Universität des Saarlandes
Naturwissenschaftlich-Technische Fakultät I
Mathematik

Masterarbeit

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

Der globale Fall

vorgelegt von
David Geis

im Januar 2015

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

Inhaltsverzeichnis

1 Einleitung

Wir betrachten eine glatte, irreduzible, projektive algebraische Kurve X über einem algebraisch abgeschlossenen Körper K. Das heißt $X \subset \mathbb{P}^n(K)$ ist die Verschwindemenge eines homogenen Primideals $I \subset K[x_0, \ldots, x_n]$, sodass die assoziierte Jacobimatrix in jedem Punkt von X Rang $n-1$ hat. Sind die definierenden Gleichungen von X bereits über einem Unterkörper $F \subset K$ definiert, so stellt sich die natürliche Frage nach der Existenz von Punkten $x \in X$ mit Koordinaten in F. Ist der Körper F endlich, so stellt sich unmittelbar die kombinatorische Frage nach der *Anzahl* $|X(F)|$ der Punkte in X über F.
Im allgemeinen Fall ist es jedoch schwierig, den genauen Wert von $|X(F)|$ zu bestimmen. Ist jedoch F_q der endliche Körper mit q Elementen und X eine über F_q definierte elliptische Kurve (das *Geschlecht* von X ist also eins) mit Aufpunkt $x_0 \in X(F_q)$, so können wir $|X(F_q)|$ genau bestimmen: es bezeichne ϕ die durch den Frobeniusautomorphismus $x \mapsto x^q$ induzierte Isogenie. Dann ist $X(F_q)$ gerade der Kern des separablen Morphismus $\mathbb{1} - \phi$. Damit erhalten wir $|X(F_q)| = \deg(\mathbb{1} - \phi)$. Durch Polarisation der Abbildung $\deg : End(X) \longrightarrow \mathbb{Q}$ erhält man eine Bilinearform Q mit $2 \cdot Q(f,g) = \deg(f+g) - \deg(f) - \deg(g)$; insbesondere kann man hieraus schließen, dass $\deg(f) = Q(f,f)$ eine quadratische Form ist und dass Q positiv definit ist. Wir erhalten mit Cauchy-Schwarz:

$$\begin{aligned} 4 \cdot 1 \cdot q = Q(\mathbb{1},\mathbb{1}) \cdot Q(\phi,\phi) \geq 4 \cdot Q(\mathbb{1},-\phi)^2 &= (\deg(\mathbb{1}-\phi) - \deg(\mathbb{1}) - \deg(\phi))^2 \\ &= (|X(F_q)| - 1 - q)^2. \end{aligned}$$

Dieses Ergebnis ist die Hasse-Schranke (1933), die (1949) von Weil wie folgt verallgemeinert wurde:

Theorem. *(Hasse-Weil-Schranke) Es sei X eine projektive, glatte, irreduzible Kurve vom Geschlecht g über F_q. Dann gilt:*

$$|X(F_q) - q - 1| \leq 2 \cdot g \cdot \sqrt{q}.$$

Wir bemerken, dass das obige Resultat Teil der sogenannten Weil-Vermutungen ist. Deren vollständiger Beweis wurde jedoch erst von Pierre Deligne (1974) erbracht.

Bezeichnen wir mit $N_q(g)$ die maximale Anzahl von Punkten einer Kurve vom Geschlecht g über dem endlichen Körper F_q, so folgt aus der Hasse-Weil-Schranke sofort

$$|N_q(g) - q - 1| \leq 2 \cdot g \cdot \sqrt{q}.$$

Nun stellt sich natürlich die Frage, ob die obige Abschätzung verbessert werden kann. Außerhalb der reinen Mathematik ist diese Fragestellung beispielsweise für die Theorie der Kodierungsverfahren interessant, die Kurven über endlichen Körpern und deren Gruppenstruktur zur Verschlüsselung verwenden; man erinnere sich an die von Goppa (1981) vorgestellten Goppa-Codes. Es ist klar, dass

man hierzu natürlich an Kurven interessiert ist, die möglichst viele Punkte über einem endlichen Körper besitzen, in der Erwartung, dass die Gruppenstruktur und damit deren Komplexität mit der Gruppenordnung wächst.
Ihara (1981) konnte mit einem einfachen Argument zeigen, dass die folgende Abschätzung für $N_q(g)$ gilt:

Theorem. *(Ihara-Schranke) Es gilt:*

$$2 \cdot N_q(g) \leq \sqrt{(8 \cdot q + 1) \cdot g^2 + (4 \cdot q^2 - 4 \cdot q) \cdot g} + 2 \cdot q + 2 - g.$$

Insbesondere ist die gegebene Abschätzung für $g > \frac{\sqrt{q} \cdot \sqrt{q} - 1}{2}$ schärfer als die Hasse-Weil-Schranke.

Diese Beobachtung und eine genaue Betrachtung der rechten Seite in der Ihara-Schranke legen es nahe, den wegen obiger Abschätzungen wohldefinierten Ausdruck

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

zu betrachten. Ein unmittelbares Korollar aus der Ihara-Schranke ist die folgende Abschätzung:

Korollar. *(Ihara) Es gilt:*

$$A_q \leq \frac{\sqrt{8 \cdot q - 1}}{2}.$$

Eine weitere, verfeinerte Abschätzung wurde schließlich von Drinfeld und Vladut gegeben:

Theorem. *(Drinfeld-Vladut-Schranke) Es gilt:*

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

Ihara hat gezeigt, dass hierbei sogar Gleichheit gilt, falls q ein Quadrat ist. Es ist nun wiederum eine natürliche Fragestellung, inwieweit die oben angegebene Abschätzung *effektiv* in dem Sinne ist, dass ein Turm von Kurven X_i mit $g(X_i) \to \infty$ existiert, der die gegebene Drinfeld-Vladut-Schranke realisiert. Analog kann man natürlich auch nach einem Turm von entsprechenden Funktionenkörpern suchen. Ein Turm von solchen Kurven beziehungsweise Funktionenkörpern heißt *asymptotisch optimal*. Ein Turm von Kurven Y_i heißt *asymptotisch gut*, falls

$$\limsup_{i \to \infty} \frac{Y_i(F_q)}{g(Y_i)} > 0.$$

Für einen Einstieg in die Konstruktion solcher Türme sei auf das Buch *Algebraic Geometric Codes: Basic Notions* [MT07] verwiesen. Dort findet man auch einen Beweis der Drinfeld-Vladut-Schranke. Beweise der übrigen zitierten Abschätzungen und mehr Hintergrundinformationen findet man beispielsweise im Buch [Sti09] sowie in der Arbeit [Iha81]. Für die allgemeine Theorie algebraischer Kurven sei auf das Buch [Har93] verwiesen.

Es stellt sich nun heraus, dass die obigen asymptotisch optimalen Kurven X_i durch gewisse Reduktionen spezieller Drinfeldscher Modulkurven realisiert werden können. Hintergründe hierzu finden sich beispielsweise in der Arbeit [Gek91]. Die Kontrolle des Geschlechts gestaltet sich hierbei als relativ aufwändig.

In der Arbeit [Gek14] wird nun eine gewisse neue Klasse sogenannter *dünn besetzter Drinfeld-Moduln vom Typ* (r, k) mit den zugehörigen Modulkurven $X^{r,k}(N)$ eingeführt. Hierbei sind r, k positive natürliche Zahlen und N ist ein nichtkonstantes Polynom mit Koeffizienten in F_q. Diese Modulkurven liefern galoissche Überlagerungen

$$\phi : X^{r,k}(N) \longrightarrow \mathbb{P}^1(C_\infty)$$

und verhalten sich bezüglich Rationalitätsfragen und Verzweigungseigenschaften ähnlich wie die klassischen Modulkurven über $\mathbb{Q}$. Hierbei bezeichnet C_∞ den komplettierten algebraischen Abschluss des Körpers $F_q((T^{-1}))$ der formalen Laurentreihen über F_q. Insbesondere lassen sich aus diesen neuen Modulkurven durch Quotientenbildung bezüglich einer geeigneten Untergruppe der Galoisgruppe von ϕ asymptotisch gute (siehe oben) Türme von Kurven über endlichen Körpern konstruieren.

Wir wollen in dieser Arbeit die Kurven vom Typ $X(N) := X^{3,2}(N)$ genauer betrachten. Genauer wollen wir für eine gewisse parabolische Untergruppe $P(N)$ der Galoisgruppe von ϕ eine explizite Formel für das Geschlecht der Kurven

$$X_0(N) := X_0^{3,2}(N) := X(N)/P(N)$$

herleiten. Als Anwendung wollen wir zeigen, dass diese Kurven $X_0(N)$ bei Reduktion nach einer geeigneten Primstelle des Grades eins von $F_q(T)$ asymptotisch gute Kurven über F_{q^3} liefern. Der Schlüssel zur Berechnung des Geschlechts liegt in der Riemann-Hurwitz-Formel, mit deren Hilfe wir das Geschlecht der Kurve $X_0(N)$ aus dem einfacher zu berechnenden Geschlecht von $X(N)$ über die galoissche Überlagerung

$$\psi : X(N) \longrightarrow X_0(N)$$

bestimmen können. Der Umweg über $X(N)$ zur Berechnung rührt daher, dass die Überlagerung

$$\pi : X_0(N) \longrightarrow \mathbb{P}^1(C_\infty)$$

nicht galoissch ist. Die Riemann-Hurwitz-Formel kann also nicht auf π angewendet werden.

Bevor wir mit den eigentlichen Untersuchungen beginnen, wollen wir kurz den Aufbau der Arbeit beschreiben. In Abschnitt 2 werden die grundlegenden Begriffe formuliert und die nötigen technischen Hilfsmittel in hinreichend präziser Form zusammengetragen. Im folgenden Abschnitt wird mit der Riemann-Hurwitz-Formel und den weiteren Resultaten aus Abschnitt 2 das Geschlecht von $X(N)$ bestimmt. Der vierte und längste Abschnitt beschäftigt sich mit der Entwicklung einer expliziten Formel für das Geschlecht der Kurve $X_0(N)$ für ein beliebiges nichtkonstantes $N \in F_q[T]$. Es stellt sich heraus, dass das Geschlecht in gewissem Sinne ein Polynom in q ist. Abschnitt 5 enthält schließlich einige Anwendungen und Folgerungen aus den Resultaten in Abschnitt 4. Insbesondere zeigen wir dort, dass die Kurven $X_0(N)$ bei geeigneter Reduktion asymptotisch gute Türme von Kurven über F_{q^3} liefern. Außerdem bestimmen wir alle Kurven vom Typ $X_0(N)$ mit Geschlecht höchstens hundert.

Danksagung. *Ich möchte mich bei allen Menschen bedanken, die mich während der Erstellung dieser Arbeit unterstützt haben. Mein ganz besonderer Dank gilt dabei Professor Gekeler, dessen nützliche Hinweise und kritische Bemerkungen in diversen Gesprächen stets in hohem Maße inspirierend gewesen sind. Außerdem bedanke ich mich bei Marius Bohn für die gelungene Zusammenarbeit und das stets angenehme Arbeitsklima. Letztlich danke ich meinen Eltern nicht nur für die finanzielle, sondern auch für die moralische Unterstützung während meines Studiums.*

2 Begriffliche Grundlagen

Wir wollen in diesem Abschnitt zunächst die für die weiteren Betrachtungen notwendigen Objekte und Notationen zusammentragen. Ferner sollen einige grundlegende Fakten zu den eingeführten Objekten vorgestellt werden. Wir beginnen mit den verwendeten Notationen.

Notation.

- $\mathbb{N} := \{0, 1, 2, \dots\}$, *die Menge der natürlichen Zahlen.*
- $\mathbb{Z} := \{0, 1, -1, 2, -2, \dots\}$, *die Menge der ganzen Zahlen.*
- $\mathbb{P} := \{2, 3, 5, 7, 11, \dots\}$, *die Menge der Primzahlen.*
- *i) Für eine Primzahl $p \in \mathbb{P}$ sei $F_p := \mathbb{Z}/(p \cdot \mathbb{Z})$ der (bis auf Isomorphie eindeutige) endliche Körper mit p Elementen.*
  ii) Ist $q = p^l$ für eine Primzahl $p \in \mathbb{P}$ und eine positive natürliche Zahl $l \in \mathbb{N}$, so bezeichne F_q die (bis auf Isomorphie eindeutige) Körpererweiterung von F_p mit Grad l: $F_q \supset F_p$ und $\dim_{F_p}(F_q) = l$.
  iii) Es bezeichne C_∞ den komplettierten algebraischen Abschluss des Körpers $F_q((T^{-1}))$ der formalen Laurentreihen über F_q.
- *Unter einem Ring R verstehen wir stets einen kommutativen Ring mit Einselement. Ist $f \in R$, so bezeichne (f) das von f in R erzeugte Hauptideal. Die Einheitengruppe von R bezeichnen wir mit R^*.*
- *Ist M ein R-Modul und $m \in M$, so bezeichne $< m >$ den vom Element m erzeugten Untermodul von M. Ist $M = R^k$ für eine positive natürliche Zahl k, so identifizieren wir M mit der Menge der k-dimensionalen Spaltenvektoren mit Einträgen in R. Wir bezeichnen für $1 \leq i \leq k$ mit e_i den i-ten Standardbasisvektor von M.*
- *Es seien R ein Ring und m, n positive ganze Zahlen. Wir bezeichnen mit $Mat(m \times n, R)$ den Ring der $m \times n$ Matrizen über R. Weiter bezeichne $GL(n, R)$ die Menge aller invertierbaren $n \times n$ Matrizen mit Koeffizienten in R. Mit $SL(n, R)$ bezeichnen wir die Menge aller Matrizen aus $GL(n, R)$ mit Determinante eins.*
- *Um eine kompakte Notation zu ermöglichen, verwenden wir gelegentlich das Symbol $\mathbb{1}$. Dieses bedeutet in Abschnitt 2 die Identitätsabbildung und in den übrigen Abschnitten bezeichnet $\mathbb{1}$ stets die Einheitsmatrix (jeweils auf einer vom Kontext abhängigen Menge beziehungsweise in einer vom Kontext abhängigen Dimension).*

Als nächstes geben wir die Definition und einige einfache Eigenschaften des für alle weiteren Betrachtungen zugrundeliegenden Ringes $R(N)$.

2.1 Definition und Struktur des Ringes $R(N)$

Wir beginnen mit der Definition von $R(N)$.

Definition 1. Es sei $p \in \mathbb{P}$ und $0 < l \in \mathbb{N}$. Für einen festen endlichen Körper F_q mit $q = p^l$ sei $A := F_q[T]$ der Polynomring in einer Variablen T. Wir verwenden auf A die Standardgraduierung $\deg : A \longrightarrow \mathbb{N} \cup \{-\infty\}$, das heißt $\deg(T) = 1$ und $\deg(0) = -\infty$. Für ein nichtkonstantes, normiertes $N \in A$ definieren wir dann den Ring $R(N)$ als den Quotienten $R(N) := A/(N)$.

Die folgende Bemerkung ist zwar recht trivial, jedoch für das Folgende unverzichtbar.

Bemerkung 1. *Für nichtkonstantes $N \in A$ gilt offenbar $F_q \subset R(N)$ via*

$$i : F_q \longrightarrow R(N), a \longmapsto \overline{a}. \tag{1}$$

Hierbei bezeichnet $\overline{a}$ die Restklasse von a modulo N. Der Ring $R(N)$ ist überdies ein F_q-Vektorraum der Dimension $\deg(N)$*. Hiermit ergibt sich schließlich*

$$|R| = q^{\deg(N)}. \tag{2}$$

Wir wollen die Struktur des Ringes $R(N)$ an dieser Stelle etwas genauer beschreiben. Hierzu formulieren wir das folgende einfache Lemma:

Lemma 1. *Der Ring A ist ein Hauptidealring und insbesondere faktoriell. Es ist also jedes $N \in A$ von der Form*

$$N = \alpha \cdot \prod_{i=1}^{s} {p_i}^{r_i}. \tag{3}$$

Hierbei sind die p_i paarweise verschiedene normierte Primelemente des Ringes A, α ist eine Einheit von A und alle r_i sowie s liegen in $\mathbb{N}$. Die obige Darstellung ist bis auf Umordnung der Faktoren eindeutig.

Beweis. Wir haben auf A die Graduierung $\deg : A \longrightarrow \mathbb{N} \cup \{-\infty\}$ zur Verfügung, die A zum euklidischen Ring macht. Da jeder euklidische Ring ein Hauptidealring ist, folgt die Behauptung. □

Als nächstes brauchen wir eine gewisse Variante des chinesischen Restsatzes, die es uns erlauben wird, den Ring $R(N)$ in kanonischer Weise mit einem direkten Produkt kanonisch bestimmter lokaler Ringe zu identifizieren. Wir geben dazu das folgende Lemma, das im Wesentlichen alle Überlegungen in Abschnitt 4 dominieren wird.

Lemma 2. *Es sei N normiert und $N = \prod_{j=1}^{s} {p_j}^{r_j}$ die wohlbestimmte Faktorisierung durch normierte Primelemente und $R := R(N)$. Für $1 \leq i \leq s$ bezeichnen wir mit $\tilde{\alpha_i} : A \longrightarrow A/({p_i}^{r_i})$ die natürliche Restklassenprojektion. Für alle betrachteten i ist das Hauptideal (N) offenbar im Kern der Abbildung $\tilde{\alpha_i}$ enthalten. Wir erhalten also einen Ringhomomorphismus $\alpha_i : R \longrightarrow A/({p_i}^{r_i})$. Diese Homomorphismen $\alpha_1, \ldots, \alpha_s$ induzieren einen kanonischen Isomorphismus*

$$\alpha = (\alpha_1, \ldots, \alpha_s) : R \longrightarrow \prod_{j=1}^{s} A/({p_j}^{r_j}). \tag{4}$$

Es folgt $|R| = \prod_{j=1}^{s} |A/{p_j}^{r_j}| = \prod_{j=1}^{s} |R({p_j}^{r_j})|$*, das heißt die Mächtigkeit von* R *ist das Produkt der Mächtigkeiten der lokalen Komponenten (siehe Bemerkung 2) von* R*.*

Beweis. Der Beweis ist der gleiche wie für den Ring $\mathbb{Z}$. Wir bezeichnen das von ${p_j}^{r_j}$ erzeugte Ideal in A mit I_j. Für die Restklasse von $f \in A$ modulo I_j schreiben wir f_j. Betrachte den natürlichen Homomorphismus:

$$\alpha : A \longrightarrow \prod_{j=1}^{s} A/{p_j}^{r_j}, f \longmapsto \prod_{j=1}^{s} f_j. \tag{5}$$

Der Kern von α ist offensichtlich genau das von N erzeugte Ideal. Wir müssen also nur zeigen, dass α surjektiv ist. Dazu reicht es zu zeigen, dass für ein fixiertes j ein $f \in A$ existiert, sodass $f - 1 \in I_j$ und $f \in I_k$ für alle $j \neq k$. Für $j \neq k$ gilt aber $\gcd({p_j}^{r_j}, {p_k}^{r_k}) = 1$ und aus dem kleinen Satz von Bézout folgt die Existenz von Elementen $a_k, b_k \in A$ mit

$$a_k \cdot {p_j}^{r_j} + b_k \cdot {p_k}^{r_k} = 1. \tag{6}$$

Wir setzen $f := \prod_{j \neq k} b_k \cdot {p_k}^{r_k}$ und sehen, dass f das Gewünschte leistet.

□

In der folgenden Bemerkung rechtfertigen wir den Ausdruck "lokale Komponente" im obigen Lemma; außerdem legen wir fest, was wir unter einer *Primfaktorisierung* verstehen wollen und listen einige einfache aber wichtige Konsequenzen auf.

Bemerkung 2. *i) Sei* r *eine natürliche Zahl. Für ein primes* $\pi \in A$ *betrachten wir den Ring* $R := R(\pi^r) = A/(\pi^r)$*. Bekanntlich ist jedes Primideal* $\mathfrak{p}' \subset R$ *von der Form* $\mathfrak{q}/(\pi^r)$ *für ein Primideal* $\mathfrak{q} \subset A$ *mit* $\pi^r \in \mathfrak{q}$*. Da* $\mathfrak{q}$ *prim, bedeutet dies* $\pi \in \mathfrak{q}$*. Da* A *aber ein Hauptidealring ist, folgt, dass* π *bereits ein Erzeuger von ganz* $\mathfrak{q}$ *ist.* R *ist also ein lokaler Ring mit maximalem Ideal* $\mathfrak{p} := (\pi)/(\pi^r)$*. Wir haben auf* R *daher eine sogenannte verstümmelte Bewertungsfunktion zur Verfügung:*

$$v_{\mathfrak{p}} : R \longrightarrow \{0, 1, \ldots, r\} \tag{7}$$

$$f \longmapsto \sup\{i \mid f \in \mathfrak{p}^i\}. \tag{8}$$

ii) Es sei $N \in A$ *nichtkonstant und normiert. Dann existieren eindeutig bestimmte normierte irreduzible Polynome* $p_j \in A$ *und natürliche Zahlen* r_j *mit*

$$N = \prod_{j=1}^{s} p_j^{r_j}. \tag{9}$$

Eine solche Faktorisierung nennen wir die Primfaktorisierung von N*.*
iii) Sei $N \in A$ *normiert und nichtkonstant mit zugehöriger Primfaktorisierung*

$N = \prod_{j=1}^{s} p_j^{r_j}$. Setze $R := R(N)$ und $R_i := R(p_i^{r_i})$ für $1 \leq i \leq s$. Der Isomorphismus α aus obigem Lemma 2 induziert für positive ganze Zahlen n, m einen natürlichen Ringisomorphismus

$$\tilde{\alpha}_{mn} : Mat(m \times n, R) \longrightarrow \prod_{j=1}^{s} Mat(m \times n, R_j). \tag{10}$$

Dieser Isomorphismus wirkt dabei auf eine Matrix M, indem $\alpha = (\alpha_1, \ldots, \alpha_s)$ auf jeden Eintrag der Matrix M wirkt:

$$(M_{ij})_{ij} \longmapsto (\alpha(M_{ij}))_{ij}. \tag{11}$$

Nach Definition liefert $\tilde{\alpha}_{nn}$ durch Einschränken sogar den folgenden natürlichen Isomorphismus von Gruppen:

$$\tilde{\alpha}_{nn} : GL(n, R) \longrightarrow \prod_{j=1}^{s} GL(n, R_j). \tag{12}$$

Man beachte hierzu, dass α Einheiten auf Einheiten abbildet.
iv) Sind $x, y, g, h \in GL(n, R)$, so gilt mit $\tilde{\alpha} := \tilde{\alpha}_{nn}$ nach Teil iii)

$$x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} = h \tag{13}$$

genau dann, wenn:

$$\tilde{\alpha}(x) \cdot \tilde{\alpha}(y) \cdot \tilde{\alpha}(g) \cdot \tilde{\alpha}(y)^{-1} \cdot \tilde{\alpha}(x)^{-1} = \tilde{\alpha}(h). \tag{14}$$

v) Es sei M eine beliebige $m \times n$ Matrix mit Einträgen in R und $b \in R^m$. Der Isomorphismus $\tilde{\alpha} := \tilde{\alpha}_{mn}$ wirke wie in Teil iii) auf beliebige Matrizen über R. Dann hat das Gleichungssystem

$$M \cdot X = b \tag{15}$$

genau dann eine Lösung $X \in R^n$, wenn das Gleichungssystem

$$\tilde{\alpha}(M) \cdot Y = \tilde{\alpha}(b) \tag{16}$$

eine Lösung $Y \in (\prod_{j=1}^{s} R_j)^n$ hat, wobei $Y = \tilde{\alpha}(X)$.

Das nächste Konzept, das wir benötigen, ist das des projektiven Raumes $\mathbb{P}^n(R)$ über dem Ring $R := R(N)$. Falls R ein Körper ist, so können wir $\mathbb{P}^n(R)$ mit der Menge der eindimensionalen Unterräume von R^{n+1} identifizieren. Diese Tatsache veranlasst uns zur folgenden Definition.

Definition 2. Sei $R := R(N)$ für ein normiertes, nichtkonstantes $N \in A$. Wir definieren den projektiven Raum $\mathbb{P}^n(R)$ als die Menge aller freien Untermoduln U vom Rang eins von R^{n+1}, für die eine Zerlegung der Form

$$R^{n+1} = U \oplus V \tag{17}$$

existiert, für einen Untermodul V von R^{n+1}.

Wir wollen diese relativ abstrakte Definition, um später etwas komfortabler damit arbeiten zu können, in der folgenden Bemerkung etwas konkreter machen.

Bemerkung 3. *i) Wir bemerken, dass der Modul V aus obiger Definition nach Konstruktion projektiv ist. Ist der zugrundeliegende Ring R lokal, so bedeutet dies, dass V bereits frei ist. In diesem Fall besteht die Menge $\mathbb{P}^n(R)$ offenbar genau aus der Menge der Vektoren $v \in R^{n+1}$, die sich zu einer Basis von R^{n+1} ergänzen lassen, modulo der Operation von R^*. Genauer: Wir bezeichnen mit P' die Menge aller invertierbaren Matrizen, deren erste Spalte ein Vielfaches des Standardbasisvektors e_1 ist. Dann ist die Abbildung*

$$f : GL(n+1,R)/P' \longrightarrow \mathbb{P}^n(R) \tag{18}$$

$$\overline{m} \longmapsto < m \cdot e_1 > \tag{19}$$

wohldefiniert und eine Bijektion (siehe Proposition 2 auf Seite 19).
ii) Sei $N = \prod_{j=1}^{s} {p_j}^{r_j}$ und $R = R(N)$ im Sinne von Definition 1. Die Bedingung (17) aus Definition 2 besteht aus $n+1$ linearen Gleichungen über dem Ring R. Ein solches Gleichungssystem ist nach Bemerkung 2, Teil v) genau dann erfüllt, wenn für alle $1 \leq i \leq s$ das unter dem Homomorphismus α_i korrespondierende Gleichungssystem erfüllt ist. Setzen wir $R_i := R({p_i}^{r_i})$, so können wir in diesem Fall also ein Element von $\mathbb{P}^n(R)$ mit einem Tupel von Elementen aus $\mathbb{P}^n(R_i)$ für $1 \leq i \leq s$ identifizieren. Da nach Bemerkung 2 alle R_i lokal sind, können wir unter Beachtung von i) ein Element aus $\mathbb{P}^n(R)$ mit einem Tupel $(x_1, \ldots, x_s)$ identifizieren für geeignete $x_i \in \mathbb{P}^n(R_i)$.
iii) Wir bemerken, dass wir noch eine dritte Beschreibung von $\mathbb{P}^n(R)$ zur Verfügung haben. Ein Vektor $v = (v_1, ..., v_{n+1}) \in R^{n+1}$ heißt primitiv, falls das von den Einträgen von v erzeugte Ideal I_v bereits der ganze Ring R ist. Mit dieser Bezeichnung gilt:

$$\mathbb{P}^n(R) = \{v \in R^{n+1} | v \text{ ist primitiv}\}/R^*. \tag{20}$$

Ein weiteres Modell für den projektiven Raum ist also gegeben durch die Menge aller primitiven Vektoren aus R^{n+1} modulo der Operation von R^*.

Mit dieser Bemerkung sind wir in der Lage, für ein beliebiges nichtkonstantes $N \in A$ ein Repräsentantensystem für $\mathbb{P}^2(R(N))$ anzugeben. Der Nutzen des folgenden Repräsentantensystems für unsere Zwecke wird sich jedoch erst im weiteren Verlauf zeigen. Wir beginnen mit dem Fall eines Ringes, der bereits selbst lokal ist; das heißt wir betrachten ein primäres $N \in A$.

Lemma 3. *Sei N normiert und primär. Der Ring $R := R(N)$ ist lokal (vergleiche Bemerkung 2) und wir schreiben $\mathfrak{p}$ für das zugehörige maximale Ideal. Betrachte die Menge aller Matrizen der Form*

$$RS_1(R) := \left\{ \begin{pmatrix} 1 & 0 & 0 \\ c_2 & 1 & 0 \\ c_3 & 0 & 1 \end{pmatrix} \;\middle|\; c_2, c_3 \in R \right\}, \tag{21}$$

$$RS_2(R) := \left\{ \begin{pmatrix} c_1 & 1 & 0 \\ 1 & 0 & 0 \\ c_3 & 0 & 1 \end{pmatrix} \;\middle|\; c_1 \in \mathfrak{p}, c_3 \in R \right\}, \tag{22}$$

$$RS_3(R) := \left\{ \begin{pmatrix} c_1 & 1 & 0 \\ c_2 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \;\middle|\; c_1, c_2 \in \mathfrak{p} \right\}. \tag{23}$$

Dann bildet die disjunkte Vereinigung $RS_1(R) \cup RS_2(R) \cup RS_3(R)$ ein Repräsentantensystem für $\mathbb{P}^2(R)$. Insbesondere erhalten wir für die Mächtigkeit von $\mathbb{P}^2(R)$:

$$|\mathbb{P}^2(R)| = |R|^2 + |R| \cdot |\mathfrak{p}| + |\mathfrak{p}|^2. \tag{24}$$

Beweis. Sei x die erste Spalte einer Matrix $\eta \in GL(3, R)$. Da R lokal mit maximalem Ideal $\mathfrak{p}$ und $\det(\eta) \in R^*$, folgt, dass nicht alle Einträge von x in $\mathfrak{p}$ liegen können: man entwickle einfach $\det(\eta)$ nach der ersten Spalte. Sei i minimal mit $x_i \notin \mathfrak{p}$. Wir bemerken, dass i wohlbestimmt ist. Nach Multiplikation mit einer Einheit von R können wir ohne Einschränkung annehmen, dass $x_i = 1$. Nach Wahl von i gilt dann offenbar $x \in RS_i(R)$. Die Wohlbestimmtheit von i bedeutet die Disjunktheit der obigen Vereinigung. Da außerdem für $1 \leq i \leq 3$ je zwei verschiedene Elemente aus $RS_i(R)$ offenbar nicht äquivalent sind, folgt die Behauptung. □

Zusammen mit Bemerkung 3, Teil ii) liefert dieses Lemma sofort die folgende Proposition:

Proposition 1. *Sei $N \in A$ nichtkonstant und normiert. Die zugehörige Primfaktorisierung sei gegeben durch $N = \prod_{j=1}^{s} {p_j}^{r_j}$. Es bezeichne $\mathfrak{p}_j$ das von p_j in $R_j := R({p_j}^{r_j})$ erzeugte maximale Ideal. Weiter sei $R := R(N)$ und wir betrachten die bijektive Abbildung $\tilde{\alpha} := \tilde{\alpha}_{nn} : GL(n, R) \longrightarrow \prod_{j=1}^{s} GL(n, R_j)$ aus Bemerkung 2, Teil iii) auf Seite 8-9. Dann gilt:*
Die Menge $\prod_{j=1}^{s}(RS_1(R_j) \cup RS_2(R_j) \cup RS_3(R_j))$ kann über die Abbildung $\tilde{\alpha}^{-1}$ mit einem Repräsentantensystem für $\mathbb{P}^2(R)$ identifiziert werden. Insbesondere erhalten wir:

$$|\mathbb{P}^2(R)| = \prod_{j=1}^{s} \left(|R_j|^2 + |R_j| \cdot |\mathfrak{p}_j| + |\mathfrak{p}_j|^2 \right). \tag{25}$$

Insgesamt zerfällt $\mathbb{P}^2(R)$ also in 3^s viele Klassen.

Wir schließen die Strukturbetrachtung des Ringes $R(N)$ für den Moment mit der folgenden Bemerkung ab, die erklärt, wie die Größe $\mathfrak{p}_j$ aus dem obigen Lemma über die Grade von p_j und deren Multiplizitäten r_j in N berechnet werden kann. Im nächsten Abschnitt wenden wir uns dann der Riemann-Hurwitz-Formel zu.

Bemerkung 4. *Ist $N \in A$ nichtkonstant und normiert mit Primfaktorisierung*

$$N = \prod_{j=1}^{s} {p_j}^{r_j} \tag{26}$$

mit

$$\deg(p_j) = d_j, \tag{27}$$

so erhalten wir:

$$|\mathfrak{p}_j^k| = q^{d_j \cdot (r_j - k)}. \tag{28}$$

Um dies einzusehen betrachten wir für $0 \leq k \leq r_j - 1$ die folgenden exakten Sequenzen (endlicher und damit) endlichdimensionaler F_q-Vektorräume:

$$\{0\} \longrightarrow \mathfrak{p}_j^{k+1} \longrightarrow \mathfrak{p}_j^k \longrightarrow \mathfrak{p}_j^k/\mathfrak{p}_j^{k+1} \longrightarrow \{0\}. \tag{29}$$

Damit können wir iterativ die Größen $|\mathfrak{p}_j^k|$ für $1 \leq k \leq r_j - 1$ bestimmen, was letztlich zu der oben gegebenen Formel führt. Man beachte dazu, dass die alternierende Summe der Dimensionen der Vektorräume, die durch eine exakte Sequenz verbunden sind, gleich null ist. Außerdem gilt:

$$|\mathfrak{p}_j^k/\mathfrak{p}_j^{k+1}| = |R({p_j}^{r_j})/\mathfrak{p}_j| = |A/p_j| = |{F_q}^{d_j}|. \tag{30}$$

Dies ermöglicht es uns, die Größe $|\mathfrak{p}_j|$ aus der nullten exakten Sequenz zu bestimmen. Damit sind dann die Größen $|\mathfrak{p}_j^k|$ aus den restlichen Sequenzen bestimmbar.

2.2 Die Riemann-Hurwitz-Formel

Wir wollen uns nun der in der Einleitung angesprochenen Riemann-Hurwitz-Formel zuwenden und diese etwas präziser formulieren. Dazu erinnern wir zuerst an einige Begriffe und Tatsachen aus der Verzweigungstheorie algebraischer Kurven. Wir werden die meisten Aussagen nicht beweisen, weil es sich um einschlägige Standardresultate handelt, die gut in der Fachliteratur zu finden sind. Es sei hierzu auf das vierte Kapitel von [Har93] sowie auf das Buch [Sti09] verwiesen.

Bemerkung 5. *Wenn im Folgenden die Rede von algebraischen Kurven ist, dann ist dabei stets eine glatte, projektive, irreduzible algebraische Kurve gemeint, die über einem algebraisch abgeschlossenen Körper positiver Charakteristik definiert ist.*

Wir wollen als nächstes den Begriff der Verzweigungsfiltrierung für galoissche Überlagerungen $\phi : X \longrightarrow Y$ algebraischer Kurven einführen. Dazu müssen wir noch etwas Vorarbeit leisten. Den Anfang macht die folgende Definition.

Definition 3. Es sei $\phi : X \longrightarrow Y$ eine verzweigte, galoissche Überlagerung algebraischer Kurven in Charakteristik p mit Galoisgruppe G. Für einen abgeschlossenen Punkt $x \in X$ bezeichnen wir mit π_x einen Erzeuger des maximalen Ideals $\mathfrak{m}_x$ im lokalen Ring $\mathcal{O}_{X,x}$ bei x und mit $G_x \subset G$ die Fixgruppe von x. Wir definieren dann für alle $i \in \mathbb{N}$ die Gruppe

$$G_{x,i} := \{\sigma \in G \mid \forall y \in \mathcal{O}_{X,x} : \sigma(y) \equiv y \bmod \pi_x^{i+1}\}. \tag{31}$$

Dann ist $G_{x,i} = \{1\}$ für alle hinreichend großen i.

Bemerkung 6. *Es ist klar, dass die obige Definition von $G_{x,i}$ nicht von der Wahl des Erzeugers von $\mathfrak{m}_x$ abhängt. Weiterhin gilt $G_{x,i} \supset G_{x,i+1}$ und $G_{x,i}$ ist eine normale Untergruppe von G für alle i. Außerdem ist $G_{x,0} = G_x$ und $G_{x,0}/G_{x,1}$ ist zyklisch mit einer zu p koprimen Ordnung. Letztlich bemerken wir noch, dass $G_{x,1}$ dann eine p-Gruppe ist.*

Mit dieser Bemerkung sind wir nun in der Lage, den Begriff der Verzweigungsfiltrierung und der Verzweigungsfunktion zu definieren:

Definition 4. i) Die absteigende Kette von normalen Untergruppen von G gegeben durch

$$G_{x,0} \supset G_{x,1} \supset G_{x,2} \supset \dots \tag{32}$$

heißt Verzweigungsfiltrierung.
ii) Für ein $\mathbb{1} \neq \sigma \in G$ definieren wir

$$i_x(\sigma) := \sup\{i \mid \sigma \in G_{x,i}\} + 1. \tag{33}$$

Die Abbildung $i_x : G_x \setminus \{\mathbb{1}\} \longrightarrow \mathbb{N}$, die jedem nichttrivialen $\sigma \in G$ den Wert $i_x(\sigma)$ zuordnet, heißt Verzweigungsfunktion. Für ein $x \in X$ definieren wir die Verzweigungszahl als die Größe

$$a_x := \sum_{\mathbb{1} \neq \sigma \in G} i_x(\sigma). \tag{34}$$

iii) Die Überlagerung $\phi : X \longrightarrow Y$ heißt *moderat verzweigt* in $x \in X$, falls $G_{x,2}$ die triviale Gruppe ist. Ist $G_{x,1}$ bereits trivial, so heißt die Überlagerung ϕ *zahm verzweigt*.

In der nächsten Bemerkung geben wir ein Kriterium für die Verzweigtheit von ϕ in $x \in X$ über die Verzweigungszahl; ferner sehen wir, dass die Verzweigungszahlen bei moderater Verzweigung relativ einfach aus der Verzweigungsfiltrierung gewonnen werden können.

Bemerkung 7. *Wir haben die folgende Äquivalenz:*

$$a_x = 0 \Longleftrightarrow G_x = \{\mathbb{1}\}. \tag{35}$$

Folglich ist ϕ genau dann in $x \in X$ verzweigt, falls $a_x \neq 0$. Ist nun ϕ außerdem moderat verzweigt in $x \in X$, so gilt $i_x(\sigma) = 1$ für alle $\sigma \in G_x \setminus G_{x,1}$ und für alle $\sigma \in G_{x,1} \setminus G_{x,2}$ haben wir $i_x(\sigma) = 2$. Insgesamt ergibt sich in diesem Fall:

$$a_x = |G_x| + |G_{x,1}| - 2. \tag{36}$$

Die Gruppe $G_{x,1}$ ist dann die wohlbestimmte p-Sylow-Untergruppe von G_x.

Es sei an dieser Stelle daran erinnert, dass die Eulerzahl $\chi(X)$ einer algebraischen Kurve X über die Beziehung

$$\chi(X) = 2 - 2 \cdot g(X) \tag{37}$$

mit dem Geschlecht $g(X)$ der Kurve X in Zusammenhang steht. Das Geschlecht $g(X)$ der Kurve X ist hierbei bekanntlich definiert als

$$g(X) := \sup\{\deg(D) - \mathfrak{l}(D) + 1 \mid D \in Div(X)\}, \tag{38}$$

wobei $Div(X)$ die Menge der Divisoren auf X und $\mathfrak{l}(D)$ die Dimension des Riemann-Roch-Raumes $\mathfrak{L}(D) := \{x \in K(X) \mid (x) \geq -D\}$ bezeichnet. Hier soll $K(X)$ den zu X gehörigen Funktionenkörper bezeichnen und (x) den vom Element x erzeugten Hauptdivisor. Damit sind wir nun in der Lage, eine für unsere Zwecke geeignete, präzise Formulierung der Riemann-Hurwitz-Formel zu geben.

Theorem 1. *Sei $\phi : X \longrightarrow Y$ eine verzweigte galoissche Überlagerung algebraischer Kurven mit Galoisgruppe G. Die Eulerzahl $\chi(X)$ von X sei $\chi(X) = e$ und Y habe Eulerzahl $\chi(Y) = e'$. Dann gilt:*

$$e = |G| \cdot e' - \sum_{x \in X} a_x. \tag{39}$$

Einen Beweis dieser Aussage findet man in [Har93]. Angesichts der Korrespondenz zwischen algebraischen Kurven und algebraischen Funktionenkörpern, verweisen wir alternativ noch einmal auf das Buch [Sti09], in dem die äquivalente Version des obigen Theorems aus der Sicht der Funktionenkörper behandelt wird.

Ist nun eine Überlagerung $\phi : X \longrightarrow Y$ algebraischer Kurven gegeben, so reicht zur Auswertung der obigen Formel für e offenbar die Kenntnis der Größen e', $|G|$, a_x. Falls ϕ überdies in einem Punkt $x \in X$ lediglich moderat verzweigt ist, so reicht nach Bemerkung 7 zur Bestimmung von a_x die Kenntnis der Größen $|G_x|$, $|G_{x,1}|$. Ist ϕ sogar zahm verzweigt in $x \in X$, so reicht bereits die Kenntnis von $|G_x|$ zur Bestimmung von a_x.

Letztlich formulieren wir noch eine Bemerkung, die wir im nächsten Unterabschnitt benötigen werden.

Bemerkung 8. *Beachte, dass jede zyklische Untergruppe C' von $GL(n, F_q)$ der Ordnung $q^n - 1$ das Bild einer Einbettung $\iota : F_{q^n}^* \longrightarrow GL(n, F_q)$ ist: Sei α ein Erzeuger von C' und $\mu = \mu_\alpha(X)$ das zugehörige Minimalpolynom über F_q. Wir zeigen, dass $\deg(\mu) = n$ und dass μ irreduzibel ist:*
i) Betrachte die Körpererweiterung L von F_q, die von den Eigenwerten von α erzeugt wird. Über L hat α eine Jordan-Form und da die Ordnung von α teilerfremd zu $char(F_q) = p$ ist, folgt, dass alle Jordan-Blöcke Länge eins haben: α ist über L sogar diagonalisierbar.
ii) Da außerdem die Primteiler von μ den Bahnen des Frobeniushomomorphismus $x \longmapsto x^q$ auf der Menge der Eigenwerte von α entsprechen, folgt die Quadratfreiheit von μ.
iii) Sei $\mu = \prod_{j=1}^{s} \mu_j$ eine Zerlegung von μ in irreduzible Faktoren. Für die Grade der Faktoren gelte $d_j := \deg(\mu_j)$ und $\sum_{j=1}^{s} d_j \leq n$. Beachte, dass

$\prod_{j=1}^{s}(q^{d_j}-1) \leq q^n - 1$ *mit Gleichheit genau dann, wenn* $s = 1$ *und* $d_1 = n$.
iv) Wir haben natürliche Isomorphismen:

$$F_q[\alpha] \cong F_q[X]/\mu(X) \cong \prod_{j=1}^{s} F_q[X]/\mu_j(X) \cong \prod_{j=1}^{s} F_{q^{d_j}}. \tag{40}$$

Das bedeutet: $q^n - 1$ *teilt* $|F_q[\alpha]^*| = \prod_{j=1}^{s}(q_j^d - 1)$. *Aus Teil iii) folgt nun die Irreduzibilität von* μ *und dass* $\deg(\mu) = n$. *Insbesondere gilt: das charakteristische Polynom* $\chi := \chi_\alpha(X)$ *von* α *stimmt mit* μ *überein.*
Sei nun λ *ein Eigenwert von* α. *Das charakteristische Polynom der Matrix* m_λ, *die die Multiplikation mit* λ *in* $F_{q^n} \cong F_q[X]/(\mu(X))$ *als* F_q*-lineare Abbildung beschreibt, ist nun aber gerade* μ. *Das heißt* $M \cdot m_\lambda \cdot M^{-1} = \alpha$ *für eine gewisse invertierbare Matrix* M*:* λ *ist also eine primitive* q^n-1*-te Einheitswurzel. Damit erhalten wir mit* $\lambda \longmapsto M \cdot m_\lambda \cdot M^{-1}$ *eine Einbettung* ι, *wie gewünscht. Insbesondere ergibt sich, dass für jede zyklische Untergruppe* C' *der Ordnung* $q^n - 1$ *von* $GL(n, F_q)$ *ein* ι *existiert, sodass* C' *konjugiert ist zum Bild der Einbettung*

$$\iota : F_{q^n}^* \longrightarrow GL(n, F_q) \tag{41}$$

$$x \longmapsto m_x, \tag{42}$$

wobei m_x *die Multiplikation mit* x *beschreibt. Ist eine Gruppe* C' *das Bild einer Einbettung* ι *wie in (41), so nennen wir* C' *vom Typ* $Car(n)$ *(siehe Theorem 2).*

Damit haben wir alle benötigten Hilfsmittel an der Hand und können nun die der Arbeit zugrundeliegende Problemstellung genau formulieren.

2.3 Formulierung der Problemstellung

Wir kehren nun zu unserem Ausgangsproblem zurück. Wir setzen von nun an stets voraus, dass $N \in A$ normiert ist, und dass $N \notin F_q$ gilt. Wir betrachten die algebraischen Kurven $X(N) := X^{3,2}(N)$ und $X_0(N) := X_0^{3,2}(N)$ aus [Gek14] zusammen mit dem Diagramm verzweigter Überlagerungen:

$$\begin{array}{ccc} X(N) & & \\ \downarrow & \searrow & \\ X(1) & \longleftarrow & X_0(N). \end{array} \tag{43}$$

Unser Ziel ist die explizite Berechnung des Geschlechts $g(X_0(N))$ der Modulkurve $X_0(N)$ für ein beliebiges nichtkonstantes $N \in A$. Wir wollen in dieser Arbeit jedoch keine explizite Beschreibung der Konstruktion der Kurven $X(N)$, $X_0(N)$ geben. Stattdessen wollen wir die Existenz und einige benötigte Eigenschaften des Diagramms (43) in dem folgenden Theorem festhalten, dessen Beweis in der Arbeit [Gek14] zu finden ist.

Theorem 2. *Es sei* l *eine positive natürliche Zahl und* $p \in \mathbb{P}$. *Setze* $q := p^l$ *und betrachte* $A := F_q[T]$. *Für jedes nichtkonstante* $N \in A$ *existiert ein Diagramm*

verzweigter Überlagerungen

$$\begin{array}{ccc} X(N) & & \\ \downarrow & \searrow & \\ X(1) & \longleftarrow & X_0(N) \end{array} \tag{44}$$

mit den folgenden Eigenschaften:
i) Für alle nichtkonstanten $N \in A$ ist $X(N)$ eine glatte, projektive, irreduzible Kurve über dem Körper C_∞. Außerdem ist durch die sogenannte j*-Invariante ein Isomorphismus*

$$\mathrm{j} : X(1) \longrightarrow \mathbb{P}^1(C_\infty) \tag{45}$$

gegeben. Wir bezeichnen die Abbildung $X(N) \longrightarrow X(1)$ mit ϕ und die Abbildung $X(N) \longrightarrow X_0(N)$ heiße ψ:

$$\phi : X(N) \longrightarrow X(1), \tag{46}$$
$$\psi : X(N) \longrightarrow X_0(N). \tag{47}$$

Wir setzen weiter

$$Z := \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \;\middle|\; a \in F_q^* \right\}. \tag{48}$$

Für positives ganzes n nennen wir eine Gruppe $H \subset GL(n, F_q) \subset GL(n, R(N))$ vom Typ $Car(n)$, falls H die Multiplikation innerhalb des Körpers F_{q^n} als lineare Abbildung im Matrizenring $GL(n, F_q) \subset GL(n, R(N))$ realisiert: das heißt, falls eine Einbettung

$$\iota : F_{q^n}^* \longrightarrow GL(n, F_q) \tag{49}$$
$$x \longmapsto m_x \tag{50}$$

existiert mit $H = \iota(F_{q^n}^*)$, wobei m_x die Multiplikation mit x beschreibt. Beachte, dass jede zyklische Untergruppe von $GL(n, F_q)$ der Ordnung $q^n - 1$ konjugiert ist zu einer Gruppe vom Typ $Car(n)$ (siehe Bemerkung 8).
ii) Die Überlagerung ϕ ist galoissch mit Galoisgruppe

$$G(N) := \{ g \in GL(3, R(N)) \;|\; \det(g) \in F_q^* \}/Z. \tag{51}$$

Setze

$$P(N) := \left\{ g = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ 0 & p_{22} & p_{23} \\ 0 & p_{32} & p_{33} \end{pmatrix} \;\middle|\; p_{ij} \in R(N), \det(g) \in F_q^* \right\}/Z. \tag{52}$$

Dann ist die Kurve $X_0(N)$ gegeben als der Quotient

$$X_0(N) = X(N)/P(N) \tag{53}$$

und die Überlagerung ψ ist galoissch mit Galoisgruppe $P(N)$.
iii) Es sei $\xi \in X(N)$. Wir wollen ξ einen elliptischen Punkt nennen, falls

$$\mathfrak{j}(\phi(\xi)) = 0. \tag{54}$$

$X(N)_{ell}$ bezeichne die Menge der elliptischen Punkte auf $X(N)$. Ein $\xi \in X(N)$ heißt eine Spitze, falls

$$\mathfrak{j}(\phi(\xi)) = \infty. \tag{55}$$

Die Menge der Spitzen auf $X(N)$ heiße $X(N)_{sp}$. Mit diesen Bezeichnungen gilt nun:
a) Wähle eine feste Gruppe H vom Typ $Car(2)$ und schreibe $Car(2) = H$. Dann existiert eine wohlbestimmte Spitze auf $X(N)$, die wir ∞ nennen wollen, mit der Eigenschaft, dass die Fixgruppe von ∞ unter ϕ gegeben ist durch:

$$G_\infty(N) := \left\{ \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix} \;\middle|\; a \in F_q^*, b, c \in R, \gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix} \in Car(2) \right\} / Z. \tag{56}$$

Die wohlbestimmte (maximale) p-Sylow-Untergruppe von $G_\infty(N)$ ist gegeben durch die Gruppe

$$U(N) := \left\{ \begin{pmatrix} a & u & v \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \;\middle|\; a \in F_q^*, u \in R, v \in R \right\} / Z. \tag{57}$$

Die Verzweigung in den Spitzen ist moderat. Das heißt, die Verzweigungsfiltrierung für die Spitze ∞ hat die folgende Form:

$$G_\infty(N) \supset U(N) \supset \{\mathbb{1}\}. \tag{58}$$

Die Gruppe $G(N)$ operiert überdies transitiv auf den Spitzen von $X(N)$. Ist $\xi \in G(N)$ und $\xi \cdot \infty$ eine weitere Spitze, so gilt für die Fixgruppe von $\xi \cdot \infty$:

$$G_{\xi \cdot \infty} = \xi \cdot G_\infty(N) \cdot \xi^{-1}. \tag{59}$$

Wir erhalten also die folgende Verzweigungsfiltrierung für die Spitze $\xi \cdot \infty$:

$$G_{\xi \cdot \infty} = \xi \cdot G_\infty(N) \cdot \xi^{-1} \supset \xi \cdot U(N) \cdot \xi^{-1} \supset \{\mathbb{1}\}. \tag{60}$$

Außerdem gilt:

$$|X(N)_{sp}| = \frac{|G(N)|}{|G_\infty(N)|} \tag{61}$$

über die natürliche Abbildung

$$G(N)/G_\infty(N) \longrightarrow X(N)_{sp} \tag{62}$$

$$\xi \longmapsto \xi \cdot \infty. \tag{63}$$

b) $\phi : X(N) \longrightarrow X(1)$ *ist verzweigt über elliptischen Punkten. Wähle eine feste Gruppe* H' *vom Typ* $Car(3)$*. Es existiert ein wohlbestimmter elliptischer Punkt* $\mathfrak{e}$ *mit Fixgruppe* $C := H'/Z$*. Die Gruppe* $G(N)$ *operiert transitiv auf den elliptischen Punkten von* $X(N)$ *und es gilt*

$$|X(N)_{ell}| = \frac{|G(N)|}{q^2+q+1} \tag{64}$$

über die Abbildung $G(N)/C \longrightarrow X(N)_{ell}$, $\xi \longmapsto \xi \cdot \mathfrak{e}$*. Die Fixgruppe* $G_{\xi\cdot\mathfrak{e}}$ *eines elliptischen Punktes* $\xi \cdot \mathfrak{e}$ *ist gegeben durch das Konjugat* ${}^{\xi}C$*. Da* $|C|$ *nicht durch* p *teilbar ist, ist die elliptische Verzweigung zahm.*

Beweis. Setze $X(N) := X^{3,2}(N)$ und $X_0(N) := X_0^{3,2}(N)$ mit den Kurven $X^{r,k}(N)$, $X_0^{r,k}(N)$ aus [Gek14]. Die Behauptung ist dann lediglich eine Auflistung von Spezialfällen der in der genannten Arbeit [Gek14] gefundenen Ergebnisse (vergleiche etwa das dortige Theorem A für $r = 3$, $k = 2$). □

Um später bequem argumentieren zu können, wollen wir an dieser Stelle die Ordnungen von $G(N)$ und $P(N)$ explizit in Abhängigkeit der Faktorisierungsdaten von $N \in A$ ausdrücken. Dies leistet die folgende Bemerkung:

Bemerkung 9. *Es sei* $p \in A$ *prim und* $\deg(p) = d$*. Schreibe* $R := R(p^r)$ *und* $\mathfrak{p}$ *für das maximale Ideal von* R *(beachte* $|\mathfrak{p}| = q^{d\cdot(r-1)}$*, siehe Bemerkung 4, Seite 11-12). Für die Mächtigkeit von* $G := G(p^r)$ *gilt dann genauer:*

$$|G| = |SL(3,R)| = \frac{|GL(3,R)|}{|R^*|} = \frac{|\mathfrak{p}|^9 \cdot \prod_{i=0}^{2}(q^{3\cdot d} - q^{i\cdot d})}{(q^d-1)\cdot|\mathfrak{p}|}. \tag{65}$$

Vereinfachen wir den letzten Ausdruck noch, so erhalten wir:

$$|G| = \frac{\prod_{i=0}^{2}(q^{3\cdot d} - q^{i\cdot d})}{(q^d-1)} \cdot |\mathfrak{p}|^8 = \frac{\prod_{i=0}^{2}(q^{3\cdot d} - q^{i\cdot d})}{(q^d-1)} \cdot q^{8\cdot d\cdot(r-1)}. \tag{66}$$

Sei nun $N = \prod_{j=1}^{s} p_j^{r_j}$ *eine Faktorisierung von* N*. Hierbei gelte* $\deg(p_j) = d_j$*. Wegen*

$$|GL(3,R(N))| = \prod_{j=1}^{s} |GL(3,R(p_j^{r_j}))| \tag{67}$$

und da außerdem

$$|R(N)^*| = \prod_{j=1}^{s} |R(p_j^{r_j})^*|, \tag{68}$$

folgt für die Mächtigkeit von $G(N)$*:*

$$|G(N)| = \prod_{j=1}^{s} |\mathfrak{p}_j|^8 \cdot \frac{\prod_{i=0}^{2}(q^{3\cdot d_j} - q^{i\cdot d_j})}{(q^{d_j}-1)} = \prod_{j=1}^{s} q^{8\cdot d_j\cdot(r_j-1)} \cdot \frac{\prod_{i=0}^{2}(q^{3\cdot d_j} - q^{i\cdot d_j})}{(q^{d_j}-1)}. \tag{69}$$

Analog erhalten wir für die Mächtigkeit von $P(N)$:

$$|P(N)| = \left(\prod_{j=1}^{s} q^{4 \cdot d_j \cdot (r_j - 1)} \cdot \prod_{i=0}^{1} (q^{2 \cdot d_j} - q^{i \cdot d_j}) \right) \cdot q^{2 \cdot \deg(N)}. \tag{70}$$

Insbesondere folgt mit Proposition 1 (siehe Seite 11):

$$|\mathbb{P}^2(R(N))| = \frac{|G(N)|}{|P(N)|}. \tag{71}$$

Wir beenden diesen Abschnitt mit einer Proposition, die die in der obigen Bemerkung aufgetauchte Beziehung der Gruppen

$$P(N) \subset G(N) \subset GL(3, R(N))/Z \tag{72}$$

zum projektiven Raum $\mathbb{P}^2(R(N))$ präzisiert.

Proposition 2. *Die Abbildung*

$$f : G(N)/P(N) \longrightarrow \mathbb{P}^2(R(N)) \tag{73}$$

$$\overline{\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \cdot Z} \longmapsto < \begin{pmatrix} a \\ b \\ c \end{pmatrix} > \tag{74}$$

ist bijektiv.

Beweis. Setze $R := R(N)$. Wir bezeichnen mit $\tilde{G}(N) \subset GL(3, R)$ die Gruppe aller Matrizen in $GL(3, R)$ mit Determinante in F_q^*. Die Gruppe $\tilde{P}(N) \subset GL(3, R)$ sei analog als das Urbild von $P(N)$ unter der natürlichen Restklassenabbildung $GL(3, R) \longrightarrow GL(3, R)/Z$ definiert. Dann ist die Abbildung

$$g : \tilde{G}(N)/\tilde{P}(N) \longrightarrow G(N)/P(N) = (\tilde{G}(N)/Z)/(\tilde{P}(N)/Z) \tag{75}$$

$$[x] \longmapsto \overline{x \cdot Z} \tag{76}$$

(wobei $x \in \tilde{G}(N)$) offensichtlich wohldefiniert, surjektiv und aus Kardinalitätsgründen damit eine Bijektion. Hierbei sei $\overline{x \cdot Z}$ beziehungsweise $[x]$ jeweils die Klasse von $x \cdot Z$ beziehungsweise x bezüglich der entsprechenden Relation. Wir setzen weiter $G'(N) := GL(3, R)$ und $P'(N)$ bezeichne die Menge aller Matrizen $m \in G'(N)$, die von der Form $m = \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$ sind. Betrachte nun die Abbildung

$$h : \tilde{G}(N)/\tilde{P}(N) \longrightarrow G'(N)/P'(N) \tag{77}$$

$$[x] \longmapsto \hat{x}, \tag{78}$$

wobei $\hat{x}$ die Linksnebenklasse von x modulo $P'(N)$ bezeichne für $x \in G'(N)$. Angenommen $x_1 = x_2 \cdot m$ für $x_i \in \tilde{G}(N)$ und $m \in \tilde{P}(N) \subset P'(N)$. Dann gilt

nach Definition $\hat{x_1} = \hat{x_2}$ und h ist wohldefiniert. Ist andererseits $\hat{x_1} = \hat{x_2}$ für $x_i \in \tilde{G}(N)$, so folgt $x_1 = x_2 \cdot m$ beziehungsweise $x_2^{-1} \cdot x_1 = m$ für eine Matrix $m \in P'$. Nach Wahl der x_i folgt $\det(m) = \det(x_2^{-1}) \cdot \det(x_1) \in F_q^*$ und h ist injektiv. Eine einfache kombinatorische Überlegung zeigt, dass

$$|\tilde{G}(N)/\tilde{P}(N)| = |G'(N)/P'(N)| \tag{79}$$

und folglich ist h sogar eine Bijektion. Betrachte letztlich die Abbildung

$$i : G'(N)/P'(N) \longrightarrow \mathbb{P}^2(R(N)) \tag{80}$$

$$\begin{pmatrix} a & * & * \\ b & * & * \\ c & * & * \end{pmatrix} \longmapsto < \begin{pmatrix} a \\ b \\ c \end{pmatrix} > . \tag{81}$$

Angenommen für $x_1, x_2 \in G'(N)$ und $m \in P'(N)$ gilt

$$x_1 = x_2 \cdot m. \tag{82}$$

Wir multiplizieren (82) von rechts mit dem ersten Standardbasisvektor e_1 von $R(N)^3$ und erhalten nach Definition von P':

$$x_1 \cdot e_1 = m_{11} \cdot x_2 \cdot e_1 \tag{83}$$

mit $m_{11} \in R(N)^*$. Folglich erzeugen die ersten Spalten von x_1 beziehungsweise x_2 den gleichen freien Untermodul und i ist wohldefiniert. Falls $i(x_1) = i(x_2)$ für $x_1, x_2 \in G'(N)$, dann erzeugen die ersten Spalten von x_1 beziehungsweise x_2 den gleichen Untermodul und es existiert also ein $u \in R(N)^*$ mit

$$x_1 \cdot e_1 = u \cdot x_2 \cdot e_1. \tag{84}$$

Multiplizieren wir (84) von links mit x_2^{-1}, so erhalten wir

$$x_2^{-1} \cdot x_1 \cdot e_1 = u \cdot e_1. \tag{85}$$

Wegen $\det(x_2^{-1} \cdot x_1) \in R(N)^*$ ist die Gültigkeit von Gleichung (85) dann aber gleichbedeutend mit $x_2^{-1} \cdot x_1 \in P'(N)$. Es folgt die Injektivität von i. Ein Vergleich der Kardinalitäten von $\mathbb{P}^2(R(N))$ und $G'(N)/P'(N)$ zeigt, dass i eine Bijektion sein muss. Wir erhalten also das folgende Diagramm bijektiver Abbildungen:

$$\begin{array}{ccc} G(N)/P(N) & \longrightarrow & \mathbb{P}^2(R(N)) \\ \uparrow & & \uparrow \\ \tilde{G}(N)/\tilde{P}(N) & \longrightarrow & G'(N)/P'(N). \end{array} \tag{86}$$

Die linke vertikale Abbildung ist hierbei die Abbildung g aus (75) und die rechte vertikale Abbildung ist die obige Abbildung i aus (80). Die untere horizontale Abbildung ist die obige Abbildung h aus (77). Damit ist die obere induzierte Abbildung $G(N)/P(N) \longrightarrow \mathbb{P}^2(R(N))$ nach Konstruktion aber gerade f:

$$f = i \circ h \circ g^{-1} : G(N)/P(N) \longrightarrow \mathbb{P}^2(R(N)). \tag{87}$$

Folglich ist auch f als Komposition bijektiver Abbildungen eine Bijektion und der Beweis ist beendet. □

3 Das Geschlecht von $X(N)$

Wie in der Einleitung bereits angesprochen, wollen wir das Geschlecht von $X_0(N)$ durch Anwendung der Riemann-Hurwitz-Formel auf die Überlagerung

$$\psi : X(N) \longrightarrow X_0(N) \tag{88}$$

bestimmen. Nach Theorem 2 ist ψ galoissch mit Gruppe $P(N)$. Zur Auswertung der Riemann-Hurwitz-Formel benötigen wir jedoch zuerst die genaue Kenntnis von $g(X(N))$. Wir wollen daher in diesem Abschnitt eine geschlossene Formel für das Geschlecht von $X(N)$ angeben. Hierzu fixieren wir nun ein nichtkonstantes, normiertes $N \in A$ mit Primfaktorisierung

$$N = \prod_{j=1}^{s} {p_j}^{r_j}. \tag{89}$$

Es sei $d_j := \deg(p_j)$ und $\mathfrak{p}_j$ bezeichne das maximale Ideal von $R({p_j}^{r_j})$. Zur Bestimmung von $g(X(N))$ betrachten wir die Überlagerung

$$\phi : X(N) \longrightarrow X(1). \tag{90}$$

Theorem 2 lehrt, dass auch ϕ galoissch ist mit Gruppe $G(N)$. Da wir $X(1)$ über die j-Invariante mit $\mathbb{P}^1(C_\infty)$ identifizieren können, gilt

$$g(X(1)) = 0. \tag{91}$$

Setze $e := \chi(X(N))$ und $e' := \chi(X(1)) = 2$, dann gilt nach Theorem 1:

$$e = |G(N)| \cdot 2 - \sum_{x \in X} a_x. \tag{92}$$

Für die Mächtigkeit von $G(N)$ gilt nach Bemerkung 9:

$$|G(N)| = \prod_{j=1}^{s} q^{8 \cdot d_j \cdot (r_j - 1)} \cdot \frac{\prod_{i=0}^{2}(q^{3 \cdot d_j} - q^{i \cdot d_j})}{(q^{d_j} - 1)}. \tag{93}$$

Das heißt, wir müssen nur die Verzweigungszahlen a_x bestimmen. Nach Theorem 2 sind die einzigen verzweigten Punkte unter ϕ die elliptischen Punkte und die Spitzen. Die Fixgruppe einer Spitze ist durch ein Konjugat der Gruppe $G_\infty(N)$ aus Theorem 2, Teil iii), a) beschrieben, während die Fixgruppe eines elliptischen Punktes das Konjugat der Gruppe C aus Theorem 2, Teil iii), b) ist. Theorem 2 liefert weiterhin, dass im elliptischen Fall die Verzweigung zahm ist, während die Verzweigung in den Spitzen moderat bleibt. Damit können wir die Verzweigungszahlen berechnen:

Lemma 4. *Es seien ∞, $\mathfrak{e}$ wie in Theorem 2, Teil ii) beziehungsweise Teil iii) sowie $\xi \in G(N)/G_\infty(N)$ beziehungsweise $\eta \in G(N)/C$. Dann gilt für die Verzweigungszahl in der Spitze $\xi \cdot \infty$:*

$$a_{\xi \cdot \infty} = q^{2 \cdot \deg(N) + 2} - 2. \tag{94}$$

Für den elliptischen Punkt $\eta \cdot \mathfrak{e}$ erhalten wir:

$$a_{\eta\cdot\mathfrak{e}} = q^2 + q. \tag{95}$$

Beweis. Wir bemerken, dass nach Theorem 2 die elliptische Verzweigung zahm und die Spitzenverzweigung moderat ist. Folglich erhalten wir für die Verzweigungszahl eines elliptischen Punktes $\eta \cdot \mathfrak{e}$:

$$a_{\eta\cdot\mathfrak{e}} = |G_{\eta\cdot\mathfrak{e}}| - 1 = |C| - 1 = q^2 + q. \tag{96}$$

Es sei nun $\xi \cdot \infty$ eine Spitze von $X(N)$. Wir erhalten für die Verzweigungszahl:

$$a_{\xi\cdot\infty} = |G_{\xi\cdot\infty}| + |G_{\xi\cdot\infty,1}| - 2 = |G_\infty(N)| + |U(N)| - 2 = q^{2\cdot\deg(N)+2} - 2. \tag{97}$$

Für das vorletzte Gleichheitszeichen beachte man, dass Konjugation die Ordnung nicht ändert. Außerdem gilt:

$$|G_\infty(N)| = (q^2-1)\cdot|R(N)|^2 = (q^2-1)\cdot q^{2\cdot\deg(N)}, \tag{98}$$

$$|U(N)| = |R(N)|^2 = q^{2\cdot\deg(N)}. \tag{99}$$

□

Mit diesem Hilfsmittel benötigen wir zur Auswertung der Riemann-Hurwitz-Formel nur noch die Anzahl der elliptischen Punkte und die Anzahl der Spitzen auf der Kurve $X(N)$. Nach Theorem 2 gilt

$$|X(N)_{ell}| = \frac{|G(N)|}{|C|} = \frac{|G(N)|}{q^2+q+1}, \tag{100}$$

$$|X(N)_{sp}| = \frac{|G(N)|}{|G_\infty(N)|}. \tag{101}$$

Das liefert uns folgendes Lemma:

Lemma 5. *Für nichtkonstantes $N \in A$ gilt:*

- $|X(N)_{sp}| = \frac{|G(N)|}{|G_\infty(N)|} = \frac{1}{(q^2-1)}\prod_{j=1}^{s}\frac{q^{8\cdot d_j\cdot(r_j-1)}\cdot\prod_{i=0}^{2}(q^{3\cdot d_j}-q^{i\cdot d_j})}{q^{2\cdot d_j\cdot r_j}\cdot(q^{d_j}-1)}$
- $|X(N)_{ell}| = \frac{|G(N)|}{q^2+q+1} = \frac{1}{(q^2+q+1)}\prod_{j=1}^{s}\frac{q^{8\cdot d_j\cdot(r_j-1)}\cdot\prod_{i=0}^{2}(q^{3\cdot d_j}-q^{i\cdot d_j})}{(q^{d_j}-1)}$

Wir können nun den folgenden Satz formulieren, der uns eine explizite Formel für die Eulercharakteristik von $X(N)$ liefert. Damit haben wir natürlich wegen

$$\chi(X(N)) = 2 - 2\cdot g(X(N)) \tag{102}$$

auch eine Formel für das Geschlecht von $X(N)$.

Satz 1. *Die Eulerzahl der Kurve $X(N)$ ist gegeben durch:*

$$\chi(X(N)) = 2\cdot|G(N)| - \frac{|G(N)|}{|G_\infty(N)|}\cdot\big(q^{2\cdot\deg(N)+2}-2\big) - \frac{|G(N)|}{q^2+q+1}\cdot\big(q^2+q\big). \tag{103}$$

Beweis. Nach der Riemann-Hurwitz-Formel gilt:

$$\chi(X(N)) = 2 \cdot |G(N)| - \sum_{x \in X(N)} a_x \tag{104}$$

$$= 2 \cdot |G(N)| - \sum_{x \in X(N)_{sp}} a_x \; - \sum_{x \in X(N)_{ell}} a_x. \tag{105}$$

Nehmen wir zur letzten Gleichung noch die Informationen aus Lemma 4 und Lemma 5 hinzu, so folgt die Behauptung. □

Bemerkung 10. *i) Wir bemerken, dass wir alle Größen, die in der Formel von $\chi(X(N))$ vorkommen, explizit aus den Faktorisierungsdaten von N bestimmen können; eine genauere Betrachtung zeigt, dass es dabei sogar nur auf die Grade der beteiligten Primteiler von N und deren Multiplizitäten in N ankommt:*
Es seien

$$N = \prod_{j=1}^{s} {p_j}^{r_j} \tag{106}$$

sowie

$$M = \prod_{j=1}^{s} {\tilde{p_j}}^{\tilde{r_j}} \tag{107}$$

Primfaktorisierungen zweier normierter Polynome N, M. Existiert nun eine Permutation π der Menge $\{1, \ldots, s\}$, sodass

$$\deg(p_{\pi(j)}) = \deg(\tilde{p_j}) \tag{108}$$

und

$$r_{\pi(j)} = \tilde{r_j}, \tag{109}$$

so haben $X(N)$ und $X(M)$ das gleiche Geschlecht.
ii) Es sei $N \in F_q[T]$ normiert und nichtkonstant mit Primfaktorisierung $N = \prod_{j=1}^{s} {p_j}^{r_j}$. Wir setzen $d := (\deg(p_1), \ldots, \deg(p_s))$ und $r := (r_1, \ldots, r_s)$ und definieren die Signatur von N als das Tripel $[q, d, r]$:

$$Sig(N) := [q, d, r]. \tag{110}$$

Das Geschlecht von $X(N)$ hängt dann nur von der Signatur des Polynoms N ab. Es wird sich herausstellen, dass die gleiche Aussage auch für das Geschlecht der Kurve $X_0(N)$ richtig ist.

Die letzte Bemerkung soll diesen Abschnitt beenden. Als nächstes greifen wir im kommenden Abschnitt die tatsächliche Berechnung von $g(X_0(N))$ an.

4 Das Geschlecht von $X_0(N)$

Wir wollen in diesem Abschnitt für ein beliebiges nichtkonstantes, normiertes $N \in A$ explizit das Geschlecht der Kurve $X_0(N)$ bestimmen. Dazu erläutern wir in 4.1 zunächst die grundsätzliche Strategie zur Berechnung. In 4.2 werden wir dann die Verzweigung in den Spitzen der Überlagerung $\psi : X(N) \longrightarrow X_0(N)$ im Fall eines primären N betrachten. Die so gewonnenen (lokalen) Daten werden dann im Unterabschnitt 4.3 benutzt, um aus ihnen eine Formel für die Spitzenverzweigung unter ψ für ein beliebiges nichtkonstantes N abzuleiten. In 4.4 wird die Verzweigung in den elliptischen Punkten abgehandelt. Im letzten Teilabschnitt 4.5 werden wir dann eine explizite Formel für $g(X_0(N))$ geben. Der chinesische Restsatz in Form von Lemma 2 spielt hierbei eine zentrale Rolle. Wir beginnen mit der Beschreibung der Strategie.

4.1 Die Grundstrategie

Wir fixieren wieder ein nichtkonstantes, normiertes $N \in A$ mit Primfaktorisierung

$$N = \prod_{j=1}^{s} {p_j}^{r_j}. \tag{111}$$

Für die Grade der Faktoren gelte

$$d_j := \deg(p_j), \tag{112}$$

und das maximale Ideal des lokalen Ringes $R({p_j}^{r_j})$ heiße $\mathfrak{p}_j$.

Im Gegensatz zur Situation im letzten Abschnitt ist die Überlagerung

$$X_0(N) \longrightarrow X(1) \tag{113}$$

nicht(!) galoissch. Wir können die Riemann-Hurwitz-Formel also nicht direkt auf diese Überlagerung anwenden. Da wir jedoch über Kenntnis des Geschlechts von $X(N)$ verfügen, können wir die Überlagerung

$$\psi : X(N) \longrightarrow X_0(N) \tag{114}$$

betrachten, von der wir nach Theorem 2 wissen, dass sie galoissch mit Gruppe $P(N)$ ist. Das weitere Vorgehen ist nun analog zum vorigen Abschnitt. Der wesentliche Unterschied liegt darin, dass sich die Berechnung der Verzweigungszahlen a_x für $x \in X(N)$ etwas schwieriger gestalten wird. Diese werden hier in der Tat vom jeweiligen x, das in Betrachung steht, abhängen.

Bevor wir mit den eigentlichen Untersuchungen beginnen, erinnern wir an die folgende Variante des Lemmas von Nakayama:

Proposition 3. *Es sei $(R, \mathfrak{p})$ ein lokaler Ring und M ein endlich erzeugter R-Modul. Dann gilt: Die Menge $\{m_1, \ldots, m_n\}$ ist ein minimales Erzeugendensystem für M genau dann, wenn die Menge $\{\overline{m_1}, \ldots, \overline{m_n}\}$ ein minimales Erzeugendensystem für den Modul $M/(\mathfrak{p} \cdot M)$ bildet.*

Ein Beweis dieser Aussage findet sich beispielsweise in [Eis04].

Wir brauchen nun zunächst einige grundsätzliche Informationen über die Natur der Verzweigung unter ψ. Wir beginnen mit dem Fall einer Spitze. Nach Theorem 2 stehen die Spitzen von $X(N)$ in natürlicher Bijektion mit der Restklassenmenge $G(N)/G_\infty(N)$:

$$G(N)/G_\infty(N) \longrightarrow X(N)_{sp} \tag{115}$$

$$\xi \longmapsto \xi \cdot \infty. \tag{116}$$

Weiter wissen wir nach Theorem 2, dass die Fixgruppe $G_{\xi\cdot\infty} \subset G(N)$ einer Spitze $\xi \cdot \infty$ gegeben ist durch

$$G_{\xi\cdot\infty} = \xi \cdot G_\infty(N) \cdot \xi^{-1} =: {}^{\xi}G_\infty(N). \tag{117}$$

Das folgende Lemma liefert nun die Verzweigungszahl $a_{\xi\cdot\infty}$ für eine Spitze $\xi\cdot\infty \in X(N)$.

Lemma 6. *Für die Verzweigungszahl einer Spitze $\xi \cdot \infty$ unter der Überlagerung $\psi : X(N) \longrightarrow X_0(N)$ gilt:*

$$a_{\xi\cdot\infty} = |P(N) \cap {}^{\xi}G_\infty(N)| + |P(N) \cap {}^{\xi}U(N)| - 2. \tag{118}$$

Beweis. Die Behauptung folgt direkt aus der Tatsache, dass $P(N) \subset G(N)$ nach Theorem 2 die Galoisgruppe der Überlagerung ψ ist. □

Es wird sich nun alles darum drehen, die Werte

$$|P(N) \cap {}^{\xi}G_\infty(N)| \tag{119}$$

für alle ξ in einem noch geeignet festzulegenden Repräsentantensystem für $G(N)/G_\infty(N)$ zu bestimmen; die entsprechenden Werte für $U(N)$ erhält man einfach, indem man den p-Teil des Wertes für $G_\infty(N)$ extrahiert. Wir wollen hierzu zunächst den Fall eines primären N betrachten.

4.2 Die Verzweigung in den Spitzen im lokalen Fall

Im gesamten Unterabschnitt sei N normiert und primär mit Primfaktorisierung

$$N = p^r. \tag{120}$$

Schreibe d für den Grad des Primelements $p \in A$ und fixiere mit $G_\infty := G_\infty(N)$ ein beliebiges Repräsentantensystem $Y \subset P := P(N)$ für P/G_∞. Wir definieren $U := U(N)$ und für das maximale Ideal von $R := R(N)$ schreiben wir $\mathfrak{p}$. Die Mengen $RS_i(R)$ für $1 \leq i \leq 3$ bilden nach Lemma 3 und Proposition 2 (siehe Abschnitt 2, Seite 10-11 und Seite 19-20) ein Repräsentantensystem für G/P. Indem wir beide Repräsentantensysteme kombinieren, erhalten wir ein vollständiges Repräsentantensystem für G/G_∞:

Lemma 7. *Die Elemente der Form*

$$\xi = x \cdot y \tag{121}$$

mit $x \in RS_1(R) \cup RS_2(R) \cup RS_3(R)$ *und* $y \in Y$ *bilden ein Repräsentantensystem für* G/G_∞.

Beweis. Sei $\xi_1 := x_1 \cdot y_1$ und $\xi_2 := x_2 \cdot y_2$ für $x_i \in RS_1(R) \cup RS_2(R) \cup RS_3(R)$ und $y_i \in Y$. Wir müssen zeigen, dass aus

$$\xi_1 \cdot G_\infty = \xi_2 \cdot G_\infty \tag{122}$$

bereits $x_1 = x_2$ und $y_1 = y_2$ folgt. Sei also $\xi_1 = \xi_2 \cdot g$ für ein $g \in G_\infty$. Wegen $G_\infty \subset P$ folgt hieraus:

$$x_1 \cdot P = x_2 \cdot P. \tag{123}$$

Nach Wahl der x_i folgt also $x_1 = x_2$. Damit verbleibt die Gleichung:

$$y_1 \cdot G_\infty = y_2 \cdot G_\infty. \tag{124}$$

Da die y_i ein Repräsentantensystem für P/G_∞ bilden, folgt auch $y_1 = y_2$. Vergleichen wir nun die Kardinalität von

$$\{\xi = x \cdot y \mid x \in RS_1(R) \cup RS_2(R) \cup RS_3(R), y \in Y\} \tag{125}$$

mit der von G/G_∞, so folgt wegen

$$|G/G_\infty| = \frac{|G|}{|P|} \cdot \frac{|P|}{|G_\infty|} \tag{126}$$

die Behauptung. □

Lemma 7 zeigt, dass wir uns bei der Berechnung von

$$|P(N) \cap {}^\eta G_\infty(N)| \tag{127}$$

auf den Fall $\eta = x \cdot y$ beschränken können, für x, y wie im zitierten Lemma. Wir betrachten nun zunächst den Fall $x \in RS_1(R)$:

$$x = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ c_2 & 1 & 0 \\ c_3 & 0 & 1 \end{pmatrix} \;\middle|\; c_2, c_3 \in R \right\}. \tag{128}$$

Angenommen, wir haben Elemente $g \cdot Z \in G_\infty$, $\eta \cdot Z \in P$, $x \in RS_1(R)$ und $y \in Y$ mit

$$x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} = \eta. \tag{129}$$

Wegen $\det(x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1}) = \det(g) \in F_q^*$ und $\eta \in P$ gilt dies genau dann, wenn:

$$x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} \cdot e_1 = \eta \cdot e_1 = \begin{pmatrix} \eta_{11} \\ 0 \\ 0 \end{pmatrix}, \tag{130}$$

wobei e_1 den ersten Standardbasisvektor bezeichnet. Multiplizieren wir die letzte Gleichung von links mit x^{-1}, so erhalten wir

$$y \cdot g \cdot y^{-1} \cdot x^{-1} \cdot e_1 = \eta_{11} \cdot x^{-1} \cdot e_1, \tag{131}$$

wobei wir $\eta_{11} \in R^*$ bemerken. Das heißt, Gleichung (129) gilt genau dann, wenn die erste Spalte von x^{-1} ein Eigenvektor der Matrix $y \cdot g \cdot y^{-1}$ zum Eigenwert η_{11} ist. Gilt

$$g = \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix} \tag{132}$$

für $a \in F_q^*$, $b, c \in R$ und $\gamma = \begin{pmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{pmatrix} \in Car(2)$, so ist das charakteristische Polynom von g gegeben durch:

$$\chi_g(X) = (X - a) \cdot \chi_\gamma(X). \tag{133}$$

Da Konjugation das charakteristische Polynom nicht ändert, haben $y \cdot g \cdot y^{-1}$ und g das gleiche charakteristische Polynom und damit auch die gleichen Eigenwerte.

Gehört die Matrix γ nun zu einem Element $\tilde{\gamma} \in F_{q^2} \setminus F_q^*$, so hat γ modulo $\mathfrak{p}$ zwei verschiedene Eigenwerte, die beide in $F_{q^2} \setminus F_q^*$ liegen. Dies impliziert notwendigerweise:

$$d \equiv 0 \mod 2. \tag{134}$$

Damit hat $\tilde{y} \cdot \gamma \cdot \tilde{y}^{-1}$ in diesem Fall modulo $\mathfrak{p}$ auch zwei verschiedene Eigenvektoren, für eine beliebige invertierbare Matrix $\tilde{y}$. Wenden wir das Lemma von Nakayama auf die (endlichen) Eigenräume von $\tilde{y} \cdot \gamma \cdot \tilde{y}^{-1}$ an, so sehen wir, dass $\tilde{y} \cdot \gamma \cdot \tilde{y}^{-1}$ auch über R zwei verschiedene Eigenrichtungen hat. Für jede dieser Eigenrichtungen können wir $|R^*|$-viele entsprechende Elemente x in $RS_1(R)$ wählen: wir nehmen als die beiden unteren Einträge von x in der ersten Spalte einfach die $|R^*|$-Vielfache der Eigenrichtung. Nach Wahl von x haben wir noch einen Freiheitsgrad in der Wahl der Parameter b, c aus der obersten Zeile von g, sodass

$$x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} \cdot Z \in P \tag{135}$$

gilt. Dies kann direkt nachgerechnet werden und ist in [Boh14] zu finden. Wir bemerken außerdem, dass $y \cdot g \cdot y^{-1}$ stets die triviale Eigenrichtung e_1 zum Eigenwert a hat, für e_1 den ersten Standardbasisvektor. Diese triviale Eigenrichtung gehört zum Element

$$x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in RS_1(R). \tag{136}$$

Bei Wahl der trivialen Eigenrichtung für x gibt es keine Einschränkungen an die Parameter b, c.

Wir bemerken, dass die obigen Überlegungen offenbar unabhängig von der konkreten Gestalt des gewählten y sind.

Bevor wir all dies bequem in einer ersten Proposition zusammenfassen können, definieren wir noch ein Symbol, das uns eine einfache Notation ermöglicht:

Definition 5. Es sei $A \ni N = \prod_{j=1}^{s} {f_i}^{r_i}$ nichtkonstant mit Primteilern f_i. Wir definieren das Symbol ω_∞ mit

$$\omega_\infty(N) := \begin{cases} 1, \ \forall i : \deg(f_i) \equiv 0 \bmod 2 \\ 0, \ \exists i : \deg(f_i) \equiv 1 \bmod 2 \end{cases} . \tag{137}$$

Der Index ∞ soll andeuten, dass das Symbol ω_∞ etwas mit der Spitzenverzweigung zu tun hat. Damit erhalten wir:

Proposition 4. *Es sei $\gamma \in Car(2)$. Schreibe $\tilde{\gamma}$ für das zu γ gehörige Element von F_{q^2}. Setze*

$$G_\infty^{(2)} := \left\{ \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix} \cdot Z \mid a \in F_q^*, \tilde{\gamma} \notin F_q^*, b, c \in R \right\} \subset G_\infty. \tag{138}$$

Dann gilt:

$$\sum_{y \in Y} \sum_{x \in RS_1(R)} |P \cap {}^{x \cdot y} G_\infty^{(2)}| = \frac{|P|}{|G_\infty|} \cdot |R| \cdot (q^2 - q) \cdot \big(|R| + \omega_\infty(N) \cdot 2 \cdot |R^*|\big). \tag{139}$$

Damit müssen wir also nur noch untersuchen, was mit den übrigen Elementen von G_∞ passiert. Dazu setzen wir analog:

$$G_\infty^{(1)} := \left\{ \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix} \cdot Z \mid a, \tilde{\gamma} \in F_q^*, b, c \in R \right\} \tag{140}$$

$$= \left\{ \begin{pmatrix} a & b & c \\ 0 & f & 0 \\ 0 & 0 & f \end{pmatrix} \cdot Z \mid a, f \in F_q^*, b, c \in R \right\} \subset G_\infty. \tag{141}$$

Um den Fall $RS_1(R)$ vollständig abzuklären, ist also nur noch der Wert der folgenden Summe zu bestimmen:

$$\sum_{y \in Y} \sum_{x \in RS_1(R)} |P \cap {}^{x \cdot y} G_\infty^{(1)}| = ? \tag{142}$$

Da alle Elemente aus $G_\infty^{(1)}$ jeweils eine diagonale Cartan-Matrix enthalten, und da Konjugation mit y eine diagonale Matrix diagonal lässt, erhalten wir für eine Matrix g mit $g \cdot Z \in G_\infty^{(1)}$ und eine Matrix $y \in Y$:

$$y \cdot g \cdot y^{-1} = y \cdot \begin{pmatrix} a & b & c \\ 0 & f & 0 \\ 0 & 0 & f \end{pmatrix} \cdot y^{-1} = \begin{pmatrix} a & \tilde{b} & \tilde{c} \\ 0 & f & 0 \\ 0 & 0 & f \end{pmatrix}. \tag{143}$$

Die Einträge $\tilde{b}$, $\tilde{c}$ sind hierbei affinlineare Funktionen in den Parametern a, b, c aus g. Fixiere nun ein $x \in RS_1(R)$ und ein $y \in Y$; mit $\overline{x}$ beziehungsweise $\overline{y}$ bezeichnen wir die Linksnebenklassen modulo Z von x beziehungsweise y. Wir berechnen dann die Kardinalität der Menge

$$S_{x,y} := \{g \in G_\infty^{(1)} \mid \overline{x} \cdot \overline{y} \cdot g \cdot \overline{y^{-1}} \cdot \overline{x^{-1}} \in P\}. \tag{144}$$

Falls $x = \mathbb{1}$ die Einheitsmatrix ist, so gilt offensichtlich:

$$|S_{\mathbb{1},y}| = (q-1) \cdot |R|^2, \tag{145}$$

denn die erste Spalte der Einheitsmatrix ist der erste Standardbasisvektor e_1, und dieser ist Eigenvektor von allen $g \in G_\infty^{(1)}$.

Wir erinnern daran, dass wir auf dem lokalen Ring R mit maximalem Ideal $\mathfrak{p}$ eine sogenannte verstümmelte Bewertung zur Verfügung haben (siehe Bemerkung 2, Teil i) auf Seite 8):

$$f \longmapsto \sup\{i \mid f \in \mathfrak{p}^i\}. \tag{146}$$

Beachte, dass das Nullelement von R die Bewertung r hat.

Damit können wir für ein x aus $RS_1(R)$ eine Hilfsgröße $h_R(x)$ einführen:

Definition 6. Es sei

$$x = \begin{pmatrix} 1 & 0 & 0 \\ c_2 & 1 & 0 \\ c_3 & 0 & 1 \end{pmatrix} \tag{147}$$

ein Element von $RS_1(R)$ und $v_\mathfrak{p}$ die zu R gehörige verstümmelte Bewertung. Wir setzen

$$h_R(x) := \min\{v_\mathfrak{p}(c_2), v_\mathfrak{p}(c_3)\}. \tag{148}$$

und nennen $h_R(x)$ die *Höhe* von x.

Mit dieser Hilfsgröße können wir die Menge $RS_1(R)$ etwas feiner unterteilen. Eine direkte Rechnung (zu finden in der Arbeit [Boh14]) zeigt, dass wir für die Kardinalitäten der oben definierten Mengen $S_{x,y}$ jeweils die folgenden Werte erhalten:

Lemma 8. *Es sei $y \in Y$ und $x \in RS_1(R)$. Wir setzen $k := h_R(x)$ und erhalten:*

$$|S_{x,y}| = \begin{cases} (q-1) \cdot q^{d \cdot r}, \ k = 0 \\ q^{d \cdot (r+2 \cdot k)}, \ 1 \leq k \leq \frac{r}{2} \\ q^{2 \cdot d \cdot r}, \ \frac{r}{2} < k < r \\ (q-1) \cdot q^{2 \cdot d \cdot r}, \ k = r \end{cases}. \tag{149}$$

Der Wert von $|S_{x,y}|$ hängt hierbei offenbar wieder nicht von der Wahl von y ab.

Indem wir geeignet über die gegebenen Kardinalitäten in Lemma 8 summieren, erhalten wir letztlich den Wert der Summe $\sum_{y\in Y}\sum_{x\in RS_1(R)}|P\cap {}^{x\cdot y}G_\infty^{(1)}|$ aus (142). Dazu müssen wir nur noch die jeweiligen Anzahlen n_k der Elemente aus $RS_1(R)$ bestimmen, die Höhe k haben. Dies geschieht im nächsten Lemma:

Lemma 9. *Sei $0\leq k<r$. Dann gilt:*

$$n_k := |\{x\in RS_1(R)\mid h_R(x)=k\}| = (q^{2\cdot d}-1)\cdot q^{2\cdot d\cdot(r-k-1)}. \tag{150}$$

Das einzige Element x aus $RS_1(R)$ mit $h_R(x)=r$ ist die Einheitsmatrix. Wir bemerken außerdem, dass $n_0=|\mathbb{P}^1(R)|\cdot|R^*|$.

Beweis. Es sei $x\in RS_1(R)$ und c_2, c_3 seien die beiden unteren Einträge der ersten Spalte von x. Die Bedingung $h_R(x)=k$ bedeutet, dass entweder $v_\mathfrak{p}(c_2)=k=v_\mathfrak{p}(c_3)$, oder dass $v_\mathfrak{p}(c_2)=k$ und $v_\mathfrak{p}(c_3)>k$, oder eben dass $v_\mathfrak{p}(c_2)>k$ und $v_\mathfrak{p}(c_3)=k$. Damit ergibt sich nach Abzählen und Aufsummieren der Möglichkeiten für jeden der obigen Fälle die Behauptung. □

Damit können wir (142) auswerten. Wir wählen $y_0\in Y$ beliebig, sowie Elemente $x_0,x_1,\ldots,x_r\in RS_1(R)$ mit $h_R(x_k)=k$ und erhalten damit:

$$\sum_{y\in Y}\sum_{x\in RS_1(R)}|P\cap {}^{x\cdot y}G_\infty^{(1)}| = |Y|\cdot\sum_{k=0}^{r}|P\cap {}^{x_k\cdot y_0}G_\infty^{(1)}| \tag{151}$$

$$= |Y|\cdot\Big(\sum_{k=0}^{r}n_k\cdot|S_{x_k,y_0}|\Big)+|Y|\cdot(q-1)\cdot q^{d\cdot r}\cdot\big(1+q^{d\cdot r}\big) \tag{152}$$

$$= |Y|\cdot\Big(\sum_{k=1}^{\lfloor\frac{r}{2}\rfloor}(q^{2\cdot d}-1)\cdot q^{2\cdot d\cdot(r-k-1)}\cdot q^{d\cdot(r+2\cdot k)}\Big) \tag{153}$$

$$+|Y|\cdot\Big(\sum_{k=\lfloor\frac{r}{2}\rfloor+1}^{r-1}(q^{2\cdot d}-1)\cdot q^{2\cdot d\cdot(r-k-1)}\cdot q^{2\cdot d\cdot r}\Big) \tag{154}$$

$$+|Y|\cdot(q^{2\cdot d}-1)\cdot q^{2\cdot d\cdot(r-1)}\cdot(q-1)\cdot q^{d\cdot r}. \tag{155}$$

Vereinfacht man in der letzten Gleichung die Summanden so weit wie möglich und wertet man die auftretenden geometrischen Reihen in q aus, so erhält man zusammen mit Gleichung (139) wegen

$$\sum_{y\in Y}\sum_{x\in RS_1(R)}|P\cap {}^{x\cdot y}G_\infty^{(1)}|+|P\cap {}^{x\cdot y}G_\infty^{(2)}| = \sum_{y\in Y}\sum_{x\in RS_1(R)}|P\cap {}^{x\cdot y}G_\infty| \tag{156}$$

eine geschlossene Formel für den letzten Ausdruck. Betrachten wir die Gruppe U, so erhält man mit Lemma 8 unter Extraktion des jeweiligen p-Teils auf die selbe Art eine geschlossene Formel für $\sum_{y\in Y}\sum_{x\in RS_1(R)}|P\cap {}^{x\cdot y}U|$. Dies wurde in [Boh14] explizit ausgeführt.

Damit erhält man letztlich insgesamt die folgende geschlossene Formel für den Beitrag der Elemente aus $RS_1(R)\cdot Y$ zur Spitzenverzweigung:

Proposition 5. *Es sei $N = p^r$ primär mit p prim und* $\deg(p) = d$. *Dann gilt:*

$$\sum_{y \in Y} \sum_{x \in RS_1(R)} |P \cap {}^{x \cdot y}G_\infty| + |P \cap {}^{x \cdot y}U| \tag{157}$$

$$= (q^{2 \cdot d} - 1) \cdot q^{3 \cdot d \cdot r - 2 \cdot d + 1} + q^{2 \cdot d \cdot r + 2} \tag{158}$$

$$+ 2 \cdot \left(q^{4 \cdot d \cdot r - 2 \cdot d \cdot \lfloor \frac{r}{2} \rfloor - 2 \cdot d} - q^{2 \cdot d \cdot r} + \lfloor \frac{r}{2} \rfloor \cdot (q^{2 \cdot d} - 1) \cdot q^{3 \cdot d \cdot r - 2 \cdot d}\right) \tag{159}$$

$$+ 2 \cdot \omega_\infty(N) \cdot (q^d - 1) \cdot q^{2 \cdot d \cdot r - d} \cdot (q^2 - q). \tag{160}$$

Mit dieser Proposition müssen wir die obige Summe jetzt nur noch für Repräsentanten x vom Typ $RS_2(R)$ und $RS_3(R)$ auswerten. Dazu sei im Folgenden stets $i \geq 2$.

Eine einfache Rechnung zeigt, dass die erste Spalte von x^{-1} in diesem Fall stets durch den zweiten Standardbasisvektor e_2 gegeben ist, unabhängig vom gewählten x:

$$i \geq 2,\ x \in RS_i(R) \Longrightarrow x^{-1} = \begin{pmatrix} 0 & * & * \\ 1 & * & * \\ 0 & * & * \end{pmatrix}. \tag{161}$$

Das bedeutet jedoch für alle $y \in Y$, $x \in RS_i(R)$, $\overline{g} \in G_\infty$, dass die Bedingung

$$\overline{x} \cdot \overline{y} \cdot \overline{g} \cdot \overline{y^{-1}} \cdot \overline{x^{-1}} \in P \tag{162}$$

genau dann erfüllt ist, wenn die zweite Spalte von y^{-1} ein Eigenvektor von g ist. Es bezeichne hierbei wieder $\bar{\cdot}$ die Linksnebenklasse modulo Z. Da die erste Spalte von y^{-1} ein R^*-Vielfaches des ersten Standardbasisvektors e_1 ist, folgt, dass die zweite Spalte von y^{-1} niemals der triviale Eigenvektor von g sein kann: der triviale Eigenvektor von g ist ja gerade der Vektor e_1 und y^{-1} ist invertierbar. Insbesondere ist die Gültigkeit von (162) unabhängig von der konkreten Gestalt von x.

Wir verwenden jetzt wieder die Unterteilung

$$G_\infty = G_\infty^{(1)} \dot\cup\, G_\infty^{(2)}, \tag{163}$$

wobei $G_\infty^{(1)}$ beziehungsweise $G_\infty^{(2)}$ so definiert ist wie in (140) beziehungsweise (138); siehe hierzu Seite 28.

Betrachten wir $g \cdot Z \in G_\infty^{(1)}$, so gilt:

$$y \cdot g \cdot y^{-1} = \begin{pmatrix} a & b' & c' \\ 0 & f & 0 \\ 0 & 0 & f \end{pmatrix} \tag{164}$$

für $a, f \in F_q^*$, $b', c' \in R$. Es bezeichne v die erste und w die zweite Spalte von y^{-1}. Wir multiplizieren (164) von links mit y^{-1} und von rechts mit e_2 und erhalten:

$$\lambda \cdot w = g \cdot y^{-1} \cdot e_2 = b' \cdot v + f \cdot w. \tag{165}$$

Hierbei haben wir benutzt, dass w nach obiger Argumentation Eigenvektor von g ist. Da v, w linear unabhängig sind, gilt dies genau dann, wenn $b' = 0$ und $\lambda = f$. Das bedeutet, die Gleichung (162) hat für jedes $x \in RS_i(R)$ und jedes $y \in Y$ die gleiche Anzahl an Lösungen $g \cdot Z \in G_\infty^{(1)}$. Diese Anzahl ist gegeben durch:

$$|P \cap {}^{x \cdot y} G_\infty^{(1)}| = (q-1) \cdot q^{d \cdot r}. \tag{166}$$

Durch Extraktion des p-Teils erhält man hieraus wieder:

$$|P \cap {}^{x \cdot y} U| = q^{d \cdot r}. \tag{167}$$

Es verbleibt noch die Betrachtung der Teilmenge $G_\infty^{(2)} \subset G_\infty$. Falls die Gleichung (162) für $g \cdot Z \in G_\infty^{(2)}$ erfüllt ist, so ist nach dem obigen Argument die zweite Spalte von y^{-1} ein Eigenvektor von g zu einem Eigenwert $\lambda \in R^*$. Nehmen wir die unteren beiden Komponenten dieses Vektors, so erhalten wir einen Eigenvektor (zum selben Eigenwert) der Cartan-Untermatrix γ von g, die im gegebenen Fall nichtdiagonal ist. Das heißt, das über F_q irreduzible charakteristische Polynom von γ hat eine Nullstelle in R und damit nach Reduktion modulo $\mathfrak{p}$ auch in F_{q^d}, was notwendigerweise dazu führt, dass d gerade sein muss:

$$d \equiv 0 \pmod 2. \tag{168}$$

Es sei nun im Folgenden d gerade und eine nichtdiagonale Cartanmatrix γ fixiert. γ hat dann über R zwei verschiedene Eigenrichtungen: γ hat nach Reduktion modulo $\mathfrak{p}$ zwei verschiedene Eigenvektoren, da γ auch nach Reduktion modulo $\mathfrak{p}$ nichtdiagonal bleibt. Das Lemma von Nakayama auf die jeweiligen Eigenräume angewendet, zeigt, dass auch zwei Eigenrichtungen über R existieren. Wir wollen nun die Anzahl aller $y \in Y$ finden, für die Elemente $a \in F_q^*$, sowie $b, c \in R$ existieren, sodass Gleichung (162) erfüllt ist, wobei

$$g := \begin{pmatrix} a & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix}. \tag{169}$$

Die Menge aller solchen $y \in Y$ heiße Y_0:

$$Y_0 := \{y \in Y | \exists x \in RS_2(R) \cup RS_3(R), a \in F_q^*, b, c \in R : \overline{x} \cdot \overline{y} \cdot \overline{g} \cdot \overline{y}^{-1} \cdot \overline{x}^{-1} \in P\}, \tag{170}$$

wobei wir nur Elemente g der Form (169) betrachten, das heißt mit dem oben fixierten γ.

Um die Kardinalität von Y_0 zu bestimmen, bestimmen wir zunächst die Anzahl aller $\tilde{y}^{-1} \in P$, für die a, b, c wie oben existieren, sodass (162) gilt; der Exponent bei $\tilde{y}^{-1}$ ist technischer Natur. Die Menge aller solchen $\tilde{y}$ bezeichnen wir mit $\tilde{Y}$. Wir schreiben dazu

$$\tilde{y} = \begin{pmatrix} \tilde{y_{11}} & \tilde{y_{12}} & \tilde{y_{13}} \\ 0 & \tilde{y_{22}} & \tilde{y_{23}} \\ 0 & \tilde{y_{32}} & \tilde{y_{33}} \end{pmatrix}. \tag{171}$$

Die obigen Argumente zeigen, dass es $2 \cdot |R^*|$ viele Möglichkeiten gibt, die Parameter $\tilde{y_{22}}$, $\tilde{y_{32}}$ zu wählen: diese müssen Eigenvektoren von γ sein. Die Einträge $\tilde{y_{23}}$, $\tilde{y_{33}}$ müssen so gewählt werden, dass

$$\det \begin{pmatrix} \tilde{y_{22}} & \tilde{y_{23}} \\ \tilde{y_{32}} & \tilde{y_{33}} \end{pmatrix} \in R^*. \tag{172}$$

Hierfür gibt es offenbar noch $(q^{2\cdot d} - q^d) \cdot q^{2\cdot d\cdot(r-1)}$ viele Möglichkeiten. Um die Bedingung $\det(\tilde{y}) \in F_q^*$ zu befriedigen, bleiben noch $(q-1)$ viele Wahlmöglichkeiten für $\tilde{y_{11}}$. Eine einfache Rechnung (analog zu den Betrachtungen in [Boh14]) zeigt, dass bei beliebiger Wahl der übrigen Parameter $\tilde{y_{12}}$, $\tilde{y_{13}}$ noch einer der Parameter b, c aus g frei gewählt werden kann, sodass (162) gilt. Wir erhalten für die Kardinalität von $\tilde{Y}$ (beachte, dass wir noch den Quotienten nach dem Zentrum Z bilden müssen):

$$|\tilde{Y}| = 2 \cdot |R^*| \cdot (q^{2\cdot d} - q^d) \cdot q^{2\cdot d\cdot(r-1)} \cdot q^{2\cdot d\cdot r}. \tag{173}$$

Da die Lösbarkeit von (162) jedoch nur von der Linksnebenklasse von y modulo G_∞ abhängt, erhalten wir:

$$|Y_0| = \frac{2 \cdot |R^*| \cdot (q^{2\cdot d} - q^d) \cdot q^{2\cdot d\cdot(r-1)}}{(q^2-1)}. \tag{174}$$

Genauer können wir zu jedem solchen y nun noch $a \in F_q^*$ beliebig und einen der Parameter b, c frei aus R wählen, um eine Lösung von (162) zu erhalten. Wir bemerken, dass all diese Überlegungen nicht von der expliziten Gestalt des eingangs fixierten γ abhängen. Zusammen mit der Tatsache, dass es genau $q^2 - q$ viele nichtdiagonale γ in der Gruppe $Car(2)$ gibt, erhalten wir die folgende Proposition, die die bisherigen Überlegungen zusammenfasst. Man behalte hierbei die Gruppe Z im Hinterkopf, nach der jeweils noch der Quotient zu nehmen ist.

Proposition 6. *Die Größe $|Y_0|$ sei definiert wie in (174). Dann gilt für den Beitrag zur Spitzenverzweigung von Elementen der Form $x \cdot y$ mit $x \in RS_2(R) \cup RS_3(R)$, $y \in Y$:*

$$\sum_{y \in Y} \sum_{x \in RS_2(R) \cup RS_3(R)} |P \cap {}^{x\cdot y}G_\infty| + |P \cap {}^{x\cdot y}U| \tag{175}$$

$$= |RS_2(R) \cup RS_3(R)| \cdot \big(|Y| \cdot q^{d\cdot r+1} + \omega_\infty(N) \cdot |Y_0| \cdot (q^2 - q) \cdot q^{d\cdot r}\big). \tag{176}$$

Die letzten beiden Propositionen klären die Spitzenverzweigung der Überlagerung ψ für ein primäres N vollständig. Wir wollen diese Bedingung an N nun fallen lassen und die Spitzenverzweigung für ein beliebiges nichtkonstantes N bestimmen.

4.3 Die Verzweigung in den Spitzen im globalen Fall

In diesem Teilabschnitt sei N stets ein beliebiges normiertes, nichtkonstantes Polynom mit Primfaktorisierung

$$N = \prod_{j=1}^{s} {p_j}^{r_j}. \tag{177}$$

Dabei bezeichne d_j den Grad des Primteilers p_j von N und das maximale Ideal im lokalen Ring $R_j := R({p_j}^{r_j})$ heiße $\mathfrak{p}_j$. Wir setzen $G := G(N)$, $R := R(N)$, $P := P(N)$, $U := U(N)$ und $G_\infty := G_\infty(N)$. Weiter definieren wir:

$$RS' := \prod_{j=1}^{s} \big(RS_1(R_j) \cup RS_2(R_j) \cup RS_3(R_j)\big). \tag{178}$$

Da G/P nach Proposition 2 (siehe Seite 19) mit $\mathbb{P}^2(R)$ in Bijektion steht, können wir die Menge RS' nach Proposition 1 (siehe Seite 11) in Abschnitt 2 unter Verwendung des kanonischen Isomorphismus $\tilde{\alpha} := \tilde{\alpha}_{33}$ aus Bemerkung 2, Teil iii) (siehe Seite 8-9) mit einem vollständigen Repräsentantensystem RS für G/P identifizieren:

$$RS := \tilde{\alpha}^{-1}\Big(\prod_{j=1}^{s} \big(RS_1(R_j) \cup RS_2(R_j) \cup RS_3(R_j)\big)\Big). \tag{179}$$

Eine genaue Betrachtung des Beweises von Lemma 7 (siehe Seite 26) zeigt, dass dieses Lemma offenbar auch für ein nichtprimäres N gültig bleibt. Ist Y ein beliebiges Repräsentantensystem für P/G_∞, so folgt also:

Die Menge $\{x \cdot y \mid x \in RS, y \in Y\}$ *bildet ein Repräsentantensystem für* G/G_∞. (180)

Es wird sich damit wieder alles darum drehen, für $x \in RS$ und $y \in Y$ die Größen $|P \cap {}^{x \cdot y}G_\infty|$ zu bestimmen, wobei wir vor dem Problem stehen, dass wir für ein $x \in RS$ nur eine konkrete Beschreibung durch lokale Daten haben.

Sind nun $x \in RS, y \in Y$ und $g \cdot Z \in G_\infty$, so müssen wir also zunächst die Bedingung

$$\overline{x} \cdot \overline{y} \cdot \overline{g} \cdot \overline{y^{-1}} \cdot \overline{x^{-1}} \in P \tag{181}$$

in lokalen Termen erfassen. Der chinesische Restsatz in Form von Lemma 2 (siehe Seite 7-8) beziehungsweise Bemerkung 2 (siehe Seite 8-9) wird sich hierbei als

zentral erweisen. Wir fixieren zunächst das folgende Repräsentantensystem für G_∞:

$$\overline{G_\infty} := \left\{ \begin{pmatrix} 1 & b & c \\ 0 & \gamma_{11} & \gamma_{12} \\ 0 & \gamma_{21} & \gamma_{22} \end{pmatrix} \mid b, c \in R, \gamma \in Car(2) \right\}. \tag{182}$$

Wir verwenden außerdem wieder eine Zerlegung (als Mengen)

$$\overline{G_\infty} = G_\infty^{(1)} \dot\cup G_\infty^{(2)}, \tag{183}$$

wobei $G_\infty^{(1)}$ die Teilmenge der Matrizen aus $\overline{G_\infty}$ mit diagonaler Cartanmatrix bezeichne. $G_\infty^{(2)}$ ist dann das Komplement von $G_\infty^{(1)}$ in $\overline{G_\infty}$. Damit können wir in (181) das herauszudividierende Z unterdrücken und auf der rechten Seite P durch

$$\tilde{P} := \left\{ g = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ 0 & p_{22} & p_{23} \\ 0 & p_{32} & p_{33} \end{pmatrix} \;\middle|\; p_{ij} \in R, \det(g) \in F_q^* \right\} \tag{184}$$

ersetzen. Wir bemerken außerdem, dass für die Elemente in (181) gilt:

$$\det(x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1}) = \det(g) \in F_q^*. \tag{185}$$

Damit können wir $\tilde{P}$ sogar durch die folgende Menge ersetzen:

$$P' := \left\{ g = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ 0 & p_{22} & p_{23} \\ 0 & p_{32} & p_{33} \end{pmatrix} \;\middle|\; p_{ij} \in R, \det(g) \in R^* \right\}, \tag{186}$$

denn die Bedingung an die Determinante für Matrizen in $\tilde{P}$ ist für Elemente der Form $x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1}$ automatisch erfüllt. Wir haben also erreicht:

$$\overline{x} \cdot \overline{y} \cdot \overline{g} \cdot \overline{y^{-1}} \cdot \overline{x^{-1}} \in P \Longleftrightarrow x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} \in P'. \tag{187}$$

Wir bezeichnen mit

$$\tilde{\alpha_i} : GL(3, R) \longrightarrow GL(3, R_i) \tag{188}$$

$$g = (g_{ij}) \longmapsto \begin{pmatrix} \alpha_i(g_{11}) & \alpha_i(g_{12}) & \alpha_i(g_{13}) \\ \alpha_i(g_{21}) & \alpha_i(g_{22}) & \alpha_i(g_{23}) \\ \alpha_i(g_{31}) & \alpha_i(g_{32}) & \alpha_i(g_{33}) \end{pmatrix} \tag{189}$$

die durch die Abbildung α_i aus Lemma 2 induzierte Abbildung. Die letzte Bedingung (187) ist dann aber nach Bemerkung 2, Teil iv) genau dann erfüllt, wenn für alle $1 \leq i \leq s$ das Bild der Bedingung unter der Abbildung $\tilde{\alpha_i}$ erfüllt ist. Ist $W \subset GL(3, R)$ eine beliebige Untergruppe, so schreiben wir für $1 \leq i \leq s$ kurz

$$W_i := \tilde{\alpha_i}(W). \tag{190}$$

Ist $m \in GL(3, R)$, so schreiben wir analog für $1 \leq i \leq s$:

$$m_i := \tilde{\alpha_i}(m). \tag{191}$$

Bemerkung 11. *i) Ist eine (diagonale oder nichtdiagonale) Matrix γ fixiert, so folgt, dass bei festem y die Anzahl der Lösungen x, g (mit festem γ) der Gleichung (187) gegeben ist durch das Produkt über alle $1 \leq j \leq s$ der Anzahlen der Lösungen x_j, g_j (mit demselben festen y und γ) des Bildes der Gleichung (187) unter $\tilde{\alpha_j}$:*

$$x_j \cdot y_j \cdot g_j \cdot y_j^{-1} \cdot x_j^{-1} \in P_j'. \tag{192}$$

Dies folgt aus dem dritten Teil von Bemerkung 2. Man beachte, dass γ in allen lokalen Komponenten R_j gleich aussieht.
ii) Ist $x \in RS$ mit (eindeutig!) assoziiertem Element $(x_1, \ldots, x_s) \in RS'$, so schreiben wir kurz, aber etwas unsauber: $x = (x_1, \ldots, x_s)$.

Zusammen mit den Überlegungen im lokalen Fall und der obigen Bemerkung erhalten wir damit die folgende Proposition:

Proposition 7. *Es sei $x = (x_1, \ldots, x_s) \in RS$ und $y \in Y$. Wir erinnern an die in Definition 6 auf Seite 29 eingeführte Höhe h_{R_j} eines Elementes aus $RS_1(R_j)$ für $1 \leq j \leq s$. Dann gilt:*
a) Falls ein i existiert mit $x_i \in RS_1(R_i)$ und $r_i > h_{R_i}(x_i) > 0$, dann folgt:

$$|P' \cap {}^{x \cdot y} G_\infty^{(1)}| = \prod_{j=1}^{s} |P_j' \cap {}^{x_j} U_j|. \tag{193}$$

b) Falls für alle i mit $x_i \in RS_1(R_i)$ gilt, dass $h_{R_i}(x_i) \in \{0, r_i\}$, so folgt:

$$|P' \cap {}^{x \cdot y} G_\infty^{(1)}| = (q-1) \cdot \prod_{j=1}^{s} |P_j' \cap {}^{x_j} U_j|. \tag{194}$$

c) Für $1 \leq i \leq s$ bezeichnen wir mit n_{i0} die Anzahl der Elemente in $RS_1(R_i)$ von Höhe null und setzen

$$\mu_i := q^{2d_i \cdot (2 \cdot r_i - \lfloor \frac{r_i}{2} \rfloor - 1)} + (q^{2 \cdot d_i} - 1) \cdot q^{d_i \cdot (3 \cdot r_i - 2)} \cdot \lfloor \frac{r_i}{2} \rfloor - |R_i|^2, \tag{195}$$

$$\nu_i := (|\mathbb{P}^2(R_i)| - |R_i|^2) \cdot |R_i| + n_{i0} \cdot |R_i| + |R_i|^2. \tag{196}$$

Wir erhalten

$$\sum_{x \in RS} \sum_{y \in Y} |P' \cap {}^{x \cdot y} G_\infty^{(1)}| + \sum_{x \in RS} \sum_{y \in Y} |P' \cap {}^{x \cdot y} U| \tag{197}$$

$$= |Y| \cdot \left(2 \cdot \left(\prod_{j=1}^{s} (\nu_j + \mu_j) - \prod_{j=1}^{s} \nu_j \right) + q \cdot \prod_{j=1}^{s} \nu_j \right) \tag{198}$$

$$= |Y| \cdot \left(2 \cdot \prod_{j=1}^{s} (\nu_j + \mu_j) + (q-2) \cdot \prod_{j=1}^{s} \nu_j \right). \tag{199}$$

Beweis. Wir bemerken, dass für $g \in G_\infty^{(1)}$ die zugehörige Cartanmatrix γ diagonal ist. Die Betrachtungen im lokalen Fall zeigen, dass die lokalisierten Bedingungen dann stets unabhängig von der genauen Gestalt von $y \in Y$ sind. Es

sei daher im Folgenden ohne Einschränkung $y = \mathbb{1}$ die Einheitsmatrix. Zum eigentlichen Beweis:
a) Sei $f \in F_q^*$ und $g \in G_\infty^{(1)}$ mit diagonaler Cartanmatrix $\gamma = f \cdot \mathbb{1}$, sodass die Bedingung $x \cdot g \cdot x^{-1} \in P'$ erfüllt ist. Wir wissen nach Bemerkung 11, Teil i), dass dies genau dann der Fall ist, wenn alle lokalisierten Gleichungen der Form (192) erfüllt sind (wobei $y = \mathbb{1}$). Angenommen nun, es gebe ein i mit $r_i > h_{R_i}(x_i) > 0$. Dann ist also insbesondere $x_i \neq \mathbb{1}$. Wir betrachten die lokalisierte Bedingung

$$x_i \cdot g_i \cdot x_i^{-1} \in P_i'. \tag{200}$$

Diese ist bekanntlich genau dann erfüllt, wenn die erste Spalte von x_i^{-1} ein Eigenvektor von g zu einem Eigenwert $\lambda \in R^*$ ist. Es sei nun $e_1 \neq v$ die erste Spalte von x_i. Wegen $h_{R_i}(x_i) > 0$ liegen die unteren beiden Einträge v_2, v_3 beide in $\mathfrak{p}_i$ und die lokalisierten Gleichungen lauten

$$\gamma \cdot \begin{pmatrix} v_2 \\ v_3 \end{pmatrix} = \lambda \cdot \begin{pmatrix} v_2 \\ v_3 \end{pmatrix}, \tag{201}$$

$$1 - v_2 \cdot b_i - v_3 \cdot c_i = \lambda. \tag{202}$$

Reduzieren wir (202) modulo $\mathfrak{p}_i$, so erhalten wir

$$1 \equiv \lambda \equiv f \ (\bmod \mathfrak{p}_i\ ). \tag{203}$$

Hierbei haben wir ausgenutzt, dass γ modulo $\mathfrak{p}_i$ genau den Eigenwert f hat. Das bedeutet $f - 1 \in \mathfrak{p}_i$. Wegen $f - 1 \in F_q$ liefert das aber schon $f = 1$. Die Behauptung in a) folgt dann zusammen mit der Definition von U_j aus Bemerkung 11, Teil i), da es für $f \neq 1$ in denjenigen Komponenten, in denen $x_j \neq \mathbb{1}$ positive Höhe hat, keine Lösungen gibt.

b) Für die zweite Aussage bemerken wir, dass unter den Bedingungen in b) die Anzahl der lokalen Lösungen jeweils unabhängig von der genauen Gestalt des gewählten diagonalen γ ist: Falls $x_i \in RS_1(R_i)$ mit $h_{R_i}(x_i) = r_i$, so ist dies trivialerweise richtig, da x_i in diesem Fall die Einheitsmatrix ist. Ist $x_i \in RS_1(R_i)$ mit $h_{R_i}(x_i) = 0$, oder gilt $x_i \in RS_2(R_i) \cup RS_3(R_i)$, so folgt die Unabhängigkeit von der genauen Gestalt von γ aus der genauen Analyse der in Abschnitt 4.2 gefundenen Ergebnisse (vergleiche etwa Lemma 8 auf Seite 29 und Beziehung (166) auf Seite 32). Die Behauptung b) folgt dann zusammen mit Bemerkung 11, Teil i).

c) Wir beweisen nun die letzte Aussage. Es gilt:

$$\sum_{x \in RS} \sum_{y \in Y} |P' \cap {}^{x \cdot y} G_\infty^{(1)}| + \sum_{x \in RS} \sum_{y \in Y} |P' \cap {}^{x \cdot y} U| \tag{204}$$

$$= |Y| \cdot \big(\sum_{x \in RS} |P' \cap {}^{x} G_\infty^{(1)}| + |P' \cap {}^{x} U| \big). \tag{205}$$

Wir untersuchen zunächst den Ausdruck $\sigma := \sum_{x \in RS} |P' \cap {}^{x}G_{\infty}^{(1)}|$. Es bezeichne M_1 die Menge aller $x \in RS$, für die die Bedingung aus Teil a) erfüllt ist. Die Menge der übrigen $x \in RS$ heiße M_2. Damit erhalten wir:

$$\sigma = \sum_{x \in M_1} |P' \cap {}^{x}G_{\infty}^{(1)}| + \sum_{x \in M_2} |P' \cap {}^{x}G_{\infty}^{(1)}|. \tag{206}$$

Wir wollen die Summe σ nun in zwei Schritten auswerten:

i) Um die Summe über alle Elemente aus M_1 auszuwerten, zerlegen wir M_1 disjunkt in Teilmengen T_i für $1 \leq i \leq s$:

$$T_i := \Big\{ x \in M_1 \mid i = \min\{j \mid x_j \in RS_1(R_j),\ r_j > h_{R_j}(x_j) > 0\} \Big\}. \tag{207}$$

Für $1 \leq j \leq s$ und $1 \leq i \leq r_j$ bezeichnen wir außerdem mit $RS_1(R_j)_i$ die Menge aller Elemente aus $RS_1(R_j)$, deren Höhe i ist. Als letztes setzen wir für obige j

$$T_{1j} := RS_1(R_j)_0 \cup RS_2(R_j) \cup RS_3(R_j), \tag{208}$$

$$T_{2j} := \bigcup_{1<i<r_j} RS_1(R_j)_i, \tag{209}$$

$$T_{3j} := RS_1(R_j) \cup RS_2(R_j) \cup RS_3(R_j). \tag{210}$$

Summieren wir nun gemäß obiger Zerlegung $M_1 = \bigcup_{1 \leq i \leq s} T_i$, so erhalten wir unter Beachtung von Teil a):

$$\sum_{x \in M_1} |P' \cap {}^{x}G_{\infty}^{(1)}| = \sum_{x \in M_1} \prod_{j=1}^{s} |P'_j \cap {}^{x_j}U_j| \tag{211}$$

$$= \sum_{i=1}^{s} \Big(\prod_{j=1}^{i-1} \sum_{x_j \in T_{1j}} |P'_j \cap {}^{x_j}U_j| \Big) \cdot \Big(\sum_{x_i \in T_{2i}} |P'_i \cap {}^{x_i}U_i| \Big) \cdot \Big(\prod_{j=i+1}^{s} \sum_{x_j \in T_{3j}} |P'_j \cap {}^{x_j}U_j| \Big). \tag{212}$$

Die auftretenden Größen $|P'_i \cap {}^{x_i}U_i|$ sind jedoch rein lokaler Natur. Diese können aus Beziehung (167) in Abschnitt 4.2 beziehungsweise mit Lemma 8 und Lemma 9 aus demselben Abschnitt bestimmt werden, je nachdem, in welcher Menge T_{ki} ein gegebenes x_i liegt. Eine direkte Rechnung liefert dann:

$$\sum_{i=1}^{s} \Big(\prod_{j=1}^{i-1} \sum_{x_j \in T_{1j}} |P'_j \cap {}^{x_j}U_j| \Big) \cdot \Big(\sum_{x_i \in T_{2i}} |P'_i \cap {}^{x_i}U_i| \Big) \cdot \Big(\prod_{j=i+1}^{s} \sum_{x_j \in T_{3j}} |P'_j \cap {}^{x_j}U_j| \Big) \tag{213}$$

$$= \sum_{i=1}^{s} \Big(\prod_{j=1}^{i-1} \nu_j \cdot \mu_i \cdot \prod_{j=i+1}^{s} (\nu_j + \mu_j) \Big). \tag{214}$$

Wir bemerken, dass

$$\sum_{i=1}^{s}(\prod_{j=1}^{i-1}\nu_j\cdot\mu_i\cdot\prod_{j=i+1}^{s}(\nu_j+\mu_j))=\prod_{j=1}^{s}(\nu_j+\mu_j)-\prod_{j=1}^{s}\nu_j, \tag{215}$$

wie eine kombinatorische Überlegung zeigt. Damit ist die erste Summe abgehandelt. Wir stellen fest, dass der letzte Ausdruck invariant unter Permutationen $\pi:\{1,\ldots,s\}\longrightarrow\{1,\ldots,s\}$ ist; dies sollte auch so sein, da unser Ergebnis nicht von der Reihenfolge der Primfaktoren in $N=\prod_{j=1}^{s}p_j^{r_j}$ abhängen sollte.

ii) Als nächstes wollen wir die Summe über alle Elemente x aus M_2 auswerten. Nach Konstruktion von M_2 sind die Voraussetzungen aus Teil b) der Proposition für alle $x\in M_2$ stets erfüllt. Wir setzen für ein beliebiges $x\in M_2$:

$$J_1(x):=\{j\mid 1\le j\le s, x_j\in RS_1(R_j)_0\}, \tag{216}$$

$$J_2(x):=\{j\mid 1\le j\le s, x_j\in RS_1(R_j)_{r_j}\}, \tag{217}$$

$$J_3(x):=\{j\mid 1\le j\le s, x_j\in RS_2(R_j)\cup RS_3(R_j)\}. \tag{218}$$

Damit erhalten wir:

$$\sum_{x\in M_2}|P'\cap{}^{x}G_\infty^{(1)}|=(q-1)\cdot\sum_{x\in M_2}\prod_{j=1}^{s}|P'_j\cap{}^{x_j}U_j| \tag{219}$$

$$=(q-1)\cdot\sum_{x\in M_2}\big(\prod_{j\in J_1(x))}|P'_j\cap{}^{x_j}U_j|\cdot\prod_{j\in J_2(x)}|P'_j\cap{}^{x_j}U_j|\cdot\prod_{j\in J_3(x)}|P'_j\cap{}^{x_j}U_j|\big). \tag{220}$$

Wir wollen die Menge aller geordneten Tripel (J_1,J_2,J_3) von (möglicherweise leeren) Teilmengen $J_i\subset\{1,\ldots,s\}$, die eine disjunkte Zerlegung von $\{1,\ldots,s\}$ liefern, mit Ω bezeichnen. Wenn nun x über alle Elemente von M_2 rangiert, dann rangieren die (geordneten) Tripel $(J_1(x),J_2(x),J_3(x))$ über alle Elemente von Ω. Wir führen für $1\le j\le s$ noch die folgenden Abkürzungen ein:

$$\sigma_{1j}:=\sum_{x_j\in RS_1(R_j)_0}|P'_j\cap{}^{x_j}U_j|, \tag{221}$$

$$\sigma_{2j}:=\sum_{x_j\in RS_1(R_j)_{r_j}}|P'_j\cap{}^{x_j}U_j|, \tag{222}$$

$$\sigma_{3j}:=\sum_{x_j\in RS_2(R_j)\cup RS_3(R_j)}|P'_j\cap{}^{x_j}U_j|. \tag{223}$$

Damit erhalten wir:

$$(q-1)\cdot\sum_{x\in M_2}\big(\prod_{j\in J_1(x)}|P'_j\cap{}^{x_j}U_j|\cdot\prod_{j\in J_2(x)}|P'_j\cap{}^{x_j}U_j|\cdot\prod_{j\in J_3(x)}|P'_j\cap{}^{x_j}U_j|\big) \tag{224}$$

$$=(q-1)\cdot\sum_{(J_1,J_2,J_3)\in\Omega}\prod_{j\in J_1}\sigma_{1j}\cdot\prod_{j\in J_2}\sigma_{2j}\cdot\prod_{j\in J_3}\sigma_{3j}. \tag{225}$$

Die Größen $\sigma_{1j}, \sigma_{2j}, \sigma_{3j}$ können wiederum aus den Resultaten aus Abschnitt 4.2 gewonnen werden. Genauer gilt für alle $1 \leq j \leq s$:

$$\sigma_{1j} = n_{jo} \cdot |R_j|, \tag{226}$$

$$\sigma_{2j} = |R_j|^2, \tag{227}$$

$$\sigma_{3j} = (|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j|. \tag{228}$$

Damit ergibt sich:

$$(q-1) \cdot \sum_{(J_1,J_2,J_3)\in\Omega} \prod_{j\in J_1} \sigma_{1j} \cdot \prod_{j\in J_2} \sigma_{2j} \cdot \prod_{j\in J_3} \sigma_{3j} \tag{229}$$

$$= (q-1) \cdot \sum_{(J_1,J_2,J_3)\in\Omega} \prod_{j\in J_1} (n_{jo} \cdot |R_j|) \cdot \prod_{j\in J_2} |R_j|^2 \cdot \prod_{j\in J_3} (|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j|). \tag{230}$$

Eine direkte kombinatorische Überlegung zusammen mit der Definition von Ω liefert schließlich:

$$(q-1) \cdot \sum_{(J_1,J_2,J_3)\in\Omega} \prod_{j\in J_1} (n_{jo} \cdot |R_j|) \cdot \prod_{j\in J_2} |R_j|^2 \cdot \prod_{j\in J_3} (|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j|) \tag{231}$$

$$= (q-1) \cdot \prod_{j=1}^{s} \big(n_{jo} \cdot |R_j| + |R_j|^2 + (|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j|\big) \tag{232}$$

$$= (q-1) \cdot \prod_{j=1}^{s} \nu_j. \tag{233}$$

Damit ist also $\sigma = \sum_{x\in RS} |P' \cap {}^{x}G_\infty^{(1)}| = (q-1) \cdot \prod_{j=1}^{s} \nu_j$. Die verbleibende Summe $\tau := \sum_{x\in RS} |P' \cap {}^{x}U|$ behandelt man völlig analog. Addiert man $|Y| \cdot \sigma$ und $|Y| \cdot \tau$, so erhält man Behauptung c). □

Damit können wir uns der Menge $G_\infty^{(2)}$ zuwenden. Um uns bequem ausdrücken zu können, setzen wir für ein $x = (x_1, \ldots, x_s) \in RS$:

$$\mathfrak{S}_1(x) := \{j \mid x_j \in RS_1(R_j)\}, \tag{234}$$

$$\mathfrak{S}_2(x) := \{j \mid x_j \in RS_2(R_j) \cup RS_3(R_j)\}. \tag{235}$$

Damit können wir die folgende Proposition formulieren, mit der wir die Spitzenverzweigung komplett abhandeln.

Proposition 8. *Wir definieren für $1 \leq j \leq s$ analog zu Abschnitt 4.2, Beziehung (173) die folgenden lokalen Größen:*

$$|\tilde{Y}_j| = 2 \cdot |R_j^*| \cdot (q^{2\cdot d_j} - q^{d_j}) \cdot q^{2\cdot d_j \cdot (r_j - 1)} \cdot q^{2\cdot d_j \cdot r_j}. \tag{236}$$

Außerdem sei S_0 die Menge aller j, für die d_j gerade ist, und S_1 bezeichne die Menge der übrigen Indizes j. Mit dieser Notation gilt:

$$\sum_{x\in RS}\sum_{y\in Y}|P'\cap {}^{x\cdot y}G_\infty^{(2)}| \tag{237}$$

$$=\frac{q\cdot\prod_{j\in S_1}|R_j|\cdot|P_j|\cdot\prod_{j\in S_0}\Big((2\cdot|R_j^*|+|R_j|)\cdot|P_j|+(|\mathbb{P}^2(R_j)|-|R_j|^2)\cdot|\tilde{Y}_j|\Big)}{(q+1)\cdot|R|}. \tag{238}$$

Beweis. Der Beweis ist relativ lang und technisch. Wir gehen deshalb in mehreren Schritten vor.

i) Wir bemerken zunächst, dass für $x\in RS$ und $y\in Y$ die Bedingung

$$x\cdot y\cdot g\cdot y^{-1}\cdot x^{-1}\in P' \tag{239}$$

mit

$$g=\begin{pmatrix}a & b & c\\ 0 & \gamma_{11} & \gamma_{12}\\ 0 & \gamma_{21} & \gamma_{22}\end{pmatrix} \tag{240}$$

bei fixiertem nichtdiagonalem γ nach Bemerkung 2, Teil iv) genau dann erfüllt ist, wenn die jeweiligen lokalisierten Bedingungen alle simultan erfüllt sind:

$$\forall j\in\mathfrak{S}_1(x): g_j\cdot x_j^{-1}\cdot e_1=\lambda_j\cdot x_j^{-1}\cdot e_1, \tag{241}$$

$$\forall i\in\mathfrak{S}_2(x): g_i\cdot y_i^{-1}\cdot e_2=\lambda_i\cdot y_i^{-1}\cdot e_2. \tag{242}$$

Hierbei haben wir verwendet, dass die erste Spalte von x_j^{-1} stets durch den zweiten Standardbasisvektor e_2 gegeben ist, falls $x_j\in RS_2(R_j)\cup RS_3(R_j)$ (vergleiche etwa Beziehung (161) aus Abschnitt 4.2). Außerdem bemerken wir, dass die lokalisierten Gleichungen für $j\in\mathfrak{S}_1(x)$ nicht von der genauen Gestalt von y_j abhängen. Im weiteren Verlauf des Beweises sei γ bis auf Weiteres fixiert und $G_{\infty,\gamma}^{(2)}$ bezeichne die Menge aller $g\in G_\infty^{(2)}$ mit fester nichtdiagonaler Cartanmatrix γ:

$$G_{\infty,\gamma}^{(2)}:=\{\begin{pmatrix}1 & b & c\\ 0 & \gamma_{11} & \gamma_{12}\\ 0 & \gamma_{21} & \gamma_{22}\end{pmatrix}\mid b,c\in R\}. \tag{243}$$

Setze außerdem wieder $G_{\infty,\gamma,j}^{(2)}:=\tilde{\alpha_j}(G_{\infty,\gamma}^{(2)})$.

ii) Wir betrachten nun zunächst bei festem y_j die Gleichung (241) für $j\in\mathfrak{S}_1(x)$. Angenommen diese habe eine Lösung x_j,g_j. Wir bezeichnen mit v_j beziehungsweise w_j den zweiten beziehungsweise dritten Eintrag der ersten Spalte von x_j. Angenommen $r_j>h_{R_j}(x_j)>0$, dann folgt aus

$$1-b_j\cdot v_j-c_j\cdot w_j=\lambda_j \tag{244}$$

nach Reduktion modulo $\mathfrak{p}_j$, dass γ über $F_{q^{d_j}}$ diagonal sein muss mit Eigenwert 1. Dann muss γ aber auch schon über R diagonal gewesen sein, im Widerspruch zur Wahl von γ. Falls $j \in \mathfrak{S}_1(x)$, dann gilt also notwendig

$$x_j = \mathbb{1} \dot{\vee} h_{R_j}(x_j) = 0, \tag{245}$$

das heißt x_j hat Höhe null oder x_j ist die Einheitsmatrix. Falls x_j Höhe null hat, so sehen wir, dass $\begin{pmatrix} v_j \\ w_j \end{pmatrix}$ Eigenvektor von γ in R_j sein muss; insbesondere folgt in diesem Fall notwendig

$$d_j \equiv 0 \ (\bmod 2\ ). \tag{246}$$

Bei der Betrachtung des lokalen Falls haben wir unter Anwendung des Lemmas von Nakayama auf die Eigenräume von γ in $(R_j/\mathfrak{p}_j)^2 \cong (F_{q^{d_j}})^2$ gesehen, dass es bei geradem d_j genau $2{\cdot}|R_j^*|$ viele Möglichkeiten für x_j gibt. Von den Parametern $b_j, c_j \in R_j$ können wir einen frei wählen, wie der lokale Fall zeigt. Falls d_j gerade, erhalten wir also bei festem γ für alle j genau

$$2 \cdot |R_j^*| \cdot |R_j| + |R_j|^2 \tag{247}$$

viele Möglichkeiten für die Wahl von x_j und g_j, sodass (241) bei festem y_j gilt. Ist d_j ungerade, so erhalten wir

$$|R_j|^2 \tag{248}$$

viele Möglichkeiten für x_j und g_j. Beachte, dass in diesem Fall notwendig x_j die Einheitsmatrix über R_j ist.

iii) Es verbleibt die Betrachtung der Gleichung (242) bei festem $x \in RS$ für $j \in \mathfrak{S}_2(x)$. Wir wollen zunächst die Anzahl aller $y \in \tilde{P}$ bestimmen, für die bei festem x Elemente $g \in G^{(2)}_{\infty,\gamma}$ existieren, sodass (241) und (242) erfüllt sind. Die Menge solcher y heiße $\tilde{Y}_x$:

$$\tilde{Y}_x := \{y \in \tilde{P} \mid \exists g \in G^{(2)}_{\infty,\gamma} : x \cdot y \cdot g \cdot y^{-1} \cdot x^{-1} \in P'\}. \tag{249}$$

Aus (249) folgt sofort:

$$y \in \tilde{Y}_x \Rightarrow y \cdot G_\infty \subset \tilde{Y}_x. \tag{250}$$

Da die Gleichungen (241) außerdem unabhängig von y_j sind, stellen diese keine Einschränkungen dar. Die Gleichungen (242) sind in Wahrheit nur Bedingungen an die zweite Spalte von y_j^{-1}; diese sei im Folgenden mit u_j bezeichnet. Eine genauere Betrachtung, wie im lokalen Fall, zeigt, dass (242) bedeutet, dass die unteren beiden Einträge von u_j ein R_j^*-Vielfaches einer Eigenrichtung von γ über R_j sein müssen. Man beachte hierzu, dass einer der beiden Einträge von u_j in R_j^* liegen muss, da sonst die Matrix y_j^{-1} über R_j nicht invertierbar wäre. Damit wäre aber auch y^{-1} über R nicht invertierbar, ein Widerspruch. Wir schließen,

dass notwendig d_j gerade sein muss. In diesem Fall gibt es dann $2 \cdot |R_j^*|$ viele Möglichkeiten für die Wahl der unteren beiden Einträge von u_j, während der obere Eintrag beliebig gewählt werden kann: man erinnere sich hierzu einfach an die Blockstruktur der Matrizen in $\tilde{P}$ und an die Lösungsstruktur der lokalisierten Bedingung. Wir bezeichnen mit S_0 die Menge aller j, für die d_j gerade ist, und mit S_1 die Menge der übrigen Indizes; ist dann n_{j0} die Anzahl der Elemente aus $RS_1(R_j)$ von Höhe null, so erhalten wir also

$$2^{|S_0 \cap \mathfrak{S}_2(x)|} \cdot \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |R_j^*| \cdot |R_j| \cdot \prod_{j \in S_0 \cap \mathfrak{S}_1(x)} n_{j0} \cdot |R_j| \cdot \prod_{j \in S_1} n_{j0} \cdot |R_j| \quad (251)$$

viele Möglichkeiten für die Wahl der zweiten Spalte von y^{-1}. Aus der Blockstruktur von y schließen wir, dass es für die dritte Spalte von y^{-1} noch genau

$$(|\mathbb{P}^1(R)| - 1) \cdot |R^*| \cdot |R| \quad (252)$$

viele Möglichkeiten gibt. Für den obersten Eintrag in der ersten Spalte bleiben dann wegen der Determinantenbedingung an Matrizen in $\tilde{P}$ noch $q-1$ viele Wahlmöglichkeiten. Insgesamt gilt also:

$$\frac{|\tilde{Y}_x|}{q-1} = 2^{|S_0 \cap \mathfrak{S}_2(x)|} \, (|\mathbb{P}^1(R)| - 1) \, |R^*| \, |R|^2 \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |R_j^*| \prod_{j \in (S_0 \cap \mathfrak{S}_1(x)) \cup S_1} n_{j0}. \quad (253)$$

Wir setzen nun (vergleiche Beziehung (173) in Abschnitt 4.2, Seite 33)

$$|\tilde{Y}_j| := 2 \cdot |R_j^*| \cdot (q^{2 \cdot d_j} - q^{d_j}) \cdot q^{2 \cdot d_j \cdot (r_j - 1)} \cdot q^{2 \cdot d_j \cdot r_j} \quad (254)$$

und bemerken, dass damit gilt:

$$\frac{|\tilde{Y}_x|}{q-1} = \prod_{j \in S_1 \cup (S_0 \cap \mathfrak{S}_1(x))} \left(n_{j0} \cdot (|\mathbb{P}^1(R_j)| - 1) \cdot |R_j^*| \cdot |R_j|^2 \right) \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |\tilde{Y}_j| \quad (255)$$

$$= \prod_{j \in S_1 \cup (S_0 \cap \mathfrak{S}_1(x))} |P_j| \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |\tilde{Y}_j|. \quad (256)$$

Sind alle x_j vom Typ $RS_1(R_j)$, so gilt offenbar

$$|\tilde{Y}_x| = |\tilde{P}|, \quad (257)$$

in Übereinstimmung mit der Tatsache, dass die jeweiligen Gleichungen in diesem Fall nicht von der konkreten Gestalt von y abhängen.

Wir bezeichnen mit Y_x das Bild von $\tilde{Y}_x$ unter der kanonischen Restklassenprojektion $\tilde{P} \to \tilde{P}/\tilde{G_\infty}$, wobei $\tilde{G_\infty}$ das Urbild von G_∞ in $GL(3,R)$ bezeichne. Mit (256) erhalten wir dann:

$$|Y_x| = \frac{\prod_{j \in S_1 \cup (S_0 \cap \mathfrak{S}_1(x))} |P_j| \cdot \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |\tilde{Y}_j|}{(q^2-1) \cdot |R|^2}. \quad (258)$$

Wir beobachten, dass $|Y_x|$ nicht von der genauen Gestalt von x abhängt. Ist außerdem d_j ungerade, so gibt es bei festem nichtdiagonalem γ wegen $j \in \mathfrak{S}_2(x)$ keine Lösungen x_j, g_j der jeweiligen lokalisierten Gleichung (242), wie die Betrachtungen im lokalen Fall zeigen. Falls d_j gerade, so zeigt der lokale Fall, dass es

$$(|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j| \tag{259}$$

viele Lösungen x_j, g_j der Gleichung (242) gibt: da $j \in \mathfrak{S}_2(x)$, ist x_j beliebig aus $RS_2(R_j) \cup RS_3(R_j)$ wählbar und in g_j kann jeweils einer der Parameter b_j, c_j frei gewählt werden.

iv) Wir bemerken, dass unsere bisherigen Ergebnisse weder von der genauen Gestalt von γ, noch von der genauen Gestalt von x abhängen; wir haben nur benutzt, dass γ nichtdiagonal ist und es war für ein gegebenes $x = (x_1, \ldots, x_s) \in RS$ bei gegebenem i nur relevant, ob $x_i \in RS_1(R_i)$, $x_i \in RS_2(R_i)$ oder ob $x_i \in RS_3(R_i)$. Wir wählen nun für $j \in S_1$ beliebige Elemente $y_j \in \tilde{P}_j$. Für $j \in S_0$ wählen wir Elemente $y_j \in \tilde{P}_j$, für welche Lösungen x_j, g_j der Gleichung (242) existieren. In Teil ii) (vergleiche Beziehung (245)) hatten wir gesehen, dass für $j \in \mathfrak{S}_1(x)$ und beliebiges $y_j \in \tilde{P}_j$ mit $|P' \cap {}^{x_j \cdot y_j} G_\infty^{(2)}| > 0$ folgt, dass $h_{R_j}(x_j) \in \{0, r_j\}$. Ist $j \in S_1$ und $y_j \in \tilde{P}_j$ beliebig, so zeigen die Überlegungen im lokalen Fall, dass aus $|P' \cap {}^{x_j \cdot y_j} G_\infty^{(2)}| > 0$ folgt, dass x_j die Einheitsmatrix über R_j ist. Falls $j \in \mathfrak{S}_2(x)$, so ist die Lösbarkeit von (242) offenbar unabhängig von der genauen Gestalt von x; wir benötigen lediglich, dass y_j so beschaffen ist, dass Lösungen existieren. Dies erklärt die obige Wahl der Elemente $y_1, \ldots, y_s$, die wir benötigen, um uns im folgenden Teil bequem ausdrücken zu können.

v) Wir erhalten für ein festes $x \in RS$ und ein festes nichtdiagonales γ unter Beachtung von Bemerkung 2, Teil iv) und Bemerkung 11:

$$\frac{\sum_{y \in Y} |P' \cap {}^{x \cdot y} G_\infty^{(2)}|}{(q^2 - q)} \tag{260}$$

$$= |Y_x| \cdot \prod_{j \in S_1} |P' \cap {}^{x_j \cdot y_j} G_{\infty,\gamma,j}^{(2)}| \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |P' \cap {}^{x_j \cdot y_j} G_{\infty,\gamma,j}^{(2)}| \prod_{j \in S_0 \cap \mathfrak{S}_1(x)} |P' \cap {}^{x_j \cdot y_j} G_{\infty,\gamma,j}^{(2)}|. \tag{261}$$

Verwenden wir die obige Formel (258) für $|Y_x|$ und bringen wir den Nenner auf der rechten Seite nach links, so erhalten wir:

$$\frac{(q+1) \cdot |R|^2 \cdot \sum_{y \in Y} |P' \cap {}^{x \cdot y} G_\infty^{(2)}|}{q} = \tag{262}$$

$$\prod_{j \in S_1} |P' \cap {}^{x_j y_j} G_{\infty,\gamma,j}^{(2)}||P_j| \prod_{j \in S_0 \cap \mathfrak{S}_2(x)} |P' \cap {}^{x_j y_j} G_{\infty,\gamma,j}^{(2)}||\tilde{Y}_j| \prod_{j \in S_0 \cap \mathfrak{S}_1(x)} |P' \cap {}^{x_j y_j} G_{\infty,\gamma,j}^{(2)}||P_j|. \tag{263}$$

Nehmen wir nun in (263) die Summe über alle $x \in RS$, so liefern alle Elemente $x = (x_1, .., x_s)$ mit der Eigenschaft, dass ein $i \in S_1$ existiert mit $x_i \neq \mathbb{1}$, keinen Beitrag zur betrachteten Summe. Wir bezeichnen mit M die Menge aller $x = (x_1, .., x_s)$, für die gilt, dass $x_i = \mathbb{1}$ für alle $i \in S_1$. Es reicht also wenn wir in (263) die Summe über alle $x \in M$ nehmen. Wir bezeichnen analog zum Beweis von Proposition 7, Teil c) mit Ω die Menge aller geordneten Paare (J_1, J_2) von

möglicherweise leeren Teilmengen $J_1, J_2 \subset S_0$ für die gilt, dass $J_1 \cup J_2 = S_0$ eine disjunkte Zerlegung ist. Läuft nun x über alle Elemente von M, so laufen die geordneten Paare $(S_0 \cap \mathfrak{S}_1(x), S_0 \cap \mathfrak{S}_2(x))$ über alle Elemente von Ω, während für alle $j \in S_1$ stets $x_j = \mathbb{1}$ die Einheitsmatrix ist. Summieren wir also (263) über alle $x \in M$ so erhalten wir mit Teil ii) (vergleiche etwa Nummer (247) und (248)) und Teil iii) (siehe etwa Nummer (259)) den Wert:

$$\sum_{(J_1,J_2)\in\Omega} \prod_{j\in S_1} |R_j|^2 \cdot |P_j| \prod_{j\in J_1} (2\cdot|R_j^*|\cdot|R_j| + |R_j|^2)\cdot|P_j| \prod_{j\in J_2} |\mathbb{P}^2(R_j)| - |R_j|^2)\cdot|R_j|\cdot|\tilde{Y}_j| \tag{264}$$

$$= \prod_{j\in S_1} |R_j|^2 \cdot |P_j| \prod_{j\in S_0} \Big((2\cdot|R_j^*|\cdot|R_j| + |R_j|^2)\cdot|P_j| + (|\mathbb{P}^2(R_j)| - |R_j|^2)\cdot|R_j|\cdot|\tilde{Y}_j| \Big). \tag{265}$$

Bei der letzten Gleichheit haben wir den Faktor $\prod_{j\in S_1} |R_j|^2 \cdot |P_j|$ aus der Summe gezogen und die Summe mit der Definition von Ω ausgewertet. Es folgt:

$$\frac{(q+1)\cdot|R|^2}{q} \cdot \sum_{x\in RS} \sum_{y\in Y} |P' \cap {}^{x\cdot y} G_\infty^{(2)}| \tag{266}$$

$$= |R| \cdot \prod_{j\in S_1} |R_j|\cdot|P_j| \prod_{j\in S_0} \Big((2\cdot|R_j^*| + |R_j|)\cdot|P_j| + (|\mathbb{P}^2(R_j)| - |R_j|^2)\cdot|\tilde{Y}_j| \Big). \tag{267}$$

Bringen wir den Faktor auf der linken Seite nach rechts und vereinfachen, so ergibt sich schließlich:

$$\sum_{x\in RS} \sum_{y\in Y} |P' \cap {}^{x\cdot y} G_\infty^{(2)}| \tag{268}$$

$$= \frac{q\cdot\prod_{j\in S_1}|R_j|\cdot|P_j|\cdot\prod_{j\in S_0}\Big((2\cdot|R_j^*|+|R_j|)\cdot|P_j| + (|\mathbb{P}^2(R_j)|-|R_j|^2)\cdot|\tilde{Y}_j|\Big)}{(q+1)\cdot|R|}. \tag{269}$$

Damit ist der Beweis beendet. □

Mit Proposition 7 und Proposition 8 haben wir jetzt die Spitzenverzweigung für ein beliebiges nichtkonstantes, normiertes $N \in A$ mit Primfaktorisierung

$$N = \prod_{j=1}^{s} p_j^{r_j} \tag{270}$$

explizit unter Kontrolle. Wir wollen dieses Ergebnis in einem Satz zusammenfassen, der diesen Unterabschnitt beendet.

Satz 2. *Es sei $N \in A$ wie in (270). Wir definieren für $1 \le j \le s$ die Größen ν_j, μ_j wie in Proposition 7:*

$$\mu_j := q^{2\cdot d_j\cdot(2\cdot r_j - \lfloor \frac{r_j}{2}\rfloor - 1)} + (q^{2\cdot d_j}-1)\cdot q^{d_j\cdot(3\cdot r_j-2)}\cdot\lfloor\frac{r_j}{2}\rfloor - |R_j|^2, \tag{271}$$

$$\nu_j := (|\mathbb{P}^2(R_j)| - |R_j|^2)\cdot|R_j| + n_{j0}\cdot|R_j| + |R_j|^2. \tag{272}$$

Hierbei bezeichnet n_{j0} wieder die Anzahl aller Elemente aus $RS_1(R_j)$ von Höhe null, im Sinne von Definition 6. Weiter setzen wir gemäß (173)

$$|\tilde{Y}_j| = 2\cdot|R_j^*|\cdot(q^{2\cdot d_j} - q^{d_j})\cdot q^{2\cdot d_j\cdot(r_j-1)}\cdot q^{2\cdot d_j\cdot r_j}. \tag{273}$$

S_1 sei die Menge aller Indizes j, für die d_j ungerade ist. Die Menge der übrigen Indizes heiße wieder S_0. Mit diesen Bezeichnungen erhalten wir für den Beitrag der Spitzen zur Verzweigung der Überlagerung $\psi : X(N) \longrightarrow X_0(N)$ den folgenden Wert:

$$\mathfrak{R}_\infty(N) := \sum_{x \in RS} \sum_{y \in Y} |P' \cap {}^{x \cdot y} G_\infty| + |P' \cap {}^{x \cdot y} U| - 2 \tag{274}$$

$$= \frac{q \cdot \prod_{j \in S_1} (|P_j| \cdot |R_j|) \cdot \prod_{j \in S_0} \Big(|P_j| \cdot (2 \cdot |R_j^*| + |R_j|) + |\tilde{Y}_j| \cdot (|\mathbb{P}^2(R_j)| - |R_j|^2) \Big)}{(q+1) \cdot |R|} \tag{275}$$

$$+ |Y| \cdot \left(2 \cdot \prod_{j=1}^{s} (\nu_j + \mu_j) + (q-2) \cdot \prod_{j=1}^{s} \nu_j \right) - 2 \cdot |G/G_\infty|. \tag{276}$$

Beweis. Der Satz folgt direkt aus Proposition 7 und Proposition 8. □

4.4 Die elliptische Verzweigung

Es sei $N \in A$ nichtkonstant und normiert mit Primfaktorisierung

$$N = \prod_{j=1}^{s} p_j^{r_j}. \tag{277}$$

Weiter gelte $\deg(p_j) = d_j$ und das maximale Ideal in $R_j := R(p_j^{r_j})$ heiße wieder $\mathfrak{p}_j$. Setze außerdem wie zuvor $R := R(N)$, $G := G(N)$ und $P := P(N)$. Sei weiter $C = G_{\mathfrak{e}}$ wie in Theorem 2, Teil iii). Wir bezeichnen mit $\tilde{G}$, $\tilde{C}$ und $\tilde{P}$ die Urbilder von G, C beziehungsweise P unter der Restklassenprojektion $GL(3,R) \longrightarrow GL(3,R)/Z$. Wir erinnern daran, dass nach Theorem 2 die elliptischen Punkte von $X(N)$ mit der Restklassenmenge $G/C = \tilde{G}/\tilde{C}$ identifiziert werden können

$$G/C \longrightarrow X(N)_{ell} \tag{278}$$

$$\xi \longmapsto \xi \cdot \mathfrak{e}. \tag{279}$$

Beachte, dass nach Theorem 2 die Fixgruppe eines elliptischen Punktes $\xi \cdot \mathfrak{e}$ gegeben ist durch

$$G_{\xi \cdot \mathfrak{e}} = {}^{\xi} C. \tag{280}$$

Zum Anfang unserer Betrachtungen geben wir nun zunächst ein Lemma, dessen (ausgelassener) Beweis völlig analog zu dem von Lemma 6 ist.

Lemma 10. *Die Verzweigungszahl eines elliptischen Punktes $\xi \cdot \mathfrak{e}$ unter der Überlagerung ψ mit Galoisgruppe P ist gegeben durch:*

$$a_{\xi \cdot \mathfrak{e}} = |P \cap {}^{\xi} C| - 1. \tag{281}$$

Wir fixieren ein Repräsentantensystem $\{\eta\}$ für $G/C = \tilde{G}/\tilde{C}$ und stehen mit dem letzten Lemma nun also noch vor dem Problem, die Summe

$$\mathfrak{R}_0(N) := \sum_{\eta \in G/C} |P \cap {}^{\eta}C| - 1 = \sum_{\eta \in \tilde{G}/\tilde{C}} \frac{|P' \cap {}^{\eta}\tilde{C}|}{q-1} - 1 \tag{282}$$

auszuwerten. Hierbei sei wieder

$$P' := \left\{ g = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ 0 & p_{22} & p_{23} \\ 0 & p_{32} & p_{33} \end{pmatrix} \;\middle|\; p_{ij} \in R, \det(g) \in R^* \right\} \tag{283}$$

und das zweite Gleichheitszeichen in (282) gilt wiederum, weil Elemente aus C automatisch durch Matrizen repräsentiert werden, deren Determinante in F_q^* liegt. Wir verwenden für $1 \leq i \leq s$ wieder die Abbildungen aus Lemma 2 (siehe Seite 7-8):

$$\tilde{\alpha_i} : GL(3,R) \longrightarrow GL(3,R_i) \tag{284}$$

$$g = (g_{ij}) \longmapsto \begin{pmatrix} \alpha_i(g_{11}) & \alpha_i(g_{12}) & \alpha_i(g_{13}) \\ \alpha_i(g_{21}) & \alpha_i(g_{22}) & \alpha_i(g_{23}) \\ \alpha_i(g_{31}) & \alpha_i(g_{32}) & \alpha_i(g_{33}) \end{pmatrix} \tag{285}$$

und schreiben $\eta_i := \tilde{\alpha_i}(\eta)$ und $P_i' := \tilde{\alpha_i}(P')$. Für einen Vektor $v = (v_1, v_2, v_3)^T \in R^3$ setzen wir

$$v_i := (\alpha_i(v_1), \alpha_i(v_2), \alpha_i(v_3))^T \in R_i^3. \tag{286}$$

Wie schon mehrfach erwähnt, ist die Bedingung

$$\eta \cdot \gamma \cdot \eta^{-1} \in P' \Longleftrightarrow \forall 1 \leq j \leq s : \; \eta_j \cdot \gamma_j \cdot \eta_j^{-1} \in P_j' \tag{287}$$

für ein $\gamma \in \tilde{C}$ genau dann erfüllt, wenn $v := \eta^{-1} \cdot e_1$ ein Eigenvektor von γ zu einem Eigenwert $\lambda \in R^*$ ist. Wir wählen für γ einen Erzeuger ϵ mit $< \epsilon >= \tilde{C}$, sodass (287) erfüllt ist. Da η^{-1} invertierbar, ist mindestens ein Eintrag von v_j eine Einheit in R_j. Es folgt, dass v_j auch noch nach Reduktion modulo $\mathfrak{p}_j$ Eigenvektor von ϵ ist, für ein beliebiges j. Die Matrix ϵ gehört notwendigerweise zu einem Element $\hat{\epsilon} \in F_{q^3}$, das nicht in F_q liegt. Damit folgt, dass für den Grad d des Minimalpolynoms von $\hat{\epsilon}$ gilt:

$$1 < d \leq 3. \tag{288}$$

Da $F_{q^2} \not\subseteq F_{q^3}$, folgt $d = 3$. Dies impliziert jedoch, dass das charakteristische Polynom χ_ϵ von ϵ irreduzibel über F_q vom Grad drei ist. Aus der Tatsache, dass ϵ Eigenvektoren über $R_j/\mathfrak{p}_j \cong F_{q^{d_j}}$ hat, folgt, dass notwendig alle d_j durch drei teilbar sein müssen:

$$\eta \cdot \epsilon \cdot \eta^{-1} \in P' \Longrightarrow \forall j : d_j \equiv 0 \; (\bmod 3). \tag{289}$$

Falls also ein i existiert, sodass d_i nicht durch drei teilbar ist, so sind alle elliptischen Punkte unverzweigt. Falls jedoch die rechte Seite von (289) erfüllt ist, so tritt elliptische Verzweigung auf, wie der folgende Satz zeigt.

Satz 3. *Es sei $N \in A$ nichtkonstant und normiert mit Primfaktorisierung*

$$N = \prod_{j=1}^{s} p_j^{r_j}. \tag{290}$$

Setze $\omega_0(N) := 1$, falls alle $d_j := \deg(p_j)$ durch drei teilbar sind; ansonsten setze $\omega_0(N) := 0$. Mit dieser Notation gilt:

$$\mathfrak{R}_0(N) = \sum_{\eta \in G/C} |P \cap {}^{\eta}C| - 1 = \omega_0(N) \cdot 3^s \cdot |P/C| \cdot (q^2 + q). \tag{291}$$

Beweis. Angenommen, alle d_j sind durch drei teilbar. Wir müssen zeigen, dass dann gilt:

$$\mathfrak{R}_0(N) = 3^s \cdot |P/C| \cdot (q^2 + q). \tag{292}$$

Es sei ϵ ein Erzeuger von $\tilde{C}$ und $\eta \in \tilde{G}$. Die Bedingung (287) ist für $\gamma \in \tilde{C}$ und η wie oben genau dann erfüllt, wenn die erste Spalte von η^{-1} ein Eigenvektor von γ ist. Da $\tilde{C}$ zyklisch ist mit Erzeuger ϵ, folgt jedoch, dass die Eigenvektoren von γ genau die Eigenvektoren von ϵ sind. Damit ist (287) für ein beliebiges γ genau dann erfüllt, wenn (287) für ϵ erfüllt ist. Damit dies der Fall ist, müssen wir η so wählen, dass $v := \eta^{-1} \cdot e_1$ ein Eigenvektor von ϵ ist. Nach Bemerkung 2, Teil iv) (siehe Seite 9) gilt jedoch:

$$\eta \cdot \epsilon \cdot \eta^{-1} \in P' \Longleftrightarrow \forall j : \ \eta_j \cdot \epsilon \cdot \eta_j^{-1} \in P'_j. \tag{293}$$

Da alle d_j durch drei teilbar sind, gibt es nach dem Lemma von Nakayama über jedem R_j genau drei Eigenrichtungen von ϵ. Diese setzen sich nach Proposition 1 zu genau 3^s verschiedenen Eigenrichtungen über R zusammen. Wir erhalten also für die Anzahl der Möglichkeiten für v den Wert

$$3^s \cdot |R^*|. \tag{294}$$

Die übrigen beiden Spalten müssen so gewählt werden, dass die Determinante der resultierenden Matrix in F_q^* liegt. Wir müssen also die Anzahl aller Matrizen in $\tilde{G}$ finden mit fester erster Spalte. Diese Anzahl hängt aber gar nicht davon ab, welchen Vektor man als erste Spalte fixiert, wie eine direkte kombinatorische Überlegung zeigt. Wir können uns zur Wahl der übrigen beiden Spalten von η^{-1} also genauso gut den Standardbasisvektor e_1 als fixierte erste Spalte denken. Dann gibt es für die Wahl der übrigen beiden Spalten von η^{-1} nach Definition von $\tilde{P}$ also noch genau $\frac{|\tilde{P}|}{|R^*|}$ viele Möglichkeiten. Damit erhalten wir:

$$|\{\eta \in \tilde{G}/\tilde{C} \mid \eta \cdot \epsilon \cdot \eta^{-1} \in \tilde{P}\}| = \frac{3^s \cdot |R^*| \cdot \frac{|\tilde{P}|}{|R^*|}}{|\tilde{C}|} = 3^s \cdot \frac{|\tilde{P}|}{|\tilde{C}|} = 3^s \cdot \frac{|P|}{|C|}. \tag{295}$$

Wir schließen:

$$\mathfrak{R}_0(N) = \sum_{\eta \in G/C} |P \cap {}^{\eta}C| - 1 = \sum_{\eta \in \tilde{G}/\tilde{C}} \frac{|P' \cap {}^{\eta}\tilde{C}|}{q-1} - 1 \tag{296}$$

$$= 3^s \cdot \frac{|P|}{|C|} \cdot (\frac{q^3-1}{q-1} - 1) = 3^s \cdot \frac{|P|}{|C|} \cdot (q^2+q). \tag{297}$$

Der Ausdruck $\frac{q^3-1}{q-1} - 1 = q^2 + q$ im letzten Faktor kommt daher, dass bei gegebenem η die Bedingung (287) für ein $\gamma \in \tilde{C}$ genau dann erfüllt ist, wenn (287) für den Erzeuger ϵ erfüllt ist. Existiert ein i, sodass d_i nicht durch drei teilbar ist, so wissen wir nach (289) bereits, dass dann jeder elliptische Punkt unverzweigt ist. Damit ist der Beweis beendet. □

Wir haben nun alle Hilfsmittel beisammen, um eine explizite Formel für $g(X_0(N))$ zu geben.

4.5 Die Formel für $g(X_0(N))$

Mit den Ergebnissen und Bezeichnungen aus Abschnitt 4.3 und Abschnitt 4.4 kommen wir nun direkt zum Hauptresultat der vorliegenden Arbeit.

Satz 4. *Es sei $N \in A$ nichtkonstant und normiert mit Primfaktorisierung*

$$N = \prod_{j=1}^{s} p_j^{r_j}. \tag{298}$$

Es bezeichne d_j den Grad von p_j und die Größen μ_j, ν_j und $|\tilde{Y}_j|$ seien für $1 \leq j \leq s$ definiert wie in Satz 2:

$$\mu_j := q^{2 \cdot d_j \cdot (2 \cdot r_j - \lfloor \frac{r_j}{2} \rfloor - 1)} + (q^{2 \cdot d_j} - 1) \cdot q^{d_j \cdot (3 \cdot r_j - 2)} \cdot \lfloor \frac{r_j}{2} \rfloor - |R_j|^2, \tag{299}$$

$$\nu_j := (|\mathbb{P}^2(R_j)| - |R_j|^2) \cdot |R_j| + n_{j0} \cdot |R_j| + |R_j|^2. \tag{300}$$

Hierbei bezeichnet n_{j0} wieder die Anzahl aller Elemente aus $RS_1(R_j)$ von Höhe null, im Sinne von Definition 6. Weiter setzen wir gemäß (173)

$$|\tilde{Y}_j| = 2 \cdot |R_j^*| \cdot (q^{2 \cdot d_j} - q^{d_j}) \cdot q^{2 \cdot d_j \cdot (r_j - 1)} \cdot q^{2 \cdot d_j \cdot r_j}. \tag{301}$$

Mit S_0 bezeichnen wir die Menge aller Indizes j, für die d_j gerade ist. Die Menge der übrigen Indizes heiße S_1 und ω_0 sei definiert wie in Satz 3:

$$\omega_0(N) := \begin{cases} 1, \ \forall i : \deg(p_i) \equiv 0 \ mod 3 \\ 0, \ \exists i : \deg(p_i)^2 \equiv 1 \ mod 3 \end{cases}. \tag{302}$$

Mit diesen Bezeichnungen erhalten wir für die Eulercharakteristik $\chi(X_0(N))$ der Kurve $X_0(N)$ die folgende Formel:

$$|P| \cdot \chi(X_0(N)) \tag{303}$$

$$= |Y| \cdot \left(2 \cdot \prod_{j=1}^{s} (\nu_j + \mu_j) + (q-2) \cdot \prod_{j=1}^{s} \nu_j \right) - 2 \cdot |G/G_\infty| \tag{304}$$

$$+ \frac{q \cdot \prod_{j \in S_1} (|P_j| \cdot |R_j|) \cdot \prod_{j \in S_0} \left(|P_j| \cdot (2 \cdot |R_j^*| + |R_j|) + |\tilde{Y}_j| \cdot (|\mathbb{P}^2(R_j)| - |R_j|^2) \right)}{(q+1) \cdot |R|} \tag{305}$$

$$+ \chi(X(N)) + \omega_0(N) \cdot 3^s \cdot |P/C| \cdot (q^2 + q). \tag{306}$$

Wegen $2 \cdot g(X_0(N)) = 2 - \chi(X_0(N))$ erhalten wir damit wie behauptet eine explizite Formel für $g(X_0(N))$.

Beweis. Der Satz ist eine unmittelbare Konsequenz aus der Riemann-Hurwitz-Formel und den Sätzen 2 und 3. □

Bemerkung 12. *Wie die obige Formel zeigt, hängt auch das Geschlecht der Kurve $X_0(N)$ nicht von der genauen Gestalt der jeweiligen Primteiler von N ab; es kommt lediglich auf deren Grade d_i und deren Multiplizitäten r_i in N an. Die Situation ist also analog zur Kurve $X(N)$. Betrachten wir q als Variable, so folgt aus Satz 4 außerdem sofort, dass bei fixierten Parametern d_i, r_i für $1 \leq i \leq s$ die Eulercharakteristik $\chi(q) := \chi(X_0(N)) \in \mathbb{Q}(q)$ eine rationale Funktion in q ist. Eine genauere Betrachtung der rechten Seite zeigt, dass wir diese in jedem Fall in der Form $a + \frac{b}{c}$ schreiben können, wobei $a, b, c \in \mathbb{Z}[q]$. Dies liegt daran, dass alle auftretenden Nenner durch normierte polynomiale Ausdrücke in q mit ganzzahligen Koeffizienten gegeben sind, und daran, dass die Zähler ebenfalls alle Koeffizienten in $\mathbb{Z}$ haben. Da auch $|P|$ durch einen normierten polynomialen Ausdruck in q mit Koeffizienten in $\mathbb{Z}$ gegeben ist, können wir aber auch $\chi(q) = \tilde{a} + \frac{\tilde{b}}{\tilde{c}}$ schreiben, wobei $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}[q]$ und $\deg(\tilde{b}) < \deg(\tilde{c})$. Wähle nun eine natürliche Zahl K, sodass für alle Primzahlpotenzen $q > K$ stets s paarweise verschiedene irreduzible Polynome $p_i \in F_q[T]$ existieren mit $\deg(p_i) = d_i$. Für alle $q > K$ gilt dann aber nach Konstruktion von χ schon automatisch $\chi(q) \in \mathbb{Z}$. Da $\deg(\bar{b}) < \deg(\bar{c})$ können wir als nächstes eine natürliche Zahl K' wählen, sodass $|\bar{b}(x)| < |\bar{c}(x)|$ für alle $x > K'$. Das heißt, für alle Primzahlpotenzen $q > \max(K, K')$ gilt notwendig $\bar{b}(q) = 0$. Da $\bar{b}$ ein Polynom ist, folgt damit aber $\bar{b} = 0$. Dies zeigt, dass $\chi(q)$ sogar ein Polynom in q mit ganzzahligen Koeffizienten ist.*

Hiermit beenden wir den vierten Abschnitt. In Abschnitt 5 wollen wir nun einige Anwendungen und Folgerungen aus unseren Resultaten geben.

5 Folgerungen und Anwendungen

Wir wollen in diesem Abschnitt zunächst beschreiben, inwieweit sich die Formel in Satz 4 vereinfacht, wenn wir zusätzliche Forderungen an N stellen. Das Polynom $N \in A$ soll hierbei wieder normiert und nichtkonstant sein mit Primfaktorisierung $N = \prod_{j=1}^{s} p_j^{r_j}$. Der Grad von p_j heiße wieder d_j. Wir beginnen mit dem folgenden Korollar:

Korollar 1. *Es sei $N = \prod_{j=1}^{s} p_j^{r_j}$ die Primfaktorisierung von N, wobei für $1 \leq j \leq s$ das Polynom p_j den Grad d_j haben soll. Dann gilt mit den gleichen Bezeichnungen wie in Satz 2 und Satz 3:*

a) Falls N quadratfrei, dann gilt:

$$\chi(X_0(N)) = \frac{|Y|}{|P|} \cdot q \cdot \prod_{j=1}^{s} \nu_j - 2 \cdot \frac{|G/G_\infty|}{|P|} + \omega_0(N) \cdot 3^s \cdot \frac{q^2+q}{|C|} + \frac{\chi(X(N))}{|P|} \tag{307}$$

$$+ \frac{q \cdot \prod_{j \in S_1} (|P_j| \cdot |R_j|) \cdot \prod_{j \in S_0} \Big(|P_j| \cdot (2 \cdot |R_j^*| + |R_j|) + |\tilde{Y}_j| \cdot (|\mathbb{P}^2(R_j)| - |R_j|^2) \Big)}{|P| \cdot (q+1) \cdot |R|} \tag{308}$$

$$= \frac{q}{q+1} \cdot 3^{|S_0|} + \frac{q}{q^2-1} \cdot \prod_{j=1}^{s} (q^{d_j}+2) + \omega_0(N) \cdot 3^s \cdot \frac{q^2+q}{q^2+q+1} - \frac{(q+2) \cdot |\mathbb{P}^2(R)|}{(q^2-1) \cdot (q^2+q+1)}. \tag{309}$$

b) Falls alle d_j ungerade sind, dann gilt:

$$\chi(X_0(N)) = \frac{2 \cdot \prod_{j=1}^{s} (\nu_j + \mu_j) + (q-2) \cdot \prod_{j=1}^{s} \nu_j - 2 \cdot |\mathbb{P}^2(R)|}{|G_\infty|} \tag{310}$$

$$+ \frac{q}{q+1} + \frac{\chi(X(N))}{|P|} + \frac{\omega_0(N) \cdot 3^s \cdot (q^2+q)}{|C|}. \tag{311}$$

c) Falls N quadratfrei und alle d_j ungerade, dann erhalten wir:

$$\chi(X_0(N)) = \frac{q}{q+1} + \frac{q}{q^2-1} \cdot \prod_{j=1}^{s} (q^{d_j}+2) + \omega_0(N) \cdot 3^s \cdot \frac{q^2+q}{q^2+q+1} - \frac{(q+2) \cdot |\mathbb{P}^2(R)|}{(q^2-1) \cdot (q^2+q+1)}. \tag{312}$$

d) Falls $0 < \deg(N) \leq 2$, dann gilt $\chi(X_0(N)) = 2$ und damit $g(X_0(N)) = 0$.

Beweis. Die Aussagen folgen alle mehr oder weniger direkt aus Satz 4 und aus dem Beweis von Proposition 7. Wir bemerken hierzu, dass die Quadratfreiheit von N gleichbedeutend damit ist, dass $r_i = 1$ für alle $1 \leq i \leq s$. Damit gilt:

$$\sum_{i=1}^{s} \Big(\prod_{j=1}^{i-1} \nu_j \cdot \mu_i \cdot \prod_{j=i+1}^{s} (\nu_j + \mu_j) \Big) = \prod_{j=1}^{s} (\nu_j + \mu_j) - \prod_{j=1}^{s} \nu_j = 0. \tag{313}$$

Eine genauere Betrachtung und insbesondere eine Herleitung der jeweils letzten Gleichheitszeichen im quadratfreien Fall ist in Bemerkung 14 auf Seite 55-56 zu finden. Man beachte außerdem, dass es wegen $\deg(N) = \sum_{i=1}^{s} d_i \cdot r_i$ für die Bedingung $0 < \deg(N) \leq 2$ nur endlich viele Möglichkeiten für die Parameter d_i, r_i gibt, sodass die Behauptung in d) direkt aus Satz 4 durch Einsetzen folgt. □

Bemerkung 12 zeigt, dass $\chi(X_0(N))$ bei gegebenen Parametern d_j, r_j ($1 \leq j \leq s$) ein Polynom mit ganzzahligen Koeffizienten in q ist. Damit folgt aber, dass auch $g(X_0(N)) \in \frac{\mathbb{Z}}{2}[q] \subset \mathbb{Q}[q]$ ein Polynom ist. Wir wollen nun im folgenden Korollar den Grad dieses Polynoms bestimmen. Dazu erinnern wir noch einmal daran, dass es für alle $s \in \mathbb{N}$ und für jede Wahl von Parametern $d_j \in \mathbb{N}$ bekanntlich eine Zahl $K_{s,d} \in \mathbb{N}$ gibt, sodass für alle Primzahlpotenzen $q > K_{s,d}$ stets s verschiedene irreduzible Polynome $p_{j,q} \in F_q[T]$ existieren mit $\deg(p_{j,q}) = d_j$. Dieses $K_{s,d}$ hängt im allgemeinen von s und den Daten d_j ab.

Korollar 2. *Es sei $s \in \mathbb{N}$ und für $1 \leq j \leq s$ seien feste Parameter $d_j, r_j \in \mathbb{N}$ gegeben mit $\sum_{j=1}^{s} d_j \cdot r_j \geq 3$. Für alle hinreichend großen q definieren wir $N_q := \prod_{j=1}^{s} p_{j,q}^{r_j}$, wobei $p_{j,q} \in F_q[T]$ normiert und irreduzibel von Grad d_j sei. Weiter bezeichnen wir mit $f \in \mathbb{Q}[T]$ den polynomialen Ausdruck, dessen Auswertung in q gerade gleich $|G(N_q)|$ ist für alle q wie oben; $h \in \mathbb{Q}[T]$ sei das Polynom mit $h(q) = g(X_0(N_q))$ für alle q wie oben. Letztlich sei $k \in \mathbb{Q}[T]$ das Polynom mit $k(q) = |P(N_q)|$ für alle oben betrachteten q. Dann gilt:*

$$\deg(h) = \deg(f) - 3 - \deg(k) = 2 \cdot \sum_{i=1}^{s} d_i \cdot r_i - 3 = 2 \cdot \deg(N) - 3. \tag{314}$$

Beweis. Es bezeichne $\tilde{h}$ das Polynom mit rationalen Koeffizienten, dessen Auswertung für alle $q > K_{s,d}$ gerade gleich $\chi(X_0(N_q))$ ist. Den Grad von $\tilde{h}$ können wir mit Satz 4 bestimmen und wegen $g(X_0(N)) = \frac{2-\chi(X_0(N))}{2}$ und $g(X_0(N)) \neq 0$ gilt $\deg(\tilde{h}) = \deg(h)$. Der dominante Term in der Formel für $|P(N_q)| \cdot \chi(X_0(N_q))$ aus Satz 4 ist aber gerade $\chi(X(N_q))$, wie ein Vergleich mit den lokalen Größen zeigt. Eine kurze Rechnung zusammen mit Satz 1 liefert nun, dass

$$\deg(\tilde{h}) = \deg(f) - 3 - \deg(k). \tag{315}$$

Damit folgt das erste Gleichheitszeichen. Das zweite folgt, indem man $|G(N_q)|$ beziehungsweise $|P(N_q)|$ betrachtet und dort jeweils den Grad in q abliest (siehe Bemerkung 9 auf Seite 18-19). □

Bemerkung 13. *Falls $\sum_{j=1}^{s} d_j \cdot r_j \leq 2$, dann ist nach Satz 4 das Geschlecht $g(X_0(N_q)) = 0$ für alle hinreichend großen q und folglich ist dann das Polynom h aus obigem Korollar das Nullpolynom. In diesem Fall gilt nach Konvention $\deg(h) = -\infty$. Man vergleiche Korollar 2 auch mit Korollar 11.17 in [Gek14].*

Wir wollen nun für eine Kurve $X_0(N)$ eine Primstelle $\mathfrak{q}$ in A des Grades eins betrachten, für die gilt $\mathfrak{q} \nmid N$. Die bezüglich $\mathfrak{q}$ reduzierte Kurve $\overline{X_0(N)}$ sei definiert wie in [Gek14] Abschnitt 10.3; wir bemerken, dass $g(\overline{X_0(N)}) = g(X_0(N))$ und dass $\overline{X_0(N)}$ über dem Körper F_q definiert ist und eine nichtgaloissche Überlagerung von $\overline{X(1)} \cong \mathbb{P}^1(F_q)$ liefert, siehe 10.3.1 in [Gek14]. Proposition 10.4 in [Gek14] liefert weiterhin, dass alle elliptischen Punkte (diejenigen, die über $\mathfrak{j} = 0$ liegen) von $\overline{X_0(N)}$ rational über F_{q^3} sind. Unter Verwendung der

ermittelten Verzweigungsdaten ist es nicht besonders schwierig zu zeigen, dass für die Anzahl $E(N)$ der elliptischen Punkte auf $\overline{X_0(N)}$ gilt:

$$E(N) = \begin{cases} \frac{|\mathbb{P}^2(R(N))|+3^s\cdot(q^2+q)}{q^2+q+1}, \ \forall i : d_i \equiv 0 \bmod 3 \\ \frac{|\mathbb{P}^2(R(N))|}{q^2+q+1}, \ sonst \end{cases} . \tag{316}$$

Um unser nächstes Korollar formulieren zu können, benötigen wir noch eine letzte Definition:

Definition 7. Es sei $(X_i)_{i\in\mathbb{N}}$ eine Folge algebraischer Kurven, definiert über dem Körper F_q, sodass $\lim_{i\to\infty} \ g(X_i) = \infty$. Wir bezeichnen die Anzahl der F_q-rationalen Punkte von X_i mit $X_i(F_q)$. Gilt dann

$$\limsup_{i\to\infty} \ \frac{X_i(F_q)}{g(X_i)} > 0, \tag{317}$$

so heißt die Folge $(X_i)_{i\in\mathbb{N}}$ *asymptotisch gut.*

Damit erhalten wir das folgende Korollar, das im Prinzip ein Spezialfall von Theorem C in [Gek14] ist:

Korollar 3. *i) Es sei $N \in A$ normiert und nichtkonstant mit Primfaktorisierung $N = \prod_{j=1}^{s} p_j^{r_j}$. Weiter nehmen wir die Existenz einer Primstelle des Grades eins $\mathfrak{q}$ in A an mit $\mathfrak{q} \nmid N$. Es bezeichne $\overline{X_0(N)}$ die an der Stelle $\mathfrak{q}$ reduzierte Kurve, siehe 10.3 in [Gek14]. Dann gilt mit den Größen $\mathfrak{R}_\infty(N)$ und $\mathfrak{R}_0(N)$, $\omega_0(N)$ aus Satz 2 beziehungsweise Satz 3:*

$$\frac{|\{a \in \overline{X_0(N)} \mid a \text{ ist rational über } F_{q^3}\}|}{g(\overline{X_0(N)})} \tag{318}$$

$$\geq \frac{|\mathbb{P}^2(R(N))| + \omega_0(N)\cdot 3^s\cdot(q^2+q)}{(1+\frac{1}{2}\cdot\frac{|\mathbb{P}^2(R(N))|\cdot(q+2)}{(q^2-1)\cdot(q^2+q+1)} - \frac{\mathfrak{R}_\infty(N)+\mathfrak{R}_0(N)+2\cdot\frac{|G(N)|}{|G_\infty(N)|}}{2\cdot|P(N)|})\cdot(q^2+q+1)}. \tag{319}$$

ii) Gegeben seien nichtkonstante, normierte Polynome N_i mit Primfaktorisierung $N_i = \prod_{j=1}^{s_i} p_{ij}^{r_{ij}}$, sodass $\lim_{i\to\infty} \deg(N_i) = \lim_{i\to\infty} \sum_{j=1}^{s_i} d_{ij}\cdot r_{ij} = \infty$. Es gebe eine Primstelle des Grades eins $\mathfrak{q}$ in A mit $\mathfrak{q} \nmid N_i$ für alle i. Es bezeichne wieder $\overline{X_0(N_i)}$ die an der Stelle $\mathfrak{q}$ reduzierte Kurve, siehe 10.3 in [Gek14]. Dann gilt:

$$\limsup_{i\to\infty} \ \frac{|\{a \in \overline{X_0(N_i)} \mid a \text{ ist rational über } F_{q^3}\}|}{g(\overline{X_0(N_i)})} \tag{320}$$

$$\geq 2\cdot\frac{q^2-1}{q+2} > 0. \tag{321}$$

Insbesondere ist die Folge $(\overline{X_0(N_i)})_{i\in\mathbb{N}}$ asymptotisch gut.

Beweis. i) Nach der Riemann-Hurwitz-Formel haben wir:

$$\chi(X(N)) = |P(N)| \cdot \chi(X_0(N)) - \mathfrak{R}_\infty(N) - \mathfrak{R}_0(N). \tag{322}$$

In Kapitel 3 haben wir gesehen, dass für die Eulerzahl von $X(N)$ folgendes gilt:

$$\chi(X(N)) = 2 \cdot |G(N)| - \frac{|G(N)|}{|G_\infty(N)|} \cdot (|G_\infty(N)| + |U(N)| - 2) - |G(N)| \cdot \frac{q^2+q}{q^2+q+1} \tag{323}$$

$$= |G(N)| + 2 \cdot \frac{|G(N)|}{|G_\infty(N)|} - \frac{|G(N)| \cdot |U(N)|}{|G_\infty(N)|} - |G(N)| \cdot \frac{q^2+q}{q^2+q+1}. \tag{324}$$

Damit folgt:

$$\frac{|G(N)|}{|P(N)|} \cdot \left(1 - \frac{|U(N)|}{|G_\infty(N)|} - \frac{q^2+q}{q^2+q+1}\right) = \chi(X_0(N)) - \frac{\mathfrak{R}_\infty(N) + 2 \cdot \frac{|G(N)|}{|G_\infty(N)|} + \mathfrak{R}_0(N)}{|P(N)|}. \tag{325}$$

Für den Faktor auf der linken Seite erhalten wir:

$$1 - \frac{|U(N)|}{|G_\infty(N)|} - \frac{q^2+q}{q^2+q+1} = \frac{1}{q^2+q+1} - \frac{1}{q^2-1} = \frac{1}{q^2+q+1} \cdot (1 - \frac{q^2+q+1}{q^2-1}) \tag{326}$$

$$= \frac{1}{q^2+q+1} \cdot \frac{q^2-1-q^2-q-1}{q^2-1} \tag{327}$$

$$= -\frac{1}{q^2+q+1} \cdot \frac{q+2}{q^2-1}. \tag{328}$$

Damit ergibt sich schließlich

$$\chi(X_0(N)) = -\frac{|\mathbb{P}^2(R(N))|}{q^2+q+1} \cdot \frac{q+2}{q^2-1} + \frac{\mathfrak{R}_\infty(N) + 2 \cdot \frac{|G(N)|}{|G_\infty(N)|} + \mathfrak{R}_0(N)}{|P(N)|}, \tag{329}$$

woraus wir unmittelbar

$$g(\overline{X_0(N)}) = g(X_0(N)) = \frac{2 - \chi(X_0(N))}{2} \tag{330}$$

$$= 1 + \frac{1}{2} \cdot \frac{|\mathbb{P}^2(R(N))|}{q^2+q+1} \cdot \frac{q+2}{q^2-1} - \frac{\mathfrak{R}_\infty(N) + 2 \cdot \frac{|G(N)|}{|G_\infty(N)|} + \mathfrak{R}_0(N)}{2 \cdot |P(N)|} \tag{331}$$

schließen können. Wie oberhalb des Korollars ausgeführt, sind alle elliptischen Punkte von $\overline{X_0(N)}$ rational über F_q^3. Es folgt:

$$\frac{|\{a \in \overline{X_0(N)} \mid a \textit{ ist rational über } F_{q^3}\}|}{g(\overline{X_0(N)})} \geq \frac{E(N)}{g(X_0(N))} \tag{332}$$

$$= \frac{|\mathbb{P}^2(R(N))| + \omega_0(N) \cdot 3^s \cdot (q^2+q)}{g(X_0(N)) \cdot (q^2+q+1)} \tag{333}$$

$$= \frac{|\mathbb{P}^2(R(N))| + \omega_0(N) \cdot 3^s \cdot (q^2+q)}{(1 + \frac{1}{2} \cdot \frac{|\mathbb{P}^2(R(N))| \cdot (q+2)}{(q^2-1) \cdot (q^2+q+1)} - \frac{\mathfrak{R}_\infty(N) + \mathfrak{R}_0(N) + 2 \cdot \frac{|G(N)|}{|G_\infty(N)|}}{2 \cdot |P(N)|}) \cdot (q^2+q+1)}. \tag{334}$$

Das ist aber gerade die erste Aussage.
ii) Nach Satz 2 gilt: $\mathfrak{R}_\infty(N_i) + 2 \cdot \frac{|G(N_i)|}{|G_\infty(N_i)|} > 0$. Ebenso liefert Satz 3 die Ungleichung $\mathfrak{R}_0(N_i) \geq 0$. Damit können wir folgendermaßen abschätzen:

$$\frac{|\mathbb{P}^2(R(N_i))| + \omega_0(N_i) \cdot 3^{s_i} \cdot (q^2+q)}{(1 + \frac{1}{2} \cdot \frac{|\mathbb{P}^2(R(N_i))| \cdot (q+2)}{(q^2-1)\cdot(q^2+q+1)} - \frac{\mathfrak{R}_\infty(N_i)+\mathfrak{R}_0(N_i)+2\cdot\frac{|G(N_i)|}{|G_\infty(N_i)|}}{2\cdot|P(N_i)|}) \cdot (q^2+q+1)} \tag{335}$$

$$\geq \frac{|\mathbb{P}^2(R(N_i))|}{(1 + \frac{1}{2} \cdot \frac{|\mathbb{P}^2(R(N_i))| \cdot (q+2)}{(q^2-1)\cdot(q^2+q+1)}) \cdot (q^2+q+1)}. \tag{336}$$

Bilden wir nun in (336) den Limes für $i \longrightarrow \infty$, so strebt $|\mathbb{P}^2(R(N_i))| \longrightarrow \infty$. Wir erhalten unter Verwendung von Teil i):

$$\limsup_{i\to\infty} \frac{|\{a \in \overline{X_0(N_i)} \mid a \textit{ ist rational über } F_{q^3}\}|}{g(\overline{X_0(N_i)})} \geq 2 \cdot \frac{q^2-1}{q+2}. \tag{337}$$

Dies beendet den Beweis. Wir bemerken, dass die gegebenen Argumente im Wesentlichen auch für Modulkurven vom Typ $X_0^{r,k}(N)$ mit $(r,k) \neq (3,2)$ funktionieren (siehe 12.4 und 12.5 in [Gek14]). □

In der nächsten Bemerkung wollen wir noch etwas zur Qualität der Abschätzung aus Teil ii) des obigen Korollars sagen.

Bemerkung 14. *In der Situation von Teil ii) des obigen Korollars gelte zusätzlich, dass alle $r_{ij} = 1$ seien. Beachte, dass dies die Quadratfreiheit aller N_i impliziert. Dann gilt:*

$$\frac{q \cdot \prod_{j=1}^{s_i} \nu_j}{|G_\infty(N_i)|} = \frac{q \cdot \prod_{j=1}^{s_i} \left((q^{d_{ij}}+1)\cdot q^{d_{ij}} + (q^{2\cdot d_{ij}}-1)\cdot q^{d_{ij}} + q^{2\cdot d_{ij}}\right)}{|G_\infty(N_i)|} \tag{338}$$

$$= \frac{q \cdot \prod_{j=1}^{s_i} \left(q^{3\cdot d_{ij}} + 2\cdot q^{2\cdot d_{ij}}\right)}{(q^2-1)\cdot q^{2\cdot\deg(N_i)}} = \frac{q \cdot q^{2\cdot\deg(N_i)} \cdot \prod_{j=1}^{s_i}\left(q^{d_{ij}}+2\right)}{(q^2-1)\cdot q^{2\cdot\deg(N_i)}} \tag{339}$$

$$= \frac{q \cdot \prod_{j=1}^{s_i}\left(q^{d_{ij}}+2\right)}{(q^2-1)} \leq \frac{q\cdot 2^{s_i}\cdot q^{\deg(N_i)}}{q^2-1} \leq \frac{q\cdot(2\cdot q)^{\deg(N_i)}}{q^2-1}. \tag{340}$$

Setzen wir weiter gemäß (173)

$$|\tilde{Y}(N_i)_j| := 2\cdot|R(N_i)^*_j| \cdot (q^{2\cdot d_{ij}} - q^{d_{ij}}) \cdot q^{2\cdot d_{ij}\cdot(r_{ij}-1)} \cdot q^{2\cdot d_{ij}\cdot r_{ij}}, \tag{341}$$

so folgt wegen

$$|P(N_i)_j| \cdot |R(N_i)_j| = q^{4\cdot d_{ij}} \cdot (q^{2\cdot d_{ij}}-1)\cdot(q^{d_{ij}}-1), \tag{342}$$

$$|P(N_i)_j| \cdot (2\cdot|R(N_i)^*_j| + |R(N_i)_j|) = q^{3\cdot d_{ij}} \cdot (q^{2\cdot d_{ij}}-1)\cdot(q^{d_{ij}}-1)\cdot(3\cdot q^{d_{ij}}-2), \tag{343}$$

$$|\tilde{Y}(N_i)_j| \cdot (|\mathbb{P}^2(R(N_i)_j))| - |R(N_i)_j|^2) = 2\cdot q^{3\cdot d_{ij}} \cdot (q^{2\cdot d_{ij}}-1)\cdot(q^{d_{ij}}-1) \tag{344}$$

nach Satz 2 die Beziehung

$$\frac{\mathfrak{R}_\infty(N_i) + 2\cdot\frac{|G(N_i)|}{|G_\infty(N_i)|}}{|P(N_i)|} = 3^{|S_0(N_i)|} \cdot \frac{q}{q+1} + \frac{q\cdot\prod_{j=1}^{s_i}\left(q^{d_{ij}}+2\right)}{(q^2-1)} \tag{345}$$

$$\leq 3^{\deg(N_i)} \cdot \frac{q}{q+1} + \frac{q\cdot(2\cdot q)^{\deg(N_i)}}{q^2-1}. \tag{346}$$

Wegen $3^{s_i} \cdot \frac{q^2+q}{q^2+q+1} \leq 3^{\deg(N_i)} \cdot \frac{q^2+q}{q^2+q+1}$ *erhalten wir damit aber nach Satz 3 für* $q \geq 4$*:*

$$\lim_{i\to\infty} \frac{|P(N_i)|}{|G(N_i)|} \cdot \frac{\mathfrak{R}_\infty(N_i) + 2 \cdot \frac{|G(N_i)|}{|G_\infty(N_i)|} + \mathfrak{R}_0(N_i)}{|P(N_i)|} = 0. \tag{347}$$

Das heißt, für alle $q \geq 4$ *und alle Folgen* $(N_i)_{i\in\mathbb{N}}$ *von quadratfreien, normierten Polynomen* N_i *hängt die Qualität der Abschätzung*

$$\limsup_{i\to\infty} \frac{|\{a \in \overline{X_0(N_i)} \mid a \text{ ist rational über } F_{q^3}\}|}{g(\overline{X_0(N_i)})} \geq 2 \cdot \frac{q^2-1}{q+2} \tag{348}$$

in gewissem Sinne also nur von der Qualität der Ungleichung

$$|\{a \in \overline{X_0(N_i)} \mid a \text{ ist rational über } F_{q^3}\}| \geq E(N_i) \tag{349}$$

ab. Mit anderen Worten:

$$\lim_{i\to\infty} \frac{E(N_i)}{g(\overline{X_0(N_i)})} = 2 \cdot \frac{q^2-1}{q+2}. \tag{350}$$

Beachte hierzu, dass $\frac{|P(N_i)|}{|G(N_i)|} = \frac{1}{|\mathbb{P}^2(R(N_i))|} \leq \frac{1}{q^{2\cdot\deg(N_i)}}$ *und dass*

$$\frac{|\mathbb{P}^2(R(N_i))| + \omega_0(N_i) \cdot 3^{s_i} \cdot (q^2+q)}{(1 + \frac{1}{2} \cdot \frac{|\mathbb{P}^2(R(N_i))|\cdot(q+2)}{(q^2-1)\cdot(q^2+q+1)} - \frac{\mathfrak{R}_\infty(N_i)+\mathfrak{R}_0(N_i)+2\cdot\frac{|G(N_i)|}{|G_\infty(N_i)|}}{2\cdot|P(N_i)|}) \cdot (q^2+q+1)} \tag{351}$$

$$= \frac{1 + \frac{\omega_0(N_i)\cdot 3^{s_i}\cdot(q^2+q)}{|\mathbb{P}^2(R(N_i))|}}{(\frac{1}{|\mathbb{P}^2(R(N_i))|} + \frac{1}{2} \cdot \frac{(q+2)}{(q^2-1)\cdot(q^2+q+1)} - \frac{\mathfrak{R}_\infty(N_i)+\mathfrak{R}_0(N_i)+2\cdot\frac{|G(N_i)|}{|G_\infty(N_i)|}}{2\cdot|P(N_i)|\cdot|\mathbb{P}^2(R(N_i))|}) \cdot (q^2+q+1)}. \tag{352}$$

Wir wollen diesen Abschnitt und damit auch diese Arbeit mit einigen Tafeln beenden, die die in dieser Arbeit gewonnenen Ergebnisse für einige Beispielkurven $X_0(N)$ illustrieren.

Ist $N \in A = F_q[T]$ nichtkonstant und normiert mit Primfaktorisierung $N = \prod_{j=1}^{s} p_j^{r_j}$, wobei p_j Grad d_j habe, so setzen wir $d := (d_1, \ldots, d_s)$ und $r := (r_1, \ldots, r_s)$. Wir haben gesehen, dass alle für diese Arbeit relevanten Daten im wesentlichen durch die Signatur $Sig(N) = [q, d, r]$, das heißt durch q, d und r bestimmt sind. Wir wollen daher nun als erstes eine Tabelle mit den Signaturen geben, die zu einem N mit $g(X_0(N)) \leq 100$ gehören. Eine genaue Betrachtung der Formel aus Satz 4 für ein fixiertes q liefert, dass wir uns hierbei auf Polynome N des Grades höchstens fünf beschränken können. Um die gewünschten Daten zu gewinnen, implementiere man einfach die Formel aus Satz 4 in einem Computeralgebrasystem und betrachte mögliche Partitionen der jeweiligen betrachteten Grade.

Wir stellen nun alle oben betrachteten Signaturen zusammen mit dem jeweiligen Geschlecht der zugehörigen Kurve $X_0(N)$ sowie der Anzahl der elliptischen Punkte auf der entsprechenden reduzierten Kurve $\overline{X_0(N)}$ in einer Tabelle zusammen. Da die reduzierte Kurve im obigen Sinne jedoch nur gebildet werden kann, falls eine Primstelle $\mathfrak{q}$ vom Grad eins in $A = F_q[T]$ existiert, die N nicht teilt, lassen wir den entsprechenden Eintrag in der Tabelle leer, falls kein solches $\mathfrak{q}$ existiert. Es sei außerdem noch einmal daran erinnert, dass alle elliptischen Punkte auf $\overline{X_0(N)}$ stets rational über F_{q^3} sind. Die rechte Spalte der folgenden Tabelle gibt also eine untere Abschätzung für die Zahl der F_{q^3}-rationalen Punkte auf $\overline{X_0(N)}$.

q	d	r	$g(X_0(N))$	$\lvert\{$ elliptische Punkte auf $\overline{X_0(N)}\ \}\rvert$
2	[3]	[1]	3	13
2	[1]	[3]	4	16
2	[2]	[2]	20	48
2	[4]	[1]	20	39
2	[1]	[4]	26	64
2	[5]	[1]	90	151
2	[1, 2]	[1, 1]	6	21
2	[1, 1]	[1, 2]	6	
2	[1, 3]	[1, 1]	36	73
2	[1, 2]	[2, 1]	36	84
2	[1, 1]	[2, 2]	42	
2	[1, 1]	[1, 3]	46	
2	[1, 1, 2]	[1, 1, 1]	66	
3	[3]	[1]	12	61
3	[1]	[3]	15	81
3	[2, 1]	[1, 1]	18	91
3	[1, 1]	[1, 2]	20	117
3	[1, 1, 1]	[1, 1, 1]	30	
4	[3]	[1]	30	201
4	[1]	[3]	36	256
4	[1, 2]	[1, 1]	40	273
4	[1, 1]	[1, 2]	45	336
4	[1, 1, 1]	[1, 1, 1]	60	441
5	[3]	[1]	60	511
5	[1]	[3]	70	625
5	[1, 2]	[1, 1]	75	651
5	[1, 1]	[1, 2]	84	775

(353)

Bemerkung 15. *Man beachte, dass jedes $N \in A$ automatisch eine Signatur $[q, d, r]$ liefert. Umgekehrt gibt es aber nicht zu jeder Signatur $[q, d, r]$ notwendigerweise ein N, das diese Signatur realisiert. Beispielsweise gibt es kein N mit Signatur $[2, [1, 1, 1], [1, 1, 1]]$, da es über F_2 bekanntlich nur zwei irreduzible*

Polynome vom Grad eins gibt. Der entscheidende Parameter ist hierbei q; wählt man d und r beliebig, so existiert ein $K \in \mathbb{N}$, sodass für alle $q > K$ stets ein N existiert mit Signatur $[q, d, r]$.

Als letztes wollen wir noch eine Tabelle geben, die zeigt, wie das Geschlecht als Polynom in q aussieht bei den in (353) betrachteten Signaturen. Man behalte hierbei Bemerkung 15 im Hinterkopf.

d	r	$g(X_0(N))(q)$
$[3]$	$[1]$	$\frac{1}{2} \cdot (q^3 - q)$
$[1]$	$[3]$	$\frac{1}{2} \cdot (q^3 + q^2 - 2 \cdot q)$
$[2]$	$[2]$	$\frac{1}{2} \cdot (q^5 + q^4 - q^3 + q^2 - 2 \cdot q)$
$[4]$	$[1]$	$\frac{1}{2} \cdot (q^5 + q^4 - 2 \cdot q^3 + 2 \cdot q^2)$
$[1]$	$[4]$	$\frac{1}{2} \cdot (q^5 + 2 \cdot q^4 - 3 \cdot q^2)$
$[5]$	$[1]$	$\frac{1}{2} \cdot (q^7 + q^6 - q^5 + q^4 + 2 \cdot q)$
$[1, 2]$	$[1, 1]$	$\frac{1}{2} \cdot (q^3 + q^2)$
$[1, 1]$	$[1, 2]$	$\frac{1}{2} \cdot (q^3 + 2 \cdot q^2 - q - 2)$
$[1, 3]$	$[1, 1]$	$\frac{1}{2} \cdot (q^5 + 2 \cdot q^4 + q^2 + 2 \cdot q)$
$[1, 2]$	$[2, 1]$	$\frac{1}{2} \cdot (q^5 + 2 \cdot q^4 + q^3 + q^2 - q - 2)$
$[1, 1]$	$[2, 2]$	$\frac{1}{2} \cdot (q^5 + 3 \cdot q^4 + 3 \cdot q^3 - 3 \cdot q^2 - 4)$
$[1, 1]$	$[1, 3]$	$\frac{1}{2} \cdot (q^5 + 3 \cdot q^4 + 3 \cdot q^3 - 5 \cdot q - 2)$
$[1, 1, 2]$	$[1, 1, 1]$	$\frac{1}{2} \cdot (q^5 + 3 \cdot q^4 + 4 \cdot q^3 + 4 \cdot q^2 + 2 \cdot q)$
$[1, 1, 1]$	$[1, 1, 1]$	$\frac{1}{2} \cdot (q^3 + 3 \cdot q^2 + 2 \cdot q)$

(354)

Man beachte, dass für alle Signaturen mit $\sum_{j=1}^{s} d_j \cdot r_j \leq 2$ das Geschlecht stets identisch null ist, weshalb wir solche Signaturen in der obigen Tabelle ausgelassen haben.

Vergleicht man unsere Ergebnisse mit der Datenbank auf der Internetseite www.manypoints.org, so stellt man fest, dass unsere Kurven leider keine neuen Rekordkurven liefern. Wir wollen unsere Betrachtungen jedoch mit der Bemerkung beenden, dass man aus den gegebenen Kurven weitere Kurven konstruieren kann, indem man Quotienten der Kurven nach gewissen Automorphismengruppen betrachtet. Es besteht hierbei eine gewisse Hoffnung, dass man auf diese Weise eventuell doch zu Rekordkurven oder zumindest in Rekordnähe kommen könnte.

Literatur

[Boh14] Bohn, Marius: *Die Geschlechter der Modulkurven zu dünn besetzten Drinfeld-Moduln des Rangs drei: der lokale Fall.* Universität des Saarlandes, Lehrstuhl Prof. Dr. Ernst-Ulrich Gekeler, Saarbrücken, 2014.

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

[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.

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

[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.

[MT07] M.A. Tsfasman, S. Vladut, D. Nagin: *Algebraic Geometric Codes: Basic Notions.* Mathematical Surveys and Monographs Volume 139, American Mathematical Society, USA, 2007.

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