich auf der Veröffentlichung von Ernst-Ulrich Gekeler [Gek14]. Darüber hinaus diente das Buch „Algebraic Function Fields and Codes“ von Henning Stichtenoth [Sti09] als einführendes Werk, um sich mit den wichtigsten Begriffen und dem nötigen Vokabular zu Funktionenkörpern vertraut zu machen.
Wir lösen uns jedoch bei der weiteren Vorgehensweise von der Perspektive der Funktionenkörper und nehmen die völlig analoge Betrachtungsweise der entsprechenden algebraischen Kurven (siehe [Har93]) ein.

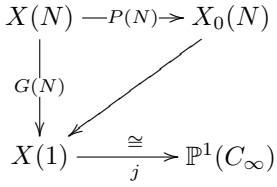
Notation
Wir bezeichnen mit $|X|$ die Kardinalität der endlichen Menge X. Wir verwenden im weiteren Verlauf die floor-Funktion $\lfloor x \rfloor := \max\{k \in \mathbb{Z} | k \leq x\}$. Außerdem bedeutet $a|b$, dass a ein Teiler von b ist. Ferner verwenden wir die übliche Schreibweise $a \equiv b \mod n \Leftrightarrow (a-b) \in n\mathbb{Z}$ für Kongruenz und eine entsprechende Notation für kongruente Elemente in Ringen.
Außerdem ist für eine Untergruppe $H \subset G$ die Menge der linken Nebenklassen gegeben durch $G/H = \{gH | g \in G\}$ und die Menge der rechten Nebenklassen schreiben wir wie üblich als $H\backslash G = \{Hg | g \in G\}$.
Operiert die Gruppe G von links auf der Menge X, so bezeichnet $G\backslash X$ die Menge der Bahnen und entprechend X/G die Menge der Bahnen für eine Rechtsoperation der Gruppe. Wie gewöhnlich bezeichnet $G_x = \{\sigma \in G | \sigma(x) = x\}$ die Fixgruppe eines Punktes $x \in X$. Um eine möglichst kompakte Notation für die auftretenden Rechnungen zu erhalten, schreiben wir auch $\{\xi\}$ für ein Repräsentantensystem von linken Nebenklassen G/H (analog für rechte Nebenklassen), mit entsprechendem Verweis auf die zugrunde liegende Gruppe G und Untergruppe H. In diesem Zusammenhang sollte sich dem Leser erschließen, dass durch Ausdrücke der Form $\xi = 1$ bzw. $\xi \neq 1$ ein Vergleich mit dem neutralen Element der Faktorgruppe G/H (falls $H \subset G$ Normalteiler ist) gemeint ist.
Darüber hinaus verwenden wir die folgenden, in der algebraischen Zahlentheorie üblichen, Bezeichnungen:

- $R^{m \times n}$ = Menge der $m \times n-$ Matrizen mit Koeffizienten aus R.
- $\mathbb{F}_q$ = Körper mit q Elementen der Charakteristik p.
- $A = \mathbb{F}_q[T]$ ist der Polynomring in der Unbestimmten T über dem Körper $\mathbb{F}_q$.
- $K_\infty = \mathbb{F}_q((\frac{1}{T}))$ ist der Körper der formalen Laurentreihen über $\mathbb{F}_q$, wobei $K := \mathbb{F}_q(T)$ den Körper der rationalen Funktionen über $\mathbb{F}_q$ bezeichnet.
- $R(N)$ bezeichnet den Restklassenring $A/(N)$, wobei $A \ni N = \prod_{i=1}^{s} p_i^{r_i}$ mit paarweise verschiedenen Primpolynomen p_i vom Grad d_i. Wir setzen in der gesamten Masterarbeit stets ein nichtkonstantes N voraus.
- $C_\infty = \hat{K}_\infty$ ist die Komplettierung des algebraischen Abschlusses von K_∞

Die weiteren Bezeichnungen werden im Verlaufe der Arbeit an der jeweils passenden Stelle eingeführt.

1 Ausgangssituation

Wir betrachten die folgende Überlagerung von projektiven, zusammenhängenden, glatten algebraischen Kurven über C_∞. Dabei sind $P(N)$ bzw. $G(N)$ die unten beschriebenen Galois-Gruppen der zugehörigen verzweigten Überlagerungen.



Die Kurven $X(N), X_0(N), X(1)$ sind hierbei die Modulkurven für dünn besetzte Drinfeld A- Moduln mit Parametern $r = 3$ und $k = 2$, welche in der Arbeit von Ernst-Ulrich Gekeler [Gek14] in Theorem A eingeführt werden. Für eine explizite Konstruktion der Kurven $X(N), X_0(N)$ verweisen wir auf [Gek14]. Die abkürzende Schreibweise bleibt nun für die gesamte weitere Arbeit gültig.

- Die Kurve $X(1)$ wird durch eine $j-$ Invariante mit der projektiven Geraden $\mathbb{P}^1(C_\infty)$ identifiziert.
- Wie bereits in der Einführung erwähnt, bezeichnet die Gruppe $Z \xrightarrow{\cong} \mathbb{F}_q^*$ die Gruppe der $\mathbb{F}_q$- wertigen Skalarmatrizen. Z ist also das Bild von $\mathbb{F}_q^*$ in $\mathrm{GL}(3, R(N))$:

$$Z = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} | a \in \mathbb{F}_q^* \right\}, \tag{1}$$

  mit $|Z| = q - 1$.
- Die Überlagerung $X(N) \longrightarrow X(1)$ ist galoissch mit Galois-Gruppe $G(N) = \mathrm{Gal}(X(N)|X(1))$, wobei $G(N)$ gegeben ist durch

$$G(N) := \{g \in GL(3, R(N)) | \det(g) \in \mathbb{F}_q^*\}/Z. \tag{2}$$

- Die Überlagerung $X(N) \longrightarrow X_0(N)$ ist galoissch mit Galois-Gruppe $P(N) = \mathrm{Gal}(X(N)|X_0(N))$, wobei $P(N)$ gegeben ist durch

$$P(N) := \left\{ g = \left(\begin{array}{c|cc} p_{11} & p_{12} & p_{13} \\ \hline 0 & & \\ 0 & & A \end{array} \right) | p_{11} \cdot \det(A) \in \mathbb{F}_q^*; A \in R(N)^{2\times 2}; p_{11}, p_{12}, p_{13} \in R(N) \right\} /Z \tag{3}$$

- Wir wollen an dieser Stelle darauf hinweisen, dass die Überlagerung $X_0(N) \longrightarrow X(1)$ nicht galoissch ist.

Unser Ziel ist die explizite Berechung des Geschlechtes $g(X_0(N))$ für ein beliebiges, nichtkonstantes $N \in A$. Da die Überlagerung der Kurven $X_0(N) \longrightarrow X(1)$ nicht galoissch ist (!), kann die Riemann-Hurwitz-Formel zur Berechnung des Geschlechts nicht direkt angewendet werden. Stattdessen werden wir die Riemann-Hurwitz-Formel auf die galoisschen Überlagerungen
$X(N) \longrightarrow X(1) \cong \mathbb{P}^1(C_\infty)$ und $X(N) \longrightarrow X_0(N)$ mit Galois-Gruppen $G(N)$ und $P(N)$ anwenden; über diesen Umweg wird es uns gelingen, das Geschlecht der Kurve $X_0(N)$ zu berechnen.
Das Hauptergebnis der vorliegenden Masterarbeit ist die explizite Berechnung des Geschlechts der Kurve $X_0(N)$ für einen primären Führer $N = p^r$, d.h die Angabe des Geschlechts $g(X_0(N))$ in Abhängigkeit von der Zahl der Körperelemente q des endlichen Körpers $\mathbb{F}_q$, dem Grad d des zugrunde liegenden Primpolynoms p und dem Exponenten r.

Bemerkung 1.

1. Wenn wir in der vorliegenden Masterarbeit von „Kurven“ sprechen, so meinen wir, wie in der Einleitung schon erwähnt, stets projektive, zusammenhängende, glatte algebraische Kurven über einem algebraisch abgeschlossenen Körper der Charakteristik $p > 0$.

2. Wir kommen im Verlaufe der Arbeit immer wieder auf die Berechnung der Geschlechter von Kurven in obigem Sinne zurück. Sprechen wir also von der Berechung von $g(X(N))$ bzw. $g(X_0(N))$, so meinen wir die Berechnung der Geschlechter der zugehörigen Funktionenkörper $C_\infty(X(N))/C_\infty$ bzw. $C_\infty(X_0(N))/C_\infty$ im Sinne der Definition des Geschlechts für Funktionenkörper (siehe [Sti09], Definition 1.4.15).

3. Wir verwenden stets die wohlbekannte Tatsache, dass die Funktionenkörper $C_\infty(X(N))/C_\infty$ und $C_\infty(X_0(N))/C_\infty$ die algebraischen Entsprechungen der geometrischen Objekte $X(N)/X(1)$ und $X_0(N)/X(1)$ sind.

Theorem 1. *(Riemann-Hurwitz-Formel)*
Sei $\phi : X \longrightarrow Y$ eine verzweigte, galoissche Überlagerung von Kurven über einem algebraisch abgeschlossenen Körper K der Charakteristik $p > 0$ mit Galois-Gruppe G. Für einen K-wertigen Punkt x von X bezeichnet $\mathcal{O}_{X,x}$ den zugehörigen lokalen Ring, π_x ein uniformisierendes Element bei x, also einen Erzeuger des maximalen Ideals $\mathfrak{m}_x$ im lokalen Ring $\mathcal{O}_{X,x}$ bei x und $G_x \subset G$ die Fixgruppe von x. Es sei

$$G_{x,i} := \{\sigma \in G |\ \sigma \text{ operiert trivial mod } \pi_x^{i+1}\}.$$

Dann gilt

$$G_x = G_{x,0} \supset G_{x,1} \supset ... \supset G_{x,r} = \{1\}$$

für hinreichend großes r. Diese absteigende Kette von normalen Untergruppen heißt Verzweigungsfiltrierung von G. Für ein Element $1 \neq \sigma \in G_x$ sei

$$i_x(\sigma) := sup\{i | \sigma \in G_{x,i}\} + 1;$$

wir nennen i_x die Verzweigungsfunktion. Damit definieren wir die Verzweigungszahl in x für die obige Verzweigungsfiltrierung durch

$$a_x := \sum_{1 \neq \sigma \in G_x} i_x(\sigma).$$

Es bezeichnen $g(X), g(Y)$ die Geschlechter der Kurven X, Y. Entsprechend ist $e(X) = 2 - 2g(X)$ und $e(Y) = 2 - 2g(Y)$ die Euler-Charakteristik der jeweiligen Kurve. Dann gilt

$$e(X) = |G|e(Y) - \sum_{x \in X} a_x. \tag{4}$$

Beweis. Eine für unsere Zwecke geeignete Formulierung vom Standpunkt der Kurven findet man etwa in [Har93] Korollar 2.4. Nimmt man dagegen die Perspektive der Funktionenkörper ein, so verweisen wir den Leser auf das Werk von Stichtenoth [Sti09]. □

Bemerkung 2. Wir halten fest, dass die folgende Kette von Äquivalenzen gilt:

$$a_x \neq 0 \Leftrightarrow G_x \neq \{1\} \Leftrightarrow \ \phi \text{ ist verzweigt in } x. \tag{5}$$

Es ist ϕ also genau dann verzweigt in x, falls $a_x \neq 0$ gilt. Darüber hinaus ist $G_{x,0}/G_{x,1}$ eine zyklische Gruppe mit einer zu p koprimen Ordnung und $G_{x,1}$ ist $p-$ Gruppe.

Definition 1.

1. Die Überlagerung $\phi : X \longrightarrow Y$ heißt moderat verzweigt in $x \in X$, falls $G_{x,2}$ die triviale Gruppe ist. Dann ist $G_{x,1}$ die eindeutig bestimmte $p-$ Sylow-Untergruppe von G_x.

2. Wir nennen die Überlagerung $\phi : X \longrightarrow Y$ zahm verzweigt in $x \in X$, falls $G_{x,1}$ schon trivial ist.

Bemerkung 3. Wir übernehmen hierbei die folgenden Feststellungen bezüglich der Verzweigung der Kurven $X(N) \longrightarrow X(1)$ und $X(N) \longrightarrow X_0(N)$ als Grundlage für unsere weitere Vorgehensweise, wie in Theorem A ([Gek14]) der Arbeit von Ernst-Ulrich Gekeler festgehalten wurde.

- Die Definition von $G_{x,i}$ ist unabhängig von der Wahl des Erzeugers π_x von $\mathfrak{m}_x$. Weiter ist $G_{x,i} \subset G$ Normalteiler für alle i.

- Wir bezeichnen die Abbildung $X(N) \longrightarrow X(1)$ mit ϕ. Ein Punkt $x \in X(N)$ heißt elliptisch, falls $j(\phi(x)) = 0$ gilt. Ein Punkt $x \in X(N)$ wird Spitze genannt, falls $j(\phi(x)) = \infty$ gilt.

- Die galoissche Überlagerung $X(N) \longrightarrow X_0(N)$ ist höchstens an Punkten $x \in X(N)$ mit $j(\phi(x)) = 0$ (elliptische Punkte) und an Punkten $x \in X(N)$ mit $j(\phi(x)) = \infty$ (Spitzen) verzweigt.

- Die Verzweigung an den elliptischen Punkten ist zahm. In den Spitzen liegt eine moderate Verzweigung vor.

Wir erinnern daran, dass das Hauptziel dieser Masterarbeit die Berechnung des Geschlechts der Kurve $X_0(N)$ im lokalen Fall ist, also die Bestimmung von $g(X_0(N))$ in der Situation $\underline{N = p^r}$.

Lokale Notation. Wir verwenden im weiteren Verlauf der Arbeit gegebenenfalls die Schreibweise $e_0(p^r)$ für die Eulercharakteristik der Kurve $X_0(p^r)$ und $g_0(p^r)$ für das Geschlecht der Kurve $X_0(p^r)$. Mit Ausnahme von dem Kapitel, welches den globalen Fall abhandelt, ist für den restlichen Teil der Arbeit die nachfolgende Notation gültig:

- $p \in A$ ist ein Primpolynom.
- $R := A/(p^r)$ wird vermöge der kanonischen Verknüpfungen von Restklassen zu einem endlichen, kommutativen Ring mit 1- Element.
- Es bezeichne $d := \deg(p)$ den Grad des Primpolynoms $p \in A$.
- Darüberhinaus verwenden wir die allgemein übliche Schreibweise für die Einheitengruppe: $R^* := \{a \in R \mid \exists b \in R : b \cdot a = a \cdot b = 1\}$.

An dieser Stelle weisen wir darauf hin, dass der Exponent r unseres Primpolynoms p nichts mit dem Rang r bei der Berechnung des Geschlechts $X^{r,r-1}(N)$ aus der Arbeit von Ernst-Ulrich Gekeler zu tun hat. Dies sollte beim Verweisen auf diese Arbeit mit der entsprechenden Notation beim Leser nicht für Verwirrung sorgen.

Bemerkung 4. Der von uns betrachtete Ring $R = A/(p^r)$ ist ein lokaler Ring mit maximalem Ideal $(p)/(p^r)$. Das maximale Ideal bezeichnen wir mit $\mathfrak{p}$. Wir schreiben dann „π“ für einen Erzeuger des maximalen Ideals in R, also $\mathfrak{p} = (\pi)$. Solange wir über dem festen Ring R arbeiten, schreiben wir stets „$\mathfrak{p}^i$ “ mit $0 \leq i \leq r$ für Potenzen unseres maximalen Ideals $\mathfrak{p}$ im Restklassenring R.

Bemerkung 5. Wir verfügen über eine „verstümmelte “ Bewertung auf $R = A/(p^r)$ vermöge

$$\begin{aligned} v_{\mathfrak{p}} : R &\longrightarrow \{0, ..., r\} \\ f &\mapsto \sup\{i | f \in \mathfrak{p}^i\} \end{aligned}$$

mit den Eigenschaften

$$v_{\mathfrak{p}}(a \cdot b) = \min\{v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b), r\} \tag{6}$$
$$v_{\mathfrak{p}}(a) = r \ \Leftrightarrow a = 0 \tag{7}$$
$$v_{\mathfrak{p}}(a + b) \geq \min\{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)\}. \tag{8}$$

Damit bemerken wir insbesondere wegen $R = R^* \dot{\cup} \mathfrak{p}$:

$$v_{\mathfrak{p}}(a) = 0 \Leftrightarrow a \in R^* \tag{9}$$
$$v_{\mathfrak{p}}(a) > 0 \Leftrightarrow a \in \mathfrak{p}. \tag{10}$$

Ist $f \in R$ beliebig, so lässt sich f in der Form $f = u\pi^k$ mit $0 \leq k \leq r$ und $u \in R^*$ schreiben.

Bemerkung 6. Wir nutzen im Laufe der Arbeit wie folgt aus, dass wir über einem lokalen Ring R mit maximalem Ideal $\mathfrak{p}$ arbeiten: Bei nahezu allen Rechnungen gehen wir zum Restklassenkörper $R/\mathfrak{p} \xrightarrow{\cong} \mathbb{F}_{q^d}$ über und folgern mit bekannten Tatsachen über endlichen Körpern unsere Ergebnisse. Dann verwenden wir je nach Situation eine geeignete Version des Lemmas von Hensel (Lemma 1) oder des Lemmas von Nakayama (Lemma 2), um die Resultate über $R/\mathfrak{p}$ nach R zu liften.

Lemma 1. *(Lemma von Hensel für vollständige lokale Ringe) Sei R ein vollständiger, lokaler Ring mit maximalem Ideal $\mathfrak{p}$ und sei $R/\mathfrak{p}$ der entsprechende Restklassenkörper. Für $f(T) \in R[T]$ sei $\overline{f}(T) \in (R/\mathfrak{p})[T]$ das Bild von f unter dem Ringhomomorphismus $R[T] \longrightarrow (R/\mathfrak{p})[T]$, induziert durch den kanonischen Ringepimorphismus $R \twoheadrightarrow R/\mathfrak{p}$. Falls sich $\overline{f}$ faktorisieren lässt zu*

$\overline{f}(T) = \overline{g}(T)\overline{h}(T)$ mit teilerfremden, normierten Polynomen $\overline{g}(T), \overline{h}(T) \in (R/\mathfrak{p})[T]$, so existieren eindeutig bestimmte, normierte Polynome $g(T), h(T) \in R[T]$, sodass $\overline{g}(T), \overline{h}(T)$ gerade die Bilder von $g(T), h(T)$ unter dem Ringhomomorphismus $R[T] \longrightarrow (R/\mathfrak{p})[T]$ sind.

Beweis. Wir verweisen auf die entsprechende Literatur zur kommutativen Algebra. Einen Beweis der für uns passenden Version des Lemmas von Hensel findet man etwa im Manuskript [Hoc12]. □

Korollar 1. *Das Lemma von Hensel in der Form von Lemma 1 gilt für den im Rahmen dieser Masterarbeit betrachteten Ring R.*

Beweis. Der hier betrachtete Ring R ist nach Bemerkung 4 lokal mit maximalem Ideal $\mathfrak{p}$. Unser Ring R ist offenbar auch vollständig, da $\mathfrak{p}^r = \{0\}$ gilt. □

Lemma 2. *(Lemma von Nakayama für lokale Ringe) Sei R ein lokaler Ring, $\mathfrak{p}$ sein maximales Ideal und $R/\mathfrak{p}$ der Restklassenkörper. Weiter sei M ein endlich erzeugter $R-$ Modul. Dann ist $\{x_1, ..., x_n\}$ ein minimales Erzeugendensystem für den $R-$ Modul M genau dann, wenn $\{\overline{x_1}, ..., \overline{x_n}\}$ eine Basis des $R/\mathfrak{p}$-Vektorraums $M/\mathfrak{p}$ ist.*

Beweis. Diese Version des Lemmas von Nakayama ist etwa im Vorlesungsskript von Dr. Thomas Markwig bewiesen ([Mar13] NAK 3). Eine geeignete Darstellung des Lemmas von Nakayama und eine gute Übersicht zu Henselschen Ringen findet man aber auch in [Eis04]. □

Beobachtung 1. Wir konstatieren: Für die kurzen exakten Sequenzen

$$0 \longrightarrow \mathfrak{p}^{j+1} \longrightarrow \mathfrak{p}^j \longrightarrow \mathfrak{p}^j/\mathfrak{p}^{j+1} \longrightarrow 0 \tag{11}$$

von endlichdimensionalen $\mathbb{F}_q-$ Vektorräumen gilt für alle $0 \leq j \leq r-1$:

$$|\mathfrak{p}^j| = q^{d(r-j)}.$$

Dies sehen wir wie folgt ein: Es gilt $|\mathfrak{p}^j/\mathfrak{p}^{j+1}| = |R/\mathfrak{p}| = |A/p| = |\mathbb{F}_{q^d}|$ für alle $0 \leq j \leq r-1$. Für $j = 0$ ergibt sich die kurze exakte Sequenz von $\mathbb{F}_q-$ Vektorräumen

$$0 \longrightarrow \mathfrak{p} \longrightarrow R \longrightarrow R/\mathfrak{p} \longrightarrow 0. \tag{12}$$

Wir wenden die Formel für die alternierende Summe der Dimensionen von Vektorräumen auf die kurze exakte Sequenz (12) an und erhalten $\dim_{\mathbb{F}_q}\mathfrak{p} = d(r-1)$. Somit ergibt sich: $|\mathfrak{p}| = q^{d(r-1)}$. Es lassen sich nun iterativ die Größen der $\mathfrak{p}^j$ für alle $2 \leq j \leq r-1$ aus der kurzen exakten Sequenz (11) bestimmen. Wir vermerken:

$$|R^*| = q^{d(r-1)}(q^d - 1). \tag{13}$$

Lemma 3. *Für eine Gruppe $H \subset GL(n, \mathbb{F}_q)$ sind äquivalent:*
(i) H ist zyklisch mit $|H| = q^n - 1$.
(ii) H ist Bild einer Einbettung $\iota_B : \mathbb{F}_{q^n}^* \hookrightarrow GL(n, \mathbb{F}_q)$. Dabei ist B eine Basis des $\mathbb{F}_q-$ Vektorraums $\mathbb{F}_{q^n}$ und $\iota_B(\lambda)$ ist die Darstellungsmatrix der Multiplikation mit λ in $\mathbb{F}_{q^n}$ bezüglich der Basis B.

Beweis. (i) $\Rightarrow$ (ii). Es sei $H =< a >$. Zunächst ist zu zeigen, dass das Minimalpolynom $\mu_a(T) \in \mathbb{F}_q[T]$ von a über $\mathbb{F}_q$ irreduzibel vom Grad n ist, also mit dem charakteristischen Polynom χ_a von a übereinstimmt. Dies ist ausführlich in [Gei15] begründet.
Es sei λ ein Eigenwert von a. Wir bemerken nun, dass das charakteristische Polynom der Darstellungsmatrix m_λ, welche die Multiplikation mit dem Element $\lambda \in \mathbb{F}_{q^n} \cong \mathbb{F}_q[T]/(\chi_a)$ bezüglich einer Basis B des $\mathbb{F}_q-$ Vektorraums $\mathbb{F}_{q^n}$ realisiert, mit χ_a übereinstimmt. Also sind a und m_λ konjugiert: $\exists A \in \mathrm{GL}(n, \mathbb{F}_q)$ mit $a = Am_\lambda A^{-1}$. Damit ist λ bereits eine primitive $(q^n - 1)-$te Einheitswurzel. Vermöge der Abbildung $\lambda \longmapsto Am_\lambda A^{-1}$ ist dann eine Einbettung $\mathbb{F}_{q^n}^* \longrightarrow \mathrm{GL}(n, \mathbb{F}_q)$, wie gewünscht, gegeben.
(ii) $\Rightarrow$ (i). Die ist klar wegen der Invarianz der Ordnung unter dem injektiven Gruppenhomomorphismus $\iota_B : \mathbb{F}_{q^n}^* \to \mathrm{GL}(n, \mathbb{F}_q)$. □

Bemerkung 7. Eine Gruppe, die den äquivalenten Eigenschaften von Lemma 3 genügt, heißt Cartan-Gruppe. Je zwei Cartan-Gruppen sind konjugiert. Im Folgenden werden wir Cartan-Gruppen in $\mathrm{GL}(n, \mathbb{F}_q)$ verwenden mit $n = 2$ oder $n = 3$. Für solche n wählen wir jeweils eine feste Cartan-Gruppe, die wir mit Car(2) bzw. Car(3) bezeichnen.

Wir benötigen für die weiteren Rechnungen die Gruppen

$$Z = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} | a \in \mathbb{F}_q^* \right\}, \tag{14}$$

$$G = \{g \in \mathrm{GL}(3, R) | \det(g) \in \mathbb{F}_q^*\}/Z, \tag{15}$$

$$P = \left\{ \left(\begin{array}{c|cc} p_{11} & p_{12} & p_{13} \\ \hline 0 & & \\ 0 & & A \end{array} \right) | p_{11} \cdot \det(A) \in \mathbb{F}_q^*; A \in R^{2\times 2};\ p_{11}, p_{12}, p_{13} \in R \right\} /Z, \tag{16}$$

$$G_\infty = \left\{ \left(\begin{array}{c|cc} a & b & c \\ \hline 0 & & \\ 0 & & \gamma \end{array} \right) | a \in \mathbb{F}_q^*;\ b, c \in R; \gamma \in \mathrm{Car}(2) \right\} /Z, \tag{17}$$

$$\text{mit } |G_\infty| = \frac{(q-1)(q^2-1)q^{2dr}}{q-1} = (q^2-1)q^{2dr}, \tag{18}$$

$$U = \left\{ \left(\begin{array}{c|cc} a & b & c \\ \hline 0 & a & 0 \\ 0 & 0 & a \end{array} \right) | a \in \mathbb{F}_q^*;\ b, c \in R \right\} /Z,\ \text{die } p-\text{Sylowuntergruppe von } G_\infty, \tag{19}$$

$$\text{mit } |U| = \frac{(q-1)q^{2dr}}{q-1} = q^{2dr}, \tag{20}$$

$$C = \mathrm{Car}(3)/Z \text{ mit } |C| = \frac{q^3-1}{q-1} = q^2 + q + 1. \tag{21}$$

Die Cartan-Gruppen $\mathrm{Car}(2), \mathrm{Car}(3)$ wurden in Lemma 3 und der anschließenden Bemerkung eingeführt. Obwohl wir gemäß Lemma 3 nicht an die Auswahl eines Minimalpolynoms gebunden sind, werden wir für die Rechnungen im zweiten Kapitel die Cartan-Gruppe Car(2) explizit durch die Wahl eines Minimalpolynoms realisieren. Wegen der Lokalität von R nutzen wir im weiteren Verlauf stets aus, dass $\det(A) \in R^* \Leftrightarrow \det(A) \not\equiv 0 \mod \mathfrak{p}$ gilt.

Bei der Gruppe $G = G(N)$ handelt es sich um die Galois-Gruppe der Überlagerung $X(N) \longrightarrow X(1)$ im lokalen Fall, also für primären Führer $N = p^r$. Ebenso ist die Gruppe $P = P(N)$ hierbei die Galois-Gruppe der Überlagerung $X(N) \longrightarrow X_0(N)$ in der lokalen Situation $N = p^r$. Weiter gilt: Es gibt einen Punkt „∞“ von $X(N)$ über $j = \infty$ mit Fixgruppe G_∞, wie oben definiert (siehe [Gek14] Theorem 8.2) und einen Punkt „e“ von $X(N)$ über $j = 0$ mit Fixgruppe C. Da $G = G(p^r)$ transitiv auf den Spitzen (den Punkten über $j = \infty$) mit Fixgruppe G_∞ und auf den elliptischen Punkten (den Punkten über $j = 0$) mit Fixgruppe C von $X(p^r)$ operiert, gilt: $|\{\text{Spitzen von } X(p^r)\}| = \frac{|G|}{|G_\infty|}$ und $|\{\text{elliptische Punkte von } X(p^r)\}| = \frac{|G|}{|C|}$.

Lemma 4. *Für* $P = \left\{ \left(\begin{array}{c|cc} p_{11} & p_{12} & p_{13} \\ \hline 0 & & \\ 0 & & A \end{array} \right) | p_{11} \cdot det(A) \in \mathbb{F}_q^*; A \in R^{2\times 2};\ p_{11}, p_{12}, p_{13} \in R \right\} / Z \subset$ *G ergibt sich:* $|P| = (q^{2d} - 1)(q^d - 1)q^{3dr}q^{3d(r-1)}$.

Beweis. Wir bestimmen zunächst $|\{(p_{11}, A)|p_{11} \cdot \det(A) \in R^*\}|$. Hierzu reduzieren wir modulo $\mathfrak{p}$. Bekannte Resultate für $\mathrm{GL}(2, \mathbb{F}_{q^d})$ liefern uns unmittelbar: $|\{A|\det(A) \in \mathbb{F}_{q^d}^*\}| = (q^{2d} - 1)(q^{2d} - q^d) = q^d(q^{2d} - 1)(q^d - 1)$. Wir liften nun wieder nach R, indem wir jeden Parameter in der $2 \times 2-$ Untermatrix A mit $|\mathfrak{p}|$ multiplizieren.
Wir haben dann für p_{11} gerade $q - 1$ Wahlmöglichkeiten, sodass die stärkere Determinantenbedingung $p_{11} \cdot \det(A) \in \mathbb{F}_q^*$ erfüllt ist. Die Parameter $p_{12}, p_{13} \in R$ sind, unabhängig von der Bedingung, frei wählbar. Wir erhalten somit nach „Herausdividieren“ der Gruppe Z

$$|P| = \frac{(q-1)q^d(q^{2d} - 1)(q^d - 1)q^{4d(r-1)}q^{2dr}}{q-1} = (q^{2d} - 1)(q^d - 1)q^{3dr}q^{3d(r-1)}. \tag{22}$$

□

Definition 2. Aus Gründen der Zweckmäßigkeit für die weiteren Rechnungen definieren wir den projektiven Raum über unserem lokalen Ring R wie folgt:

$$\mathbb{P}^n(R) := \{(a_0, ..., a_n) \in R^{n+1} : \sum_{i=0}^{n} Ra_i = R\}/\sim, \tag{23}$$

wobei

$$(a_0, ...a_n) \sim (b_0, ..., b_n) \tag{24}$$
$$:\Leftrightarrow \exists u \in R^* : ua_i = b_i\ \forall i = 0, ..., n. \tag{25}$$
$$\tag{26}$$

Lemma 5. *Für unsere lokale Situation erhalten wir:*

$$|\mathbb{P}^n(R)| = q^{dn(r-1)}(q^{dn} + q^{d(n-1)} + ... + 1) =: \epsilon_n \tag{27}$$

Wir extrahieren nun die folgenden Fälle:

1. $\mathbb{P}^1(R)$ *ist die „projektive Gerade“ über* R*, mit* $\epsilon_1 = (q^d+1)q^{d(r-1)}$.

2. $\mathbb{P}^2(R)$ *ist die „projektive Ebene“ über* R*, mit* $\epsilon_2 = (q^{2d}+q^d+1)q^{2d(r-1)}$.

Beweis. Die Bedingung an $(a_0,...,a_n)$ in (23) bedeutet: Wenigstens eines der a_i $(0 \leq i \leq n)$ liegt in R^*. Setzen wir dasjenige a_i mit kleinstem Index i vermöge (24) auf 1, so ergibt sich:

$$\begin{aligned}
\mathrm{RS}(1) &:= (1, b_1, b_2, ..., b_n), \quad b_i \in R \ \ \forall\ 1 \leq i \leq n && (28)\\
\mathrm{RS}(2) &:= (c_1, 1, b_2, ..., b_n), \quad c_1 \in \mathfrak{p},\ b_i \in R \ \ \forall\ 2 \leq i \leq n && (29)\\
&\qquad\qquad \text{usw.} && (30)\\
\mathrm{RS}(n) &:= (c_1, c_2, ..., c_n, 1), \quad c_i \in \mathfrak{p} \ \ \forall\ 1 \leq i \leq n. && (31)
\end{aligned}$$

Wir summieren nun über das disjunkte System von Repräsentanten auf und erhalten

$$\sum_{i=0}^{n-1} q^{dr(n-i)} q^{di(r-1)} = \frac{q^{dn(r-1)}(q^{d(n+1)}-1)}{q^d-1} = |\mathbb{P}^n(R)|. \tag{32}$$

□

Bemerkung 8. Wir benötigen die folgenden Identifikationen.

$$\begin{array}{ccccc}
G/P & \xrightarrow{\cong} & \tilde{G}/\tilde{P} & \xrightarrow{\cong} & \mathbb{P}^2(R) \\
& \nwarrow^{\cong} \quad \swarrow_{\cong} & & & \\
& G'/P' & & &
\end{array}$$

Hierbei ist $\tilde{G} = \mathrm{GL}(3,R)$ und entsprechend $\tilde{G} \supset \tilde{P} = \{\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}\}$. Außerdem ist $G' = \{g \in \mathrm{GL}(3,R) | \det(g) \in \mathbb{F}_q^*\}$ und somit $P' = \tilde{P} \cap G'$. Die Bijektionen der Nebenklassenmengen sind kanonisch definiert und die rechte Abbildung wird in folgendem Lemma beschrieben.

Lemma 6. *Wir identifizieren die Menge der linken Nebenklassen* G/P *mit der „projektive Ebene“ über* R*, wie folgt:*

$$\varphi : G/P \xrightarrow{\cong} \tilde{G}/\tilde{P} \xrightarrow{\cong} \mathbb{P}^2(R) \tag{33}$$

$$\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \mapsto (a:b:c) \tag{34}$$

Dabei stehen an den mit $*$ *gekennzeichneten Stellen beliebige Einträge aus* R.

Beweis. 1. Wohldefiniertheit.
Sei $\left(\begin{smallmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{smallmatrix}\right)$ in der gleichen Nebenklasse wie $\left(\begin{smallmatrix} a & * & * \\ b & * & * \\ c & * & * \end{smallmatrix}\right)$. Dann existiert ein $\left(\begin{smallmatrix} p_{11} & * & * \\ 0 & * & * \\ 0 & * & * \end{smallmatrix}\right) \in \tilde{P}$ mit:

$$\begin{pmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{pmatrix} = \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \cdot \begin{pmatrix} p_{11} & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix} = \begin{pmatrix} p_{11}a & * & * \\ p_{11}b & * & * \\ p_{11}c & * & * \end{pmatrix} \tag{35}$$

Also erhalten wir offensichtlich:

$$\varphi(\begin{pmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{pmatrix}) = (p_{11}a : p_{11}b : p_{11}c) \overset{p_{11} \in R^*}{=} (a : b : c).$$

Damit ist die Abbildung φ wohldefiniert.

2. Injektivität.
Es sei

$$\varphi(\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix}) = \varphi(\begin{pmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{pmatrix}). \tag{36}$$

Dies ist äquivalent zu

$$(a : b : c) = (a' : b' : c') \tag{37}$$
$$\Leftrightarrow \exists u \in R^* : (a', b', c') = u(a, b, c). \tag{38}$$

Damit ergibt sich aber offenbar:

$$\begin{pmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{pmatrix} = \begin{pmatrix} ua & * & * \\ ub & * & * \\ uc & * & * \end{pmatrix} = \begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \cdot \begin{pmatrix} u & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix},$$

wobei $\left(\begin{smallmatrix} u & * & * \\ 0 & * & * \\ 0 & * & * \end{smallmatrix}\right) \in \tilde{P}$ gewählt wird. Also gilt schon $\left(\begin{smallmatrix} a' & * & * \\ b' & * & * \\ c' & * & * \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & * & * \\ b & * & * \\ c & * & * \end{smallmatrix}\right) \in \tilde{G}/\tilde{P}$.

3. Surjektivität.
Offensichtlich finden wir zu jedem Tupel $(a : b : c) \in \mathbb{P}^2(R)$ eine passendes Element $\left(\begin{smallmatrix} a & * & * \\ b & * & * \\ c & * & * \end{smallmatrix}\right) \in \tilde{G}/\tilde{P}$, indem wir unsere frei wählbaren Parameter geeignet wählen.

□

Bemerkung 9.

1. Eine analoge Identifikation ist auch mit rechten Nebenklassen $P\backslash G$ möglich; dies ist bei der Bestimmung der Verzweigungszahlen an den elliptischen Punkten von Bedeutung.

2. Wegen der obigen Isomorphie ergibt sich $|G| = \epsilon_2|P|$. Dies folgt auch direkt durch Vergleich von G mit $\mathrm{SL}(3, R)$, wie in [Gek14] 11.1.2 zu sehen ist. Die Strategie, zunächst die Kardinalität von P zu bestimmen, war jedoch hier eingängiger, weil das Prinzip der Reduktion modulo des maximalen Ideals $\mathfrak{p}$ von R mit anschließender Liftung, welches grundlegend für die gesamte Arbeit ist, zur Anwendung kommt.

2 Spitzenverzweigung

Wir wollen im nachfolgenden Abschnitt die Verzweigung der Überlagerung $X(p^r) \longrightarrow X_0(p^r)$ an den Spitzen berechnen. Mit den Parametern $r = 3$ und $k = 2$ gemäß der Ausarbeitung von Ernst-Ulrich Gekeler existiert eine ausgezeichnete Spitze von $X(p^r)$, die wir mit „∞“ bezeichnen, sodass die Fixgruppe von ∞ in der verzweigten Überlagerung $X(p^r) \longrightarrow X(1)$ gerade die Gruppe $G_\infty = G_\infty(p^r)$, wie zuvor definiert, ist. Dies rechtfertigt die Schreibweise G_∞ ([Gek14] Theorem 8.2 mit anschließender Bemerkung). Diese Resultate sind Grundlage der weiteren Rechnungen.

Bemerkung 10. Da $G(p^r)$ transitiv auf den Spitzen von $X(p^r)$ mit Fixgruppe G_∞ operiert, erhalten wir:

1. Die Spitzen von $X(p^r)$ stehen in kanonischer Bijektion zu G/G_∞. Ist $\{\xi\}$ ein Repräsentantensystem für G/G_∞, so gilt:

$$G/G_\infty \xrightarrow{\cong} \{\text{Spitzen von } \mathrm{X}(p^r)\}. \tag{39}$$
$$\xi \longmapsto \xi(\infty) \tag{40}$$

2. Die Spitzen von $X_0(p^r)$ stehen in Bijektion zu $P\backslash G/G_\infty$, also

$$P\backslash G/G_\infty \xrightarrow{\cong} \{\text{Spitzen von } \mathrm{X}_0(p^r)\}. \tag{41}$$

Bemerkung 11. Ist $\{x\}$ ein Repräsentantensystem für G/P und $\{y\}$ ein Repräsentantensystem für P/G_∞, so ist $\{\xi\} = \{x \cdot y\}$ ein Repräsentantensystem für G/G_∞.

$$U \subset \underbrace{\overbrace{G_\infty \subset}^{\{y\}} P \overbrace{\subset G}^{\{x\}}}_{\{\xi\}=\{x\cdot y\}} \tag{42}$$

Lemma 7. *Ist $\{\xi\}$ ein Repräsentantensystem für G/G_∞ so ist ${}^{\xi}G_\infty := \xi G_\infty \xi^{-1}$ Fixgruppe zur Spitze $\xi(\infty) = Q$; mit $\xi = x \cdot y$ ist dann ${}^{\xi}G_\infty = {}^{x}({}^{y}G_\infty)$. Für die Verzweigungszahlen a_Q von Q der Überlagerung $X(p^r) \longrightarrow X_0(p^r)$ an den Spitzen erhalten wir:*

$$a_Q = |P \cap {}^{\xi}G_\infty| + |P \cap {}^{\xi}U| - 2. \tag{43}$$

Beweis. Wir müssen zeigen: ${}^{\xi}G_\infty = G_Q$.
Es sei $g \in G$. Dann gilt:

$$g(Q) = Q \tag{44}$$
$$\Leftrightarrow g(\xi(\infty)) = \xi(\infty) \tag{45}$$
$$\Leftrightarrow \xi^{-1} g \xi(\infty) = \infty \tag{46}$$
$$\Leftrightarrow \xi^{-1} g \xi \in G_\infty \tag{47}$$
$$\Leftrightarrow g\xi \in \xi G_\infty \tag{48}$$
$$\Leftrightarrow g \in \xi G_\infty \xi^{-1}, \tag{49}$$

also erhalten wir $G_Q = {}^{\xi}G_\infty$. Ebenso leicht rechnen wir unter Beachtung von Bemerkung 11 nach, dass

$$\begin{aligned} {}^{\xi}G_\infty &= \xi G_\infty \xi^{-1} && (50)\\ &= (x \cdot y) G_\infty (x \cdot y)^{-1} && (51)\\ &= (x \cdot y) G_\infty (y^{-1} \cdot x^{-1}) && (52)\\ &= x(y\ G_\infty y^{-1}) x^{-1} && (53)\\ &= {}^{x}({}^{y}G_\infty) && (54) \end{aligned}$$

gilt. Die Formel für die Verzweigungszahlen a_Q erhalten wir unmittelbar aus der Verzweigungsfiltrierung bei $j = \infty$. Es liegt eine moderate Verzweigung vor, d.h. die zweite Verzweigungsgruppe $G_{\infty,2}$ ist trivial (siehe [Gek14] (8.3.2) und Theorem 8.4). □

Für nachfolgende Rechnungen und Lemmata ignorieren wir bei der Schreibweise von Elementen aus $U,\ G_\infty,\ P \subset G$ für gewöhnlich die Gruppe Z. Hierbei meinen wir aber immer die entsprechende Nebenklasse.

Bemerkung 12. Wir können die, in Bemerkung 7 eingeführte, Cartan-Gruppe Car(2) durch die Wahl eines Minimalpolynoms $f(T) \in \mathbb{F}_q[T]$ explizit konstruieren. Hierzu wählen wir $f(T) = T^2 - KT - L \in \mathbb{F}_q[T]$ irreduzibel. Damit hat die Cartan-Gruppe Car(2) die Gestalt

$$\mathrm{Car}(2) = \{ \begin{pmatrix} \gamma_{11} & L\gamma_{21} \\ \gamma_{21} & \gamma_{11} + K\gamma_{21} \end{pmatrix} | \gamma_{11}, \gamma_{21} \in \mathbb{F}_q, (\gamma_{11}, \gamma_{21}) \neq (0,0) \}, \tag{55}$$

wobei wir für $\mathrm{char}(\mathbb{F}_q) \neq 2$ annehmen können, dass $K = 0$ gilt.

Beobachtung 2. Ein $h \in {}^{y}G_\infty = yG_\infty y^{-1}$ ist von der Form $\left(\begin{array}{c|cc} a & b' & c' \\ \hline 0 & & \\ 0 & & \gamma' \end{array}\right)$ mit $a \in \mathbb{F}_q^*$ und $b', c' \in R$. Hierbei läuft $\gamma' \in \mathrm{GL}(2,R)$ durch eine konjugierte Gruppe von $\mathrm{Car}(2) \subset \mathrm{GL}(2,R)$. Man überzeugt sich leicht, dass

$$\gamma'_{11} = \gamma_{11} + \frac{a_{12}a_{22} - a_{21}a_{11}L - a_{21}a_{12}K}{\det(A)}\gamma_{21} =: \gamma_{11} + \alpha_1\gamma_{21} \tag{56}$$

$$\gamma'_{22} = \gamma_{11} + \frac{-a_{12}a_{22} + a_{21}a_{11}L + a_{11}a_{22}K}{\det(A)}\gamma_{21} =: \gamma_{11} + \alpha_2\gamma_{21} \tag{57}$$

$$\gamma'_{12} = \frac{La_{11}^2 - a_{12}^2 + a_{11}a_{12}K}{\det(A)}\gamma_{21} =: \beta_1\gamma_{21} \tag{58}$$

$$\gamma'_{21} = \frac{a_{22}^2 - a_{21}^2L - a_{22}a_{21}K}{\det(A)}\gamma_{21} =: \beta_2\gamma_{21} \tag{59}$$

gilt. Außerdem erhalten wir

$$b' = \frac{1}{\det(A)}\Big\{a(a_{21}p_{13} - a_{22}p_{12}) + p_{11}(a_{22}b - a_{21}c) + \gamma_{11}(a_{22}p_{12} - a_{21}p_{13}) \tag{60}$$

$$+ \gamma_{21}(a_{22}p_{13} - a_{21}p_{13}K - a_{21}p_{12}L)\Big\} \tag{61}$$

$$c' = \frac{1}{\det(A)}\Big\{a(a_{12}p_{12} - a_{11}p_{13}) - p_{11}(a_{11}c - a_{12}b) + \gamma_{11}(a_{11}p_{13} - a_{12}p_{12}) \tag{62}$$

$$+ \gamma_{21}(-a_{12}p_{13} + a_{11}p_{13}K + a_{11}p_{12}L)\Big\}; \tag{63}$$

hierbei sind die Elemente aus $\{y\}$ von der Form $\left(\begin{smallmatrix} p_{11} & p_{12} & p_{13} \\ 0 & a_{11} & a_{12} \\ 0 & a_{21} & a_{22} \end{smallmatrix}\right)$. Wir erhalten die Gestalt von ${}^yG_\infty$ unmittelbar durch Nachrechnen.

$$\begin{array}{ccc} {}^y\mathrm{Car}(2) & \hookrightarrow & \mathrm{GL}(2,R) \\ & \searrow^{\kappa} & \downarrow \\ & & \mathrm{GL}(2,R/\mathfrak{p}) \end{array}$$

Wir bemerken, dass ${}^y\mathrm{Car}(2)$ vermöge κ wieder auf eine Cartan-Gruppe in $\mathrm{GL}(2,R/\mathfrak{p})$ projiziert wird.

Bemerkung 13. Es erweist sich im Nachfolgenden als zweckmäßig, das folgende Repräsentantensystem $\{x\}$ für G/P zu fixieren.

$$\{x\} = \{\begin{pmatrix} 1 & 0 & 0 \\ v & 1 & 0 \\ w & 0 & 1 \end{pmatrix} | v,w \in R\} \dot\cup \{\begin{pmatrix} u & 1 & 0 \\ 1 & 0 & 0 \\ w & 0 & 1 \end{pmatrix} | u \in \mathfrak{p}, w \in R\} \dot\cup \{\begin{pmatrix} u & 1 & 0 \\ v & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} | u,v \in \mathfrak{p}\} \tag{64}$$

$$=: \mathrm{RS}(1) \dot\cup \mathrm{RS}(2) \dot\cup \mathrm{RS}(3) \tag{65}$$

Um eine korrekte Notation zu gewährleisten, erweist es sich außerdem als sinnvoll, ein beliebiges Repräsentantensystem Y für P/G_∞ zu fixieren. Insbesondere schreiben wir im Nachfolgenden auch kurz „$x \in \mathrm{RS}$“, falls $x \in \mathrm{RS}(1) \dot\cup \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$. Außerdem bezeichnen wir mit „y“ im Nachfolgenden stets Elemente aus unserem Repräsentantensystem Y.

Bemerkung 14. Wir verwenden die disjunkte Aufteilung $G_\infty = G_\infty^{(1)} \dot\cup G_\infty^{(2)}$, wobei

$$G_\infty^{(1)} = \left\{ \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & 0 \\ 0 & 0 & \gamma_{11} \end{pmatrix} \right\} \tag{66}$$

$$G_\infty^{(2)} = G_\infty \setminus G_\infty^{(1)} \tag{67}$$

Außerdem sei $x \in \mathrm{RS}$ und $y \in Y$. Dann erhalten wir mit dieser Aufteilung:

$$|P \cap {}^x({}^yG_\infty)| = \begin{cases} |G_\infty| & \text{, falls} \quad x = 1 \\ |P \cap {}^x({}^yG_\infty^{(1)})| + |P \cap {}^x({}^yG_\infty^{(2)})| & \text{, falls} \quad x \neq 1 \end{cases}. \tag{68}$$

Gilt $x = 1$, so ist die Behauptung wegen ${}^yG_\infty \subset P$ klar. Wir werden im Nachfolgenden feststellen, dass die Kardinalität des Schnittes $P \cap {}^x({}^yG_\infty^{(1)})$ unabhängig von y ist. Außerdem werden wir zeigen, dass $P \cap {}^x({}^yG_\infty^{(2)})$ für $x \neq 1$ nur bei geradem Grad d unseres Primpolynoms p nichtleer ist.

Lemma 8. *Wir erhalten* $|P \cap {}^x({}^yG_\infty^{(1)})| = |P \cap {}^xG_\infty^{(1)}|$. *Für* $g \in G_\infty^{(1)}$ *können wir also* $y = 1$ *annehmen und gemäß Satz* 1 *abzählen.*

Beweis. Ist $g \in G_\infty^{(1)}$, so erhalten wir für ${}^yg$ mit den Bezeichnungen wie in Beobachtung 2 unmittelbar $\gamma' = \gamma$. Man überzeugt sich nun mit der expliziten Gestalt von b', c' aus Beobachtung 2 und mit einem genaueren Blick auf die Abzählargumente aus Satz 1, dass der Schnitt $P \cap {}^x({}^yG_\infty^{(1)})$ lediglich von x abhängt, wir also $y = 1$ setzen können. □

Satz 1. *Für* $x \in RS(1)$ *mit den Koordinaten* v, w *sei* $k(v,w) := min\{v_\mathfrak{p}(v), v_\mathfrak{p}(w)\}$. *Dann erhalten wir für den Beitrag* $|P \cap {}^xG_\infty^{(1)}|$*:*

$$|P \cap {}^xG_\infty^{(1)}| = \begin{cases} (q-1)q^{dr} & , falls \quad k = 0 \\ q^{d(r+2k)} & , falls \quad 1 \leq k < \frac{r}{2} \\ q^{2dr} & , falls \quad \frac{r}{2} \leq k \leq r-1 \\ (q^2-1)q^{2dr} & , falls \quad k = r \\ (q-1)q^{dr} & , falls \quad x \in RS(2) \dot\cup RS(3). \end{cases} \tag{69}$$

Beweis. 1. Ist $1 \neq x \in \mathrm{RS}(1)$, so erhalten wir mit $g = \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & 0 \\ 0 & 0 & \gamma_{11} \end{pmatrix} \in G_\infty^{(1)}$

$$ {}^xg \in P \Leftrightarrow \begin{pmatrix} v \\ w \end{pmatrix} \text{ ist Eigenvektor von } \gamma \text{ zum Eigenwert } a' := a - (vb + wc) \tag{70}$$

$$\Leftrightarrow (a - (vb + wc) - \gamma) \cdot \begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ in } R^2, \tag{71}$$

wie eine leichte Rechnung zeigt.

a) Es gelte $\binom{v}{w} \not\equiv \binom{0}{0} \mod \mathfrak{p}$. Es sei O.B.d.A. $v \not\equiv 0 \mod \mathfrak{p}$. Wir suchen eine Lösung der Gleichungen

$$(a' - \gamma_{11})v = \gamma_{12}w \tag{72}$$

$$(a' - \gamma_{11})w = \gamma_{21}v \tag{73}$$

Wegen $\gamma_{12} = \gamma_{21} = 0$ ergibt sich unmittelbar $\gamma = \left(\begin{smallmatrix} a' & 0 \\ 0 & a' \end{smallmatrix}\right)$. Unsere Cartan-Matrix γ ist nun durch $a' \in \mathbb{F}_q^*$ eindeutig festgelegt. Mit $a \in \mathbb{F}_q^*$ können wir $c \in R$ frei wählen, denn wegen $v \not\equiv 0 \mod \mathfrak{p}$ erhalten wir

$$-wc - vb = a' - a \in \mathbb{F}_q^* \tag{74}$$

$$\Leftrightarrow b = -\frac{wc + a' - a}{v}. \tag{75}$$

Also b ist dann bei Wahl von $a \in \mathbb{F}_q^*$ und $c \in R$ festgelegt. Wir erhalten folglich nach „Herausdividieren“ der Gruppe Z: $|P \cap {}^xG_\infty^{(1)}| = \frac{(q-1)^2q^{dr}}{q-1} = (q-1)q^{dr}$.

b) Es sei nun $\binom{v}{w} \equiv \binom{0}{0} \mod \mathfrak{p}$. Wir schreiben $v = u_1\pi^k$ und $w = u_2\pi^l$ mit $u_1, u_2 \in R^*$ und $k, l > 0$. Wegen $\gamma_{12} = \gamma_{21} = 0$ nehmen unsere Eigenwertgleichungen die Gestalt

$$(a' - \gamma_{11}) \equiv 0 \mod \mathfrak{p}^{r-k} \tag{76}$$
$$(a' - \gamma_{11}) \equiv 0 \mod \mathfrak{p}^{r-l} \tag{77}$$

an. Wir nehmen nun O.B.d.A an, dass $v_\mathfrak{p}(v) = k \leq l$. Damit genügt es die erste Kongruenz zu betrachten:

$$a' \equiv \gamma_{11} \mod \mathfrak{p}^{r-k} \tag{78}$$
$$\Leftrightarrow a - (vb + wc) \equiv \gamma_{11} \mod \mathfrak{p}^{r-k}, \tag{79}$$

also ergibt sich $\gamma = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$. Wir erhalten demnach die Gleichung

$$vb + wc \equiv 0 \mod \mathfrak{p}^{r-k} \tag{80}$$
$$\Leftrightarrow p^k(u_1 b + u_2 c p^{l-k}) \equiv 0 \mod \mathfrak{p}^{r-k}. \tag{81}$$

Wir wählen nun $c \in R$ beliebig und unterscheiden Fälle für $k = v_\mathfrak{p}(v) \leq v_\mathfrak{p}(w)$.

i. Es sei zunächst $1 \leq k < \frac{r}{2}$.

$$\Leftrightarrow u_1 b + u_2 c p^{l-k} \equiv 0 \mod \mathfrak{p}^{r-2k} \tag{82}$$
$$\Leftrightarrow b \equiv -\frac{u_2}{u_1} c p^{l-k} \mod \mathfrak{p}^{r-2k} \tag{83}$$

Offenbar gibt es nach obiger Kongruenz nach Wahl von $c \in R$ für b gemäß Beobachtung 1 gerade $q^{d(r-(r-2k))} = q^{2dk}$ Wahlmöglichkeiten. Also ergibt sich $|P \cap {}^x G_\infty^{(1)}| = \frac{(q-1)q^{dr}q^{2dk}}{q-1} = q^{d(r+2k)}$.

ii. Es sei nun $\frac{r}{2} \leq k \leq r-1$. Wir erhalten nach obiger Kongruenz keine Einschränkung für b. Also folgt unmittelbar $|P \cap {}^x G_\infty^{(1)}| = \frac{(q-1)q^{2dr}}{q-1} = q^{2dr}$.

In beiden Fällen wurde beim Abzählen wie gehabt zum Schluss die Gruppe $Z \cong \mathbb{F}_q^*$ berücksichtigt.

2. Ist $x \in \mathrm{RS}(2) \cup \mathrm{RS}(3)$ und $g \in G_\infty^{(1)}$ wie zuvor, so folgt

$${}^x g \in P \Leftrightarrow b = 0 \text{ und } \gamma_{21} = 0 \tag{84}$$

nach einer leichten Rechnung. Wir können den Parameter c aus R frei wählen; bei der Wahl einer diagonalen Cartan-Matrix γ, sowie $a \in \mathbb{F}_q^*$ erhalten wir also nach „Herausdividieren“ der Gruppe Z: $|P \cap {}^x({}^y G_\infty^{(1)})| = \frac{(q-1)^2 q^{dr}}{q-1} = (q-1)q^{dr}$.

□

Beobachtung 3. Gilt $d \equiv 1 \mod 2$, so ist $P \cap {}^x({}^y G_\infty^{(2)}) = \emptyset$. Dies machen wir uns wie folgt klar: Ist $g \in G_\infty^{(2)}$, so überzeugt man sich mit $h = {}^y g$ leicht, dass die Konjugation mit $1 \neq x \in \mathrm{RS}(1)$

auf das Eigenwertproblem (70) mit Parametern $\gamma' \in {}^{y}\mathrm{Car}(2)$ und $\tilde{a} := a - (vb' + wc')$ führt. Eine einfache Rechnung zeigt, dass γ und γ' das gleiche charakteristische Polynom haben. Dann ist aber $\tilde{a}$ Nullstelle des irreduziblen (weil γ nichtdiagonal ist!) charakteristischen Polynoms $\chi_{\gamma'} = \chi_\gamma$. Es ergibt sich nach Reduktion modulo $\mathfrak{p}$

$$\chi_\gamma(\tilde{a}) \equiv 0 \mod \mathfrak{p} \tag{85}$$

$$\rightsquigarrow \tilde{a} \in \mathbb{F}_{q^2}, \tag{86}$$

mit $\mathbb{F}_{q^2} \subset \mathbb{F}_{q^d}$. Dann muss aber für den Grad d unseres Primpolynoms p offenbar schon gelten:

$$d \equiv 0 \mod 2. \tag{87}$$

Die Konjugation mit $x \in \mathrm{RS}(2) \cup \mathrm{RS}(3)$ liefert die Bedingung $\beta_2 = 0$, wie in Satz 2 zu sehen sein wird. Die Rechnungen in Lemma 10 werden zeigen, dass diese Bedingung für $d \equiv 1 \mod 2$ nicht erfüllt sein kann. Um eine übersichtliche Darstellung zu erreichen, verwenden wir daher im Nachfolgenden die Funktion

$$\omega(d) = \begin{cases} 0 & \text{, falls} \quad d \equiv 1 \mod 2 \\ 1 & \text{, falls} \quad d \equiv 0 \mod 2. \end{cases} \tag{88}$$

Satz 2. *Es sei $x \in RS$ wie zuvor. Außerdem sei $y \in Y$. Darüber hinaus benötigen wir die, in Beobachtung 2 eingeführte, Hilfsgröße β_2. Es gilt mit $x_0 \in RS(2) \dot\cup RS(3)$:*

$$\sum_{1 \neq x \in RS} \sum_{y \in Y} |P \cap {}^{x}({}^{y}G_\infty^{(2)})| = \omega(d)\Big\{ |Y| \cdot \sum_{1 \neq x \in RS(1)} |P \cap {}^{x}G_\infty^{(2)}| \tag{89}$$

$$+ |\{RS(2) \dot\cup RS(3)\}| \cdot |\{y \in Y | \beta_2 = 0\}| \cdot |P \cap {}^{x_0}({}^{y}G_\infty^{(2)})|\Big\} \tag{90}$$

$$= \omega(d)\Big\{ |Y| \cdot 2|R^*| q(q-1)q^{dr} \tag{91}$$

$$+ |\{RS(2) \dot\cup RS(3)\}| \cdot |\{y \in Y | \beta_2 = 0\}| \cdot q(q-1)q^{dr}\Big\}. \tag{92}$$

Beweis. Wir betrachten nun $g \in G_\infty^{(2)}$. Ist $h = {}^{y}g$ von der Form $\left(\begin{array}{c|cc} a & b' & c' \\ \hline 0 & & \\ 0 & \multicolumn{2}{c}{\gamma'} \end{array}\right)$ mit $a \in \mathbb{F}_q$, $b', c' \in R$ und ${}^{y}\gamma = \gamma' \in \mathrm{GL}(2, R)$, so führt die Konjugation mit $1 \neq x \in \mathrm{RS}(1)$ auf das Eigenwertproblem (70) mit Parametern a, b', c' und γ'. Gilt nun $\binom{v}{w} \equiv \binom{0}{0} \mod \mathfrak{p}$, so hat das Eigenwertproblem keine Lösung, denn das Argument nach (79) zeigt, dass eine Lösung nur für ein diagonales γ' existiert, d.h. für $g \in G_\infty^{(1)}$. Die $R/\mathfrak{p}$- linear unabhängigen Eigenvektoren $\binom{v_1}{w_1}, \binom{v_2}{w_2} \not\equiv 0 \mod \mathfrak{p}$ spannen Eigenräume $< \binom{v_1}{w_1} >_{R/\mathfrak{p}}$ und $< \binom{v_2}{w_2} >_{R/\mathfrak{p}}$ über $R/\mathfrak{p}$ auf, welche sich unter Beachtung der für uns passenden Version des Lemmas von Nakayama (Lemma 2) zu zwei Eigenrichtungen nach R liften, sodass wir gerade

$$|\{(v, w) \in R^2 |\ P \cap {}^{x}({}^{y}G_\infty^{(2)}) \neq \emptyset\}| = 2|R^*| \tag{93}$$

erhalten. Wir können nun wie in Satz 1 mit $\binom{v}{w} \not\equiv \binom{0}{0} \mod \mathfrak{p}$ annehmen, dass O.B.d.A $v \not\equiv 0 \mod \mathfrak{p}$ gilt. Dann erhalten wir analog zu (74) und (75):

$$-wc' - vb' = a' - a \in \mathbb{F}_q^* \tag{94}$$

$$\Leftrightarrow b' = -\frac{wc' + a' - a}{v}. \tag{95}$$

Also ist dann b' bei Wahl von $a \in \mathbb{F}_q^*$ durch $c' \in R$ festgelegt. Wie man sich mit Beobachtung 2 leicht überzeugt, stehen die Parameter b', c' über invertierbare Einträge aus P so mit den Parametern b, c in Zusammenhang, dass wir bei Auflösen nach b', c' auch stets nach b, c auflösen können. Daher tritt der Beitrag $|P \cap {}^x({}^yG_\infty^{(2)})|$ für $1 \neq x \in \mathrm{RS}(1)$ unabhängig von y auf. Bei Wahl einer nichtdiagonalen Cartan-Matrix γ, $a \in \mathbb{F}_q^*$ und $c \in R$ ergibt sich nach „Herausdividieren“ der Gruppe Z und Aufsummieren über alle $1 \neq x \in \mathrm{RS}(1)$, für welche der Schnitt $|P \cap {}^x({}^yG_\infty^{(2)})|$ nichtleer ist, sowie alle (frei wählbaren) $y \in Y$, also die Behauptung.
Es sei wie gehabt $h = {}^yg$ mit $g \in G_\infty^{(2)}$. Die Konjugation mit $x_0 \in \mathrm{RS}(2) \cup \mathrm{RS}(3)$ liefert

$${}^{x_0}h \in P \Leftrightarrow b' = 0 \text{ und } \gamma'_{21} = 0 \tag{96}$$

$$\Leftrightarrow b' = 0 \text{ und } (\gamma_{21} = 0) \vee (\beta_2 = 0) \tag{97}$$

$$\overset{g \in G_\infty^{(2)}}{\Leftrightarrow} b' = 0 \text{ und } \beta_2 = 0 \tag{98}$$

Der Beitrag $|P \cap {}^x({}^yG_\infty^{(2)})|$ tritt also unabhängig von $x_0 \in \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$ auf. Die explizite Gleichung für $b' = 0$ zeigt, dass wir einen der Parameter b oder c aus R frei wählen und bei der Wahl einer nichtdiagonalen Cartan-Matrix γ von $g \in G_\infty^{(2)}$, sowie $a \in \mathbb{F}_q^*$, stets nach dem jeweils anderen Parameter auflösen können. Damit erhalten wir also wiederum nach „Herausdividieren“ der Gruppe Z und Aufsummieren über alle (frei wählbaren) $x_0 \in \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$, sowie alle zulässigen $y \in Y$ (d.h. diejenigen y, für welche die Hilfsgröße β_2 verschwindet!), die Behauptung. □

Wir müssen nun noch die Anzahl der Nebenklassen $x \in \mathrm{RS}(1)$ abzählen, für welche die Werte aus Satz 1 auftreten.

Lemma 9. *Es sei $x \in RS(1)$ mit Parametern v, w wie gehabt. Für die Hilfsgröße $n_k := |\{(v, w) \in R^2 |\ min\{v_\mathfrak{p}(v), v_\mathfrak{p}(w)\} = k\}|$ ergibt sich dann:*

$$n_k = \begin{cases} 1 & , falls \quad k = r \\ (q^{2d} - 1)q^{2d(r-k-1)} & , falls \quad k \neq r \end{cases}. \tag{99}$$

Beweis. Wir müssen $n_k = \{(u\pi^k, \alpha) | \alpha \in \mathfrak{p}^k\} \dot\cup \{(\alpha, u\pi^k) | \alpha \in \mathfrak{p}^{k+1}\}$ abzählen. Mit der Überlegung

$u\pi^k = u'\pi^k \Leftrightarrow u - u' \equiv 0 \mod \mathfrak{p}^{r-k}$ für $k \neq r$, ergibt sich:

$$\begin{aligned} n_k &= |\mathfrak{p}^k| \cdot |R^*/\mathfrak{p}^{r-k}| + |\mathfrak{p}^{k+1}| \cdot |R^*/\mathfrak{p}^{r-k}| && (100)\\ &= |R^*/\mathfrak{p}^{r-k}| \cdot (|\mathfrak{p}^k| + |\mathfrak{p}^{k+1}|) && (101)\\ &= \frac{q^{dr} - q^{d(r-1)}}{q^{d(r-(r-k))}} \cdot (q^{d(r-k)} + q^{d(r-k-1)}) && (102)\\ &= (q^{d(r-k)} - q^{d(r-k-1)}) \cdot (q^{d(r-k)} + q^{d(r-k-1)}) && (103)\\ &= q^{2d(r-k)} - q^{2d(r-k-1)} && (104)\\ &= (q^{2d} - 1)q^{2d(r-k-1)}. && (105) \end{aligned}$$

Für $k = r$ gilt offenbar $v_\mathfrak{p}(v) = v_\mathfrak{p}(w) = r \Leftrightarrow (v, w) = (0, 0)$, also $n_k = 1$. Man kann sich zur Bestätigung der obigen Formel auch leicht davon überzeugen, dass $\sum_{k=0}^{r} n_k = q^{2dr}$ gilt. □

Korollar 2. *Wir werten nun als Zwischenfazit die Summe* $\mathcal{S} := \sum_{k=0}^{r-1} n_k(|P \cap {}^xG_\infty^{(1)}| + |P \cap {}^xU|)$ *aus:*

$$\begin{aligned} \mathcal{S} &= \sum_{k=0}^{r-1} n_k(|P \cap {}^xG_\infty^{(1)}| + |P \cap {}^xU|) && (106)\\ &= (q + 2\lfloor\frac{r}{2}\rfloor)(q^{2d} - 1)q^{d(3r-2)} + 2q^{2dr}(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)} - 1). && (107) \end{aligned}$$

Beweis. Es erweist sich trotz der Fallunterscheidung aus Satz 1 für $k(v, w) = \min\{v_\mathfrak{p}(v), v_\mathfrak{p}(w)\}$ als zweckmäßig, unsere Summe in die folgenden Bereiche von k aufzuteilen. Wir entnehmen die Werte für die jeweilige Verzweigung aus Satz 1.

1. $k = 0$ liefert den Beitrag $(q^{2d} - 1)q^{d(3r-2)+1}$.

2. Für $1 \leq k \leq \lfloor\frac{r}{2}\rfloor$ erhalten wir durch Auswerten der Summe den Beitrag $2\lfloor\frac{r}{2}\rfloor(q^{2d}-1)q^{d(3r-2)}$.

3. Im Bereich $\lfloor\frac{r}{2}\rfloor + 1 \leq k \leq r - 1$ ergibt sich der Wert $2q^{2dr}(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)} - 1)$.

Aufsummieren der Einzelbeiträge in den jeweiligen Bereichen für k liefert den Wert für $\mathcal{S}$. □

Wir erinnern den Leser daran, dass der Schnitt $P \cap {}^{x_0}({}^yG_\infty^{(2)})$ bei Konjugation mit $x_0 \in \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$ genau dann nichtleer ist, wenn die in Beobachtung 2 eingeführte Hilfsgröße β_2 verschwindet. Wir zählen im nachfolgenden Lemma nun die Anzahl aller Nebenklassen $y \in Y$ ab, sodass die Bedingung $\beta_2 = 0$ erfüllt ist.

Lemma 10. *Es sei* $\tilde{y} = \begin{pmatrix} p_{\tilde{1}1} & p_{\tilde{1}2} & p_{\tilde{1}3} \\ 0 & a_{\tilde{1}1} & a_{\tilde{1}2} \\ 0 & a_{\tilde{2}1} & a_{\tilde{2}2} \end{pmatrix} \in P$. *Es sei weiterhin* $\tilde{\gamma} \in {}^{\tilde{y}}Car(2)$ *konjugiert zu einem fest gewählten* $\gamma \in Car(2)$ *(mit Minimalpolynom* $f(T) = T^2 - KT - L \in \mathbb{F}_q[T]$*). Mit* $\tilde{\gamma_{21}} = \frac{a_{\tilde{2}2}{}^2 - a_{\tilde{2}1}{}^2 L - a_{\tilde{2}2}a_{\tilde{2}1}K}{det(\tilde{A})}\gamma_{21} =: \tilde{\beta}_2\gamma_{21}$, *erhalten wir*

$$|\{\tilde{y} \in P | \tilde{\beta}_2 = 0\}| = 2(q^d - 1)^2 q^d q^{3d(r-1)} q^{2dr}. \quad (108)$$

Dann gibt es

$$\frac{2(q^d-1)^2q^dq^{3d(r-1)}}{q^2-1} \tag{109}$$

Nebenklassen $y \in Y$ mit $\beta_2 = 0$ (Hierbei gelten die Bezeichnungen aus Beobachtung 2).

Beweis. Wir führen eine Fallunterscheidung nach der Charakteristik durch. Wie schon bemerkt, können wir für $\underline{\text{char}(\mathbb{F}_q) \neq 2}$ annehmen, dass $K = 0$ gilt. Wir nehmen O.B.d.A an, dass $a_{12}, a_{21} \in R^*$ und formen unsere Bedingung $\tilde{\beta}_2 = 0$ geeignet um. Um eine übersichtliche Notation zu erhalten, ignorieren wir für die nachfolgenden Rechnungen die Tilde bei den so gekennzeichneten Einträgen $p_{\tilde{ij}}, a_{\tilde{ij}}$ aus P.

$$\tilde{\beta}_2 = 0 \tag{110}$$
$$\Leftrightarrow a_{22}^2 - a_{21}^2 L = 0 \tag{111}$$
$$\Leftrightarrow a_{22}^2 = a_{21}^2 L \tag{112}$$
$$\Leftrightarrow a_{22} = \pm a_{21}\sqrt{L} \tag{113}$$

Wir reduzieren modulo $\mathfrak{p}$ und können unsere Rechnung auf die Bestimmung von $|\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & \pm\sqrt{L}a_{21} \end{pmatrix}\}|\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & \pm\sqrt{L}a_{21} \end{pmatrix} \in \mathbb{F}_{q^d}^*\}|$ beschränken. Offensichtlich haben wir $a_{12}, a_{21} \in \mathbb{F}_{q^d}^*$ und einen frei wählbaren Parameter $a_{11} \in \mathbb{F}_{q^d}$. Wir liften nun nach R, indem wir jeden der Parameter a_{11}, a_{12}, a_{21} mit $|\mathfrak{p}|$ multiplizieren.
Wir haben dann für p_{11} gerade $q-1$ Wahlmöglichkeiten, sodass die stärkere Determinantenbedingung erfüllt ist. Die Parameter $p_{12}, p_{13} \in R$ sind, unabhängig von der Bedingung, frei wählbar. Wir erhalten somit nach „Herausdividieren“ der Gruppe Z

$$|\{\tilde{y} \in P | \beta_2 = 0\}| = \frac{2(q-1)(q^d-1)^2q^dq^{3d(r-1)}q^{2dr}}{q-1} = 2(q^d-1)^2q^dq^{3d(r-1)}q^{2dr}. \tag{114}$$

G_∞ operiert kanonisch von links auf der Menge $\{\tilde{y} \in P | \tilde{\beta}_2 = 0\}$. Mit $|G_\infty| = (q^2-1)q^{2dr}$ ergibt sich dann die Behauptung.
Es gelte nun $\underline{\text{char}(\mathbb{F}_q) = 2}$. Wir können wiederum O.B.d.A annehmen, dass $a_{12}, a_{21} \in R^*$ gilt und formen unsere Bedingung $\tilde{\beta}_2 = 0$ geeignet um.

$$\tilde{\beta}_2 = 0 \tag{115}$$
$$\Leftrightarrow a_{22}^2 - a_{21}^2 L - a_{22}a_{21}K = 0 \tag{116}$$
$$\overset{a_{21} \in R^*}{\Leftrightarrow} (\frac{a_{22}}{a_{21}})^2 + \frac{a_{22}}{a_{21}}K + L = 0 \tag{117}$$
$$\Leftrightarrow \frac{a_{22}}{a_{21}} \in \mathbb{F}_{q^2} \tag{118}$$

Wir bemerken, dass das irreduzible Polynom $f(T) = T^2 - KT - L \in \mathbb{F}_q[T]$ in $\mathbb{F}_{q^2}$ zwei einfache Nullstellen λ, λ' hat (endliche Körper sind vollkommen). Folglich gilt:

$$(a_{22} = \lambda a_{21}) \vee (a_{22} = \lambda' a_{21}) \tag{119}$$

Also gibt es bei Wahl von a_{21} genau zwei Möglichkeiten für die Wahl von a_{22}. Damit können wir vorgehen wie in der Situation $\mathrm{char}(\mathbb{F}_q) \neq 2$. □

Beobachtung 4. Mit den Werten $|P \cap {}^{x}({}^{y}G_\infty)|$ und $|P \cap {}^{x}({}^{y}U)|$ (siehe Satz 1 und Satz 2) und den Hilfsgrößen können wir nun die Verzweigungszahlen a_Q an den Spitzen $\xi(\infty) = Q$ angeben und durch Aufsummieren den Beitrag zur Riemann-Hurwitz-Formel

$$\sum_{x \in \mathrm{RS}} \sum_{y \in Y} |P \cap {}^{x}({}^{y}G_\infty)| + |P \cap {}^{x}({}^{y}U)| =: \Gamma$$

berechnen. Wir teilen Γ gemäß des Repräsentantensystems $\mathrm{RS}(1) \dot\cup \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$ in drei Teilsummen $\Gamma = \Gamma_1 + \Gamma_2 + \Gamma_3$ auf und verwenden die, in Beobachtung 3 eingeführte, Hilfsfunktion $\omega(d)$.

$$\begin{aligned}
\Gamma_1 &= \sum_{x \in \mathrm{RS}(1)} \sum_{y \in Y} |P \cap {}^{x}({}^{y}G_\infty)| + |P \cap {}^{x}({}^{y}U)| && (120)\\
&= |Y| \left(|G_\infty| + |U| + \sum_{1 \neq x \in \mathrm{RS}(1)} |P \cap {}^{x}G_\infty^{(1)}| + |P \cap {}^{x}U| + \omega(d) |P \cap {}^{x}({}^{y}G_\infty^{(2)})| \right) && (121)\\
&= |Y| \left(q^{2+2dr} + \sum_{k=0}^{r-1} n_k (|P \cap {}^{x}G_\infty^{(1)}| + |P \cap {}^{x}U|) + \omega(d) 2 |R^*| q(q-1) q^{dr} \right) && (122)\\
&= |Y| \left(q^{2+2dr} + \mathcal{S} + \omega(d) 2 |R^*| q(q-1) q^{dr} \right) && (123)\\
&= \frac{(q^d-1)(q^{2d}-1)}{q^2-1} \left(q^{d(6r-3)+2} + q^{d(4r-3)} \mathcal{S} + \omega(d) 2 (q-1)(q^d-1) q^{d(6r-4)+1} \right) && (124)
\end{aligned}$$

Wir summieren nun über Repräsentanten vom Typ RS(2).

$$\begin{aligned}
\Gamma_2 &= \sum_{x \in \mathrm{RS}(2)} \sum_{y \in Y} |P \cap {}^{x}({}^{y}G_\infty)| + |P \cap {}^{x}({}^{y}U)| && (125)\\
&= |\{x \in \mathrm{RS}(2)\}| \left(|Y| (|P \cap {}^{x}G_\infty^{(1)}| + |P \cap {}^{x}U|) + \omega(d) |\{y \in Y | \beta_2 = 0\}| |P \cap {}^{x}({}^{y}G_\infty^{(2)})| \right) && (126)\\
&= |\{x \in \mathrm{RS}(2)\}| \left(|Y| q^{dr+1} + \omega(d) |\{y \in Y | \beta_2 = 0\}| q(q-1) q^{dr} \right) && (127)\\
&= q^{dr} q^{d(r-1)} \left(\frac{(q^d-1)(q^{2d}-1)}{q^2-1} q^{d(5r-3)+1} + \omega(d) \frac{2(q^d-1)^2 q^d q^{3d(r-1)}}{q^2-1} q(q-1) q^{dr} \right) && (128)\\
&= \frac{(q^d-1)(q^{2d}-1)}{q^2-1} \left(q^{d(7r-4)+1} + \omega(d) \frac{2(q-1)}{q^d+1} q^{d(6r-3)+1} \right) && (129)
\end{aligned}$$

Analog summieren wir über Repräsentanten vom Typ RS(3).

$$\begin{aligned}
\Gamma_3 &= |\{x \in \mathrm{RS}(3)\}| \left(|Y| q^{dr+1} + \omega(d) |\{y \in Y | \beta_2 = 0\}| q(q-1) q^{dr} \right) && (130)\\
&= \frac{(q^d-1)(q^{2d}-1)}{q^2-1} \left(q^{d(7r-5)+1} + \omega(d) \frac{2(q-1)}{q^d+1} q^{d(6r-4)+1} \right) && (131)
\end{aligned}$$

Wir erhalten die Verzweigung an den Spitzen, indem wir die Einzelsummen Γ_i wieder zu Γ zusammensetzen, also

$$\Gamma = \frac{(q^d-1)(q^{2d}-1)}{q^2-1}\left(q^{d(7r-5)+1}(q^d+1) + q^{d(6r-3)+2} + q^{d(4r-3)}\mathcal{S} + \omega(d)2(q-1)q^{d(6r-3)+1}\right). \tag{132}$$

Damit lässt sich nun eine etwas unhandliche, aber explizite, Formel mit Parametern q, d, r für die Verzweigung an den Spitzen angeben. Es ergibt sich nach einigen Umformungen:

$$\Gamma = \frac{(q^d-1)(q^{2d}-1)}{q^2-1}\Big\{q^{d(7r-5)}\left(q(q^d+1) + (q+2\lfloor\frac{r}{2}\rfloor)(q^{2d}-1)\right) \tag{133}$$

$$+ q^{d(6r-3)}\left(q^2 + 2(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)}-1) + \omega(d)2q(q-1)\right)\Big\}. \tag{134}$$

3 Verzweigung an den elliptischen Punkten

Um die Riemann-Hurwitz-Formel auf die Überlagerung $X(p^r) \longrightarrow X_0(p^r)$ mit Galois-Gruppe P anwenden zu können, bleibt nun noch die Verzweigung über $j = 0$, also den elliptischen Punkten, zu berechnen. Wie in Bemerkung 3 festgehalten wurde, ist die Verzweigung der Überlagerung $X(N) \longrightarrow X(1)$ an den elliptischen Punkten zahm. Bei der Überlagerung $X(N) \longrightarrow X(1)$ wird die Fixgruppe der elliptischen Punkte (also der über $j = 0$ verzweigten Punkte) durch die, im Anschluss an Bemerkung 7 eingeführte, Gruppe $C = \mathrm{Car}(3)/Z$ beschrieben.

Lemma 11. *Ist $\{\xi\}$ ein Repräsentantensystem für G/C so ist ${}^{\xi}C := \xi C \xi^{-1}$ Fixgruppe des elliptischen Punktes $\xi(e) = Q$. Dann gilt für die Verzweigungszahlen a_Q der Überlagerung $X(p^r) \to X_0(p^r)$ an den elliptischen Punkten:*

$$a_Q = |P \cap {}^{\xi}C| - 1. \tag{135}$$

Wir müssen also den Beitrag $\sum_{\xi \in G/C}(|P \cap {}^{\xi}C| - 1)$ berechnen.

Beweis. Analog zur Spitzenverzweigung rechnet man nach, dass ${}^{\xi}C$ einen elliptischen Punkt $Q = \xi(e)$ fest lässt. Die Verzweigung in den elliptischen Punkten (also über $j = 0$) ist zahm (siehe [Gek14] Theorem A). □

Beobachtung 5.

1. $|P \cap {}^{\xi}C|$ hängt nur von $\eta \in P\backslash G/C$ ab.

2. Die Doppelnebenklassen $P\backslash G/C$ sind gegeben durch die Bahnen von C bezüglich der Rechtsoperation auf $P\backslash G$. Sei $\{\eta\}$ ein Repräsentantensystem für $P\backslash G/C$. Damit ergibt sich insbesondere:

$$\sum_{\xi \in G/C}(|P \cap {}^{\xi}C| - 1) = \sum_{\eta \in P\backslash G/C} \sum_{\xi \sim \eta}(|P \cap {}^{\xi}C| - 1). \tag{136}$$

3. $c \in C$ lässt $P\eta$ fest genau dann, wenn $c \in {}^{\eta^{-1}}P \cap C$. Also bestehen die Nebenklassen $P\eta C$ aus $\frac{|C|}{|P \cap {}^{\eta}C|}$ vielen Klassen aus $P\backslash G$. Also ergibt sich

$$P\eta C = \dot{\bigcup_{1 \le i \le \frac{|P|}{|P \cap {}^{\eta}C|}}} P\xi_i C \tag{137}$$

$$|P\eta C| = \frac{|P||C|}{|P \cap {}^{\eta}C|}. \tag{138}$$

Somit erhalten wir:

$$\sum_{\xi \in G/C}(|P \cap {}^{\xi}C| - 1) = \sum_{\eta \in P\backslash G/C} \frac{|P|}{|P \cap {}^{\eta}C|}(|P \cap {}^{\eta}C| - 1) \tag{139}$$

Dabei ist die Größe der Stabilisatorgruppe in C von $P\eta \in P\backslash G$ gleich der Größe der Stabilisatorgruppe in P von $\eta C \in G/C$, also $|{}^{\eta^{-1}}P \cap C| = |P \cap {}^{\eta}C|$.

Lemma 12. *Die Bahnen von* $\mathbb{P}^2(R) \xrightarrow{\cong} P\backslash G$ *(man beachte Bemerkung 9) unter Operation der Gruppe* C *von rechts haben* q^2+q+1 *viele Elemente, mit Ausnahme des Falls* $d \equiv 0 \mod 3$*, in welchem es drei Bahnen der Länge* 1 *gibt.*

Beweis. Die Rechtsoperation der Gruppe C auf $\mathbb{P}^2(R)$ ist kanonisch definiert.

$$\mathbb{P}^2(R) \times C \longrightarrow \mathbb{P}^2(R) \tag{140}$$
$$((a:b:c),\gamma) \longmapsto (a':b':c') \tag{141}$$

Wir haben offensichtlich die folgenden Korrespondenzen für ein $m \in \mathbb{P}^2(R)$:

$$|mC| = q^2+q+1 \overset{1:1}{\longleftrightarrow} |C_m| = 1 \tag{142}$$
$$|mC| = 1 \overset{1:1}{\longleftrightarrow} |C_m| = q^2+q+1. \tag{143}$$

Wir berechnen also die Fixgruppe eines Punktes $m \in \mathbb{P}^2(R)$.
„ $\Rightarrow$ “. Sei $m \in \mathbb{P}^2(R)$ fest gewählt.

$$1 \neq \gamma \in C_m \tag{144}$$
$$\Leftrightarrow m \cdot \gamma = m \tag{145}$$
$$\Leftrightarrow (a':b':c') = (a:b:c) \tag{146}$$

wobei $(a':b':c')$ gegeben ist durch:

$$a' = a\gamma_{11} + b\gamma_{21} + c\gamma_{31} \tag{147}$$
$$b' = a\gamma_{12} + b\gamma_{22} + c\gamma_{32} \tag{148}$$
$$c' = a\gamma_{13} + b\gamma_{23} + c\gamma_{33} \tag{149}$$

Nun gilt aber:

$$(a':b':c') = (a:b:c) \tag{150}$$
$$\Leftrightarrow \exists \lambda \in R^* : (a',b',c') = \lambda(a,b,c) \tag{151}$$
$$\Leftrightarrow (a,b,c)\cdot(\lambda E - \gamma) = 0 \tag{152}$$
$$\Leftrightarrow (a,b,c) \in \mathrm{Kern}(\lambda E - \gamma) \tag{153}$$
$$\Leftrightarrow (a,b,c) \text{ ist Eigenvektor von } \gamma \text{ zum Eigenwert } \lambda \in R^*. \tag{154}$$

Wir betrachten das Problem nun modulo $\mathfrak{p}$, d.h. wir gehen über zu $R/\mathfrak{p} \xrightarrow{\cong} \mathbb{F}_{q^d}$. Wir schreiben $\overline{m}$ für die Restklasse bei Reduktion modulo $\mathfrak{p}$ und entsprechend $\overline{\lambda}$. Dann gilt nach obigen Vorüberlegungen offenbar:

$$1 \neq \gamma \in C_m \tag{155}$$
$$\Rightarrow \exists\ \overline{\lambda} \in R/\mathfrak{p} : \overline{m} \in \mathrm{Eig}(\gamma, \overline{\lambda}). \tag{156}$$
$$\rightsquigarrow \overline{\lambda} \in \mathbb{F}_{q^3}, \tag{157}$$

denn das charakteristische Polynom χ_γ eines Elementes $\gamma \in C$ zerfällt über $\mathbb{F}_{q^3}$ vollständig in paarweise verschiedene Linearfaktoren. Dann muss aber für den Grad d unseres Primpolynoms p wegen $R/\mathfrak{p} \xrightarrow{\cong} \mathbb{F}_{q^d}$ schon gelten: $d \equiv 0 \mod 3$. Da $\chi_\gamma(T) \in \mathbb{F}_q[T]$ mit $\deg(\chi_\gamma) = 3$, so gilt dies für genau drei $\overline{m} \in \mathbb{P}^2(R/\mathfrak{p})$. Wegen des Lemmas von Nakayama (Lemma 2) gibt es also auch genau drei $m \in \mathbb{P}^2(R)$ mit $|C_m| = q^2 + q + 1$.
„ $\Leftarrow$ “. Es gelte nun umgekehrt $d = \deg(p) \equiv 0 \mod 3$. Nutzt man aus, dass die Gruppe $C =< \epsilon >$ zyklisch ist, so genügt es, den Erzeuger ϵ der Gruppe C mit nichtdiagonaler Cartan-Matrix zu betrachten; die Eigenvektoren von $\gamma \in C$ sind genau die Eigenvektoren von ϵ. Dann gibt es genau drei paarweise verschiedene $\overline{\lambda_1}, \overline{\lambda_2}, \overline{\lambda_3}$ aus $R/\mathfrak{p}$, sodass

$$(a,b,c)\epsilon \equiv \overline{\lambda_j}(a,b,c) \mod \mathfrak{p} \quad (1 \leq j \leq 3). \tag{158}$$

für einen Vektor $(a,b,c) \in R^3$ mit $(a,b,c) \not\equiv (0,0,0) \mod \mathfrak{p}$. Zu jedem der paarweise verschiedenen, reduzierten Eigenwerte $\overline{\lambda_j}$ von ϵ gibt es, gemäß des Lemmas von Hensel (Lemma 1), eine wohlbestimmte Liftung zu einem $\lambda_j \in R$, sodass $\epsilon(\tilde{a},\tilde{b},\tilde{c}) \equiv \lambda_j(\tilde{a},\tilde{b},\tilde{c})$ gilt, wobei $(\tilde{a},\tilde{b},\tilde{c}) \in R^3$, mit $(\tilde{a},\tilde{b},\tilde{c}) \equiv (a,b,c) \mod \mathfrak{p}$.
Zu jedem dieser λ_j $(1 \leq j \leq 3)$ gehört somit genau ein Eigenvektor (a,b,c), der bis auf Skalierung mit R^* eindeutig bestimmt ist. Also C lässt $(a:b:c)$ fest, was zu einer Bahnlänge 1 führt.

□

Korollar 3. *Der Beitrag der elliptischen Punkte T_{ell} zur Riemann-Hurwitz-Formel ist im lokalen Fall gegeben durch*

$$T_{ell} = \begin{cases} 0 & ,\textit{falls} \quad d \not\equiv 0 \mod 3 \\ 3\frac{|P|}{|C|}(q^2+q) & ,\textit{falls} \quad d \equiv 0 \mod 3 \end{cases} \tag{159}$$

$$= \psi(d) 3 \frac{q^2+1}{q^2+q+1}, \tag{160}$$

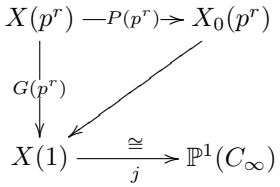
wobei die Hilfsfunktion ψ definiert ist durch

$$\psi(d) := \begin{cases} 0 & ,\textit{falls} \quad d \not\equiv 0 \mod 3 \\ 1 & ,\textit{falls} \quad d \equiv 0 \mod 3. \end{cases} \tag{161}$$

Beweis. Wir verwenden die Aussage von Lemma 12 und erhalten mit den Vorüberlegungen (Beobachtung 5) die Behauptung. □

4 Berechnung des Geschlechts

Wir erinnern den Leser daran, dass unser Ziel die Berechnung des Geschlechts $g_0(p^r)$ durch zweifache Anwendung der Riemann-Hurwitz-Formel auf die folgenden Überlagerungen von Kurven ist.



Lemma 13. *Bei Anwendung der Riemann-Hurwitz-Formel auf die Galois-Überlagerung* $X(p^r) \longrightarrow X(1) \xrightarrow{\cong} \mathbb{P}^1(C_\infty)$ *ergibt sich für die Eulercharakteristik*

$$e(p^r) = (q^{2d} + q^d + 1)q^{5d(r-1)}(q^{2d} - 1)(q^d - 1)q^{3dr}\left(\frac{1}{q^2+q+1} - \frac{q^{2dr}+2}{(q^2-1)q^{2dr}}\right) \tag{162}$$

und somit für das Geschlecht

$$g(p^r) = 1 - \frac{1}{2}(q^{2d} + q^d + 1)q^{5d(r-1)}(q^{2d} - 1)(q^d - 1)q^{3dr}\left(\frac{1}{q^2+q+1} - \frac{q^{2dr}+2}{(q^2-1)q^{2dr}}\right). \tag{163}$$

Beweis. Wir nutzen aus, dass $g(X(1)) = g(\mathbb{P}^1(C_\infty)) = 0$ gilt und wenden dann die Riemann-Hurwitz-Formel an.

$$e(p^r) = 2|G| - \frac{|G|}{|G_\infty|}(|G_\infty| + |U| - 2) - \frac{|G|}{|C|}(q^2+q) \tag{164}$$

$$= |G| - \frac{|G|}{|G_\infty|}(|U| + 2) - \frac{|G|}{|C|}(q^2+q) \tag{165}$$

Mit einigen weitere Äquivalenzumformungen bringt man die Formel für die Eulercharakteristik auf die Gestalt

$$e(p^r) = |G|\left(\frac{1}{q^2+q+1} - \frac{q^{2dr}+2}{(q^2-1)q^{2dr}}\right). \tag{166}$$

Nach Ausschreiben der Kardinalität von G in Termen von q, d, r folgt die Behauptung. □

In den vorangehenden Kapiteln haben wir alle Berechnungen durchgeführt, um die Riemann-Hurwitz-Formel auch auf die Überlagerung $X(p^r) \longrightarrow X_0(p^r)$ anwenden zu können. Es ist übersichtlicher, zunächst mit der Euler-Charakteristik $e(p^r)$ bzw. $e_0(p^r)$ zu arbeiten. Wir erhalten also mit $g(X(1)) = g(\mathbb{P}^1(C_\infty)) = 0$ offenbar

$$e(p^r) = 2|G| - \frac{|G|}{|G_\infty|}(|G_\infty| + |U| - 2) - \frac{|G|}{|C|}(q^2+q) \tag{167}$$

$$= |P|e_0(p^r) - \sum_{\xi \in G/G_\infty} (|P \cap {}^{\xi}G_\infty| + |P \cap {}^{\xi}U| - 2) - T_{\text{ell}}. \tag{168}$$

Wir fassen geschickt zusammen, indem wir ausnutzen dass $G/P \xrightarrow{\cong} \mathbb{P}^2(R)$ und somit insbesondere $\frac{|G|}{|P|} = \epsilon_2$ gilt. Wir können dann nach $e_0(p^r)$ auflösen.

$$|P|e_0(p^r) = 2|G| - \frac{|G|}{|G_\infty|}(|G_\infty| + |U|) - \frac{|G|}{|C|}(q^2+q) + \Gamma + T_{\text{ell}} \tag{169}$$

$$e_0(p^r) = \epsilon_2 \left(1 - \frac{1}{q^2-1} - \frac{q^2+q}{q^2+q+1}\right) + \frac{\Gamma}{|P|} + \frac{T_{\text{ell}}}{|P|} \tag{170}$$

$$= -\frac{\epsilon_2(q+2)}{(q^2-1)(q^2+q+1)} + \frac{\Gamma}{|P|} + \frac{T_{\text{ell}}}{|P|} \tag{171}$$

Wir verwenden die explizite Darstellung von Γ und den Wert für T_{ell}. Damit können wir einige Terme kürzen und formen weiter um.

$$e_0(p^r) = -\frac{\epsilon_2(q+2)}{(q^2-1)(q^2+q+1)} + \frac{1}{(q^2-1)q^{d(6r-3)}}\Big\{q^{d(7r-5)}\left(q(q^d+1) + (q+2\lfloor\frac{r}{2}\rfloor)(q^{2d}-1)\right) \tag{172}$$

$$+ q^{d(6r-3)}\left(q^2 + 2(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)} - 1) + \omega(d)2q(q-1)\right)\Big\} + \psi(d)3\frac{q^2+q}{q^2+q+1} \tag{173}$$

Wir setzen nun noch die Kardinalität $\epsilon_2 = (q^{2d}+q^d+1)q^{2d(r-1)}$ für die „projektive Ebene“ in die Formel ein und fassen weiter zusammen.

$$e_0(p^r) = -\frac{(q+2)(q^{2d}+q^d+1)q^{2d(r-1)}}{(q^2-1)(q^2+q+1)} + \frac{1}{q^2-1}\Big\{q^{d(r-2)}\left(q(q^d+1) + (q+2\lfloor\frac{r}{2}\rfloor)(q^{2d}-1)\right) \tag{174}$$

$$+ q^2 + 2(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)} - 1) + \omega(d)2q(q-1)\Big\} + \psi(d)3\frac{q^2+q}{q^2+q+1} \tag{175}$$

Wir erhalten somit insbesondere eine explizite Formel für $g_0(p^r) = 1 - \frac{e_0(p^r)}{2}$ in Abhängigkeit von der Zahl der Körperelemente q, dem Grad d unseres Primpolynoms p und dem Exponenten r:

$$g_0(p^r) = 1 + \frac{(q+2)(q^{2d}+q^d+1)q^{2d(r-1)}}{2(q^2-1)(q^2+q+1)} - \frac{1}{2(q^2-1)}\Big\{q^{d(r-2)}\left(q(q^d+1) + (q+2\lfloor\frac{r}{2}\rfloor)(q^{2d}-1)\right) \tag{176}$$

$$+ q^2 + 2(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)} - 1) + \omega(d)2q(q-1)\Big\} - \psi(d)\frac{3(q^2+q)}{2(q^2+q+1)}. \tag{177}$$

Bemerkung 15.

1. Wir konstatieren, dass die so entwickelte Formel für die Eulercharakteristik $e_0(p^r)$ und das Geschlecht $g_0(p^r)$ mit der von Ernst-Ulrich Gekeler bestimmten Geschlechtsformel für die Kurve $X_0^{3,2}(T^n)$ in der speziellen Situation $d = 1$ übereinstimmt (siehe [Gek14] 11.13.3).

2. Für $r = 1$, also im Körperfall $R \xrightarrow{\cong} \mathbb{F}_{q^d}$, entnehmen wir demnach

$$e_0 = -\frac{(q+2)(q^{2d}+q^d+1)}{(q^2-1)(q^2+q+1)} + \frac{q^{d+1}+q^2+q+\omega(d)2q(q-1)}{q^2-1} + \psi(d)\frac{3(q^2+q)}{q^2+q+1} \tag{178}$$

als Formel für die Eulercharakteristik unserer Kurve und verfügen somit auch über die entsprechende Gechlechtsformel

$$g_0 = 1 + \frac{(q+2)(q^{2d}+q^d+1)}{2(q^2-1)(q^2+q+1)} - \frac{q^{d+1}+q^2+q+\omega(d)2q(q-1)}{2(q^2-1)} - \psi(d)\frac{3(q^2+q)}{2(q^2+q+1)}. \tag{179}$$

Bringt man den Ausdruck unter einen Bruchstrich und fasst Terme im Zähler zusammen, so ergibt sich keine wesentliche Vereinfachung mehr.

3. Wir erhalten für das Geschlecht $g_0(p^r)$ mit dem Grad d unseres Primpolynoms p und dem Exponenten r insbesondere ein Polynom in q mit rationalen Koeffizienten; die Eulercharakteristik ist sogar ein Polynom in q mit ganzen Koeffizienten; dies ist ausführlich in [Gei15] begründet.

4. Wir reduzieren unsere Kurve $X_0(p^r)$ für eine Primstelle $\mathfrak{q} \neq \mathfrak{p}$, wobei $\mathfrak{q}$ eine Stelle des Grades eins ist, die $\mathfrak{p}$ nicht teilt; wir erhalten dann eine Kurve $\overline{X_0(p^r)}$ mit gleichem Geschlecht $g(\overline{X_0(p^r)}) = g(X_0(p^r))$ (siehe [Gek14], 10.3). Im Nachfolgenden bezeichnen wir mit $\overline{X_0(p^r)}$ die bezüglich $\mathfrak{q}$ reduzierte Kurve. Diese Kurve ist über dem Körper $\mathbb{F}_q = A/\mathfrak{q}$ definiert und liefert eine nichtgaloissche Überlagerung von $\overline{X(1)} \xrightarrow{\cong} \mathbb{P}^1(\mathbb{F}_q)$ (siehe [Gek14], 10.3.1).

Bemerkung 16. Für unsere reduzierte Kurve $\overline{X_0(p^r)}$ erhalten wir als Zahl der elliptischen Punkte (also der über $j = 0$ liegenden Punkte) $E(p^r)$ offenbar

$$E(p^r) = \begin{cases} \frac{\epsilon_2}{q^2+q+1} & \text{, falls} \quad d \not\equiv 0 \mod 3 \\ \frac{\epsilon_2}{q^2+q+1} + 3\frac{q^2+q}{q^2+q+1} & \text{, falls} \quad d \equiv 0 \mod 3, \end{cases} \tag{180}$$

wobei alle elliptischen Punkte von $\overline{X_0(p^r)}$ rational über $\mathbb{F}_{q^3}$ sind (siehe [Gek14], Proposition 10.4). Hierbei wurde $\epsilon_2 = |\mathbb{P}^2(R)|$ in Lemma 5 definiert.

Lemma 14.

1. *Für $d \cdot r \leq 2$ ergibt sich stets $g_0(q,d,r) = 0$.*

2. *Für die an der Stelle $\mathfrak{q}$ (mit $\mathfrak{q} \neq \mathfrak{p}$ vom Grad eins) reduzierte Kurve $\overline{X_0(p^r)}$ ergibt sich:*

$$\limsup_{r\to\infty} \frac{|\{P \in \overline{X_0(p^r)}\} | P \text{ ist rational über } \mathbb{F}_{q^3}\}|}{g(\overline{X_0(p^r)})} \geq 2\frac{q^2-1}{q+2}. \tag{181}$$

Beweis. Wertet man die Formel für $g_0(q,d,r)$ in der Situation $(d,r) \in \{(1,1),(1,2),(2,1)\}$ aus, so erhält man das Nullpolynom; also ergibt sich (1). Wir betrachten zunächst den Ausdruck $\frac{g_0}{q^{2d(r-1)}}$.

$$\frac{g_0}{q^{2d(r-1)}} = \frac{1}{q^{2d(r-1)}} + \frac{(q+2)(q^{2d}+q^d+1)}{2(q^2-1)(q^2+q+1)} - \frac{1}{q^{2d(r-1)}2(q^2-1)}\Big\{q^{d(r-2)}\left(q(q^d+1)+(q+2\lfloor\frac{r}{2}\rfloor)(q^{2d}-1)\right) \tag{182}$$

$$+ q^2 + 2(q^{2d(r-\lfloor\frac{r}{2}\rfloor-1)}-1) + \omega(d)2q(q-1)\Big\} - \psi(d)\frac{3(q^2+q)}{q^{2d(r-1)}2(q^2+q+1)} \tag{183}$$

Wir bemerken, dass der erste, der dritte und vierte Summand in unserem Ausdruck $\frac{g_0}{q^{2d(r-1)}}$ für $r \to \infty$ verschwinden. Entscheidend für die Asymptotik ist offenbar nur der zweite Summand. Es ist also

$$\lim_{r\to\infty} \frac{g_0}{q^{2d(r-1)}} = \frac{(q+2)(q^{2d}+q^d+1)}{2(q^2-1)(q^2+q+1)}. \tag{184}$$

Damit erhalten wir

$$\limsup_{r\to\infty} \frac{|\{P \in \overline{X_0(p^r)}\}|P \text{ ist rational über } \mathbb{F}_{q^3}\}|}{g(\overline{X_0(p^r)})} \geq \lim_{r\to\infty} \frac{E(p^r)}{g_0} \geq \lim_{r\to\infty} \frac{\mathbb{P}^2(R)}{(q^2+q+1)g_0}. \tag{185}$$

Hierbei gilt

$$\lim_{r\to\infty} \frac{\mathbb{P}^2(R)}{(q^2+q+1)g_0} = \lim_{r\to\infty} \frac{q^{2d}+q^d+1}{q^2+q+1} \cdot \frac{q^{2d(r-1)}}{g_0} \tag{186}$$

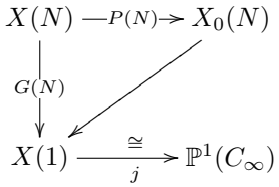
$$= \frac{q^{2d}+q^d+1}{q^2+q+1} \cdot \frac{2(q^2-1)(q^2+q+1)}{(q+2)(q^{2d}+q^d+1)} \tag{187}$$

$$= 2\frac{q^2-1}{q+2} \tag{188}$$

und es folgt (2). □

5 Die globale Formel

Wir rufen dem Leser die von uns betrachtete Überlagerung von Kurven in Erinnerung.



Wir wollen in diesem Kapitel kurz auf die Globalisierung eingehen, also die Formel für das Geschlecht der Kurve $X_0(N)$ mit $A \ni N = \prod_{i=1}^{s} p_i^{r_i}$ angeben. Für die meisten der hierzu benötigten Aussagen werden wir allerdings nur Beweisskizzen angeben. Eine ausführliche Entwicklung der globalen Formel findet man in der Masterarbeit von David Geis ([Gei15]). Wir betrachten in der globalen Situation die Gruppen $U(N) \subset G_\infty(N) \subset P(N) \subset G(N)$, wobei die entsprechenden Matrixeinträge diesmal aus dem Ring $R := R(N) = A/(\prod_{i=1}^{s} p_i^{r_i})$ stammen; dieser zerfällt in die lokalen Komponenten $A/(\prod_{i=1}^{s} p_i^{r_i}) \xrightarrow{\cong} \prod_{i=1}^{s} A/(p_i^{r_i}) =: \prod_{i=1}^{s} R_i$. Es zerfällt $G := G(N) \xrightarrow{\cong} \prod_{i=1}^{n} G_i$ in die lokalen Bestandteile mit Einträgen aus den jeweiligen lokalen Ringen R_i. Eine leichte Überlegung liefert ebenso den Zerfall der Gruppen $P := P(N) \xrightarrow{\cong} \prod_{i=1}^{s} P_i$ und $U := U(N) \xrightarrow{\cong} \prod_{i=1}^{s} U_i$ in die lokalen Bestandteile.

Bemerkung 17. Wir weisen nochmal darauf hin, dass nur in diesem Kapitel die Bezeichnung R für den Ring $A/(\prod_{i=1}^{s} p_i^{r_i})$ gilt. Ebenso gelten lediglich im Nachfolgenden die Bezeichnungen $U \subset G_\infty \subset P \subset G$ für entsprechende Gruppen mit Einträgen aus dem „globalen“ Ring R. Diese Schreibweise, mit der Zerlegung in die lokalen Komponenten $R \xrightarrow{\cong} \prod_{i=1}^{s} R_i$, kollidiert zwar mit der zuvor festgelegten lokalen Notation, war aber naheliegend und stimmt mit der Notation in [Gei15] überein. Dies sollte den Leser nicht weiter irritieren.

Bemerkung 18. Analog zu Bemerkung 13 fixieren wir ein Repräsentantensystem $\{x\} = \mathrm{RS}(1) \dot\cup \mathrm{RS}(2) \dot\cup \mathrm{RS}(3)$ für G/P mit Einträgen aus dem „globalen“ Ring R. Ebenso fixieren wir ein Repräsentantensystem Y für P/G_∞. Am kompliziertesten stellt sich die Bestimmung der Verzweigungszahlen in den Spitzen heraus. Das Hauptproblem liegt hierbei in der Berechnung des Schnittes $P \cap {}^{x}({}^{y}G_\infty)$, mit $x \in \mathrm{RS}$ und $y \in Y$. Hierbei verwenden wir wie gehabt die Aufteilung $G_\infty^{(1)} \dot\cup G_\infty^{(2)}$. Wir bemerken, dass sich $x \in \mathrm{RS}$ aus lokalen Komponenten x_i zusammensetzt, wobei $\{x_i\} = \mathrm{RS}_i(1) \dot\cup \mathrm{RS}_i(2) \dot\cup \mathrm{RS}_i(3)$ ein Repräsentantensystem von $G_i/P_i \xrightarrow{\cong} \mathbb{P}^2(R_i)$ ist. Wir können jedoch Y nicht aus lokalen Repräsentantensystemen zusammensetzen(!). Die abkürzende Schreibweise „$x \in \mathrm{RS}$“ bzw. „$x_i \in \mathrm{RS}_i$“ ist hierbei analog zur, in Bemerkung 13 festgelegten, Notation zu verstehen.

Lemma 15. *Es sei $x = (x_1, ..., x_s)$, wobei $x_i \in RS_i$ für alle $1 \leq i \leq s$. Außerdem sei $y \in Y$. Dann*

gilt:

$$|P \cap {}^{x}({}^{y}U)| = |P \cap {}^{x}U| = \prod_{i=1}^{s} |P_i \cap {}^{x_i}U_i| \tag{189}$$

$$|P \cap {}^{x}({}^{y}G_{\infty}^{(1)})| = |P \cap {}^{x}G_{\infty}^{(1)}| = \alpha(x) \prod_{i=1}^{s} |P_i \cap {}^{x_i}U_i|. \tag{190}$$

Hierbei ist die Höhe h_{R_i} für alle $1 \leq i \leq s$ definiert durch

$$h_{R_i}(x) = min\{v_{\mathfrak{p}}(v_i), v_{\mathfrak{p}}(w_i)\},\ \textit{falls } x_i \textit{ vom Typ } RS_i(1), \tag{191}$$

wobei v_i, w_i die lokalen Einträge in Matrizen vom Repräsentantensystem des Typs $RS_i(1)$ sind. Dann ist die Funktion $\alpha(x)$ gegeben durch

$$\alpha(x) = \begin{cases} 1 & ,\textit{falls} \quad \exists i \in \{1, ..., s\} \quad \textit{mit } 0 < h_{R_i}(x) < r_i \\ q-1 & ,\textit{falls} \quad \forall 1 \leq i \leq s: \quad h_{R_i}(x) \in \{0, r_i\} \textit{ oder } x_i \in RS_i(2) \dot{\cup} RS_i(3) \\ & \quad \textit{und } (h_{R_1}, ..., h_{R_s}) \neq (r_1, ..., r_s). \end{cases} \tag{192}$$

Beweis. Die Aussage ist in einer etwas allgemeineren Fassung in [Gei15] bewiesen. Als zentral beim Beweis stellt sich die Verwendung des chinesischen Restsatzes heraus. Hiermit lassen sich die lokalen Lösungen in allen R_i vermöge des gewünschten Produktes zu einer Lösung in R zusammensetzen. □

Bemerkung 19. Für die kompakte Notation der globalen Formel verwenden wir die Hilfsfunktionen ($1 \leq i \leq s$):

$$\mu_i := q^{2d_i(2r_i - \lfloor \frac{r_i}{2} \rfloor - 1)} + (q^{2d_i} - 1) q^{d_i(3r_i - 2)} \lfloor \frac{r_i}{2} \rfloor - |R_i|^2 \tag{193}$$

$$\nu_i := (|\mathbb{P}^2(R_i)| - |R_i|^2)|R_i| + n_{0_i}|R_i| + |R_i|^2. \tag{194}$$

Hierbei beschreibt die Hilfsgröße n_{0_i} die Menge aller Elemente vom Typ $\mathrm{RS}_i(1)$ aus R_i mit Höhe Null, ist also gegeben durch $n_{0_i} := (q^{2d_i} - 1) q^{2d_i(r_i - 1)}$.

Es bleibt nun noch der Zusatzbeitrag auszurechnen, also die Menge $G_{\infty}^{(2)}$ zu betrachten. Hierzu fixieren wir ein nichtdiagonales $\gamma \in \mathrm{Car}(2)$.

Lemma 16. *Es sei $1 \neq x \in RS$ und $y \in Y$. Wir erinnern daran, dass P lokalisiert, also es gilt $P \xrightarrow{\cong} \prod_{i=1}^{s} P_i$. Es sei $\beta'_{2_j} := |\{\tilde{y} \in P | \tilde{\beta_{2_j}} = 0\}| = 2(q^{d_j} - 1)^2 q^{d_j} q^{3d_j(r_j - 1)} q^{2r_j d_j}$. Hierbei bezeichnet $\tilde{\beta_{2_j}}$ die in Beobachtung 2 eingeführte Hilfsgröße bezüglich eines R_j, auf welche in Lemma 10 zurückgegriffen wurde. Dann erhalten wir*

$$|P \cap {}^{x}({}^{y}G_{\infty}^{(2)})| = \Lambda, \tag{195}$$

wobei Λ gegeben ist durch

$$\Lambda = \prod_{j:\ d_j \equiv 1 \mod 2} |P_j||R_j|^2 \cdot \prod_{j:\ d_j \equiv 0 \mod 2} |P_j|(2|R_j^*||R_j| + |R_j|^2) + \beta'_{2_j}|R_j|(|R_j|q^{d_j(r_j-1)} + q^{2d_j(r_j-1)}). \tag{196}$$

Beweis. Es sei wiederum auf die Masterarbeit von David Geis ([Gei15]) verwiesen. Der Zusatzbeitrag Λ kommt hierbei, entgegen der Intuition, auf nichttriviale Weise zu Stande. □

Bemerkung 20. Aus technischen Gründen wurde die Identität $x = 1$, also $(h_{R_1}, ..., h_{R_s}) = (r_1, ..., r_s)$, zunächst nicht berücksichtigt. Offenbar gilt aber $|P \cap {}^x({}^yG_\infty)| = (q^2-1)|R|^2$, falls x global die Identität ist.
Wir verfügen nun über die einzelnen Beiträge $|P \cap {}^x({}^yG_\infty^{(1)})|$ und $|P \cap {}^x({}^yG_\infty^{(2)})|$, müssen allerdings noch über alle $x = (x_1, ..., x_s) \in \mathrm{RS}$ und $y \in Y$ aufsummieren. Dies liefert

$$\sum_{x\in \mathrm{RS}} \sum_{y\in Y} |P \cap {}^x({}^yG_\infty)| + |P \cap {}^x({}^yU)| = \sum_{x\in \mathrm{RS}} \sum_{y\in Y} |P \cap {}^x({}^y(G_\infty^{(1)} \dot\cup G_\infty^{(2)}))| + |P \cap {}^x({}^yU)| \quad (197)$$

$$= \sum_{x\in \mathrm{RS}} \sum_{y\in Y} |P \cap {}^x({}^yG_\infty^{(1)})| + |P \cap {}^x({}^yU)| \quad (198)$$

$$+ \sum_{x\in \mathrm{RS}} \sum_{y\in Y} |P \cap {}^x({}^yG_\infty^{(2)})| \quad (199)$$

$$=: \sigma_1 + \sigma_2. \quad (200)$$

Beobachtung 6.

1. Es ergibt sich für den Standardbeitrag σ_1 mit diagonalen Cartan-Matrizen und $x = (x_1, x_2, ..., x_s)$, wobei $x_i \in \{\mathrm{RS}_i(1), \mathrm{RS}_i(2), \mathrm{RS}_i(3)\}$:

$$\sigma_1 = \sum_{x=(x_1,...,x_s)} \sum_{y\in Y} \prod_{i=1}^{s} (\alpha(x)+1)|P_i \cap {}^{x_i}({}^yU_i)| \quad (201)$$

$$= \sum_{x=(x_1,...,x_s)} (\alpha(x)+1) \sum_{y\in Y} \prod_{i=1}^{s} |P_i \cap {}^{x_i}({}^yU_i)| \quad (202)$$

$$= \sum_{x=(x_1,...,x_s)} (\alpha(x)+1) \prod_{i=1}^{s} |P_i \cap {}^{x_i}U_i|. \quad (203)$$

Nach Vertauschen von Summen und Produktzeichen und weiteren umfangreichen Vereinfachungen folgt durch Verwenden der eingeführten Funktionen μ_i und ν_i:

$$\sigma_1 = \frac{|P|}{|G_\infty|} 2 \cdot \sum_{i=1}^{s} \mu_i \cdot \prod_{j<i} \nu_j \cdot \prod_{j>i} (|\mathbb{P}^2(R_j)| - |R_j|^2)|R_j| + q^{2d_j(2r_j - \lfloor \frac{r_j}{2} \rfloor - 1)} \quad (204)$$

$$+ (q^{2d_j} - 1) q^{d_j(3r_j-2)} (1 + \lfloor \frac{r_j}{2} \rfloor) + q^2|R|^2 + q \prod_{i=1}^{s} \nu_i - q|R|^2. \quad (205)$$

2. Der Zusatzbeitrag σ_2 mit nichtdiagonalen Cartan-Matrizen und $x = (x_1, x_2, ..., x_s)$ wie gehabt, wobei $x_i \in \{\mathrm{RS}_i(1), \mathrm{RS}_i(2), \mathrm{RS}_i(3)\}$, berechnet sich zu

$$\sigma_2 = \frac{q(q-1)}{(q^2-1)|R|^2} \Big\{ \prod_{j:\ d_j \equiv 1 \mod 2} |P_j||R_j|^2 \cdot \prod_{j:\ d_j \equiv 0 \mod 2} (|P_j|(2|R_j^*||R_j| + |R_j|^2) + \quad (206)$$

$$\beta'_{2_j} |R_j|(|R_j| q^{d_j(r_j-1)} + q^{2d_j(r_j-1)})) - |P||R|^2 \Big\}; \quad (207)$$

dies ist ausführlich in ([Gei15]) begründet.

Die Verzweigungszahlen an den elliptischen Punkten lässt sich, im Gegensatz zur Spitzenverzweigung, vergleichsweise einfach auch in der globalen Situation angeben.

Lemma 17. *Der elliptische Beitrag T_{ell} ist im globalen Fall gegeben durch*

$$T_{ell} := \begin{cases} 3^s \frac{|P|}{|C|}(q^2+q) & , \textit{falls} \quad \forall\ 1 \leq i \leq s:\ d_i \equiv 0 \mod 3 \\ 0 & , \textit{sonst.} \end{cases} \tag{208}$$

$$= \Psi(d_1, ..., d_s) 3^s \frac{|P|}{|C|}(q^2+q), \tag{209}$$

wobei die Hilfsfunktion Ψ definiert ist durch

$$\Psi(d_1, ..., d_s) = \begin{cases} 1 & , \textit{falls } \forall\ 1 \leq i \leq s:\ d_i \equiv 0 \mod 3 \\ 0 & , \textit{sonst.} \end{cases} \tag{210}$$

Beweis. Wir können das „Bahnenlemma“ (Lemma 12) aus dem dritten Kapitel für die Operation der Gruppe C auf $P \backslash G \xrightarrow{\cong} \mathbb{P}^2(R)$ analog übernehmen, indem wir bezüglich eines $\mathfrak{p}_i$ reduzieren, also zum Restklassenkörper $R/\mathfrak{p}_i \xrightarrow{\cong} R_i/\mathfrak{p}_i$ übergehen. Somit erhalten wir in jedem der $R_i/\mathfrak{p}_i$ drei Ausnahmebahnen, die sich dann zu 3^s Ausnahmebahnen in R zusammensetzen. □

Damit haben wir nun alle Ergebnisse zusammengestellt, um die Riemann-Hurwitz-Formel auch global auf unsere Überlagerung $X(N) \longrightarrow X_0(N)$ anwenden zu können. Wir arbeiten wieder aus Gründen der Übersicht zunächst mit der Eulercharakteristik $e(X_0(N))$. Indem wir ausnutzen, dass $g(X(1)) = g(\mathbb{P}^1(C_\infty)) = 0$ gilt, erhalten wir nach einigen Umformungen

$$|P| e(X_0(N)) = 2|G| - \frac{|G|}{|G_\infty|}(|G_\infty| + |U|) - \frac{|G|}{|C|}(q^2+q) + \Psi(d_1, ..., d_s) 3^s \frac{|P|}{|C|}(q^2+q) + \sigma_1 + \sigma_2. \tag{211}$$

Bemerkung 21. Wir verfügen nun bei Auflösen nach $e(X_0(N))$ mit $g(X_0(N)) = 1 - \frac{e(X_0(N))}{2}$ über eine explizite Formel für das Geschlecht der Kurve $X_0(N)$. Dies gestattet insbesondere die computergestützte Auswertung. Hierzu wurde das Computeralgebrasystem GAP (Groups, Algorithms, Programming) verwendet (siehe Anhang). Eine Auflistung von interessanten Geschlechtern ist in der Masterarbeit von David Geis zu finden ([Gei15]).

Die vorliegende Masterarbeit macht deutlich, mit welcher Komplexität das Ausrechnen der Geschlechter von Kurven des Typs $X^{r,k}(N)$ bei der Wahl von $k = r - 1$, schon in der speziellen Situation $r = 3$, verbunden ist.

Numerische Auswertung der Riemann-Hurwitz-Formel

In Lemma 13 wurde eine explizite Formel für das Geschlecht $g(p^r)$ angegeben. Die Überlegungen in Kapitel 2 und Kapitel 3 liefern die, in Kapitel 4 ausgearbeitete, explizite Formel für $g_0(p^r)$ mit Eingabewerten q, d, r. Die lokale Formel hat hierbei noch eine verhältnismäßig übersichtliche Gestalt.
In Kapitel 5 wurden dann die Ergebnisse der Masterarbeit von David Geis ([Gei15]) verwendet, um eine globale Formel für das Geschlecht $g(X_0(N))$ für $N = \prod_{i=1}^{s} p_i^{r_i}$ zu bestimmen. Zur Auswertung mit Hilfe des Rechners wurde das Computeralgebrasystem GAP (Groups, Algorithms, Programming) verwendet.
Insbesondere erschien es, angesichts der umfangreichen Umformungen beim Ausarbeiten der lokalen Formel, angebracht, deren Richtigkeit auch numerisch zu bestätigen.

GAP-Code für $g(X_0(p^r))$.

```
floor:= function(r)
if r mod 2 = 0 then
return r/2;
else
return (r-1)/2;
fi;
end;

omega:= function(d)
if d mod 2 = 0 then
return 1;
else
return 0;
fi;
end;

psi:= function(d)
if d mod 3 = 0 then
return 1;
else
return 0;
fi;
end;

glokal:= function(q, d, r)
local s1, s2, s2_2, s3;
s1:= ((q+2)*(q^(2*d)+ q^d+ 1)*q^(2*d*(r-1)))/(2*(q^2-1)*(q^2+q+1));
s2:= q^(d*(r-2))*(q*(q^d+1)+(q+2*floor(r))*(q^(2*d)-1))
     + q^2+ 2*(q^(2*d*(r-floor(r)-1))-1)+ omega(d)*2*q*(q-1);
s2_2:= s2/(2*(q^2-1));
```

```
s3:= psi(d)*(1/2)*3*((q^2+q)/(q^2+q+1));
return 1+ s1- s2_2- s3;
end;
```

Durch Eingabe von glokal (q, d, r) erhalten wir nun das Geschlecht der Kurve $X_0(p^r)$ in Abhängigkeit von der Zahl der Körperelemente des endlichen Körpers $\mathbb{F}_q$, dem Grad d des Primpolynoms p und dem Exponenten r.

GAP-Code für $g(X_0(N))$.

```
gglobal:=function(arg)
local q, s, d, r, i, phi, drei, epsilon_1, epsilon_2, group, ring, inf, U, e, P, dell,
 zeile1, zeile2, floor, j, prod1, prod2, sum, prod3, beta2, zu1, zu2, zu,
 zeile3, enull, gnull, eps2, rlok, p, nnull, k;

q:= arg[1];
d:= arg[2];
r:= arg[3];
s:= Length(r);
phi:= 1;
drei:= 1;
epsilon_1:= 1;
epsilon_2:= 1;
ring:= 1;
floor:=[];
prod1:=[];
prod2:=[];
sum:= 0;
prod3:= 1;
beta2:=[];
rlok:=[];
eps2:=[];
nnull:=[];
p:=[];
zu1:= 1;
zu2:= 1;
zu:= 1;
k:= 0;

dell:= 0;

for i in [1..s] do
phi:=phi*q^(d[i]*(r[i]-1))*(q^d[i]-1);
od;

for i in [1..s] do
```

```
ring:= ring*q^(d[i]*r[i]);
rlok[i]:= q^(d[i]*r[i]);
od;

for i in [1..s] do
epsilon_1:= epsilon_1*(q^d[i]+1)*q^(d[i]*(r[i]-1));
od;

for i in [1..s] do
epsilon_2:= epsilon_2*(q^(2*d[i])+q^d[i]+1)*q^(2*d[i]*(r[i]-1));
eps2[i]:= (q^(2*d[i])+q^d[i]+1)*q^(2*d[i]*(r[i]-1));
od;

group:= phi^2*ring^3*epsilon_1*epsilon_2;

inf:= (q^2-1)*ring^2;
U:= ring^2;
e:= 2*group - (group/inf)*(inf+U-2) - (group/(q^2+q))*(q^2+q);

for i in [1..s] do
if((d[i] mod 3 = 0)=true) then
dell:=dell+1;
fi;
od;

if dell = s then
dell:= 1;
else
dell:= 0;
fi;

P:= phi^2*ring^3*epsilon_1;

zeile1:= 2*group - (group/inf)*(inf+U)- (group/(q^2+q+1))*(q^2+q)
        + dell*3^s*(P/(q^2+q+1))*(q^2+q);

for i in [1..s] do
nnull[i]:=(q^(2*d[i])-1)*q^(2*d[i]*(r[i]-1));
od;

for i in [1..s] do
if((r[i] mod 2 = 0)=true) then
floor[i]:= r[i]/2;
else
floor[i]:= (r[i]-1)/2;
```

```
fi;
od;
sum:= 0;
for i in [1..s] do
prod1[i]:=1;
prod2[i]:=1;
od;


for i in [1..s] do
for j in [1..i-1] do
prod1[i]:= prod1[i]*((eps2[j]-rlok[j]^2)*rlok[j]+ rlok[j]*nnull[j]+ rlok[j]^2);
od;

for j in [i+1..s] do
prod2[i]:= prod2[i]*((eps2[j]-rlok[j]^2)*rlok[j]+ q^(2*d[j]*(2*r[j]-floor[j]-1))
           + (q^(2*d[j])-1)*q^(3*d[j]*r[j]-2*d[j])*(1+floor[j]));
od;
od;

for i in [1..s] do
sum:=sum+ (q^(2*d[i]*(2*r[i]-floor[i]-1))- rlok[i]^2
       + (q^(2*d[i])-1)*q^(3*d[i]*r[i]-2*d[i])*floor[i])*prod1[i]*prod2[i];
  od;


for i in [1..s] do
prod3:=prod3*((eps2[i]- rlok[i]^2)*rlok[i]+ rlok[i]^2+ nnull[i]*rlok[i]);
od;

zeile2:= (P/inf)*(2*sum+ ring^2*q^2+ q*prod3 - q*ring^2);


for j in [1..s] do
beta2[j]:= 2*(q^(d[j])-1)^2*q^(d[j])*q^(3*d[j]*(r[j]-1))*q^(2*d[j]*r[j]);
od;

for j in [1..s] do
p[j]:= (q^(2*d[j])-1)*(q^d[j]-1)*q^(3*d[j]*(r[j]-1))*q^(3*d[j]*r[j]);
od;

for j in [1..s] do
if((d[j] mod 2 = 1)=true) then
zu1:= zu1*p[j]*rlok[j]^2;
fi;
```

```
if((d[j] mod 2 = 1)=false) then
zu2:= zu2*(p[j]*(2*(q^d[j]-1)*q^(d[j]*(r[j]-1))*rlok[j]+ rlok[j]^2)
      + beta2[j]*rlok[j]*(q^(2*d[j]*(r[j]-1))+ q^(d[j]*(r[j]-1))*rlok[j]));
fi;
zu:= zu1*zu2;
od;

zeile3:= ((q*(q-1))/((q^2-1)*ring^2))*(zu-P*ring^2);

enull:= (zeile1 + zeile2 + zeile3)/P;
gnull:=(2-enull)/2;

return gnull;
end;
```

Die Eingabe von gglobal$(q, [d_1, ...d_s], [r_1, ..., r_s])$ mit den gewünschten Werten für die Zahl der Körperelemente q und der vektoriellen Darstellung der Grade d_i der Primpolynome p_i mit Exponenten r_i liefert nun das Geschlecht der Kurve $X_0(N)$.
Die Eingabe von gglobal$(q, [d], [r])$ und glokal(q, d, r) ermöglicht nun insbesondere einen Vergleich der Formel für das Geschlecht der Kurve $X_0(N)$ in der lokalen Situation $N = p^r$ mit der expliziten Formel für den lokalen Fall $N = p^r$ (festgehalten in (176) und (177)). Beim Test auf Kongruenzen modulo 6 des Grades d unseres Primpolynoms p wurden keine Abweichungen festgestellt.

Literatur

[Eis04] Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics 150, Springer Verlag, New York, 2004.

[Gei15] Geis, David: *Die Geschlechter der Modulkurven zu dünn besetzten Drinfeld-Moduln des Rangs drei: der globale Fall.* Universität des Saarlandes, Lehrstuhl Prof. Dr. Ernst-Ulrich Gekeler, Saarbrücken, 2015.

[Gek91] Gekeler, Ernst-Ulrich: *On Finite Drinfeld Modules.* Max-Planck-Institut für Mathematik Bonn 1989, Reprinted from Journal of Algebra Vol. 141, New York und London, 1991.

[Gek14] Gekeler, Ernst-Ulrich: *Towers of GL(r)-Type of Modular Curves.* Universität des Saarlandes, Saarbrücken, 2014.

[Gop88] Goppa, V.D.: *Geometry and Codes.* Springer-Science + Business Media, B.V., Computer Center of the Academy of the U.d.S.S.R., Moskau, 1988.

[Har93] Hartshorne, R.: *Algebraic Geometry.* Graduate Texts in Mathematics 52, Springer Verlag, New York, Berlin und Heidelberg, 1993.

[HJ08] Hirschfeld J.W.P., Korchmarós G., Torres F.: *Algebraic Curves Over a Finite Field.* Princeton Series in Applied Mathematics, Princeton University Press, Hardcover, Princeton, 2008.

[Hoc12] Hochster, Mel: *Lectures on commutative Algebra II.* Vorlesungsmanuskript in Michigan, University of Michigan, Math 615, Michigan, 2012.

[Iha81] Ihara, Y.: *Some remarks on the number of rational points of algebraic curves over finite fields.* J.Fac.Sci.Tokyo Volume 28, S. 721-724, Tokyo, 1981.

[Mar13] Markwig, Dr. Thomas: *Commutative Algebra.* Vorlesungsmanuskript in Kaiserslautern, in Latex geschrieben von Simon Hampe 2007/2008, Kaiserslautern, 2013.

[Sti09] Stichtenoth, H.: *Algebraic Function Fields and Codes.* Graduate Texts in Mathematics 254, Springer Verlag, Berlin und Heidelberg, 2009.

[TM07] Tsfasman M.A., Vladut S., Nagin D.: *Algebraic Geometric Codes: Basic Notions.* Mathematical Surveys and Monographs Volume 139, American Mathematical Society, USA, 2007.