Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern

vorgelegt von
Diplom-Mathematikerin
Katharina Geißler
aus Hanau

Von der Fakultät II - Mathematik- und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation

Berlin 2003
D83

Promotionsausschuß:

Vorsitzender: Prof. Dr. D. Krüger
Berichter: Prof. Dr. M. E. Pohst
Berichter: Prof. Dr. F. Leprévost

Tag der wissenschaftlichen Aussprache: 17. April 2003

Inhaltsverzeichnis

Einleitung

Sei $f(x) \in K[x]$ ein normiertes, irreduzibles und separables Polynom vom Grad n. Ziel dieser Arbeit ist es, einen effizienten Algorithmus zur Berechnung der Galoisgruppe des Polynoms f über verschiedenen Grundkörpern K mit möglichst hohen Polynomgraden zu entwickeln.

Algorithmen zur Berechnung der Galoisgruppe von f sind wichtige Hilfsmittel der konstruktiven Zahlentheorie [70, 12]. Darüber hinaus finden sie beispielsweise Anwendung bei der Auflösbarkeit von Gleichungen durch Radikale [33], der Bestimmung von Eigenschaften des Zerfällungskörpers und der inversen Galoistheorie [44].

Das Problem der Bestimmung der Galoisgruppe führt auf Berechnungen, die Evariste Galois als „impracticables“ (nicht durchführbar) beschreibt und mit deren Ausführung „qu'il ne voudrait charger ni lui ni personne de faire“ (er weder sich selber noch andere Personen beauftragen möchte). Dennoch wird es von Berwick [4] (1929), van der Waerden [83] (1937) und Tschebotarev, Schwerdtfeger [81] (1950) aufgegriffen. Die Ergebnisse van der Waerdens belegen, daß sich das Problem der Galoisgruppenberechnung auf das Problem der Faktorisierung eines Polynoms vom Grad $n!$ mit Koeffizienten in K, welche symmetrische Funktionen der Nullstellen von f sind, reduzieren läßt. Grundsätzlich folgt somit aus der Existenz eines Faktorisierungsalgorithmus auch immer ein Algorithmus zur Galoisgruppenberechnung. Trotzdem ist bis heute kein allgemeiner polynomieller Algorithmus zur Berechnung von Galoisgruppen bekannt.

Erst mit der zunehmenden Leistungsfähigkeit der Computer folgen speziell in den letzten Jahrzehnten zwei effiziente Methoden zur Galoisgruppenberechnung. Diese lassen sich in die absolute Resolventenmethode (Soicher [77], 1981; Soicher, McKay [58], 1985; Mattman, McKay [56], 1997) und die relative Resolventenmethode (Stauduhar [78], 1973), welche auch als Verfahren von Stauduhar bezeichnet wird, unterteilen. Gemeinsam ist beiden Methoden, daß sie die Klassifikation der transitiven Gruppen benötigen, welche bis zum Grad 31 (Hulpke [36]) bekannt ist.

Die absolute Resolventenmethode ist ein allgemeines Verfahren über Körpern,

für die die entsprechende Arithmetik und ein Polynomfaktorisierungsalgorithmus vorhanden sind. Bei diesem Verfahren werden für Rechnungen nur die exakt gegebenen Koeffizienten des Eingabepolynoms, von dem die Galoisgruppe bestimmt werden soll, verwendet, so daß die Korrektheit der Ergebnisse ohne weiteres gewährleistet ist. Nachteilig wirkt sich hier aus, daß selbst für kleine Grade des Eingabepolynoms das absolute Resolventenpolynom, dessen Faktorisierung für die Bestimmung der Galoisgruppe notwendig ist, schon recht hohen Grad hat. An dieser Stelle muß also mit erheblichen Laufzeiten gerechnet werden, weshalb sich dieses symbolische Verfahren für effektive Berechnungen auf Eingabepolynome eines Grads bis maximal acht beschränkt. Ein weiterer Nachteil dieser Methode ist, daß nur der Isomorphietyp der Galoisgruppe, aber keine explizite Operation auf den Nullstellen erhalten wird. Die Kenntnis der Operation der Galoisgruppe auf den Nullstellen ist aber zum Beispiel wichtiger Bestandteil in den oben genannten Algorithmen der inversen Galoistheorie und für die Auflösbarkeit von Gleichungen durch Radikale. Bestehende Implementierungen der absoluten Resolventenmethode findet man in den Computeralgebrasystemen MAPLE [76] für Polynome über $\mathbb{Q}$ und $\mathbb{Q}(t_1, \ldots, t_r)$, $(r \in \mathbb{Z}_{>0})$ bis zum Grad 8, GAP [54] für rationale Polynome bis zum Grad 15 und KASH [38] für Polynome über $\mathbb{Q}$ und $\mathbb{Q}(t)$ bis zum Grad 8.

Im Gegensatz zur absoluten Resolventenmethode werden bei der relativen Resolventenmethode Nullstellen von Resolventen, d.h. Polynomen, deren Zerfällungskörper ein Teilkörper des Zerfällungskörpers von f ist, im Grundkörper gesucht. Die Nullstellen können entweder symbolisch [14, 15] oder mittels Approximationen [19, 22, 23, 29, 30, 78, 88] der Nullstellen von f berechnet werden. Obwohl der symbolische Ansatz attraktiv erscheint, sind zur Durchführung umfangreiche invariantentheoretische Algorithmen und Gröbner-Basen Berechnungen notwendig, so daß er mit den anderen Methoden sowohl in Einfachheit als auch Effizienz nicht konkurrieren kann. Bei der anderen Variante lassen sich die Approximationen der Nullstellen des Polynoms f komplex oder auch p-adisch berechnen. Komplexe Arithmetik führt in der Regel zur Verwendung von sehr hohen Präzisionen, um bewiesene oder auch unbewiesene, aber in der Praxis korrekte Ergebnisse zu erhalten. Deshalb ist es wünschenswert, p-adische Methoden zur Galoisgruppenberechnung zu untersuchen und einzusetzen.

Implementierungen der relativen Resolventenmethode über $\mathbb{Q}$ unter Benutzung komplexer Approximationen wurden durchgeführt zuerst von Stauduhar (1973) bis Grad 7, gefolgt von Geyer (1993) bis Grad 9, dann Eichenlaub und Olivier (1995) bis Grad 11 in PARI [2] und schließlich Geißler (1997) bis Grad 12 in KASH [38]. Andere Grundkörper als $\mathbb{Q}$ wurden nicht berücksichtigt. Die p-adischen Verfahren zur Galoisgruppenberechnung wurden erstmals von Darmon

und Ford [19] (1989) und später von Yokoyama [88] (1997) eingesetzt. Theoretische Arbeiten und Implementierungen, ASIR/RISA [63] bis Grad 8 und Rybowicz, Lenzinger [74] bis Grad 9, beschränken sich bisher aber immer nur auf Polynome kleinen Grads über $\mathbb{Q}$.

Die in dieser Arbeit entwickelten Algorithmen ermöglichen die Berechnung von Galoisgruppen für Polynome bis zum Grad 23 über beliebigen algebraischen Zahlkörpern und Funktionenkörpern über $\mathbb{Q}$ und $\mathbb{F}_q$. Unsere Hauptergebnisse teilen sich grob in drei Bereiche ein.

- Wir erweitern die bisher im wesentlichen nur für $\mathbb{Q}$ existierenden Verfahren auf beliebige algebraische Zahlkörper und Funktionenkörper über $\mathbb{Q}$ und $\mathbb{F}_q$.

- Die absolute Resolventenmethode, relative Resolventenmethode und das Verfahren zur Teilkörperberechnung der betrachteten Körper werden kombiniert, um einen effizienten Algorithmus zu erhalten.

- In der Gruppen- und Invariantentheorie berechnen wir für die Grade 12 bis 23 erstmals die erforderlichen Daten und geben Algorithmen an, mittels derer spezielle, optimierte Invarianten bestimmt werden.

Wir haben diesen Algorithmus für Zahlkörper und rationale Funktionenkörper bis Grad 23 in den Computeralgebrasystemen KASH [38] und MAGMA [5, 16] implementiert. Bisherige effiziente Implementationen zur Galoisgruppenberechnung existierten nur bis Grad 12, wobei allerdings die Korrektheit der berechneten Ergebnisse nicht immer gewährleistet war. Wir gehen auf die genannten Punkte im folgenden etwas näher ein.

Bei der Berechnung der Nullstellen des Ausgangspolynoms verwenden wir p-adische Approximationen. Wie schon erwähnt ist ein entscheidender Teil der relativen Resolventenmethode, Nullstellen von Resolventen im Grundkörper zu bestimmen. Dies stellt ein Problem dar, da wir in unseren Berechnungen nur mit (p-adischen) Approximationen arbeiten. Wir werden im Zahl- und Funktionenkörperfall einen Algorithmus herleiten, der bei Eingabe von p-adischen Approximationen der Nullstellen der Resolvente in Abhängigkeit von der Präzision exakte Nullstellen (falls existent) im Grundkörper rekonstruiert. Zur Realisierung des Rekonstruktionsalgorithmus werden Techniken verwendet, die auf Gittern basieren. Derartige Ansätze wurden in der Literatur für Zahlkörper und Funktionenkörper über endlichen Körper schon untersucht [25, 49, 67, 71]. Mittels einer unterschiedlichen Herangehensweise erhalten wir für diese Körper und auch für Funktionenkörper über $\mathbb{Q}$ alternative Verfahren und Schranken, welche für unseren Fall besonders günstig sind.

Rekonstruktionsalgorithmen bieten eine Fülle von Anwendungen: Bei Polynomfaktorisierungen [25, 67], Irreduzibilitätstests, Berechnung r-ter Wurzeln algebraischer Zahlen [25] und in unserem Fall von besonderer Bedeutung bei der Berechnung von Teilkörpern des Körpers $K(\alpha)$ [42, 43]. So konnte der entwickelte Rekonstruktionsalgorithmus erfolgreich bei der Teilkörperberechnung relativer algebraischer Zahlkörper eingesetzt werden, welche wir ebenfalls im Computeralgebrasystem KASH [38] implementiert haben.

Betrachtet man die Grade $12 \leq n \leq 23$, so stellt sich heraus, daß das ursprüngliche Verfahren von Stauduhar in diesen Bereichen nicht mehr effizient genug ist. Die Schwierigkeiten liegen hierbei im wesentlichen in der erheblichen Anzahl der transitiven Gruppen, der exponentiell wachsenden Ordnung der Gruppen, sowie der Größe der Indizes der S_n bzw. A_n zu den anderen transitiven Gruppen, was sich im Grad der Resolvente wiederspiegelt. Unser Ziel war es daher, für alle auftretenden Probleme Lösungsstrategien zu entwickeln, so daß effektive Galoisgruppenberechnungen auch in diesen Fällen möglich sind.

Eine entscheidende Verbesserung ist die Verwendung von Teilkörpern des Körpers $K(\alpha)$, wobei α eine Nullstelle von f ist. Unter Verwendung dieser Information läßt sich auf Blocksysteme der Galoisgruppe schließen. Somit wird es möglich, die Galoisgruppe in geeignete Kranzprodukte einzubetten und die Einstiegspunkte in der relativen Resolventenmethode variabel zu halten. Handelt es sich bei der Galoisgruppe um eine primitive Gruppe, so stellt die Verwendung von Teilkörpern keine Verbesserung dar. Deshalb sind primitive Gruppen bei dieser Methode algorithmisch schwieriger zu handhaben. Um auch in diesem Fall sehr gute Laufzeiten zu erzielen, präsentieren wir eine Kombination der beiden Resolventenmethoden. Grob gesprochen wird die Galoisgruppe zunächst mit einer heuristischen p-adischen Präzision berechnet, was zu einem unbewiesenen Ergebnis führt, und anschließend mittels der absoluten Resolventenmethode unter Umgehung der Verwendung hoher p-adischer Präzisionen verifiziert. Darüber hinaus läßt sich hier der Frobenius-Automorphismus des zugehörigen p-adischen Körpers gewinnbringend einsetzen, da er Erzeuger einer Untergruppe der Galoisgruppe ist. Durch ihn lassen sich sogenannte verkürzte Nebenklassenrepräsentantensysteme berechnen, die für die zeitkritischen Stellen in der relativen Resolventenmethode enorme Verbesserungen darstellen.

Die Arbeit gliedert sich wie folgt:

Im ersten Kapitel fixieren wir Notationen und stellen die theoretischen Grundlagen für Permutationsgruppen und Galoisgruppen zusammen, die für die folgenden Kapitel benötigt werden. Darüber hinaus werden grundlegende p-adische Algorithmen wie das Newton-Lifting behandelt.

Im zweiten Kapitel kommen wir zur Beschreibung des Verfahrens von Stauduhar. Nach einer Motivation dieser Methode erläutern wir die allgemeine Strategie und liefern Kernsätze für den Algorithmus, der anschließend in einer Übersicht unter Berücksichtigung aller bisher behandelten Aussagen formuliert wird. Abschließend stellen wir die absolute Resolventenmethode vor.

Im dritten und vierten Kapitel leiten wir die p-adischen Algorithmen für das Verfahren von Stauduhar für normierte, irreduzible und separable Polynome über algebraischen Zahl- und Funktionenkörpern über $\mathbb{Q}$ und endlichen Körpern her. Dazu gehören sowohl die Nullstellenberechnung in p-adischen unverzweigten Erweiterungen als auch ein entsprechender Rekonstruktionsalgorithmus. Für letzteren Algorithmus werden neue Schranken bestimmt, um die Korrektheit der Ergebnisse bei der Berechnung der Galoisgruppen zu garantieren. Darüber hinaus vergleichen wir unseren Rekonstruktionsansatz mit Methoden aus der Literatur, wobei hier der Schwerpunkt auf dem Artikel [25] liegt.

Kapitel 5 ist ganz den Erweiterungen des Verfahrens von Stauduhar gewidmet. Wir integrieren Methoden basierend auf Algorithmen zur Teilkörperberechnung, führen verkürzte Nebenklassenrepräsentantensysteme zur Bewältigung großer Gruppenindizes ein und geben einen effizienten Algorithmus zur Berechnung derselben an. Darüber hinaus beschreiben wir die Kombination der beiden Resolventenmethoden, mittels derer die Verwendung großer p-adischer Präzisionen im Verfahren umgangen werden kann, und präsentieren den zugehörigen Algorithmus für die betrachteten Grundkörper, wie er in unserer Implementierung für primitive Gruppen angewendet wird. Abschließend geben wir das Verfahren inklusive aller Erweiterungen nochmals in einer Übersicht an, unter spezieller Berücksichtigung der Wahl des Primideals, bezüglich dessen die p-adischen Berechnungen durchgeführt werden.

Im sechsten Kapitel beschreiben wir Berechnungsmethoden der Daten, die für das Verfahren von Stauduhar notwendig sind. Dabei gehen wir ausführlich auf die Konstruktion und Berechnung von G-relativen H-invarianten Polynomen ($H < G \leq S_n$) ein, die für einen effizienten Algorithmus unerläßlich sind, und geben eine Reihe illustrativer Beispiele an.

Im letzten Kapitel demonstrieren wir anhand einer Vielzahl von Beispielen die Leistungsfähigkeit unserer Algorithmen, auch im Vergleich mit anderen Computeralgebrasystemen.

Abschließend weisen wir auf die Partitionstabellen für die primitiven Permutationsgruppen der Grade 12 bis 23 im Anhang dieser Arbeit hin.

Ich möchte an dieser Stelle Herrn Prof. Dr. M. E. Pohst ganz herzlich für seine Hinweise, Unterstützung und die gute Zusammenarbeit während der Anfertigung dieser Arbeit danken.

Ferner danke ich Herrn Prof. Dr. F. Leprévost für die Übernahme des Koreferats, allen Mitgliedern der Kant-Gruppe, Dr. F. Heß für viele anregende Diskussionen und die Durchsicht einer vorläufigen Fassung der Arbeit, Dr. J. Klüners für seine Unterstützung und die Bereitstellung seiner Programme und Dr. C. Fieker für computertechnische Hilfestellungen.

Darüber hinaus gilt mein Dank Herrn Prof. Dr. J. J. Cannon für seine Unterstützung bei der Berechnung gruppentheoretischer Daten und für den Aufenthalt mit der Magma-Gruppe in Sydney.

Notationen

Die meisten der hier verwendeten Notationen sind in der Literatur üblich. Um aber Unklarheiten zu vermeiden, seien einige der in dieser Arbeit verwendeten Konventionen und Notationen zusammengestellt. Darüber hinaus verweisen wir auf das Symbolverzeichnis am Ende dieser Arbeit.

Mengen

Sind Ω und Δ zwei Mengen mit $\Delta \subset \Omega$, so bezeichnet $|\Omega|$ die Kardinalität von Ω und $\Omega \backslash \Delta$ die Menge der Elemente von Ω, die nicht in Δ sind.

Gruppen

Alle in dieser Arbeit betrachteten Gruppen sind endlich und werden multiplikativ notiert. Das Einselement einer Gruppe G bezeichnen wir mit 1 oder 1_G, um die Zugehörigkeit hervorzuheben.

Ist H eine (echte) Untergruppe von G, so wollen wir dies in der Form $H \leq G$ ($H < G$) notieren. Gilt zusätzlich, daß H normal in G ist, so verwenden wir die Notation $H \trianglelefteq G$ ($H \lhd G$). Gruppen operieren von links. Dementsprechend betrachten wir Nebenklassen der Form gH, die wir als Linksnebenklassen aus der Nebenklassenmenge G/H bezeichnen. Vollständige (fest gewählte) Repräsentantensysteme bezeichnen wir mit $G//H$. Die Anzahl der linken Nebenklassenrepräsentanten von $G//H$ ist der Index von H in G, den wir mit $[\,G\!:\!H\,]$ bezeichnen wollen. Abbildungen werden ebenfalls von links geschrieben.

Für $n, m, k \in \mathbb{N}$ sei

S_n die symmetrische Permutationsgruppe vom Grad n,

A_n die alternierende Gruppe vom Grad n,

$C(n)$ die zyklische Gruppe vom Grad n,

$D(n)$ die Diedergruppe der Ordnung $2n$ vom Grad n,

$D_m(n)$ die Diedergruppe der Ordnung m vom Grad n,

$E(n) = \underbrace{C(m) \times \ldots \times C(m)}_{k}$ mit $n = m^k$ die elementare Gruppe vom Grad n.

Speziell ist

$E(4) = C(2) \times C(2)$ die Kleinsche Vierergruppe,

$F(n)$ die Frobeniusgruppe vom Grad n,

$F_m(n)$ die Frobeniusgruppe der Ordnung m vom Grad n,

$M(n)$ die Mathieugruppe vom Grad n.

Für eine ausführliche Erläuterung dieser Namensgebung sei auf Conway et al. [18] verwiesen.

Permutationen und Permutationsgruppen

Permutationen werden als Produkt disjunkter Zykel geschrieben, und die Identität notieren wir mit id.
Konsistent mit der Linksoperation ergeben sich Produkte der Form $\tau\sigma(\omega) = \tau(\sigma(\omega))$ für $\tau, \sigma \in S_n$. Es gilt also $(1,3,4)(3,4) = (3,1)$.
Unter einem Zykeltyp einer Permutation $\tau \in S_n$ verstehen wir die Menge der Zykellängen, die in der Dekomposition der Permutation vorkommen, gezählt mit Multiplizitäten (exponentiell geschrieben). Mit anderen Worten stellt der Zykeltyp eine Charakterisierung der Konjugationsklasse $\{ \sigma\tau\sigma^{-1} \mid \sigma \in S_n \}$ von τ dar. Ist τ vom Zykeltyp $2{,}4^2$, so ist τ das Produkt von drei disjunkten Zykeln von denen einer der Länge 2 und zwei der Länge 4 sind.
Für Permutationsgruppen verwenden wir zwei Bezeichnungen. Zum einen die 'T'-Notation, die auf einer Durchnummerierung der transitiven Permutationsgruppen basiert (vgl. Butler, McKay [8] oder Conway et al. [18]). Mit nT_k sei also die k-te transitive Permutationsgruppe vom Grad n bezeichnet. Handelt es sich um eine gerade Gruppe, so wollen wir dies zusätzlich mit $^+$ kennzeichnen. Gleichzeitig verwenden wir auch die Namensgebung aus Conway et al. [18].

Kapitel 1

Grundlagen

In diesem Kapitel werden die dieser Arbeit zugrundeliegenden Definitionen und theoretischen sowie algorithmischen Aussagen für Galoisgruppen bereitgestellt und Notationen vereinbart. Für die Theorie der Galoisgruppen verweisen wir auf [53, 59, 70, 72], für algorithmische Aspekte auf [12, 70].

1.1 Permutationsgruppen

Bei dem zu beschreibenden Algorithmus zur Galoisgruppenberechnung werden wir Galoisgruppen nicht als abstrakte Automorphismengruppen einer endlichen Körpererweiterung betrachten, sondern sie mit ihrem isomorphen Bild als Untergruppe einer entsprechenden symmetrischen Gruppe identifizieren. Ziel des Algorithmus wird es dann sein, diese isomorphe Permutationsgruppe zu bestimmen. Wir fassen hier die wesentlichen Grundlagen über Permutationsgruppen zusammen, wie wir sie an späterer Stelle benötigen.

1.1.1 Operationen und Permutationsdarstellungen

Für eine nichtleere Menge Ω sei mit S_Ω die Menge aller Permutationen von Ω bezeichnet. Diese Menge bildet bezüglich der Hintereinanderausführung von Permutationen eine Gruppe.

Operiert eine Gruppe G auf der Menge Ω (von links), d.h. gibt es eine Abbildung $G \times \Omega \longrightarrow \Omega$, $(g, \omega) \longmapsto g\omega$ mit $1_G\omega = \omega$ und $(gh)\omega = g(h\omega)$, $g, h \in G$, so erhalten wir einen Gruppenhomomorphismus τ von G in S_Ω definiert durch $\tau(g)(\omega) = g(\omega)$. Der Homomorphismus τ wird als *Permutationsdarstellung* von G auf Ω bezeichnet. Umgekehrt korrespondiert zu jeder Permutationsdarstellung von G auf Ω eine Operation von G auf Ω, d.h. Permutationsdarstellungen und

Operationen sind zwei verschiedene Darstellungsmöglichkeiten für die gleiche Situation. Besteht der Kern τ aus der Identität, so heißt die Permutationsdarstellung *treu* und der erste Homomorphiesatz besagt, daß das Bild τ isomorph zu G ist. In diesem Fall bezeichnen wir (G, Ω) als *Permutationsgruppe*. Der *Grad* einer Permutationsgruppe entspricht der Kardinalität von Ω.

Vergleicht man Permutationsdarstellungen einer Gruppe G, so wird man feststellen, daß manche im wesentlichen gleich sind und sich nur in der Bezeichnung der Punkte der zugrundeliegenden Mengen unterscheiden. In anderen Fällen dagegen sind die Darstellungen klar verschieden. So kann zum Beispiel die nicht abelsche Gruppe der Ordnung 6 sowohl durch eine Permutationsgruppe der Ordnung 3 (S_3), als auch durch eine Permutationsgruppe der Ordnung 6 ($D_6(6)$) treu dargestellt werden. Aufgrund dieser Beobachtung definiert man für Permutationsgruppen eine stärkere Eigenschaft, als die bloße Isomorphie zwischen abstrakten Gruppen:

1.1. Definition. Zwei Permutationsgruppen (G, Ω) und (H, Δ) heißen *äquivalent*, wenn es einen Gruppenisomorphismus $\phi : G \longrightarrow H$ und eine Bijektion $\psi : \Omega \longrightarrow \Delta$ gibt, die in dem Sinne zusammenpassen, daß $\psi(g\omega) = \phi(g)(\psi(\omega))$ für alle $\omega \in \Omega$ und $g \in G$ gilt.

Stimmen die Mengen Ω und Δ überein, so ist ψ eine Permutation auf Ω, und die Bedingung läuft auf die Konjugiertheit von G und H in der Gruppe S_Ω hinaus. Besitzt die Menge Ω die Kardinalität n, so können wir Ω durch Umnumerierung der Elemente mit einem Anfangsstück der natürlichen Zahlen identifizieren, und eine Permutationsgruppe (G, Ω) ist somit äquivalent zu einer Untergruppe der symmetrischen Gruppe S_n.

Die Operation einer Gruppe G auf einer Menge Ω teilt die Menge in disjunkte *Bahnen* ein. Dies sind Äquivalenzklassen unter der Relation $\omega_1 \sim \omega_2 :\Leftrightarrow g\omega_1 = \omega_2$ für ein $g \in G$. Die *Bahn* eines $\omega \in \Omega$ bezeichnen wir mit

$$\mathrm{Orb}_G(\omega) := \{\, g(\omega) \mid g \in G \,\}.$$

Die Operation heißt *transitiv*, wenn Ω nur aus einer Bahn besteht, d.h. wenn es zu allen $\omega_1, \omega_2 \in \Omega$ ein $g \in G$ gibt mit $g\omega_1 = \omega_2$, ansonsten *intransitiv*. Eine duale Rolle zu der Menge der Bilder von ω spielt die Menge der Elemente von G, die ω invariant lassen:

$$\mathrm{Stab}_G(\omega) := \{\, g \in G \mid g(\omega) = \omega \,\}$$

heißt der *Stabilisator* oder *Punktstabilisator* von ω in G. Es besteht die folgende Bahn-Stabilisator Beziehung:

1.2. Satz (Bahnensatz). *Die Abbildung* $g\mathrm{Stab}_G(\omega) \longrightarrow g\omega$ *ist eine Bijektion zwischen der Menge der linken Nebenklassen von* $\mathrm{Stab}_G(\omega)$ *in* G *und der Bahn von* ω *unter* G*.*

Die Aussage des Bahnensatzes kann dahingehend interpretiert werden, daß jede transitive Permutationsgruppe (G, Ω) bei Wahl eines festen $\omega \in \Omega$ äquivalent ist zur Permutationsgruppe $(G, G/\mathrm{Stab}_G(\omega))$, die auf den Nebenklassen per Linksmultiplikation operiert. Umgekehrt lassen sich alle transitiven Permutationsdarstellungen einer Gruppe G durch Operation auf den Nebenklassen einer Untergruppe H finden (es gibt also nur endlich viele). Der Kern der Permutationsdarstellung auf den Nebenklassen ist der Durchschnitt aller Konjugierten gHg^{-1}, $g \in G//H$.

1.3. Definition. Seien $\tau, g \in G$ und $H \leq G$. Dann heißt $\{g\tau g^{-1} \,|\, g \in G\}$ die G-Konjugationsklasse von τ, und die Menge $\{gHg^{-1} \,|\, g \in G\}$ bezeichnen wir als die G-Konjugationsklasse von H.

Somit ist die G-Konjugationsklasse einer Untergruppe H von G nichts anderes als die Bahn von H unter den Permutationen von G, wobei G auf der Menge $\Omega = G$ durch Konjugation operiert. Den Stabilisator von H in G bezüglich dieser Operation heißt der *Normalisator* von H in G, und wir bezeichnen ihn mit

$$N_G(H) := \{g \in G \,|\, gHg^{-1} = H\}.$$

1.1.2 Blöcke und imprimitive Permutationsgruppen

Betrachtet man nichtleere Teilmengen B von Ω, so läßt sich die Operation der Gruppe G in natürlicher Weise auf diese ausdehnen, indem man $gB := \{\, gb \,|\, b \in B\}$, $g \in G$ für alle $\emptyset \neq B \subseteq \Omega$ definiert. Eine nichtleere Teilmenge $B \subseteq \Omega$ nennen wir *Block* oder *Imprimitivitätsgebiet* von G, falls für jedes $g \in G$ entweder $gB = B$ oder $gB \cap B = \emptyset$ gilt. Konsistent mit dieser Namensgebung bezeichnen wir den Mengenstabilisator $\mathrm{Stab}_G(B) := \{\, g \in G \,|\, gB = B\}$ von B dann als *Blockstabilisator*. Jeder Block ist Teil eines Blocksystems, da mit B auch gB, $g \in G$ ein Block ist. Mit anderen Worten ist $\mathcal{B}$ genau dann ein *Blocksystem* für G, wenn $\mathcal{B}$ eine Partition von Ω ist, die unter der Operation von G invariant ist. Offensichtlich besitzt jede transitive Gruppe die trivialen Blocksysteme $\mathcal{B}_0 = \{\, \{\omega\} \mid \omega \in \Omega\,\}$ und $\mathcal{B}_\infty = \{\, \Omega\,\}$, alle anderen Blocksysteme heißen nichttrivial. Die gleiche Namensgebung gilt für die in den Blocksystemen enthaltenen Blöcke. Da ein Blocksystem von G bezüglich der Permutationen aus G invariant ist, enthält man zu jedem Blocksystem eine Permutationsdarstellung von G in die Gruppe $S_\mathcal{B}$. Für $\mathcal{B}_0$ ergibt sich eine zu G äquivalente Gruppe, für $\mathcal{B}_\infty$ die triviale Gruppe. Eine

transitive Permutationsgruppe, die ausschließlich triviale Blocksysteme hat, nennen wir *primitiv*, ansonsten sprechen wir von *imprimitiven* Permutationsgruppen. Für imprimitive Gruppen gilt der folgende Zusammenhang (vgl. Wielandt [87], Theorem 7.5):

1.4. Satz. *Es existiert eine Bijektion zwischen den nichttrivialen Blöcken B von G, die ω enthalten, und den Untergruppen H von G mit* $\mathrm{Stab}_G(\omega) < H < G$.

Die *Blocklänge* bzw. Kardinalität von B entspricht dabei gerade dem Index $[\,H : \mathrm{Stab}_G(\omega)\,]$, und die Anzahl der Blöcke eines Blocksystems dem Index $[\,G : H\,]$. Folglich kann Satz 1.4 auch dahingehend interpretiert werden, daß eine transitive Permutationsgruppe genau dann primitiv ist, wenn der Stabilisator jeden Elements eine maximale Untergruppe von G ist.

Die Imprimitivität einer transitiven Permutationsgruppe führt auf die Einbettung in ein gruppentheoretisches Produkt, daß sogenannte Kranzprodukt. Dieses wird zunächst als Spezialfall des semidirekten Produktes definiert.

Seien Gruppen G und H gegeben und Γ eine Menge auf der H operiert. Mit $Abb(\Gamma, G)$ sei die Menge aller Abbildungen von Γ nach G bezeichnet, die mit der punktweisen Verknüpfung $\sigma_1\sigma_2(\gamma) := \sigma_1(\gamma)\sigma_2(\gamma)$, $\sigma_1, \sigma_2 \in Abb(\Gamma, G)$, $\gamma \in \Gamma$ eine Gruppe bildet. Für $h \in H$ und $\sigma \in Abb(\Gamma, G)$ definieren wir eine Permutationsabbildung $\phi : H \longrightarrow Aut(Abb(\Gamma, G))$ durch

$$\phi_h(\sigma)(\gamma) := \sigma \circ h^{-1}(\gamma),\ \gamma \in \Gamma.$$

Durch Nachrechnen verifiziert man leicht, daß ϕ ein Homomorphismus und ϕ_h ein Automorphismus ist.

1.5. Definition. Das zu $\phi : H \longrightarrow Aut(Abb(\Gamma, G)) : h \mapsto \phi_h(\sigma)$ gehörende semidirekte Produkt

$$G \wr_\Gamma H := Abb(\Gamma, G) \rtimes_\phi H$$

heißt das Kranzprodukt von G und H bezüglich Γ.

Die Untergruppe $\{(\sigma, 1) \,|\, \sigma \in Abb(\Gamma, G)\} \cong Abb(\Gamma, G)$ bezeichnen wir als *Basis* oder *Basisnormalteiler* von $G \wr_\Gamma H$. Da hier nur endliche Gruppen und Mengen betrachtet werden, erhalten wir für die Ordnung des Kranzproduktes

$$|G \wr_\Gamma H| = |Abb(\Gamma, G) \rtimes_\phi H| = |Abb(\Gamma, G)||H| = |G|^{|\Gamma|}|H|.$$

Gehen wir nun davon aus, daß es sich bei den Gruppen G und H nicht um abstrakte Gruppen handelt, sondern um Permutationsgruppen $G \leq S_\Lambda$ und $H \leq$

S_Γ, so läßt sich eine Abbildung von $G \wr_\Gamma H$ auf dem kartesischen Produkt $\Lambda \times \Gamma$ wie folgt definieren:

$$(\sigma, h)(\lambda, \gamma) := (\sigma(h(\gamma))(\lambda),\, h(\gamma)) \text{ für alle } (\lambda, \gamma) \in \Lambda \times \Gamma \tag{1.6}$$

Es gilt

$$\begin{aligned}
\big((\sigma_1, h_1)(\sigma_2, h_2)\big)(\lambda, \gamma) &= \big((\sigma_1 \phi_{h_1}(\sigma_2), h_1 h_2)\big)(\lambda, \gamma) \\
&= (\sigma_1(\sigma_2 \circ h_1^{-1})((h_1 h_2)(\gamma))(\lambda),\, h_1 h_2(\gamma)) \\
&= (\sigma_1((h_1 h_2)(\gamma)) \cdot (\sigma_2 \circ h_1^{-1})((h_1 h_2)(\gamma))(\lambda),\, h_1 h_2(\gamma)) \\
&= (\sigma_1((h_1 h_2)(\gamma)) \cdot \sigma_2((h_2)(\gamma))(\lambda),\, h_1(h_2(\gamma))) \\
&= (\sigma_1, h_1)\big((\sigma_2(h_2(\gamma))(\lambda), h_2(\gamma)\big) \\
&= (\sigma_1, h_1)\big((\sigma_2, h_2)(\lambda, \gamma)\big),
\end{aligned}$$

so daß es sich bei der Abbildung (1.6) um eine Operation der Gruppe $G \wr_\Gamma H$ auf der Menge $\Lambda \times \Gamma$ handelt. Die zugehörige Permutationsdarstellung ist treu, da $(\sigma, h)(\lambda, \gamma) = (\sigma(h(\gamma))(\lambda),\, h(\gamma)) = (\lambda, \gamma)$ für alle $(\lambda, \gamma) \in \Lambda \times \Gamma$ sofort $h = \mathrm{id}_H$ in der zweiten Komponente impliziert. In der ersten Komponente folgt ebenfalls $\sigma = \mathrm{id}_{Abb(\Gamma, G)}$, da mit γ auch $h(\gamma)$ alle Werte in Γ durchläuft. Wir haben gezeigt

1.7. Lemma. *Sind Λ und Γ nichtleere Mengen und $G \leq S_\Lambda$, $H \leq S_\Gamma$, so ist das Kranzprodukt $G \wr_\Gamma H$ isomorph zu einer Untergruppe von $S_{\Lambda \times \Gamma}$ bezüglich der Abbildung $G \wr_\Gamma H \longrightarrow S_{\Lambda \times \Gamma} : (\sigma, h) \mapsto (\sigma(h(\gamma))(\lambda),\, h(\gamma))$, $(\lambda, \gamma) \in \Lambda \times \Gamma$.*

1.8. Bemerkung. (i) Operiert G transitiv auf Λ und H transitiv auf Γ, so operiert $G \wr_\Gamma H$ als Permutationsgruppe betrachtet transitiv, aber imprimitiv auf der Menge $\Lambda \times \Gamma$. Die Mengen $B_\gamma = \{(\lambda, \gamma) \mid \lambda \in \Lambda\}$ bilden als Bahnen des Basisnormalteilers ein Blocksystem.

(ii) Ist $\Lambda = \{1, \ldots, l\}$ und $\Gamma = \{1, \ldots, m\}$, so können wir (λ, γ) auf $l(\gamma - 1) + \lambda$ abbilden und somit $\Lambda \times \Gamma$ mit $\{1, \ldots, lm\}$ identifizieren. Dann entsprechen den Blöcken $B_\gamma = \Lambda \times \{\gamma\}, (\gamma \in \Gamma)$ die Elemente der Menge $\mathcal{B} = \{\{1, \ldots, l\}, \{l + 1, \ldots, 2l\}, \ldots, \{(m-1)l + 1, \ldots, ml\}\}$, und somit ist $\mathcal{B}$ ein Blocksystem zum Kranzprodukt $(G \wr_\Gamma H, \{1, \ldots, ml\})$. Aus (1.6) folgt, daß die Elemente $(1, h)$ gerade eine Vertauschung der Blöcke bewirken, während die Permutationen $(\sigma, 1)$ die Elemente innerhalb der Blöcke vertauschen.

So besteht zum Beispiel das Kranzprodukt der symmetrischen Gruppen S_Λ und S_Γ aus allen Permutationen von $S_{\Lambda \times \Gamma}$ für die $B_\gamma = \Lambda \times \{\gamma\}$, $\gamma \in \Gamma$ Blöcke sind und die diese untereinander permutieren, d.h. $S_\Lambda \wr_\Gamma S_\Gamma = \mathrm{Stab}_{S_{\Lambda \times \Gamma}}(\{B_{\gamma_1}, \ldots, B_{\gamma_m}\})$ für $|\Gamma| = m$. Es folgt

1.9. Proposition. *Das Kranzprodukt der symmetrischen Gruppen S_Λ und S_Γ ist eine maximale Untergruppe von $S_{\Lambda \times \Gamma}$.*

Beweis. Gäbe es eine Gruppe H mit $S_\Lambda \wr_\Gamma S_\Gamma < H < S_{\Lambda\times\Gamma}$, so könnte diese wegen $S_\Lambda \wr_\Gamma S_\Gamma = \mathrm{Stab}_{S_{\Lambda\times\Gamma}}(\{B_1,\ldots,B_m\})$ nur triviale Blöcke besitzen, wäre also primitiv. Mit $S_\Lambda \wr S_\Gamma$ enthält auch H Transpositionen. Nach Huppert [37], Kapitel II, Satz 4.5 fällt aber eine primitive Gruppe, die eine Transposition enthält mit der vollen symmetrischen Gruppe zusammen. □

Die Umkehrung von Proposition 1.9 gilt ebenfalls und beruht auf dem Einbettungssatz von Krasner und Kaloujnine [46], der besagt, daß sich jede imprimitive Permutationsgruppe in ein geeignetes Kranzprodukt vom gleichen Grad einbetten läßt. Somit nehmen die Kranzprodukte in gewissen Sinn die Rolle der „universellen“ imprimitiven Permutationsgruppen ein.

1.10. Satz (Einbettungssatz). *Sei (G,Ω) eine transitive, imprimitive Permutationsgruppe mit Blocksystem $\mathcal{B} = \{B_1,\ldots,B_m\}$ und $U = \mathrm{Stab}_G(B_i)$ der Stabilisator eines fest gewählten Blockes $B_i \in \mathcal{B}$. Bezeichne $\tau : G \longrightarrow S_\Gamma$, $\Gamma := \{1,\ldots,m\}$ die Permutationsdarstellung von G bezüglich $\mathcal{B}$ und $\varphi : U \longrightarrow S_{B_i}$ die Permutationsdarstellung von U auf B_i. Dann ist (G,Ω) äquivalent zu einer Untergruppe von $(\varphi(U) \wr_\Gamma \tau(G), \Lambda\times\Gamma)$, wobei $\Lambda = B_i$.*

Beweis. Für B_i bildet die Menge $\{\, g_jB_i \mid g_j \in G//\mathrm{Stab}_G(B_i)\,\}$ das Blocksystem $\mathcal{B}$ von G, und wir können o.B.d.A durch Umnumerierung die $g_j \in G//\mathrm{Stab}_G(B_i)$ so anordnen, daß $g_jB_i = B_j$ für $1 \le j \le m$ und $g_i = \mathrm{id}_G$ gilt.

Seien nun $\lambda,\lambda_k \in \Lambda$ und $\gamma,\gamma_k \in \Gamma$, $k = 1,2$. Wir wählen eine bijektive Abbildung $\psi : \Omega \longrightarrow \Lambda\times\Gamma$ mit der Eigenschaft $\psi(\omega) = (\lambda_1,\gamma_1) \Longrightarrow \omega \in B_{\gamma_1}$ und $\lambda_1 = g_{\gamma_1}^{-1}(\omega)$. Mit Hilfe dieser Abbildung fassen wir G als transitive, imprimitive Permutationsgruppe von $\Lambda\times\Gamma$ mit den Blöcken $B_\gamma = \Lambda\times\{\gamma\}$ auf. Wir erklären eine Abbildung

$$\phi : G \longrightarrow \varphi(U) \wr_\Gamma \tau(G)$$

durch $\phi(g) = (\sigma,h)$ mit $h := \tau(g)$ und $\sigma(\gamma) := g_\gamma^{-1} g g_{h^{-1}(\gamma)}$ und behaupten, daß ϕ operationsverträglich und monomorph ist. Dazu zeigen wir zunächst, daß

$$\phi(g)\psi(\omega) = \psi(g(\omega)) \text{ für alle } g \in G \text{ und } \omega \in \Omega \tag{1.11}$$

gilt: Sei $\phi(g) = (\sigma,h)$ und $\psi(\omega) = (\lambda_1,\gamma_1)$. Aus Lemma 1.7 folgt $\phi(g)\psi(\omega) = (\sigma,h)(\lambda_1,\gamma_1) = (\sigma(h(\gamma_1))(\lambda_1), h(\gamma_1))$. Ist $\psi(g(\omega)) = (\lambda_2,\gamma_2)$, so zeigen wir, daß $\lambda_2 = \sigma(h(\gamma_1))(\lambda_1)$ und $\gamma_2 = h(\gamma_1)$ gilt. Aus der Definition von ψ und da nach Voraussetzung $\omega \in B_{\gamma_1}$ ist, erhalten wir $g(\omega) \in B_{\gamma_2} = g(B_{\gamma_1}) = B_{h(\gamma_1)}$, woraus die Gleichheit in der zweiten Komponente folgt. Ebenfalls mittels der Definition von ψ und der Definition von σ erhalten wir dann $\lambda_2 = g_{\gamma_2}^{-1}(g(\omega)) = g_{\gamma_2}^{-1}(g(g_{\gamma_1}g_{\gamma_1}^{-1}\omega)) = g_{h(\gamma_1)}^{-1} g g_{\gamma_1}(\lambda_1) = \sigma(h(\gamma_1))(\lambda_1)$. Aus Gleichung (1.11) folgt nun die Homomorphieeigenschaft von ϕ:

$$\phi(g_1g_2)(\psi(\omega)) = \psi(g_1g_2(\omega)) = \phi(g_1)\psi(g_2(\omega)) = (\phi(g_1)\phi(g_2))\psi(\omega),\ g_1,g_2 \in G.$$

Dies gilt für alle $\omega \in \Omega$ und folglich für alle $(\lambda, \gamma) \in \Lambda \times \Gamma$, da ψ eine Bijektion zwischen Ω und $\Lambda \times \Gamma$ ist. Letztlich ist $\phi(g)$ die Identität auf $\Lambda \times \Gamma$ genau dann, wenn $\phi(g)(\psi(\omega)) = \psi(\omega)$, d.h. $\psi(g(\omega)) = \psi(\omega)$ für alle $\omega \in \Omega$ ist. Da ψ eine Bijektion ist, muß $g(\omega) = \omega$ für alle $\omega \in \Omega$ gelten, also $g = \mathrm{id}_G$. □

1.2 Galoistheorie

Galoistheorie ist das Zusammenspiel zwischen Polynomen, Körpern und Gruppen. Bei der Beschreibung eines effizienten Verfahrens zur Berechnung der Galoisgruppe eines normierten, irreduziblen und separablen Polynoms werden wir oftmals Gebrauch von diesem Zusammenhang machen. So stellt die Berechnung von Teilkörpern eine wesentliche Grundlage für die in den späteren Kapiteln entwickelten Algorithmen dar. Teilkörper hängen bekanntermaßen mit den Galoisgruppen über den Hauptsatz der Galoistheorie zusammen.

1.12. Satz. *(Hauptsatz der Galoistheorie) Sei E/K eine endliche Galoiserweiterung. Dann ist die Abbildung $\phi : F \mapsto G(E/F)$ eine Bijektion zwischen der Menge der Teilkörper F von E/K und der Menge der Untergruppen H von $G(E/K)$. Die Umkehrabbildung von ϕ ist $H \mapsto Fix(E, H)$, wobei $Fix(E, H)$ den Fixkörper von H bezeichne. Die Erweiterung F/K ist genau dann galoissch, wenn $G(E/F)$ ein Normalteiler von $G(E/K)$ ist. In diesem Fall erhält man per Restriktion eine natürliche Isomorphie $G(F/K) \cong G(E/K)/G(E/F)$.*

Ist speziell E/K eine Erweiterung endlicher Körper, so gelten stärkere Aussagen.

1.13. Satz. *Sei E/K eine beliebige Erweiterung endlicher Körper und q die Elementezahl von K. Dann ist E/K galoissch mit zyklischer Galoisgruppe, und zwar wird $G(E/K)$ von dem Frobenius-Automorphismus $\sigma_q : \alpha \mapsto \alpha^q$ von E erzeugt.*

Der Zusammenhang zu Polynomen ergibt sich, indem die Galoisgruppe des Zerfällungskörpers $N(f, K)$ eines nichtkonstanten Polynoms f über dem Körper K als Galoisgruppe des Polynoms f definiert wird. Die Galoisgruppe $G(f, K) = G(N(f, K)/K)$ des Polynoms $f \in K[x]$ ist also die Gruppe der Automorphismen des Körpers $N(f, K)$, die K elementweise festlassen. Hat das Polynom f genau n verschiedene Nullstellen in $N(f, K)$, so definiert die Operation von $G(f, K)$ auf der Menge der Nullstellen eine treue Permutationsdarstellung $G(f, K) \longrightarrow S_n$, da die Identität das einzige Element von $G(f, K)$ ist, welches alle Nullstellen von f punktweise fixiert. Somit ist $G(f, K)$ für eine fest gewählte Anordnung der Nullstellen isomorph zu einer Untergruppe der symmetrischen Gruppe S_n, welche wir mit $\mathcal{G}(f, K)$ bezeichnen. Ändert man die Anordnung der Nullstellen $\alpha_1, \ldots, \alpha_n$ von f mittels einer Permutation $\tau \in S_n$, d.h. $\alpha'_i = \alpha_{\tau(i)}$, so folgt

$G(f,K) \cong \tau^{-1}\mathcal{G}(f,K)\tau$. Daher wollen wir ohne dies explizit zu vermerken im folgenden immer von einer fest gegebenen Anordnung der Nullstellen des Polynoms f ausgehen. Ist darüber hinaus f irreduzibel, so ist die Operation der Galoisgruppe auf der Menge der Nullstellen transitiv und aufgrund der Separabilität von f gilt auch die Umkehrung dieser Aussage. Da wir uns in unseren Ausführungen auf normierte, irreduzible und separable Polynome f vom Grad n beschränken, interessieren wir uns also ausschließlich für transitive Permutationsgruppen eines bestimmten Grads und identifizieren die Galoisgruppe mit ihrem Bild $\mathcal{G}(f,K) \leq S_n$.

1.2.1 Ein Reduktionsprinzip der Galoistheorie

Ein erstes Kriterium, um gewisse Teilinformationen über $\mathcal{G}(f,K)$ zu erhalten, stellt das van der Waerden-Kriterium dar (vgl. van der Waerden [83], S.198).

1.14. Satz. *(van der Waerden-Kriterium) Seien R ein ZPE-Ring, $\bar{R} = R/\mathfrak{p}$ der Restklassenring für ein Primideal $\mathfrak{p}$ in R und K, $\bar{K}$ die zugehörigen Quotientenkörper. Weiterhin sei f ein normiertes Polynom aus $R[x]$, dessen homomorphes Bild wir mit $\bar{f} \in \bar{R}[x]$ bezeichnen. Die Polynome f und $\bar{f}$ seien beide separabel. Dann ist bei passender Nullstellenanordnung $\mathcal{G}(\bar{f},\bar{K})$ eine Untergruppe von $\mathcal{G}(f,K)$.*

In dem Algorithmus zur Galoisgruppenberechnung, der in einer ersten Übersicht in Kapitel 2 vorgestellt wird, verwenden wir eine direkte Folgerung von Satz 1.14:

1.15. Korollar. *Seien R ein ZPE-Ring mit Quotientenkörper K, f ein normiertes Polynom mit Koeffizienten in R und $\mathfrak{p}$ ein Primideal, so daß $R/\mathfrak{p}$ ein endlicher Körper ist und das von f bestimmte Polynom $\bar{f}$ von $(R/\mathfrak{p})[x]$ separabel ist. Die Primfaktorzerlegung von $\bar{f}$ in $(R/\mathfrak{p})[x]$ laute*

$$\bar{f} = \bar{f}_1 \cdots \bar{f}_r,$$

und n_i bezeichne jeweils den Grad von $\bar{f}_i$. Aufgefaßt als Permutationsgruppe der Nullstellen von f enthält die Galoisgruppe $\mathcal{G}(f,K)$ eine Permutation σ, deren Zykelzerlegung die Gestalt $\sigma = \sigma_1 \cdots \sigma_r$ mit Länge $\sigma_i = n_i$, $(1 \leq i \leq r)$ besitzt.

Der Beweis dieses Korollars kann Kapitel 2.9, Abschnitt 8 von Pohst, Zassenhaus [70] entnommen werden. Wir merken an, daß dort die Voraussetzung an R in Satz 1.14 und Korollar 1.15 auf einen kommutativen Ring mit Eins abgeschwächt wird. Korollar 1.15 wird in unserem Algorithmus ausschließlich zur Elimination von transitiven Permutationsgruppen (möglichen Galoisgruppen $\mathcal{G}(f,K)$) verwendet. Bei jeder Faktorisierung des Polynoms $f \in R[x]$ modulo eines Primideals $\mathfrak{p}$,

welches nicht die Diskriminante $\mathrm{disc}(f)$ teilt, entfallen die Untergruppen der S_n, die kein Element mit entsprechendem Zykeltyp besitzen. Da zwei Elemente σ und τ genau dann in S_n konjugiert sind, wenn ihre Zykelzerlegungen vom gleichen Typ sind, folgt, daß bei Elimination einer Gruppe H auch alle konjugierten Gruppen $\sigma H \sigma^{-1}$, $(\sigma \in S_n)$ entfallen. Somit läßt sich sehr schnell die Galoisgruppe $G(f, K) = S_n$ bestimmen, da für diese Gruppe jedwede Zykeltypen auftreten. Analoges gilt auch für Galoisgruppen $G(f, K) = A_n$, wenn man sich auf Körper K mit $\mathrm{char}(K) \neq 2$ beschränkt unter Verwendung des Diskriminantenkriteriums (vgl. Satz 2.11 (*iii*)). Für alle anderen Fälle aber ist die Tatsache von Bedeutung, daß es zu jedem auftretenden Zykeltyp $(n_1, \ldots, n_r)$ einer Permutationsgruppe unendlich viele Primideale gibt, so daß f im endlichen Restklassenkörper in r Primpolynome der Gerade $n_1, \ldots, n_r$ zerfällt. Diese Primideale tauchen mit der erwarteten Häufigkeit auf (vgl. Tschebotarevscher Dichtigkeitssatz, Koch [65], Theorem 1.116, Theorem 1.113 unter Verwendung von $|\{\, \mathfrak{p} \in Cl(\mathbb{Z}, K) \,|\, \mathrm{N}(\mathfrak{p}) \leq x \,\}| \sim \frac{x}{\log(x)}$ aus Goldstein [32], Narkiewicz [60], S.372).

1.16. Satz. *Sei K ein algebraischer Zahlkörper, f ein nichtkonstantes Polynom mit Koeffizienten in $Cl(\mathbb{Z}, K)$, $(n_1, \ldots, n_r)$ ein Zykeltyp und C die Menge der Elemente von $\mathcal{G}(f, K)$, die diesen Zykeltyp haben. Mit A sei die Menge der Primideale $\mathfrak{p}$ von $Cl(\mathbb{Z}, K)$ bezeichnet, für die $f \equiv f_1 \cdots f_r \bmod \mathfrak{p}$ mit Grad $f_i = n_i$ ist. Dann gilt:*

$$\lim_{x \to \infty} \frac{|\{\mathfrak{p} \in A \,|\, \mathrm{N}(\mathfrak{p}) \leq x\}|}{|\{\mathfrak{p} \in Cl(\mathbb{Z}, K) \,|\, \mathrm{N}(\mathfrak{p}) \leq x\}|} = \frac{|C|}{|\mathcal{G}(f, K)|}.$$

1.17. Bemerkung. (*i*) Satz 1.16 gilt vollkommen analog für globale Körper (vgl. Fried, Jarden [27], Chapter 5, Theorem 5.6).

(*ii*) Für unsere Berechnungen ist Satz 1.16 von keinem besonderen Nutzen. Interessanter wären explizite Fehlerabschätzungen oder obere Abschätzungen für die kleinste $\mathrm{N}(\mathfrak{p})$ eines $\mathfrak{p} \in A$, so daß $f \bmod \mathfrak{p}$ das gesuchte Faktorisierungsverhalten aufweist. Alle diesbezüglichen Resultate sind in der Praxis leider nicht brauchbar, da die angegebenen Schranken zu groß sind (vgl. Lagarias et al. [47], Oesterlé [64], sogar unter Annahme der verallgemeinerten Riemannschen Vermutung).

(*iii*) Durch Anwendung von Korollar 1.15 kann nach ausreichend vielen Faktorisierungen von $f \bmod \mathfrak{p}$ eine recht gute Vermutung über die tatsächliche Galoisgruppe $\mathcal{G}(f, K)$ getroffen werden. Wir merken jedoch an, daß Grad 8 der kleinste Grad ist, für den es Gruppenpaare mit gleichen Zykeltypen gibt, die mit der gleichen Häufigkeit auftreten: $8T_{10}^{+}/8T_{11}^{+}$, $8T_{32}^{+}/8T_{33}^{+}$, $8T_{39}^{+}/8T_{41}^{+}$. Folglich kann der Tschebotarevsche Dichtigkeitssatz in diesen Fällen nicht als mögliches Unterscheidungskriterium dienen.

1.18. Beispiel. Es sei $f(t,x) = x^5 - t(5x-4) \in \mathbb{Z}[t][x]$. Die Diskriminante von f hat die Primfaktorzerlegung $\mathrm{disc}(f) = 2^8 5^5 t^4 (t-1)$, ist also kein Quadrat eines Elements in $\mathbb{Z}[t]$. Somit kommen nach Satz 2.11 (*iii*) nur ungerade Permutationsgruppen als Galoisgruppen in Frage. Wir wenden nun Satz 1.14 rekursiv an: Zunächst bestimmen wir die Faktorisierung von f modulo dem Primideal $(t+1)\mathbb{Z}[t]$. Es gilt

$$f(t,x) \equiv x^5 + 5x - 4 \bmod (t+1)\mathbb{Z}[t],$$

und die Galoisgruppe von $x^5 + 5x - 4$ ist bei entsprechender Anordnung der Nullstellen isomorph zu einer Untergruppe von $\mathcal{G}(f, \mathbb{Q}(t))$. Durch Anwendung von Korollar 1.15 erhalten wir für die Primzahlen 3 und 7 (die Primzahlen 2 und 5 sind Diskriminantenteiler und entfallen aus diesem Grund)

$$\begin{aligned} x^5 + 5x - 4 &\equiv x^5 + 2x + 2 \bmod 3 \\ x^5 + 5x - 4 &\equiv (x^2 + 5x + 5)(x^3 + 2x^2 + 6x + 2) \bmod 7. \end{aligned}$$

Nach der ersten Faktorisierung entfällt keine der beiden ungeraden Permutationsgruppen vom Grad 5, aber mittels der zweiten Faktorisierung läßt sich die Frobeniusgruppe $F(5)$ eliminieren und übrig bleibt die Gruppe S_5. Dieses Ergebnis kann auch theoretisch sehr leicht verifiziert werden, wenn man bedenkt, daß eine Untergruppe der S_n, die einen Zyklus der Länge n und eine Transposition enthält, mit der vollen symmetrischen Gruppe S_n übereinstimmt, wenn n eine Primzahl ist.

Da die bekannten Algorithmen zum Faktorisieren von Polynomen über endlichen Körpern sehr schnell sind, können innerhalb kürzester Zeit verschiedene Zykeltypen bestimmt werden. Testdurchläufe belegen, daß mittels dieses Verfahrens eine sehr gute Annäherung von „unten“ an die Galoisgruppe stattfindet, d.h. daß fast alle in Frage kommenden Gruppen H mit $H \leq \mathcal{G}(f,K)$ durch diese Tests eliminiert werden.

1.3 Bewertungen und Vervollständigungen

Der Körper $\mathbb{R}$ der reellen Zahlen ist die Vervollständigung von $\mathbb{Q}$ bezüglich des gängigen Absolutbetrags $|\cdot|$. Ein beliebiges Polynom über $\mathbb{Q}$ hat dann alle seine Nullstellen im Körper $\mathbb{C}$ der komplexen Zahlen, welcher eine Erweiterung vom Grad 2 von $\mathbb{R}$ ist, und man kann mit den Nullstellen in approximierter Form rechnen. Später betrachten wir die analoge Situation für p-adische Absolutbeträge von $\mathbb{Q}$ (und anderen Körpern) und stellen in diesem Abschnitt die wesentlichen, von uns benötigten Aussagen über Bewertungen und Vervollständigungen zusammen.

Ein Absolutbetrag $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ (vom Rang eins) eines Körpers K heißt *archimedisch*, falls die Menge $\{\,|n|\,|\,n \in \mathbb{Z}\}$ nicht beschränkt ist. Im anderen Fall heißt $|\cdot|$ nicht-archimedisch. Zu jedem nicht-archimedischen Betrag von K gehört eine *(exponentielle) Bewertung* $\nu : K \longrightarrow \mathbb{R} \cup \{\infty\}$ mit $\nu\,(\cdot) = -\log|\cdot|$, welche die Eigenschaften (i) $\nu(a) = \infty \Longleftrightarrow a = 0$, (ii) $\nu(ab) = \nu(a) + \nu(b)$ und (iii) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ erfüllt. Umgekehrt läßt sich aber auch zu jeder Bewertung von K, d.h. einer Abbildung mit den Eigenschaften $(i) - (iii)$, durch

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0} \text{ mit } |\cdot| = c^{-\nu(\cdot)} \tag{1.19}$$

für fixiertes $c > 1$ und $c^{-\infty} := 0$ ein nicht-archimedischer Betrag definieren. Aufgrund dieser Äquivalenz sollen im folgenden Definitionen und Namensgebungen für (nicht-archimedische) Beträge auch gleichermaßen für Bewertungen verwendet werden. Ein Betrag heißt *diskret*, wenn $|K^\times|$ eine diskrete Untergruppe ungleich $\{1\}$ von $\mathbb{R}_{>0}$ ist. Es folgt, daß diskrete Beträge nicht-archimedisch sind und in diesem Fall $\nu(K) = -\log|K| \cong \mathbb{Z} \cup \{\infty\}$ gilt. Ist insbesondere $\nu(K^\times) = \mathbb{Z}$, so nennen wir den diskreten Betrag *normiert*.

1.20. Definition. Unter einer Stelle $[\,|\cdot|_p\,]$ eines Körpers verstehen wir die Klasse aller zu einem nicht-trivialen Betrag $|\cdot|_p$ von K äquivalenten Beträge von K. Die Menge aller Stellen bezeichnen wir mit $\mathbb{S}(K)$.

1.21. Definition und Satz. *Sei $|\cdot|$ ein nicht-archimedischer Betrag eines Körpers K. Dann gelten:*

(i) Die Menge $\mathcal{O} := \{\,a \in K\,|\,|a| \leq 1\,\}$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{q} := \{\,a \in K\,|\,|a| < 1\,\}$.

(ii) Ist $|\cdot|$ ein diskreter Betrag, so ist $\mathcal{O}$ ein Hauptidealring, und ein Element $\pi \in \mathfrak{q}$ mit $\mathfrak{q} = \pi\mathcal{O}$ heißt Primelement von $\mathfrak{q}$.

Da $\mathfrak{q}$ maximales Ideal in $\mathcal{O}$ ist, ist die Menge $\bar{K}_\mathfrak{q} := \mathcal{O}/\mathfrak{q}$ ein Körper, der Restklassenkörper von K bezüglich $|\cdot|$.

$\mathcal{O}$ hat die Eigenschaft, daß

$$\text{für jedes } a \in K^\times \text{ entweder } a \in \mathcal{O} \text{ oder } a^{-1} \in \mathcal{O} \text{ ist.} \tag{1.22}$$

Ein echter Teilring $\mathcal{O}$ von K, der die Bedingung (1.22) erfüllt, heißt *Bewertungsring* von K. Ist $\mathcal{O}$ gleichzeitig ein Hauptidealring, so sprechen wir von einem *diskreten Bewertungsring*. Das eindeutig bestimmte maximale Ideal $\mathfrak{q} := \mathcal{O}\backslash\mathcal{O}^\times$ nennen wir *Bewertungsideal*, welches in diesem Fall von der Form $\pi\mathcal{O}$ mit einem irreduziblen Element π ist. Umgekehrt können wir von einem Bewertungsideal $\mathfrak{q}$ durch $\mathcal{O}_\mathfrak{q} := \{a \in K\,|\,a^{-1} \notin \mathfrak{q}\}$ eindeutig seinen Bewertungsring erhalten. Es gilt der folgende Satz (P. M. Cohn [13], 1.4, Bemerkung nach Theorem 4.1)

1.23. Satz. *Sei $\mathcal{O}_\mathfrak{q}$ ein diskreter Bewertungsring eines Körpers K mit Bewertungsideal $\mathfrak{q}$. Dann hat jedes $0 \neq a \in K$ eine eindeutige Darstellung der Form $a = \pi^k u$ mit $\pi \in \mathfrak{q}, k \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$.*

Somit läßt sich zu dem Bewertungsideal $\mathfrak{q}$ mit Primelement π durch

$$\nu_\mathfrak{q} : K \to \mathbb{Z} \cup \{\infty\} : a \mapsto \begin{cases} k, & a = \pi^k u \neq 0 \\ \infty, & a = 0 \end{cases} \tag{1.24}$$

eine normierte, diskrete Bewertung und mittels (1.19) ein Betrag $|\cdot|_\mathfrak{q}$ von K definieren. Diese Definition hängt nur von dem Bewertungsideal $\mathfrak{q}$ ab und nicht von der Wahl des Primelements π. Mit (1.24) erhalten wir dann eine Bijektion zwischen der Menge der Äquivalenzklassen der normierten, diskreten Beträge von K und der Menge $\mathbb{P}(K) := \{\, \mathfrak{q} \mid \mathfrak{q}$ ist maximales Ideal eines diskreten Bewertungsrings $\mathcal{O}_\mathfrak{q}$ von $K\}$ durch

$$\begin{array}{ccccccc} \mathbb{S}(K)_{norm.diskr.} & \longrightarrow & \mathbb{P}(K) & : & [\,|\cdot|_\mathfrak{p}\,] & \mapsto & \{\, a \in K \mid |a|_\mathfrak{p} < 1 \,\} \\ \mathbb{P}(K) & \longrightarrow & \mathbb{S}(K)_{norm.diskr.} & : & \mathfrak{q} & \mapsto & [\,|\cdot|_\mathfrak{q}\,] \end{array} \tag{1.25}$$

Sei F/K eine endliche separable Körpererweiterung und $\mathcal{P}$ und $\mathfrak{p}$ Bewertungsideale diskreter Bewertungsringe von F bzw. K mit $\mathfrak{p} \subseteq \mathcal{P}$. In diesem Fall sagen wir „$\mathcal{P}$ *liegt über* $\mathfrak{p}$“, notieren dies mit $\mathcal{P}|\mathfrak{p}$, und es gilt $\mathfrak{p} = \mathcal{P} \cap K$. Sind $\nu_\mathcal{P}$ bzw. $\nu_\mathfrak{p}$ die zugehörigen normierten Bewertungen, so existiert $e(\mathcal{P}|\mathfrak{p}) \in \mathbb{Z}_{>0}$ mit $\nu_\mathcal{P}(a) = e(\mathcal{P}|\mathfrak{p})\nu_\mathfrak{p}(a)$ für alle $a \in K$. Somit ist $\nu_\mathcal{P}$ keine Fortsetzung von $\nu_\mathfrak{p}$, wenn $e(\mathcal{P}|\mathfrak{p}) \neq 1$. Die Zahl $e(\mathcal{P}|\mathfrak{p})$ heißt *Verzweigungsindex* von $\mathcal{P}$ über $\mathfrak{p}$, und der Grad der Restklassenkörper $f(\mathcal{P}|\mathfrak{p}) := [\,\bar{F}_\mathcal{P} : \bar{K}_\mathfrak{p}\,] \in \mathbb{Z}_{>0}$ wird als *Trägheitsgrad* oder *Restklassengrad* von $\mathcal{P}$ über $\mathfrak{p}$ bezeichnet. Sind $\mathcal{P}_1, \ldots, \mathcal{P}_r$ alle Bewertungsideale von F, welche über $\mathfrak{p}$ liegen, so gilt $\sum_{i=1}^r e(\mathcal{P}_i|\mathfrak{p}) f(\mathcal{P}_i|\mathfrak{p}) = [F : K]$.

1.26. Bezeichnung. *Die Vervollständigung eines Körpers F bezüglich eines Betrags (Bewertung, Stelle, „geeignetem“ Primideal) von F wird mit kalligraphischen Buchstaben $\mathcal{F}$ bezeichnet. Die Fortsetzung von $|\cdot|$ bzw. der zugehörigen Bewertung ν auf $\mathcal{F}$ bezeichnen wir ebenfalls mit $|\cdot|$ bzw. ν.*

Schließlich treffen wir für spätere Anwendungen allgemein folgende Definitionen:

1.27. Definition. (*i*) Für eine unitäre Ringerweiterung der Integritätsringe $R \subseteq S$ definieren wir $Cl(R, S)$ als den Ring der über R ganzalgebraischen Elemente von S.

(*ii*) Sei R ein Integritätsring mit Quotientenkörper $Q := \mathrm{Quot}(R)$. Für ein Polynom g mit Koeffizienten in Q bezeichnen wir den Zerfällungskörper von g über Q mit $N(g, Q)$. Dabei betrachten wir $N(g, Q)$ als Teilkörper eines fest gewählten algebraischen Abschlusses von Q.

1.4 Newton-Lifting

Ein wesentliche Grundlage des Algorithmus, den wir beschreiben werden, ist die Bestimmung der Nullstellen des Polynoms $f \in K[x]$, dessen Galoisgruppe wir berechnen wollen. Ist zum Beispiel K ein algebraischer Zahlkörper, so können wir ohne größere Probleme die Nullstellen von f in $\mathbb{C}$ approximieren. Meistens sind wir aber an einer Darstellung der Nullstellen in einer geeigneten unverzweigten $\mathfrak{p}$-adischen Erweiterung interessiert. Dafür fassen wir in diesem Abschnitt die bekannten Ergebnisse zum Newton-Lifting zusammen, wie wir sie später für unsere Algorithmen benötigen.

1.28. Lemma. *(Quadratisches Newton-Lifting) Sei R ein kommutativer Ring mit Eins und $\mathfrak{q}$ ein Ideal in R. Gegeben seien ein Polynom $g(x) \in R[x]$ und ein Element $\beta_k \in R$, $(k \in \mathbb{Z}_{\geq 0})$ mit*

$$g(\beta_k) \equiv 0 \bmod \mathfrak{q}^{2^k} \text{ und } g'(\beta_k) \text{ ist invertierbar modulo } \mathfrak{q}. \tag{1.29}$$

Dann existiert ein Element $\beta_{k+1} \in R$ mit

$$\beta_{k+1} \equiv \beta_k - g(\beta_k)g'(\beta_k)^{-1} \bmod \mathfrak{q}^{2^{k+1}}, \tag{1.30}$$

und es gilt $g(\beta_{k+1}) \equiv 0 \bmod \mathfrak{q}^{2^{k+1}}$, $\beta_{k+1} \equiv \beta_k \bmod \mathfrak{q}^{2^k}$ und $g'(\beta_{k+1})$ ist invertierbar modulo $\mathfrak{q}$. Darüber hinaus ist $\beta_{k+1} \in R$ modulo $\mathfrak{q}^{2^{k+1}}$ eindeutig bestimmt: Ist $\gamma_{k+1} \in R$ mit $g(\gamma_{k+1}) \equiv 0 \bmod \mathfrak{q}^{2^{k+1}}$ und $\gamma_{k+1} \equiv \beta_{k+1} \equiv \mathfrak{q}^{2^k}$, so gilt $\gamma_{k+1} \equiv \beta_{k+1} \bmod \mathfrak{q}^{2^{k+1}}$.

Beweis. Analog zum Beweis von Lemma 9.21, Theorem 9.27 in von zur Gathen, Gerhard [85]. □

Mittels der Rekursion (1.30) lassen sich also iterativ immer bessere Approximationen einer exakten Nullstelle des Polynoms g berechnen. Wie wir in (1.30) gesehen haben wird bei jeder Iteration eine Division benötigt, die aber für die Implementation durch drei (schnellere) Multiplikationen ersetzt werden kann.

1.31. Proposition. *Sei R ein kommutativer Ring mit Eins und $\mathfrak{q}$ ein Ideal in R. Gegeben seien ein Polynom $h(x) \in R[x]$ und ein Element $\beta_0 \in R$, so daß $h(\beta_0)$ modulo $\mathfrak{q}$ invertierbar ist. Darüber hinaus sei $(s_i)_{i\in\mathbb{N}_0}$ eine Folge in R, die wie folgt definiert ist: s_0 sei das Inverse von $h(\beta_0)$ modulo $\mathfrak{q}$ und $s_{i+1} \equiv 2s_i - h(\beta_0)s_i^2 \bmod \mathfrak{q}^{2^{i+1}}$. Dann gilt $s_i h(\beta_0) \equiv 1 \bmod \mathfrak{q}^{2^i}$ für alle $i \in \mathbb{Z}_{\geq 0}$.*

Beweis. Für $i = 0$ gilt $s_0 h(\beta_0) \equiv 1 \bmod \mathfrak{q}$. Wir nehmen nun an, daß das Ergebnis für fest gewähltes $i > 0$ bewiesen ist und zeigen, daß die Behauptung auch für

$i+1$ gilt:

$$\begin{aligned} 1 - s_{i+1}h(\beta_0) &\equiv 1 - (2s_i - h(\beta_0)s_i^2)h(\beta_0) \bmod \mathfrak{q}^{2^{i+1}} \\ &\equiv 1 - 2s_ih(\beta_0) - h(\beta_0)^2 s_i^2 \bmod \mathfrak{q}^{2^{i+1}} \\ &\equiv (1 - s_ih(\beta_0))^2 \bmod \mathfrak{q}^{2^{i+1}} \\ &\equiv 0 \bmod \mathfrak{q}^{2^{i+1}} \end{aligned}$$

□

1.32. Algorithmus. *(Quadratisches Newton-Lifting)*

Eingabe: *Ein Polynom $g(x) \in R[x]$ eines kommutativen Rings R mit Eins, ein Ideal $\mathfrak{q} \subset R$, $\beta_0 \in R$ mit $g(\beta_0) \equiv 0 \bmod \mathfrak{q}$ und $g'(\beta_0)$ ist invertierbar modulo $\mathfrak{q}$, $k \in \mathbb{Z}_{>0}$.*

Ausgabe: *$\beta_k \in R$ mit $g(\beta_k) \equiv 0 \bmod \mathfrak{q}^k$ und $\beta_k \equiv \beta_0 \bmod \mathfrak{q}$.*

1. *(Inverses von $g'(\beta_0) \bmod \mathfrak{q}$) Berechne $s_0 \in R$ mit $s_0 g'(\beta_0) \equiv 1 \bmod \mathfrak{q}$.*
2. *(Schleife über i) Setze $r := \lceil \log_2(k) \rceil$. Für $1 \leq i < r$ berechne $\beta_i, s_i \in R$ mit*
   (1) $\beta_i \equiv \beta_{i-1} - g(\beta_{i-1})s_{i-1} \bmod \mathfrak{q}^{2^i}$
   (2) $s_i \equiv s_{i-1}(2 - g'(\beta_i)s_{i-1}) \bmod \mathfrak{q}^{2^i}$
3. *(Ende) Berechne $\beta_r \in R$ mit $\beta_r \equiv \beta_{r-1} - g(\beta_{r-1})s_{r-1} \bmod \mathfrak{q}^{2^r}$. Ausgabe von $\beta_k = \beta_r$. Terminiere.*

1.33. Bemerkung. Da es sich in unseren Anwendungen immer um ein maximales Ideal $\mathfrak{q}$ eines kommutativen Rings R mit Eins handelt, für welches $\operatorname{disc}(g) \notin \mathfrak{q}$ ist, können wir in Schritt 1 das Element s_0 mittels des erweiterten euklidischen Algorithmus für Polynome (g, g') über dem Körper $R/\mathfrak{q}$ bestimmen.

Kapitel 2

Galoisgruppenberechnung

In diesem und den folgenden Kapiteln werden wir einen Algorithmus zur Berechnung von Galoisgruppen für Polynome über algebraischen Zahlkörpern und algebraischen Funktionenkörpern in einer Variablen über $\mathbb{Q}$ und endlichen Körpern beschreiben. Der Algorithmus basiert auf dem von Stauduhar [78] vorgestellten Verfahren zur Berechnung der Galoisgruppe eines irreduziblen Polynoms mit ganzrationalen Koeffizienten und wird in erweiterter Form mit einer Variante der absoluten Resolventenmethode (vgl. McKay, Soicher [58]) kombiniert. Das hier vorgestellte Verfahren ist eine Weiterentwicklung der Methoden aus [29], wobei diese an mehreren Stellen um Größenordnungen verbessert werden konnten.

2.1 Das Verfahren von Stauduhar

Ziel dieses Abschnitts ist es, die wesentlichen Komponenten des Verfahrens von Stauduhar bereitzustellen. Das Verfahren von Stauduhar basiert im wesentlichen auf sogenannten Resolventen. Das sind Polynome $R(X) \in K[X]$, deren Zerfällungskörper ein Teilkörper des Zerfällungskörpers des Polynoms $f(x) \in K[x]$ ist, dessen Galoisgruppe wir bestimmen wollen.

2.1.1 Die Idee des Verfahrens

Sei R ein Integritätsring (mit Eins) mit Quotientenkörper K. R sei ganzabgeschlossen in K und $f(x) \in R[x]$ ein normiertes, separables, irreduzibles Polynom vom Grad n. Darüber hinaus bezeichnen wir die Nullstellen von f in einem Zerfällungskörper $N(f, K)$ mit $\alpha_1, \ldots, \alpha_n$. Eine Grundmotivation für das Verfahren von Stauduhar und die dort verwendeten Resolventen liefert die Betrachtung von rationalen (symmetrischen) Funktionenkörpern. Sei $L := K(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen und bezeichne $M := K(s_1, \ldots, s_n)$ den Körper

der rationalen symmetrischen Funktionen, wobei die s_i für $1 \leq i \leq n$ die elementarsymmetrischen Funktionen in den Unbestimmten $x_1, \ldots, x_n$ sind. Für transitive Permutationsgruppen $H \leq G \leq S_n$,, welche auf der Menge $\{x_1, \ldots, x_n\}$ durch Permutation der Indizes operieren, sei folgende Situation gegeben:

$$\begin{array}{ccc} L = K(x_1, \ldots, x_n) & \longleftrightarrow & \{\mathrm{id}\} \\ \cup & & \cap \\ Fix(L, H) & \longleftrightarrow & H \\ \cup & & \cap \\ Fix(L, G) & \longleftrightarrow & G \\ \cup & & \cap \\ M = K(s_1, \ldots, s_n) & \longleftrightarrow & G(L/M) \cong S_n \end{array} \tag{2.1}$$

Da L/M eine Galoiserweiterung ist, ist die Erweiterung der Fixkörper $Fix(L, H)/Fix(L, G)$ endlich und separabel. Nach dem Satz vom primitiven Element existiert somit ein primitives Element $F \in Fix(L, H)$ mit $Fix(L, H) = Fix(L, G)(F)$. Es ist immer möglich F ganzalgebraisch über $K[s_1, \ldots, s_n]$ zu wählen: Multiplikation mit dem k.g.V. der Nenner des Minimalpolynoms von F über $K(s_1, \ldots, s_n)$ ergibt ein ganzalgebraisches Element. Da der faktorielle Ring $K[x_1, \ldots, x_n]$ ganz abgeschlossen in seinem Quotientenkörper ist, folgt, daß F ein Element von $K[x_1, \ldots, x_n]$ ist. Durch Multiplikation mit einem Skalar aus R können wir sogar erreichen, daß F ein Element aus $R[x_1, \ldots, x_n]$ ist.

Wir nehmen nun zusätzlich an, daß die Galoisgruppe von f, als Permutationsgruppe betrachtet, eine Untergruppe von G ist. Dann gilt

$$\mathcal{G}(f, K) \leq H \Longleftrightarrow \sigma F = F \text{ für alle } \sigma \in \mathcal{G}(f, K).$$

Wertet man $F(x_1, \ldots, x_n)$ an den Nullstellen $\alpha_1, \ldots, \alpha_n \in N(f, K)$ von f aus, so folgt

$$\mathcal{G}(f, K) \leq H \Longrightarrow F(\alpha_1, \ldots, \alpha_n) \in K \text{ bzw. } \in R.$$

Um die umgekehrte Richtung zu beweisen, d.h. um zeigen zu können, daß aus $F(\alpha_1, \ldots, \alpha_n) \in K$ bzw. $\in R$ folgt, daß $\mathcal{G}(f, K) \leq H$ ist, müssen wir zusätzlich annehmen, daß für alle $\sigma \in G$ gilt:

$$\sigma F \neq F \Longrightarrow \sigma F(\alpha_1, \ldots, \alpha_n) \neq F(\alpha_1, \ldots, \alpha_n)$$

Dann können wir schließen, daß

$$\mathcal{G}(f, K) \leq H \Longleftrightarrow F(\alpha_1, \ldots, \alpha_n) \in K \text{ bzw. } \in R.$$

Die letzte Äquivalenz ist die zentrale Aussage, auf der der Algorithmus von Stauduhar beruht. Unter Voraussetzung der Kenntnis geeigneter primitiver Elemente

für alle Gruppenpaare $H < G \leq S_n$ lautet eine vereinfachte Form des Algorithmus: Angenommen $\mathcal{G}(f, K) \leq G$ für eine transitive Untergruppe G von S_n bezüglich der gewählten Anordnung der Nullstellen des Polynoms f. Dies ist aufgrund der Irreduzibilität und Separabilität von f für S_n immer erfüllt. Unter Benutzung der letzten Äquivalenz läßt sich bestimmen, ob $\mathcal{G}(f, K) \leq H$ für eine maximale transitive Untergruppe H von G gilt. Ist $\mathcal{G}(f, K)$ in keiner maximalen transitiven Untergruppe H von G enthalten, so folgt $\mathcal{G}(f, K) = G$. Ansonsten gilt $\mathcal{G}(f, K) \leq H$, und wir setzen $G := H$ und wiederholen den Vorgang. Hierbei spielt die Wahl der Gruppe H keine Rolle, da aus $\mathcal{G}(f, K) \leq H_1$ und $\mathcal{G}(f, K) \leq H_2$ folgt, daß $\mathcal{G}(f, K) \leq H_1 \cap H_2$ gilt. Folglich durchläuft der Algorithmus das Untergruppengitter der transitiven Permutationsgruppen vom Grad n von der größten Gruppe bis zur aktuellen Galoisgruppe. Auf das Körperdiagramm (2.1) bezogen bedeutet dies, daß das Verfahren den Fixkörper $Fix(L, \mathcal{G}(f, K))$, dessen Bild unter Einsetzung der Nullstellen gleich K ist, von unten ausschöpft.

Diese vereinfachte Darstellung des Algorithmus beinhaltet natürlich noch einige Ineffizienzen. So ist zum Beispiel eine solche Vorgehensweise in der Praxis aufgrund der großen Anzahl der zu betrachtenden Gruppenpaare und der damit verbundenen Kenntnis primitiver Elemente für jedes dieser Gruppenpaare nicht sinnvoll. In den nächsten Abschnitten werden wir darauf eingehen.

2.1.2 Die Resolvente

Kehren wir zu der Ausgangssituation des Körperdiagramms (2.1) zurück. Die primitive Element Eigenschaft von F ist äquivalent zu der Tatsache, daß $\mathrm{Stab}_G(F) = \{\sigma \in G \,|\, \sigma F = F\} = H$ ist. Darüber hinaus ist das Minimalpolynom von F über $Fix(L, G)$ durch $\prod_{\sigma \in G//H}(x - \sigma F)$ gegeben, wobei $G//H$ ein vollständiges System von linken Nebenklassenrepräsentanten ist. Wir bezeichnen das Minimalpolynom von F auch als *generische relative Resolvente* von G und H bezüglich F. Dies führt nun zu der für das Verfahren wichtigen Definition von G-relativen H-invarianten Resolventenpolynomen. Sie sind gerade die spezialisierten generischen Resolventen.

2.2. Definition. Seien $H < G \leq S_n$ Permutationsgruppen, welche durch Permutation der Indizes auf der Menge $\{x_1, \ldots, x_n\}$ operieren und $F \in K[x_1, \ldots, x_n]$. Gilt

$$\mathrm{Stab}_G(F) = \{\sigma \in G \,|\, \sigma F = F\} = H,$$

so nennen wir das Polynom F ein G-relatives H-invariantes Polynom. In diesem Fall bezeichnen wir

$$R_{(G,H,F)}(X) := \prod_{\sigma \in G//H} (X - (\sigma F)(\alpha_1, \ldots, \alpha_n))$$

als das korrespondierende G-relative H-invariante Resolventenpolynom. Ist $G = S_n$, so nennen wir $R_{(G,H,F)}$ auch absolute Resolvente.

2.3. Bemerkung. (*i*) Für jedes Gruppenpaar $H < G \leq S_n$ folgt die Existenz eines Polynoms (primitiven Elements) $F \in K[x_1, \ldots, x_n]$ mit $\mathrm{Stab}_G(F) = H$ aus der Endlichkeit und Separabilität der Erweiterung $Fix(L, H)$ über $Fix(L, G)$ in (2.1). Für konstruktive Aussagen verweisen wir auf Kapitel 6, Sektion 6.1.

(*ii*) In der Situation von Definition 2.2 ist σF ein G-relatives $\sigma H \sigma^{-1}$-invariantes Polynom für $\sigma \in G$. In diesem Fall bezeichnen wir σF auch als konjugiertes Polynom von F. Darüber hinaus gibt es genau $[\,G : H\,]$ viele paarweise verschiedene konjugierte Polynome σF bezüglich der Permutationen aus G, da $\sigma_1 F = \sigma_2 F \Leftrightarrow \sigma_1 H = \sigma_2 H$ für $\sigma_1, \sigma_2 \in G$.

(*iii*) Die Resolvente $R_{(G,H,F)}$ hängt im allgemeinen von der gewählten Anordnung der Nullstellen α_i für $1 \leq i \leq n$ ab. Ausnahmen hiervon sind absolute Resolventen deren Koeffizienten symmetrische Funktionen der Nullstellen von f sind. Andererseits ist das Resolventenpolynom $R_{(G,H,F)}$ nicht von der Gruppe H, sondern nur von der G-Konjugationsklasse von H in G abhängig: Ist $\sigma \in G$, so ist $R_{(G,H,F)}$ auch ein G-relatives $\sigma H \sigma^{-1}$-invariantes Resolventenpolynom für σF (vgl. auch Satz 2.8).

Fassen wir nun die Ergebnisse aus Abschnitt 2.1.1 in bezug auf die Resolventenpolynome zusammen, so erhalten wir den zentralen Satz für das Verfahren von Stauduhar.

2.4. Satz. *Sei $f(x) \in R[x]$ ein normiertes, separables, irreduzibles Polynom vom Grad n und $\alpha_1, \ldots, \alpha_n \in N(f, K)$ eine fest gewählte Anordnung der Nullstellen von f. Sei G eine transitive Untergruppe von S_n, so daß für die Galoisgruppe $\mathcal{G}(f, K)$ von f gilt: $\mathcal{G}(f, K) \leq G$. Sei H eine Untergruppe von G und $F(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ ein G-relatives H-invariantes Polynom und $R_{(G,H,F)}$ das korrespondierende Resolventenpolynom. Dann gilt*

(i) $R_{(G,H,F)}(X) = \prod_{\sigma \in G//H} (X - \sigma F(\alpha_1, \ldots, \alpha_n)) \in R[X]$.

(ii) Sei $Q(X) = \prod_{i=1}^{l} (X - \sigma_i F(\alpha_1, \ldots, \alpha_n))$ ein Faktor von $R_{(G,H,F)}$, so daß Q und $R_{(G,H,F)}/Q$ teilerfremd sind, und sei $S := \mathrm{Stab}_G(\{\sigma_1 F, \ldots, \sigma_l F\})$. Dann ist $\mathcal{G}(f, K) \leq S$ genau dann, wenn $Q(X) \in R[X]$ („$\Rightarrow$“ gilt auch ohne die Bedingung teilerfremd).

(iii) Ist insbesondere $\sigma F(\alpha_1, \ldots, \alpha_n)$ eine einfache Nullstelle von $R_{(G,H,F)}$, dann gilt $\mathcal{G}(f, K) \leq \sigma H \sigma^{-1}$ genau dann, wenn $\sigma F(\alpha_1, \ldots, \alpha_n)$ ein Element in R ist.

(iv) Sei $\sigma F(\alpha_1, \ldots, \alpha_n) \in R$ eine einfache Nullstelle der Resolvente $R_{(G,H,F)}$, so daß $\mathcal{G}(f,K) \leq \sigma H \sigma^{-1}$ ist. Ordnet man die Nullstellen von f so an, daß $\alpha'_j = \alpha_{\sigma(j)}$ gilt, so ist $F(\alpha'_1, \ldots, \alpha'_n) \in R$ und aufgrund der neuen Anordnung gilt $\mathcal{G}(f,K) \leq H$.

Beweis. (i) Die Koeffizienten von $R_{(G,H,F)}(X)$ werden von G und folglich auch von $\mathcal{G}(f,K)$ fixiert, deshalb muß $R_{(G,H,F)}(X) \in K[X]$ gelten. Da aber die Koeffizienten von $R_{(G,H,F)}(X)$ gleichzeitig ganzalgebraisch über R sind und nach Voraussetzung R ganzabgeschlossen in seinem Quotientenkörper K ist, erhalten wir $R_{(G,H,F)}(X) \in R[X]$.

(ii) Sei zunächst $\mathcal{G}(f,K) \leq S$ vorausgesetzt. Dann folgt, daß die Menge $\{\sigma_1 F(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_l F(\alpha_1, \ldots, \alpha_n)\}$ von $\mathcal{G}(f,K)$ invariant gelassen wird. Wie in Teil (i) erhalten wir $Q[X] \in R[X]$.

Umgekehrt sei nun $Q[X] \in R[X]$ gegeben, so daß $Q(X)$ und $R_{(G,H,F)}/Q$ teilerfremd sind, und sei $r := [\,G\!:\!H\,]$. Wir setzen $\sigma_1, \ldots, \sigma_l$ zu einem vollständigen System $\sigma_1, \ldots, \sigma_r$ von Nebenklassenrepräsentanten fort. Ist nun $Q(X) \in R[X]$ und $\tau \in \mathcal{G}(f,K)$, so gilt für $1 \leq i \leq l$, daß $\tau(\sigma_i F) = \sigma_j F$, wobei $j \in \{1, \ldots, r\}$. Da $Q(X) \in R[X]$ ist, folgt $\tau(\sigma_i F(\alpha_1, \ldots, \alpha_n)) = \sigma_k F(\alpha_1, \ldots, \alpha_n)$ mit $k \in \{1, \ldots, l\}$. Damit haben wir $\sigma_k F(\alpha_1, \ldots, \alpha_n) = \sigma_j F(\alpha_1, \ldots, \alpha_n)$, und aufgrund der Teilerfremdheit von Q und $R_{(G,H,F)}/Q$ folgt, daß auch $j \in \{1, \ldots, l\}$ ist.

(iii) Da $\mathrm{Stab}_G(\sigma F) = \sigma H \sigma^{-1}$ ist, folgt die Behauptung aus Teil (ii) für $l = 1$.

(iv) Bezüglich der gewählten Anordnung gilt $\mathcal{G}(f,K) \leq \sigma^{-1} H \sigma$. Änderung der Anordnung durch eine Permutation σ hat die Konjugation der Gruppe $\mathcal{G}(f,K)$ mit σ zur Folge. Wir erhalten somit bezüglich der neuen Anordnung $\mathcal{G}(f,K) \leq H$. Das G-relative H-invariante Polynom bezüglich der neuen Anordnung verhält sich wie das G-relative $\sigma H \sigma^{-1}$-invariante Polynom bezüglich der alten Anordnung. Da $F(\alpha'_1, \ldots, \alpha'_n) = \sigma F(\alpha_1, \ldots, \alpha_n)$ ist, folgt $F(\alpha'_1, \ldots, \alpha'_n) \in R$. □

2.5. Bemerkung. (i) Wird in Satz 2.4 die Voraussetzung der Transitivität an $G \leq S_n$ fallengelassen, so gelten die Aussagen für normierte, separable (und nicht notwendigerweise irreduzible) Polynome $f(x) \in R[x]$.

(ii) Unter Beachtung von 2.4 (iii) ist eine entscheidende Voraussetzung für den Algorithmus, daß eine der folgenden Situationen eintritt: Es existiert eine einfache Nullstelle der Resolvente in R oder die Resolvente hat keine Nullstelle in R. Durch Transformation des Ausgangspolynoms f ist es für Körper K mit unendlich vielen Elementen immer möglich eine Resolvente mit paarweise verschiedenen Nullstellen zu erhalten. Wir verweisen auf Abschnitt 2.1.3.

(iii) Offen ist an dieser Stelle, wie die Nullstellenberechnung und der Inklusionstest $\sigma F(\alpha_1, \ldots, \alpha_n) \in R$ konkret durchzuführen sind. Dies wird für algebraische

Zahlkörper in Kapitel 3 und für algebraische Funktionenkörper in einer Variablen über $\mathbb{Q}$ und endlichen Körpern in Kapitel 4 beschrieben.

(*iv*) Mittels Bedingung (*iv*) aus Satz 2.4 wird während des Algorithmus zu jedem Zeitpunkt durch Umordnung der Nullstellen gesichert, daß die Galoisgruppe als Permutationsgruppe betrachtet eine direkte Untergruppe einer transitiven Untergruppe der S_n ist, wie sie z.B. in MAGMA [5, 16] bis Grad 23 oder Conway et al. [18] bis Grad 15 vorgegeben wird. Dies ist besonders wichtig, da beim Verfahren von Stauduhar einige Daten bezüglich eines fest gewählten Vertretersystems der S_n-Konjugationsklassen transitiver Gruppen vorberechnet werden.

Für spätere Anwendungen ist die folgende Verallgemeinerung von Satz 2.4 von Interesse.

2.6. Satz. *Sei $f(x) \in R[x]$ ein normiertes, separables, irreduzibles Polynom vom Grad n und $\alpha_1, \ldots, \alpha_n \in N(f,K)$ eine fest gewählte Anordnung der Nullstellen von f. Sei G eine transitive Untergruppe von S_n, so daß $\mathcal{G}(f,K) \leq G$ ist. Sei $F(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ und $\mathcal{O} \subseteq \mathrm{Orb}_{S_n}(F)$, so daß $F \in \mathcal{O}$ und $\mathrm{Orb}_G(\mathcal{O}) \subseteq \mathcal{O}$. Bezeichne $\tau : G \longrightarrow S_{|\mathcal{O}|}$ die Permutationsdarstellung von G, welche durch Operation von G auf der Menge $\mathcal{O}$ gegeben ist. Sei H eine Untergruppe von G mit $\mathrm{Orb}_H(F) \subsetneq \mathrm{Orb}_G(F)$. Dann gilt:*

(i) $\mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F)) \lneqq \tau(G)$.

(ii) Ist der Faktor $Q(X) = \prod_{\sigma \in \tau(H)//\mathrm{Stab}_{\tau(H)}(F)} (X - (\sigma F)(\alpha_1, \ldots, \alpha_n))$ der Resolvente $T(X) = \prod_{\sigma \in \tau(G)//\mathrm{Stab}_{\tau(G)}(F)} (X - (\sigma F)(\alpha_1, \ldots, \alpha_n))$ teilerfremd zu T/Q, so gilt die Äquivalenz:

$$Q(X) \in R[X] \Longleftrightarrow \tau(\mathcal{G}(f,K)) \leq \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F)).$$

Beweis. (*i*) Nach Definition des Stabilisators gilt zunächst $\mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F)) \leq \tau(G)$. Da $\mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_G(F)) = \tau(G)$ und $\mathrm{Orb}_H(F) \subsetneq \mathrm{Orb}_G(F)$ nach Voraussetzung ist, kann $\mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F)) = \tau(G)$ nicht gelten.

(*ii*) Sei zunächst $\tau(\mathcal{G}(f,K)) \leq \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F))$ vorausgesetzt. Wir bemerken, daß $\mathrm{Orb}_H(F) = \{\sigma F \,|\, \sigma \in \tau(H)//\mathrm{Stab}_{\tau(H)}(F)\}$ gilt. Es folgt, daß die Menge $\{(\sigma F)(\alpha_1, \ldots, \alpha_n) \,|\, \sigma \in \tau(H)//\mathrm{Stab}_{\tau(H)}(F)\}$ von $\tau(\mathcal{G}(f,K))$ und somit von $\mathcal{G}(f,K)$ invariant gelassen wird. $Q(X)$ hat folglich Koeffizienten in K und da die $(\sigma F)(\alpha_1, \ldots, \alpha_n)$, $\sigma \in \tau(H)//\mathrm{Stab}_{\tau(H)}(F)$ ganzalgebraisch über R sind, erhalten wir $Q[X] \in R[X]$.

Sei nun $Q[X] \in R[X]$ gegeben, so daß Q und T/Q teilerfremd sind, und sei $l := [\,\tau(H) : \mathrm{Stab}_{\tau(H)}(F)\,]$ und $r := [\,\tau(G) : \mathrm{Stab}_{\tau(G)}(F)\,]$. Wir setzen die $\sigma_1, \ldots, \sigma_l \in$

$\tau(H)//\mathrm{Stab}_{\tau(H)}(F)$ zu einem Nebenklassenrepräsentantensystem $\sigma_1, \ldots, \sigma_r$ von $\tau(G)//\mathrm{Stab}_{\tau(G)}(F)$ fort. Dies ist möglich, da $\sigma_i\mathrm{Stab}_{\tau(H)}(F) \neq \sigma_j\mathrm{Stab}_{\tau(H)}(F) \Leftrightarrow \sigma_i\mathrm{Stab}_{\tau(G)}(F) \neq \sigma_j\mathrm{Stab}_{\tau(G)}(F)$, $(i \neq j)$ ist: Wäre nämlich $\sigma_i\sigma_j^{-1} \notin \mathrm{Stab}_{\tau(H)}(F)$ und $\sigma_i\sigma_j^{-1} \in \mathrm{Stab}_{\tau(G)}(F)$, so würde $\sigma_i\sigma_j^{-1} \in \tau(H) \cap \mathrm{Stab}_{\tau(G)}(F) = \mathrm{Stab}_{\tau(H)}(F)$ gelten. Der Rest des Beweises folgt analog zum Beweis von Satz 2.4 (ii). □

2.7. Korollar. *Es gelten die Voraussetzungen von Satz 2.6. Ist die Permutationsdarstellung $\tau : G \longrightarrow S_{|\mathcal{O}|}$ treu und H eine maximale transitive Untergruppe von G, so ist $\tau(H) = \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F))$, und es gilt:*

$$Q(X) \in R[X] \Longleftrightarrow \mathcal{G}(f, K) \leq H.$$

Beweis. Da $\tau(H) = \mathrm{Stab}_{\tau(H)}(\mathrm{Orb}_H(F))$ ist, muß $\tau(H) \leq \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F))$ gelten. Wäre $\tau(H) \lneqq \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F))$, so würde aufgrund der Injektivität von τ und Satz 2.6 (i) $H \lneqq \mathrm{Stab}_G(\mathrm{Orb}_H(F)) \lneqq G$ sein, im Widerspruch zur Maximalität von H in G. Nach Satz 2.6 ist $Q(X) \in R[X]$ somit äquivalent zur Bedingung $\tau(\mathcal{G}(f, K)) \leq \mathrm{Stab}_{\tau(G)}(\mathrm{Orb}_H(F)) = \tau(H)$, und aufgrund der Injektivität von τ folgt die Behauptung. □

Kehren wir zurück zur vereinfachten Beschreibung des Algorithmus. Eine Ineffizienz dieses Verfahrens lag darin, daß für jede maximale Untergruppe H von G und somit a priori für jedes Element der Menge $\mathcal{C}_{S_n}(G, H) := \{\, \tau H\tau^{-1} \,|\, \tau \in S_n \text{ und } \tau H\tau^{-1} < G \,\}$ ein invariantes Polynom benötigt wird. Nach Bemerkung 2.3 (ii) sind bei Kenntnis eines G-relativen H-invarianten Polynoms F auch gleich G-relative $\sigma H\sigma^{-1}$-invariante Polynome bekannt für $\sigma \in G\backslash H$. Da es nach 2.3 (ii) genau $[\, G\!:\!H \,]$ viele verschiedene Polynome σF bezüglich der Permutationen $\sigma \in G$ gibt, können wir durch Hinzunahme einer Menge von Nebenklassenrepräsentanten (d.h. durch Betrachtung aller Nullstellen der Resolvente) entscheiden, ob die Galoisgruppe $\mathcal{G}(f, K)$ in H oder in einer G-konjugierten Gruppe von H enthalten ist. Dies bedeutet bezüglich der Menge der zu betrachtenden maximalen Untergruppen von G nichts anderes als eine Unterteilung in G-Konjugationsklassen. Somit verbleibt der Fall, daß wir Vertreter zweier S_n-Konjugationsklassen gegeben haben, die maximal in G sind, aber nicht in G zueinander konjugiert sind. Für maximale Untergruppen H_1, H_2, die in derselben $N_{S_n}(G)$-Konjugationsklasse liegen, gilt jedoch der folgende Satz (vgl. Eichenlaub, Olivier [23], Proposition 4)

2.8. Satz. *Sind H_1 und H_2 zwei Untergruppen von G, die in $N_{S_n}(G)$ zueinander konjugiert sind, d.h. $H_2 = \tau H_1\tau^{-1}$, $\tau \in N_{S_n}(G)$ und $F \in R[x_1, \ldots, x_n]$ein G-relatives H_1-invariantes Polynom. Dann gilt*

(i) τF ist ein G-relatives H_2-invariantes Polynom.

(ii) $R_{(G,H_2,\tau F)} = \prod_{\sigma \in G//H_1} (X - \tau\sigma F(\alpha_1, \ldots, \alpha_n))$.

Ist insbesondere τ *in* G*, so gilt* $R_{(G,H_2,\tau F)} = R_{(G,H_1,F)}$.

Nach Satz 2.8 genügt für alle maximalen Untergruppen H von G, die bezüglich eines Elements $\tau \in N_{S_n}(G)$ zueinander konjugiert sind, die Kenntnis genau eines G-relativen H-invarianten Polynoms F. Da $N_{S_n}(G)$ durch Konjugation auf der Menge $\mathcal{C}_{S_n}(G,H)$ operiert, bedeutet dies nichts anderes als die Kenntnis eines invarianten Polynoms für jede Bahn von $\mathcal{C}_{S_n}(G,H)$ unter den Permutationen von $N_{S_n}(G)$. Die Bahn eines Elements $\tau H \tau^{-1} \in \mathcal{C}_{S_n}(G,H)$ unter $N_{S_n}(G)$ ist gerade die Konjugationsklasse von $\tau H \tau^{-1}$ bezüglich den Permutationen aus $N_{S_n}(G)$.

2.9. Bemerkung. In der Praxis haben wir bis Grad 23 berechnet, daß mit Ausnahme von Grad 16 maximale transitive Untergruppen von $G \leq S_n$, welche in der symmetrischen Gruppe S_n zueinander konjugiert sind, dies schon in $N_{S_n}(G)$ sind. Für Grad 16 lassen sich insgesamt 26 Gruppen G finden, die maximale transitive Untergruppen haben, die nicht in $N_{S_n}(G)$ zueinander konjugiert sind, nämlich

$16T_{31}^{+}/16T_{8}^{+}$	$16T_{96}^{+}/16T_{21}^{+}$	$16T_{110}^{+}/16T_{15}^{+}$	$16T_{115}^{+}/16T_{19}^{+}$	$16T_{115}^{+}/16T_{34}^{+}$
$16T_{151}^{+}/16T_{40}^{+}$	$16T_{169}^{+}/16T_{53}^{+}$	$16T_{383}^{+}/16T_{88}^{+}$	$16T_{412}^{+}/16T_{90}^{+}$	$16T_{494}^{+}/16T_{384}^{+}$
$16T_{497}^{+}/16T_{368}^{+}$	$16T_{497}^{+}/16T_{383}^{+}$	$16T_{603}^{+}/16T_{267}^{+}$	$16T_{628}^{+}/16T_{318}^{+}$	$16T_{635}^{+}/16T_{412}^{+}$
$16T_{638}^{+}/16T_{312}^{+}$	$16T_{640}^{+}/16T_{307}^{+}$	$16T_{640}^{+}/16T_{412}^{+}$	$16T_{647}^{+}/16T_{383}^{+}$	$16T_{656}^{+}/16T_{295}^{+}$
$16T_{784}^{+}/16T_{635}^{+}$	$16T_{784}^{+}/16T_{640}^{+}$	$16T_{793}^{+}/16T_{497}^{+}$	$16T_{793}^{+}/16T_{647}^{+}$	$16T_{801}^{+}/16T_{632}^{+}$
$16T_{1330}^{+}/16T_{1209}^{+}$				

Tabelle 2.1: Transitive Gruppen G mit maximalen Untergruppen vom Gruppentyp T_i, deren G-Konjugationsklassen nicht in $N_{S_n}(G)$, $(n \leq 23)$ zueinander konjugiert sind

Bei dem letzten Gruppenpaar wird die Menge $\mathcal{C}_{S_n}(G,H)$ unter den Permutationen von $N_{S_n}(G)$ in drei disjunkte Bahnen zerlegt, während alle anderen Gruppenpaare zwei $N_{S_n}(G)$-Bahnen besitzen. In allen Fällen genügt es somit zu einem transitiven Gruppenpaar $H < G \leq S_n$ zu jeder $N_{S_n}(G)$-Bahn von $\mathcal{C}_{S_n}(G,H)$ ein G-relatives H-invariantes Polynom F zu finden und eine Menge von Nebenklassenrepräsentanten $\sigma \in G//H$ zu berechnen. Für die nichttrivialen Bahnen $\mathrm{Orb}_G(\tau H \tau^{-1})$, d.h. $\mathrm{Orb}_G(\tau H \tau^{-1}) \neq \mathrm{Orb}_G(H)$ ist τF eine G-relative $\tau H \tau^{-1}$-Invariante. Hier muß also zusätzlich die Permutation τ mitberechnet werden.

Für den Fall $G = A_n, (n \geq 5)$ können wir konkrete Aussagen über die Anzahl der A_n-Bahnen von $\mathcal{C}_{S_n}(A_n,H)$ machen (vgl. [29], Korollar 3.3.5)

2.10. Korollar. *Sei* $n \geq 5$ *und* H *eine maximale transitive Untergruppe von* A_n*. Dann gilt*

(i) $\mathcal{C}_{S_n}(A_n, H) = \{\, \tau H \tau^{-1} \mid \tau \in S_n \,\}$,

(ii) *Ist* $N_{S_n}(H) = H$, *so gibt es genau zwei* A_n*-Bahnen von* $\mathcal{C}_{S_n}(A_n, H)$, *nämlich* $\mathrm{Orb}_{A_n}(H)$ *und* $\mathrm{Orb}_{A_n}(\tau H \tau^{-1})$, *wobei* τ *eine ungerade Permutation ist.*

(iii) *Für* $N_{S_n}(H) \neq H$ *ist* $\mathcal{C}_{S_n}(A_n, H) = \mathrm{Orb}_{A_n}(H)$.

Korollar 2.10 wird zur Vereinfachung der durchgeführten Berechnungen herangezogen. Wir beenden diesen Abschnitt mit einem Unterscheidungskriterium für gerade und ungerade Galoisgruppen.

2.11. Satz. *Für* $\mathrm{char}(K) \neq 2$ *gilt*

(i) $F = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ *ist ein* S_n*-relatives* A_n*-invariantes Polynom.*

(ii) $R_{(S_n, A_n, F)}(X) = X^2 - \mathrm{disc}(f)$, *wobei* $\mathrm{disc}(f) = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2$ *die Diskriminante von* f *ist.*

(iii) *Die Galoisgruppe* $\mathcal{G}(f, K)$ *ist genau dann eine Untergruppe der alternierenden Gruppe* A_n, *wenn die Diskriminante* $\mathrm{disc}(f)$ *des Polynoms* f *ein Quadrat eines Elements in* R *ist.*

Beweis. Für das spezielle Polynom F gilt für jede Permutation $\sigma \in S_n$, daß $\sigma F = \mathrm{sign}(\sigma) F$ ist. Damit ist klar, daß $\mathrm{Stab}_{S_n}(F) = A_n$ gilt. Für die zugehörige Resolvente folgt

$$\begin{aligned} R_{(S_n, A_n, F)}(X) &= (X - \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j))(X + \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)) \\ &= X^2 - \textstyle\prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2 \end{aligned}$$

Die Resolvente ist also von der Gestalt $R_{(S_n, A_n, F)}(X) = X^2 - \mathrm{disc}(f)$, und nach Satz 2.4 (i) hat das Resolventenpolynom Koeffizienten in R. Wir sehen auch, daß $R_{(S_n, A_n, F)}$ keine doppelten Nullstellen haben kann, da $\mathrm{disc}(f) \neq 0$ aufgrund der Separabilität und Irreduzibilität von f ist. Somit haben wir für $\mathrm{char}(K) \neq 2$ $\mathcal{G}(f, K) \leq A_n \Longleftrightarrow \mathrm{disc}(f)$ ist ein Quadrat in R. □

Da für $\mathrm{char}(K) = 2$ das Polynom F aus Satz 2.11 (i) eine symmetrische Funktion ist, gilt insbesondere $F(\alpha_1, \ldots, \alpha_n) \in R$ und die Diskriminante $\mathrm{disc}(f)$ ist immer ein Quadrat eines Elements aus R. Um in diesem Fall speziell zwischen der symmetrischen und der alternierenden Gruppe zu unterscheiden, gilt es ein S_n-relatives A_n-invariantes Polynom zu finden, welches sich nicht nur durch das Vorzeichen unterscheidet. Wir verweisen auf Bemerkung 6.5.

2.12. Bemerkung. (i) Das Resultat von Satz 2.11 kann sofort dahingehend verallgemeinert werden, daß im Fall $\mathrm{char}(K) \neq 2$ für jede ungerade Gruppe G und jede gerade Gruppe H oben genanntes F ein G-relatives H-invariantes Polynom und $R_{(G,H,F)}$ die zugehörige Resolvente ist.

(ii) Um bei dem Durchlauf durch das Untergruppengitter der S_n nicht alle Inklusionen betrachten zu müssen, teilen wir die transitiven Gruppen in drei Mengen ein: In die geraden imprimitiven Gruppen, die ungeraden imprimitiven Gruppen und die (geraden und ungeraden) primitiven Gruppen. Ob es sich bei einer Galoisgruppe $\mathcal{G}(f, K)$ um eine gerade oder ungerade Gruppe handelt, läßt sich für $\mathrm{char}(K) \neq 2$ sofort durch Betrachtung der Diskriminante ermitteln. Zum Beispiel gibt es im Fall $n = 3$ nur zwei transitive Gruppen, nämlich A_3 und S_3, welche ohne großen Rechenaufwand mittels Satz 2.11 unterschieden werden können. Da für größere Grade die Anzahl der primitiven transitiven Gruppen eher gering ist, sind nach Betrachtung der Diskriminante zuerst Tests bezüglich maximaler imprimitiver Gruppen sinnvoll. Erhält man hier keine Inklusionen, so handelt es sich bei der Galoisgruppe um eine primitive Gruppe. Im Fall $\mathrm{char}(K) = 2$ erweist es sich als sinnvoll, das Untergruppengitter der ungeraden (imprimitiven bzw. primitiven) Gruppen solange zu durchlaufen, bis von einer aktuellen ungeraden Gruppe G kein Abstieg mehr in eine maximale ungerade Untergruppe H möglich ist. Hat die Gruppe G maximale gerade Untergruppen, so sind diese auf Inklusion zu testen und anschließend das Untergruppengitter der geraden Gruppen in obiger Weise zu durchlaufen.

2.1.3 Separabilität

Wie das folgende Beispiel zeigt, wird es oft passieren, daß die Nullstellen des Resolventenpolynom in R ausschließlich mehrfache Nullstellen sind.

2.13. Beispiel. Sei $f(x) = x^7 - 2 \in \mathbb{Z}[x]$ und $G = S_7$. Die 1-dimensionale affine Gruppe $H = AGL(1, 7)$ des endlichen Körpers $\mathbb{F}_7$, welche aus allen Permutationen der Form $\xi \mapsto a\xi + b$ mit $a, b \in \mathbb{F}_7$, $a \neq 0$ besteht, hat die Ordnung 42 und ist maximale Untergruppe von S_7. Sei $F(x_1, \ldots, x_7) = x_1x_2x_4 + x_1x_2x_6 + x_1x_3x_4 + x_1x_3x_7 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_5 + x_2x_3x_7 + x_2x_4x_5 + x_2x_6x_7 + x_3x_4x_6 + x_3x_5x_6 + x_4x_5x_7 + x_4x_6x_7 \in \mathbb{Z}[x_1, \ldots, x_7]$. Der Stabilisator von F in S_7 ist die Gruppe $AGL(1, 7)$, wie man durch direktes Nachrechnen erhalten kann. Wir wählen $[\, S_7 : AGL(1, 7)\,] = 120$ Nebenklassenrepräsentanten von $AGL(1, 7)$ in S_7 und werten die Konjugierten von F an den Nullstellen des Polynoms f aus. Seien $\xi = \exp(2\pi i/7)$ primitive siebte Einheitswurzel und $\alpha_1 = \sqrt[7]{2}$, $\alpha_2 = \sqrt[7]{2}\xi^3$, $\alpha_3 = \sqrt[7]{2}\xi$, $\alpha_4 = \sqrt[7]{2}\xi^2$, $\alpha_5 = \sqrt[7]{2}\xi^4$, $\alpha_6 = \sqrt[7]{2}\xi^6$, $\alpha_7 = \sqrt[7]{2}\xi^5$ die Nullstellen des Poly-

noms f. Mit der gewählten Reihenfolge erhalten wir

$$\begin{aligned}(4,5,6)F(\alpha_1,\dots\alpha_7)&=0 & (2,5,4,7)F(\alpha_1,\dots,\alpha_7)&=0\\ (2,6)F(\alpha_1,\dots\alpha_7)&=0 & (2,5)(4,6,7)F(\alpha_1,\dots,\alpha_7)&=0\\ (2,4)(5,7,6)F(\alpha_1,\dots\alpha_7)&=0 & (2,6,5,4)F(\alpha_1,\dots,\alpha_7)&=0\\ (2,4)F(\alpha_1,\dots\alpha_7)&=0 & (2,7,5,6,4)F(\alpha_1,\dots,\alpha_7)&=0\end{aligned}$$

Somit ist Null achtfache Nullstelle der Resolvente in $\mathbb{Z}$; alle anderen Nullstellen liegen in $\mathbb{C}\backslash\mathbb{Q}$.

Um dennoch Satz 2.4 anwenden zu können, werden wir für Körper unendlicher Kardinalität zeigen, daß es durch sogenannte Tschirnhausentransformation immer möglich ist, eine Resolvente mit paarweise verschiedenen Nullstellen zu erhalten.

2.14. Definition. Sei $g \in K[x]$ ein normiertes, irreduzibles und separables Polynom vom Grad n und α eine Nullstelle von g. Eine Transformation des primitiven Elements α zu einem anderen primitiven Element $\beta = h(\alpha)$ mit $h(x) \in K[x]$ und $K(\alpha) = K(\beta)$ heißt Tschirnhausentransformation. Entsprechend sagt man, daß die zugehörigen Minimalpolynome m_α und m_β durch Tschirnhausentransformation ineinander übergehen.

2.15. Bemerkung. Sei $f = (x-\alpha_1)\cdots(x-\alpha_n)$ die Faktorisierung von f in $N(f,K)[x]$. Sind die Nullstellen des Polynoms ${}^h f := (x-h(\alpha_1))\cdots(x-h(\alpha_n))$, $h \in K[x]$ ebenfalls paarweise verschieden, so ist $h(\alpha_i)$, $(1 \le i \le n)$ primitives Element und ${}^h f$ durch Tschirnhausentransformation aus f hervorgegangen. Für die zugehörigen Galoisgruppen $G(f,K)$ und $G({}^h f,K)$ gilt die Gleichheit. Ist $G(f,K) \cong \mathcal{G}(f,K)$ bezüglich der fest gewählten Anordnung $\alpha_1,\dots,\alpha_n$, so folgt für die Anordnung $h(\alpha_1),\dots,h(\alpha_n)$ der Nullstellen von ${}^h f$, daß $G({}^h f,K) \cong \mathcal{G}(f,K)$ gilt. Das G-relative H-Resolventenpolynom von ${}^h f$ bezüglich des Polynoms $F(x_1,\dots,x_n)$ können wir auch als Resolvente von f bezüglich des Polynoms $F(h(x_1),\dots,h(x_n))$ auffassen. In diesem Sinne bedeutet eine Tschirnhausentransformation nichts anderes als der Übergang zu einem neuen G-relativen H-invarianten Polynom.

Eine Existenzaussage über die von uns gesuchten Tschirnhausentransformationen stellt der nächste Satz dar (vgl. Girstmair [31]).

2.16. Satz. *Sei $|K| = \infty$ und $R_{(G,H,F(x_1,\dots,x_n))}(X) = \prod_{\sigma\in G//H}(X - \sigma F(x_1,\dots,x_n))$ die Darstellung der generischen Resolvente in $K[x_1,\dots,x_n,X]$. Dann gibt es eine endliche Menge $H_n \subset K[X]$ mit der folgenden Eigenschaft: Zu jedem normierten, irreduziblen, separablen Polynom $f \in K[x]$ vom Grad n mit den Nullstellen $\alpha_1,\dots,\alpha_n \in \overline{K}$ existiert ein Polynom $h \in H_n$, so daß $R_{(G,H,F(h(\alpha_1),\dots,h(\alpha_n)))}$ und ${}^h f$ paarweise verschiedene Nullstellen in $\overline{K}$ haben.*

Beweis. Wir geben an dieser Stelle nur die Beweisidee an und verweisen für eine ausführliche Darstellung auf [29], Satz 3.4.2. Seien $[\,G\!:\!H\,] = m$ und die Elemente von $G//H$ mit σ_i, $(1 \leq i \leq m)$ bezeichnet. Die Bedingung der Separabilität ist erfüllt, wenn das Polynom

$$P(x_1, \ldots, x_n) := \prod_{1 \leq j < k \leq m} (\sigma_j F(x_1, \ldots, x_n) - \sigma_k F(x_1, \ldots, x_n)) \prod_{1 \leq i < l \leq n} (x_i - x_l).$$

ausgewertet an den Stellen $h(\alpha_1), \ldots, h(\alpha_n)$ ungleich Null ist. Ist $d \in \mathbb{Z}_{>0}$ größer als der Totalgrad des Polynoms $P(x_1, \ldots, x_n)$ und U eine d-elementige Teilmenge von K, so hat $H_n := \{\, \sum_{j=1}^{n} u_j X^{j-1} \,|\, u_1, \ldots, u_n \in U \,\}$ die gewünschte Eigenschaft. Die Koeffizienten von h lassen sich zu gegebenen $\alpha_1, \ldots, \alpha_n$ sukzessive aus der Menge U wählen, so daß die Separabilitätsbedingung erfüllt ist. □

2.17. Bemerkung. (i) Für beliebige Körper K mit unendlicher Kardinalität kann die Menge U immer als Teilmenge von R gewählt werden. Ist speziell $K = \mathbb{Q}$, ein algebraischer Zahlkörper oder ein algebraischer Funktionenkörper über $\mathbb{Q}$, so können wir uns auf Mengen $U \subseteq \mathbb{Z}$ beschränken. Für algebraische Funktionenkörper über endlichen Körpern $\mathbb{F}_q$ sind dagegen je nach Anzahl der Elemente von $\mathbb{F}_q$ nicht immer Tschirnhausentransformationen mit $U \subseteq \mathbb{F}_q$ möglich.

(ii) Aus dem Beweis von Satz 2.16 kann man obere Schranken für die maximale Anzahl verschiedener Tschirnhausentransformationen, die zur Erreichung von Separabilität erforderlich sind, ableiten. Diese Schranken sind allerdings wesentlich zu groß und damit nicht von praktischem Nutzen. In der Praxis führen meist schon ein bis zwei zufällige Tschirnhausentransformationen zum Erfolg. Um festzustellen, ob das Element $h(\alpha)$ für ein zufällig gewähltes Polynom $h(X) \in K[X]$ primitiv ist, genügt es die Separabilität des charakteristischen Polynoms $char_{h(\alpha)}$ zu überprüfen.

2.18. Proposition. *Es gelten die Voraussetzungen von Satz 2.4 und bezeichne $\{\sigma_1 \ldots, \sigma_r\}$ ein fest gewähltes Nebenklassenrepräsentantensystem von H in G. Sei $Q(X) = \prod_{i \in I}(X - (\sigma_i F)(\alpha_1, \ldots, \alpha_n))$ der Faktor der Resolvente, der aus allen Nullstellen von $R_{(G,H,F)}(X)$ in R besteht. Existiert nach endlich vielen Tschirnhausentransformationen bezüglich eines Polynom $h(X) \in R[X]$ eine einfache Nullstelle $(\sigma_{i_0} F)(h(\alpha_1), \ldots, h(\alpha_n))$, $(i_0 \in I)$ in R von $Q'(X) = \prod_{i \in I}(X - (\sigma_i F)(h(\alpha_1), \ldots, h(\alpha_n)))$, so gilt $\mathcal{G}(f, K) \leq \sigma_{i_0} H \sigma_{i_0}^{-1}$.*

Beweis. Nach Voraussetzung sind $Q(X)$ und $R_{(G,H,F)}(X)/Q(X)$ teilerfremd und nach Satz 2.4 (ii) gilt somit $\mathcal{G}(f, K) \leq \mathrm{Stab}_G(\{\sigma_i F \,|\, i \in I\})$. Wir nehmen nun an, daß nach endlich vielen Tschirnhausentransformationen $Q'(X)$ eine einfache Nullstelle $\gamma := (\sigma_{i_0} F)(h(\alpha_1), \ldots, h(\alpha_n))$ in R besitzt. Sei $J := \{j \in \{1, \ldots, r\} \,|\, (\sigma_j F)$

$(h(\alpha_1),\ldots,h(\alpha_n))=\gamma\}$. Dann sind $S'(X)=\prod_{j\in J}(X-(\sigma_jF)(h(\alpha_1),\ldots,h(\alpha_n)))$ und $R'(X)=R_{(G,H,F(h(X_1),\ldots,h(X_n)))}(X)/S'(X)$ teilerfremd und wiederum nach Satz 2.4 (ii) erhalten wir $\mathcal{G}(f,K)\leq \mathrm{Stab}_G(\{\sigma_jF\mid j\in J\})$. Somit folgt

$$\begin{aligned}\mathcal{G}(f,K) &\leq \mathrm{Stab}_G(\{\sigma_iF\mid i\in I\})\cap\mathrm{Stab}_G(\{\sigma_jF\mid j\in J\})\\ &= \mathrm{Stab}_G(\sigma_{i_0}F)=\sigma_{i_0}H\sigma_{i_0}^{-1}.\end{aligned}$$

□

Aufgrund der letzten Proposition brauchen wir nach einer Tschirnhausentransformation des Polynoms f nicht alle Nullstellen der neu erhaltenen Resolvente $R_{(G,H,F(h(X_1),\ldots,h(X_n)))}$ zu berechnen, sondern nur den Faktor, dessen Nullstellen zu den mehrfachen Nullstellen von $R_{(G,H,F)}$ in R korrespondieren. Diese Tatsache ist besonders für Abstiege im Untergruppengitter zwischen Gruppenpaaren mit großem Index von Bedeutung.

2.19. Bemerkung. In Beispiel 2.13 erhalten wir nach einer Tschirnhausentransformation von f mittels des Polynoms $h(X)=3X+2\in\mathbb{Z}[X]$ eine einfache Nullstelle $(2,5,4,7)F(h(\alpha_1),\ldots,h(\alpha_n))=1750\in\mathbb{Z}$ des Faktors der neuen Resolvente, der zu dem Faktor X^8 von $R_{(S_7,AGL(1,7),F)}(X)\in\mathbb{Z}[X]$ korrespondiert. Nach Vertauschung der Nullstellen bezüglich der Permutation $(2,5,4,7)$ folgt mit der neuen Anordnung $\alpha_1\leftarrow\alpha_1$, $\alpha_2\leftarrow\alpha_5$, $\alpha_3\leftarrow\alpha_3$, $\alpha_4\leftarrow\alpha_7$, $\alpha_5\leftarrow\alpha_4$, $\alpha_6\leftarrow\alpha_6$, $\alpha_7\leftarrow\alpha_2$, daß $\mathcal{G}(f,\mathbb{Q})\leq AGL(1,7)$ gilt. Die Diedergruppe $D(7)$ der Ordnung 14 ist die einzige maximale Untergruppe von $AGL(1,7)$. Da die zugehörige Resolvente keine Nullstellen in $\mathbb{Z}$ hat, erhalten wir $\mathcal{G}(x^7-2,\mathbb{Q})=AGL(1,7)$.

2.1.4 Zusammenfassung

Wir beenden dieses Kapitel mit einer Übersicht über die Daten, welche für jeden Grad für das Verfahren von Stauduhar berechnet werden müssen, und einem Algorithmus, der den Ablauf einer Galoisgruppenberechnung in einer Übersicht darstellt. Dabei werden die bisher behandelten Methoden eingeordnet.

Gegeben sei eine Liste $\mathcal{L}$ der Vertreter der S_n-Konjugationsklassen transitiver Gruppen. Folgende Aufgaben müssen für jedes $G\in\mathcal{L}$ bewältigt werden:

1. Berechne ein Repräsentantensystem $\mathcal{R}_G(G)$ der Menge der G-Konjugationsklassen maximaler transitiver Untergruppen von G.

2. Finde alle $T\in\mathcal{L}$, für die eine Permutation $\varrho\in S_n$ existiert, so daß $\varrho T\varrho^{-1}\in\mathcal{R}_G(G)$ ist. Dies ergibt die Menge $\mathcal{L}_G:=\{T_1,\ldots,T_k\}$. Für $i\in\{1,\ldots,k\}$ setze

$$\mathcal{R}_G(G,T_i):=\{H\in\mathcal{R}_G(G)\mid\text{es existiert }\varrho\in S_n\text{ mit }H=\varrho T_i\varrho^{-1}\}.$$

3. Sei $T_i \in \mathcal{L}_G$. Wir unterteilen $\mathcal{R}_G(G, T_i)$ in maximale, disjunkte Teilmengen von $N_{S_n}(G)$-konjugierten Gruppen und bilden die Menge $\mathcal{R}_{N_{S_n}(G)}(G, T_i)$ bestehend aus je einem Vertreter dieser Teilmengen. $\mathcal{R}_{N_{S_n}(G)}(G, T_i)$ ist somit ein Repräsentantensystem der Menge der $N_{S_n}(G)$-Konjugationsklassen maximaler transitiver Untergruppen von G vom transitiven Gruppentyp wie T_i. Für jeden Repräsentanten $H_{i,j} \in \mathcal{R}_{N_{S_n}(G)}(G, T_i)$ berechnen wir nun insgesamt folgende Daten,

   - eine Permutation $\varrho_{i,j} \in S_n$ mit $H_{i,j} = \varrho_{i,j} T_i \varrho_{i,j}^{-1}$,
   - eine Menge $\mathcal{P}(G, T_i, H_{i,j})$ von Permutationen aus $N_{S_n}(G)$, so daß für jedes im Normalisator $N_{S_n}(G)$ zu $H_{i,j}$ konjugierte $H \in \mathcal{R}_G(G, T_i)$ genau ein $\tau \in \mathcal{P}(G, T_i, H_{i,j})$ existiert mit $\tau H_{i,j} \tau^{-1} = H$,
   - ein Nebenklassenrepräsentantensystem $G//H_{i,j}$ und
   - ein G-relatives $H_{i,j}$-invariantes Polynom $F_{i,j}(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$.

4. Ist $G \neq S_n$, so berechne alle Zykeltypen von G.

Bezeichne $\mathcal{L}_u$ die Menge der ungeraden Gruppen und $\mathcal{L}_g$ die Menge der geraden Gruppen in $\mathcal{L}$. Wir kommen nun zu einer Übersicht des Verfahrens. Die gewählten Bezeichnungen der Daten werden, wenn nicht anders vermerkt, beibehalten.

2.20. Algorithmus. *(Galoisgruppenberechnung)*

Eingabe: *Ein normiertes, irreduzibles, separables Polynom $f(x) \in R[x]$ vom Grad n.*

Ausgabe: *Die Galoisgruppe von f, inklusive der zugehörigen Nullstellenanordnung.*

1. *(Grad von f?) Ist $n = 2$, so terminiere mit Ausgabe von $\mathcal{G}(f, K) \leftarrow S_2$ und einer beliebigen Nullstellenanordnung.*

2. *(Diskriminante?) Ist* $\mathrm{char}(K) = 2$ *oder* $\mathrm{disc}(f)$ *kein Quadrat in R, setze $G \leftarrow S_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_u$. Andernfalls setze $G \leftarrow A_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_g$. Ist $n = 3$ und* $\mathrm{char}(K) \neq 2$*, so terminiere mit Ausgabe von $\mathcal{G}(f, K) \leftarrow G$ und einer beliebigen Nullstellenanordnung.*

3. *(Faktorisierung* $\bmod \mathfrak{p}$*) Existieren Primideale $\mathfrak{p} \subset R$, so daß $R/\mathfrak{p}$ ein endlicher Körper ist und* $\mathrm{disc}(f) \notin \mathfrak{p}$ *gilt, so faktorisiere f modulo einiger solcher Primideale und setze $\mathcal{L}_z \leftarrow \{$ Menge aller Gruppen in $\mathcal{L}$, die mindestens ein Element der gegebenen Zykeltypen enthalten $\}$.*

4. *(Galoisgruppe gefunden?) Ist* $\mathrm{char}(K) \neq 2$ *und* $\tilde{\mathcal{L}} \cap \mathcal{L}_z = \{T\}$*, so terminiere mit Ausgabe von* $\mathcal{G}(f, K) \leftarrow T$ *und einer beliebigen Nullstellenanordnung.*

5. *(Nullstellenberechnung) Berechne Nullstellen* $\alpha_1, \ldots, \alpha_n$ *von* f*.*

6. *(Initialisierung der Kandidaten) Setze* $\tilde{\mathcal{L}_G} \leftarrow \mathcal{L}_G \cap \tilde{\mathcal{L}} \cap \mathcal{L}_z$*. Wenn* $\tilde{\mathcal{L}_G} = \emptyset$*, gehe zu Schritt 15.*

7. *(Schleife über maximale transitive Untergruppen) Für* $T_i \in \tilde{\mathcal{L}_G}$ *mache:*

8. *(Schleife über die Repräsentanten von* $\mathcal{R}_{N_{S_n}(G)}(G, T_i)$*) Für jedes in 2.1.4 3. für* G *und* T_i *erhaltene* $\varrho_{i,j} \in S_n$ *mache:*

9. *(Einlesen der Daten und Initialisierung) Setze* $H_{i,j} \leftarrow \varrho_{i,j} T_i \varrho_{i,j}^{-1} \leq G, \mathcal{C} \leftarrow G//H_{i,j}, F_{i,j} \leftarrow G$*-relatives* $H_{i,j}$*-invariantes Polynom und* $h(x) \leftarrow x$*.*

10. *(Schleife über die zu* $H_{i,j}$ *in* $N_{S_n}(G)$ *konjugierten Gruppen von* $\mathcal{R}_G(G, T_i)$*) Für alle* τ *in* $\mathcal{P}(G, T_i, H_{i,j})$ *mache:*

11. *(Nullstellen des Resolventenpolynoms) Berechne* $\tau\sigma F_{i,j}(h(\alpha_1), \ldots, h(\alpha_n))$ *für alle* $\sigma \in \mathcal{C}$*.*

12. *(Einfache, mehrfache oder keine Nullstellen in R?) Gibt es eine einfache Nullstelle in* R *und sind* τ, σ *die zugehörigen Permutationen, so setze* $\alpha_l \leftarrow \alpha_{\tau\sigma\varrho_{i,j}(l)}$ *für* $1 \leq l \leq n$*,* $G \leftarrow T_i$ *und gehe zu Schritt 7. Gibt es keine Nullstelle in* R*, so gehe zu Schritt 13. Ansonsten führe eine zufällige Tschirnhausentransformation mittels eines Polynoms* $\tilde{h}(x) \in R[x]$ *vom Grad* $\leq n-1$ *durch, setze* $\mathcal{C} \leftarrow \{\sigma \in \mathcal{C} \mid \tau\sigma F_{i,j}(h(\alpha_1), \ldots, h(\alpha_n)) \in R\}$*,* $h \leftarrow \tilde{h}$ *und gehe zu Schritt 11.*

13. *(Nächstes* τ*?) Wenn noch nicht alle* $\tau \in P(G, T_i, H_{i,j})$ *getestet wurden, setze* $\mathcal{C} \leftarrow G//H_{i,j}, h(x) \leftarrow x$ *und gehe zu Schritt 10.*

14. *(Nächster Repräsentant von* $\mathcal{R}_{N_{S_n}(G)}(G, T_i)$*?) Wenn noch nicht alle Repräsentanten von* $\mathcal{R}_{N_{S_n}(G)}(G, T_i)$ *getestet wurden, gehe zu Schritt 8.*

15. *(Nächstes* T_i*?) Gibt es noch nicht getestete maximale transitive Gruppen in* $\tilde{\mathcal{L}_G}$*, so gehe zu Schritt 7. Ist* $\mathrm{char}(K) = 2$ *und* $\tilde{\mathcal{L}} = \mathcal{L}_u$*, so setze* $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_g$ *und gehe zu Schritt 6. Sonst setze* $\mathcal{G}(f, K) \leftarrow G$*. Terminiere mit Ausgabe von* $\mathcal{G}(f, K)$ *und der aktuellen Nullstellenanordnung.*

2.2 Die absolute Resolventenmethode

In diesem Abschnitt stellen wir die absolute Resolventenmethode vor, auf die wir an späterer Stelle in modifizierter Form zurückgreifen werden. Wie der Name schon andeutet, werden für das Verfahren selber ausschließlich absolute Resolventen verwendet, d.h. G ist immer die symmetrische Gruppe S_n.

Betrachten wir zunächst noch einmal eine etwas allgemeinere Situation: Sei $G \leq S_n$ eine transitive Gruppe mit maximaler Untergruppe H. Nehmen wir wieder an, daß die Galoisgruppe als Permutationsgruppe betrachtet eine Untergruppe von G ist. Dann operiert $\mathcal{G}(f,K)$ auf der Menge der linken Nebenklassen G/H. Ist die zugehörige Resolvente separabel, so operiert $\mathcal{G}(f,K)$ auch auf der Menge der Nullstellen von $R_{(G,H,F)}$, und jede Anordnung der Nullstellen von $R_{(G,H,F)}$ in $\bar{K}$ ergibt einen Homomorphismus von $\mathcal{G}(f,K)$ nach S_r, wobei $r := [\,G:H\,] = \deg(R_{(G,H,F)})$ ist. Diese Beobachtung führt auf den für die absolute Resolventenmethode wichtigen Satz (vgl. Soicher [77] und Soicher, McKay [58]):

2.21. Satz. *Es gelten die Voraussetzungen von Satz 2.4. Sei $r = [\,G:H\,]$ und bezeichne $\tau : \mathcal{G}(f,K) \to S_r$ die Permutationsdarstellung, welche durch Operation von $\mathcal{G}(f,K)$ auf der Menge der linken Nebenklassen G/H gegeben ist. Ist $R_{(G,H,F)}(X) \in R[X]$ separabel, so ist die Galoisgruppe von $R_{(G,H,F)}$, als Untergruppe von S_r betrachtet, gleich der Gruppe $\tau(\mathcal{G}(f,K))$.*

Beweis. Bezeichne $\Delta := \{\sigma_1 H, \ldots, \sigma_r H\}$ die Menge der linken Nebenklassen G/H und sei $\Omega := \{(\sigma_1 F)(\alpha_1,\ldots,\alpha_n), \ldots, (\sigma_r F)(\alpha_1,\ldots,\alpha_n)\}$. Durch $\bar{\psi} : \Delta \to \Omega : \sigma_i H \mapsto (\sigma_i F)(\alpha_1,\ldots,\alpha_n)$ wird eine Bijektion der Mengen Δ und Ω definiert: Wohldefiniertheit und Injektivität von $\bar{\psi}$ ergeben sich aufgrund der folgenden Äquivalenzen

$$\begin{aligned} \sigma_i H = \tilde{\sigma}_i H \quad &\iff \quad \tilde{\sigma}_i^{-1}\sigma_i \in H \\ &\iff \quad \tilde{\sigma}_i^{-1}\sigma_i(F) = F \\ &\overset{R_{(G,H,F)}\text{ sep.}}{\iff} \quad (\sigma_i F)(\alpha_1,\ldots,\alpha_n) = (\tilde{\sigma}_i F)(\alpha_1,\ldots,\alpha_n) \end{aligned}$$

und die Surjektivität folgt aufgrund der gleichen Kardinalität von Δ und Ω. Mittels der Bijektion $\bar{\psi}$ läßt sich dann in gewohnter Weise ein Isomorphismus der Permutationsgruppen S_Δ und S_Ω durch $\psi : S_\Delta \longrightarrow S_\Omega : \psi(\omega)((\sigma_i F)(\alpha_1,\ldots,\alpha_n)) := \bar{\psi}(\omega(\sigma_i H))$ definieren. Sei $\sigma \in \mathcal{G}(f,K)$. Die Permutationsdarstellung τ' von $\mathcal{G}(f,K)$ nach S_Δ definieren wir durch $\tau'(\sigma)(\sigma_i H) := \sigma\sigma_i H$, und den Homomorphismus φ durch Einschränkung des zu σ gehörigen Körperautomorphismus von $G(N(f,K)/K)$ auf den Zerfällungskörper von $R_{(G,H,F)}$. Wir wollen nun zei-

gen, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} & \mathcal{G}(f,K) & \\ {\scriptstyle\tau'}\swarrow & & \searrow{\scriptstyle\varphi} \\ S_\Delta \geq \tau'(\mathcal{G}(f,K)) & \xrightarrow{\psi} & \mathcal{G}(R_{(G,H,F)},K) \leq S_\Omega \end{array}$$

Damit folgt

$$\varphi(\sigma)((\sigma_i F)(\alpha_1,\ldots,\alpha_n)) = (\sigma\sigma_i F)(\alpha_1,\ldots,\alpha_n) \text{ für } 1 \leq i \leq r,$$

und wir erhalten

$$\begin{aligned} \varphi(\sigma)((\sigma_i F)(\alpha_1,\ldots,\alpha_n)) &= (\sigma\sigma_i F)(\alpha_1,\ldots,\alpha_n) \\ &= \bar{\psi}(\sigma\sigma_i H) = \bar{\psi}(\tau'(\sigma)(\sigma_i H)) \\ &= \psi(\tau'(\sigma))((\sigma_i F)(\alpha_1,\ldots,\alpha_n)), \end{aligned}$$

Da φ surjektiv ist, folgt $\mathcal{G}(R_{(G,H,F)},K) = \varphi(\mathcal{G}(f,K)) = \psi(\tau'(\mathcal{G}(f,K)))$. Identifizierung von Δ und Ω mit $\{1,\ldots,r\}$ liefert schließlich die Behauptung. Man vergleiche auch Proposition 5.13, (ii). □

Somit hängt die Galoisgruppe der Resolvente für fest gewählte Gruppen G und H ausschließlich von $\mathcal{G}(f,K)$ ab. Umgekehrt liefert uns die Kenntnis der Galoisgruppe der Resolvente Informationen über $\mathcal{G}(f,K)$. So sind zum Beispiel die irreduziblen Faktoren von $R_{(G,H,F)}$ in $R[X]$ von besonderem Interesse.

2.22. Bemerkung. Nach Satz 2.21 ist die Menge der Grade der irreduziblen Faktoren von $R_{(G,H,F)}(X)$ in $R[X]$ gleich der Menge der Bahnenlängen der Operation von $\tau(\mathcal{G}(f,K))$ auf der Menge $\{1,\ldots,r\}$.

Nach Satz 2.4 (ii) kann man für eine separable Resolvente $R_{(G,H,F)}$, welche nicht irreduzibel ist, eine echte Inklusion in der Gruppe G ableiten. Im Gegensatz zum Verfahren von Stauduhar, wo man dies für einen linearen Faktor von $R_{(G,H,F)}$ macht, besteht hier aber die Schwierigkeit, eine Anordnung der Nullstellen zu finden, die eine Inklusion in einer Gruppe von [5, 16] erlauben. Deshalb ist man bestrebt, nur absolute Resolventen zu verwenden, für die das Problem der Anordnung der Nullstellen nicht auftritt.

Für jede mögliche Galoisgruppe $\mathcal{G}(f,K)$ und jede Gruppe H können die Grade der irreduziblen Faktoren einer absoluten Resolvente im voraus tabelliert werden. Eine solche Tabelle wird auch Partitionstabelle genannt. Die absolute Resolventenmethode besteht nun darin, eine Partitionstabelle für eine Menge spezieller Testgruppen aufzustellen, mittels derer man alle Gruppen eines bestimmten Grades unterscheiden kann (vgl. z.B. Partitionstabellen in Eichenlaub [22] für die

Grade 8 bis 11 und die Tabellen im Anhang für primitive Gruppen der Grade 12 bis 23). Die Galoisgruppe des Polynoms f wird dann durch Faktorisierung der absoluten Resolventen, welche zu den Gruppen H gehören, identifiziert. Da der Grad der Resolvente dem Index von H in S_n entspricht, hängt die Effizienz der absoluten Resolventenmethode stark von der Wahl der Gruppe H ab. Untergruppen mit möglichst kleinem Index als Testgruppen sind also wünschenswert. Deshalb beschränkt man sich nicht mehr nur auf transitive Gruppen, sondern betrachtet nun auch intransitive Untergruppen der symmetrischen Gruppe S_n. Hierbei spielen die intransitiven Gruppen der Form $S_r \times S_{n-r}$, $(1 \leq r \leq \lfloor n/2 \rfloor)$ eine besondere Rolle, da sie für $r < n/2$ maximale Untergruppen vom Index $\binom{n}{r}$ in der symmetrischen Gruppe S_n sind (vgl. Satz 6.25), und darüber hinaus sehr einfache S_n-relative $S_r \times S_{n-r}$-invariante Polynome F besitzen. Wir können zum Beispiel

$$F(x_1, \ldots, x_n) = x_1 \cdots x_r \quad \text{oder} \quad F(x_1, \ldots, x_n) = x_1 + \ldots + x_r$$

wählen. Aufgrund der Gestalt der Polynome F werden die zugehörigen Resolventen $R_{(S_n, S_r \times S_{n-r}, F)}$ auch r-set Resolventen genannt. Diese Resolventen haben außerdem den Vorteil, daß sie sehr leicht nur unter Verwendung der Koeffizienten des Polynoms f berechnet werden können:

Durch Betrachtung von Resultanten der Form $\mathrm{Res}_y(f(x-y), f(y))$ bzw. $\mathrm{Res}_y(y^m f(x/y), f(y))$ lassen sich für Körper beliebiger Charakteristik Polynome berechnen, die die Summe oder das Produkt aller r-elementigen Teilmengen der Nullstellen des Ausgangspolynoms f als Nullstellen haben (vgl. Loos [51]). Speziell für Körper der Charakteristik Null existieren aber wesentlich schnellere Verfahren, die die Tatsache verwenden, daß absolute Resolventen symmetrische Polynome sind. In dem Artikel von Casperson, McKay [10] werden explizite Formeln und Algorithmen angegeben, wie sich aus den elementarsymmetrischen Funktionen der Nullstellen des Eingabepolynoms f die Potenzsummen der Nullstellen der r-set Resolventen berechnen lassen. Anwendung der inversen Newtonrelationen (dies ist einer der Gründe, warum diese Methode i.a. nicht für Körper K mit $\mathrm{char}(K) = p$ funktioniert) liefert dann die Koeffizienten der r-set Resolventen.

Wir geben im folgenden einen Algorithmus zur Berechnung von r-set Resolventen $R_{(S_n, S_r \times S_{n-r}, F)}$ mit $F(x_1, \ldots, x_n) = x_1 \cdots x_r \in R[x_1, \ldots x_n]$ mittels Resultanten an, den wir an späterer Stelle für Körper endlicher Charakteristik benötigen. Algorithmus 2.23 berechnet für die Eingabewerte $f(x) \in R[x], r \in \mathbb{Z}_{>0}$ mit $r \leq n$ und $m = 1$ die gesuchte r-set Resolvente. Zur Vereinfachung verwenden wir die folgende Bezeichnung. Wir definieren

$$P_{(f,r,m)}(X) = \prod \{X - \alpha_{i_1} \cdots \alpha_{i_{r-1}} \cdot \alpha_j^m \mid 1 \leq i_1 < \cdots < i_{r-1} \leq n, j \neq i_1, \ldots, i_{r-1}\},$$

wobei $r, m \in \mathbb{Z}_{>0}$ mit $r \leq n$ und $\alpha_1, \ldots, \alpha_n \in N(f, K)$ wieder die Nullstellen von f seien. Es gilt $P_{(f,r,m)}(X) \in R[X]$.

2.23. Algorithmus. *(Berechnung von r-set Resolventen mittels Resultanten)*

Eingabe: *Ein normiertes Polynom $f(x) \in R[x]$ vom Grad n und $r, m \in \mathbb{Z}_{>0}$ mit $r \leq n$.*

Ausgabe: *Das Polynom $P_{(f,r,m)}(X) \in R[X]$.*

1. *Ist $r = 1$, dann Ausgabe von $P_{(f,r,m)}(X) \leftarrow \mathrm{Res}_Y(f(Y), X - Y^m)$. Terminiere.*
2. *Rufe Algorithmus 2.23 mit f, $r-1$ und 1 auf und erhalte das Polynom $R_1(X) \leftarrow P_{(f,r-1,1)}(X)$. Rufe Algorithmus 2.23 mit f, 1 und m auf und erhalte das Polynom $R_2(X) \leftarrow P_{(f,1,m)}(X)$.*
3. *Berechne $R_3(X) \leftarrow \mathrm{Res}_Y(Y^{\deg(R_1)} R_1(X/Y), R_2(Y))$.*
4. *Rufe Algorithmus 2.23 mit f, $r-1$ und $m+1$ auf und erhalte das Polynom $R_4(X) \leftarrow P_{(f,r-1,m+1)}(X)$. Setze $R(X) \leftarrow R_3(X)/R_4(X)$.*
5. *Gilt $m = 1$, dann Ausgabe von $P_{(f,r,m)}(X) \leftarrow \sqrt[r]{R(X)}$ (normierte Wurzel), ansonsten Ausgabe von $P_{(f,r,m)}(X) \leftarrow R(X)$. Terminiere.*

Nach Loos [51], Theorem 6 und 7 wird in Schritt 1 das normierte Polynom mit Nullstellen $\alpha_i^m, (1 \leq i \leq n)$ berechnet, und in Schritt 3 ist $R_3(X)$ das normierte Polynom, welches als Nullstellen die Produkte der Nullstellen von $R_1(X)$ und $R_2(X)$ hat. Schreiben wir dafür $R_3(X) = R_1(X) * R_2(X)$ so gelten die Gleichungen

$$P_{(f,r-1,1)}(X) * P_{(f,1,m)}(X) = \begin{cases} P_{(f,r,m)}(X)^r \, P_{(f,r-1,m+1)}(X) & \text{für } m = 1, \\ P_{(f,r,m)}(X) \, P_{(f,r-1,m+1)}(X) & \text{sonst.} \end{cases}$$

Der Algorithmus ergibt sich dann direkt aus diesen Gleichungen.

Wie schon angesprochen, hängt die Effizienz der absoluten Resolventenmethode entscheidend von dem Faktorisierungsschritt ab, welcher mit wachsendem Grad n schnell recht aufwendig wird. Damit beschränkt sich der Anwendungsbereich dieses Verfahrens auf die Bestimmung von Galoisgruppen von Polynomen mit kleinen Graden (ungefähr $n \leq 11$). Darüber hinaus wird die Galoisgruppe $\mathcal{G}(f, K)$ auch nur bis auf Konjugation bestimmt, da die Anordnung der Nullstellen unbekannt bleibt. Andererseits hat die absolute Resolventenmethode den Vorteil, daß Präzisionsprobleme praktisch nicht existieren, wenn man die Resolventen symbolisch berechnet. Wir beenden dieses Kapitel mit einem Beispiel zur absoluten Resolventenmethode:

2.24. Beispiel. Sei $f(x) = x^{15} + 12x^{13} + 2x^{12} + 54x^{11} + 18x^{10} + 134x^9 + 54x^8 + 153x^7 + 22x^6 + 162x^5 - 24x^4 + 77x^3 - 9x - 1 \in \mathbb{Z}[x]$. Es gilt $\mathrm{disc}(f) = 3^{42}\,31^8\,3637^2\,11969^2$ und mittels des Diskriminantenkriterium folgt, daß $\mathcal{G}(f, \mathbb{Q}) \leq A_{15}$ gilt. Durch Betrachtung des Polynoms f modulo einiger Primideale erhalten wir, daß $\mathcal{G}(f, \mathbb{Q})$ eine der Gruppen $15T_{20}^+$, $15T_{21}^+$, $15T_{28}^+$, $15T_{42}^+$, $15T_{47}^+$, $15T_{54}^+$, $15T_{62}^+$, $15T_{72}^+$, $15T_{77}^+$, $15T_{84}^+$, $15T_{89}^+$, $15T_{103}^+ = A_{15}$ sein muß. Da diese Methode eine recht gute Annäherung von unten an die tatsächliche Galoisgruppe liefert, liegt die Vermutung nahe, daß $\mathcal{G}(f, \mathbb{Q}) = 15T_{20}^+$ oder $\mathcal{G}(f, \mathbb{Q}) = 15T_{21}^+$ gilt, weil dies die Gruppen der kleinsten Ordnung sind. Durch Berechnung einer Partitionstabelle für alle Gruppen vom Grad 15 stellen wir fest, daß man die Gruppe $15T_{20}^+$ mittels Faktorisierung einer 4-set Resolvente vom Grad 1365 von allen anderen Gruppen unterscheiden kann. Für das Polynom f erhalten wir, daß die zugehörige 4-set Resolvente über $\mathbb{Q}$ in 10 Faktoren der Grade $30, 45, 60, 60, 90, 180, 180, 180, 180$ und 360 faktorisiert. Wie man auch anhand der Partitionstabellen für primitive Gruppen vom Grad 15 im Anhang ersehen kann, erhalten wir aus diesem Faktorisierungsverhalten in der Tat $\mathcal{G}(f, \mathbb{Q}) = 15T_{20}^+$.

Kapitel 3

Algebraische Zahlkörper

Die wesentlichen Probleme des Verfahrens von Stauduhar bei der Übertragung auf andere Grundringe bestehen in der Darstellung bzw. Identifizierung der Nullstellen des Polynoms f, dessen Galoisgruppe wir berechnen wollen, und in der Durchführung des Inklusionstests mit dem Ziel, korrekte Ergebnisse zu erhalten. In diesem Abschnitt geben wir Lösungsmöglichkeiten dieser Probleme für den relativen Zahlkörperfall an.

3.1 Grundlagen

Seien mit F und E algebraische Zahlkörper bezeichnet für die $\mathbb{Q} \subseteq F \subseteq E$ gelten soll. Der Grad von $F/\mathbb{Q}$ sei m, und wir wollen annehmen, daß F durch Adjunktion einer Wurzel $\delta = x+h(x)\mathbb{Q}[x]$ eines normierten irreduziblen Polynoms $h(x) \in \mathbb{Z}[x]$ erzeugt wird, d.h. $F = \mathbb{Q}[x]/h(x)\mathbb{Q}[x] = \mathbb{Q}(\delta)$. Die r_1 reellen und $2r_2$ komplexen Nullstellen von $h(x)$ seien wie gewohnt so angeordnet, daß $\delta^{(1)}, \ldots, \delta^{(r_1)} \in \mathbb{R}$ und $\delta^{(r_1+1)}, \ldots, \delta^{(m)} \in \mathbb{C}\backslash\mathbb{R}$ mit $\delta^{(r_1+j)} = \overline{\delta^{(r_1+r_2+j)}}$ für $1 \leq j \leq r_2$ gilt. Wir erhalten damit m $\mathbb{Q}$-lineare Einbettungen $.^{(j)} : F \longrightarrow \mathbb{C} : \delta \mapsto \delta^{(j)}$, $(1 \leq j \leq m)$ von F nach $\mathbb{C}$, welche sich durch Operation auf den Koeffizienten auf den Polynomring $F[x]$ fortsetzen lassen. Das Element $\delta^{(j)} \in \mathbb{C}$ wird dann als die j-te Konjugierte von δ bezeichnet, und unter der Signatur von F verstehen wir das Tupel (r_1, r_2). Über die Konjugierten läßt sich durch $< \cdot, \cdot >: F \times F \longrightarrow \mathbb{R} : (x, y) \mapsto \sum_{j=1}^{m} x^{(j)}\overline{y^{(j)}}$ ein Skalarprodukt auf dem $\mathbb{Q}$-Vektorraum F einführen. Dies liefert uns durch $T_2 : F \longrightarrow \mathbb{R}_{\geq 0} : x \mapsto < x, x >$ eine positiv definite quadratische Form, die sogenannte T_2-Norm, welche bei algorithmischen Untersuchungen eine zentrale Rolle spielt, da sie eine Größenfunktion auf dem Körper F darstellt.

Bei der Herleitung des Inklusionstests spielen die ganzalgebraischen Zahlen von F über $\mathbb{Z}$ eine entscheidende Rolle. Sie bilden einen Ring mit $\mathbb{Z}$-Basis $\omega_1, \ldots, \omega_m$,

die sogenannte Maximalordnung $\mathfrak{o}_F$ von F. Somit trägt $\mathfrak{o}_F$ die Struktur eines freien $\mathbb{Z}$-Moduls vom Rang m; entsprechendes gilt für die Ideale von $\mathfrak{o}_F$. Da $\mathfrak{o}_F$ ein Dedekindring ist, definiert jedes Primideal $\mathfrak{p} \subset \mathfrak{o}_F$ eine surjektive, exponentielle Bewertung $\nu_\mathfrak{p} : F \longrightarrow \mathbb{Z} \cup \{\infty\}$, die mit der Bewertung zum Bewertungsideal $\boldsymbol{p}_{\nu_\mathfrak{p}}$ übereinstimmt, und es gilt $\boldsymbol{p}_{\nu_\mathfrak{p}} = \mathfrak{p}\boldsymbol{O}_{\nu_\mathfrak{p}}$, $\mathfrak{o}_F/\mathfrak{p} \cong \boldsymbol{O}_{\nu_\mathfrak{p}}/\boldsymbol{p}_{\nu_\mathfrak{p}}$. Die Primideale von $\mathfrak{o}_F$ korrespondieren also eineindeutig und bewertungserhaltend zu den normierten diskreten Bewertungen von $F/\mathbb{Q}$ (vgl. Fröhlich,Taylor [28], Chapter 2, Theorem 7). Für beliebige Ordnungen von F, d.h. unitäre Teilringe $\mathfrak{o} \subseteq \mathfrak{o}_F$, welche freie $\mathbb{Z}$-Moduln vom Rang m sind, gilt nach Neukirch [62], Kapitel I, §12, Satz 12.10 der folgende Sachverhalt: Ist das Primideal $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ kein Indexteiler, d.h $[\mathfrak{o}_F : \mathfrak{o}] \notin \tilde{\mathfrak{p}}$, so ist die Lokalisierung von $\mathfrak{o}$ nach $\tilde{\mathfrak{p}}$ ein diskreter Bewertungsring von F und mit (1.24) erhalten wir eine normierte, diskrete Bewertung auf $F/\mathbb{Q}$. Somit lassen sich Verzweigungsindex und Restklassengrad für Primideale von Ordnungen von F, die teilerfremd zum Index sind, als Verzweigungsindex und Restklassengrad der zugehörigen Bewertungsideale definieren. Zwischen den Stellen von $F/\mathbb{Q}$ besteht eine Abhängigkeitsrelation in Gestalt der Produktformel für algebraische Zahlkörper, d.h. für alle $a \in F^\times$ gilt

$$\prod_{\mathfrak{p}} |a|_\mathfrak{p} \prod_{1 \le j \le m} |a|_j = 1, \tag{3.1}$$

wobei $|a|_\mathfrak{p} = \mathrm{N}(\mathfrak{p})^{-\nu_\mathfrak{p}(a)}$ und $|\cdot|_j := |\cdot^{(j)}|$ für $1 \le j \le m$. Die $|\cdot|_j$ für $1 \le j \le r_1 + r_2$ sind (eindeutige) Repräsentanten der archimedischen Stellen von $F/\mathbb{Q}$, und es gilt $|\cdot|_{r_1+r_2+j} = |\cdot|_{r_1+j}$ für $1 \le j \le r_2$. Im folgenden werden wir die nicht-archimedischen Stellen von F auch als endliche Stellen und die archimedischen Stellen von F als unendliche Stellen bezeichnen.

In unseren Anwendungen ist es oftmals nicht möglich oder auch nicht wünschenswert, mit der Maximalordnung $\mathfrak{o}_F$ direkt zu arbeiten. Anstatt dessen bietet es sich an, die Gleichungsordnung $\mathbb{Z}[\delta]$ oder eine andere Ordnung von F zu benutzen. In diesem Zusammenhang ist der folgende Satz von Bedeutung, dessen Beweis in Pohst, Zassenhaus [70], Sektion 6.2 nachgelesen werden kann:

3.2. Satz. *Sei p eine Primzahl mit $p \nmid \mathrm{disc}(h)$ und $\mathfrak{p}$ ein Primideal von $\mathfrak{o}_F$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Weiterhin seien $\tilde{\mathfrak{p}} = \mathfrak{p} \cap \mathbb{Z}[\delta]$ und $\bar{h} = \bar{h}_1 \cdots \bar{h}_r$ die Zerlegung von h in normierte, irreduzible Faktoren von $(\mathbb{Z}/p\mathbb{Z})[x]$. Dann folgt:*

(i) $\tilde{\mathfrak{p}}$ *ist maximales Ideal von* $\mathbb{Z}[\delta]$ *und* $\mathfrak{o}_F/\mathfrak{p} \cong \mathbb{Z}[\delta]/\tilde{\mathfrak{p}}$.

(ii) $p\mathbb{Z}[\delta] = \tilde{\mathfrak{p}}_1 \cdot \cdots \cdot \tilde{\mathfrak{p}}_r$ *mit* $\tilde{\mathfrak{p}}_i = p\mathbb{Z}[\delta] + h_i(\delta)\mathbb{Z}[\delta]$, $e(\tilde{\mathfrak{p}}_i|p) = 1$ *und* $f(\tilde{\mathfrak{p}}_i|p) = \deg(h_i)$, $(1 \le i \le r)$.

(iii) $p\mathfrak{o}_F = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r$ *mit* $\mathfrak{p}_i = p\mathfrak{o}_F + h_i(\delta)\mathfrak{o}_F$, $e(\mathfrak{p}_i|p) = 1$ *und* $f(\mathfrak{p}_i|p) = \deg(h_i)$, $(1 \le i \le r)$.

wobei $h_i(x)$ *ein beliebiger Vertreter von* $\bar{h}_i(x)$ *in* $\mathbb{Z}[x]$ *ist.*

Analoge Aussagen gelten natürlich auch für die Maximalordnung $\mathfrak{o}_E$ von E.

Um die Darstellung zu vereinfachen, beschränken wir uns in diesem Kapitel auf normierte, irreduzible Polynome f mit Koeffizienten in $\mathfrak{o}_F$. Jedes Polynom $f(x) = \sum_{i=0}^{n} a_i x^i, (a_i \in F)$ läßt sich durch Substitution $g(x) = a_n^{n-1} b^n f(\frac{x}{a_n b})$ in ein Polynom mit Koeffizienten in einer Ordnung $\mathfrak{o}$ von F transformieren, wobei b das kleinste gemeinsame Vielfache der Nenner aller $a_i \neq 0$ ist. Als Nenner eines Elements $a \in F$ bezeichnen wir hierbei die kleinste Zahl $d \in \mathbb{Z}_{>0}$, für die $da \in \mathfrak{o}$ ist. Sind $\alpha_1, \ldots, \alpha_n \in N(f, F)$ die Nullstellen von f, so sind $a_n b\alpha_1, \ldots, a_n b\alpha_n \in N(f, F)$ die Nullstellen von g, und unter Beibehaltung der Nullstellenanordnung gilt $\mathcal{G}(f, F) = \mathcal{G}(g, F)$.

3.2 Nullstellenberechnung

Wir wollen die Nullstellen von f in einem geeigneten Erweiterungskörper von F bestimmen. Dies ist zum Beispiel für den Körper der komplexen Zahlen $\mathbb{C}$ ohne größere Probleme möglich. Bekanntlich führt aber die Verwendung von reeller Arithmetik bei der Galoisgruppenberechnung zu einer sehr hohen Anzahl von Dezimalstellen, will man bewiesene Ergebnisse erhalten (vgl. Eichenlaub [22] und Ford, McKay [26] für $F = \mathbb{Q}$), und demzufolge zu sehr schlechten Laufzeiten. Deshalb machen wir in unseren Berechnungen nur dann Gebrauch von komplexen Approximationen, wenn es darum geht, Aussagen über die Größe der Nullstellen herzuleiten. Statt dessen wollen wir den Ansatz von Darmon, Ford [19] und Yokoyama [88] verfolgen, der zur Galoisgruppenberechnung von rationalen Polynomen verwendet wurde, und die Nullstellen in einer geeigneten unverzweigten $\mathfrak{p}$-adischen Erweiterung der Vervollständigung von F an einem Primideal $\mathfrak{p} \subset \mathfrak{o}_F$ berechnen.

Wir bezeichnen die ganzen p-adischen Zahlen mit $\mathbb{Z}_p$ und ihren Quotientenkörper mit $\mathbb{Q}_p$. Alle in diesem Kapitel auftretenden Primideale seien über $\mathbb{Q}$ unverzweigt. Für unsere Berechnungen wählen wir ein unverzweigtes Primideal $\mathfrak{p} \neq \{0\}$ von $\mathfrak{o}_F$, welches zusätzlich folgende Bedingungen erfüllt:

- $\operatorname{disc}(f) \notin \mathfrak{p}$. (3.3)
- Für die Primzahl $p \in \mathfrak{p}$ ist $f(\mathfrak{p}|p) = 1$. (3.4)

Die Bestimmung des Primideals $\mathfrak{p}$ erfolgt mittels Satz 3.2 durch Wahl einer Primzahl p mit $p \nmid \operatorname{disc}(h)\, \mathrm{N}_{F/\mathbb{Q}}(\operatorname{disc}(f))$, um Unverzweigtheit und Bedingung (3.3) zu

gewährleisten. Die verschärfte Forderung $p \nmid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$ wird an späterer Stelle ausgenutzt. Nach Koch [65], Theorem 1.112, Theorem 1.113 unter Verwendung von $|\{\,\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq x\,\}| \sim \frac{x}{\log(x)}$ (vgl. Goldstein [32], Narkiewicz [60], S.372) folgt, daß in $\mathfrak{o}_F$ unendlich viele Primideale $\mathfrak{p}$ mit $f(\mathfrak{p}|p) = 1$ existieren und diese mit der gewünschten Häufigkeit auftreten: Es gilt

$$\lim_{x\to\infty} \frac{|\{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq x, f(\mathfrak{p}|p) = 1\}|}{|\{\mathfrak{p} \mid \mathrm{N}(\mathfrak{p}) \leq x\,\}|} = 1.$$

Dies bestätigt sich auch in der Praxis. Es ist nicht schwer, eine Primzahl p zu finden, für die neben $p \nmid \mathrm{disc}(h)$ und (3.3) das Polynom h mod $p\mathbb{Z}$ einen Linearfaktor hat und somit für das zugehörige Primideal $\mathfrak{p}$ von $\mathfrak{o}_F$ $f(\mathfrak{p}|p) = 1$ gilt.

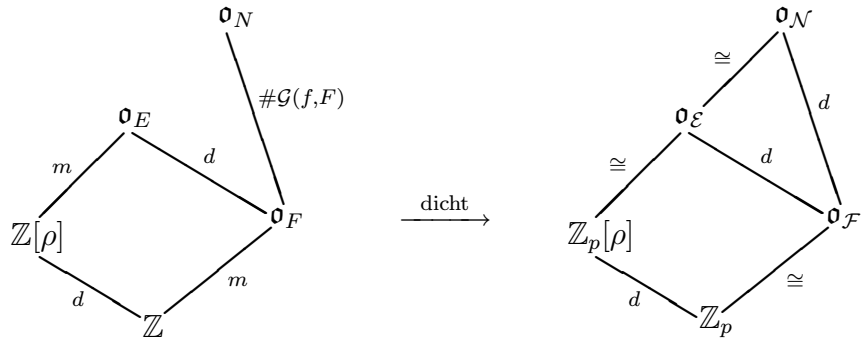
Bezeichne nun $\mathcal{F}$ die Vervollständigung von F an $\mathfrak{p}$. Um Approximationen der Nullstellen des Polynoms f in einem algebraischen Abschluß von $\mathcal{F}$ zu berechnen, benutzen wir das folgende Lemma.

3.5. Lemma. *Sei $\mathfrak{p}$ ein Primideal vom Grad eins und $d \in \mathbb{Z}_{>0}$ minimal mit der Eigenschaft, daß $f(x)$ mod $\mathfrak{p}$ n verschiedene Nullstellen in $\mathbb{F}_{p^d}$ hat. Weiterhin sei $g(x) \in \mathbb{Z}[x]$ normiert vom Grad d, so daß $\mathbb{F}_{p^d}$ von einer Wurzel von $g(x)$ mod $\mathfrak{p}$ über $\mathbb{F}_p$ erzeugt wird. Dann ist $g(x)$ irreduzibel über $\mathcal{F}$. Darüber hinaus sei $\mathcal{E} := \mathcal{F}(\rho)$ und $E := F(\rho)$ mit $g(\rho) = 0$. Dann ist $\mathcal{E}$ die eindeutig bestimmte unverzweigte Erweiterung von $\mathcal{F}$ vom Grad d und ist zugleich der Zerfällungskörper von $f(x)$ über $\mathcal{F}$. Das Primideal $\mathfrak{p}$ ist träge in E/F, $\mathfrak{p}\mathfrak{o}_E = \mathfrak{P}$, und die $\mathfrak{P}$-adische Vervollständigung von E ist gleich $\mathcal{E}$.*

Beweis. Sei $f \equiv f_1 \cdots f_u$ mod $\mathfrak{p}$ die Faktorisierung von f mod $\mathfrak{p}$. Der Restklassenkörper $\bar{\mathcal{F}}_\mathfrak{p}$ von $\mathcal{F}$ bezüglich des Primideals $\mathfrak{p}\mathfrak{o}_\mathcal{F}$ ist ein endlicher Körper und in diesem Fall isomorph zu $\mathbb{F}_p$. Die ganze Zahl d entspricht dann dem k.g.V. der Grade der Faktoren $f_1, \ldots, f_u$, da jede endliche Erweiterung von $\mathbb{F}_p$ normal ist. Nach Lorenz [52], §24, Satz 3, gibt es zu jeder endlichen Erweiterung von $\bar{\mathcal{F}}_\mathfrak{p}$ vom Grade d genau eine unverzweigte Erweiterung $\mathcal{E}/\mathcal{F}$ vom Grad d. Da das Polynom g über dem Restklassenkörper von F bzw. $\mathcal{F}$ irreduzibel ist, ist es über $\mathcal{F}$ irreduzibel. Wir haben somit $\mathrm{disc}(g) \notin \mathfrak{p}$ und aus Satz 3.2 folgt $\mathfrak{p}\mathfrak{o}_E = \mathfrak{P}$. Da $\mathrm{disc}(f) \notin \mathfrak{P}$, hat die Faktorisierung von f mod $\mathfrak{P}$ keine doppelten Faktoren. Mit dem Henselschen Lemma (vgl. Lorenz [52], §23, Satz 3) und weil $\mathbb{F}_{p^d}$ der Zerfällungskörper von f mod $\mathfrak{p}$ ist, erhält man, daß $\mathcal{E}$ der Zerfällungskörper von f über $\mathcal{F}$ ist. □

3.6. Bemerkung. Sei $\nu_\mathfrak{P} : \mathcal{E} \longrightarrow \mathbb{Z} \cup \{\infty\}$ die normierte, diskrete Bewertung von $\mathcal{E}/\mathcal{F}$. Da E dicht in $\mathcal{E}$ liegt, gibt es für alle $\gamma^* \in \mathcal{E}$ und $k \in \mathbb{Z}_{>0}$ Approximationen $\gamma^*_{(k)} \in E$, so daß $\nu_\mathfrak{P}(\gamma^* - \gamma^*_{(k)}) \geq k$ gilt. Diese können mit dem Newton-Lifting (vgl. Sektion 1.4) berechnet werden. Mit anderen Worten lassen sich alle Berechnungen in algebraischen Zahlkörpern durchführen.

Letztere Bemerkung wollen wir genauer untersuchen. Dazu betrachten wir das folgende Diagramm, wobei mit $N := N(f, F)$ und $\mathcal{N} := N(f, \mathcal{F})$ Zerfällungskörper von f über F bzw. $\mathcal{F}$ bezeichnet seien:



(3.2)

Da wir ein unverzweigtes Primideal vom Grad eins gewählt haben, ist $\mathbb{Z}_p \cong \mathfrak{o}_\mathcal{F}$ und die Maximalordnung bzw. der Bewertungsring $\mathfrak{o}_\mathcal{E}$ enthält alle Nullstellen des Polynoms f. Außerdem folgt durch Betrachtung des Restklassengrads und Verzweigungsindexes der Gesamterweiterung $\mathcal{E}/\mathbb{Q}_p$, daß $\mathcal{E} \cong \mathbb{Q}_p(\rho)$ ist. Dann existiert eine quadratische Transformationsmatrix zwischen $\mathbb{Z}_p[\rho]$ und $\mathfrak{o}_\mathcal{E}$, und aus $\operatorname{disc}(g) \notin \mathfrak{p}$ folgt, daß die Primzahl p die Determinante der Transformationsmatrix von $\mathbb{Z}_p[\rho]$ nach $\mathfrak{o}_\mathcal{E}$ nicht teilt. Somit ist diese eine Einheit in $\mathbb{Z}_p$, und die Übergangsmatrix einer Basis von $\mathfrak{o}_\mathcal{E}$ zu einer Basis von $\mathbb{Z}_p[\rho]$ ist invertierbar. Dies bedeutet aber nichts anderes, als daß die Gleichungsordnung $\mathbb{Z}_p[\rho]$ schon die Maximalordnung $\mathfrak{o}_\mathcal{E}$ ist. Also können wir die Nullstellen von f in der Gleichungsordnung $\mathbb{Z}[\rho]$ approximieren, indem wir bezüglich des trägen Primideals $p\mathbb{Z}[\rho]$ arbeiten, da $\mathbb{Z}[\rho]/p\mathbb{Z}[\rho] \cong \mathfrak{o}_E/\mathfrak{P}$. Wir erhalten folgende Bemerkung:

3.7. Bemerkung. Für die Erweiterung $\mathcal{F}/\mathbb{Q}_p$ gilt $[\,\mathcal{F}:\mathbb{Q}_p\,] = e(\mathfrak{p}|p) \cdot f(\mathfrak{p}|p) = 1$, d.h. es existiert ein bewertungserhaltender Monomorphismus $\iota_\mathfrak{p} : F \to \mathbb{Q}_p$ mit $\iota_\mathfrak{p}(\mathfrak{o}_F) \subseteq \mathbb{Z}_p$ und $\nu_\mathfrak{p}(a) = \nu_p(\iota_\mathfrak{p}(a))$ für alle $a \in F$. Somit haben wir für $\mathfrak{o}_\mathcal{E}$ als $\mathbb{Z}_p$-Modul betrachtet folgende Isomorphie:

$$\mathfrak{o}_\mathcal{E} \cong \bigoplus_{i=1}^{d} \mathbb{Z}_p \cdot \rho^{i-1} \cong \bigoplus_{i=1}^{d} \mathbb{Z}_p.$$

Durch Operation auf den Koeffizienten läßt sich der Monomorphismus $\iota_\mathfrak{p}$ auf die Polynomringe $F[x]$ und $\mathbb{Q}_p[x]$ und dann auf $N(f, F)[x]$ und $\mathbb{Q}_p(\rho)[x]$ fortsetzen, indem man die Nullstellen $\alpha_1, \ldots, \alpha_n \in N(f, F)$ auf die exakten Nullstellen $\alpha_1^*, \ldots, \alpha_n^* \in \mathbb{Z}_p[\rho]$ von $\iota_\mathfrak{p}(f)$ in der richtigen Reihenfolge abbildet. Die Fortsetzung wollen wir ebenfalls mit $\iota_\mathfrak{p}$ bezeichnen, und wir identifizieren $\mathbb{Q}$ mit dem Bild in $\mathbb{Q}_p$, so daß $\mathbb{Q} \subseteq \mathbb{Q}_p$ und $\mathbb{Z} \subseteq \mathbb{Z}_p$ gilt. Nach Cohn [13], Chapter 2, Theorem 2.5 läßt

sich die normierte diskrete Bewertung ν_p von $\mathbb{Q}_p$ eindeutig zu einer normierten, diskreten Bewertung auf $\mathbb{Q}_p(\rho)$ fortsetzen, da die Erweiterung $\mathbb{Q}_p(\rho)/\mathbb{Q}_p$ unverzweigt ist. Diese bezeichnen wir auch mit ν_p. Definieren wir $\nu_\mathfrak{p}(a) := \nu_p(\iota_\mathfrak{p}(a))$ für alle $a \in N(f,F)$, so erhalten wir eine Fortsetzung von $\nu_\mathfrak{p}$ auf $N(f,F)$, bezüglich derer die Einbettung $\iota_\mathfrak{p}$ bewertungserhaltend ist.

Das Diagramm (3.2) beleuchtet die Situation vom mathematischen Standpunkt. Algorithmisch ist für uns die folgende Proposition von Bedeutung:

3.8. Proposition. *Ist $\tilde{f} \in \mathbb{Z}[x]$ ein normiertes Polynom vom Grad n mit $\tilde{f} \equiv f \bmod \mathfrak{p}^k$, $k \in \mathbb{Z}_{>0}$, so gibt es zu jeder Nullstelle $\alpha^* \in \mathbb{Z}_p[\rho]$ von $\iota_\mathfrak{p}(f)$ eine Nullstelle $\beta^* \in \mathbb{Z}_p[\rho]$ von $\iota_\mathfrak{p}(\tilde{f}) = \tilde{f}$ mit $\nu_p(\alpha^* - \beta^*) \geq k$.*

Beweis. Aus $f \equiv \tilde{f} \bmod \mathfrak{p}$ folgt die Existenz einer Nullstelle $\beta^* \in \mathbb{Z}_p[\rho]$ von $\iota_\mathfrak{p}(\tilde{f})$ mit $\beta^* \equiv \alpha^* \bmod p\mathbb{Z}_p[\rho]$. Es gilt $\iota_\mathfrak{p}(f)(\beta^*) = \iota_\mathfrak{p}(f)(\beta^*) - \iota_\mathfrak{p}(\tilde{f})(\beta^*) + \iota_\mathfrak{p}(\tilde{f})(\beta^*) = \iota_\mathfrak{p}(f - \tilde{f})(\beta^*)$ und somit $\nu_p(\iota_\mathfrak{p}(f)(\beta^*)) = \nu_p(\iota_\mathfrak{p}(f - \tilde{f})(\beta^*)) \geq k$. Mit $\iota_\mathfrak{p}(f)(\beta^*) = \iota_\mathfrak{p}(f)(\alpha^*) + \iota_\mathfrak{p}(f')(\alpha^*)(\beta^* - \alpha^*) + r(\alpha^*, \beta^*)(\beta^* - \alpha^*)^2$ für ein Polynom $r \in \mathbb{Z}_p[\rho][x]$ erhalten wir

$$k \leq \nu_p\left(\iota_\mathfrak{p}(f)(\beta^*) - \iota_\mathfrak{p}(f)(\alpha^*)\right) = \nu_p\left(\iota_\mathfrak{p}(f')(\alpha^*)(\beta^* - \alpha^*) + r(\alpha^*, \beta^*)(\beta^* - \alpha^*)^2\right).$$

Sei nun $\alpha \in N(f,F)$ mit $\iota_p(\alpha) = \alpha^*$. Da $\operatorname{disc}(f) = (-1)^{\binom{n}{2}} \mathrm{N}_{F(\alpha)/F}(f'(\alpha)) \notin \mathfrak{p}$, ist $\nu_p(\iota_\mathfrak{p}(f')(\alpha^*)) = 0$ und aus $\beta^* \equiv \alpha^* \bmod p\mathbb{Z}_p[\rho]$ folgt

$$\begin{aligned} k &\leq \nu_p\left(\iota_\mathfrak{p}(f')(\alpha^*)(\beta^* - \alpha^*) + r(\alpha^*, \beta^*)(\beta^* - \alpha^*)^2\right) \\ &= \min\{\nu_p\left(\iota_\mathfrak{p}(f')(\alpha^*)(\beta^* - \alpha^*)\right), \nu_p\left(r(\alpha^*, \beta^*)(\beta^* - \alpha^*)^2\right)\} \\ &= \nu_p(\beta^* - \alpha^*) \end{aligned}$$

□

Mittels der folgenden Proposition können Elemente aus $\mathfrak{o}_F$ in $\mathbb{Z}$ approximiert werden.

3.9. Proposition. *Sei $\mathfrak{o}$ eine Ordnung von F und $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ ein unverzweigtes Primideal vom Grad eins. Dann gilt:*

$$\mathfrak{o} = \mathbb{Z} + \tilde{\mathfrak{p}}^k, \ k \in \mathbb{Z}_{>0}.$$

Beweis. Sei p die Primzahl, welche unter $\tilde{\mathfrak{p}}$ liegt, d.h. $p\mathfrak{o} \subseteq \tilde{\mathfrak{p}}$. Wir betrachten die Lokalisierung $\mathfrak{o}_{\tilde{\mathfrak{p}}} := \mathfrak{o}S^{-1}$ mit $S = \mathfrak{o}\backslash\tilde{\mathfrak{p}}$ und zeigen zuerst durch Induktion über k, daß

$$\mathfrak{o}_{\tilde{\mathfrak{p}}} = \mathbb{Z} + \tilde{\mathfrak{p}}^k\mathfrak{o}_{\tilde{\mathfrak{p}}}, \ k \in \mathbb{Z}_{>0} \quad \text{gilt.}$$

Es ist $\tilde{\mathfrak{p}}\mathfrak{o}_{\tilde{\mathfrak{p}}} = p\mathfrak{o}\mathfrak{o}_{\tilde{\mathfrak{p}}} = p\mathfrak{o}_{\tilde{\mathfrak{p}}}$, und es gilt $\mathfrak{o}_{\tilde{\mathfrak{p}}} = \mathbb{Z} + \tilde{\mathfrak{p}}\mathfrak{o}_{\tilde{\mathfrak{p}}}$, da $\mathfrak{o}_{\tilde{\mathfrak{p}}}/\tilde{\mathfrak{p}}\mathfrak{o}_{\tilde{\mathfrak{p}}} \cong \mathbb{Z}/p\mathbb{Z}$ ist. Ferner haben wir

$$\mathfrak{o}_{\tilde{\mathfrak{p}}} = \mathbb{Z} + \tilde{\mathfrak{p}}\mathfrak{o}_{\tilde{\mathfrak{p}}} = \mathbb{Z} + p\mathfrak{o}_{\tilde{\mathfrak{p}}} \overset{Ind.Ann.}{=} \mathbb{Z} + p(\mathbb{Z} + \tilde{\mathfrak{p}}^k\mathfrak{o}_{\tilde{\mathfrak{p}}}) = \mathbb{Z} + \tilde{\mathfrak{p}}^{k+1}\mathfrak{o}_{\tilde{\mathfrak{p}}}, \ \ k \in \mathbb{Z}_{>0}$$

Da $\mathfrak{o} \subseteq \mathfrak{o}_{\tilde{\mathfrak{p}}}$ gilt auch $\mathfrak{o} = \mathbb{Z} + \tilde{\mathfrak{p}}^k$ für alle $k \in \mathbb{Z}_{>0}$. Denn für alle $a \in \mathfrak{o}$ existiert ein $z \in \mathbb{Z}$ mit $a - z \in \tilde{\mathfrak{p}}^k \mathfrak{o}_{\tilde{\mathfrak{p}}} \cap \mathfrak{o} = \tilde{\mathfrak{p}}^k$. Also $a \in z + \tilde{\mathfrak{p}}^k \subseteq \mathbb{Z} + \tilde{\mathfrak{p}}^k$. □

Wir erhalten nun den folgenden Algorithmus zur Nullstellenberechnung:

3.10. Algorithmus. *(Nullstellenberechnung algebraische Zahlkörper)*

Eingabe: *Ein normiertes Polynom $f \in \mathfrak{o}_F[x]$ vom Grad n, ein unverzweigtes Primideal $\mathfrak{p} \subset \mathfrak{o}_F$ mit $f(\mathfrak{p}|p) = 1$, $\operatorname{disc}(f) \notin \mathfrak{p}$ und $k \in \mathbb{Z}_{>0}$.*

Ausgabe: *Approximationen $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \in \mathbb{Z}[\rho]$ der Nullstellen von $\iota_{\mathfrak{p}}(f) \bmod p^k\mathbb{Z}_p[\rho]$.*

1. *(Approximiere f) Finde normiertes $\tilde{f} \in \mathbb{Z}[x]$ mit $f - \tilde{f} \equiv 0 \bmod \mathfrak{p}^k$.*
2. *(Faktorisierung über endlichem Körper) Für die Faktorisierung $\tilde{f} \equiv \tilde{f}_1 \ldots \tilde{f}_u \bmod p\mathbb{Z}$ setze $d := \operatorname{kgV}\{\deg(\tilde{f}_1), \ldots, \deg(\tilde{f}_u)\}$.*
3. *(Gleichungsordnung $\mathbb{Z}[\rho]$) Bestimme normiertes $g \in \mathbb{Z}[x]$ vom Grad d, so daß $g \bmod p\mathbb{Z}$ irreduzibel ist. Erhalte $\mathbb{Z}[\rho]$ für $g(\rho) = 0$.*
4. *(Startwerte für Newton-Lifting) Bestimme $\alpha^*_{1,(1)}, \ldots, \alpha^*_{n,(1)} \in \mathbb{Z}[\rho]$ mit $\tilde{f}(\alpha^*_{i,(1)}) \equiv 0 \bmod p\mathbb{Z}[\rho]$.*
5. *(Newton-Lifting) Bestimme $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \in \mathbb{Z}[\rho]$ mit $\tilde{f}(\alpha^*_{i,(k)}) \equiv 0 \bmod p^k\mathbb{Z}[\rho]$.*
6. *(Ende) Ausgabe von $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \in \mathbb{Z}[\rho]$. Terminiere.*

Das Polynom f läßt sich durch ein Polynom $\tilde{f}$ approximieren, indem man die Koeffizienten von f mittels des Ideals $\mathfrak{p}^k$ in $\mathbb{Z}$ wie in Proposition 3.9 approximiert. Somit entspricht die Bildung des Polynoms $\tilde{f}$ gerade der Anwendung der Abbildung $\iota_{\mathfrak{p}}$ auf das Polynom f, d.h. $\tilde{f}$ stellt eine p-adische Approximation von $\iota_{\mathfrak{p}}(f)$ dar. Da die Diskriminanten von f und $\tilde{f}$ modulo dem Primideal $\mathfrak{p}$ übereinstimmen folgt, daß die Primzahl p die Diskriminante von $\tilde{f}$ nicht teilt, und wir können mit Hilfe des erweiterten Euklidischen Algorithmus für Polynome über endlichen Körpern das Inverse von $\tilde{f}'(\alpha^*_{i,(1)}) \bmod p\mathbb{Z}[\rho]$ berechnen. Somit sind alle Voraussetzungen des Newton-Liftings für das Polynom $\tilde{f} \in \mathbb{Z}[\rho][x]$ erfüllt. Betrachtet man $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \in \mathbb{Z}[\rho]$ als Elemente von $\mathfrak{o}_E$, so sind sie zugleich n verschiedene approximierte Nullstellen von f in $\mathfrak{o}_E \bmod \mathfrak{P}^k$, da $f(\alpha^*_{i,(k)}) \equiv \tilde{f}(\alpha^*_{i,(k)}) \equiv 0 \bmod \mathfrak{P}^k$. Mit anderen Worten liefern unsere Berechnungen in $\mathbb{Z}[\rho]$ dasselbe Ergebnis, wie wenn wir mit dem Polynom f in $\mathfrak{o}_E$ gerechnet hätten. Diese Technik führt zu einer erheblichen Laufzeitverbesserung. Darüber hinaus läßt sich in Schritt 5 auch

das Hensel-Lifting (vgl. Pohst, Zassenhaus [70], Sektion 4.5, Lemma 5.76) auf die Kongruenz $\tilde{f} \equiv (x - \alpha^*_{1,(1)}) \cdots (x - \alpha^*_{1,(n)}) \bmod p\mathbb{Z}[\rho]$ anwenden, um die Approximationen der Nullstellen zur gewünschten Präzision zu liften. Dieser Ansatz bietet den Vorteil, daß die speziell für das Hensel-Lifting entwickelte Methode aus Klüners [42], Kapitel III.2 angewendet werden kann. Die Idee hierbei ist, die unverzweigte p-adische Erweiterung $\mathbb{Q}_p(\rho)/\mathbb{Q}_p$ sukzessive als Körperturm zu erzeugen, um einzelne Berechnungen in Teilkörpern von $\mathbb{Q}_p(\rho)$ durchzuführen.

3.11. Bemerkung. Proposition 3.8 und Algorithmus 3.10 gelten vollkommen analog für normierte, irreduzible Polynome $f(x) \in \mathfrak{o}[x]$ mit Koeffizienten in einer beliebigen Ordnung $\mathfrak{o}$ des algebraischen Zahlkörpers F und einem Primideal $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ vom Grad eins mit $\mathrm{disc}(\mathfrak{o}) \notin \tilde{\mathfrak{p}}$ und $\mathrm{disc}(f) \notin \tilde{\mathfrak{p}}$: Da $\tilde{\mathfrak{p}}$ insbesondere nicht den Index $[\,\mathfrak{o}_F : \mathfrak{o}\,]$ teilt, ist $\tilde{\mathfrak{p}}\mathfrak{o}_F$ nach Pohst, Zassenhaus [70] Sektion 6.2, Lemma 2.26 ein Primideal von $\mathfrak{o}_F$, und mit den Bezeichnungen aus Lemma 3.5 erhalten wir für $\mathfrak{p} = \tilde{\mathfrak{p}}\mathfrak{o}_F$ und $k \in \mathbb{Z}_{>0}$ das folgende Diagramm:

$$\begin{array}{ccccc} \mathbb{Z}[\rho]/p^k\mathbb{Z}[\rho] & \xrightarrow{\cong} & \mathfrak{o}[\rho]/(\tilde{\mathfrak{p}}[\rho])^k & \xrightarrow{\cong} & \mathfrak{o}_E/\mathfrak{P}^k \\ \uparrow g & & \uparrow g & & \uparrow g \\ \mathbb{Z}/p^k\mathbb{Z} & \xrightarrow[f(\mathfrak{p}|p)=f(\tilde{\mathfrak{p}}|p)=1]{\cong} & \mathfrak{o}/\tilde{\mathfrak{p}}^k & \xrightarrow[p\nmid[\mathfrak{o}_F:\mathfrak{o}]]{\cong} & \mathfrak{o}_F/\mathfrak{p}^k \end{array} \tag{3.12}$$

Nullstellen von $f(x) \in \mathfrak{o}[x]$ können also wie bisher in $\mathbb{Z}[\rho]$ approximiert werden. Es folgt, daß die Maximalordnung $\mathfrak{o}_F$ zur Berechnung der Nullstellen nicht explizit bekannt sein muß.

3.3 Inklusionstest

Wir betrachten nun die Situation

$$\begin{array}{ccc} Cl(\mathfrak{o}_F, N(f,F)) & \xrightarrow{\iota_{\mathfrak{p}}} & \mathbb{Z}_p[\rho] \\ \uparrow & & \uparrow \\ \mathfrak{o}_F & \xrightarrow{\iota_{\mathfrak{p}}} & \mathbb{Z}_p \end{array} \tag{3.13}$$

und haben approximierte Nullstellen der Resolvente in $\mathbb{Z}_p[\rho]$ gegeben, die wir nach einigen Berechnungen mit den approximierten Nullstellen des Polynoms $\iota_{\mathfrak{p}}(f)$ erhalten haben. Um festzustellen, ob wir einen Abstieg im Untergruppengitter der transitiven Permutationsgruppen machen können, müssen wir beweisen oder widerlegen, ob das aktuelle Resolventenpolynom $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ eine einfache

Nullstelle in $\mathfrak{o}_F$ besitzt. Dieses Problem ist eng mit der verschärften Aufgabenstellung verknüpft, zu beweisen oder zu widerlegen, ob es sich bei einer vorgegebenen, zur approximierten Nullstelle $\gamma^*_{(k)} \in \mathbb{Z}_p[\rho]$ gehörenden Nullstelle $\gamma \in N(f,F)$ (hätten wir mit den exakten Nullstellen $\alpha_1, \ldots, \alpha_n$ von f in $N(f,F)$ gerechnet) um ein Element aus $\mathfrak{o}_F$ handelt, wenn nur die Approximation $\gamma^*_{(k)}$ bekannt ist. Es ist klar, daß mit einer Lösung des zweiten Problems auch das erste gelöst werden kann, wenn gleich möglicherweise auch nicht so effizient. Beide Aufgabenstellungen lassen sich unter Verwendung eines Basisalgorithmus lösen, der bei Eingabe einer Approximation $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ der exakten Nullstelle $\gamma^* \in \mathbb{Z}_p[\rho]$ der Resolvente $\iota_{\mathfrak{p}}(R_{(G,H,F)})$ mit $\gamma^*_{(k)} \equiv \gamma^* \bmod p^k\mathbb{Z}_p[\rho]$ und der Präzision k die folgenden Spezifikationen aufweist:

- Ist $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ mit einer Präzision gegeben, die größer ist als eine (berechenbare, noch zu bestimmende) Schranke S_1, so wird entweder die korrekte Aussage „$\gamma \notin \mathfrak{o}_F$“ oder ein $\gamma' \in \mathfrak{o}_F$ mit $\iota_{\mathfrak{p}}(\gamma') \equiv \gamma^* \bmod p^k\mathbb{Z}_p[\rho]$ zurückgegeben.

- Ist $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ mit einer Präzision gegeben, die größer ist als eine (berechenbare, noch zu bestimmende) Schranke $S_2 \geq S_1$, so wird entweder die korrekte Aussage „$\gamma \notin \mathfrak{o}_F$“ oder eine *Nullstelle* γ' von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ mit $\gamma' \in \mathfrak{o}_F$ und $\iota_{\mathfrak{p}}(\gamma') \equiv \gamma^* \bmod p^k\mathbb{Z}_p[\rho]$ zurückgegeben.

Die Schranke S_1 wird sicherstellen, daß Elemente in $\mathfrak{o}_F$ korrekt rekonstruiert werden, während mit der Schranke S_2 bewiesen wird, ob mögliche Nullstellenkandidaten der Resolvente auch wirklich Nullstellen sind. In beiden Fällen haben wir $\gamma' = \gamma$, falls $\gamma \in \mathfrak{o}_F$. Der Basisalgorithmus gliedert sich informell in zwei Teile:

- *Rekonstruktion* : Finde „kleines“ $\gamma' \in \mathfrak{o}_F$ mit $\iota_{\mathfrak{p}}(\gamma') \equiv \gamma^*_{(k)} \bmod p^k\mathbb{Z}_p[\rho]$.

- *Nullstellenbeweis* : Beweise, daß $R_{(G,H,F)}(\gamma') = 0$ gilt.

Wir wollen nun den obigen Algorithmus herleiten und fixieren dazu für den Rest dieses Kapitels eine Ganzheitsbasis $\omega_1, \ldots, \omega_m$ von $\mathfrak{o}_F$. Für eines der ω_i gilt $p \nmid \iota_{\mathfrak{p}}(\omega_i)$, da sonst alle ω_i im Ideal $\mathfrak{p}$ liegen würden. Wir wollen o.B.d.A annehmen, daß $p \nmid \iota_{\mathfrak{p}}(\omega_1)$ gilt. Bezüglich der Basis von $\mathfrak{o}_F$ läßt sich jedes Element $\gamma = \sum_{i=1}^m \lambda_i\omega_i$ von F durch den m-elementigen Vektor $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Q}^m$ eindeutig darstellen. Speziell ist $\gamma \in \mathfrak{o}_F$ genau dann, wenn die $\lambda_i, (1 \leq i \leq m)$ ganzrational sind. Ferner vereinbaren wir folgende Bezeichnungen

3.14. Bezeichnung. *Sei $k \in \mathbb{Z}_{>0}$ beliebig.*

	$Cl(\mathfrak{o}_F, N(f,F))$ $\xrightarrow{\iota_\mathfrak{p}}$ $\mathbb{Z}_p[\rho]$
exakte Nullstelle	γ, γ_σ $\qquad$ $\gamma^*, \gamma^*_\sigma$
Approximation	$\gamma^*_{(k)}, \gamma^*_{\sigma,(k)} \in \mathbb{Z}[\rho]$ *mit* $\gamma^*_{(k)} \equiv \gamma^* \bmod p^k\mathbb{Z}_p[\rho]$ $\gamma^*_{\sigma,(k)} \equiv \gamma^*_\sigma \bmod p^k\mathbb{Z}_p[\rho]$
	$\alpha_{j,i} \in \mathbb{C}$ *Nullstellen von* $f^{(j)}(x) \in \mathbb{C}[x]$ $\sigma F(\alpha_{j,1}, \ldots, \alpha_{j,n}) \in \mathbb{C}$, $(1 \le j \le m)$ *Nullstellen von* $R^{(j)}_{(G,H,F)}(X) \in \mathbb{C}[X]$

Exakte Nullstellen der Resolvente $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ und des isomorphen Bildes $\iota_\mathfrak{p}(R_{(G,H,F)}) \in \mathbb{Z}_p[X]$ werden mit γ bzw. γ^* bezeichnet. Die Nullstellen werden mit σ indiziert, wenn wir zwischen verschiedenen Nullstellen der Resolvente unterscheiden müssen oder die Zugehörigkeit zur Invariante $\sigma F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, $\sigma \in G//H$ hervorheben wollen. Unter einer Approximation von $\gamma^* \in \mathbb{Z}_p[\rho]$ verstehen wir ein Element $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ mit $\gamma^*_{(k)} \equiv \gamma^* \bmod p^k\mathbb{Z}_p[\rho]$. Zu einer Approximation $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ sei $\gamma^*_{(k,i)}$ als der i-te Koeffizient in $\gamma^*_{(k)} = \sum_{i=1}^{d} \gamma^*_{(k,i)}\rho^{i-1}$ definiert. Ferner bezeichnen wir die komplexen Nullstellen von $f^{(j)}(x) \in \mathbb{C}[x]$, $(1 \le j \le m)$ mit $\alpha_{j,1}, \ldots, \alpha_{j,n} \in \mathbb{C}$. Somit sind $\sigma F(\alpha_{j,1}, \ldots, \alpha_{j,n})$, $\sigma \in G//H$ die komplexen Nullstellen von $R^{(j)}_{(G,H,F)}(X) \in \mathbb{C}[X]$.

3.15. Bemerkung. Sei $\gamma^* \in \mathbb{Z}_p[\rho]$ eine Nullstelle der Resolvente $\iota_\mathfrak{p}(R_{(G,H,F)})(X)$ in $\mathbb{Z}_p[X]$. Nach Bemerkung 3.7 ist $\gamma^* \in \mathbb{Z}_p$ eine notwendige Bedingung, um γ^* zu $\gamma \in \mathfrak{o}_F$ rekonstruieren zu können. Für eine Approximation $\gamma^*_{(k)}$ von γ^* muß also gelten $\gamma^*_{(k)} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$ für alle $k \in \mathbb{Z}_{>0}$, d.h. $p^k \mid \gamma^*_{(k,i)}$ für $2 \le i \le d$.

Um zu entscheiden, ob es sich bei einer Nullstelle der Resolvente um eine Zahl aus $\mathfrak{o}_F$ handelt, muß folgende p-adische diophantische Approximationsaufgabe (bei ausreichend großer Präzision) gelöst werden:

$$\begin{aligned}&\text{Zu } \gamma^* \in \mathbb{Z}_p \text{ finde } \lambda_i \in \mathbb{Z} \text{ mit } \gamma^* = \textstyle\sum_{i=1}^{m} \lambda_i\, \iota_\mathfrak{p}(\omega_i) \text{ oder entscheide,}\\ &\text{daß keine } \lambda_i \text{ mit dieser Eigenschaft existieren.}\end{aligned} \tag{3.16}$$

Die Bildmenge $\iota_\mathfrak{p}(\mathfrak{o}_F) \subseteq \mathbb{Z}_p$ ist ein freier $\mathbb{Z}$-Modul vom Rang m mit Basis $\iota_\mathfrak{p}(\omega_1)$, $\ldots, \iota_\mathfrak{p}(\omega_m)$. Also sind die $\iota_\mathfrak{p}(\omega_i)$ auch $\mathbb{Z}$ linear unabhängig über $\mathbb{Z}_p$. Dies hat zur Folge, daß es in (3.16) entweder genau eine Lösung $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m$ oder gar keine Lösung gibt.

Mittels Proposition 3.9 können wir den $\omega_i, (1 \le i \le m)$ eindeutig Approximationen $\omega^*_{i,(k)} \in \mathbb{Z}$ mit $\omega_i - \omega^*_{i,(k)} \in \mathfrak{p}^k$ zuordnen, indem wir zusätzlich $\omega^*_{i,(k)} \in$

$[-(p^k-1)/2, p^k/2]$ fordern. Für die Korrektheit der Ausführungen ist die Eindeutigkeit nicht von Bedeutung, aber für die praktischen Berechnungen von Vorteil. Bezeichnet $\gamma^*_{(k)} \in \mathbb{Z}[\rho]$ eine approximierte Nullstelle der Resolvente, so sind wir an einer $\mathbb{Z}$-Linearkombination zwischen den $\omega^*_{i,(k)}$ und den $\gamma^*_{(k,1)}$ interessiert. Wären die $\omega^*_{i,(k)}$ mit unendlicher Präzision gegeben, so gäbe es genau eine $\mathbb{Z}$-Linearkombination oder gar keine. Da wir aber nur mit einer endlichen Präzision arbeiten können, sind in $\mathbb{Z}/p^k\mathbb{Z}$ die Restklassen $\omega^*_{1,(k)} + p^k\mathbb{Z}, \ldots, \omega^*_{m,(k)} + p^k\mathbb{Z}$ nicht mehr $\mathbb{Z}$-linear unabhängig und die ganze Zahl $\gamma^*_{(k,1)}$ läßt sich immer als $\mathbb{Z}$-Linearkombination der $\omega^*_{i,(k)}+p^k\mathbb{Z}$ schreiben. Ist die Präzision groß genug gewählt, so erwarten wir, daß diese „unerwünschten“ Relationen große Koeffizienten haben, während die gesuchte $\mathbb{Z}$-Linearkombination im Vergleich dazu kleine Koeffizienten hat. Es gilt also Schranken für die Präzision herzuleiten, mittels derer wir die gesuchte $\mathbb{Z}$-Linearkombination (falls existent) von den anderen „unerwünschten„ $\mathbb{Z}$-Linearkombinationen in $\mathbb{Z}/p^k\mathbb{Z}$ unterscheiden können.

3.17. Proposition. *Sei $\gamma^* \in \mathbb{Z}_p[\rho]$ mit $\gamma^*_{(k)} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$ für alle $k \in \mathbb{Z}_{>0}$ eine p-adische Nullstelle des Resolventenpolynoms. Die Abbildung*

$$\begin{array}{rcl} \phi : \mathbb{Z} \times \cdots \times \mathbb{Z} & \longrightarrow & \mathbb{Z}/p^k\mathbb{Z} \\ (\lambda_1, \ldots, \lambda_{m+1}) & \mapsto & \lambda_1\omega^*_{1,(k)} + \cdots + \lambda_m\omega^*_{m,(k)} + \lambda_{m+1}\gamma^*_{(k,1)} + p^k\mathbb{Z} \end{array} \tag{3.18}$$

ist ein surjektiver $\mathbb{Z}$-Modulhomomorphismus. $\operatorname{Kern}\phi$ *ist ein freier $\mathbb{Z}$-Modul vom Rang $m+1$ und die Vektoren*

$$\begin{array}{rcl} u_{1,(k)} & = & (p^k, 0, \ldots, 0), \\ u_{2,(k)} & = & (-\omega^{*\,-1}_{1,(k)}\omega^*_{2,(k)}, 1, 0, \ldots, 0), \\ u_{3,(k)} & = & (-\omega^{*\,-1}_{1,(k)}\omega^*_{3,(k)}, 0, 1, \ldots, 0), \\ \vdots & & \vdots \\ u_{m,(k)} & = & (-\omega^{*\,-1}_{1,(k)}\omega^*_{m,(k)}, 0, \ldots, 1, 0), \\ u_{m+1,(k)} & = & (-\omega^{*\,-1}_{1,(k)}\gamma^*_{(k,1)}, 0, \ldots, 0, 1) \end{array} \tag{3.19}$$

bilden eine Basis von $\operatorname{Kern}\phi$.

Beweis. Da $p \nmid \iota_{\mathfrak{p}}(\omega_1)$ gilt auch $p \nmid \omega^*_{1,(k)}$ für alle $k \in \mathbb{Z}_{>0}$. Damit folgt die Surjektivität. Nach dem ersten Isomorphiesatz ist $|\,\mathbb{Z}^{m+1} / \operatorname{Kern}\phi\,| = p^k$. Da also $\operatorname{Kern}\phi$ endlichen Index in $\mathbb{Z}^{m+1}$ hat und $\mathbb{Z}$ ein Hauptidealring ist, muß $\operatorname{Kern}\phi$ den Rang $m+1$ haben. Sei nun $U :=< u_{1,(k)}, \ldots, u_{m+1,(k)} >$. Es ist $U \subseteq \operatorname{Kern}\phi \subseteq \mathbb{Z}^{m+1}$, und es gilt $[\,\mathbb{Z}^{m+1} : U\,] = p^k$. Daraus folgt $\operatorname{Kern}\phi = U$. □

3.20. Definition und Korollar. $\Lambda_{\gamma^*_{(k,1)},(k)} := \operatorname{Kern}\phi$ *ist ein Gitter der Dimension $m+1$ im $\mathbb{R}^{m+1}$ mit Basis $u_{1,(k)}, \ldots, u_{m+1,(k)}$. Das Teilgitter von $\Lambda_{\gamma^*_{(k,1)},(k)}$,*

welches nur aus den Relationen der $\omega^*_{i,(k)}$, $(1 \le i \le m)$ *besteht (*$\lambda_{m+1} = 0$ *in* (3.18)*), bezeichnen wir mit* $\Lambda'_{\gamma^*_{(k,1)},(k)}$. *Die Vektoren* $u_{1,(k)}, \ldots, u_{m,(k)}$ *bilden eine Basis von* $\Lambda'_{\gamma^*_{(k,1)},(k)}$.

3.21. Bezeichnung. *Die Euklidische Norm eines Vektors* $x \in \mathbb{R}^m$, $m \in \mathbb{Z}_{>0}$ *bezeichnen wir mit* $\| x \|$. *Für eine Matrix* $M \in \mathbb{R}^{m\times m}$, $m \in \mathbb{Z}_{>0}$ *sei* $\| M \|$ *eine mit der Euklidischen Norm verträgliche Norm, d.h. es gelte:* $\| Mx \| \le \| M \| \| x \|$. *Transponierte Vektoren bzw. Matrizen versehen wir wie gewöhnlich mit dem Exponenten* ^{tr}.

Wir nehmen nun an, daß die p-adische Nullstelle $\gamma^* \in \mathbb{Z}_p[\rho]$ des Resolventenpolynoms einer Nullstelle $\gamma = \sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}_F$ entspricht, um obere Schranken der euklidischen Norm des Vektors $(\lambda_1, \ldots, \lambda_m)$ herzuleiten. Dazu betrachten wir das zum $\mathbb{Z}$-Modul $\mathfrak{o}_F$ isomorphe Gitter, welches durch die Minkowskiabbildung $\mu : F \longrightarrow \mathbb{R}^m : x \mapsto \big(x^{(1)}, \ldots, x^{(r_1)}, \sqrt{2}\,\mathrm{Re}(x^{(r_1+1)}), \sqrt{2}\,\mathrm{Im}(x^{(r_1+1)}), \ldots, \sqrt{2}\,\mathrm{Re}(x^{(r_1+r_2)}), \sqrt{2}\,\mathrm{Im}(x^{(r_1+r_2)})\big)^{tr}$ gegeben wird. $\mathbb{Q}$-linear unabhängige Elemente werden hierdurch in $\mathbb{R}$-linear unabhängige Vektoren überführt, daher handelt es sich bei $\mu(\mathfrak{o}_F)$ um ein vollständiges Gitter im $\mathbb{R}^m$. Es gilt $\|\mu(x)\| = T_2(x)^{\frac{1}{2}}$ für $x \in F$.

3.22. Definition. Seien $M_j \in \mathbb{R}$, $(1 \le j \le m)$ obere Schranken der Absolutbeträge der komplexen Nullstellen der konjugierten Resolventen $R^{(j)}_{(G,H,F)}(X) \in \mathbb{C}[X]$, also $|\sigma F(\alpha_{j,1}, \ldots, \alpha_{j,n})| \le M_j$ für alle $\sigma \in G//H$. Wir definieren

$$A := \| \left(\mu(\omega_1), \ldots, \mu(\omega_m)\right)^{-1} \| \, (\sum_{j=1}^m M_j^2)^{\frac{1}{2}} + 1 \in \mathbb{R}. \tag{3.23}$$

Die Matrix $(\mu(\omega_1), \ldots, \mu(\omega_m))$ in (3.23) läßt sich aufgrund von $\mathrm{disc}(\omega_1, \ldots, \omega_m) \neq 0$ invertieren.

3.24. Proposition.

(i) Sei $\gamma = \sum_{i=1}^m \lambda_i\omega_i$ *eine Nullstelle des Resolventenpolynoms, welche in* $\mathfrak{o}_F$ *liegt. Dann erhalten wir für die Euklidische Norm der Vektoren* $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m$ *und* $(\lambda_1, \ldots, \lambda_m, 1) \in \mathbb{Z}^{m+1}$

$$\|(\lambda_1, \ldots, \lambda_m)\| < A \text{ und } \|(\lambda_1, \ldots, \lambda_m, 1)\| \le A. \tag{3.25}$$

(ii) Ist umgekehrt $(\mu_1, \ldots, \mu_m) \in \mathbb{Z}^m$ *mit* $\|(\mu_1, \ldots, \mu_m)\| < A$, *so folgt für* $1 \le j \le m$

$$| \sum_{i=1}^m \mu_i\omega_i |_j < A\, W_j \text{ mit}$$

$$W_j := \Big(\|(\mathrm{Re}(\omega_1^{(j)}),\ldots,\mathrm{Re}(\omega_m^{(j)}))\|^2 + \|(\mathrm{Im}(\omega_1^{(j)}),\ldots,\mathrm{Im}(\omega_m^{(j)}))\|^2 \Big)^{\frac{1}{2}} \tag{3.26}$$

Beweis. (i) Da $\gamma \in \mathfrak{o}_F$ nach Voraussetzung eine Nullstelle der Resolvente ist, gilt $|\gamma^{(j)}| \leq M_j$ für $1 \leq j \leq m$, und wir erhalten $\|(\lambda_1, \ldots, \lambda_m)\| \leq \| (\mu(\omega_1), \ldots, \mu(\omega_m))^{-1} \| \, T_2(\gamma)^{\frac{1}{2}} \leq \| (\mu(\omega_1), \ldots, \mu(\omega_m))^{-1} \| \, (\sum_{j=1}^{m} M_j^2)^{\frac{1}{2}} \leq A - 1$. Damit folgt $\|(\lambda_1, \ldots, \lambda_m, 1)\| \leq A$, und (ii) ergibt sich durch direktes Nachrechnen. □

Für eine Approximation $\gamma^*_{(k)}$ einer Nullstelle γ^* der Resolvente mit $\gamma^*_{(k)} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$ gilt für die erste Koordinate der Approximation $(\omega^{*\,-1}_{1,(k)} \gamma^*_{(k,1)}) \cdot \omega^*_{1,(k)} \equiv \gamma^*_{(k,1)} \bmod p^k\mathbb{Z}$. Die Zahl $\gamma^*_{(k,1)}$ läßt sich also bereits modulo p^k als $\mathbb{Z}$-Linearkombination der $\omega^*_{i,(k)}$, $(1 \leq i \leq m)$ schreiben, aber diese $\mathbb{Z}$-Linearkombination genügt im allgemeinen nicht der Schranke (3.25). Auf jeden Fall gilt für $\gamma = \sum_{i=1}^{m} \lambda_i \omega_i$ aber $\|(\lambda_1, \ldots, \lambda_m, 1)\| \leq A$ und das Ziel ist, alle Vektoren in $\operatorname{Kern} \phi$ mit Norm $\leq A$ zu finden. Gleichzeitig wollen wir allerdings die Präzision so einstellen, daß die Norm der Vektoren aus $\operatorname{Kern} \phi$, die nicht zu der eindeutig bestimmten $\mathbb{Z}$-Linearkombination von γ korrespondieren, deutlich größer ist als A.

3.27. Proposition. *Sei* $\Lambda'_{\gamma^*_{(k,1)},(k)} = \{ \sum_{i=1}^{m} z_i u_{i,(k)} \mid z_1, \ldots, z_m \in \mathbb{Z} \}$ *das Teilgitter von* $\Lambda_{\gamma^*_{(k,1)},(k)}$, *welches nur aus den Relationen der* $\omega^*_{i,(k)}$, $(1 \leq i \leq m)$ *besteht. Dann gilt: Es existiert ein* $B : \mathbb{Z}_{>0} \to \mathbb{R}$ *mit*

(i) $\lim\limits_{k \to \infty} B(k) = \infty$,

(ii) $\|x_{(k)}\| \geq B(k)$ *für alle* $x_{(k)} \in \Lambda'_{\gamma^*_{(k,1)},(k)} \setminus \{0\}$,

(iii) $B(k) > 2^{\frac{m}{2}}(A^2 + A)$ *für* $k > m \log_p(2^{\frac{m}{2}}(A^2 + A)) + \sum_{j=1}^{m} \log_p(W_j)$.

Beweis. Sei $x_{(k)} := (\mu_1, \ldots, \mu_m, 0) \in \Lambda'_{\gamma^*_{(k,1)},(k)} \setminus \{0\} \subseteq \mathbb{Z}^{m+1}$. Dann gilt $\phi(x_{(k)}) \equiv 0 \bmod p^k$. Setze $a := \sum_{i=1}^{m} \mu_i \, \omega_i$. Dann ist $a \in \mathfrak{o}_F \setminus \{0\}$ und nach der Produktformel gilt

$$\prod_{\mathfrak{p}} |\, a \,|_{\mathfrak{p}} \prod_{1 \leq j \leq r_1 + 2r_2} |\, a \,|_j = 1.$$

Für das ausgezeichnete Primideal $\mathfrak{p}$ vom Grad eins, welches über p liegt, erhalten wir $|\, a \,|_{\mathfrak{p}} \leq p^{-k}$ und für alle anderen endlichen Stellen gilt $|\, a \,|_{\mathfrak{p}} \leq 1$, da die ω_i, $(1 \leq i \leq m)$ ganzalgebraisch sind. Für das Produkt der unendlichen Stellen muß deshalb $\prod_{j=1}^{r_1+2r_2} |\, a \,|_j \geq p^k$ gelten. Damit folgt

$$\begin{aligned}
p^k &\leq \prod_{j=1}^{r_1+2r_2} |\, (\omega_1, \ldots, \omega_m) \cdot {x_{(k)}}^{tr} \,|_j \\
&\leq \prod_{j=1}^{r_1} \Big(\| \, (\omega_1^{(j)}, \ldots, \omega_m^{(j)}) \, \| \, \| \, x_{(k)} \, \| \Big) \prod_{j=r_1+1}^{2r_2} |\, (\omega_1^{(j)}, \ldots, \omega_m^{(j)}) \cdot {x_{(k)}}^{tr} \,| \\
&\leq \| \, x_{(k)} \, \|^{r_1+2r_2} \prod_{j=1}^{r_1} \| \, (\omega_1^{(j)}, \ldots, \omega_m^{(j)}) \, \| \cdot \\
&\qquad \prod_{j=r_1+1}^{2r_2} \Big(\|(\mathrm{Re}(\omega_1^{(j)}), .., \mathrm{Re}(\omega_m^{(j)}))\|^2 + \|(\mathrm{Im}(\omega_1^{(j)}), .., \mathrm{Im}(\omega_m^{(j)}))\|^2 \Big)^{\frac{1}{2}}
\end{aligned} \tag{3.28}$$

und wir erhalten mit (3.26)

$$\|x_{(k)}\| \geq \left(\frac{p^k}{\prod_{j=1}^m W_j}\right)^{\frac{1}{m}} =: B(k)$$

Es ist offensichtlich, daß $\lim_{k\to\infty} B(k) = \infty$ gilt und (iii) folgt sofort durch umformen. □

3.29. Proposition. *Sei $\gamma = \sum_{i=1}^m \lambda_i\omega_i$ eine Nullstelle des Resolventenpolynoms, welche in $\mathfrak{o}_F$ liegt und $v := (-\lambda_1, \ldots, -\lambda_m, 1)$. Dann sind v und $-v$ die kürzesten Vektoren von $\Lambda_{\gamma^*_{(k,1)},(k)}$ für $k > m\log_p(2^{\frac{m}{2}}(A^2+A)) + \sum_{j=1}^m \log_p(W_j)$.*

Beweis. Es gilt $\phi(v) = -\lambda_1\omega^*_{1,(k)} - \cdots - \lambda_m\omega^*_{m,(k)} + \gamma^*_{(k,1)} = 0 + p^k\mathbb{Z}$. Deshalb ist v ein Element von $\Lambda_{\gamma^*_{(k,1)},(k)}$. Für die Norm von v ergibt sich aus Proposition 3.24, daß $\| v \| \leq A$ gilt. Nach Definition ist $\Lambda_{\gamma^*_{(k,1)},(k)} = \mathbb{Z}\, u_{m+1,(k)} + \Lambda'_{\gamma^*_{(k,1)},(k)}$. Da $u_{m+1,(k)} - v \in \Lambda'_{\gamma^*_{(k,1)},(k)}$ ist, gilt auch $\Lambda_{\gamma^*_{(k,1)},(k)} = \mathbb{Z}\, v + \Lambda'_{\gamma^*_{(k,1)},(k)}$. Sei nun $x_{(k)} \in \Lambda'_{\gamma^*_{(k,1)},(k)}$ und $z \in \mathbb{Z}$ mit

$$\|z\, v + x_{(k)}\| \leq 2^{\frac{m}{2}} A. \tag{3.30}$$

Es genügt zu beweisen, daß $zv + x_{(k)}$ nicht kürzer als v sein kann. Ist $x_{(k)} \neq 0$, so folgt $\| z\, v + x_{(k)} \| \geq | \| x_{(k)} \| - \| z\, v \| | \geq B(k) - 2^{\frac{m}{2}} A^2$, da man mittels (3.30) die Ungleichung $|z| < 2^{\frac{m}{2}} A$ erhält (v hat eine eins an letzter Koordinate). Nach Proposition 3.27 ist aber $2^{\frac{m}{2}} A < B(k) - 2^{\frac{m}{2}} A^2$ im Widerspruch zu (3.30). Somit erhalten wir $x_{(k)} = 0$, und $\|zv\| \leq 2^{\frac{m}{2}} A$. Dies ergibt, daß v und $-v$ in der Tat die kürzesten Elemente von $\Lambda_{\gamma^*_{(k,1)},(k)}$ sind. □

3.31. Bemerkung. Für $k \in \mathbb{Z}_{>0}$ wie in Proposition 3.29 sind verschiedene Nullstellen $\gamma \in \mathfrak{o}_F$ der Resolvente wegen Proposition 3.29 bereits modulo $\mathfrak{p}^k$ verschieden, d.h.

$$\gamma, \tilde{\gamma} \in \mathfrak{o}_F : \gamma = \tilde{\gamma} \Longleftrightarrow \gamma \equiv \tilde{\gamma} \bmod \mathfrak{p}^k.$$

Sind nämlich $\gamma = \sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}_F$ und $\tilde{\gamma} = \sum_{i=1}^m \tilde{\lambda}_i\omega_i \in \mathfrak{o}_F$ verschiedene Nullstellen der Resolvente, die modulo $\mathfrak{p}^k$ gleich sind, so folgt aus Proposition 3.29 mit der dortigen Voraussetzung an $k \in \mathbb{Z}_{>0}$, daß die Vektoren $v = (-\lambda_1, \ldots, -\lambda_m, 1)$ und $\tilde{v} = (-\tilde{\lambda}_1, \ldots, -\tilde{\lambda}_m, 1)$ kürzeste Vektoren des Gitters $\Lambda_{\gamma^*_{(k,1)},(k)} = \Lambda_{\tilde{\gamma}^*_{(k,1)},(k)}$ sind. Da sich die kürzesten Vektoren nur um eine Einheit in $\mathbb{Z}$ unterscheiden, und v als auch $\tilde{v}$ an letzter Koordinate eine Eins stehen haben, müssen sie gleich sein. Es folgt $\gamma = \tilde{\gamma}$.

3.32. Proposition. *Unter den Voraussetzungen von Proposition 3.29 sind v und $-v$ die einzigen ersten LLL-reduzierten Basiselemente des Gitters $\Lambda_{\gamma^*_{(k,1)},(k)}$.*

Beweis. Für das erste LLL-reduzierte Basiselement b_1 gilt $\| b_1 \|^2 \leq 2^m \| x \|^2$ für alle $x \in \Lambda_{\gamma^*_{(k,1)},(k)} \backslash \{0\}$. Es gilt also $\| b_1 \| \leq 2^{\frac{m}{2}} A$ wie in (3.30) und nach dem Beweis von Proposition 3.29 ist $b_1 \in \mathbb{Z}\, v$. Da b_1 Basiselement von $\Lambda_{\gamma^*_{(k,1)},(k)}$ ist, folgt $b_1 = \pm v$. □

Nun können wir den zentralen Satz des Verfahrens von Stauduhar im relativen Zahlkörperfall formulieren.

3.33. Satz. *Seien $M_j \in \mathbb{R}$, $(1 \leq j \leq m)$ obere Schranken der Absolutbeträge der komplexen Nullstellen der Konjugierten $R^{(j)}_{(G,H,F)}(X) \in \mathbb{C}[X]$ wie in Definition 3.22 und $k \in \mathbb{Z}_{>0}$ mit*

$$p^k > \max \left\{ \prod_{j=1}^{m} (2M_j)^{[G:H]},\ 2^{\frac{m^2}{2}} (A^2 + A)^m \prod_{j=1}^{m} W_j \right\}.$$

Ist $\gamma^*_\sigma \in \mathbb{Z}_p[\rho]$ eine Nullstelle von $\iota_\mathfrak{p}(R_{(G,H,F)})(X) \in \mathbb{Z}_p[X]$ mit

(i) $\gamma^*_{\sigma,(k)} \in \mathbb{Z} + p^k \mathbb{Z}[\rho]$,

(ii) $\gamma^*_{\sigma,(k)} \not\equiv \gamma^*_{\tilde{\sigma},(k)} \bmod p^k \mathbb{Z}[\rho]$ für alle $\tilde{\sigma} \in G \,//\, H$ mit $\tilde{\sigma} \neq \sigma$, dann folgt:

Sei der Vektor $v := (-\lambda_1, \ldots, -\lambda_m, \lambda_{m+1})$ erstes LLL-reduziertes Element des Gitters $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$. Sind die Bedingungen

$$(\star)\ \ \lambda_{m+1} = \pm 1 \quad \textit{und} \quad |\sum_{i=1}^{m} \lambda_i \omega_i|_j \leq M_j,\ (1 \leq j \leq m)$$

erfüllt, so gilt $\gamma_\sigma = \lambda_{m+1} \sum_{i=1}^m \lambda_i \omega_i$, $\gamma_\sigma \in \mathfrak{o}_F$ und γ_σ ist eine einfache Nullstelle von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$.
Sei umgekehrt $\gamma_\sigma = \sum_{i=1}^m \lambda_i \omega_i \in \mathfrak{o}_F$ eine einfache Nullstelle von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ und $\lambda_{m+1} := 1$. Dann gelten die Bedingungen $(\star)$ und $v := (-\lambda_1, \ldots, -\lambda_m, \lambda_{m+1})$ ist erstes LLL-reduziertes Element des Gitters $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$.

Beweis. Da v und $-v$ erste LLL-reduzierte Elemente des Gitters $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$ sind, können wir unter den gegebenen Bedingungen ohne Einschränkung $v = (-\lambda_1, \ldots, -\lambda_m, 1)$ annehmen. Nach Voraussetzung gilt $p^k \,|\, \gamma^*_{\sigma,(k,i)}$ für $i = 2, \ldots, [\,\mathbb{Q}(\rho) : \mathbb{Q}\,]$ und aufgrund der Definition des Gitters erhalten wir $\iota_\mathfrak{p}(\sum_{i=1}^m \lambda_i \omega_i) \equiv \gamma^*_{\sigma,(k)} \bmod p^k \mathbb{Z}_p[\rho]$. Es folgt

$$\begin{aligned} \iota_\mathfrak{p}(R_{(G,H,F)})(\iota_\mathfrak{p}(\sum_{i=1}^{m} \lambda_i \omega_i)) &\equiv \iota_\mathfrak{p}(R_{(G,H,F)})(\gamma^*_{\sigma,(k)}) \bmod p^k \mathbb{Z}_p[\rho] \\ &\equiv \iota_\mathfrak{p}(R_{(G,H,F)})(\gamma^*_\sigma) \bmod p^k \mathbb{Z}_p[\rho] \\ &\equiv 0 \bmod p^k \mathbb{Z}_p[\rho] \end{aligned} \tag{3.34}$$

Da $\iota_{\mathfrak{p}}$ ein bewertungserhaltender Monomorphismus ist, gilt $\nu_{\mathfrak{p}}(a) = \nu_p(\iota_{\mathfrak{p}}(a))$ für alle $a \in \mathfrak{o}_F$, und es folgt

$$R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i) \equiv 0 \bmod \mathfrak{p}^k \tag{3.35}$$

Da nach Voraussetzung $|\sum_{i=1}^{m} \lambda_i \omega_i|_j \leq M_j$ und $|\sigma F(\alpha_{j,1}, \ldots, \alpha_{j,n})| \leq M_j$ gilt, erhalten wir

$$\begin{aligned} |R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)|_j &= \prod_{\sigma \in G//H} |\sum_{i=1}^{m} \lambda_i \omega_i^{(j)} - \sigma F(\alpha_{j,1}, \ldots, \alpha_{j,n})| \\ &\leq \prod_{\sigma \in G//H} 2M_j \\ &\leq (2M_j)^{[G:H]}, \qquad (1 \leq j \leq m) \end{aligned}$$

und somit

$$\prod_{j=1}^{m} |R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)|_j < p^k. \tag{3.36}$$

Aus $\mathfrak{p}^k \mid R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)$ folgt einerseits $|R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)|_{\mathfrak{p}} \leq p^{-k}$ für das ausgezeichnete Primideal $\mathfrak{p}$ vom Grad eins, welches über p liegt, und für alle anderen endlichen Stellen gilt $|R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)|_{\mathfrak{p}} \leq 1$, da $R_{(G,H,F)} \in \mathfrak{o}_F[X]$ und die ω_i ganzalgebraisch sind. Für das Produkt der unendlichen Stellen erhalten wir deshalb nach der Produktformel $\prod_{j=1}^{m} |R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i)|_j \geq p^k$. Dies steht im Widerspruch zu (3.36) und wiederum nach der Produktformel muß $R_{(G,H,F)}(\sum_{i=1}^{m} \lambda_i \omega_i) = 0$ gelten. Mittels Annahme (ii) erhalten wir $\gamma_\sigma = \sum_{i=1}^{m} \lambda_i \omega_i \in \mathfrak{o}_F$, und daß γ_σ eine einfache Wurzel von $R_{(G,H,F)}$ ist. Die Rückrichtung folgt aus Proposition 3.32. □

3.37. Bemerkung. Das Pendant zu Satz 3.33 für den absoluten Zahlkörperfall, wie es zuerst von Darmon und Ford [19] zur Verifikation von Polynomen mit Galoisgruppe $M(11)$ und $M(12)$ benutzt wurde, erhält man wie folgt: Im absoluten Fall gilt $m = 1$, $r_1 = 1, r_2 = 0$, $\mathfrak{o}_F = \mathbb{Z}$, und als Ganzheitsbasis haben wir $\omega_1 = 1$. Mittels Lemma 3.5 erhalten wir die Erweiterungen $\mathcal{E} := \mathbb{Q}_p(\rho)$ und $E := \mathbb{Q}(\rho)$ für $F = \mathbb{Q}$ und eine Primzahl p, so daß $f \in \mathbb{Z}[x]$ modulo p separabel ist. Die Zahl $M := M_1 \in \mathbb{R}$ ist dann eine obere Schranke der Absolutbeträge der komplexen Nullstellen des Resolventenpolynoms, $W_1 = 1$ und $A = M + 1$. Für $\gamma^*_{\sigma,(k)} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$ vereinfacht sich das Gitter $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$ zu

$$\Lambda_{\gamma^*_{\sigma,(k,1)},(k)} = \left\{ \mathbb{Z}\,(p^k, 0) + \mathbb{Z}\,(\gamma^*_{\sigma,(k,1)}, 1) \right\}.$$

Bezeichnet $\lfloor \gamma^*_{\sigma,(k,1)} \rfloor_{p^k}$ den eindeutig bestimmten Repräsentanten von $\gamma^*_{\sigma,(k,1)} \in \mathbb{Z}$ in $[-(p^k-1)/2,\, p^k/2]$, so ist das betrachtete erste LLL-reduzierte Element v von

der Gestalt $v = (\lfloor \gamma^*_{\sigma,(k,1)} \rfloor_{p^k}, 1)$ mit $|\lfloor \gamma^*_{\sigma,(k,1)} \rfloor_{p^k}| \leq M$ (falls $\gamma_\sigma \in \mathbb{Z}$ ist). Der Inklusionstest vereinfacht sich in diesem Fall und kann wie folgt durchgeführt werden (vgl. [30]):
Sei $k \in \mathbb{Z}$ mit $p^k > (2M)^{[G:H]}$. Ist $\gamma^*_\sigma \in \mathbb{Z}_p[\rho]$ eine Nullstelle von $R_{(G,H,F)}(X) \in \mathbb{Z}[X]$ mit (i) $\gamma^*_{\sigma,(k)} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$, (ii) $\gamma^*_{\sigma,(k)} \not\equiv \gamma^*_{\tilde{\sigma},(k)} \bmod p^k\mathbb{Z}[\rho]$ für alle $\tilde{\sigma} \in G // H$ mit $\tilde{\sigma} \neq \sigma$, (iii) $|\lfloor \gamma^*_{\sigma,(k,1)} \rfloor_{p^k}| \leq M$, so ist $\gamma_\sigma = \lfloor \gamma^*_{\sigma,(k,1)} \rfloor_{p^k} \in \mathbb{Z}$ eine einfache Nullstelle von $R_{(G,H,F)}(X) \in \mathbb{Z}[X]$. Umgekehrt erfüllt jede einfache Nullstelle von $R_{(G,H,F)}$ in $\mathbb{Z}$ die Bedingungen $(i) - (iii)$.

Wir erhalten den folgenden Rekonstruktionsalgorithmus:

3.38. Algorithmus. *(Rekonstruktion $F = \mathbb{Q}(\delta)$)*

Eingabe: *Approximierte Nullstelle der Resolvente $\gamma^*_{\sigma,(k)} \in \mathbb{Z}[\rho]$ für $k \in \mathbb{Z}_{>0}$ wie in Proposition 3.29, (fixierte) Ganzheitsbasis $\omega_1, \ldots, \omega_m$ von $\mathfrak{o}_F$, unverzweigtes Primideal $\mathfrak{p} \subset \mathfrak{o}_F$ vom Grad eins wie in Algorithmus 3.10, obere Schranken $M_j \in \mathbb{R}$, $(1 \leq j \leq m)$ der Absolutbeträge der komplexen Nullstellen der Konjugierten $R^{(j)}_{(G,H,F)}(X) \in \mathbb{C}[X]$ wie in Satz 3.33, Schranke $A \in \mathbb{R}$ wie in* (3.23).

Ausgabe: *Aussage „$\gamma_\sigma \notin \mathfrak{o}_F$“ oder*
$\gamma'_\sigma \in \mathfrak{o}_F$ mit $\gamma'_\sigma \equiv \gamma_\sigma \bmod \mathfrak{p}^k$. Ist $\gamma_\sigma \in \mathfrak{o}_F$, dann ist $\gamma'_\sigma = \gamma_\sigma$.
Ist $k > [G:H] \sum_{j=1}^m \log_p(2M_j)$, dann Aussage „$\gamma_\sigma \notin \mathfrak{o}_F$“ oder eine Nullstelle $\gamma'_\sigma \in \mathfrak{o}_F$ der Resolvente mit $\gamma'_\sigma \equiv \gamma_\sigma \bmod \mathfrak{p}^k$.
Ist $\gamma_\sigma \in \mathfrak{o}_F$, dann ist $\gamma'_\sigma = \gamma_\sigma$.

1. *(Pseudo-Test) Ist $\gamma^*_{\sigma,(k)} \notin \mathbb{Z} + p^k\mathbb{Z}[\rho]$, so gebe „$\gamma_\sigma \notin \mathfrak{o}_F$“ aus und terminiere.*
2. *(Aufstellung des Gitters $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$) Bestimme $\omega^*_{i,(k)} \in \mathbb{Z}$ mit $\omega^*_{i,(k)} \equiv \omega_i \bmod \mathfrak{p}^k$ und setze $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)} =< u_{1,(k)}, \ldots, u_{m+1,(k)} >$ für Vektoren $u_{i,(k)}$, $(1 \leq i \leq m+1)$ aus* (3.19).
3. *(LLL-Reduktion) Berechne erstes LLL-reduziertes Basiselement $v = (\lambda_1, \ldots, \lambda_{m+1})$ von $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$.*
4. *(Ende) Ist $\lambda_{m+1} = \pm 1$, $\|v\| \leq A$ und $|\sum_{i=1}^m \lambda_i \omega_i|_j \leq M_j$, $(1 \leq j \leq r_1 + r_2)$, so gebe $\gamma'_\sigma := -\lambda_{m+1} \sum_{i=1}^m \lambda_i \omega_i$ aus. Ansonsten, gebe „$\gamma_\sigma \notin \mathfrak{o}_F$“ aus. Terminiere.*

Beweis. Die Korrektheit des Algorithmus ergibt sich aus den folgenden Überlegungen: Gibt der Algorithmus „$\gamma_\sigma \notin \mathfrak{o}_F$“ zurück, so ist dies korrekt. Denn wäre $\gamma_\sigma = \sum_{i=1}^m \lambda_i \omega_i$ eine Nullstelle der Resolvente in $\mathfrak{o}_F$, so wären die Bedingung in

Schritt 1 nach Bemerkung 3.15 erfüllt. In Schritt 4 wäre dann $v = (\lambda_1, \ldots, \lambda_m, -1)$ nach Proposition 3.29, Proposition 3.32 und der Voraussetzung an k und somit Bedingung $\lambda_{m+1} = \pm 1$ erfüllt. Aus Proposition 3.24 (i) folgt dann $\|v\| \leq A$, da die M_j, $(1 \leq j \leq m)$ groß genug gewählt sind. Schließlich erhalten wir aufgrund der Annahme, daß $\gamma_\sigma = \sum_{i=1}^m \lambda_i \omega_i \in \mathfrak{o}_F$ eine Nullstelle der Resolvente ist, daß auch $|\sum_{i=1}^m \lambda_i \omega_i|_j \leq M_j$ gelten muß. Nehmen wir nun an, daß $\gamma'_\sigma \in \mathfrak{o}_F$ zurückgegeben wird. Aufgrund der Definition des Gitters $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$ gilt $\gamma'_\sigma \equiv \gamma_\sigma \bmod \mathfrak{p}^k$. Ist $\gamma_\sigma \in \mathfrak{o}_F$, so folgt $\gamma_\sigma = \gamma'_\sigma$ aufgrund von Proposition 3.29, Proposition 3.32 und der Voraussetzung an k. Ist die Präzision größer als $[\,G:H\,]\sum_{j=1}^m \log_p(2M_j)$ und wird $\gamma'_\sigma \in \mathfrak{o}_F$ zurückgegeben, so verbleibt zu zeigen, daß γ'_σ eine Nullstelle der Resolvente ist. Es gilt $|\sum_{i=1}^m \lambda_i \omega_i|_j \leq M_j, (1 \leq j \leq r_1 + r_2)$ und der Beweis zu Satz 3.33 liefert in der Tat, daß γ'_σ Nullstelle der Resolvente ist. □

Somit haben wir gesehen, daß für den Nullstellenbeweis kein gesonderter Algorithmus benötigt wird. Wir vereinbaren folgende

3.39. Bezeichnung. *Wir bezeichnen* $m \log_p(2^{\frac{m}{2}}(A^2 + A)) + \sum_{j=1}^m \log_p(W_j)$ *aus Proposition 3.29 im folgenden auch als Gitterpräzision und* $[G:H]\sum_{j=1}^m \log_p(2M_j)$ *aus Algorithmus 3.38 als Nullstellenpräzision.*

3.40. Bemerkung. (i) Die oberen Schranken $M_j \in \mathbb{R}$, $(1 \leq j \leq r_1 + r_2)$ der Absolutbeträge der komplexen Nullstellen der Konjugierten $R^{(j)}_{(G,H,F)}$ werden in unserer Implementierung zur Laufzeit berechnet. Pro Galoisgruppenberechnung berechnen wir einmal $\alpha_{j,\max} := \max_{1 \leq i \leq n}\{\, |\alpha_{j,i}| \mid f^{(j)}(\alpha_{j,i}) = 0\} \in \mathbb{R}$ für $1 \leq j \leq r_1 + r_2$ und speichern diese Werte. Das aktuelle G-relative H-invariante Polynom $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ wird dann geeignet an den Stellen $x_1 = \cdots = x_n = \alpha_{j,\max}$ ausgewertet, um M_j zu erhalten. Unter geeignet verstehen wir, daß bei G-relativen H-invarianten Polynomen, beispielsweise der Form $(x_1 - x_2)(x_1 - x_3)\cdots$, Subtraktionen durch Additionen ersetzt werden. Zu beachten ist, daß im Fall einer Tschirnhausentransformation die $\alpha_{j,\max}$ für $1 \leq j \leq r_1 + r_2$ natürlich aktualisiert werden müssen.

(ii) Zur effektiven Berechnung der Schranke $A \in \mathbb{R}$ aus (3.25) müssen wir eine Matrixnorm wählen, die mit der Euklidischen Vektornorm des $\mathbb{R}^m$ verträglich ist. Die von der Vektornorm induzierte Matrixnorm $\| M \|_{ind} := sup_{\| x \| = 1} \frac{\| Mx \|}{\| x \|}$, $(M \in \mathbb{R}^{m \times m}, x \in \mathbb{R}^m)$ liefert die beste Abschätzung, ist aber schlecht zu berechnen. In Stewart [79], Kapitel 4, Satz 2.12 und Stummel, Hainer [82], S. 107 (21) wird gezeigt, daß für die symmetrische Matrix $M\,M^{tr}$ die induzierte Matrixnorm $\|M\,M^{tr}\|_{ind}$ gleich $\|M\|^2_{ind}$ ist und $\|M\,M^{tr}\|_{ind}$ gerade den Absolutbetrag des größten Eigenwertes λ_{max} von $M\,M^{tr}$ darstellt. Außerdem genügt jeder Eigenwert der quadratischen Matrix $M\,M^{tr}$, also insbesondere λ_{max}, der Ungleichung

$$|\lambda_{max}| \leq \|M\,M^{tr}\|,$$

für jede beliebige, mit der Euklidischen Vektornorm auf dem $\mathbb{R}^m$ verträglichen Matrixnorm. Zur Abschätzung von $|\lambda_{max}|$ haben wir in unserer Implementierung für die Matrix $MM^{tr} = (m_{ij})_{1\leq i,j\leq m}$ die mit der Euklidischen Vektornorm verträgliche Quadratsummennorm

$$\|M\,M^{tr}\| = \left(\sum_{i,j=1}^{m} |m_{ij}|^2\right)^{\frac{1}{2}}$$

(vgl. Stummel, Hainer [82], S.98) gewählt.

(*iii*) In Schritt 2 von Algorithmus 3.38 ist es sinnvoll, das Gitter $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$ nicht für jede Nullstelle $\gamma^*_{\sigma,(k)} \in \mathbb{Z}[\rho]$ komplett neu zu berechnen. Zu einer gegebenen Präzision wird ein Gitter des $\mathbb{R}^m$, welches wir aus dem Gitter $\Lambda'_{\gamma^*_{(k,1)},(k)} \subset \mathbb{R}^{m+1}$ durch Streichung der $m+1$-ten Koordinaten (diese sind Null) aller Basisvektoren erhalten, vorberechnet und LLL-reduziert. Dadurch kann der Rechenaufwand für Schritt 3 insgesamt wesentlich verringert werden. Für Primideale $\mathfrak{p}$ vom Grad eins kann die Berechnung des Ideals $\mathfrak{p}^k$ sehr effektiv gestaltet werden, so daß sich auch hier Berechnungszeiten einsparen lassen. Die Ideen hierzu werden in Pohst [67] ausführlich dargestellt (siehe aber auch Sektion 3.5 und (3.45)).

(*iv*) Wie schon in der Einleitung erwähnt, können wir bei Betrachtung einer einzigen Nullstelle der Resolvente und den gewählten Präzisionen mit dem Basisalgorithmus 3.38 nicht entscheiden, ob das zur Approximation $\gamma^*_{\sigma,(k)} \in \mathbb{Z}[\rho]$ gehörende Element γ_σ ein Element in $\mathfrak{o}_F$ ist. Wir können nur feststellen, ob es eine Wurzel γ'_σ der Resolvente in $\mathfrak{o}_F$ gibt, die zu γ_σ kongruent modulo dem Primideal $\mathfrak{p}^k$ ist. Durch Betrachtung aller anderen Nullstellen der Resolvente ist dieser Algorithmus aber vollkommen ausreichend für den Inklusionstest, bei dem es nur darum geht, zu beweisen oder zu widerlegen, ob die Resolvente eine einfache Nullstelle in $\mathfrak{o}_F$ hat. War nämlich γ_σ kein Element in $\mathfrak{o}_F$, obwohl der Algorithmus bei $k > \max\{\text{Nullstellenpräzision, Gitterpräzision}\}$ eine Nullstelle $\gamma'_\sigma \in \mathfrak{o}_F$ zurückgegeben hat, so ist nach Berechnung aller Nullstellen der Resolvente γ'_σ mindestens eine doppelte Nullstelle. Dies hat dann aber eine Tschirnhausentransformation in Algorithmus 2.20 zur Folge, falls es keine andere einfache Nullstelle gibt.

(*v*) In unserer Implementierung liften wir die Approximationen zunächst zu einer heuristischen Schranke k' mit

$$\begin{aligned} k' = \max\{\ &\min\{\, 3\textstyle\sum_{j=1}^{m} \log_p(2M_j),\ [\,G\!:\!H\,] \sum_{j=1}^{m} \log_p(2M_j)\,\},\\ &m \log_p(2^{\frac{m}{2}}(A^2+A)) + \textstyle\sum_{j=1}^{m} \log_p(W_j)\,\}. \end{aligned}$$

Approximationen $\gamma^*_{\sigma,(k')}$, deren Koeffizienten der ρ-Potenzen nicht durch $p^{k'}$ teilbar sind, erfüllen den Pseudo-Test in Schritt 1 nicht und können somit zu keiner

ganzalgebraischen Nullstelle korrespondieren. Dieser Test ist natürlich nur anwendbar, wenn der Grad des Minimalpolynoms von ρ größer als eins ist, und ist dann allerdings sehr effektiv. In einem zweiten Durchlauf liften wir die restlichen Nullstellen zu der aktuellen Präzision k.

3.4 Nenner

Oftmals möchte man vermeiden, die Maximalordnung $\mathfrak{o}_F$ explizit auszurechnen, in manchen Fällen ist es auch kaum möglich. Statt dessen bietet es sich an, die Gleichungsordnung $\mathbb{Z}[\delta]$ oder eine andere Ordnung $\mathfrak{o}$ von F zu benutzen. Ziel dieses Abschnittes ist es, den Inklusionstest auf den Fall zu verallgemeinern, für den wir die Galoisgruppe für ein normiertes irreduzibles Polynom $f(x) \in \mathfrak{o}[x]$ berechnen möchten. Sei also $p \in \tilde{\mathfrak{p}} \subset \mathfrak{o}$ ein Primideal vom Grad eins mit $\operatorname{disc} \mathfrak{o} \notin \tilde{\mathfrak{p}}$ wie in Bemerkung 3.11 gegeben. Bezeichne $\varpi_1, \ldots, \varpi_m$ eine fest gewählte $\mathbb{Z}$-Basis von $\mathfrak{o}$, wobei wir wieder o.B.d.A annehmen wollen, daß $\varpi_1 \notin \tilde{\mathfrak{p}}$ ist. Es gilt $F = \mathbb{Q}\varpi_1 + \cdots + \mathbb{Q}\varpi_m$.
Wir betrachten als erstes die folgende allgemeine Rekonstruktionsaufgabe: Sei $d \in \mathbb{Z}_{>0}$ mit $p \nmid d$ beliebig und $\gamma \in \mathfrak{o}/d$. Es gilt $\iota_{\mathfrak{p}}(\mathfrak{o}/d) \subseteq \mathbb{Z}_p$. Wir gehen davon aus, daß d und die Darstellung von γ in der Basis von $\mathfrak{o}$ unbekannt sind und wollen diese nun ausgehend von einer Approximation $\gamma^*_{(k)}$ von γ in $\mathbb{Z}_p$ berechnen bzw. rekonstruieren. Wir benötigen dazu zusätzlich

(*i*) entweder ein Vielfaches $d_V \in \mathbb{Z}_{>0}$ des Nenners d,

(*ii*) oder eine obere Schranke $d_S \in \mathbb{Z}_{>0}$ des Nenners d.

Außerdem setzen wir wieder $A := \|(\mu(\varpi_1), \ldots, \mu(\varpi_m))^{-1}\| \, T_S^{1/2} + 1$ für eine obere Schranke T_S der T_2-Norm von γ und $W_j := (\|(\operatorname{Re}(\varpi_1^{(j)}), \ldots, \operatorname{Re}(\varpi_m^{(j)}))\|^2 + \|(\operatorname{Im}(\varpi_1^{(j)}), \ldots, \operatorname{Im}(\varpi_m^{(j)}))\|^2)^{1/2}$ für $1 \leq j \leq m$ (vgl. Definition 3.22 und Proposition 3.24).
Im Fall (*i*) betrachten wir das Element $d_V\gamma^*_{(k)}$. Dies ist eine Approximation des Elements $d_V\gamma \in \mathfrak{o}$, und wir können so das Problem der Rekonstruktion von Elementen aus $\mathfrak{o}/d$ unter Benutzung der Basis von $\mathfrak{o}$ in ein Problem der Rekonstruktion von Elementen aus $\mathfrak{o}$ ohne Nenner reduzieren. Dazu verwenden wir W_j wie oben, für die Schranke A bezüglich $d_V\gamma$ den Wert $d_V(A-1)+1$, und das Gitter $\Lambda_{d_V\gamma^*_{(k)},(k)}$ bezüglich der Basis $\varpi_1, \ldots, \varpi_m$. Ist die Präzision größer als

$$k > m \log_p \left(2^{\frac{m}{2}} \left(\left(d_V(A-1)+1 \right)^2 + d_V(A-1)+1 \right) \right) + \sum_{j=1}^{m} \log_p(W_j) \qquad (3.41)$$

so liefert uns das erste LLL-reduzierte Basiselement die Koeffizienten von $d_V\gamma$ in der Basis von $\mathfrak{o}$. Nach Division durch d_V erhalten wir die gesuchte Darstellung von γ in der Basis von $\mathfrak{o}$.

Im Fall (ii) betrachten wir das Gitter $\Lambda_{\gamma^*_{(k)},(k)}$ bezüglich der Basis $\varpi_1,\ldots,\varpi_m$. Gilt $\gamma=\sum_{i=1}^m(\lambda_i/d)\,\varpi_i\in\mathfrak{o}/d$, so liegt der Vektor $v:=(-\lambda_1,\ldots,-\lambda_m,d)\in\mathbb{Z}^{m+1}$ in dem Gitter $\Lambda_{\gamma^*_{(k)},(k)}$, und es gilt $\|v\|\le|d|A$. Ähnlich wie in den Beweisen von Proposition 3.29 und Proposition 3.32 läßt sich zeigen, daß v und $-v$ die kürzesten Vektoren und einzigen ersten LLL-reduzierten Basiselemente des Gitters $\Lambda_{\gamma^*_{(k)},(k)}$ für $k>m\log_p(2^{m/2}|d|^2(A^2+A))+\sum_{j=1}^m\log_p(W_j)$ sind. Diese Forderung an die Präzision ist sicherlich für

$$k \;>\; m\log_p(2^{\frac{m}{2}}d_S^2(A^2+A))+\sum_{j=1}^m\log_p(W_j) \tag{3.42}$$

erfüllt. Nach Division durch d erhalten wir wieder die gesuchte Darstellung von γ in der Basis von $\mathfrak{o}$.

Für den Fall, daß bereits $\gamma\in\mathfrak{o}_F$ gilt, erhalten wir aufgrund des bekannten Zusammenhang zwischen der Ordnung $\mathfrak{o}$ und der Maximalordnung $\mathfrak{o}_F$ (vgl. Neukirch [62], Kapitel I, §2, Satz 2.12),

3.43. Proposition. *Für den Index* $[\,\mathfrak{o}_F:\mathfrak{o}\,]$ *gilt* $[\,\mathfrak{o}_F:\mathfrak{o}\,]\,\mathfrak{o}_F\subseteq\mathbb{Z}\varpi_1+\cdots+\mathbb{Z}\varpi_m$, *und* $[\,\mathfrak{o}_F:\mathfrak{o}\,]^2$ *ist ein Teiler von* $\operatorname{disc}(\mathfrak{o})=\operatorname{disc}(\varpi_1,\ldots,\varpi_m)$.

daß $d_V:=|\operatorname{disc}(\mathfrak{o})|$ und $d_S:=\sqrt{|\operatorname{disc}(\mathfrak{o})|}$ gilt. Die benötigte Präzision (3.42) von Methode (ii) ist hier geringer als die Präzision (3.41) von Methode (i), weil $d_S=\sqrt{d_V}$ ist. Somit hängt der Unterschied dieser beiden Methoden von der Kenntnis eines günstigen berechenbaren Nennervielfachen ab.

Kommen wir nun zu unserer Ausgangsfragestellung zurück und wenden uns dem Nullstellenbeweis des rekonstruierten Elements zu. Wir nehmen an, daß wir ein Element $\gamma'=\sum_{i=1}^m(\lambda_i/d)\,\varpi_i$ mit $|\gamma'|_j\le M_j$, $(1\le j\le m)$ für $M_j\in\mathbb{R}$ wie in Definition 3.22 und $R_{(G,H,F)}(\gamma')\equiv 0\bmod\tilde{\mathfrak{p}}^k$ für ein $k\in\mathbb{Z}_{>0}$ gegeben haben. Prinzipiell bieten sich nun zwei Vorgehensweisen an, da man entweder für $\operatorname{disc}(\mathfrak{o})\gamma'\in\mathfrak{o}$ oder für γ' den Nullstellenbeweis antreten kann. Im ersten Fall ist das Element $\operatorname{disc}(\mathfrak{o})\gamma'\in\mathfrak{o}$ Nullstelle des Polynoms $\tilde{R}(X):=\operatorname{disc}(\mathfrak{o})^{[G:H]}R_{(G,H,F)}(X/\operatorname{disc}(\mathfrak{o}))\in\mathfrak{o}[X]$, wenn

$$k>[\,G:H\,]\sum_{j=1}^m\log_p(2|\operatorname{disc}(\mathfrak{o})|M_j) \tag{3.44}$$

ist, wobei $|\operatorname{disc}(\mathfrak{o})|M_j$ obere Schranken der Absolutbeträge der komplexen Nullstellen der Konjugierten von $\tilde{R}^{(j)}(X)\in\mathbb{C}[X]$ für $1\le j\le m$ sind. Im zweiten

Fall haben wir für die Nullstellenpräzision von γ' zwei Möglichkeiten: Entweder verwenden wir die Präzision wie in (3.44). Der zusätzliche Faktor $|\mathrm{disc}(\mathfrak{o})|^{[G:H]m}$ ergibt sich, wenn in diesem Fall im Beweis von Satz 3.33 das Produkt der über d liegenden Primideale der Maximalordnung $\prod_{\mathfrak{p}|d} |R_{(G,H,F)}(\sum_{i=1}^{m}(\lambda_i/d)\,\varpi_i)|_{\mathfrak{p}}$ durch $|\mathrm{disc}(\mathfrak{o})|^{[G:H]m}$ abgeschätzt wird. Die zweite Möglichkeit besteht aus einem zusätzlichen Test, der es uns dann aber erlaubt, mit einer niedrigeren Präzision zu rechnen. Überprüft wird, ob γ' ganzalgebraisch ist (dies kann anhand des Minimalpolynoms ersehen werden). Ist dies der Fall, so dürfen wir dann mit der niedrigen Nullstellenpräzision von $k > [\,G:H\,]\sum_{j=1}^{m}\log_p(2M_j)$ wie in Satz 3.33 rechnen.

Somit braucht die Maximalordnung von F zur Durchführung des Inklusionstests nicht explizit bekannt zu sein. Wie wir an den Ausführungen sehen, muß dafür mit einer größeren Präzision gerechnet werden.

3.5 Vergleich mit anderen Verfahren

Wir befinden uns wieder in der Situation wie in Abschnitt 3.4. Zum Problem der Rekonstruktion von algebraischen Zahlen findet man in der Literatur verschiedene Verfahren (Lenstra [49], Pohst [67], Roblot [71] und Fieker, Friedrichs [25]). Gemeinsam ist allen Arbeiten, daß sie für $d = 1$ versuchen, die modulare Lösung $\gamma^*_{(k)}$ modulo der Idealbasis von $\tilde{\mathfrak{p}}^k$ so abzuändern, daß sie den kürzesten Repräsentanten bzw. ein Element mit kleinster T_2-Norm von $\gamma^*_{(k)} + \tilde{\mathfrak{p}}^k$ finden. Dies geschieht unter zu Hilfenahme geeigneter m-dimensionaler Gitter. Während Pohst [67] und Roblot [71] unter Verwendung der Minkowski-Abbildung mit reellen Gittern arbeiten und reelle LLL-Reduktion verwenden, benutzen Fieker und Friedrichs [25] ganzzahlige Gitter und wie wir den ganzzahligen LLL-Algorithmus. Eine weitere Möglichkeit für beliebiges d besteht in der Betrachtung eines $(m+1)$-dimensionalen Gitters, für welches bei entsprechender Wahl von k das erste LLL-reduzierte Basiselement die gesuchte Rekonstruktion darstellt. Diese Methode wird ebenfalls in Fieker und Friedrichs [25] beschrieben. Wir wollen im folgenden ihre Methoden mit der unsrigen vergleichen.

Zunächst einmal fällt die unterschiedliche Betrachtungsweise des Problems auf, die darauf hoffen läßt, verschiedene Präzisionen für die Rekonstruktion zu erhalten. In der Praxis stellt es sich nämlich heraus, daß die Berechnung der LLL-reduzierten Basis des verwendeten Gitters am zeitaufwendigsten ist, weshalb kleine Exponenten k wünschenswert sind. Während uns daran gelegen ist, im Relationenmodul $\mathrm{Kern}\,\phi$ (vgl. Proposition 3.17) eine Linearkombination mit möglichst „kleinen“ Koeffizienten der $\varpi_{i,(k)}$ und des zu rekonstruierenden $\gamma^*_{(k)}$ zu finden,

verfolgen Fieker und Friedrichs die oben beschriebenen Ansätze. In ihrem Artikel beschreiben sie genauer gesagt zwei verschiedene Methoden zur Rekonstruktion:

Die erste Methode rekonstruiert Elemente ohne Nenner ($d = 1$) einer beliebigen Ordnung $\mathfrak{o}$ und verwendet das zur Ordnung $\mathfrak{o}$ isomorphe Gitter $\Lambda_{\mathfrak{o}} := \mathbb{Z}^m$ bezüglich der Abbildung $\delta_{\mathbb{Z}} : \mathfrak{o} \to \mathbb{Z}^m : \sum_{i=1}^{m} \lambda_i \varpi_i \mapsto (\lambda_1, \ldots, \lambda_m)^{tr}$. Für ein Primideal $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ ist das Gitter $\Lambda_{\tilde{\mathfrak{p}}^k}$ definiert als $\delta_{\mathbb{Z}}(\tilde{\mathfrak{p}}^k)$. Diese Methode benötigt nur eine initiale LLL-Reduktion für die Idealbasis von $\tilde{\mathfrak{p}}^k$, und die gesuchten Elemente werden durch Runden gebrochen rationaler Koeffizienten erhalten.

Die zweite Methode wurde zu dem Zweck entwickelt, nicht ganzalgebraische Elemente für beliebiges $d \in \mathbb{Z}_{>0}$ und beliebige Ordnungen zu rekonstruieren. Hier wird das zum Ideal $\tilde{\mathfrak{p}}^k$ isomorphe Gitter $\Lambda_{\tilde{\mathfrak{p}}^k}$ in das Gitter $\mathbb{Z}^{m+1}$ mittels der Abbildung $\mathbb{Z}^m \to \mathbb{Z}^{m+1} : (z_1, \ldots, z_m)^{tr} \mapsto (0, z_1, \ldots, z_m)^{tr}$ eingebettet und um den Vektor $(1, \varpi_{1,(k)}^{*-1} \gamma_{(k)}^{*}, 0, \ldots, 0)^{tr}$ erweitert, wobei wir o.B.d.A. $\varpi_1 \notin \tilde{\mathfrak{p}}$ annehmen. Dieses Gitter wollen wir mit $\Lambda_{\tilde{\mathfrak{p}}^k,\gamma}$ bezeichnen und mit unserem Gitter vergleichen.

Seien das Primideal $\tilde{\mathfrak{p}}$ vom Grad eins und die Basis $\varpi_1 \ldots \varpi_m$ von $\mathfrak{o}$ wie in Sektion 3.4 fixiert und mit $\beta_1, \ldots \beta_m$ eine $\mathbb{Z}$-Basis des Ideals $\tilde{\mathfrak{p}}^k$ bezeichnet. Die Übergangsmatrix $B = (b_{ij}) \in \mathbb{Z}^{m \times m}$ der Basis von $\mathfrak{o}$ zu der $\mathbb{Z}$-Basis des Ideals $\tilde{\mathfrak{p}}^k$ kann in oberer Dreiecksgestalt mit $b_{ii} \geq 0$ und $b_{ii} > b_{ij}$ $(1 \leq i < j)$ gewählt werden (vgl. Pohst [68], S.11, Satz 1.3). Da wir für die Basis von $\mathfrak{o}$ o.B.d.A $\varpi_1 \notin \tilde{\mathfrak{p}}$ angenommen hatten, folgt aus $\nu_{\tilde{\mathfrak{p}}}(b_{11}\varpi_1) = \nu_{\tilde{\mathfrak{p}}}(\beta_1) \geq k$, daß $\nu_{\tilde{\mathfrak{p}}}(b_{11}) \geq k$. Somit ist b_{11} ein Vielfaches von p^k. Da $p^k = \mathrm{N}(\tilde{\mathfrak{p}}^k) = \det(B)$ gilt, ist $b_{11} = p^k$ und B ist von der Gestalt

$$(\beta_1, \ldots, \beta_m) = (\varpi_1, \ldots, \varpi_m) \begin{pmatrix} p^k & b_{12} & b_{13} & \ldots & b_{1m} \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \cdots & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \tag{3.45}$$

Es folgt $\beta_i \equiv b_{1,i}\varpi_1 + \varpi_i \bmod \tilde{\mathfrak{p}}^k$, was äquivalent ist zu $b_{1,i} \equiv -\varpi_1^{-1}\varpi_i \bmod \tilde{\mathfrak{p}}^k$, $(2 \leq i \leq m)$. Dies bedeutet aber nichts anderes, als daß die Gitter $\Lambda_{\tilde{\mathfrak{p}}^k,-\gamma}$ und $\Lambda_{\gamma_{(k)}^{*},(k)}$ isomorph sind.

Die benötigte Gitterpräzision zur Rekonstruktion in [25] wurde leider nur für die erste Methode, d.h. $d = 1$, vollständig ausgearbeitet, so daß wir zunächst einmal diese Präzision mit unserer aus (3.41) bzw. (3.42) für $d = 1$ vergleichen. Wir merken an, daß diese Präzision in adaptierter Form auch für die zweite Methode (Rekonstruktion mit Nenner) in KASH-Implementierungen [38] verwendet wird.

In unserer Notation lautet die Schranke aus Fieker und Friedrichs [25], Theorem 1:

$$p^k \;>\; 2^{\frac{m^2(m-1)}{8}+m}\, A^m \left(\frac{1}{m}\sum_{j=1}^{m} W_j^2\right)^{\frac{m}{2}}. \tag{3.46}$$

Wir bemerken, daß in der Notation von Fieker und Friedrichs $c_2 c = A^2$ und $c_1 = \sum_{j=1}^{m} W_j^2$ gilt. Vergleicht man diese Schranke mit unserer Schranke

$$p^k \;>\; 2^{\frac{m^2}{2}} (A^2 + A)^m \prod_{j=1}^{m} W_j \tag{3.47}$$

so fällt besonders ins Gewicht, daß bei Fieker und Friedrichs in der zweier Potenz der Exponent von m kubisch eingeht. Dies erklärt auch das Verhalten bei den Testdurchläufen: Je größer der Grad m, desto größer die Differenz der verschiedenen Präzisionen. Bei gleichbleibendem Grad m und betraglich wachsender Nullstellengröße geht allerdings in (3.46) die Größe A nur linear ein. Dieser Vorteil würde sich in der Gesamtbetrachtung bei uns allerdings nicht wesentlich bemerkbar machen, da die Nullstellenpräzision ohnehin quadratisch (Index $[\,G : H\,]$ ist mindestens 2) von der Nullstellengröße abhängt. Schließlich wollen wir noch anmerken, daß aufgrund der Ungleichung zwischen dem geometrischen und dem arithmetischen Mittel $(\frac{1}{m}\sum_{j=1}^{m} W_j^2)^{\frac{m}{2}} \geq \prod_{j=1}^{m} W_j$ gilt, so daß (3.47) auch im Hinblick auf den Einfluß der W_j günstiger ist als (3.46). Dieser Unterschied ergibt sich aus der von uns verwendeten Abschätzung des ersten sukzessiven Minimums des Gitters $\Lambda_{\tilde{\mathfrak{p}}^k}$ (vgl. Beweis zu Proposition 3.27)

$$\lambda_1(\Lambda_{\mathfrak{p}^k}) \geq \left(\frac{p^k}{\prod_{j=1}^{m} W_j}\right)^{\frac{2}{m}}, \tag{3.48}$$

welche schärfer ist als die in Friedrichs und Fieker [25] verwendete Abschätzung

$$\lambda_1(\Lambda_{\mathfrak{p}^k}) \geq \frac{m}{\sum_{j=1}^{m} W_j^2} \left(p^k\right)^{\frac{2}{m}}. \tag{3.49}$$

Wir wollen nun noch kurz die zweite Methode für beliebiges $d \in \mathbb{Z}_{>0}$ zur Rekonstruktion von nicht-ganzalgebraischen Zahlen vergleichen, bei der die Gitter $\Lambda_{\tilde{\mathfrak{p}}^k,-\gamma}$ und $\Lambda_{\gamma^*_{(k)},(k)}$ übereinstimmen. In [25], Lemma 7 wird zunächst eine untere Schranke an die Größe des ersten sukzessiven Minimums $\lambda_1(\Lambda_{\tilde{\mathfrak{p}}^k})$ hergeleitet, so daß es bis auf das Vorzeichen genau einen Vektor im Gitter $\Lambda_{\tilde{\mathfrak{p}}^k,-\gamma}$ gibt, dessen

T_2-Norm kleiner als eine vorgegebene Schranke ist. Unter Benutzung der Beweismethode von Proposition 3.29 erhalten wir eine für den Zweck hinreichende, aber schwächere Aussage:

3.50. Proposition. *Ist* $\lambda_1(\Lambda_{\tilde{\mathfrak{p}}^k}) > |d|^2(A_1A + A_1)^2$*, dann gibt es bis auf das Vorzeichen genau ein* Basiselement $b_1 \in \Lambda_{\gamma^*_{(k)},(k)}$ *mit* $\|b_1\| \leq A_1$*, und es gilt* $b_1 = \pm v$.

Da ein Element, welches das erste sukzessive Minimum realisiert, zu einer Basis fortgesetzt werden kann, folgt außerdem, daß $\pm v$ der kürzeste Vektor in $\Lambda_{\gamma^*_{(k)},(k)}$ ist. Für ein LLL-reduziertes erstes Basiselement $b_1 \in \Lambda_{\gamma^*_{(k)},(k)}$ gilt nun $\|b_1\| \leq 2^{m/2}|d|A$ wegen $\|v\| = \|(-\lambda_1, \ldots, -\lambda_m, d)\| \leq |d|A$. Wir wenden die Proposition mit $A_1 := 2^{m/2}|d|A$ an und erhalten $b_1 = \pm v$. Für [25], Lemma 7 muß hingegen $\lambda_1(\Lambda_{\tilde{\mathfrak{p}}^k}) > 16A_1^4$ erfüllt sein, welches zu einer um den Faktor 2^m höheren unteren Schranke an $\lambda_1(\Lambda_{\tilde{\mathfrak{p}}^k})$ führt. Bei großem m und kleinem A bedeutet dies, daß wir (zusätzlich zu (3.48)) mit der Hälfte der Präzision auskommen als [25].

Kapitel 4

Algebraische Funktionenkörper

In diesem Kapitel wird das Verfahren der Galoisgruppenberechnung eines algebraischen Funktionenkörpers F/K, $K \in \{\mathbb{F}_q, \mathbb{Q}\}$ über dem Konstantenkörper K beschrieben. Die generelle Vorgehensweise ist ähnlich wie im Zahlkörperfall, beruht aber darauf, daß das korrespondierende Problem der Galoisgruppenberechnung im Restklassenkörper des Funktionenkörpers gelöst (implementiert) ist.

4.1 Grundlagen

Wir werden den Funktionenkörperfall über $\mathbb{F}_q$, wobei $\mathbb{F}_q$ der endliche Körper mit q Elementen der Charakteristik p sei, und $\mathbb{Q}$ soweit als möglich simultan behandeln und setzen deshalb $R \in \{\mathbb{F}_q, \mathbb{Z}\}$ und $K := \mathrm{Quot}(R)$ als den Quotientenkörper von R. Sei F/K ein algebraischer Funktionenkörper einer Variablen, wobei F als separable algebraische Erweiterung des rationalen Funktionenkörpers $K(t)$ dargestellt sei. Somit existiert ein irreduzibles, in x normiertes und separables Polynom $h(t,x) \in K[t][x]$ mit $F = K(t)[x]/h(t,x)K(t)[x] = K(t,\delta)$, wobei $\delta = x + h(t,x)K(t)[x]$ ist. Für unsere Berechnungen wollen wir annehmen, daß $h(t,x)$ absolut irreduzibel ist und Koeffizienten in $R[t]$ hat. Der algebraische Abschluß von K in F hat endlichen Grad über K und wird als der exakte Konstantenkörper $\tilde{K}$ von F/K bezeichnet. Somit kann F auch immer als Funktionenkörper über $\tilde{K}$ betrachtet werden, und für absolut irreduzibles Minimalpolynom $h(t,x)$ gilt $\tilde{K} = K$. Da der Zwischenkörper $K(t)$ keine Invariante der Erweiterung F/K darstellt, sondern von der Wahl des transzendenten Elements $t \in F$ abhängt, fixieren wir mit F auch t für den Rest des Kapitels und setzen $m := [\,F\!:\!K(t)\,] = \deg_x(h)$.

Aufgrund der Bijektion (1.25) wollen wir das eindeutig bestimmte, maximale Ideal $\mathcal{P} \in \mathbb{P}(F)$ eines (diskreten) Bewertungsringes $\mathcal{O}_\mathcal{P}$ von F/K auch als Stelle von F/K bezeichnen. Der Restklassenkörper $\mathcal{O}_\mathcal{P}/\mathcal{P}$ von $\mathcal{P}$ ist eine endliche

Erweiterung von K, deren Erweiterungsgrad als Grad von $\mathcal{P}$ definiert ist. Mit $\nu_{\mathcal{P}} : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ bezeichnen wir die zu $\mathcal{P} \in \mathbb{P}(F)$ gehörende normierte, diskrete Bewertung bzw. mit $|\cdot|_{\mathcal{P}} : F \longrightarrow \mathbb{R}_{\geq 0}$ den Absolutbetrag, so daß $|a|_{\mathcal{P}} = c^{-\nu_{\mathcal{P}}(a)}$ für alle $a \in F^{\times}$ gilt. Im Fall $K = \mathbb{F}_q$ sei $c := \#\mathbb{F}_q$, ansonsten $c > 1$ beliebig aber fest gewählt.

Alle Bewertungen von F/K erhält man durch Fortsetzung der Bewertungen des rationalen Funktionenkörpers $K(t)/K$. Die Bewertungen von $K(t)$, die auf K trivial sind, sind nach Cohn [13], Chapter 1, Proposition 4.4 alle diskret (d.h. insbesondere nicht-archimedisch). Jede dieser Bewertungen korrespondiert entweder zu einem über K irreduziblen Polynom $p(t)$ (endliche Stelle) oder zu t^{-1} (unendliche Stelle), wobei wir im folgenden die zu t^{-1} gehörende Bewertung von $K(t)$ mit $\nu_{\infty}(g/h) : K(t) \longrightarrow \mathbb{Z} \cup \{\infty\} : \deg(h) - \deg(g)$, $g, h \in K[t]$, das Bewertungsideal mit $\boldsymbol{p}_{\infty}$ und die Menge der Stellen über $\boldsymbol{p}_{\infty}$ mit $\mathbb{P}_{\infty}(F)$ bezeichnen wollen. Der Durchschnitt der Bewertungsringe von $K(t)$ ist K, und zusammen mit der Produktformel $\sum_{p \in \mathbb{P}(K(t))} \deg(\boldsymbol{p})\ \nu_{\boldsymbol{p}}(a) = 0,\ a \in K(t)^{\times}$ folgt, daß die Bewertungen auf K und somit auf den algebraischen Erweiterungen von K Null sind. Es gilt insbesondere $\nu_{\mathcal{P}}(a) = 0$ für alle $a \in \tilde{K}^{\times}, \mathcal{P} \in \mathbb{P}(F)$. Gehen wir also von K zu einer endlichen Erweiterung K_0 in F über, so ändern sich Stellen, Bewertungsringe und Restklassenkörper nicht. Für den Grad $\deg_{K_0}(\mathcal{P})$ einer Stelle $\mathcal{P}$ bezüglich K_0 von F gilt dann $\deg(\mathcal{P}) = [\, K_0 : K \,] \deg_{K_0}(\mathcal{P})$. Im folgenden werden wir die Stellen $\mathbb{P}(F) \backslash \mathbb{P}_{\infty}(F)$ auch als endliche Stellen und die Stellen aus $\mathbb{P}_{\infty}(F)$ als unendliche Stellen von F/K bezeichnen.

Analog zu $\mathbb{Z}$ in $\mathbb{Q}$ übernimmt jetzt $K[t]$ die Rolle der ganzen Zahlen in $K(t)$, und wir können von dem ganzen Abschluß von $K[t]$ in F sprechen. Mit $\mathfrak{o}_F := Cl(K[t], F)$ sei die Maximalordnung von F bezüglich $K[t]$ bezeichnet. Wie im Zahlkörperfall ist $\mathfrak{o}_F$ ist ein Dedekindring und gleich dem Schnitt aller Bewertungsringe $\boldsymbol{O}_{\mathcal{P}}$, $\mathcal{P} \in \mathbb{P}(F) \backslash \mathbb{P}_{\infty}(F)$. Die Primideale von $\mathfrak{o}_F$ entsprechen eineindeutig und bewertungserhaltend den endlichen Stellen von F/K. Da $K[t]$ ein Hauptidealring ist, besitzt $\mathfrak{o}_F$ eine Ganzheitsbasis, d.h. es existieren $\omega_1, \ldots, \omega_m \in \mathfrak{o}_F$ mit $\mathfrak{o}_F = \oplus_{i=1}^{m} K[t]\omega_i$. Entsprechendes gilt für die Ideale von $\mathfrak{o}_F$, d.h. jedes Ideal $\neq 0$ von $\mathfrak{o}_F$ ist ein freier $K[t]$-Modul vom Rang m.

Ein algebraischer Funktionenkörper F'/K' heißt eine algebraische Erweiterung von F/K, wenn die Erweiterung $F' \supseteq F$ algebraisch ist und $K' \supseteq K$ gilt. Ist darüber hinaus F' das Kompositum von F und K', d.h. $F' = FK'$, so heißt die algebraische Erweiterung F'/K' Konstantenkörpererweiterung von F/K. Wie bei der Theorie algebraischer Zahlkörper 3.2 haben wir den folgenden Satz (vgl. Stichtenoth [80], I.2.1, III.3.7 und Beweis zu II.3.7 unter Beachtung von Neukirch [62],§11, 11.1):

4.1. Satz. *Sei $p(t) \in K[t]$ normiert und irreduzibel mit $p(t) \nmid \operatorname{disc}(h)$, $\boldsymbol{p} \in$*

$\mathbb{P}(K(t))$ die zu $p(t)$ gehörende Stelle und $\bar{h} = \bar{h}_1 \cdots \bar{h}_r$ eine Faktorisierung in paarweise verschiedene, normierte, irreduzible Polynome über $\overline{K(t)}_p := \boldsymbol{O}_p/\boldsymbol{p}$. Dann existiert für $i = 1, \ldots, r$ eine eindeutig bestimmte Stelle $\boldsymbol{\mathcal{P}}_i \in \mathbb{P}(F)$, die man durch Lokalisierung von $\boldsymbol{O}_p[\delta]$ nach dem Ideal $p(t)\boldsymbol{O}_p[\delta] + h_i(\delta)\boldsymbol{O}_p[\delta]$ für ein Urbild $h_i \in K[t][x]$ von $\bar{h}_i$ erhält. $\boldsymbol{\mathcal{P}}_1, \ldots, \boldsymbol{\mathcal{P}}_r$ sind alle Stellen von $\mathbb{P}(F)$, die über $\boldsymbol{p}$ liegen. $p(t)$ ist Primelement von $\boldsymbol{\mathcal{P}}_i$, $e(\boldsymbol{\mathcal{P}}_i|\boldsymbol{p}) = 1$, $f(\boldsymbol{\mathcal{P}}_i|\boldsymbol{p}) = \deg(\bar{h}_i)$, und der Restklassenkörper von $\boldsymbol{\mathcal{P}}_i$ ist isomorph zu $\overline{K(t)}_p[x]/\bar{h}_i(x)\overline{K(t)}_p[x]$.

4.2. Bemerkung. Für $K = \mathbb{Q}$ ist es in Satz 4.1 immer möglich $p(t) = t - t_0 \in \mathbb{Z}[t]$ zu wählen, d.h. $\boldsymbol{p}$ ist Stelle vom Grad eins.

4.3. Bemerkung. In der Situation von Satz 4.1 erhalten wir für die Primidealzerlegung von Idealen der Gleichungsordnung $K[t][\delta]$ und der Maximalordnung $\mathfrak{o}_F$ von F

$$\begin{aligned} p(t)\boldsymbol{O}_p[\delta] \cap K[t][\delta] = p(t)K[t][\delta] = \tilde{\tilde{\mathfrak{P}}}_1 \cdots \tilde{\tilde{\mathfrak{P}}}_r \text{ mit} \\ \tilde{\tilde{\mathfrak{P}}}_i := p(t)K[t][\delta] + h_i(\delta)K[t][\delta],\ (1 \le i \le r) \end{aligned} \tag{4.4}$$

$$\begin{aligned} p(t)\boldsymbol{O}_p[\delta] \cap \mathfrak{o}_F = p(t)\mathfrak{o}_F = \tilde{\mathfrak{P}}_1 \cdots \tilde{\mathfrak{P}}_r \text{ mit} \\ \tilde{\mathfrak{P}}_i := p(t)\mathfrak{o}_F + h_i(\delta)\mathfrak{o}_F,\ (1 \le i \le r) \end{aligned} \tag{4.5}$$

und die Restklassenkörper von $\boldsymbol{\mathcal{P}}_i, \tilde{\mathfrak{P}}_i$ und $\tilde{\tilde{\mathfrak{P}}}_i$ sind isomorph zueinander (siehe Stichtenoth [80], III.2.9; $K[t][\delta]/\tilde{\tilde{\mathfrak{P}}}_i \cong \mathfrak{o}_F/\tilde{\mathfrak{P}}_i$, da $p(t) \nmid \operatorname{disc}(h)$ und somit $p(t)$ kein Indexteiler von $[\,\mathfrak{o}_F : K[t][\delta]\,]$ ist).

Um die Vervollständigung von F an einer Stelle $\boldsymbol{\mathcal{P}} \in \mathbb{P}(F)$ betrachten zu können, treffen wir folgende allgemeine Definition

4.6. Definition und Satz. *Für eine endliche Körpererweiterung E/K und $k \in \mathbb{Z}_{>0}$ bezeichne*

$$E((t^{-\frac{1}{k}})) := \left\{ \sum_{i=l}^{\infty} a_i (t^{-\frac{1}{k}})^i \,|\, l \in \mathbb{Z}, a_i \in E \right\} \tag{4.7}$$

den Körper der Puiseuxreihen mit endlichem Hauptteil in der Variablen $t^{-\frac{1}{k}}$ über E, und für $a = \sum_{i=l}^{\infty} a_i t^{-\frac{i}{k}} \in E((t^{-\frac{1}{k}}))$ ist

$$\nu_{t^{-\frac{1}{k}}} : E((t^{-\frac{1}{k}})) \longrightarrow \mathbb{Z} \cup \{\infty\} : a \mapsto \begin{cases} \infty & a = 0 \\ \min\{i \in \mathbb{Z} \,|\, a_i \neq 0\} & \textit{sonst} \end{cases} \tag{4.8}$$

eine surjektive exponentielle Bewertung auf $E((t^{-\frac{1}{k}}))$, wobei wir $-\nu_{t^{-1/k}}(a)$ auch als Grad von a bezeichnen. Für $b := [\,E : K\,]$ sei $|\cdot|_{t^{-1/k}} = c^{-b\nu_{t^{-1/k}}(\cdot)}$ der zugehörige Absolutbetrag, und den Bewertungsring von $E((t^{-\frac{1}{k}}))$ bezüglich $\nu_{t^{-1/k}}(\cdot)$ notieren wir mit $E[[t^{-\frac{1}{k}}]]$.

Die Konjugierten $\delta^{(j)}$, $(1 \leq j \leq m)$ von δ erhalten wir im Funktionenkörperfall, indem wir das gleiche Prinzip wie im Zahlkörperfall verfolgen:

$$K(t) \xrightarrow[\substack{\text{Vervollständigung}\\ \text{bzgl. } p_\infty}]{} K((t^{-1})) \xrightarrow[\substack{\text{Algebraischer}\\ \text{Abschluß}}]{} \overline{K((t^{-1}))}$$

Die Fortsetzung von ν_∞ auf $K((t^{-1}))$ ist nach (4.8) bis auf K-Isomorphie gerade $\nu_{t^{-1}}$. $\nu_{t^{-1}}$ läßt sich eindeutig zu einer Bewertung auf $\overline{K((t^{-1}))}$ fortsetzen (vgl. Lorenz[52], §23, Satz 4′), welche wir ebenfalls mit $\nu_{t^{-1}}$ bezeichnen. Seien $\sigma_1, \ldots, \sigma_m$ die sämtlichen verschiedenen $K(t)$-Homomorphismen von F in $\overline{K((t^{-1}))}$, dann definiert jedes σ_i eine Bewertung auf F vermöge $\nu_{t^{-1}}(\sigma_i(a))$ für alle $a \in F$. Das Polynom $h(t,x) \in K[t][x]$ besitzt über $K((t^{-1}))$ eine Primfaktorzerlegung der Gestalt

$$h = h_1 \cdots h_s, \ (s \leq m)$$

in der keine mehrfachen Faktoren auftreten. Zu jedem h_i wählen wir eine Nullstelle δ_i von h_i in $\overline{K((t^{-1}))}$ und ordnen die σ_i so an, daß $\sigma_i(\delta) = \delta_i$, $(1 \leq i \leq s)$ gilt. Bewertungen konjugierter Elemente sind gleich, da sie dasselbe Minimalpolynom h_i haben und die eindeutige Fortsetzung von $\nu_{t^{-1}}$ auf $\overline{K((t^{-1}))}$ durch die Norm gegeben ist. Deshalb ist die Anzahl der verschiedenen Bewertungsfortsetzungen von ν_∞ auf F höchstens s. Umgekehrt sind die $\nu_{t^{-1}} \circ \sigma_1, \ldots, \nu_{t^{-1}} \circ \sigma_s$ paarweise nicht äquivalent, da sonst δ_i und δ_j für $i \neq j, 1 \leq i, j \leq s$ über $K((t^{-1}))$ zueinander konjugiert sein müßten. Es liegen also genau s Stellen über $\boldsymbol{p}_\infty$, d.h. $\mathbb{P}_\infty(F) = \{\mathcal{P}_1, \ldots, \mathcal{P}_s\}$, und wir erhalten (vgl. Lorenz [52], §23, Satz 5, §24, Satz 2)

4.9. Definition und Satz. *Bezeichne $\mathcal{F}_i \cong K((t^{-1}))(\delta_i)$ die Vervollständigung von F bzgl. $\mathcal{P}_i$ für $1 \leq i \leq s$. Dann gilt*

$$K((t^{-1})) \otimes_{K(t)} F \cong \prod_{i=1}^{s} \mathcal{F}_i \ \text{ und } \ [\,\mathcal{F}_i : K((t^{-1}))\,] = m_i = e_i \deg(\mathcal{P}_i) \tag{4.10}$$

mit $e_i := e(\mathcal{P}_i|\boldsymbol{p}_\infty)$ und $\sum_{i=1}^{s} m_i = m$. Wir definieren $\nu_i := \nu_{\mathcal{P}_i}$ bzw. $|\cdot|_i := c^{-\nu_i(\cdot)}$.

Die Konjugierten $\delta^{(1)}, \ldots, \delta^{(m)}$ von δ lassen sich demnach so anordnen, daß

$$(\delta^{(1)}, \ldots, \delta^{(m)}) = (\delta^{(1,1)}, \ldots, \delta^{(1,m_1)}, \delta^{(2,1)}, \ldots, \delta^{(2,m_2)}, \ldots, \delta^{(s,1)}, \ldots, \delta^{(s,m_s)}) \tag{4.11}$$

mit $h_i(\delta^{(i,j)}) = 0$, $(1 \leq j \leq m_i)$ gilt. Ist $\boldsymbol{p}_\infty$ zahm verzweigt, d.h. $\operatorname{char}(K) \nmid e := \operatorname{kgV}(e_1, \ldots, e_s)$ lassen sich die Nullstellen von $h(t,x)$ als Puiseuxreihen entwickeln und es gilt der folgende Satz:

4.12. Satz. *Es gelte $\operatorname{char}(K) \nmid e := \operatorname{kgV}(e_1, \ldots, e_s)$, und seien die $\delta^{(i,j)}$, $(1 \leq i \leq s,\ 1 \leq j \leq m_i)$ wie in (4.11) angeordnet. Dann existiert ein endlicher Erweiter-*

ungskörper E von K vom Grad b, der die Restklassenkörper $\mathcal{O}_{\mathcal{P}_i}/\mathcal{P}_i$ und alle e_i-ten Einheitswurzeln enthält, so daß

$$\delta^{(i,j)} \in E((t^{-\frac{1}{e_i}})) \subset E((t^{-\frac{1}{e}})) \tag{4.13}$$

die Entwicklungen an $\mathcal{P}_i$ für $1 \leq i \leq s$ sind.

Beweis. Für $K = \mathbb{F}_q$ siehe Schörnig [75], Theorem III.5. Im Fall $K = \mathbb{Q}$ läßt sich der Beweis vollkommen analog durchführen. □

4.14. Bemerkung. Die Reihenentwicklungen der $\delta^{(i,j)}$ lassen sich im zahm verzweigten Fall mit dem Newton-Puiseux Verfahren berechnen. Diese Methode ist für algebraisch abgeschlossene Körper in Walker [86] beschrieben und läßt sich im Fall $K = \mathbb{F}_q$ anwenden. Für $K = \mathbb{Q}$ existiert ein wesentlich effizienterer Algorithmus, welcher in Duval [21] dargestellt ist. Im wild verzweigten Fall ist im allgemeinen keine Entwicklung in Puiseuxreihen möglich (vgl. Chevalley [11]).

Für den Inklusionstest werden wir wie im Zahlkörperfall geometrische Methoden benötigen. Die Geometrie der Zahlen algebraischer Funktionenkörper unterscheidet sich insofern zu der von Zahlkörpern, als daß diese Körper kein Skalarprodukt, sondern nur eine ultrametrische Norm erlauben:

4.15. Definition und Satz. *Die Funktion*

$$\|\cdot\|_{T_2} : F \longrightarrow \mathbb{R}_{\geq 0} : a \mapsto \max_{1\leq i\leq s}\{|a|_i^{\frac{1}{e_i}}\} = c^{-\min\limits_{1\leq i\leq s}\{\frac{1}{e_i}\nu_i(a)\}}$$

ist eine Norm auf F, d.h. sie erfüllt die Eigenschaften

$$\begin{aligned} &(i) \quad \|a\|_{T_2} = 0 \Leftrightarrow a = 0, \\ &(ii) \quad \|\lambda a\|_{T_2} = |\lambda|_\infty \|a\|_{T_2} \\ &(iii) \quad \|a+b\|_{T_2} \leq \max\{\|a\|_{T_2}, \|b\|_{T_2}\} \text{ für } a, b \in F,\ \lambda \in K(t), \end{aligned} \tag{4.16}$$

wobei $|\lambda|_\infty := c^{-\nu_\infty(\lambda)}$ für alle $\lambda \in K(t)^\times$ gilt.

Beweis. Siehe Schörnig [75], Definition und Satz II.15. □

Wie die Bezeichnung schon andeutet korrespondiert die Norm $\|\cdot\|_{T_2}$ zur T_2-Norm bei Zahlkörpern und spielt bei konstruktiven Untersuchungen von F eine zentrale Rolle.

4.17. Definition. Eine Basis $\omega_1, \ldots, \omega_m$ eines freien $K[t]$-Moduls $\mathfrak{o}$ vom Rang m heißt reduziert, wenn für jedes Element $\sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}$, $(\lambda_1, \ldots, \lambda_m \in K[t])$ gilt

$$\|\sum_{i=1}^m \lambda_i\omega_i\|_{T_2} = \max_{1\leq i\leq m}\{\,\|\lambda_i\omega_i\|_{T_2}\,\}.$$

Im zahm verzweigten Fall können wir nach Satz 4.12 den algebraischen Funktionenkörper F mittels der Abbildung

$$\mu : F \longrightarrow E((t^{-\frac{1}{e}}))^m : \sum_{j=0}^{m-1} a_j \delta^j \mapsto \left(\sum_{j=0}^{m-1} a_j (\delta^{(i)})^j \right)_{1 \le i \le m} \tag{4.18}$$

in den m-dimensionalen Raum $E((t^{-\frac{1}{e}}))^m$ einbetten. Dort läßt sich ebenfalls eine Norm definieren, deren Zusammenhang zur $\|\cdot\|_{T_2}$-Norm in Proposition 4.29 gezeigt wird.

4.19. Definition und Satz. *Sei* $b := [\, E : K \,]$ *und* $\nu : E((t^{-\frac{1}{k}}))^m \longrightarrow \mathbb{Z} \cup \{\infty\} : u = (u_1, \ldots, u_m)^{tr} \mapsto \min_{1 \le i \le m} \{\nu_{t^{-\frac{1}{k}}}(u_i)\}$. *Durch*

$$\| \cdot \|_{t^{-\frac{1}{k}}} \;\; : \;\; E((t^{-\frac{1}{k}}))^m \longrightarrow \mathbb{R}_{\ge 0} : u = (u_1, \ldots, u_m)^{tr} \mapsto c^{-b\,\nu(u)}$$

wird auf $E((t^{-\frac{1}{k}}))^m$ *eine Norm definiert, welche für alle* $u, v \in E((t^{-\frac{1}{k}}))^m$ *und* $\lambda \in E((t^{-\frac{1}{k}}))$ *bezüglich des Betrags aus Definition 4.6 den Eigenschaften* (i), (ii) *und* (iii) *aus* (4.16) *genügt.*

4.20. Bemerkung. Wie für nicht-archimedische Absolutbeträge eines Körpers, gilt auch hier der „Zusatz zur starken Dreiecksungleichung“: Aus $\|u\|_{t^{-\frac{1}{k}}} \neq \|v\|_{t^{-\frac{1}{k}}}$ folgt $\|u+v\|_{t^{-\frac{1}{k}}} = \max\{\|u\|_{t^{-\frac{1}{k}}}, \|v\|_{t^{-\frac{1}{k}}}\}$ für $u, v \in E((t^{-\frac{1}{k}}))^m$.

Die Funktion $-\nu(\cdot)$ entspricht dem Spaltengrad eines Vektors u aus $E((t^{-\frac{1}{k}}))^m$, also dem Maximum der Grade der Einträge von u. Nun können wir wie im Zahlkörperfall freie $E[t^{\frac{1}{k}}]$-Module im m-dimensionalen Raum $E((t^{-\frac{1}{k}}))^m$ betrachten.

4.21. Definition. Seien die Spaltenvektoren $u_1, \ldots, u_r \in E((t^{-\frac{1}{k}}))^m$ linear unabhängig über dem Körper $E((t^{-\frac{1}{k}}))$ und S ein Teilring von $E[t^{\frac{1}{k}}]$. Dann nennt man den S-Modul

$$\Lambda := \left\{ \sum_{i=1}^{r} \lambda_i u_i \,|\, \lambda_1, \ldots \lambda_m \in S \right\}$$

ein S-Gitter der Dimension r.

Eine wichtige Eigenschaft eines Gitters ist seine Diskretheit, d.h. daß jeder Punkt des Gitters Λ eine Umgebung besitzt, in der kein weiterer Gitterpunkt liegt. Zu $\sum_{i=1}^{m} \lambda_i u_i \in \Lambda$ ist $\{a_1 u_1 + \cdots + a_m u_m \,|\, a_i \in E((t^{-\frac{1}{k}})), \nu_{t^{-1/k}}(\lambda_i - a_i) > 0 \text{ für } 1 \le i \le m\}$ eine solche Umgebung. Für E/K mit $K = \mathbb{F}_q$ enthält darüber hinaus jede beschränkte Menge im $E((t^{-\frac{1}{k}}))^m$ höchstens endlich viele Gitterpunkte; es gibt also immer nur endlich viele Vektoren $v = \sum_{i=1}^{m} \lambda_i u_i$ in Λ mit beschränkten $-\nu(v)$-

bzw. Spaltengrad-Werten. Da $K = \mathbb{Q}$ nicht endlich ist, gilt letztere Bemerkung in diesem Fall nicht mehr.

Die LLL-Reduktion, wie wir sie im Fall von Gittern über $\mathbb{Z}$ kennen, kann hier nicht verwendet werden, da Gitter über $E[t^{\frac{1}{k}}]$ kein Skalarprodukt erlauben. Als Ersatz nehmen wir einen Reduktionsalgorithmus, der in Schörnig [75], Kapitel III für $\mathbb{F}_{q^d}[t]$-Gitter im $\mathbb{F}_{q^d}((t^{-\frac{1}{e}}))^m$, $d \in \mathbb{Z}_{>0}$ mit $\mathrm{char}(\mathbb{F}_q) \nmid e$ bzw. in Heß [35] für allgemeine Grundkörper angegeben wurde.

Auch für Basen bezüglich der $\|\cdot\|_{T_2}$-Norm kann reduziert werden. Für Techniken zum wild verzweigten Fall verweisen wir auf Heß [35] und für eine detaillierte algorithmische Beschreibung im zahm verzweigten Fall auf Paulus [66], Pohst, Schörnig [69] und Schörnig [75].

4.22. Definition. Die Basis $u_1, \ldots, u_r$ des S-Gitters Λ der Dimension r wird reduziert genannt, wenn für jedes Element $\sum_{i=1}^{r} \lambda_i u_i \in \Lambda$, $(\lambda_1, \ldots, \lambda_r \in S)$ die folgende Gleichung gilt

$$\|\sum_{i=1}^{r} \lambda_i u_i\|_{t^{-\frac{1}{k}}} = \max_{1 \le i \le r} \{\, |\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}} \,\}.$$

4.23. Bemerkung. Zu jeder Basis $u_1, \ldots, u_r$ eines S-Gitters Λ existiert eine reduzierte Basis, welche durch endlich viele elementare unimodulare S-Transformationen berechnet werden kann, aber nicht eindeutig ist (vgl. auch Heß [35]).

Die folgende Aussage zeigt, daß der Reduktionsalgorithmus im Funktionenkörperfall dem LLL-Algorithmus im Zahlkörperfall überlegen ist.

4.24. Definition und Satz. *Für einen Teilring S von $E[t^{\frac{1}{k}}]$ mit $E[t] \subseteq S$ sei $\Lambda \subseteq E((t^{-\frac{1}{k}}))^m$ ein S-Gitter der Dimension m und $M_i := \min\{\gamma \in \mathbb{R}_{>0} \mid \exists\, S\text{-linear unabhängige } v_1, \ldots, v_i \in \Lambda \text{ mit } \|v_j\|_{t^{-\frac{1}{k}}} \le \gamma,\ 1 \le j \le i\}$ das i-te sukzessive Minimum von Λ bzgl. $\|\cdot\|_{t^{-\frac{1}{k}}}$. Dann sind für eine Basis $u_1, \ldots, u_m$ von Λ äquivalent:*

(i) $u_1, \ldots, u_m$ ist reduziert.

(ii) $u_1, \ldots, u_m$ realisieren die sukzessiven Minima.

Beweis. Sei $u_1, \ldots, u_m$ eine reduzierte Basis von Λ, welche der Größe nach sortiert sei, d.h. $\|u_1\|_{t^{-\frac{1}{k}}} \le \cdots \le \|u_m\|_{t^{-\frac{1}{k}}}$. Ist $U_j := Su_1 + \cdots + Su_j$ das Teilgitter von Λ, welches von den ersten j Vektoren erzeugt wird, so gilt $U_{j+1} = U_j + Su_{j+1}$ für $j \in \mathbb{Z}_{>0}$. Wir beweisen nun durch Induktion über die Dimension von Λ, daß $u_1, \ldots, u_m$ die sukzessiven Minima realisieren. Das Gitter U_1 hat das erste sukzessive Minimum $\|u_1\|_{t^{-\frac{1}{k}}}$, da für alle $0 \neq \lambda u_1 \in U_1$ gilt $\|\lambda u_1\|_{t^{-\frac{1}{k}}} \ge \|u_1\|_{t^{-\frac{1}{k}}}$.

Wir nehmen nun an, daß in U_j die sukzessiven Minima durch $u_1, \ldots, u_j$ realisiert werden und behaupten, daß U_{j+1} die sukzessiven Minima $M_1, \ldots, M_j$ von U_j hat und $M_{j+1} = \|u_{j+1}\|_{t^{-\frac{1}{k}}}$ gilt. Sei $v = \sum_{i=1}^{j+1} \lambda_i u_i \in U_{j+1}$ beliebig mit $\lambda_{j+1} \neq 0$. Aufgrund der Reduziertheit der Basis $u_1, \ldots, u_{j+1}$ erhalten wir, daß $\|v\|_{t^{-\frac{1}{k}}} = \max_{1 \leq i \leq j+1}\{|\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}}\} \geq \|u_{j+1}\|_{t^{-\frac{1}{k}}}$ gilt. Somit hat jeder Vektor aus U_{j+1}, der nicht in U_j liegt, eine Norm, die größer gleich $\|u_{j+1}\|_{t^{-\frac{1}{k}}}$ ist. Da die Basis der Größe nach sortiert ist, folgt außerdem $\|u_{j+1}\|_{t^{-\frac{1}{k}}} \geq M_j$. Somit stimmen die ersten j sukzessiven Minima aus U_{j+1} mit den sukzessiven Minima von U_j überein und können durch Vektoren aus U_j realisiert werden. Es folgt, daß $M_i = \|u_i\|_{t^{-\frac{1}{k}}}$ für $1 \leq i \leq j$ ist. Da die Vektoren, die die ersten $j+1$ sukzessiven Minima realisieren, nach Definition linear unabhängig sein müssen, erhalten wir darüber hinaus $M_{j+1} = \|u_{j+1}\|_{t^{-\frac{1}{k}}}$.

Realisiere nun umgekehrt u_i, $(1 \leq i \leq m)$ das i-te sukzessive Minimum, und sei $0 \neq v = \sum_{i=1}^{m} \lambda_i u_i \in \Lambda$ beliebig. Wir nehmen an, daß

$$\|v\|_{t^{-\frac{1}{k}}} < \max_{1 \leq i \leq m} \{\, |\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}} \} \tag{4.25}$$

gilt. Wir wählen $j \in M := \{1, \ldots, m\}$ maximal mit $|\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}} = \max_{1 \leq i \leq m} \{\, |\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}} \}$ und setzen $I := \{\, i \mid |\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}} = |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}} \}$. Dann gilt

$$\|\sum_{i \in I} \lambda_i u_i\|_{t^{-\frac{1}{k}}} < |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}. \tag{4.26}$$

Wäre nämlich $\|\sum_{i \in I} \lambda_i u_i\|_{t^{-\frac{1}{k}}} = |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}$, so würde aus $\|\sum_{i \in M \setminus I} \lambda_i u_i\|_{t^{-\frac{1}{k}}} < |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}$ aufgrund des „Zusatzes zur starken Dreiecksungleichung“ (Bemerkung 4.20) folgen, daß $\|\sum_{i \in I} \lambda_i u_i + \sum_{i \in M \setminus I} \lambda_i u_i\|_{t^{-\frac{1}{k}}} = |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}$ ist. Dies steht aber im Widerspruch zu (4.25).

Sei nun $\lambda_i = \sum_{\nu=0}^{\deg(\lambda_i)} \lambda_{i,\nu} t^\nu$ für $i \in M$. Da für die $\|\cdot\|_{t^{-\frac{1}{k}}}$ Norm nur die maximalen Grade von t ausschlaggebend sind, ist $\|\sum_{i \in I} \lambda_{i,\deg(\lambda_i)} t^{\deg(\lambda_i)} u_i\|_{t^{-\frac{1}{k}}} = \|\sum_{i \in I} \lambda_i u_i\|_{t^{-\frac{1}{k}}}$ und $|\lambda_{j,\deg(\lambda_j)} t^{\deg(\lambda_j)}|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}} = |\lambda_j|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}$, und es folgt aus (4.26)

$$\|\sum_{i \in I} \lambda_{i,\deg(\lambda_i)} t^{\deg(\lambda_i)} u_i\|_{t^{-\frac{1}{k}}} < |t^{\deg(\lambda_j)}|_{t^{-\frac{1}{k}}} \|u_j\|_{t^{-\frac{1}{k}}}. \tag{4.27}$$

Da $\|u_i\|_{t^{-\frac{1}{k}}} \leq \|u_j\|_{t^{-\frac{1}{k}}}$ für $i \leq j$ gilt, aber $\|t^{\deg(\lambda_i)} u_i\|_{t^{-\frac{1}{k}}} = \|t^{\deg(\lambda_j)}\, u_j\|_{t^{-\frac{1}{k}}}$ für alle $i \in I$ ist, muß $\deg(\lambda_i) \geq \deg(\lambda_j)$ gelten. Damit folgt dann aber aus (4.27) mittels Division durch $|t^{\deg(\lambda_j)}|_{t^{-\frac{1}{k}}}$, daß

$$\|\sum_{i \in I} \lambda_{i,\deg(\lambda_i)} t^{\deg(\lambda_i) - \deg(\lambda_j)} u_i\|_{t^{-\frac{1}{k}}} < \|u_j\|_{t^{-\frac{1}{k}}} \tag{4.28}$$

ist. Der Vektor $\sum_{i\in I} \lambda_{i,\deg(\lambda_i)} t^{\deg(\lambda_i)-\deg(\lambda_j)} u_i$ hat Koeffizienten in dem Ring $E[t]$, da $\deg(\lambda_i) \geq \deg(\lambda_j)$ gilt, und ist außerdem linear unabhängig von $u_1, \ldots, u_{j-1}$, weil $\lambda_{j,\deg(\lambda_j)} \neq 0$ ist. Somit steht Ungleichung (4.28) im Widerspruch zur Voraussetzung, daß u_j das j-te sukzessive Minima realisiert. Für den Vektor v muß deshalb $\|v\|_{t^{-\frac{1}{k}}} = \max_{1\leq i\leq m} \{ |\lambda_i|_{t^{-\frac{1}{k}}} \|u_i\|_{t^{-\frac{1}{k}}} \}$ gelten, d.h. die Basis $u_1, \ldots, u_m$ von Λ ist reduziert. □

Schließlich zeigen wir, daß die beiden Reduktionsbegriffe aus Definition 4.17 und Definition 4.22 im zahm verzweigten Fall übereinstimmen.

4.29. Proposition. *Für* $\mathrm{char}(K) \nmid e$ *ist* $\mu(\mathfrak{o}_F) = \oplus_{i=1}^m K[t]\mu(\omega_i)$ *ein* m*-dimensionales* $K[t]$*-Gitter im* $E((t^{-\frac{1}{e}}))^m$*, und es gilt* $\|a\|_{T_2} = \|\mu(a)\|_{t^{-\frac{1}{e}}}^{\frac{1}{[E:K]e}}$ *für alle* $a \in F$*.*

Beweis. Wir zeigen zunächst die Gittereigenschaft: Die $\omega_1, \ldots, \omega_m \in F$ bilden eine Basis von F/K, deshalb ist $\mathrm{disc}(\omega_1, \ldots, \omega_m) \neq 0$. Da $\mathrm{disc}(\omega_1, \ldots, \omega_m) = \det(\omega_i^{(j)})_{1\leq i,j\leq m}^2$ sind die $\mu(\omega_i)$ also insbesondere $E((t^{-\frac{1}{e}}))$-linear unabhängig.
Sei nun $b := [\, E : K \,]$. Bezeichnen wir die verschiedenen Einbettungen von F nach $E((t^{-\frac{1}{e}}))$ mit $\sigma_i^{(j)} : \sum_{l=0}^{m-1} a_l \delta^l \mapsto \sum_{l=0}^{m-1} a_l (\delta^{(i,j)})^l \in E((t^{-\frac{1}{e_i}})) \subset E((t^{-\frac{1}{e}}))$, $(1 \leq i \leq s,\ 1 \leq j \leq m_i)$ mit $(\delta^{(i,j)})$ wie in (4.11), so erhalten wir nach Definition 4.6 und Satz 4.12 für $a \in F$, $r \in E$

$$\sigma_i^{(j)}(a) = r \cdot (t^{-\frac{1}{e_i}})^{\nu_i(a)} + \text{höhere Terme} = r \cdot (t^{-\frac{1}{e}})^{\frac{e}{e_i}\nu_i(a)} + \text{höhere Terme}.$$

Daraus folgt $\nu_{t^{-\frac{1}{e}}}(\sigma_i^{(j)}(a)) = \frac{e}{e_i}\nu_i(a)$ und $\|\mu(a)\|_{t^{-\frac{1}{e}}} = c^{-b \min_{1\leq i\leq m}\{\frac{e}{e_i}\nu_i(a)\}}$. Mit Definition 4.15 erhalten wir somit $\|a\|_{T_2} = \|\mu(a)\|_{t^{-\frac{1}{e}}}^{\frac{1}{be}}$ und die Behauptung folgt. □

4.2 Nullstellenberechnung

Um unsere bisherigen Ergebnisse für algebraische Zahlkörper verwenden zu können, beschränken wir uns auf irreduzible, in x normierte und separable Polynome f mit Koeffizienten in $R[t, \delta] \subseteq \mathfrak{o}_F$. Ein beliebiges Polynom aus $F[x]$ läßt sich wie im Zahlkörperfall durch geeignete Substitution in ein Polynom mit Koeffizienten in $R[t, \delta]$ transformieren. Wir merken jedoch an, daß insbesondere im Fall $K = \mathbb{Q}$ diese Transformation ein nicht zu vernachlässigendes Koeffizientenwachstum mit sich bringen kann.

Die Vorgehensweise ist ähnlich wie im Zahlkörperfall: Wir möchten in einem Zerfällungskörper von f über F Berechnungen ausführen und anschließend prüfen, ob Elemente des Zerfällungskörpers in F liegen. Spezieller gesagt: Sei $\mathfrak{o}$ eine $K[t]$-Ordnung von F, d.h. ein unitärer Teilring von $\mathfrak{o}_F$, der $K[t]$-Maximalordnung von

F, welcher ebenfalls ein freier $K[t]$-Modul vom Rang m ist, und $f \in R[t,\delta][x] \subseteq \mathfrak{o}[x]$ irreduzibel, in x normiert und separabel. Wir wollen im ganzalgebraischen Abschluß von $\mathfrak{o}$ in einem Zerfällungskörper von f rechnen und später testen, ob Elemente dieses Abschlusses in $\mathfrak{o}_F$ liegen. Für unsere Berechnungen nutzen wir $\mathcal{P}$-adische Approximationen in einer geeigneten unverzweigten $\mathcal{P}$-adischen Erweiterung der Vervollständigung von F an einer endlichen Stelle $\mathcal{P} \in \mathbb{P}(F)\backslash\mathbb{P}_\infty(F)$. Die Vervollständigung von F bezüglich der Stelle $\mathcal{P}$ ist der Körper der formalen Laurentreihen mit endlichem Hauptteil in der Variablen π für ein Primelement π von $\mathcal{P}$. Bezeichnen wir die Vervollständigung mit $\mathcal{F}$, und sei V mit $0 \in V$ ein vollständiges Vertretersystem des Restklassenkörpers von F, so besitzt jedes $a \neq 0$ von $\mathcal{F}$ eine eindeutige Darstellung $a = \sum_{i=k}^{\infty} a_i\pi^i, a_i \in V$ mit $\nu_{\mathcal{P}}(a) = \min\{i \in \mathbb{Z} \mid a_i \neq 0\} = \nu_\pi(a)$ (vgl. Lorenz, [52], §24, F2 und nachfolgendes Beispiel).

Bevor wir mit der theoretischen Idee und der algorithmischen Beschreibung beginnen, wollen wir in allgemeinem Rahmen den für die Nullstellenberechnung zentralen Satz beweisen. Dazu vereinbaren wir folgende

4.30. Bezeichnung. *Für einen Integritätsring S und ein Element $d \in S\backslash\{0\}$ sei $S_{(d)}$ der Ring $\{\frac{s}{d^k} \mid s \in S, k \in \mathbb{Z}\} \subseteq Q$ für $Q := \mathrm{Quot}(S)$.*

4.31. Satz. *Sei S ein Integritätsring, $Q := \mathrm{Quot}(S)$ und $r \in S[[\pi]][x]$ ein in x normiertes Polynom mit Koeffizienten aus dem Potenzreihenring $S[[\pi]]$, so daß $\bar{r}(x) := r(0,x) \in S[x]$ separabel ist. Für einen Teiler $\bar{r}_1$ von $\bar{r}$ betrachten wir die separable Q-Algebra $Q[\bar{\beta}]$, wobei $\bar{r}_1$ Minimalpolynom von $\bar{\beta}$ über Q ist, und darin $S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}] \subseteq Q[\bar{\beta}]$. Dann folgt:*

(i) Es existiert eine Nullstelle β' von r in dem Potenzreihenring $S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}][[\pi]]$.

(ii) Sei T ein Integritätsring, $\psi : S \to T$ ein Ringmonomorphismus und $\phi : S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}] \to T$ ein ψ-Ringhomomorphismus mit $\phi(sa) = \psi(s)\phi(a)$ für alle $s \in S$, $a \in S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}]$. Setzen wir den Homomorphismus ψ koeffizientenweise zu einem Homomorphismus $S_{(\mathrm{disc}(\bar{r}_1))}[[\pi]][x] \to T[[\pi]][x]$ und ϕ koeffizientenweise zu einem Homomorphismus von $S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}][[\pi]] \to T[[\pi]]$ für Variablen π und x fort, so gilt: Ist $\beta' \in S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}][[\pi]]$ eine Nullstelle von r, so ist $\phi(\beta')$ eine Nullstelle von $\psi(r)$.

(iii) Sei $V := \mathrm{Quot}(\psi(S))$. Für jede Nullstelle ${\bar{\beta}_i}^* \in N(\psi(\bar{r}_1), V)$ von $\psi(\bar{r}_1)$ ist

$$\phi_i : S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}] \to \psi(S_{(\mathrm{disc}(\bar{r}_1))})[{\bar{\beta}_i}^*] : \sum_{j=0}^{\deg(\bar{r}_1)-1} g_j\bar{\beta}^j \mapsto \sum_{j=0}^{\deg(\bar{r}_1)-1} \psi(g_j){\bar{\beta}_i^*}^j,$$

mit $g_j \in S_{(\mathrm{disc}(\bar{r}_1))}$ ein ψ-Ringhomomorphismus. Für die Fortsetzung von ϕ_i wie in (ii) sind $\phi_i(\beta') \in \psi(S_{(\mathrm{disc}(\bar{r}_1))})[\bar{\beta}_i^*][[\pi]]$ $\deg(\bar{r}_1)$ verschiedene Nullstellen von $\psi(r)$ in $N(\psi(\bar{r}_1), V)[[\pi]]$ für $1 \leq i \leq \deg(\bar{r}_1)$.

(iv) Alle Nullstellen von $\psi(\bar{r})$ in $N(\psi(\bar{r}),V)$ sind in $Cl(\psi(S),\ N(\psi(\bar{r}),V))$ enthalten, und alle Nullstellen von $\psi(r)$ in $N(\psi(\bar{r}),V)[[\pi]]$ liegen bereits in $Cl(\psi(S),N(\psi(\bar{r}),V))_{(\mathrm{disc}(\psi(\bar{r})))}[[\pi]]$.

Beweis. (i) Wir zeigen, daß die Voraussetzungen für das Newton-Lifting (vgl. Sektion 1.4) in dem Ring $\tilde{S} := S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}][[\pi]]$ mit dem Ideal $\pi\tilde{S}$ für das Polynom r erfüllt sind. Nach Definition von $\bar{\beta}$ gilt $r(\pi,\bar{\beta}) \equiv \bar{r}_1(\bar{\beta}) \equiv 0 \bmod \pi\tilde{S}$. Außerdem ist $r'(\pi,\bar{\beta}) \bmod \pi\tilde{S}$ invertierbar: $\bar{r}_1(x) \in S[x]$ ist separabel, d.h. $\mathrm{ggT}(\bar{r}_1(x),\bar{r}_1'(x)) = 1$ über $Q[x]$, und wir können mit dem erweiterten Euklidischen Algorithmus für Polynome über Q Kofaktoren $k_1(x),k_2(x) \in Q[x]$ mit $\bar{r}_1(x)k_1(x) + \bar{r}_1'(x)k_2(x) = 1$ finden. Dann ist $\bar{r}_1'(\bar{\beta})k_2(\bar{\beta}) = 1$ in $Q[\bar{\beta}]$. Zu zeigen ist nun noch, daß $k_2(\bar{\beta})$ in $S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}] \subseteq Q[\bar{\beta}]$ liegt: Da $\bar{\beta}$ ganz über S ist, ist die separable Algebra $S[\bar{\beta}]$ ein endlich erzeugter freier S-Modul. Sei nun $a := \bar{r}_1'(\bar{\beta}) \in S[\bar{\beta}]$ und $char_a(x) \in S[x]$ das charakteristische Polynom von a. Dann existiert $g \in S[x]$ mit $char_a(x) = g(x)x + (-1)^{\deg(\bar{r}_1)}\mathrm{N}_{Q(\bar{\beta})/Q}(a)$. Es folgt $0 = g(a)a + (-1)^{\deg(\bar{r}_1)}\mathrm{N}_{Q(\bar{\beta})/Q}(a)$, wobei $\pm\mathrm{N}_{Q(\bar{\beta})/Q}(a) = \mathrm{disc}(\bar{r}_1) \neq 0$ ist. Somit existiert $\mathrm{N}_{Q(\bar{\beta})/Q}(a)^{-1} \in Q$, und es ist $\left(\frac{\pm g(a)}{\mathrm{N}_{Q(\bar{\beta})/Q}(a)}\right)a = 1$. Damit folgt $a^{-1} \in S_{(\mathrm{N}_{Q(\bar{\beta})/Q}(a))}[\bar{\beta}]$, was gleichbedeutend ist mit $\bar{r}_1'(\bar{\beta})^{-1} \in S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}]$. Somit sind die Voraussetzungen des Newton-Liftings erfüllt, und wir erhalten $\beta_k' = \bar{\beta} + \sum_{j=1}^{k} b_j\pi^j$ mit $b_j \in S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}]$ und $\beta' \equiv \beta_k' \bmod \pi^{k+1}\tilde{S}$. Durch Grenzübergang $k \to \infty$ folgt die Behauptung.

(ii) Es gilt $\psi(r)(\phi(\beta')) = \phi(r(\beta')) = 0$.

(iii) Es ist zu zeigen, daß ϕ_i für $1 \leq i \leq \deg(\bar{r}_1)$ ein ψ-Ringhomomorphismus ist. Sei dazu $\mu_i : S_{(\mathrm{disc}(\bar{r}_1))}[x] \to T[\bar{\beta}_i^*] : g(x) \mapsto \psi(g(x))(\bar{\beta}_i^*)$ der Einsetzhomomorphismus. Dann ist $\bar{r}_1(x)S_{(\mathrm{disc}(\bar{r}_1))}[x] \subseteq \mathrm{Kern}\,\mu_i$ und somit existiert ein eindeutig bestimmter Homomorphismus $\varphi_i : S_{(\mathrm{disc}(\bar{r}_1))}[x]/\bar{r}_1(x)S_{(\mathrm{disc}(\bar{r}_1))}[x] \to T[\bar{\beta}_i^*]$. Nach Voraussetzung ist aber $S_{(\mathrm{disc}(\bar{r}_1))}[x]/\bar{r}_1(x)S_{(\mathrm{disc}(\bar{r}_1))}[x] \cong S_{(\mathrm{disc}(\bar{r}_1))}[\bar{\beta}]$. Dies liefert den gewünschten ψ-Homomorphismus, da $\varphi_i(g(x) + \bar{r}_1(x)S_{(\mathrm{disc}(\bar{r}_1))}[x]) = \psi(g(x))(\bar{\beta}_i^*)$ für alle $g(x) \in S_{(\mathrm{disc}(\bar{r}_1))}[x]$ ist. Aus (ii) folgt, daß $\phi_i(\beta')$ für $1 \leq i \leq \deg(\bar{r}_1)$ eine Nullstelle von $\psi(r)$ ist, und wir wollen nun beweisen, daß $\phi_i(\beta') \neq \phi_j(\beta')$ für $i \neq j$ gilt. Die Absolutterme von $\phi_i(\beta')$ bzw. $\phi_j(\beta')$ sind aber gerade $\bar{\beta}_i^*$ bzw. $\bar{\beta}_j^*$, welche aufgrund der Separabilität von $\psi(\bar{r}_1)$ (ψ Monomorphismus) verschieden sind.

(iv) Da $\psi(\bar{r}) \in \psi(S)[x]$ ist, sind die $\bar{\beta}_i^* \in N(\psi(\bar{r}),V)$ ganzalgebraisch über $\psi(S)$, d.h. Elemente von $Cl(\psi(S),\ N(\psi(\bar{r}),V))$. Mittels (iii) erhalten wir $\deg(\bar{r}_1)$ Nullstellen von $\psi(r)$ in $Cl(\psi(S),\ N(\psi(\bar{r}_1),V))_{(\mathrm{disc}(\psi(\bar{r}_1)))}[[\pi]]$. Ist $\bar{r} = \bar{r}_1 \cdots \bar{r}_u$ die Faktorisierung von $\bar{r}$ über Q, so erhalten wir für die anderen Faktoren von $\bar{r}$ analoge Aussagen. Somit liegen in $Cl(\psi(S),\ N(\psi(\bar{r}),V))_{(\mathrm{kgV}\{\mathrm{disc}(\psi(\bar{r}_1)),\ldots,\mathrm{disc}(\psi(\bar{r}_u))\})}[[\pi]] \subseteq Cl(\psi(S),\ N(\psi(\bar{r}),V))_{(\mathrm{disc}(\psi(\bar{r})))}[[\pi]]$ alle Nullstellen von $\psi(r)$ nach Definition der Diskriminante. □

4.32. Bezeichnung. *Wir bezeichnen mit $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f in $N(f, F)$. Die korrespondierenden Strukturen der Restklassenkörper bezüglich einer Stelle $\mathcal{P} \in \mathbb{P}(F)$ bzw. $\mathfrak{p} = \mathcal{P} \cap K(t) \in \mathbb{P}(K(t))$ notieren wir bis auf die Ausnahmen $N(\cdot,\cdot)$ und $\mathcal{G}(\cdot,\cdot)$ mit $\bar{\cdot}$ und indizieren sie gegebenenfalls. Sei also $\bar{F}_{\mathcal{P}}$ der Restklassenkörper von F bezüglich einer Stelle $\mathcal{P}$, $\bar{f} := f \bmod \mathcal{P} \in \bar{F}_{\mathcal{P}}[x]$ und $\mathcal{G}(\bar{f}, \bar{F}_{\mathcal{P}})$ die Galoisgruppe von $\bar{f}$, welche auf den Wurzeln $\bar{\alpha}_1, \ldots, \bar{\alpha}_n \in N(\bar{f}, \bar{F}_{\mathcal{P}})$ operiert. Analog seien mit $\delta_1, \ldots, \delta_m \in N(h, K(t))$ die Nullstellen des Minimalpolynoms h von F/K über $K(t)$ und mit $\bar{\delta}_1, \ldots, \bar{\delta}_m \in N(\bar{h}, \overline{K(t)}_p)$ die Nullstellen von $\bar{h} := h \bmod \mathfrak{p} \in \overline{K(t)}_p[x]$ über $\overline{K(t)}_p$ notiert. Ferner sei $\bar{h} \equiv \bar{h}_1 \ldots \bar{h}_r \bmod \mathfrak{p}$ die Faktorisierung von $\bar{h}$ über $\overline{K(t)}_p$. Ist $\bar{F}_{\mathcal{P}}$ ein algebraischer Zahlkörper, so bezeichnet $\tilde{\mathfrak{p}}$ ein Primideal einer Ordnung von $\bar{F}_{\mathcal{P}}$.*

Die theoretische Idee zur Nullstellenberechnung ist die folgende:
Wir wählen eine über $K(t)$ unverzweigte Stelle $\mathcal{P}$ von F, so daß $\mathfrak{o}$ im Bewertungsring $\mathcal{O}_{\mathcal{P}}$ der Stelle $\mathcal{P}$ liegt und $\operatorname{disc}(f)$ eine Einheit von $\mathcal{O}_{\mathcal{P}}$ ist. Für eine Variable π läßt sich $\mathcal{O}_{\mathcal{P}}$ bzw. $\mathfrak{o}$ bewertungserhaltend ($\nu_{\mathcal{P}} = \nu_\pi \circ \iota_{\mathcal{P}}$) folgendermaßen einbetten:

$$\begin{array}{ccccc} \mathcal{O}_{\mathcal{P}} & \xrightarrow{\iota_{\mathcal{P}}|_{\mathcal{O}_{\mathcal{P}}}} & \bar{F}_{\mathcal{P}}[[\pi]] & \longrightarrow & N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]] \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{O}_{\mathcal{P}}/\mathcal{P} & \xrightarrow{\cong} & \bar{F}_{\mathcal{P}}[[\pi]]/\pi\bar{F}_{\mathcal{P}}[[\pi]] & \longrightarrow & N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]]/\pi N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]] \end{array} \tag{4.33}$$

Die Einbettung $\iota_{\mathcal{P}} : F[x] \longrightarrow \bar{F}_{\mathcal{P}}((\pi))[x]$ ist i.a. nicht eindeutig. Wir werden zeigen, daß alle Nullstellen von $\iota_{\mathcal{P}}(f)(\pi, x)$ in $N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]]$ liegen und $N(\bar{f}, \bar{F}_{\mathcal{P}})$ ein Zerfällungskörper von $\iota_{\mathcal{P}}(f)(0, x)$ ist. Wir wollen nun die obige theoretische Idee algorithmisch umsetzen:
Zur Bestimmung einer über $K(t)$ unverzweigten Stelle $\mathcal{P} \in \mathbb{P}(F)$ mit

$$\operatorname{disc}(f) \notin \mathcal{P} \tag{4.34}$$

verwenden wir Satz 4.1 und wählen ein normiertes, irreduzibles Polynom $p(t) \in R[t]$ minimalen Grades mit $p(t) \nmid \operatorname{disc}(h)$ und $p(t) \nmid \mathrm{N}_{F/K(t)}(\operatorname{disc}(f))$, um Unverzweigtheit und Bedingung (4.34) zu gewährleisten. Die zu $p(t)$ gehörende nun fest gewählte Stelle $\mathcal{P} \in \mathbb{P}(F)$ bzw. $\mathfrak{p} = \mathcal{P} \cap K(t) \in \mathbb{P}(K(t))$ ist aufgrund von Satz 4.1 auch kein Teiler des Index $[\,\mathfrak{o}_F : K[t][\delta]\,]$.

4.35. Bezeichnung. *Für den Rest dieses Kapitels sei nun $\bar{F}_{\mathcal{P}} \cong \overline{K(t)}_p(\bar{\delta}_1) \cong \overline{K(t)}_p[x]/\ \bar{h}_1(x)\overline{K(t)}_p[x]$ und t_0 eine Nullstelle von $p(t)$ aus dem algebraischen Abschluß von K, so daß $\overline{K(t)}_p \cong K(t_0)$ gilt. Aufgrund der Isomorphie wollen wir $\overline{K(t)}_p$ mit $K(t_0)$ und $\bar{F}_{\mathcal{P}}$ mit $K(t_0, \bar{\delta}_1)$ identifizieren.*

Wir beginnen nun die Einbettung $\iota_{\mathcal{P}} : F[x] \longrightarrow \bar{F}_{\mathcal{P}}((\pi))[x]$ zu konstruieren. K ist ein Teilkörper von $K(t_0, \bar{\delta}_1) = \bar{F}_{\mathcal{P}}$. Dies liefert eine Einbettung

$$\iota_{\mathcal{P}}|_{K(t)} \; : \; K(t) \longrightarrow \bar{F}_{\mathcal{P}}((\pi)) : t \mapsto \pi + t_0 \tag{4.36}$$

Durch Operation auf den Koeffizienten läßt sich die Abbildung $\iota_{\mathcal{P}}|_{K(t)}$ auf die Polynomringe $K(t)[x]$ und $\bar{F}_{\mathcal{P}}((\pi))[x]$ fortsetzen. Das Bild des Polynoms $h(t,x) \in R[t][x]$ sei mit $h_{\mathcal{P}}(\pi, x) \in R[t_0][\pi][x] \subset \bar{F}_{\mathcal{P}}((\pi))[x]$ bezeichnet. $h_{\mathcal{P}}(\pi, x)$ ist dann normiert und $h_{\mathcal{P}}(0, x) = \bar{h}(x) \in R[t_0][x]$ separabel, da $p(t) \nmid \operatorname{disc}(h)$. Aufgrund von Satz 4.31 (i) erhalten wir für eine Nullstelle $\bar{\delta}_1 \in N(\bar{h}, \overline{K(t)}_p)$ des irreduziblen Faktors $\bar{h}_1$ von $\bar{h}$ eine Nullstelle δ_1' von $h_{\mathcal{P}}(\pi, x)$ in dem Potenzreihenring $R[t_0]_{(\operatorname{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]]$.

Damit läßt sich die Einbettung $\iota_{\mathcal{P}}$ nun vollständig beschreiben: Nach Meyberg [59], Satz 6.5.5 läßt sich der Körperisomorphismus von $K(t) \longrightarrow K(\pi + t_0) : t \mapsto \pi + t_0$ für Nullstellen $\delta \in F$ von h und $\delta_1' \in \bar{F}_{\mathcal{P}}((\pi))$ von $h_{\mathcal{P}}$ auf $K(t, \delta)$ und $K(\pi + t_0, \delta_1') \subseteq \bar{F}_{\mathcal{P}}((\pi))$ fortsetzen. Wir erhalten die Einbettung

$$\iota_{\mathcal{P}} \; : \; F = K(t, \delta) \longrightarrow \bar{F}_{\mathcal{P}}((\pi)) : \begin{cases} t \mapsto \pi + t_0 \\ \delta \mapsto \delta_1' \end{cases} \tag{4.37}$$

und durch Operation auf den Koeffizienten die Einbettung der zugehörigen Polynomringe. Es gilt $\nu_{\mathcal{P}}(p(t)) = \nu_\pi(p(\pi + t_0)) = 1$, da eine Faktorisierung von $p(t) = (t - t_0) \cdot \cdots \cdot (t - t_{\deg(p(t))-1})$ in dem algebraischen Abschluß von K unter der Einbettung $\iota_{\mathcal{P}}$ auf $p(\pi + t_0) = (\pi) \cdot \cdots \cdot (\pi - (t_{\deg(p(t))-1} - t_0))$ abgebildet wird und alle Nullstellen von $p(t)$ verschieden und nicht Null sind. Darüber hinaus werden Einheiten bzgl. $\iota_{\mathcal{P}}$ auf Einheiten abgebildet und die Einbettung ist somit bewertungserhaltend.

Wir können nun das Polynom $f \in R[t, \delta]$ mittels der Abbildung $\iota_{\mathcal{P}}$ auf $f_{\mathcal{P}} := \iota_{\mathcal{P}}(f) \in R[t_0]_{(\operatorname{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]][x] \subseteq \bar{F}_{\mathcal{P}}[[\pi]][x]$ abbilden. $f_{\mathcal{P}}$ ist normiert und $f_{\mathcal{P}}(0,x) = \bar{f}(x) \in R[t_0, \bar{\delta}_1][x]$ separabel, da $\operatorname{disc}(f) \notin \mathcal{P}$. Aus Satz 4.31 erhalten wir für $S := R[t_0]_{(\operatorname{disc}(\bar{h}_1))}[\bar{\delta}_1]$, $T := N(\bar{f}, \bar{F}_{\mathcal{P}})$, $\psi := \mathrm{id}$ und $r := f_{\mathcal{P}}$ die folgende Proposition:

4.38. Proposition. *$N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]]$ ist der kleinste Potenzreihenring über einem Körper, der alle Nullstellen von $f_{\mathcal{P}}$ enthält.*

Beweis. Da die Absolutkoeffizienten der Nullstellen von $f_{\mathcal{P}}$ als Potenzreihen geschrieben, gerade die Nullstellen $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ von $\bar{f}$ über $\bar{F}_{\mathcal{P}}$ sind (vgl. auch Beweis zu Satz 4.31 (i)), ist der Körper $N(\bar{f}, \bar{F}_{\mathcal{P}})$ minimal mit der Eigenschaft, daß der Potenzreihenring $N(\bar{f}, \bar{F}_{\mathcal{P}})[[\pi]]$ alle Nullstellen von $f_{\mathcal{P}}$ enthält. □

Im Fall $F = \mathbb{F}_q(t, \delta)$ ist es einfach, den Zerfällungskörper von $\bar{f}$ exakt anzugeben. Dies ist gerade $\mathbb{F}_{q^{\deg(\mathcal{P})d}}$ für $d := \mathrm{kgV}\{$Grade der irreduziblen Faktoren von $\bar{f}$ über

$\bar{F}_{\mathcal{P}} = \mathbb{F}_q(t_0, \bar{\delta}_1) = \mathbb{F}_{q^{\deg(\mathcal{P})}}\}$. Für $F = \mathbb{Q}(t, \delta)$ ist es praktisch unmöglich, Berechnungen in $N(\bar{f}, \bar{F}_{\mathcal{P}})$ durchzuführen, schon alleine die Berechnung des Zerfällungskörpers kann für $[N(\bar{f}, \bar{F}_{\mathcal{P}}) : \bar{F}_{\mathcal{P}}] > 150$ schnell extrem zeitaufwendig werden (vgl. z.B. Anai, Noro und Yokoyama [1]). Deshalb bietet es sich an $N(\bar{f}, \bar{F}_{\mathcal{P}})$ in einen anderen Körper einzubetten und zu approximieren. Dazu haben wir im Prinzip zwei Möglichkeiten:

$$N(\bar{f}, \bar{F}_{\mathcal{P}}) \hookrightarrow \begin{cases} \mathbb{Q}_p(\rho) & p, \rho \text{ für } \bar{f} \text{ wie in Sektion 3.2 unter Beachtung, daß } p \nmid \operatorname{disc}(\bar{h}_1) \\ \mathbb{C} & \end{cases} \tag{4.39}$$

Wie auch im Zahlkörperfall führt die Verwendung von komplexen Approximationen zu extrem großen Präzisionen, will man bewiesene Ergebnisse bei der Galoisgruppenberechnung erhalten. Deshalb benutzen wir auch hier komplexe Approximationen der Koeffizienten nur, um Schranken für deren Absolutbeträge zu erhalten.

Betrachtet man nun die separable $\bar{F}_{\mathcal{P}}$-Algebra $\bar{F}_{\mathcal{P}}[\bar{\alpha}]$, wobei $\bar{f}$ Minimalpolynom von $\bar{\alpha}$ über $\bar{F}_{\mathcal{P}}$ ist, so gilt:

4.40. Proposition. *Es existiert eine Nullstelle α' von $f_{\mathcal{P}} \in R[t_0]_{(\operatorname{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]][x]$ in dem Potenzreihenring $R[t_0, \bar{\delta}_1]_{(\operatorname{disc}(\bar{h}_1)\operatorname{disc}(\bar{f}))}[\bar{\alpha}][[\pi]]$.*

Beweis. Da $R[t_0]_{(\operatorname{disc}(\bar{h}_1))}[\bar{\delta}_1]_{(\operatorname{disc}(\bar{f}))}[\bar{\alpha}][[\pi]] = R[t_0, \bar{\delta}_1]_{(\operatorname{disc}(\bar{h}_1)\operatorname{disc}(\bar{f}))}[\bar{\alpha}][[\pi]]$ folgt die Behauptung direkt aus Satz 4.31 (i). □

Mit Satz 4.31 (iii) erhalten wir dann durch Anwendung der folgenden ψ-Homomorphismen ϕ_i die Nullstellen von $\psi(f_{\mathcal{P}})$:

$R = \mathbb{F}_q$ und $R[t_0, \bar{\delta}_1] = \mathbb{F}_{q^{\deg(\mathcal{P})}}$:

Es ist $\mathbb{F}_q[t_0, \bar{\delta}_1][[\pi]][x] \subseteq \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]][x]$ und die Einbettung ψ ist gleich der Inklusionsabbildung. Da $\mathbb{F}_q[t_0, \bar{\delta}_1]_{(\operatorname{disc}(\bar{h}_1)\operatorname{disc}(\bar{f}))} = \mathbb{F}_q[t_0, \bar{\delta}_1]$ folgt

$$\begin{aligned} &\phi_i : \mathbb{F}_q[t_0, \bar{\delta}_1][\bar{\alpha}][[\pi]] \to \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]] : \bar{\alpha} \mapsto \bar{\alpha}_i \\ &\quad \text{für Nullstellen } \bar{\alpha}_i \in \mathbb{F}_{q^{\deg(\mathcal{P})d}} \text{ von } \bar{f} \in \mathbb{F}_q[t_0, \bar{\delta}_1][x],\ (1 \le i \le n). \end{aligned} \tag{4.41}$$

$\Rightarrow$ Erhalte alle Nullstellen $\alpha_i' := \phi_i(\alpha') \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$ von $f_{\mathcal{P}} \in \mathbb{F}_q[t_0, \bar{\delta}_1][[\pi]][x]$.

$R = \mathbb{Z}$ und $R[t_0, \bar{\delta}_1] \cong \mathbb{Z}[\bar{\delta}_1]$ mit $p(t) = t - t_0 \in \mathbb{Z}[t]$ nach Bemerkung 4.2:

$$\begin{aligned} &\psi : \mathbb{Z}[\bar{\delta}_1]_{(\operatorname{disc}(\bar{h}_1)\operatorname{disc}(\bar{f}))}[[\pi]][x] \to \mathbb{Z}_p[[\pi]][x] : \bar{\delta}_1 \mapsto \bar{\delta}_1^* \\ &\quad \text{für eine Nullstelle } \bar{\delta}_1^* \in \mathbb{Z}_p \text{ von } \psi(\bar{h}_1) \in \mathbb{Z}_p[x], \end{aligned} \tag{4.42}$$

welche für ein Primideal $\tilde{\mathfrak{p}} \mid p$ aus $\mathbb{Z}[\bar{\delta}_1]$ nach den Methoden von Sektion 3.2 gewonnen werden kann. $\psi(\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}) \subseteq \mathbb{Z}_p$, da nach Wahl von $\tilde{\mathfrak{p}}|p$ (vgl. Bemerkung 3.11) für die Primzahl $p \nmid \mathrm{disc}(\bar{h}_1)\mathrm{N}_{\mathbb{Q}(\bar{\delta}_1)/\mathbb{Q}}(\mathrm{disc}(\bar{f}))$ gilt und $\psi(\mathrm{disc}(\bar{h}_1))$ und $\psi(\mathrm{disc}(\bar{f}))$ somit Einheiten in $\mathbb{Z}_p$ sind. Es folgt

$$\phi_i \ : \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}][[\pi]] \to \mathbb{Z}_p[\rho][[\pi]] : \begin{cases} \bar{\delta}_1 \mapsto \bar{\delta}_1^* \\ \bar{\alpha} \ \mapsto \bar{\alpha}_i^* \end{cases} \tag{4.43}$$

für $\bar{\delta}_1^* \in \mathbb{Z}_p[\rho]$ aus (4.42) und Nullstellen $\bar{\alpha}_i^* \in \mathbb{Z}_p[\rho]$ von $\psi(\bar{f}) \in \mathbb{Z}_p[x]$, $(1 \le i \le n)$.

$\Rightarrow$ Erhalte alle Nullstellen $\alpha_i'' := \phi_i(\alpha') \in \mathbb{Z}_p[\rho][[\pi]]$ von $\psi(f_{\mathcal{P}}) \in \mathbb{Z}_p[[\pi]][x]$.

Wir wollen nun $f_{\mathcal{P}}(x) \in \mathbb{Z}_{(\mathrm{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]][x] \subseteq \mathbb{Q}(\bar{\delta}_1)[[\pi]][x]$, $(t_0 \in \mathbb{Z})$ nach $\mathbb{C}[[\pi]][x]$ einbetten, um die Nullstellen der Einbettungen über $\mathbb{C}((\pi))$ zu berechnen. Dazu haben wir genau m Möglichkeiten für $\deg(\bar{h}_1) = m$. Wir erhalten

$$\psi_j = .^{(j)} : \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[[\pi]][x] \to \mathbb{C}[[\pi]][x] : \bar{\delta}_1 \mapsto \bar{\delta}_1^{(j)} \tag{4.44}$$

für eine Nullstelle $\bar{\delta}_1^{(j)} \in \mathbb{C}$ von $\bar{h}_1^{(j)} = \bar{h}_1 \in \mathbb{C}[x]$, $(1 \le j \le m)$

und somit

$$\phi_{j,i} \ : \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}][[\pi]] \to \mathbb{C}[[\pi]] : \begin{cases} \bar{\delta}_1 \mapsto \bar{\delta}_1^{(j)} \\ \bar{\alpha} \ \mapsto \bar{\alpha}^{(j,i)} \end{cases} \tag{4.45}$$

für $\bar{\delta}_1^{(j)} \in \mathbb{C}$ aus (4.44) und Nullstellen $\bar{\alpha}^{(j,i)} \in \mathbb{C}$ von $\bar{f}^{(j)} \in \mathbb{C}[x]$, $(1 \le i \le n)$.

$\Rightarrow$ Erhalte alle Nullstellen $\phi_{j,i}(\alpha') \in \mathbb{C}[[\pi]]$ von $f_{\mathcal{P}}{}^{(j)} \in \mathbb{C}[[\pi]][x]$.

4.46. Bemerkung. Vom implementationstechnischen Standpunkt kann es das Programmieren wesentlich vereinfachen, wenn $\bar{f}$ über $F_{\mathcal{P}}$ irreduzibel ist bzw. $\bar{\alpha}$ eine Nullstelle von $\bar{f}$ in einem Körper ist. Betrachtet man die Situation für den absoluten Funktionenkörperfall $F = K(t)$, so existieren nach dem Hilbertschen Irreduzibilitätssatz im Fall $K = \mathbb{Q}$ (vgl. z.B. Völklein [84], Korollar 1.8) unendlich viele Spezialisierungen $t_0 \in \mathbb{Z}$ (welche in der Praxis auch leicht zu finden sind), so daß das Polynom $\bar{f}(x) = f(t_0, x)$ irreduzibel ist. Eine ähnliche Aussage für Stellen eines Funktionkörpers $F = \mathbb{Q}(t, \delta)$ geben wir später an. Da $K = \mathbb{F}_q$ nicht hilbertsch ist, gilt diese Aussage für $F = \mathbb{F}_q(t, \delta)$ nicht. Falls das Polynom $\bar{f}$ nicht irreduzibel ist, so haben wir nach dem Chinesischen Restsatz die Isomorphie

$$\begin{aligned} &R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}] \\ &\qquad \cong R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x]/\bar{f}(x)R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x] \end{aligned} \tag{4.47}$$

$$\cong \bigoplus_{i=1}^{u} R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x]/\bar{f}_i(x)R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x]$$
$$\cong \bigoplus_{i=1}^{u} R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_i],$$

wobei $\bar{f} = \prod_{i=1}^{u} \bar{f}_i$ die Zerlegung von $\bar{f}$ in normierte, irreduzible Faktoren über $\bar{F}_{\mathcal{P}}$ sei. Die $\bar{f}_i$ sind paarweise koprim, da $\bar{f}$ separabel ist, und für $R = \mathbb{F}_q$ ist der Chinesische Restsatz anwendbar. Im Fall $R = \mathbb{Z}$ ist es nicht sofort ersichtlich, daß die Voraussetzungen zur Anwendung des Chinesischen Restsatz gegeben sind. Wir zeigen zunächst, daß $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ ein Dedekindring ist. Dazu beweisen wir die äquivalente Bedingung, daß jedes Ideal $\{0\} \neq \mathfrak{A} \subseteq \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ Produkt von Primidealen aus $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ ist:

Für $\{0\} \neq \mathfrak{A} \subsetneq \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ ist $\mathfrak{A} \cap \mathbb{Z}[\bar{\delta}_1]$ ein Ideal in $\mathbb{Z}[\bar{\delta}_1]$ mit $\mathrm{disc}(\bar{h}_1) \notin \mathfrak{A} \cap \mathbb{Z}[\bar{\delta}_1]$, welches komaximal zu $\mathrm{disc}(\bar{h}_1)\mathbb{Z}[\bar{\delta}_1]$ ist: Dies folgt aus der Tatsache, daß in $\mathfrak{A} \cap \mathbb{Z}_{(\mathrm{disc}(\bar{h}_1))}$ ein Element $0 \neq x = a/b$, $(a, b \in \mathbb{Z})$ mit $\mathrm{ggT}(a, \mathrm{disc}(\bar{h}_1)) = 1$ und $b \,|\, \mathrm{disc}(\bar{h}_1)^k, (k \in \mathbb{Z}_{\geq 0})$ existiert. Damit erhalten wir $a = bx \in \mathfrak{A} \cap \mathbb{Z}$ und $\mathfrak{A} \cap \mathbb{Z} + \mathrm{disc}(\bar{h}_1)\mathbb{Z} = \mathbb{Z}$, und es folgt die Komaximalität. Ist $\mathfrak{f} := \{x \in \mathfrak{o}_{\bar{F}_{\mathcal{P}}} \,|\, x\mathfrak{o}_{\bar{F}_{\mathcal{P}}} \subseteq \mathbb{Z}[\bar{\delta}_1]\}$ der Führer von $\mathbb{Z}[\bar{\delta}_1]$ in $\mathfrak{o}_{\bar{F}_{\mathcal{P}}}$ für $\bar{F}_{\mathcal{P}} = \mathbb{Q}(t_0, \bar{\delta}_1) = \mathbb{Q}(\bar{\delta}_1)$, $(t_0 \in \mathbb{Z})$, so ist $\mathrm{disc}(\bar{h}_1)\mathbb{Z}[\bar{\delta}_1] \subseteq \mathfrak{f}$, und es gilt

$$\mathfrak{A} \cap \mathbb{Z}[\bar{\delta}_1] + \mathrm{disc}(\bar{h}_1)\mathbb{Z}[\bar{\delta}_1] = \mathfrak{A} \cap \mathbb{Z}[\bar{\delta}_1] + \mathfrak{f} = \mathbb{Z}[\bar{\delta}_1]. \tag{4.48}$$

Nach Pohst, Zassenhaus [70] Sektion 6.2, Lemma 2.26 (iii) hat jedes Ideal der Menge $\{\mathfrak{a} \subseteq \mathbb{Z}[\bar{\delta}_1] \,|\, \{0\} \neq \mathfrak{a}$ ist Ideal von $\mathbb{Z}[\bar{\delta}_1]$ mit $\mathfrak{a} + \mathfrak{f} = \mathbb{Z}[\bar{\delta}_1]\}$ eine eindeutige Darstellung als Produkt von Primidealen. Es folgt daher

$$\mathfrak{A} \cap \mathbb{Z}[\bar{\delta}_1] = \tilde{\mathfrak{p}}_1^{e_1} \cdot \cdots \cdot \tilde{\mathfrak{p}}_r^{e_r} \tag{4.49}$$

für Primideale $\tilde{\mathfrak{p}}_i \subset \mathbb{Z}[\bar{\delta}_1]$ mit $\tilde{\mathfrak{p}}_i \cap \{\mathrm{disc}(\bar{h}_1)^k \,|\, k \in \mathbb{Z}_{\geq 0}\} = \emptyset$. Nach Neukirch [62] Kapitel I, §11, Satz 11.1 und Pohst, Zassenhaus [70] Sektion 4.2, 2. stehen die Primideale $\tilde{\mathfrak{p}}$ von $\mathbb{Z}[\bar{\delta}_1]$ mit $\tilde{\mathfrak{p}} \cap \{\mathrm{disc}(\bar{h}_1)^k \,|\, k \in \mathbb{Z}_{\geq 0}\} = \emptyset$ in Bijektion zu den Primidealen von $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ unter Erhaltung der Idealstruktur bzgl. Addition, Multiplikation und Schnittbildung. Es folgt

$$\mathfrak{A} = (\tilde{\mathfrak{p}}_1\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))})^{e_1} \cdots (\tilde{\mathfrak{p}}_r\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))})^{e_r}, \tag{4.50}$$

für Primideale $\tilde{\mathfrak{p}}_i\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ aus $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$. Somit besitzt $\mathfrak{A}$ eine Darstellung als Produkt von Primidealen aus $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$.

Diesen Sachverhalt können wir in unserer Situation anwenden, um zu zeigen, daß die $\bar{f}_i$ für $1 \leq i \leq u$ Koeffizienten in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}$ haben. Da $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ als Dedekindring insbesondere ganz abgeschlossen in seinem Quotientenkörper ist, ist nach dem Lemma von Gauß jede Zerlegung von $\bar{f} \in \mathbb{Z}[\bar{\delta}_1][x]$ über $\bar{F}_{\mathcal{P}}$ eine

Zerlegung über $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))} \subseteq \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}$. Um den Chinesischen Restsatz anwenden zu können, muß nun noch gezeigt werden, daß die $\bar{f}_i$ paarweise komaximale Ideale in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x]$ erzeugen. Aufgrund der Separabilität von $\bar{f}$ ist klar, daß über $\bar{F}_{\mathcal{P}} = \mathbb{Q}(\bar{\delta}_1)$

$$1 = \bar{f}_i(x)r_i(x) + \bar{f}_j(x)r_j(x) \tag{4.51}$$

für Polynome $r_i, r_j \in \mathbb{Q}(\bar{\delta}_1)[x]$, $i \neq j$ gilt. Es folgt $1 = \bar{f}_i(\bar{\alpha}_j)r_i(\bar{\alpha}_j)$ in $\mathbb{Q}(\bar{\delta}_1)[\bar{\alpha}_j]$ für $\bar{\alpha}_j \in N(\bar{f}_j, \bar{F}_{\mathcal{P}})$ mit $\bar{f}_j(\bar{\alpha}_j) = 0$. Im Beweis von Satz 4.31 (i) hatten wir gesehen, daß $\bar{f}_i(\bar{\alpha}_j)$ in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_j]$ invertierbar ist, wenn $N_{\bar{F}_{\mathcal{P}}(\bar{\alpha}_j)/\bar{F}_{\mathcal{P}}}(\bar{f}_i(\bar{\alpha}_j))$ in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}$ invertierbar ist. Da aber $N_{\bar{F}_{\mathcal{P}}(\bar{\alpha}_j)/\bar{F}_{\mathcal{P}}}(\bar{f}_i(\bar{\alpha}_j)) = \mathrm{Res}_x(\bar{f}_i, \bar{f}_j)$ (vgl. Cohen [12], Proposition 4.3.4) und $\mathrm{Res}_x(\bar{f}_i, \bar{f}_j) \mid \mathrm{disc}(\bar{f})$ gilt, folgt $\bar{f}_i(\bar{\alpha}_j)^{-1} = r_i(\bar{\alpha}_j) \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_j]$. Somit ist $r_i \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[x]$; analoges gilt für r_j und die Behauptung folgt.

Man hat also aufgrund der Isomorphie (4.47) die Möglichkeit, für jede Nullstelle $\bar{\alpha}_i$ eines Faktors $\bar{f}_i$ von $\bar{f}$ Satz 4.31 (i) und anschließend den Homomorphismus (4.41) anzuwenden. Dies erfordert dann u-faches Newton-Lifting, wobei man beim Newton-Lifting aber mit kleineren Nennern, kleineren Koeffizienten und kleineren Erweiterungs- bzw. Polynomgraden rechnen kann, als wenn man in $R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}]$ Berechnungen durchführt. Diesen Ansatz haben wir in unserer Implementierung des absoluten globalen Funktionenkörperfalls gewählt, da er sich besser in das bestehende Gesamtkonzept (welches auf Körper ausgelegt ist) eingliedern lies.

Für $F = \mathbb{Q}(t, \delta)$ läßt sich eine Verallgemeinerung des Hilbertschen Irreduzibilitätssatzes auf Stellen des algebraischen Funktionenkörpers beweisen. Damit können wir die Stelle $\mathcal{P} \in \mathbb{P}(F)$ dann so wählen, daß $\bar{f} = f \bmod \mathcal{P}$ irreduzibel ist. Wie im Zahlkörperfall haben wir zunächst den folgenden

4.52. Satz. *Sei $F = \mathbb{Q}(t, \delta)$ ein algebraischer Funktionenkörper.*

(i) Ist $f(x) \in F[x]$ ein irreduzibles Polynom, so existiert $k(t) \in \mathbb{Z}[t]$, so daß $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x - k(t)\delta)) \in \mathbb{Q}(t)[x]$ irreduzibel ist.

(ii) Ist umgekehrt $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x)) \in \mathbb{Q}(t)[x]$ irreduzibel, so ist $f(x) \in F[x]$ irreduzibel.

Beweis. Die Aussagen und Beweise von Pohst, Zassenhaus [70], Section 5.4, Lemma 4.8 und Lemma 4.10 gelten vollkommen analog für $F = \mathbb{Q}(t, \delta)$ und $f(x) \in F[x]$. Behauptung (i) ist dann eine direkte Folgerung der beiden Lemmata und (ii) folgt aus der Multiplikativität der Norm. □

Im Beweis zu Satz 4.52 (i) zeigt sich, daß es nur endlich viele Möglichkeiten für das Polynom $k(t) \in \mathbb{Z}[t]$ gibt, so daß $\mathrm{N}_{F(x)/\mathbb{Q}(t,x)}(f(x - k(t)\delta))$ nicht irreduzibel ist. Deshalb kann man sich auf konstante Polynome aus $\mathbb{Z}[t]$ beschränken. In der Praxis erhält man schon nach ein paar Versuchen $k(t) = \pm 1, \pm 2, \ldots$ ein irreduzibles Polynom $f(x - k(t)\delta)$ mit irreduzibler Norm, wobei die Norm durch Berechnung der Resultanten $\mathrm{Res}_y(h(t,y), f((t,y), x - k(t)y))$ bzgl. der Variablen y erhalten werden kann.

4.53. Satz. *Sei $F = \mathbb{Q}(t,\delta)$ ein algebraischer Funktionenkörper und $f(x) \in F[x]$ ein nichtkonstantes irreduzibles Polynom. Dann existieren unendlich viele Stellen $\mathcal{P}$ vom Grad m von F, so daß $f \bmod \mathcal{P}$ über $\bar{F}_{\mathcal{P}}$ irreduzibel ist.*

Beweis. Sei $h \in \mathbb{Q}(t)[x]$ das Minimalpolynom von $F/\mathbb{Q}(t)$ mit $\deg_x(h) = m$. Wir nehmen zunächst einmal an, daß $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x)) \in \mathbb{Q}(t)[x]$ irreduzibel ist. Nach dem Hilbertschen Irreduzibilitätssatz (vgl. Völklein [84], Korollar 1.8) gibt es dann unendlich viele Spezialisierungen $t_0 \in \mathbb{Z}$, so daß $h(t_0, x)$ und $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x))|_{t=t_0}$ irreduzibel in $\mathbb{Q}[x]$ sind und $(t - t_0) \nmid \mathrm{disc}(h(t,x))$ in $\mathbb{Q}(t)$ gilt. Bezeichne t_0 eine festgewählte beliebige solche Spezialisierung und $\boldsymbol{p}$ die zu $t - t_0$ gehörige Stelle in $\mathbb{Q}(t)$. Nach Satz 4.1 existiert eine eindeutig bestimmte Stelle $\boldsymbol{\mathcal{P}} \in \mathbb{P}(F)$ vom Grad m mit Primelement $t - t_0$ und Restklassenkörper isomorph zu $\mathbb{Q}[x]/h(t_0,x)\mathbb{Q}[x] \cong \mathbb{Q}(\bar{\delta}_1)$. Wir erhalten das folgende kommutative Diagramm:

$$\begin{array}{ccccc} f(x) \in \mathbb{Q}(t,\delta)(x) & = & \mathbb{Q}(x)(t,\delta) & \xrightarrow{\bmod \mathcal{P}'} & \mathbb{Q}(x)(\bar{\delta}_1) \ni f((t_0,\bar{\delta}_1),x) \\ \mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(.) \Big\downarrow & & m & & m \Big\downarrow \mathrm{N}_{\mathbb{Q}(x)(\bar{\delta}_1)/\mathbb{Q}(x)}(.) \\ \mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x)) \in \mathbb{Q}(t)(x) & = & \mathbb{Q}(x)(t) & \xrightarrow{\bmod \mathcal{p}'} & \mathbb{Q}(x) \ni \mathrm{N}_{\mathbb{Q}(x)(\bar{\delta}_1)/\mathbb{Q}(x)}(f((t_0,\bar{\delta}_1),x)) \end{array} \tag{4.54}$$

Da x transzendent über $\mathbb{Q}(t)$ und $F = \mathbb{Q}(t,\delta)$ ist, folgt nach Stichtenoth [80] Lemma III.1.10, daß $[\,F(x) : Q(t)(x)\,] = m$ und h und f über $\mathbb{Q}(t)(x)$ bzw. $F(x)$ irreduzibel sind. Zu $t - t_0$ erhalten wir eine Stelle $\boldsymbol{p}'$ in $\mathbb{Q}(x)(t)$ mit $\boldsymbol{p} = \boldsymbol{p}' \cap \mathbb{Q}(t)$ und nach Satz 4.1 eine Stelle $\boldsymbol{\mathcal{P}}' \in \mathbb{P}(F(x))$ vom Grad m mit $\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{P}}' \cap F$ und Restklassenkörper isomorph zu $\mathbb{Q}(x)[y]/h(t_0,y)\mathbb{Q}(x)[y] \cong \mathbb{Q}(x)(\bar{\delta}_1)$. Da der Restklassenkörper bezüglich der Stelle $\boldsymbol{\mathcal{P}}'$ vollen Grad hat, erhält man in diesem Fall eine Darstellungsmatrix von $f((t_0,\bar{\delta}_1),x)$ durch Reduktion einer Darstellungsmatrix von $f(x)$ modulo der Stelle $\boldsymbol{p}'$, und es gilt

$$\begin{aligned} \mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x))|_{t=t_0} &= \mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x)) \bmod \boldsymbol{p}' \\ &= \mathrm{N}_{\mathbb{Q}(x)(\bar{\delta}_1)/\mathbb{Q}(x)}(f(x) \bmod \boldsymbol{\mathcal{P}}') \\ &= \mathrm{N}_{\mathbb{Q}(x)(\bar{\delta}_1)/\mathbb{Q}(x)}(\,f((t_0,\bar{\delta}_1),x)\,). \end{aligned} \tag{4.55}$$

Nach Wahl von t_0 ist aber $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x))|_{t=t_0}$ irreduzibel über $\mathbb{Q}$. Mit dem Analogon von Satz 4.52 für algebraische Zahlkörper folgt somit, daß $f(x)$ mod

$\mathcal{P}' = f(x) \bmod \mathcal{P}$ irreduzibel über $\bar{F}_{\mathcal{P}} = \mathbb{Q}(\bar{\delta}_1)$ ist. Da es aber unendlich viele t_0 gibt, die obige Eigenschaften erfüllen, gibt es auch unendlich viele Stellen $\mathcal{P} \in \mathbb{P}(F)$ vom Grad m, so daß $f(x) \bmod \mathcal{P}$ irreduzibel über $\bar{F}_{\mathcal{P}}$ ist.

Ist nun $\mathrm{N}_{F(x)/\mathbb{Q}(t)(x)}(f(x))$ nicht irreduzibel über $\mathbb{Q}(t)$, so betrachten wir nach Satz 4.52 das irreduzible Polynom $f(x-k(t)\delta) \in F[x]$, $k(t) \in \mathbb{Z}[t]$ mit irreduzibler Norm. Nach dem bisher gezeigten erhalten wir unendlich viele Stellen $\mathcal{P} \in \mathbb{P}(F)$, so daß $f(x-k(t)\delta) \bmod \mathcal{P} = f((t_0, \bar{\delta}_1), x-k(t_0)\bar{\delta}_1)$ über $\bar{F}_{\mathcal{P}}$ irreduzibel ist. Da Separabilität und Irreduzibilität bei der Transformationen $x \mapsto x+k(t_0)\bar{\delta}_1$, $(k(t_0) \in \mathbb{Z})$ in $\bar{F}_{\mathcal{P}}[x]$ erhalten bleiben, ist $f(x) \bmod \mathcal{P}$ über $\bar{F}_{\mathcal{P}}$ irreduzibel. □

4.56. Bemerkung. Damit im Fall $K = \mathbb{Q}$ das Polynom $\bar{f}$ über $\bar{F}_{\mathcal{P}}$ irreduzibel ist, sind bei der Wahl der Stelle $\mathcal{P}$ mit Primelement $p(t) = t - t_0 \in \mathbb{Z}[t]$ nun insgesamt folgende Kriterien zu beachten:

(*i*) Bestimme $k \in \mathbb{Z}$, so daß $\mathrm{N}_{F(x)/\mathbb{Q}(t,x)}(f(x-k\delta))$ irreduzibel über $\mathbb{Q}(t)$.

(*ii*) Wähle $t_0 \in \mathbb{Z}$ mit
$\mathrm{N}_{F(x)/\mathbb{Q}(t,x)}(f(x-k\delta))|_{t=t_0}$ irreduzibel über $\mathbb{Q}$,
$h(t_0, x) = \bar{h}$ irreduzibel über $\mathbb{Q}$,
$(t-t_0) \nmid \mathrm{N}_{F/\mathbb{Q}(t)}(\mathrm{disc}(f))$ und
$(t-t_0) \nmid \mathrm{disc}(h)$.

Abschließend wollen wir die Algorithmen zur Nullstellenberechnung für den globalen Funktionenkörperfall und für den Funktionenkörperfall über $\mathbb{Q}$ mit $\tilde{\mathfrak{p}}$-adischem Koeffizientenbereich konkret ausführen.

4.57. Algorithmus. *(Nullstellenberechnung Funktionenkörperfall $F = \mathbb{F}_q(t, \delta)$)*

Eingabe: *Ein in x normiertes, separables Polynom $f \in \mathbb{F}_q[t, \delta][x]$ vom Grad n, Minimalpolynom $h \in \mathbb{F}_q[t][x]$ von δ über $\mathbb{F}_q(t)$ vom Grad m, eine Stelle $\mathcal{P} \in \mathbb{P}(F)$ mit Primelement $p(t) \in \mathbb{F}_q[t]$ minimalen Grades, welche der Bedingungen (4.34) genügt, und $l \in \mathbb{Z}_{>0}$.*

Ausgabe: *Approximationen $\alpha'_{1,(l)}, \ldots, \alpha'_{n,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})\,d}}[\pi]$ der Nullstellen von $\iota_{\mathcal{P}}(f)$ $\bmod \pi^l \mathbb{F}_{q^{\deg(\mathcal{P})\,d}}[[\pi]]$ für $\iota_{\mathcal{P}}$ aus (4.37).*

1. *(Initialisierung) Wähle $t_0 \in \mathbb{F}_{q^{\deg(\mathcal{P})}}$ mit $p(t_0) = 0$, $\pi := t - t_0$, $\boldsymbol{p} := \mathcal{P} \cap \mathbb{F}_q(t)$, $\bar{h} := h \bmod \boldsymbol{p} \in \mathbb{F}_q(t_0)[x]$ mit $\bar{h} = \bar{h}_1 \cdots \bar{h}_r$ Faktorisierung in irreduzible Faktoren über $\mathbb{F}_q(t_0)$, wähle $\bar{\delta}_1 \in \mathbb{F}_{q^{\deg(\mathcal{P})}}$ mit $\bar{h}_1(\bar{\delta}_1) = 0$, $\bar{f} := f \bmod \mathcal{P} \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[x]$ mit $\bar{f} = \bar{f}_1 \cdots \bar{f}_u$ Faktorisierung in irreduzible Faktoren über $\mathbb{F}_{q^{\deg(\mathcal{P})}}$ und $d := \mathrm{kgV}\{\deg(\bar{f}_1), \ldots, \deg(\bar{f}_u)\}$.*

2. *(Nullstellen von $\bar{f}_1, \ldots, \bar{f}_u$) Für $i = 1, \ldots, u$ berechne Nullstellen $\bar{\alpha}_{i,1}, \ldots, \bar{\alpha}_{i,n_i} \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}$ von $\bar{f}_i$ über $\mathbb{F}_{q^{\deg(\mathcal{P})d}}$.*

3. *(Newton-Lifting für $\bar{\alpha}_{i,1}$) Für $i = 1, \ldots, u$ bestimme mittels Newton-Lifting für $\bar{\alpha}_{i,1}$ eine Approximation $\alpha'_{i,1,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[\bar{\alpha}_{i,1}][\pi]$ mit $\iota_{\mathcal{P}}(f)(\alpha'_{i,1,(l)}) \equiv 0 \bmod \pi^l \mathbb{F}_{q^{\deg(\mathcal{P})}}[\bar{\alpha}_{i,1}][[\pi]]$.*

4. *(Homomorphismen ϕ_i (4.41)) Für $i = 1, \ldots, u$ und $j = 2, \ldots, n_i$ erhalte $\alpha'_{i,j,(l)}$ durch Substitution von $\bar{\alpha}_{i,1}$ durch $\bar{\alpha}_{i,j}$ in $\alpha'_{i,1,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[\bar{\alpha}_{i,1}][\pi]$.*

5. *(Ende) Ausgabe von $\alpha'_{1,1,(l)}, \ldots, \alpha'_{1,n_1,(l)}, \alpha'_{2,1,(l)}, \ldots, \alpha'_{u,n_u,(l)} = \alpha'_{1,(l)}, \ldots, \alpha'_{n,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}[\pi]$. Terminiere.*

4.58. Bemerkung. Die Ausführung der Rechnung kann beschleunigt werden, wenn man t durch $t+t_0$ substituiert. Dadurch wird erreicht, daß nur $\bmod t$ gerechnet wird, womit man beim Newton-Lifting Zeit spart und und außerdem Nullstellen mit geringerer l-Präzision einfach durch abschneiden der höheren l-Potenzen erhält. Ist t_0 kein Element von $\mathbb{F}_q$, so erfordert dies eine Konstantenkörpererweiterung, wobei aber für den im folgenden Abschnitt beschriebenen Inklusionstest zurücksubstituiert werden muß.

4.59. Algorithmus. *(Nullstellenberechnung Funktionenkörperfall $F = \mathbb{Q}(t, \delta)$)*

Eingabe: *Ein in x normiertes, separables irreduzibles Polynom $f \in \mathbb{Z}[t, \delta][x]$ vom Grad n, Minimalpolynom $h \in \mathbb{Z}[t][x]$ von δ über $\mathbb{Q}(t)$ vom Grad m, eine Stelle $\mathcal{P} \in \mathbb{P}(F)$ mit Primelement $p(t) = t - t_0 \in \mathbb{Z}[t]$, welche den Bedingungen (4.56) genügt, und $k, l \in \mathbb{Z}_{>0}$.*

Ausgabe: *Approximationen $\alpha''_{1,(k,l)}, \ldots, \alpha''_{n,(k,l)} \in \mathbb{Z}[\rho][\pi]$ der Nullstellen von $(\psi \circ \iota_{\mathcal{P}})(f) \bmod p^k \mathbb{Z}_p[\rho][[\pi]] + \pi^l \mathbb{Z}_p[\rho][[\pi]]$ für ψ, $\iota_{\mathcal{P}}$ aus (4.42) bzw. (4.37).*

1. *(Initialisierung) $\pi := t - t_0$, $\boldsymbol{p} := \mathcal{P} \cap \mathbb{Q}(t)$, $\bar{h}_1 := \bar{h} := h \bmod \boldsymbol{p} \in \mathbb{Z}[x]$ Minimalpolynom von $\bar{\delta}_1 \in N(\bar{h}_1, \mathbb{Q})$ über $\mathbb{Q}$, $\bar{F}_{\mathcal{P}} := \mathbb{Q}(\bar{\delta}_1)$, $\bar{f} := f \bmod \mathcal{P} \in \mathbb{Z}[\bar{\delta}_1][x]$ Minimalpolynom von $\bar{\alpha} = x + \bar{f}(x)\bar{F}_{\mathcal{P}}[x] \in \bar{F}_{\mathcal{P}}[x]/\bar{f}(x)\bar{F}_{\mathcal{P}}[x]$ über $\bar{F}_{\mathcal{P}}$.*

2. *(Nullstellenapproximationen von $\psi(\bar{h}_1)$ und $\psi(\bar{f})$) Bestimme Primideal $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$ nach Bemerkung 3.11 mit $p \in \tilde{\mathfrak{p}}$ und wende Algorithmus 3.10 auf $\bar{h}_1$, $\bar{f}$ und Gleichungsordnung $\mathbb{Z}[\bar{\delta}_1]$ an : Erhalte eine Approximation $\bar{\delta}^*_{1,(k)} \in \mathbb{Z}[\rho]$ mit $\bar{h}_1(\bar{\delta}^*_{1,(k)}) \equiv 0 \bmod p^k \mathbb{Z}[\rho]$ und Approximationen $\bar{\alpha}^*_{1,(k)}, \ldots, \bar{\alpha}^*_{n,(k)} \in \mathbb{Z}[\rho]$ mit $\tilde{\bar{f}}(\bar{\alpha}^*_{i,(k)}) \equiv 0 \bmod p^k \mathbb{Z}[\rho]$ für $\tilde{\bar{f}} \in \mathbb{Z}[x]$ mit $\tilde{\bar{f}} - \bar{f} \equiv 0 \bmod \tilde{\mathfrak{p}}^k$ aus Algorithmus 3.10.*

3. *(Newton-Lifting für $\bar{\alpha} = x + \bar{f}(x)\bar{F}_{\mathcal{P}}[x]$) Bestimme mittels Newton-Lifting für $\bar{\alpha} \in \bar{F}_{\mathcal{P}}[x]/\bar{f}(x)\bar{F}_{\mathcal{P}}[x]$ eine Approximation $\alpha'_{(l)} \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h})\mathrm{disc}(\bar{f}))}[\bar{\alpha}][\pi]$ mit $\iota_{\mathcal{P}}(f)(\alpha'_{(l)}) \equiv 0 \bmod \pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h})\mathrm{disc}(\bar{f}))}[\bar{\alpha}][[\pi]]$.*

4. *(Homomorphismen ϕ_i (4.43)) Für $i = 1, \ldots, n$ erhalte $\alpha''_{i,(k,l)} \in \mathbb{Z}[\rho][\pi]$ durch Substitution von $\bar{\delta}_1$ durch $\bar{\delta}^*_{1,(k)}$ und $\bar{\alpha}$ durch $\bar{\alpha}^*_{i,(k)}$ in $\alpha'_{(l)} \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h})\mathrm{disc}(\bar{f}))}[\bar{\alpha}][\pi]$.*

5. *(Ende) Ausgabe von $\alpha''_{1,(k,l)}, \ldots, \alpha''_{n,(k,l)} \in \mathbb{Z}[\rho][\pi]$. Terminiere.*

4.60. Bemerkung. Die Nullstellenberechnung über $\mathbb{C}((\pi))$ verläuft analog wie in Algorithmus 4.59 bei Verwendung komplexer Approximationen einer Nullstelle von $\bar{h} \in \mathbb{C}[x]$ und der Nullstellen von $\bar{f}^{(j)} \in \mathbb{C}[x]$, $(1 \leq j \leq r_1 + r_2)$. Der Parameter k wird dann für die reelle Präzision verwendet.

4.3 Inklusionstest

Wir betrachten nun die Situation

$$\begin{array}{ccccc}
\begin{array}{c} Cl(\mathbb{Z}[t], N(f,F))[x] \\ Cl(\mathfrak{o}_F, N(f,F))[x] \end{array} & \xrightarrow{\iota_{\mathcal{P}}} & \begin{array}{c} \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_1, \ldots, \bar{\alpha}_n][[\pi]][x] \\ \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]][x] \end{array} & \xrightarrow{\psi} & \begin{array}{c} \mathbb{Z}_p[\rho][[\pi]][x] \\ \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]][x] \end{array} \\
\uparrow & & \uparrow & & \uparrow \\
\begin{array}{c} Cl(\mathbb{Z}[t], F)[x] \\ \mathfrak{o}_F[x] \end{array} & \xrightarrow{\iota_{\mathcal{P}}} & \begin{array}{c} \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[[\pi]][x] \\ \mathbb{F}_{q^{\deg(\mathcal{P})}}[[\pi]][x] \end{array} & \xrightarrow{\psi} & \begin{array}{c} \mathbb{Z}_p[[\pi]][x] \\ \mathbb{F}_{q^{\deg(\mathcal{P})}}[[\pi]][x]. \end{array}
\end{array} \tag{4.61}$$

Die Monomorphismen $\iota_{\mathcal{P}}$ und ψ aus (4.41) bzw. (4.42) setzen wir zu bewertungserhaltenden Monomorphismen der Ringe der oberen Zeile von (4.61) fort: Alle Nullstellen $\alpha_1, \ldots, \alpha_n$ des Polynoms $f \in \mathbb{Z}[t, \delta][x]$ sind in $Cl(\mathbb{Z}[t], N(f,F))$ enthalten, da $\delta \in Cl(\mathbb{Z}[t], F)$. Außerdem erhält man mittels Satz 4.31 alle Nullstellen $\alpha'_1, \ldots, \alpha'_n$ von $\iota_{\mathcal{P}}(f)$ in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_1, \ldots, \bar{\alpha}_n][[\pi]]$ bzw. $\mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$ und alle Nullstellen $\alpha''_1, \ldots, \alpha''_n$ von $(\psi \circ \iota_{\mathcal{P}})(f)$ in $\mathbb{Z}_p[\rho][[\pi]]$. Indem wir α_i auf α'_i und $\bar{\alpha}_i$ auf $\bar{\alpha}^*_i \in \mathbb{Z}_p[\rho]$, $(1 \leq i \leq n)$ in der richtigen Reihenfolge abbilden (und somit α'_i auf α''_i), erhalten wir die Fortsetzungen von $\iota_{\mathcal{P}}$ und ψ auf obige Ringe und deren Quotientenkörper, welche wir ebenfalls mit $\iota_{\mathcal{P}}$ und ψ bezeichnen wollen. Im globalen Funktionenkörperfall ist die Abbildung ψ die Identität. Nach Lorenz [52], §23, Satz 5 existiert genau eine Fortsetzung der Bewertung ν_π von $F_{\mathcal{P}}((\pi))$ auf $N(\bar{f}, \bar{F}_{\mathcal{P}})((\pi))$. Bezeichnen wir diese ebenfalls mit ν_π und setzen $\nu_{\mathcal{P}}(a) := \nu_\pi(\iota_{\mathcal{P}}(a))$ für alle $a \in N(f,F)$, so ist die Fortsetzung $\iota_{\mathcal{P}}$ bewertungserhaltend. Analog erhalten wir für das Primideal $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$ eine bewertungserhaltende Fortsetzung von $\nu_{\tilde{\mathfrak{p}}}$ auf den Zerfällungskörper $N(\bar{f}, \bar{F}_{\mathcal{P}})$, indem wir $\nu_{\tilde{\mathfrak{p}}}(a) := \nu_p(\psi(a))$ für alle $a \in N(\bar{f}, \bar{F}_{\mathcal{P}})$ setzen.

Wir betrachten nun approximierte Nullstellen der Resolvente in $\mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$ bzw. $\mathbb{Z}_p[\rho][[\pi]]$, die wir nach einigen Berechnungen mit den approximierten Nullstellen

des Polynoms $(\psi \circ \iota_{\mathcal{P}})(f)$ erhalten haben. Wir möchten beweisen oder widerlegen, ob das Resolventenpolynom $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ eine einfache Nullstelle in $\mathfrak{o}_F$ besitzt. Die Lösung dieser Aufgabenstellung besteht wie im Zahlkörperfall (vgl. Sektion 3.3) in der Entwicklung eines zweiteiligen Basisalgorithmus mit den dort genannten Spezifikationen. Zusätzlich gilt es zu berücksichtigen, daß im Fall $K = \mathbb{Q}$ die Koeffizienten der approximierten Nullstellen nicht exakt gegeben sind.

Für den Rest dieses Kapitels fixieren wir eine $K[t]$-Basis $\omega_1, \ldots, \omega_m$ von $\mathfrak{o}_F$. Für eines der ω_i gilt $\pi \nmid \iota_{\mathcal{P}}(\omega_i)$, da sonst alle ω_i im Primideal $\mathcal{P} \cap \mathfrak{o}_F$ liegen würden. Wir wollen o.B.d.A annehmen, daß $\pi \nmid \iota_{\mathcal{P}}(\omega_1)$ gilt. Bezüglich der Basis von $\mathfrak{o}_F$ läßt sich jedes Element $\gamma = \sum_{i=1}^{m} \lambda_i \omega_i$ von F durch den m-elementigen Vektor $(\lambda_1, \ldots, \lambda_m) \in K(t)^m$ eindeutig darstellen. Speziell ist $\gamma \in \mathfrak{o}_F$ genau dann, wenn die $\lambda_i \in K[t]$, $(1 \leq i \leq m)$ sind.

4.62. Bezeichnung. *Sei* $S := \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_1, \ldots, \bar{\alpha}_n]$ *und* $k, l \in \mathbb{Z}_{>0}$. *Wir vereinbaren folgende Bezeichnungen:*

	$\begin{matrix} Cl(\mathbb{Z}[t], N(f,F)) \\ Cl(\mathfrak{o}_F, N(f,F)) \end{matrix} \xrightarrow{\iota_{\mathcal{P}}}$	$\begin{matrix} S[[\pi]] \\ \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]] \end{matrix} \xrightarrow{\psi}$	$\mathbb{Z}_p[\rho][[\pi]]$
exakte Nullstelle	γ, γ_σ	γ', γ'_σ	$\gamma'', \gamma''_\sigma$
Approximation		$\gamma'_{(l)}, \gamma'_{\sigma,(l)} \in \{S[\pi], \mathbb{F}_{q^{\deg(\mathcal{P})d}}[\pi]\}$ *vom Grad* $l-1$ *mit* $\gamma'_{(l)} \equiv \gamma' \bmod \pi^l S[[\pi]]$ $\gamma'_{(l)} \equiv \gamma' \bmod \pi^l \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$ $\gamma'_{\sigma,(l)} \equiv \gamma'_\sigma \bmod \pi^l S[[\pi]]$ $\gamma'_{\sigma,(l)} \equiv \gamma'_\sigma \bmod \pi^l \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$	$\gamma''_{(k,l)}, \gamma''_{\sigma,(k,l)} \in \mathbb{Z}[\rho][\pi]$ *vom Grad* $l-1$ *mit* $\gamma''_{(k,l)} \equiv \gamma'' \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$ $\gamma''_{\sigma,(k,l)} \equiv \gamma''_\sigma \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$
		$\gamma'^{[j]}_{(l)}, \gamma'^{[j]}_{\sigma,(l)} \in \mathbb{C}[\pi]$, $(1 \leq j \leq m)$ *vom Grad* $l-1$ *mit* $\gamma'^{[j]}_{(l)} \equiv \gamma'^{[j]} \bmod \pi^l\mathbb{C}[[\pi]]$ *für* $\gamma'^{[j]} := F(\phi_{j,1}(\alpha'), \ldots, \phi_{j,n}(\alpha')) \in \mathbb{C}[[\pi]]$ $\gamma'^{[j]}_{\sigma,(l)} \equiv \gamma'^{[j]}_{\sigma} \bmod \pi^l\mathbb{C}[[\pi]]$ *für* $\gamma'^{[j]}_{\sigma} := \sigma F(\phi_{j,1}(\alpha'), \ldots, \phi_{j,n}(\alpha')) \in \mathbb{C}[[\pi]]$	

Exakte Nullstellen des Resolventenpolynoms $R_{(G,H,F)}$ *und der isomorphen Bilder* $\iota_{\mathcal{P}}(R_{(G,H,F)}), (\psi \circ \iota_{\mathcal{P}})(R_{(G,H,F)})$ *werden mit* γ, γ' *bzw.* γ'' *bezeichnet. Indizierung mit* σ *erfolgt analog wie in Bezeichnung 3.14. Unter einer* (k,l)*-Approximation von* $\gamma'' \in \mathbb{Z}_p[\rho][[\pi]]$ *verstehen wir ein Polynom* $\gamma''_{(k,l)} \in \mathbb{Z}[\rho][\pi]$ *vom Grad* $l-1$ *mit* $\gamma''_{(k,l)} \equiv \gamma'' \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$. *Entsprechend sei eine* l*-Approximation von* γ' *wie in obiger Tabelle definiert. Durch Auswertung von* $\sigma F(x_1, \ldots, x_n)$, $\sigma \in G//H$ *an den Stellen* $\phi_{j,1}(\alpha'), \ldots, \phi_{j,n}(\alpha') \in \mathbb{C}[[\pi]]$ *aus* (4.45) *erhalten wir die exakten Nullstellen von* $R^{(j)}_{(G,H,F)} \in \mathbb{C}[[\pi]][X]$, $(1 \leq j \leq m)$ *in* $\mathbb{C}[[\pi]]$. *Diese werden mit* $\gamma'^{[j]}, \gamma'^{[j]}_{\sigma}$ *und die zugehörigen* l*-Approximationen mit* $\gamma'^{[j]}_{(l)}$ *bzw.* $\gamma'^{[j]}_{\sigma,(l)}$

notiert. Schließlich sei für ein Polynom $\Gamma = \Gamma_0 + \Gamma_1\pi + \cdots + \Gamma_{l-1}\pi^{l-1} \in \mathbb{C}[\pi]$ *mit* $\|\Gamma\|_\infty := \max_{0\le\nu\le l-1}\{\,|\Gamma_\nu|\,\}$ *die Maximumnorm bezeichnet und für die Reihe* $\Gamma = \sum_{\nu=0}^{\infty}\Gamma_\nu \in \mathbb{C}[[\pi]]$ *setzen wir* $\|\Gamma\|_{\infty,(l)} := \max_{0\le\nu\le l-1}\{\,|\Gamma_\nu|\,\}$.

4.63. Bemerkung. Um eine Nullstelle γ der Resolvente in $\mathfrak{o}_F$ rekonstruieren zu können, ist $\gamma'_{(l)} \in \bar{F}_{\mathcal{P}}[\pi]$ für alle $l \in \mathbb{Z}_{>0}$ eine notwendige Bedingung.

Da wir im Fall $K = \mathbb{Q}$ die Nullstellen der Resolvente in $\mathbb{Z}_p[\rho][[\pi]]$ gegeben haben, ist zunächst eine Rekonstruktion der Koeffizienten erforderlich. Für eine Nullstelle $\gamma \in Cl(\mathbb{Z}[t], F)$ der Resolvente mit (k,l)-Approximation

$$\gamma''_{(k,l)} \equiv (\psi\circ\iota_{\mathcal{P}})(\gamma) \bmod p^k\mathbb{Z}_p[\rho][\pi] + \pi^l\mathbb{Z}_p[\rho][\pi] \text{ von } (\psi\circ\iota_{\mathcal{P}})(\gamma) \text{ und}$$

$$\gamma''_{(k,l)} \;=\; \sum_{\nu=0}^{l-1} g^*_{(k),\nu}\pi^\nu \in \mathbb{Z}[\rho][\pi]$$

wollen wir $\gamma''_{(k,l)}$ koeffizientenweise zu $\gamma'_{(l)} \equiv \iota_{\mathcal{P}}(\gamma) \bmod \pi^l\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_1,\ldots,\bar{\alpha}_n][[\pi]]$ in $\iota_{\mathcal{P}}(Cl(\mathbb{Z}[t],F)) \subseteq \bar{F}_{\mathcal{P}}[[\pi]]$ rekonstruieren. Beliebige Elemente aus dem Restklassenkörper $\bar{F}_{\mathcal{P}}$ können nicht ohne Zusatzinformationen, d.h. Schranken über die Größe von Zähler und Nenner, rekonstruiert werden. In Sektion 3.4 hatten wir gesehen, daß auftretende Nenner zu höheren Rekonstruktionspräzisionen führen. Deshalb hätten wir gerne, daß die zu rekonstruierenden Koeffizienten von $\gamma'_{(l)}$ möglichst „ganz“ sind. Aufgrund unserer Ausführungen zur Nullstellenberechnung wissen wir, daß bei der Rekonstruktion der $g^*_{(k),\nu} \in \mathbb{Z}[\rho]$ nur Vielfache der Diskriminanten von $\mathrm{disc}(\bar{h}_1)$ und $\mathrm{disc}(\bar{f})$ als Nenner auftreten können, da man $\gamma''_{(k,l)}$ durch Addition, Multiplikation und Subtraktion der $\alpha''_{1,(k,l)},\ldots,\alpha''_{n,(k,l)}$ erhält. Andererseits stellt sich aufgrund der Annahme $\gamma \in Cl(\mathbb{Z}[t],F)$ die Frage, welche Nenner auftreten können, wenn wir γ mittels der Einbettung $\iota_{\mathcal{P}}$ nach $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}_1,\ldots,\bar{\alpha}_n][[\pi]]$ einbetten.

4.64. Proposition. *Sei* γ *eine Nullstelle der Resolvente, welche in* $Cl(\mathbb{Z}[t],F)$ *liegt. Dann liefert Multiplikation des* ν*-ten Koeffizienten der zugehörigen Reihe* $\iota_{\mathcal{P}}(\gamma) \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[[\pi]]$ *mit* $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,\,1\}}$, $(\nu \in \mathbb{Z}_{\ge 0})$ *ein Element in* $\mathbb{Z}[\bar{\delta}_1]$.

Beweis. Nach Voraussetzung gilt $\gamma \in Cl(\mathbb{Z}[t],F)$ und mittels Neukirch [62], Kapitel I, §2, Lemma 2.9 folgt $Cl(\mathbb{Z}[t],F) \subseteq \mathbb{Z}[t,\delta]/\mathrm{disc}(h)$. Unter der Abbildung $\iota_{\mathcal{P}}$ erhält $\mathbb{Z}[t,\delta]$ Nenner $\mathrm{disc}(\bar{h}_1)^k$, $(k \in \mathbb{Z}_{>0})$, da δ nach (4.37) auf $\delta'_1 \in \mathbb{Z}_{(\mathrm{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]]$ abgebildet wird, welches mittels Newton-Lifting erhalten wurde. Aus der linearen Newton-Iteration folgt, daß $\delta'_1 = \bar{\delta}_1 + \sum_{\nu=1}^{\infty}\frac{b_\nu}{d_\nu}\pi^\nu$, $(b_\nu \in \mathbb{Z}[\bar{\delta}_1], d_\nu \in \mathbb{Z}_{>0})$ an der ν-ten Stelle maximal den Nenner $d_\nu = \mathrm{disc}(\bar{h}_1)^{2\nu-1}$ hat. Da der Absolutkoeffizient von $\iota_{\mathcal{P}}(\mathrm{disc}(h))$ gerade $\mathrm{disc}(\bar{h}) = \mathrm{disc}(\bar{h}_1) \neq 0$ ist, läßt sich

$\iota_{\mathcal{P}}(\mathrm{disc}(h))$ in $\bar{F}_{\mathcal{P}}[[\pi]]$ invertieren. Bildet man das Inverse von $\iota_{\mathcal{P}}(\mathrm{disc}(h)) \in \bar{F}_{\mathcal{P}}[[\pi]]$, so sieht man durch Koeffizientenvergleich, daß $\iota_{\mathcal{P}}(\mathrm{disc}(h))^{-1}$ an der ν-ten Stelle maximal den Nenner $\mathrm{disc}(h)(t_0)^{\nu+1} = \mathrm{disc}(\bar{h})^{\nu+1} = \mathrm{disc}(\bar{h}_1)^{\nu+1}$, $(\nu \in \mathbb{Z}_{\geq 0})$ hat. Multiplikation der beiden Potenzreihen ergibt dann an der ν-ten Stelle maximal den Nenner $\mathrm{disc}(\bar{h}_1)$ für $\nu = 0$ und ansonsten $\mathrm{disc}(\bar{h}_1)^{2\nu}$ für $\nu > 0$. □

Mit dieser Proposition können wir nach Sektion 3.4 $\gamma''_{(k,l)} = \sum_{\nu=0}^{l-1} g^*_{(k),\nu}\pi^\nu \in \mathbb{Z}[\rho][\pi]$ zu $\gamma'_{(l)} \in \mathbb{Z}_{(\mathrm{disc}(h_1))}[\bar{\delta}_1][\pi]$ rekonstruieren, indem wir die Elemente $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,\,1\}} g^*_{(k),\nu}$, $(\nu \in \mathbb{Z}_{\geq 0})$ der Gleichungsordnung $\mathbb{Z}[\bar{\delta}_1]$ rekonstruieren. Dies geschieht mittels Algorithmus 3.38 für das Primideal $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$ aus Algorithmus 4.59, Basis $1, \bar{\delta}_1, \ldots, \bar{\delta}_1^{m-1}$ von $\mathbb{Z}[\bar{\delta}_1]$ und einer k-Präzision von

$$\begin{aligned} k \;>\; & m \log_p \big(2^{\frac{m}{2}} \big(\big(|\mathrm{disc}(\bar{h}_1)|^{\max\{2\nu,\,1\}} (A_{\bar{F}_{\mathcal{P}},\nu} - 1) + 1 \big)^2 + \\ & |\mathrm{disc}(\bar{h}_1)|^{\max\{2\nu,\,1\}} (A_{\bar{F}_{\mathcal{P}},\nu} - 1) + 1 \big) \big) + \sum_{j=1}^{m} \log_p(W_{\bar{F}_{\mathcal{P}},j}) \end{aligned} \tag{4.65}$$

für

$$\begin{aligned} A_{\bar{F}_{\mathcal{P}},\nu} \;&=\; \| \big(\mu(1), \ldots, \mu(\bar{\delta}_1^{m-1})\big)^{-1} \| \, (\textstyle\sum_{j=1}^{m} M^2_{\bar{F}_{\mathcal{P}},j,\nu})^{1/2} + 1, \text{ wobei} \\ &\quad\; \mu : \mathbb{Q}(\bar{\delta}_1) \to \mathbb{R}^m \text{ die Minkowskiabbildung bezeichne,} \\ M_{\bar{F}_{\mathcal{P}},j,\nu} \;&=\; \text{Reelle obere Schranke von } |g_{j,\nu}| \text{ für } \gamma'^{[j]}_{(l)} = \textstyle\sum_{\nu=0}^{l-1} g_{j,\nu}\pi^\nu \in \mathbb{C}[\pi], \\ W_{\bar{F}_{\mathcal{P}},j} \;&=\; \Big(\|(1, \mathrm{Re}(\bar{\delta}_1^{(j)}), \ldots, \mathrm{Re}(\bar{\delta}_1^{m-1\,(j)}))\|^2 + \|(0, \mathrm{Im}(\bar{\delta}_1^{(j)}), \ldots, \mathrm{Im}(\bar{\delta}_1^{m-1\,(j)}))\|^2 \Big)^{1/2}. \end{aligned} \tag{4.66}$$

4.67. Bemerkung. (i) Es ist an dieser Stelle nicht klar, ob die k-Präzision ausreicht, zu beweisen, daß das zu $\gamma''_{(k,l)} = \sum_{\nu=0}^{l-1} g^*_{(k),\nu}\pi^\nu \in \mathbb{Z}_p[\rho][\pi]$ rekonstruierte Polynom in $\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi]$ auch wirklich eine Nullstelle des Resolventenpolynoms $\iota_{\mathcal{P}}(R_{(G,H,F)})$ ist. War $\gamma' \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]$, so stimmt aber das rekonstruierte Polynom mit $\gamma'_{(l)}$ modulo $\pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]$ überein.

(ii) Zur Bestimmung der $M_{\bar{F}_{\mathcal{P}},j,\nu} \in \mathbb{R}$, $(1 \leq j \leq r_1 + r_2,\ 1 \leq \nu \leq l-1)$ machen wir Gebrauch von den Nullstellen der verschiedenen komplexen Einbettungen des Polynoms $\iota_{\mathcal{P}}(f) \in \mathbb{Z}_{(\mathrm{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]][x]$ nach $\mathbb{C}[[\pi]]$. Mit den Bezeichnungen von (4.45) erhalten wir die Nullstellen

$$\phi_{j,i}(\alpha') = \sum_{\nu=0}^{\infty} a_{j,i,\nu}\pi^\nu \in \mathbb{C}[[\pi]],\ (1 \leq i \leq n)$$

von $\iota_{\mathcal{P}}(f)^{(j)}$ für $1 \leq j \leq r_1 + r_2$. Für $0 \leq \nu \leq l-1$ sei $c_{j,\nu} := \max_{1 \leq i \leq n}\{|a_{j,i,\nu}|\}$ und

$$C^{[j]}_{(l)}(\pi) := c_{j,0} + c_{j,1}\pi + \cdots + c_{j,l-1}\pi^{l-1} \in \mathbb{R}[\pi],\ \ (1 \leq j \leq r_1 + r_2).$$

Durch geeignete Auswertung (vgl. auch Bemerkung 3.40 (i)) des G-relativen H-invarianten Polynoms $F(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ an den Stellen $x_1 = \cdots = x_n = C_{(l)}^{[j]}$ erhalten wir modulo π^l ein Polynom

$$M_{\bar{F}_\mathcal{P},(l)}^{[j]}(\pi) := M_{\bar{F}_\mathcal{P},j,0} + M_{\bar{F}_\mathcal{P},j,1}\pi + \cdots + M_{\bar{F}_\mathcal{P},j,l-1}\pi^{l-1} \in \mathbb{R}[\pi],$$

so daß für alle Nullstellen $\gamma'^{[j]}_\sigma = \sigma F(\phi_{j,1}(\alpha'),\ldots,\phi_{j,n}(\alpha')) \in \mathbb{C}[[\pi]],\ \sigma \in G//H$ der Resolvente $\iota_\mathcal{P}(R_{(G,H,F)})^{(j)}$ mit l-Approximation $\gamma'^{[j]}_{\sigma,(l)} \equiv \gamma'^{[j]}_\sigma \bmod \pi^l\mathbb{C}[[\pi]]$

$$|g_{\sigma,j,\nu}| \le M_{\bar{F}_\mathcal{P},j,\nu} \ \text{ für } \gamma'^{[j]}_{\sigma,(l)} = \sum_{\nu=0}^{l-1} g_{\sigma,j,\nu}\pi^\nu, \tag{4.68}$$

also auch $|g_{j,\nu}| \le M_{\bar{F}_\mathcal{P},j,\nu}$ für $g_{j,\nu}$ aus (4.66) gilt. Insbesondere erhalten wir aus (4.68) für alle l-Approximationen der Nullstellen der Resolvente $\iota_\mathcal{P}(R_{(G,H,F)})^{(j)} \in \mathbb{C}[[\pi]][X]$

$$\|\gamma'^{[j]}_{\sigma,(l)}\|_\infty \le \|M_{\bar{F}_\mathcal{P},(l)}^{[j]}\|_\infty.$$

Wir können nun davon ausgehen, daß wir für $K = \mathbb{F}_q$ und $K = \mathbb{Q}$ eine Approximation $\gamma'_{(l)} \in \bar{F}_\mathcal{P}[\pi]$ gegeben haben, da ansonsten die exakte Nullstelle $\gamma' \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$ bzw. $\gamma'' \in \mathbb{Z}_p[\rho][[\pi]]$ zu keinem Element in $\mathfrak{o}_F$ korrespondieren kann. Um zu entscheiden, ob es sich bei der Nullstelle $\gamma'_{(l)}$ der Resolvente, um ein Element aus $\mathfrak{o}_F$ handelt, muß folgende $\mathcal{P}$-adische Approximationsaufgabe (bei ausreichend großer Präzision) gelöst werden:

> Zu $\gamma' \in \bar{F}_\mathcal{P}[[\pi]]$ finde $\lambda'_i \in \iota_\mathcal{P}(K[t])$ mit $\gamma' = \sum_{i=1}^m \lambda'_i\,\iota_\mathcal{P}(\omega_i)$ oder entscheide, daß keine λ'_i mit dieser Eigenschaft existieren. (4.69)

Da das Minimalpolynom $h(t,x) \in R[t][x]$ des Funktionenkörpers F absolut irreduzibel ist, ist die Bildmenge $\iota_\mathcal{P}(\mathfrak{o}_F) \subseteq \bar{F}_\mathcal{P}[[\pi]]$ ein freier $\bar{F}_\mathcal{P}[\pi]$-Modul vom Rang m mit Basis $\iota_\mathcal{P}(\omega_1),\ldots,\ \iota_\mathcal{P}(\omega_m)$. Also sind die $\iota_\mathcal{P}(\omega_i)$ auch $\bar{F}_\mathcal{P}[\pi]$-linear unabhängig über $\bar{F}_\mathcal{P}[[\pi]]$. Dies hat zur Folge, daß es in (4.69) entweder genau eine Lösung $(\lambda'_1,\ldots,\lambda'_m) \in \bar{F}_\mathcal{P}[\pi]^m$ gibt oder gar keine Lösung. Gibt es eine Lösung, so ist zu testen, ob $(\lambda'_1(t-t_0),\ldots,\lambda'_m(t-t_0)) \in K[t]^m$ ist.

Wir können den $\omega_i, (1 \le i \le m)$ mittels der Abbildung $\iota_\mathcal{P}$ Elemente in $\bar{F}_\mathcal{P}[[\pi]]$ und somit l-Approximationen $\omega'_{i,(l)} \in \bar{F}_\mathcal{P}[\pi]$ mit $\omega'_{i,(l)} \equiv \iota_\mathcal{P}(\omega_i) \bmod \pi^l\bar{F}_\mathcal{P}[[\pi]]$ zuordnen. Wir sind dann an einer $\bar{F}_\mathcal{P}[\pi]$-Linearkombination zwischen den $\omega'_{i,(l)}$ und $\gamma'_{(l)}$ interessiert. Wären die $\omega'_{i,(l)}$ mit unendlicher Präzision gegeben, so gäbe es genau eine $\bar{F}_\mathcal{P}[\pi]$-Linearkombination oder gar keine. Da wir aber nur mit einer endlichen Präzision arbeiten können, sind in $\bar{F}_\mathcal{P}[\pi]/\pi^l\bar{F}_\mathcal{P}[\pi]$ die Restklassen

$\omega'_{1,(l)} + \pi^l \bar{F}_{\mathcal{P}}[\pi], \ldots, \omega'_{m,(l)} + \pi^l \bar{F}_{\mathcal{P}}[\pi]$ nicht mehr $\bar{F}_{\mathcal{P}}[\pi]$-linear unabhängig und das Polynom $\gamma'_{(l)}$ läßt sich immer als $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination der $\omega'_{i,(l)} + \pi^l \bar{F}_{\mathcal{P}}[\pi]$ schreiben. Ist die Präzision groß genug gewählt, so erwarten wir, daß die „unerwünschten“ Relationen einen hohen Grad haben, während die gesuchte $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination im Vergleich dazu einen kleinen Grad hat. Es gilt also Schranken für die Präzision herzuleiten, mittels derer wir die gesuchte $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination (falls existent) von den anderen $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombinationen in $\bar{F}_{\mathcal{P}}[\pi]/\pi^l \bar{F}_{\mathcal{P}}[\pi]$ unterscheiden können.

4.70. Proposition. *Sei $\gamma'_{(l)} \in \bar{F}_{\mathcal{P}}[\pi]$ für alle $l \in \mathbb{Z}_{>0}$ eine $\mathcal{P}$-adische Nullstelle des Resolventenpolynoms. Dann ist die Abbildung*

$$\begin{aligned} \phi : \bar{F}_{\mathcal{P}}[\pi] \times \cdots \times \bar{F}_{\mathcal{P}}[\pi] &\longrightarrow \bar{F}_{\mathcal{P}}[\pi]/\pi^l \bar{F}_{\mathcal{P}}[\pi] \\ (\lambda'_1, \ldots, \lambda'_{m+1}) &\mapsto \lambda'_1 \omega'_{1,(l)} + \ldots + \lambda'_m \omega'_{m,(l)} + \lambda'_{m+1} \gamma'_{(l)} + \pi^l \bar{F}_{\mathcal{P}}[\pi] \end{aligned} \tag{4.71}$$

ein surjektiver $\bar{F}_{\mathcal{P}}[\pi]$-Modulhomomorphismus. $\operatorname{Kern}\phi$ *ist ein freier $\bar{F}_{\mathcal{P}}[\pi]$-Modul vom Rang $m+1$ und die Vektoren*

$$\begin{aligned} u_{1,(l)} &= (\pi^l, 0, \ldots, 0), \\ u_{2,(l)} &= (-{\omega'}^{-1}_{1,(l)} \omega'_{2,(l)}, 1, 0, \ldots, 0), \\ u_{3,(l)} &= (-{\omega'}^{-1}_{1,(l)} \omega'_{3,(l)}, 0, 1, \ldots, 0), \\ &\vdots \qquad\qquad \vdots \\ u_{m,(l)} &= (-{\omega'}^{-1}_{1,(l)} \omega'_{m,(l)}, 0, \ldots, 1, 0), \\ u_{m+1,(l)} &= (-{\omega'}^{-1}_{1,(l)} \gamma'_{(l)}, 0, \ldots, 0, 1) \end{aligned} \tag{4.72}$$

bilden eine Basis von $\operatorname{Kern}\phi$.

Beweis. Da $\pi \nmid \iota_{\mathcal{P}}(\omega_1)$ gilt auch $\pi \nmid \omega'_{1,(l)} \in \bar{F}_{\mathcal{P}}[\pi]$ für alle $l \in \mathbb{Z}_{>0}$. Damit folgt die Surjektivität. Nach dem ersten Isomorphiesatz ist $\bar{F}_{\mathcal{P}}[\pi]^{m+1} / \operatorname{Kern}\phi \cong \bar{F}_{\mathcal{P}}[\pi]/\pi^l \bar{F}_{\mathcal{P}}[\pi]$ ein $\bar{F}_{\mathcal{P}}[\pi]$-Modul- bzw. $\bar{F}_{\mathcal{P}}$-Vektorraumisomorphismus. Da die rechte Seite dieser Isomorphie Dimension $l < \infty$ über $\bar{F}_{\mathcal{P}}$ hat, gilt dies auch für die linke Seite. Damit folgt $\operatorname{Rang}_{\bar{F}_{\mathcal{P}}[\pi]} \operatorname{Kern}\phi = \operatorname{Rang}_{\bar{F}_{\mathcal{P}}[\pi]} \bar{F}_{\mathcal{P}}[\pi]^{m+1} = m+1$ unter Beachtung der Tatsache, daß $\bar{F}_{\mathcal{P}}[\pi]$ ein Hauptidealring ist. Betrachten wir nun den $\bar{F}_{\mathcal{P}}[\pi]$-Modul $U :=< u_{1,(l)}, \ldots, u_{m+1,(l)} >$, so gilt $U \subseteq \operatorname{Kern}\phi \subseteq \bar{F}_{\mathcal{P}}[\pi]^{m+1}$ und somit $\bar{F}_{\mathcal{P}}[\pi]^{m+1}/\operatorname{Kern}\phi \subseteq \bar{F}_{\mathcal{P}}[\pi]^{m+1}/U$. $\bar{F}_{\mathcal{P}}[\pi]^{m+1}/U$ ist ebenfalls ein l-dimensionaler $\bar{F}_{\mathcal{P}}$-Vektorraum, da die Matrix $\begin{pmatrix} u_{1,(l)} \\ \vdots \\ u_{m+1,(l)} \end{pmatrix}$ bis auf π^l lauter Einsen auf der Diagonalen hat. Wir erhalten $\bar{F}_{\mathcal{P}}[\pi]^{m+1}/\operatorname{Kern}\phi = \bar{F}_{\mathcal{P}}[\pi]^{m+1}/U$, und es folgt $\operatorname{Kern}\phi = U$. □

4.73. Definition und Korollar. $\Lambda_{\gamma'_{(l)},(l)} := \operatorname{Kern}\phi$ *ist ein $\bar{F}_{\mathcal{P}}[\pi]$-Gitter der Dimension $m+1$ im $\bar{F}_{\mathcal{P}}((\pi^{-1}))^{m+1}$ mit Basis $u_{1,(l)}, \ldots, u_{m+1,(l)}$. Das Teilgitter von*

$\Lambda_{\gamma'_{(l)},(l)}$, *welches nur aus den Relationen der* $\omega'_{i,(l)}$, $(1 \le i \le m)$ *besteht* ($\lambda'_{m+1} = 0$ *in* (4.71)*), bezeichnen wir mit* $\Lambda'_{\gamma'_{(l)},(l)}$. *Es gilt* $\Lambda'_{\gamma'_{(l)},(l)} = \{\sum_{i=1}^{m} z_i u_{i,(l)} \mid z_1, \ldots, z_m \in \bar{F}_{\mathcal{P}}[\pi]\}$, *und die Vektoren* $u_{1,(l)}, \ldots, u_{m,(l)}$ *bilden eine Basis von* $\Lambda'_{\gamma'_{(l)},(l)}$.

Wir nehmen nun an, daß $\gamma = \sum_{i=1}^{m} \lambda_i \omega_i \in \mathfrak{o}_F$ ist, und wollen obere Schranken an die Grade der λ_i herleiten. Analog zur Minkowskischen Geometrie der Zahlen betrachten wir im zahm verzweigten Fall dazu zunächst Elemente des Funktionenkörpers F/K als Punkte im m-dimensionalen Raum $E((t^{-1/e}))^m$ mittels Einbettung 4.18

$$\mu : F \longrightarrow E((t^{-\frac{1}{e}}))^m : \sum_{j=0}^{m-1} a_j \delta^j \mapsto \left(\sum_{j=0}^{m-1} a_j (\delta^{(i)})^j \right)_{1 \le i \le m}$$

für $\delta^{(i)}$, $(1 \le i \le m)$ wie in (4.11) bzw. Satz 4.12. Nach Proposition 4.29 können wir damit den freien $K[t]$-Modul $\mathfrak{o}_F$ mit einem Gitter im $E((t^{-\frac{1}{e}}))^m$ identifizieren.

4.74. Bezeichnung. *Seien* $\nu_1, \ldots, \nu_s$ *die Bewertungen, die zu den unendlichen Stellen aus* $\mathbb{P}_\infty(F)$ *korrespondieren. Nach Lorenz [52], §23, Satz 5 existiert eine Fortsetzung der Bewertung* ν_j *für* $1 \le j \le s$ *auf den Zerfällungskörper* $N(f, F)$ *von* f. *Diese wollen wir ebenfalls mit* ν_j *bezeichnen.*

4.75. Definition. Seien $M_j \in \mathbb{Q}$, $(1 \le j \le s)$ untere Schranken der Bewertungen ν_j der Nullstellen der Resolvente $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ in $N(f, F)$, d.h. $\nu_j(\sigma F(\alpha_1, \ldots, \alpha_n)) \ge M_j$ für alle $\sigma \in G//H$. Zu $M_j \in \mathbb{Q}$ definieren wir $A \in \mathbb{Q}$ als

$$A := \begin{cases} \max\limits_{1 \le i \le m} \min\limits_{1 \le j \le s} \left\{ \frac{\nu_j(\omega_i)}{e_j} \right\} - \min\limits_{1 \le j \le s} \left\{ \frac{M_j}{e_j} \right\}, & \omega_1, \ldots, \omega_m \text{ ist reduzierte Ganzheitsbasis} \\ -\frac{1}{e} \min\limits_{1 \le i,j \le m} \left\{ \nu_{t^{-\frac{1}{e}}}(\tilde{\omega}_{i,j}) \right\} - \min\limits_{1 \le j \le s} \left\{ \frac{M_j}{e_j} \right\}, & \text{char}(K) \nmid e. \end{cases} \tag{4.76}$$

wobei $(\tilde{\omega}_{i,j})_{1 \le i,j \le m}$ die zur Matrix $(\mu(\omega_j))_{1 \le j \le m}$ inverse Matrix bezeichne, welche nach Proposition 4.29 existiert.

4.77. Proposition.

(i) Sei $\gamma = \sum_{i=1}^{m} \lambda_i \omega_i$ *eine Nullstelle des Resolventenpolynoms, welche in* $\mathfrak{o}_F$ *liegt. Dann gilt:*

$$\max_{1 \le i \le m} \{\deg(\lambda_i)\} \le A. \tag{4.78}$$

(ii) Ist umgekehrt $(\mu_1, \ldots, \mu_m) \in K[t]^m$ *gegeben mit* $\max_{1\le i\le m}\{\deg(\mu_i)\} < A$, *so gilt*

$$\nu_j(\sum_{i=1}^{m} \mu_i\omega_i) \ge -e_j\, A + W_j, \quad (1 \le j \le s)$$

für $W_j := \min\limits_{1\le i\le m} \{\nu_j(\omega_i)\} \in \mathbb{Q}$. (4.79)

Beweis. (*i*) Wir wollen zuerst annehmen, daß die Ganzheitsbasis $\omega_1, \ldots, \omega_m$ von $\mathfrak{o}_F$ reduziert sei. Dann gilt nach Definition 4.17

$$\begin{array}{rcl} \|\gamma\|_{T_2} = \|\sum\limits_{i=1}^{m} \lambda_i\omega_i\|_{T_2} & \underset{\text{Basis}}{\overset{\text{red.}}{=}} & \max\limits_{1\le i\le m} \{\, \|\lambda_i\omega_i\|_{T_2}\,\} \\ & \ge & \max\limits_{1\le i\le m} \{\, |\lambda_i|_\infty\,\} \min\limits_{1\le i\le m} \{\, \|\omega_i\|_{T_2}\,\}. \end{array} \tag{4.80}$$

Aufgrund der Voraussetzung, daß γ Nullstelle von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ ist, erhalten wir $\nu_j(\gamma) \ge M_j$ für $1 \le j \le m$, und es folgt aus (4.80) mittels der Definition der $\|\cdot\|_{T_2}$-Norm (vgl. 4.15)

$$\max_{1\le i\le m} \left\{c^{-\nu_\infty(\lambda_i)}\right\} \;\le\; c^{-\min\limits_{1\le j\le s}\left\{\frac{1}{e_j}\nu_j(\gamma)\right\}} \max_{1\le i\le m} \left\{ c^{\min\limits_{1\le j\le s}\left\{\frac{1}{e_j}\nu_j(\omega_i)\right\}} \right\}$$

Beidseitiges Logarithmieren zur Basis c ergibt

$$\begin{array}{rcl} \max\limits_{1\le i\le m} \{\deg(\lambda_i)\} & \le & -\min\limits_{1\le j\le s} \left\{\frac{\nu_j(\gamma)}{e_j}\right\} + \max\limits_{1\le i\le m} \min\limits_{1\le j\le s} \left\{\frac{\nu_j(\omega_i)}{e_j}\right\} \\ & \le & -\min\limits_{1\le j\le s} \left\{\frac{M_j}{e_j}\right\} + \max\limits_{1\le i\le m} \min\limits_{1\le j\le s} \left\{\frac{\nu_j(\omega_i)}{e_j}\right\} = A. \end{array}$$

Im zahm verzweigten Fall erhalten wir aus $\gamma = \sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}_F$, daß $\mu(\gamma) = \sum_{i=1}^m \lambda_i\mu(\omega_i) \in E((t^{-\frac{1}{e}}))^m$ ist. Wegen Proposition 4.29 ist die Matrix $(\mu(\omega_i))_{1\le i\le m} = (\omega_j^{(i)})_{1\le i,j\le m}$ invertierbar, und es gilt:

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} = \begin{pmatrix} \tilde\omega_{1,1} & \tilde\omega_{1,2} & \ldots & \tilde\omega_{1,m} \\ \vdots & & & \vdots \\ \tilde\omega_{m,1} & \tilde\omega_{m,2} & \ldots & \tilde\omega_{m,m} \end{pmatrix} \begin{pmatrix} \gamma^{(1)} \\ \vdots \\ \gamma^{(m)} \end{pmatrix}$$

Es folgt

$$|\lambda_i|_{t^{-\frac{1}{e}}} \;=\; |\sum_{j=1}^{m} \tilde\omega_{i,j}\gamma^{(j)}|_{t^{-\frac{1}{e}}} \;\le\; \max_{1\le j\le m} |\tilde\omega_{i,j}|_{t^{-\frac{1}{e}}} |\gamma^{(j)}|_{t^{-\frac{1}{e}}}.$$

Unter Beachtung von $\nu_j(t^{-1}) = e_j$ und somit $\nu_{t^{-\frac{1}{e}}}(t^{-1}) = \frac{e}{e_j}\nu_j(t^{-1})$ erhalten wir für die zugehörigen Bewertungen

$$\begin{array}{rcl} -\nu_{t^{-\frac{1}{e}}}(\lambda_i) & \le & \max\limits_{1\le j\le m} \{-\nu_{t^{-\frac{1}{e}}}(\tilde\omega_{i,j}) - \frac{e}{e_j}\nu_j(\gamma)\} \\ \Longrightarrow \quad -\nu_{t^{-\frac{1}{e}}}(\lambda_i) & \le & \max\limits_{1\le j\le m} \{-\nu_{t^{-\frac{1}{e}}}(\tilde\omega_{i,j})\} + \max\limits_{1\le j\le m} \{-\frac{e}{e_j}\nu_j(\gamma)\} \end{array}$$

$$\begin{aligned}
\iff \qquad e\,\deg(\lambda_i) &\leq \max_{1\leq j\leq m}\{-\nu_{t^{-\frac{1}{e}}}(\tilde{\omega}_{i,j})\} + \max_{1\leq j\leq m}\{-\tfrac{e}{e_j}\nu_j(\gamma)\} \\
\implies \max_{1\leq i\leq m}\{\deg(\lambda_i)\} &\leq -\tfrac{1}{e}\min_{1\leq i,j\leq m}\{\nu_{t^{-\frac{1}{e}}}(\tilde{\omega}_{i,j})\} - \min_{1\leq j\leq s}\{\tfrac{1}{e_j}\nu_j(\gamma)\} \\
&\leq -\tfrac{1}{e}\min_{1\leq i,j\leq m}\{\nu_{t^{-\frac{1}{e}}}(\tilde{\omega}_{i,j})\} - \min_{1\leq j\leq s}\{\tfrac{1}{e_j}M_j\}
\end{aligned}$$

und die erste Behauptung folgt.

(*ii*) Für $(\mu_1,\ldots,\mu_m)\in K[t]^m$ mit $\max_{1\leq i\leq m}\{\deg(\mu_i)\} < A$ gilt

$$\begin{aligned}
\nu_j(\sum_{i=1}^{m}\mu_i\omega_i) \geq \min_{1\leq i\leq m}\{\nu_j(\mu_i\omega_i)\} &\geq e_j\min_{1\leq i\leq m}\{\nu_\infty(\mu_i)\} + \min_{1\leq i\leq m}\{\nu_j(\omega_i)\} \\
&\geq -e_j\max_{1\leq i\leq m}\{\deg(\mu_i)\} + \min_{1\leq i\leq m}\{\nu_j(\omega_i)\} \\
&> -e_j\,A + W_j.
\end{aligned}$$

□

4.81. Bemerkung. Da bei der Einbettung $\iota_{\mathcal{P}} : \mathfrak{o}_F \longrightarrow \bar{F}_{\mathcal{P}}[[\pi]]$ der Ring $K[t]$ auf $K[\pi]$ und das Primelement t auf $\pi + t_0$ abgebildet wird, gilt die Abschätzung 4.78 (*i*) auch für den Grad von $\max_{1\leq i\leq m}\{\deg(\iota_{\mathcal{P}}(\lambda_i))\}$.

Für eine Approximation $\gamma'_{(l)}$ einer Nullstelle γ' der Resolvente mit $\gamma'_{(l)}\in\bar{F}_{\mathcal{P}}[\pi]$ gilt $({\omega'}^{-1}_{1,(l)}\gamma'_{(l)})\cdot\omega'_{1,(l)} \equiv \gamma'_{(l)} \bmod \pi^l$. Das Polynom $\gamma'_{(l)}$ läßt sich also bereits $\bmod \pi^l$ als $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination der $\omega'_{i,(l)}$, $(1\leq i\leq m)$ schreiben, aber diese $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination genügt im allgemeinen nicht der Schranke (4.78). Auf jeden Fall gilt für $\gamma = \sum_{i=1}^{m}\lambda_i\omega_i$ aber $\max_{1\leq i\leq m}\{\deg(\iota_{\mathcal{P}}(\lambda_i))\}\leq A$ und das Ziel ist, alle Vektoren in $\operatorname{Kern}\phi$ mit maximalem Koordinatengrad $\leq A$ zu finden, um danach testen zu können, ob es sich bei einer $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination nach Substitution von $\pi\mapsto t-t_0$ um eine $K[t]$-Linearkombination handelt. Gleichzeitig wollen wir allerdings die Präzision so einstellen, daß der Grad der Vektoren aus $\operatorname{Kern}\phi$, die nicht zu der eindeutig bestimmten $\bar{F}_{\mathcal{P}}[\pi]$-Linearkombination von γ korrespondieren, deutlich größer als A ist. Dazu benötigen wir noch eine Proposition, die garantiert, daß es in einer Konstantenkörpererweiterung von F/K eine Stelle $\mathcal{P}'$ vom Grad eins gibt, so daß die $\mathcal{P}$-adische Entwicklung der ω_i mit der $\mathcal{P}'$-adischen Entwicklung der ω_i übereinstimmt.

4.82. Proposition. *Sei F/K ein algebraischer Funktionenkörper und $\mathcal{P}\in\mathbb{P}(F)$ eine Stelle mit Bewertungsring $\mathcal{O}_{\mathcal{P}}$ und Restklassenkörper $\bar{F}_{\mathcal{P}}$. Dann gilt in der algebraischen Konstantenkörpererweiterung $F' := F\bar{F}_{\mathcal{P}}$ über $\bar{F}_{\mathcal{P}}$ von F/K:*

(i) Es existiert eine über $\mathcal{P}$ unverzweigte Stelle $\mathcal{P}'\in\mathbb{P}(F')$ vom Grad eins, so daß der Restklassenkörper $\bar{F}_{\mathcal{P}'}$ bezüglich $\mathcal{P}'$ isomorph zu $\bar{F}_{\mathcal{P}}$ ist.

(ii) Für eine Variable π sei $\iota_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}} \longrightarrow \bar{F}_{\mathcal{P}}[[\pi]]$ ein bewertungserhaltender Einbettungshomomorphismus, der jedem Element von $\mathcal{O}_{\mathcal{P}}$ seine $\mathcal{P}$-adische Entwicklung zuordnet und $\mathcal{P}'|\mathcal{P}, \mathcal{P}' \in \mathbb{P}(F')$ wie in (i). Dann existiert eine bewertungserhaltende Fortsetzung von $\iota_{\mathcal{P}}$ auf den Bewertungsring $\mathcal{O}_{\mathcal{P}'}$.

Beweis. (*i*) Für den Funktionenkörper F mit exaktem Konstantenkörper $\tilde{K}$ ist nach Stichtenoth [80], III.6.3 (a) die Erweiterung F'/F unverzweigt. Nach Stichtenoth [80], III.6.3 (g) existiert also eine über $\mathcal{P}$ unverzweigte Stelle $\mathcal{P}'$, deren Restklassenkörper $\bar{F}'_{\mathcal{P}'}$ gerade isomorph zu $\bar{F}_{\mathcal{P}}$ ist.

(*ii*) Zu $\iota_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}} \longrightarrow \bar{F}_{\mathcal{P}}[[\pi]]$ und $\iota_{\mathcal{P}'} : \mathcal{O}_{\mathcal{P}'} \longrightarrow \bar{F}_{\mathcal{P}'}[[\pi']]$ gibt es genau einen Homomorphismus $\tau : \bar{F}_{\mathcal{P}}[[\pi]] \longrightarrow \bar{F}_{\mathcal{P}'}[[\pi']]$, so daß das Diagramm

$$\begin{array}{ccc} \mathcal{O}_{\mathcal{P}} & \xrightarrow{\iota_{\mathcal{P}}} & \bar{F}_{\mathcal{P}}[[\pi]] \\ \downarrow & & \downarrow \tau \\ \mathcal{O}_{\mathcal{P}'} & \xrightarrow{\iota_{\mathcal{P}'}} & \bar{F}_{\mathcal{P}'}[[\pi']] \end{array}$$

kommutiert. Dies gilt, weil $\mathcal{O}_{\mathcal{P}}$ und $\mathcal{O}_{\mathcal{P}'}$ durch $\iota_{\mathcal{P}}$ und $\iota_{\mathcal{P}'}$ in ihre Vervollständigungen eingebettet werden und weil $\mathcal{P}'$ über $\mathcal{P}$ liegt. Darüber hinaus ist τ ein bewertungserhaltender Isomorphismus, da $\mathcal{P}'$ über $\mathcal{P}$ unverzweigt ist und der Relativgrad wegen isomorpher Restklassenkörper eins ist. Die gesuchte Fortsetzung ist dann durch $\tau^{-1} \circ \iota_{\mathcal{P}'}$ gegeben. □

4.83. Bezeichnung. *Die Menge der Stellen von $F'/\bar{F}_{\mathcal{P}}$, $F' := F\bar{F}_{\mathcal{P}}$ über der unendlichen Stelle $\mathfrak{p}'_\infty \in \mathbb{P}(\bar{F}_{\mathcal{P}}(t))$ mit Bewertung ν'_∞ bezeichnen wir mit $\mathbb{P}_\infty(F') := \{\mathcal{P}'_1, \ldots, \mathcal{P}'_{s'}\}$, die zugehörigen Bewertungen mit $\nu'_1, \ldots, \nu'_{s'}$ und die Verzweigungsindizes mit $e'_i := e(\mathcal{P}'_i \,|\, \mathfrak{p}'_\infty)$.*

4.84. Proposition. *Sei $\Lambda'_{\gamma'_{(l)},(l)} = \{ \sum_{i=1}^m z_i u_{i,(l)} \,|\, z_1, .., z_m \in \bar{F}_{\mathcal{P}}[\pi]\} \subseteq \bar{F}_{\mathcal{P}}[\pi]^{m+1}$ das Teilgitter von $\Lambda_{\gamma'_{(l)},(l)}$, welches aus den Relationen zwischen den $\omega'_{i,(l)}$, $(1 \leq i \leq m)$ besteht. Dann gilt: Es existiert $B : \mathbb{Z}_{>0} \to \mathbb{R}$ mit*

(i) $\lim\limits_{l\to\infty} B(l) = \infty$,

(ii) $\max\limits_{1\leq j\leq m}\{\deg(\mu'_j)\} \geq B(l)$ *für alle* $(\mu'_1, \ldots, \mu'_m, 0) \in \Lambda'_{\gamma'_{(l)},(l)} \setminus \{0\}$,

(iii) $B(l) > 3A$ *für* $l > s' \left(3A \min\limits_{1\leq i\leq s}\{e_i\} - \min\limits_{1\leq i\leq s}\{W_i\}\right)$.

Beweis. Für beliebiges $(\mu'_1, \ldots, \mu'_m, 0) \in \Lambda'_{\gamma'_{(l)},(l)} \setminus \{0\}$ gilt $\phi((\mu'_1, \ldots, \mu'_m, 0)) \equiv 0 \bmod \pi^l \bar{F}_{\mathcal{P}}[\pi]$. Wir substituieren $\pi \mapsto t - t_0$ und setzen $\mu_i := \mu'_i(t - t_0) \in \bar{F}_{\mathcal{P}}[t]$

für $1 \leq i \leq m$. In der Konstantenkörpererweiterung $F' := F\bar{F}_{\mathcal{P}}$ über $\bar{F}_{\mathcal{P}}$ gilt $a := \sum_{i=1}^{m} \mu_i \omega_i \in \mathfrak{o}_{F'} \backslash \{0\}$ und mittels der Produktformel für $F'/\bar{F}_{\mathcal{P}}$ folgt

$$\sum_{\mathcal{P}' \in \mathbb{P}(F')} \nu_{\mathcal{P}'}(a) \deg(\mathcal{P}') = 0.$$

Nach Proposition 4.82 gibt es eine Stelle $\mathcal{P}'|\mathcal{P}$, $\mathcal{P}' \in \mathbb{P}(F')$ vom Grad eins, so daß die $\mathcal{P}$-adische Entwicklung der ω_i für $1 \leq i \leq m$ mit der $\mathcal{P}'$-adischen Entwicklung der ω_i übereinstimmt. Für diese Stelle erhalten wir dann $\nu_{\mathcal{P}'}(a) \geq l$ und für alle anderen endlichen Stellen $\mathcal{P}' \in \mathbb{P}(F') \backslash \mathbb{P}_\infty(F')$ gilt $\nu_{\mathcal{P}'}(a) \geq 0$, da die ω_i für $1 \leq i \leq m$ ganzalgebraisch sind. Für die Summe der unendlichen Stellen mit zugehörigen Bewertungen $\nu'_1, \ldots, \nu'_{s'}$ muß deshalb $\sum_{i=1}^{s'} \deg(\mathcal{P}'_i)\nu'_i(a) \leq -l$ gelten. Damit folgt

$$\begin{aligned}
-l \geq \sum_{i=1}^{s'} \nu'_i(\sum_{j=1}^{m} \mu_j \omega_j) &\geq \sum_{i=1}^{s'} \min_{1 \leq j \leq m} \{\nu'_i(\mu_j \omega_j)\} \\
&\geq s' \min_{1 \leq i \leq s'} \min_{1 \leq j \leq m} \{\nu'_i(\mu_j) + \nu'_i(\omega_j)\} \\
&\geq s' \min_{1 \leq i \leq s'} \min_{1 \leq j \leq m} \{\nu'_i(\mu_j)\} + s' \min_{1 \leq i \leq s} \min_{1 \leq j \leq m} \{\nu_i(\omega_j)\} \qquad (4.85) \\
&\geq s' \min_{1 \leq i \leq s'} \{e'_i\} \min_{1 \leq j \leq m} \{\nu'_\infty(\mu_j)\} + s' \min_{1 \leq i \leq s} \{W_i\} \\
&= -s' \min_{1 \leq i \leq s} \{e_i\} \max_{1 \leq j \leq m} \{\deg(\mu_j)\} + s' \min_{1 \leq i \leq s} \{W_i\}
\end{aligned}$$

Die letzte Gleichheit gilt, da die algebraischen Konstantenkörpererweiterungen F'/F und $\bar{F}_{\mathcal{P}}(t)/K(t)$ unverzweigt sind und somit für $1 \leq i \leq s'$ aus $e(\mathcal{P}'_i, \mathfrak{p}_\infty) = e(\mathcal{P}'_i, \mathcal{P}_j)\, e(\mathcal{P}_j, \mathfrak{p}_\infty) = e(\mathcal{P}'_i, \mathfrak{p}'_\infty)\, e(\mathfrak{p}'_\infty, \mathfrak{p}_\infty)$ für $j \in \{1, \ldots, s\}$ folgt, daß $e'_i = e(P'_i \,|\, \mathfrak{p}'_\infty) = e(P_j \,|\, \mathfrak{p}_\infty) = e_j$ ist. Wir erhalten

$$\max_{1 \leq j \leq m} \{\deg(\mu'_j)\} \geq \max_{1 \leq i \leq s} \{e_i^{-1}\} \left(\frac{l}{s'} + \min_{1 \leq i \leq s} \{W_i\} \right) =: B(l), \qquad (4.86)$$

da der Grad von μ_j bezüglich t dergleiche ist, wie von μ'_j bezüglich π, $(1 \leq j \leq m)$. Es ist offensichtlich, daß $\lim_{l \to \infty} B(l) = \infty$ gilt und (iii) folgt sofort durch umformen. □

4.87. Proposition. *Sei $\gamma = \sum_{i=1}^{m} \lambda_i \omega_i$ eine Nullstelle des Resolventenpolynoms, welche in $\mathfrak{o}_F$ liegt und $v := (-\lambda'_1, \ldots, -\lambda'_m, 1) \in \bar{F}_{\mathcal{P}}[\pi]$ mit $\lambda'_i := \iota_{\mathcal{P}}(\lambda_i)$ für $1 \leq i \leq m$. Dann sind die Vektoren av, für alle $a \in \bar{F}_{\mathcal{P}}^{\times}$, die kürzesten Vektoren des Gitters $\Lambda_{\gamma'_{(l)}, (l)}$ für $l > s'(3A \min_{1 \leq i \leq s}\{e_i\} - \min_{1 \leq i \leq s}\{W_i\})$.*

Beweis. Es gilt $\phi(v) = -\lambda'_1 \omega'_{1,(l)} - \cdots - \lambda'_m \omega'_{m,(l)} + \gamma'_{(l)} = 0 + \pi^l \bar{F}_{\mathcal{P}}[\pi]$. Deshalb ist v ein Element von $\Lambda_{\gamma'_{(l)}, (l)}$. Für den maximalen Grad der Koordinaten von

v ergibt sich aus Proposition 4.78 (i), daß $\max_{1\le i\le m}\{\deg(\lambda'_i)\} \le A$ gilt. Nach Definition ist $\Lambda_{\gamma'_{(l)},(l)} = \bar{F}_{\mathcal{P}}[\pi]\, u_{m+1,(l)} + \Lambda'_{\gamma'_{(l)},(l)}$. Da $u_{m+1,(l)} - v \in \Lambda'_{\gamma'_{(l)},(l)}$ ist, gilt auch $\Lambda_{\gamma'_{(l)},(l)} = \bar{F}_{\mathcal{P}}[\pi]\, v + \Lambda'_{\gamma'_{(l)},(l)}$. Sei nun $x_{(l)} := (\mu'_1, \ldots, \mu'_{m+1}) \in \Lambda'_{\gamma'_{(l)},(l)}$ und $z' \in \bar{F}_{\mathcal{P}}[\pi]$ mit

$$\max_{1\le i\le m+1} \{\, \deg(z'\,\lambda'_i + \mu'_i)\,\} \le\ A, \tag{4.88}$$

wobei $\lambda'_{m+1} := 1$ sei. Es genügt zu beweisen, daß der maximale Grad der Koordinaten von $z'v + x_{(l)}$ nicht kleiner als der maximale Grad der Koordinaten von v sein kann. Ist $x_{(l)} \neq 0$, so folgt

$$\begin{aligned} \max_{1\le i\le m+1}\{\deg(z'\lambda'_i + \mu'_i)\} &\ge |\max_{1\le i\le m+1}\{\deg(\mu'_i)\} - \max_{1\le i\le m+1}\{\deg(z'\lambda'_i)\}| \\ &\ge B(l) - 2A, \end{aligned}$$

nach 4.84 (ii), und da man mittels (4.88) die Ungleichung $\deg(z') \le A$ erhält (v hat eine Eins an letzter Koordinate und $x_{(l)}$ eine Null). Nach Proposition 4.84 ist aber $A < B(l) - 2A$ im Widerspruch zu (4.88). Somit folgt $x_{(l)} = 0$ und $\max_{1\le i\le m+1}\{\deg(z'\,\lambda'_i)\} \le A$. Dies ergibt, daß av für jede Einheit $a \in \bar{F}_{\mathcal{P}}^{\times}$ kürzester Vektor von $\Lambda_{\gamma'_{(l)},(l)}$ ist. □

4.89. Bemerkung. Für $l \in \mathbb{Z}_{>0}$ wie in Proposition 4.87 sind verschiedene Nullstellen $\gamma \in \mathfrak{o}_F$ der Resolvente wegen Proposition 4.87 bereits modulo $\mathcal{P}^l$ verschieden, d.h.

$$\tilde{\gamma}, \gamma \in \mathfrak{o}_F : \tilde{\gamma} = \gamma \Longleftrightarrow \tilde{\gamma} \equiv \gamma \bmod \mathcal{P}^l.$$

Um zu zeigen, daß aus $\tilde{\gamma} \equiv \gamma \bmod \mathcal{P}^l$ folgt, daß $\tilde{\gamma} = \gamma$ ist, kann die analoge Schlußweise wie in Bemerkung 3.31 angewendet werden.

4.90. Proposition. *Unter den Voraussetzungen von Proposition 4.87 sind av für alle $a \in \bar{F}_{\mathcal{P}}^{\times}$ die einzigen ersten reduzierten Basiselemente des Gitters $\Lambda_{\gamma'_{(l)},(l)}$.*

Beweis. Das kürzeste Element des Gitters $\Lambda_{\gamma'_{(l)},(l)}$ stimmt nach Satz 4.24 mit dem ersten reduzierten Basiselement überein. □

Nun können wir den zentralen Satz des Verfahrens von Stauduhar für relative algebraische Funktionenkörper für den Fall formulieren, bei dem wir die Nullstellenapproximationen von $\iota_{\mathcal{P}}(f)$ in einem Laurentreihenring berechnen können, dessen Koeffizientenbereich exakt gegeben ist.

4.91. Satz. *Seien $M_j \in \mathbb{Q}$ untere Schranken der Bewertungen ν_j, $(1 \le j \le s)$ der Nullstellen von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ in $N(f,F)$ wie in Definition 4.75 und $l \in \mathbb{Z}_{>0}$ mit*

$$l > \max\left\{ -[\,G\!:\!H\,] \sum_{j=1}^{s} \deg(\mathcal{P}_j) M_j,\ s'\left(3A \min_{1\le j\le s}\{e_j\} - \min_{1\le j\le s}\{W_j\}\right)\right\}.$$

Ist $\gamma'_\sigma \in N(\bar{f}, \bar{F}_\mathcal{P})[[\pi]]$ *eine Nullstelle von* $\iota_\mathcal{P}(R_{(G,H,F)})(X) \in \iota_\mathcal{P}(\mathfrak{o}_F)[X]$ *mit*

(i) $\gamma'_{\sigma,(l)} \in \bar{F}_\mathcal{P}[\pi]$,

(ii) $\gamma'_{\sigma,(l)} \not\equiv \gamma'_{\tilde{\sigma},(l)} \bmod \pi^l N(\bar{f}, \bar{F}_\mathcal{P})[\pi]$ *für alle* $\tilde{\sigma} \in G//H$ *mit* $\tilde{\sigma} \neq \sigma$, *dann folgt:*

Sei $v' := (-\lambda'_1, \ldots, -\lambda'_m, \lambda'_{m+1})$ *erstes reduziertes Element des Gitters* $\Lambda_{\gamma'_{\sigma,(l)},(l)}$ *und* $\lambda_i := {\lambda'}_{m+1}^{-1}\lambda'_i(t - t_0)$ *für* $1 \leq i \leq m$. *Sind die Bedingungen*

$$(\star)\ \ \lambda'_{m+1} \in \bar{F}_\mathcal{P}^\times, \quad \lambda_i \in K[t],\ (1 \leq i \leq m), \quad \nu_j(\sum_{i=1}^m \lambda_i\omega_i) \geq M_j,\ (1 \leq j \leq s)$$

erfüllt, so gilt $\gamma_\sigma = \sum_{i=1}^m \lambda_i\omega_i$, $\gamma_\sigma \in \mathfrak{o}_F$ *und* γ_σ *ist eine einfache Nullstelle von* $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$.
Sei umgekehrt $\gamma_\sigma = \sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}_F$ *eine einfache Nullstelle von* $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$, $\lambda'_i := \iota_\mathcal{P}(\lambda_i) \in \bar{F}_\mathcal{P}[\pi]$ *für* $1 \leq i \leq m$ *und* $\lambda'_{m+1} := 1$. *Dann gelten die Bedingungen* $(\star)$ *und* $v := (-\lambda'_1, \ldots, -\lambda'_m, \lambda'_{m+1})$ *ist erstes reduziertes Element des Gitters* $\Lambda_{\gamma'_{\sigma,(l)},(l)}$.

Beweis. Sei v' erstes reduziertes Element des Gitters $\Lambda_{\gamma'_{\sigma,(l)},(l)}$ mit $\lambda'_{m+1} \in \bar{F}_\mathcal{P}^\times$. Dann ist $v := (-{\lambda'}_{m+1}^{-1}\lambda'_1, \ldots, -{\lambda'}_{m+1}^{-1}\lambda'_m, 1)$ ebenfalls erstes reduziertes Element von $\Lambda_{\gamma'_{\sigma,(l)},(l)}$, und nach Voraussetzung existieren $\lambda_i \in K[t]$ mit $\iota_\mathcal{P}(\lambda_i) = \lambda'_i$, $(1 \leq i \leq m)$. Aufgrund der Definition des Gitters gilt $\iota_\mathcal{P}(\sum_{i=0}^m \lambda_i\omega_i) \equiv \gamma'_{\sigma,(l)} \bmod \pi^l\bar{F}_\mathcal{P}[[\pi]]$, und es folgt

$$\begin{aligned} \iota_\mathcal{P}(R_{(G,H,F)})(\iota_\mathcal{P}(\sum_{i=0}^m \lambda_i\omega_i)) &\equiv \iota_\mathcal{P}(R_{(G,H,F)})(\gamma'_{\sigma,(l)}) \bmod \pi^l N(\bar{f}, \bar{F}_\mathcal{P})[[\pi]] \\ &\equiv \iota_\mathcal{P}(R_{(G,H,F)})(\gamma'_\sigma) \bmod \pi^l N(\bar{f}, \bar{F}_\mathcal{P})[[\pi]] \\ &\equiv 0 \bmod \pi^l N(\bar{f}, \bar{F}_\mathcal{P})[[\pi]] \end{aligned} \tag{4.92}$$

Da $\iota_\mathcal{P}$ ein bewertungserhaltender Homomorphismus ist, gilt $\nu_\mathcal{P}(a) = \nu_\pi(\iota_\mathcal{P}(a))$ für alle $a \in N(f, F)$. Aus $\iota_\mathcal{P}(R_{(G,H,F)})(\iota_\mathcal{P}(\sum_{i=0}^m \lambda_i\omega_i)) = \iota_\mathcal{P}(R_{(G,H,F)}(\sum_{i=0}^m \lambda_i\omega_i))$ erhalten wir dann

$$R_{(G,H,F)}(\sum_{i=1}^m \lambda_i\omega_i) \equiv 0 \bmod \mathcal{P}^l. \tag{4.93}$$

Da $\nu_j(\sum_{i=1}^m \lambda_i\omega_i) \geq M_j$ und $\nu_j(\sigma F(\alpha_1, \ldots, \alpha_n)) \geq M_j$ für Nullstellen $\alpha_i \in N(f, F)$ von f ist, folgt

$$\nu_j(R_{(G,H,F)}(\sum_{i=1}^m \lambda_i\omega_i)) \ = \ \nu_j\left(\prod_{\sigma\in G//H}(\sum_{i=1}^m \lambda_i\omega_i - \sigma F(\alpha_1, \ldots, \alpha_n))\right)$$

$$\begin{aligned} &= \sum_{\sigma\in G//H} \nu_j\left(\sum_{i=1}^{m}\lambda_i\omega_i - \sigma F(\alpha_1,\ldots,\alpha_n)\right) \\ &\geq \sum_{\sigma\in G//H} M_j \\ &\geq [\,G\!:\!H\,]\,M_j, \quad (1\leq j\leq s) \end{aligned} \tag{4.94}$$

und somit

$$\sum_{j=1}^{s}\deg(\boldsymbol{\mathcal{P}}_j)\,\nu_j(R_{(G,H,F)}(\sum_{i=1}^{m}\lambda_i\omega_i)) > -l. \tag{4.95}$$

Für die fest gewählte Stelle $\boldsymbol{\mathcal{P}}$ des Funktionenkörpers F gilt nach (4.93), daß $\nu_{\boldsymbol{\mathcal{P}}}(R_{(G,H,F)}(\sum_{i=1}^{m}\lambda_i\omega_i)) \geq l$ ist, und für alle anderen endlichen Stellen $\tilde{\boldsymbol{\mathcal{P}}} \in \mathbb{P}(F)\backslash\mathbb{P}_\infty(F)$ haben wir $\nu_{\tilde{\boldsymbol{\mathcal{P}}}}(R_{(G,H,F)}(\sum_{i=1}^{m}\lambda_i\omega_i)) \geq 0$, da $R_{(G,H,F)} \in \mathfrak{o}_F[X]$ und die ω_i ganzalgebraisch sind. Für die Summe der unendlichen Stellen erhalten wir dann mittels der Produktformel für Funktionenkörper $\sum_{j=1}^{s}\deg(\boldsymbol{\mathcal{P}}_j)\,\nu_j(R_{(G,H,F)}(\sum_{i=1}^{m}\lambda_i\omega_i)) \leq -l$. Dies steht im Widerspruch zu (4.95), und nach der Produktformel muß deshalb $R_{(G,H,F)}(\sum_{i=1}^{m}\lambda_i\omega_i) = 0$ folgen. Mittels Annahme (ii) erhalten wir $\gamma_\sigma = \sum_{i=1}^{m}\lambda_i\omega_i \in \mathfrak{o}_F$ und daß γ_σ eine einfache Wurzel von $R_{(G,H,F)}$ ist. Die Rückrichtung folgt aus Proposition 4.90. □

4.96. Bemerkung. Für die Bestimmung der Schranken $M_j \in \mathbb{Q}$ ist eine Berechnung des Zerfällungskörpers $N(f,F)$ nicht notwendig, wie in Satz 4.112 gezeigt wird.

Satz 4.91 liefert den Nullstellenbeweis des rekonstruierten Elements, wenn die Koeffizienten von $N(\bar{f},\bar{F}_{\boldsymbol{\mathcal{P}}})[[\pi]]$ exakt gegeben sind. Damit ist er in der Praxis auf globale Funktionenkörper anwendbar. Ist $N(\bar{f},\bar{F}_{\boldsymbol{\mathcal{P}}})$ ein algebraischer Zahlkörper, so sind Berechnungen in diesem Körper für unsere Anwendungen impraktikabel, weshalb wir mit (p-adischen) Koeffizientenapproximationen arbeiten. In diesem Fall folgt der Nullstellenbeweis des rekonstruierten Elements aus dem folgenden Satz.

4.97. Satz. *Seien $M_j \in \mathbb{Q}$ untere Schranken der Bewertungen ν_j, $(1\leq j\leq s)$ der Nullstellen von $R_{(G,H,F)}(X) \in Cl(\mathbb{Z}[t],F)[X]$ in $N(f,F)$ wie in Definition 4.75 und $l\in\mathbb{Z}_{>0}$ mit*

$$l > \max\left\{-[\,G\!:\!H\,]\sum_{j=1}^{s}\deg(\boldsymbol{\mathcal{P}}_j)M_j,\ s'\,(3A\min_{1\leq j\leq s}\{e_j\} - \min_{1\leq j\leq s}\{W_j\})\right\}.$$

Für $[\,\bar{F}_{\boldsymbol{\mathcal{P}}}:\mathbb{Q}\,] = m$ seien $M^{[j]}_{\bar{F}_{\boldsymbol{\mathcal{P}}},(l)}(\pi) \in \mathbb{R}[\pi]$, $(1\leq j\leq m)$ Polynome vom Grad $l-1$, so daß für alle Nullstellen $\gamma'^{[j]}_\sigma \in \mathbb{C}[[\pi]]$ von $\iota_{\boldsymbol{\mathcal{P}}}(R_{(G,H,F)})^{(j)}(X) \in \mathbb{C}[[\pi]][X]$

die Ungleichung $\|\gamma'^{[j]}_{\sigma}\|_{\infty,(l)} \leq \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_{\infty}$ *gilt. Sei* $k \in \mathbb{Z}_{>0}$ *mit*

$$p^k > \max\left\{ \prod_{j=1}^{m} (2\|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_{\infty})^{[G:H]} \cdot \binom{[G:H]+(l-1)-1}{l-1} \cdot |\mathrm{disc}(\bar{h}_1)|^{2(l-1)+[G:H]-1}, \right.$$
$$\left. 2^{\frac{m^2}{2}} \left(\left(|\mathrm{disc}(\bar{h}_1)|^{2(l-1)}(A_{\bar{F}_{\mathcal{P}}}-1)+1\right)^2 + |\mathrm{disc}(\bar{h}_1)|^{2(l-1)}(A_{\bar{F}_{\mathcal{P}}}-1)+1 \right)^m \prod_{j=1}^{m} W_{\bar{F}_{\mathcal{P}},j} \right\},$$

wobei $\bar{h}_1(x) \in \mathbb{Z}[x]$ *das Minimalpolynom von* $\bar{F}_{\mathcal{P}}/\mathbb{Q}$ *sei mit* $\bar{h}_1(\bar{\delta}_1) = 0$ *und* $A_{\bar{F}_{\mathcal{P}}} := \max_{0\leq\nu\leq l-1}\{A_{\bar{F}_{\mathcal{P}},\nu}\}$ *mit* $A_{\bar{F}_{\mathcal{P}},\nu}$ *aus* (4.66). *Ist* $\gamma''_{\sigma} \in \mathbb{Z}_p[\rho][[\pi]]$ *eine Nullstelle von* $(\psi \circ \iota_{\mathcal{P}})(R_{(G,H,F)})(X) \in \mathbb{Z}_p[[\pi]][X]$ *mit den folgenden Eigenschaften:*

(i) Seien $g^*_{\sigma,(k),\nu} \in \mathbb{Z}[\rho]$ *mit* $\gamma''_{\sigma,(k,l)} = \sum_{\nu=0}^{l-1} g^*_{\sigma,(k),\nu}\pi^{\nu}$, *so gilt für alle* $g^*_{\sigma,(k),\nu}$*:*

(1) $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}} g^*_{\sigma,(k),\nu} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$

(2) Das Gitter $\Lambda_{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}} g^*_{\sigma,(k,1),\nu},(k)}$ *besitzt ein LLL-reduziertes erstes Element der Gestalt* $v_{\nu} := (-\lambda_{1,\nu},\ldots,-\lambda_{m,\nu},1)$ *mit*

$$\left| \sum_{i=1}^{m} \frac{\lambda_{i,\nu}}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}}} \bar{\delta}_1^{i-1} \right|_j \leq \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_{\infty}, \ (1 \leq j \leq m).$$

(ii) $\gamma''_{\sigma,(k,l)} \not\equiv \gamma''_{\tilde{\sigma},(k,l)} \bmod p^k\mathbb{Z}[\rho][\pi] + \pi^l\mathbb{Z}[\rho][\pi]$ *für alle* $\tilde{\sigma} \in G//H$ *mit* $\tilde{\sigma} \neq \sigma$.

Dann gilt für $g_{\sigma,\nu} := \sum_{i=1}^{m} \frac{\lambda_{i,\nu}}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}}} \bar{\delta}_1^{i-1} \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$*:*

(a) Das Polynom $g_{\sigma} := \sum_{\nu=0}^{l-1} g_{\sigma,\nu}\pi^{\nu} \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi] \subseteq \bar{F}_{\mathcal{P}}[\pi]$ *ist Nullstelle von* $\iota_{\mathcal{P}}(R_{(G,H,F)})(X) \in \iota_{\mathcal{P}}(Cl(\mathbb{Z}[t],F))[X]$ *mod* $\pi^l\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi]$ *und* $g_{\sigma} \equiv \gamma'_{\sigma,(l)} \bmod \pi^l\mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi]$.

(b) $g_{\sigma} \not\equiv \gamma'_{\tilde{\sigma},(l)} \bmod \pi^l N(\bar{f},\bar{F}_{\mathcal{P}})[\pi]$ *für alle* $\tilde{\sigma} \in G//H$ *mit* $\tilde{\sigma} \neq \sigma$.

Beweis. Aufgrund der Definition des Gitters $\Lambda_{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}} g^*_{\sigma,(k,1),\nu},(k)}$ erhalten wir $\psi(g_{\sigma,\nu}) \equiv g^*_{\sigma,(k),\nu} \bmod p^k\mathbb{Z}_p[\rho]$, und somit gilt $\psi(g_{\sigma}) \equiv \gamma''_{\sigma,(k,l)} \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$. Es folgt

$$\begin{aligned} &\psi(\iota_{\mathcal{P}}(R_{(G,H,F)}))(\psi(g_{\sigma})) \\ &\quad\equiv \psi(\iota_{\mathcal{P}}(R_{(G,H,F)}))(\gamma''_{\sigma,(k,l)}) \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]] \\ &\quad\equiv \psi(\iota_{\mathcal{P}}(R_{(G,H,F)}))(\gamma''_{\sigma}) \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]] \\ &\quad\equiv 0 \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]. \end{aligned} \tag{4.98}$$

Da ψ ein Homomorphismus mit $\nu_{\tilde{\mathfrak{p}}}(a) = \nu_p(\psi(a))$, $a \in N(\bar{f}, \bar{F}_{\mathcal{P}})$ ist, erhalten wir aus $\psi(\iota_{\mathcal{P}}(R_{(G,H,F)}))(\psi(g_\sigma)) = \psi(\iota_{\mathcal{P}}(R_{(G,H,F)})(g_\sigma))$

$$\iota_{\mathcal{P}}(R_{(G,H,F)})(g_\sigma) \equiv 0 \bmod \tilde{\mathfrak{p}}^k \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]] + \pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]. \tag{4.99}$$

für das über p liegende unverzweigte Primideal $\tilde{\mathfrak{p}}$ vom Grad eins von $\mathbb{Z}[\bar{\delta}_1]$ aus Algorithmus 4.59. Aus den Ungleichungen $\|\gamma'^{[j]}_{\tilde{\sigma}}\|_{\infty,(l)} \leq \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty$ mit $\gamma'^{[j]}_{\tilde{\sigma}} = \tilde{\sigma}F(\phi_{j,1}(\alpha'), \ldots, \phi_{j,n}(\alpha')) \in \mathbb{C}[[\pi]]$ für alle $\tilde{\sigma} \in G//H$ und $\|g^{(j)}_\sigma\|_\infty \leq \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty$ nach Voraussetzung folgt

$$\begin{aligned}
&\| \iota_{\mathcal{P}}(R_{(G,H,F)})^{(j)}(g^{(j)}_\sigma) \|_{\infty,(l)} \\
&\qquad = \| \prod_{\tilde{\sigma} \in G//H} g^{(j)}_\sigma - \gamma'^{[j]}_{\tilde{\sigma}} \|_{\infty,(l)} \\
&\qquad \leq \| \prod_{\tilde{\sigma} \in G//H} 2 \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty (1 + \pi + \cdots + \pi^{l-1}) \|_{\infty,(l)} \\
&\qquad = (2 \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty)^{[G:H]} \cdot \|(1 + \pi + \cdots + \pi^{l-1})^{[G:H]}\|_{\infty,(l)} \\
&\qquad = (2 \|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty)^{[G:H]} \cdot \tbinom{[G:H]+(l-1)-1}{l-1},
\end{aligned} \tag{4.100}$$

wobei die letzte Gleichheit nach Proposition 4.107 gilt. Somit erhalten wir

$$\prod_{j=1}^{m} \| \iota_{\mathcal{P}}(R_{(G,H,F)})^{(j)}(g^{(j)}_\sigma) \|_{\infty,(l)} < p^k \, |\mathrm{disc}(\bar{h}_1)|^{-(2(l-1)+[G:H]-1)\,m}. \tag{4.101}$$

Gilt $\iota_{\mathcal{P}}(R_{(G,H,F)})(g_\sigma) = \sum_{\nu=0}^{\infty} \Gamma_\nu \pi^\nu \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]$, so haben nach (4.99) die ersten l Koeffizienten einen $\tilde{\mathfrak{p}}$-Betrag von

$$|\,\Gamma_\nu\,|_{\tilde{\mathfrak{p}}} \leq p^{-k}, \ (0 \leq \nu \leq l-1) \tag{4.102}$$

und für alle anderen endlichen Stellen $\tilde{\mathfrak{p}}' \subset \mathbb{Z}[\bar{\delta}_1]$, die nicht die Diskriminante von $\bar{h}_1$ teilen gilt $|\,\Gamma_\nu\,|_{\tilde{\mathfrak{p}}'} \leq 1$ für $0 \leq \nu \leq l-1$, da $\Gamma_\nu \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}$ für diese Stellen ganz ist. Dagegen erhalten wir für die endlichen Stellen $\mathfrak{p} \subset \mathfrak{o}_{\bar{F}_{\mathcal{P}}}$, $(\bar{p} \in \mathfrak{p})$, die die Diskriminante teilen, mittels Proposition 4.108

$$\begin{aligned}
|\,\Gamma_\nu\,|_{\mathfrak{p}} = \mathrm{N}(\mathfrak{p})^{-\nu_{\mathfrak{p}}(\Gamma_\nu)} &= \bar{p}^{\,-f(\mathfrak{p}|\bar{p})\nu_{\mathfrak{p}}(\Gamma_\nu)} \\
&= \bar{p}^{\,-f(\mathfrak{p}|\bar{p})e(\mathfrak{p}|\bar{p})\nu_{\bar{p}}(\Gamma_\nu)} \\
&\leq \bar{p}^{\,f(\mathfrak{p}|\bar{p})e(\mathfrak{p}|\bar{p})\,\nu_{\bar{p}}(\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+[G:H]-1})} \\
&\leq \bar{p}^{\,m\,\nu_{\bar{p}}(\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+[G:H]-1})} \\
&\leq |\mathrm{disc}(\bar{h}_1)|^{(\max\{2\nu,1\}+[G:H]-1)\,m}, \ (0 \leq \nu \leq l-1)
\end{aligned} \tag{4.103}$$

Aus der Produktformel für algebraische Zahlkörper folgt dann für das Produkt der unendlichen Stellen

$$\begin{aligned}
\prod_{j=1}^{m} |\Gamma_\nu|_j &\geq p^k \, |\mathrm{disc}(\bar{h}_1)|^{-(\max\{2\nu,1\}+[G:H]-1)\,m} \\
&\geq p^k \, |\mathrm{disc}(\bar{h}_1)|^{-(\max\{2(l-1),1\}+[G:H]-1)\,m}, \ (0 \leq \nu \leq l-1).
\end{aligned} \tag{4.104}$$

Dies steht im Widerspruch zu (4.101) und aus der Produktformel folgt $\Gamma_0 = \Gamma_1 = \cdots = \Gamma_{l-1} = 0$. Damit erhalten wir

$$\iota_{\mathcal{P}}(R_{(G,H,F)})(g_\sigma) \equiv 0 \bmod \pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]. \tag{4.105}$$

Schließlich folgt mittels Annahme (ii), daß

$$g_\sigma \equiv \gamma'_{\sigma,(l)} \bmod \pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi] \tag{4.106}$$

gilt und $g_\sigma \not\equiv \gamma'_{\tilde{\sigma},(l)} \bmod \pi^l N(\bar{f}, \bar{F}_{\mathcal{P}})[\pi]$ für alle $\tilde{\sigma} \in G//H$ mit $\tilde{\sigma} \neq \sigma$ ist. □

Somit befinden wir uns mittels Satz 4.97 nun in der Situation von Satz 4.91 für die l-Approximation g_σ von γ'_σ.

4.107. Proposition. *Seien $l, m \in \mathbb{Z}_{>0}$ mit $l > m$. Dann gilt*

$$\|(1 + \pi + \cdots + \pi^{l-1})^m\|_{\infty,(l)} = \tbinom{m+(l-1)-1}{l-1}.$$

Beweis. Wir beweisen durch vollständige Induktion über m die Kongruenz

$$(1 + \pi + \cdots + \pi^{l-1})^m \equiv \sum_{j=0}^{l-1} \tbinom{m+j-1}{j} \pi^j \bmod \pi^l.$$

Die Behauptung folgt dann aus der Tatsache, daß $\binom{m+j-1}{j}$ für $j = l-1$ maximal ist: Für $m = 1$ erhalten wir $1 + \pi + \cdots + \pi^{l-1} \stackrel{!}{\equiv} \sum_{j=0}^{l-1} \binom{1+j-1}{j} \pi^j \bmod \pi^l$, was offensichtlich korrekt ist. Wir nehmen nun an, daß die Behauptung für m bereits bewiesen ist und zeigen

$$(1 + \pi + \cdots + \pi^{l-1})^{m+1} \equiv \sum_{j=0}^{l-1} \tbinom{(m+1)+j-1}{j} \pi^j \bmod \pi^l :$$

Es gilt

$$\begin{aligned} (1 + \pi + \cdots + \pi^{l-1})^{m+1} &\equiv (1 + \pi + \cdots + \pi^{l-1}) \sum_{j=0}^{l-1} \tbinom{m+j-1}{j} \pi^j \bmod \pi^l \\ &\equiv \sum_{j=0}^{l-1} \pi^j \left(\sum_{\nu=0}^{j} \tbinom{m+\nu-1}{\nu} \right) \bmod \pi^l. \end{aligned}$$

Da $\sum_{\nu=0}^{j} \binom{m+\nu-1}{\nu} = \sum_{\nu=0}^{j} \binom{m+\nu-1}{m-1} = \binom{m+1+j-1}{m} = \binom{m+1+j-1}{j}$ ist, folgt die Behauptung. □

4.108. Proposition. *Sei $g_\sigma \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi]$ wie in Satz 4.97 definiert und $m < l$. Dann gilt:*

(i) Ist $g_\sigma^m = \sum_{\nu=0}^{(l-1)\cdot m} \Gamma_\nu \pi^\nu$, *so liefert Multiplikation des* ν*-ten Koeffizienten von* g_σ^m *mit* $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+(m-1)}$ *ein Element in* $\mathbb{Z}[\bar{\delta}_1]$ *für* $0 \leq \nu \leq l-1$.

(ii) Ist $\iota_{\mathcal{P}}(R_{(G,H,F)}(g_\sigma) = \sum_{\nu=0}^{\infty} \Gamma_\nu \pi^\nu$, *so liefert Multiplikation des* ν*-ten Koeffizienten von* $\iota_{\mathcal{P}}(R_{(G,H,F)}(g_\sigma)$ *mit* $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+[G:H]-1}$ *ein Element in* $\mathbb{Z}[\bar{\delta}_1]$ *für* $0 \leq \nu \leq l-1$.

Beweis. Da wir hier Aussagen über die Nenner der Γ_ν beweisen wollen, seien im folgenden mit $\star$ nicht näher definierte Elemente aus $\mathbb{Z}[\bar{\delta}_1]$ bezeichnet. Zur kürzeren Schreibweise schreiben wir nur $g_\sigma^m \bmod \pi^l$ und meinen damit $g_\sigma^m \bmod \pi^l \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[\pi]$.

(i) Wir zeigen durch vollständiges Induktion über m, daß

$$g_\sigma^m \equiv \sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+(m-1)}}\ \pi^\nu \bmod \pi^l$$

gilt. Da nach Voraussetzung $g_\sigma = \sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}}} \pi^\nu$ ist, ist die Induktionsannahme für $m = 1$ korrekt. Wir nehmen nun an, daß die Behauptung für m bereits bewiesen ist und zeigen

$$g_\sigma^{m+1} \equiv \sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+m}}\ \pi^\nu \bmod \pi^l.$$

Es gilt

$$\begin{aligned} g_\sigma^{m+1} = g_\sigma g_\sigma^m &\equiv \left(\sum_{\mu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\mu,1\}}} \pi^\mu\right)\left(\sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+(m-1)}} \pi^\nu\right) \bmod \pi^l \\ &\equiv \sum_{\nu=0}^{l-1} \pi^\nu \left(\sum_{\mu=0}^{\nu} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2(\nu-\mu),1\}+(m-1)} \cdot \mathrm{disc}(\bar{h}_1)^{\max\{2\mu,1\}}}\right) \bmod \pi^l \\ &\equiv \sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+m}} \pi^\nu \bmod \pi^l. \end{aligned}$$

wobei die letzte Kongruenz folgt, wenn die innere Summe der Zeile davor auf Hauptnenner gebracht wird: Für $\nu - \mu \geq 1$ und $\mu \geq 1$ ist klar, daß $\mathrm{disc}(\bar{h}_1)^{\max\{2(\nu-\mu),1\}+(m-1)} \cdot \mathrm{disc}(\bar{h}_1)^{\max\{2\mu,1\}} \leq \mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+m}$ ist, und für $\nu = \mu$ bzw. $\mu = 0$ folgt dies durch Einsetzen und ausrechnen.

(ii) Da $R_{(G,H,F)}(X)$ nach Voraussetzung Koeffizienten in $Cl(\mathbb{Z}[t], F)$ hat, folgt nach Proposition 4.64, daß $\iota_{\mathcal{P}}(R_{(G,H,F)})$ von der Gestalt

$$\iota_{\mathcal{P}}(R_{(G,H,F)})(X) = \Gamma_0(\pi) + \Gamma_1(\pi)X + \cdots + \Gamma_{[G:H]-1}(\pi)X^{[G:H]-1} + X^{[G:H]}$$

mit $\Gamma_i(\pi) = \sum_{\nu=0}^{\infty} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}}} \pi^\nu \in \mathbb{Z}[\bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1))}[[\pi]]$ ist. Es folgt

$$\Gamma_i g_\sigma^i \equiv \left(\sum_{\mu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\mu,1\}}} \pi^\mu\right)\left(\sum_{\nu=0}^{l-1} \frac{\star}{\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}+(i-1)}} \pi^\nu\right) \bmod \pi^l$$

$$\equiv \sum_{\nu=0}^{l-1} \frac{\star}{\operatorname{disc}(\bar{h}_1)^{\max\{2\nu,1\}+i}} \pi^\nu \bmod \pi^l,$$

analog wie im Beweis von (i). Darüber hinaus gilt nach (i)

$$g_\sigma^{[G:H]} \equiv \sum_{\nu=0}^{l-1} \frac{\star}{\operatorname{disc}(\bar{h}_1)^{\max\{2\nu,1\}+([G:H]-1)}} \pi^\nu \bmod \pi^l.$$

Ordnen wir $\sum_{\nu=0}^{[G:H]-1} \Gamma_\nu g_\sigma^\nu + g_\sigma^{[G:H]}$ nach π-Potenzen und bringen die Koeffizienten auf maximal auftretenden Hauptnenner, so folgt

$$\iota_{\mathcal{P}}(R_{(G,H,F)})(g_\sigma) \equiv \sum_{\nu=0}^{l-1} \frac{\star}{\operatorname{disc}(\bar{h}_1)^{\max\{2\nu,1\}+([G:H]-1)}} \pi^\nu \bmod \pi^l.$$

□

4.109. Bemerkung. Satz 4.97 und Satz 4.91 vereinfachen sich für den absoluten Funktionenkörperfall über $\mathbb{Q}(t)$ wie folgt: Sei $f \in \mathbb{Z}[t][x]$ irreduzibel und in x normiert. Im absoluten Fall gilt $F = \mathbb{Q}(t)$, $\mathfrak{o}_F = \mathbb{Q}[t]$ mit Ganzheitsbasis $\omega_1 = 1$, $m = 1$, und s, s' sind immer eins. Nach dem Hilbertschen Irreduzibilitätssatz existiert $t_0 \in \mathbb{Z}$, so daß $\bar{f} = f(t_0, x) \in \mathbb{Z}[x]$ irreduzibel und $t - t_0 \nmid \operatorname{disc}(f)$ gilt. Die zu $\pi := t - t_0$ gehörende Stelle $\mathcal{P}$ ist dann vom Grad eins, und wir erhalten $\bar{F}_{\mathcal{P}} = \mathbb{Q}$. Die Nullstellen von f liegen in $\mathbb{Z}_p[\rho][[\pi]]$, wobei wir p, ρ wie in Sektion 3.2 wählen. Die Zahl $M := M_1 \in \mathbb{Q}$ ist dann eine untere Schranke einer Fortsetzung der Gradbewertung $\nu_1 = \nu_\infty$ der Nullstellen des Resolventenpolynoms $R_{(G,H,F)}(X) \in \mathbb{Z}[t][X]$ in $N(f, \mathbb{Q}(t))$. Darüber hinaus gilt $W_1 = 0$, $A = -M$, und $M^{[1]}_{\bar{F}_{\mathcal{P}},(l)} \in \mathbb{R}[\pi]$ ist ein Polynom vom Grad $l-1$, so daß für alle Nullstellen $\gamma'^{[1]}_\sigma \in \mathbb{C}[[\pi]]$ von $\iota_{\mathcal{P}}(R_{(G,H,F)})(X) \in \mathbb{C}[[\pi]][X]$ die Ungleichung $\|\gamma'^{[1]}_\sigma\|_{\infty,(l)} \leq \|M^{[1]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty$ gilt. Für $\gamma'_{\sigma,(l)} \in \mathbb{Z}[\pi]$ vereinfacht sich das Gitter $\Lambda_{\gamma'_{(l)},(l)}$ zu

$$\Lambda_{\gamma'_{(l)},(l)} = \left\{ \mathbb{Q}[\pi]\,(\pi^l, 0) + \mathbb{Q}[\pi]\,(\gamma'_{\sigma,(l)}, 1) \right\}.$$

Nach Heß [34], Lemma 1.5 ist die Basis des Gitters $\Lambda_{\gamma'_{(l)},(l)}$ reduziert, wenn die Summe der Zeilengrade (Maximum der Grade der Einträge eines Vektors) der Vektoren $(\pi^l, 0)$ und $(\gamma'_{\sigma,(l)}, 1)$ gleich dem Grad der Determinante der Matrix $M := \left(\begin{smallmatrix} \pi^l & 0 \\ \gamma'_{\sigma,(l)} & 1 \end{smallmatrix}\right)$ ist. Ist $\gamma'_{\sigma,(l)}$ keine Konstante, so ist die Summe der Zeilengrade echt größer als l, während Grad von $\det(M) = l$ gilt. Die Basis von $\Lambda_{\gamma'_{(l)},(l)}$ wäre also nicht reduziert. Um in diesem Fall eine reduzierte Basis zu erhalten, schreiben wir π^l mittels Division mit Rest als $\pi^l = g(\pi)\gamma'_{\sigma,(l)} + r(\pi)$, $\deg(r) < \deg(\gamma'_{\sigma,(l)})$ für $g(\pi), r(\pi) \in \mathbb{Q}[\pi]$. Addition von $-g(\pi)$ mal der zweiten Zeile von M zu der ersten Zeile von M ergibt

$$\begin{pmatrix} \pi^l - g(\pi)\gamma'_{\sigma,(l)} & -g(\pi) \\ \gamma'_{\sigma,(l)} & 1 \end{pmatrix} = \begin{pmatrix} r(\pi) & -g(\pi) \\ \gamma'_{\sigma,(l)} & 1 \end{pmatrix}.$$

Unter der Annahme, daß $\deg(g) \geq \deg(r)$ ist, ist die Summe der Zeilengrade $\deg(g) + \deg(\gamma'_{\sigma,(l)}) = l = \det(M)$. Somit ist die Basis von $\Lambda_{\gamma'_{(l)},(l)}$ reduziert, und $(\gamma'_{\sigma,(l)}, 1)$ ist erstes reduziertes Basiselement. Um $\deg(g) \geq \deg(r)$ zu gewährleisten, muß $l \geq 2\deg(\gamma'_{\sigma,(l)}) - 1$ gelten, da dann $\deg(g) = l - \deg(\gamma'_{\sigma,(l)}) \geq \deg(\gamma'_{\sigma,(l)}) - 1 \geq \deg(r)$ gilt. Unter Verwendung der Definition vom A bzw. M folgt also für $l > 2A = -2M$ ($\deg(\gamma'_{\sigma,(l)}) \leq -M$ nach Definition von M), daß $(\gamma'_{\sigma,(l)}, 1)$ kürzester Vektor des Gitters $\Lambda_{\gamma'_{(l)},(l)}$ ist. Der Inklusionstest vereinfacht sich in diesem Fall und kann wie folgt durchgeführt werden (vgl. auch Bemerkung 3.37):
Seien l, $k \in \mathbb{Z}_{>0}$ mit $l > -[\,G:H\,]M$ und $p^k > (2\|M^{[1]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty)^{[\,G:H\,]} \cdot \binom{[G:H]+(l-1)-1}{l-1}$. Ist $\gamma''_\sigma \in \mathbb{Z}_p[\rho][[\pi]]$ eine Nullstelle von $(\psi \circ \iota_{\mathcal{P}})(R_{(G,H,F)})(X) \in \mathbb{Z}_p[[\pi]][X]$ mit $\gamma''_{\sigma,(k,l)} = \sum_{\nu=0}^{l-1} g^*_{\sigma,(k),\nu}\pi^\nu$ und

(*i*) $g^*_{\sigma,(k),\nu} \in \mathbb{Z} + p^k\mathbb{Z}[\rho]$ und $|\lfloor g^*_{\sigma,(k,1),\nu}\rfloor_{p^k}| \leq \|M^{[1]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty$ für $0 \leq \nu \leq l-1$,

(*ii*) $\gamma''_{\sigma,(k,l)} \not\equiv \gamma''_{\tilde{\sigma},(k,l)} \bmod p^k\mathbb{Z}[\rho][\pi] + \pi^l\mathbb{Z}[\rho][\pi]$ für alle $\tilde{\sigma} \in G//H$ mit $\tilde{\sigma} \neq \sigma$,

(*iii*) $\nu_\infty\left(\sum_{\nu=0}^{l-1} \lfloor g^*_{\sigma,(k,1),\nu}\rfloor_{p^k}\pi^\nu\right) \geq M$,

so ist $\gamma_\sigma = \sum_{\nu=0}^{l-1} \lfloor g^*_{\sigma,(k,1),\nu}\rfloor_{p^k}\, t^\nu \in \mathbb{Z}[t]$ eine einfache Nullstelle von $R_{(G,H,F)}(X) \in \mathbb{Z}[t][X]$. Umgekehrt erfüllt jede einfache Nullstelle von $R_{(G,H,F)}$ in $\mathbb{Z}[t]$ die Bedingungen $(i) - (iii)$.

Wir erhalten die folgenden Rekonstruktionsalgorithmen, wobei wir die Variable π wie bei der Nullstellenberechnung zu $t - t_0$ spezialisieren wollen.

4.110. Algorithmus. *(Rekonstruktion $F = \mathbb{F}_q(t,\delta)$)*

Eingabe: *Approximierte Nullstelle der Resolvente $\gamma'_{\sigma,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}[\pi]$ für $l \in \mathbb{Z}_{>0}$ wie in Proposition 4.87, (fixierte) Ganzheitsbasis $\omega_1, \ldots, \omega_m$ von $\mathfrak{o}_F$, die im wild verzweigten Fall $(\mathrm{char}(\mathbb{F}_q) \mid e)$ reduziert ist, Stelle $\mathcal{P} \in \mathbb{P}(F)\backslash\mathbb{P}_\infty(F)$ aus Algorithmus 4.57, untere Schranken M_j, $(1 \leq j \leq s)$ der Bewertungen ν_j der Nullstellen von $R_{(G,H,F)}(X) \in \mathfrak{o}_F[X]$ in $N(f,F)$ wie in Satz 4.91, Schranke $A \in \mathbb{Q}$ wie in (4.76).*

Ausgabe: *Aussage „$\gamma_\sigma \notin \mathfrak{o}_F$“ oder*
$\tilde{\gamma}_\sigma \in \mathfrak{o}_F$ mit $\tilde{\gamma}_\sigma \equiv \gamma_\sigma \bmod \mathcal{P}$. Ist $\gamma_\sigma \in \mathfrak{o}_F$, dann ist $\gamma_\sigma = \tilde{\gamma}_\sigma$.
Ist $l > -[\,G:H\,]\sum_{j=1}^s \deg(\mathcal{P}_j)M_j$, dann Aussage „$\gamma_\sigma \notin \mathfrak{o}_F$“ oder eine Nullstelle $\tilde{\gamma}_\sigma \in \mathfrak{o}_F$ der Resolvente mit $\tilde{\gamma}_\sigma \equiv \gamma_\sigma \bmod \mathcal{P}$.
Ist $\gamma_\sigma \in \mathfrak{o}_F$, dann ist $\gamma_\sigma = \tilde{\gamma}_\sigma$.

1. *(Pseudo-Test) Ist* $\gamma'_{\sigma,(l)} \notin \mathbb{F}_{q^{\deg(\mathcal{P})}}[\pi]$, *so gebe „*$\gamma_\sigma \notin \mathfrak{o}_F$*“ aus und terminiere.*

2. *(Aufstellung des Gitters* $\Lambda_{\gamma'_\sigma,(l)}$*) Bestimme* $\omega'_{i,(l)} \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[\pi]$ *mit* $\omega'_{i,(l)} \equiv \iota_{\mathcal{P}}(\omega_i) \bmod \pi^l \mathbb{F}_{q^{\deg(\mathcal{P})}}[\pi]$ *und setze* $\Lambda_{\gamma'_{\sigma,(l)},(l)} =< u_{1,(l)}, \ldots, u_{m+1,(l)} >$ *mit Vektoren* $u_{i,(l)}$ *aus* (4.72).

3. *(Reduktion) Berechne erstes reduziertes Basiselement* $(a\lambda'_1, \ldots, a\lambda'_m, a)$ *von* $\Lambda_{\gamma'_{\sigma,(l)},(l)}$.

4. *(Ende) Ist* $a \in \mathbb{F}^\times_{q^{\deg(\mathcal{P})}}$, $\lambda_i := \lambda'_i(t - t_0) \in \mathbb{F}_q[t]$ *für* $1 \le i \le m$, $\max_{1\le i\le m}\{\deg(\lambda_i)\} \le A$ *und* $\nu_j(\sum_{i=1}^m \lambda_i\omega_i) \ge M_j$, *so gebe* $\tilde{\gamma}_\sigma := -\sum_{i=1}^m \lambda_i\omega_i \in \mathfrak{o}_F$ *aus. Ansonsten, gebe „*$\gamma_\sigma \notin \mathfrak{o}_F$*“ aus. Terminiere.*

Beweis. Die Korrektheit des Algorithmus folgt analog wie im Beweis zu Algorithmus 3.38. □

4.111. Algorithmus. *(Rekonstruktion* $F = \mathbb{Q}(t, \delta)$*)*

Eingabe: *Approximierte Nullstelle* $\gamma''_{\sigma,(k,l)} = \sum_{\nu=0}^{l-1} g^*_{\sigma,(k),\nu}\pi^\nu \in \mathbb{Z}[\rho][\pi]$ *der Resolvente für* $l \in \mathbb{Z}_{>0}$ *wie in Proposition 4.87 und* $k \in \mathbb{Z}_{>0}$ *wie in* (4.65) *für* $\nu = l - 1$, *(fixierte) Ganzheitsbasis* $\omega_1, \ldots, \omega_m$ *von* $\mathfrak{o}_F$, *Stelle* $\mathcal{P} \in \mathbb{P}(F)\backslash\mathbb{P}_\infty(F)$ *aus Algorithmus 4.59, untere Schranken* M_j, $(1 \le j \le s)$ *der Bewertungen* ν_j *der Nullstellen von* $R_{(G,H,F)}(X) \in Cl(\mathbb{Z}[t], F)[X]$ *in* $N(f, F)$ *wie in Satz 4.97, Schranke* $A \in \mathbb{Q}$ *wie in* (4.76), *Primideal* $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$ *der Gleichungsordnung des Restklassenkörpers* $\bar{F}_{\mathcal{P}} = \mathbb{Q}(\bar{\delta}_1)$ *wie in Algorithmus 4.59, Minimalpolynom* $\bar{h}_1(x) \in \mathbb{Z}[x]$ *vom Grad* m *von* $\mathbb{Q}(\bar{\delta}_1)/\mathbb{Q}$, *Schranken* $\|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty \in \mathbb{R}[\pi]$, $(1 \le j \le m)$ *wie in Satz 4.97 und Schranke* $A_{\bar{F}_{\mathcal{P}}} \in \mathbb{R}$ *wie in Satz 4.97.*

Ausgabe: *Aussage „*$\gamma_\sigma \notin Cl(\mathbb{Z}[t], F)$*“ oder*
$\tilde{\gamma}_\sigma \in Cl(\mathbb{Z}[t], F)$ *mit* $\tilde{\gamma}_\sigma \equiv \gamma_\sigma \bmod \mathcal{P}$. *Ist* $\gamma_\sigma \in Cl(\mathbb{Z}[t], F)$, *dann ist* $\gamma_\sigma = \tilde{\gamma}_\sigma$.
Ist $l > -[\,G\!:\!H\,]\sum_{j=1}^s \deg(\mathcal{P}_j)M_j$, $k > \sum_{j=1}^m [\,G\!:\!H\,]\log_p(2\,\|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty) + \log_p(\binom{[G:H]+(l-1)-1}{l-1}) + \log_p(|\mathrm{disc}(\bar{h}_1)|^{2(l-1)+[G:H]-1})$, *dann Aussage „*$\gamma_\sigma \notin Cl(\mathbb{Z}[t], F)$*“ oder*
eine Nullstelle $\tilde{\gamma}_\sigma \in Cl(\mathbb{Z}[t], F)$ *der Resolvente mit* $\tilde{\gamma}_\sigma \equiv \gamma_\sigma \bmod \mathcal{P}$. *Ist* $\gamma_\sigma \in Cl(\mathbb{Z}[t], F)$, *dann ist* $\gamma_\sigma = \tilde{\gamma}_\sigma$.

1. *(Koeffizienten-Reduktion und Pseudo-Test) Für* $\nu = 0, \ldots, l-1$ *wende Algorithmus 3.38 auf* $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}} g^*_{\sigma,(k),\nu}$, *Basis der Gleichungsordnung* $1, \bar{\delta}_1, \ldots, \bar{\delta}_1^{m-1}$, *Primideal* $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$, *Schranken* $\|M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}\|_\infty$, $(1 \le j \le m)$

und $|\mathrm{disc}(\bar{h}_1)|^{2(l-1)}(A_{\bar{F}_\mathfrak{p}}-1)+1 \in \mathbb{R}$ *an: Wird „*$\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}} g_{\sigma,\nu} \notin \mathbb{Z}[\bar{\delta}_1]$*“ zurückgegeben, so gebe „*$\gamma_\sigma \notin Cl(\mathbb{Z}[t],F)$*“ aus und terminiere. Ansonsten erhalte nach Division mit* $\mathrm{disc}(\bar{h}_1)^{\max\{2\nu,1\}}$ *das Element* $g_{\sigma,\nu} \in \mathbb{Q}(\bar{\delta}_1)$.

2. *(Aufstellung des Gitters* $\Lambda_{g_{\sigma,(l)}}$*) Setze* $g_\sigma = \sum_{\nu=0}^{l-1} g_{\sigma,\nu}\pi^\nu$. *Bestimme Polynome* $\omega'_{i,(l)} \in \mathbb{Q}(\bar{\delta}_1)[\pi]$ *vom Grad* $l-1$ *mit* $\omega'_{i,(l)} \equiv \iota_\mathcal{P}(\omega_i) \bmod \pi^l\mathbb{Q}(\bar{\delta}_1)[\pi]$ *und setze* $\Lambda_{g_\sigma,(l)} =< u_{1,(l)},\ldots,u_{m+1,(l)} >$ *mit Vektoren* $u_{i,(l)}$ *aus* (4.72).

3. *(Reduktion) Berechne erstes reduziertes Basiselement* $(a\lambda'_1,\ldots,a\lambda'_m,a)$ *von* $\Lambda_{\gamma'_{\sigma,(l)},(l)}$.

4. *(Ende) Ist* $a \in \mathbb{Q}(\bar{\delta}_1)^\times$, $\lambda_i := \lambda'_i(t-t_0) \in \mathbb{Q}[t]$ *für* $1 \le i \le m$, $\max_{1\le i\le m}\{\deg(\lambda_i)\} \le A$ *und* $\nu_j(\sum_{i=1}^m \lambda_i\omega_i) \ge M_j$, *so gebe* $\tilde{\gamma}_\sigma := -\sum_{i=1}^m \lambda_i\omega_i \in Cl(\mathbb{Z}[t],F)$ *aus. Ansonsten, gebe „*$\gamma_\sigma \notin Cl(\mathbb{Z}[t],F)$*“ aus. Terminiere.*

Zur Berechnung der unteren Schranken $M_j \in \mathbb{Q}$, $(1 \le j \le s)$ der Bewertungen der Nullstellen von $R_{(G,H,F)}$ in $N(f,F)$ verwenden wir die Bewertungen der Nullstellen $\alpha_1,\ldots,\alpha_n \in N(f,F)$. Nach Neukirch [62], Kapitel II, §6, Satz 6.3 lassen sich diese mit Hilfe des Newton-Polygons wie folgt berechnen:

4.112. Satz. *Sei* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_0 \neq 0$ *ein normiertes Polynom mit Koeffizienten in dem Funktionenkörper* F *und* $\nu_1,\ldots,\nu_s$ *die Bewertungen, die zu den Stellen aus* $\mathbb{P}_\infty(F)$ *korrespondieren. Eine Fortsetzung von* ν_j *auf den Zerfällungskörper von* f *bezeichnen wir ebenfalls mit* ν_j, $(1 \le j \le s)$. *Dann gilt*

$$\nu_{j,1} := \min_{1\le i\le n}\{\nu_j(\alpha_i)\} = \min_{1\le r\le n}\left\{\frac{\nu_j(a_{n-r})}{r}\right\}, \tag{4.113}$$

und für $\nu_{j,1} = \frac{\nu_j(a_{n-k_1})}{k_1}$ *gibt es genau* k_1 *Nullstellen von* f *mit Bewertung* $\nu_{j,1}$. *Ist* $k_1 < n$, *so lassen sich rekursiv die Bewertungen*

$$\nu_{j,r+1} := \min_{1\le i\le n}\{\nu_j(\alpha_i) \,|\, \nu_j(\alpha_i) > \nu_{j,r}\} \tag{4.114}$$

der restlichen Nullstellen bestimmen durch

$$\nu_{j,r+1} = \min_{k_r<l\le n} \frac{\nu_j(a_{n-l}) - \sum_{\mu=1}^r k_\mu\nu_{j,\mu}}{l-k_r}. \tag{4.115}$$

Gilt $\nu_{j,r+1} = \frac{\nu_j(a_{n-k_{r+1}}) - \sum_{\mu=1}^r k_\mu\nu_{j,\mu}}{k_{r+1}-k_r}$, *so haben* $k_{r+1}-k_r$ *Nullstellen von* f *die Bewertung* $\nu_{j,r+1}$.

Beweis. Die Behauptungen folgenden direkt aus dem Beweis von Satz 6.3 aus Neukirch [62], Kapitel II, §6. □

4.116. Proposition. *Seien $\nu_{j,1} \leq \cdots \leq \nu_{j,n} \in \mathbb{Q}$ Bewertungen der Nullstellen $\alpha_1, \ldots, \alpha_n \in N(f, F)$ des Polynoms $f \in F[x]$ und $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ ein G-relatives H-invariantes Polynom. Dann läßt sich eine untere Schranke $M_j \in \mathbb{Q}$ mit $\nu_j(F(\alpha_1, \ldots, \alpha_n)) \geq M_j$, $(1 \leq j \leq s)$ rekursiv durch (i), (ii) und (iii) berechnen.*

(i) Seien $i_1, \ldots, i_k$ paarweise verschiedene Zahlen der Menge $\{1, \ldots, n\}$ und $r_1, \ldots, r_k \in \mathbb{Z}_{>0}$ mit $r_1 \leq \cdots \leq r_k$. Dann folgt für das Monom $x_{i_1}^{r_1} \cdots x_{i_k}^{r_k}$

$$\nu_j(\alpha_{i_1}^{r_1} \cdots \alpha_{i_k}^{r_k}) \geq r_k \nu_{j,1} + r_{k-1} \nu_{j,2} + \cdots + r_1 \nu_{j,k}.$$

(ii) Aus $F = F_1 + F_2$ folgt

$$\nu_j(F(\alpha_1, \ldots, \alpha_n)) \geq \min\{\nu_j(F_1(\alpha_1, \ldots, \alpha_n)), \nu_j(F_2(\alpha_1, \ldots, \alpha_n))\}.$$

(iii) Aus $F = F_1 \cdot F_2$ folgt

$$\nu_j(F(\alpha_1, \ldots, \alpha_n)) = \nu_j(F_1(\alpha_1, \ldots, \alpha_n)) + \nu_j(F_2(\alpha_1, \ldots, \alpha_n)).$$

Beweis. Die Behauptungen folgenden direkt aus den Eigenschaften der nichtarchimedischen Bewertungen ν_j für $1 \leq j \leq s$. □

4.117. Bemerkung. *(i)* Die Schranke $M_j \in \mathbb{Q}$ von $\nu_j(F(\alpha_1, \ldots, \alpha_n))$ aus Proposition 4.116 ist auch untere Schranke von $\nu_j(\sigma F(\alpha_1, \ldots, \alpha_n)) \geq M_j$ für alle $\sigma \in G//H$.

(ii) In unserer Implementierung des absoluten Funktionenkörperfalls über $\mathbb{F}_q$ und $\mathbb{Q}$ liften wir die Approximationen zunächst zu einer heuristischen Schranke

$$l' = 2 \text{ bzw. } k' = \min\{\, 3 \log_p(2\|M^{[1]}_{\bar{F}_\mathcal{P},(l)}\|_\infty),\ [\,G\!:\!H\,] \log_p(2\|M^{[1]}_{\bar{F}_\mathcal{P},(l)}\|_\infty)\,\}.$$

Im Fall $K = \mathbb{F}_q$ können Approximationen $\gamma'_{\sigma,(l')}$, deren Koeffizienten nicht in $\bar{F}_\mathcal{P}$ liegen, den Pseudo-Test in Schritt 1 nicht erfüllen und können somit zu keiner ganzalgebraischen Nullstelle korrespondieren. Dieser Test ist im Fall $K = \mathbb{F}_q$ natürlich nur anwendbar, wenn die Faktorisierung von $f \bmod \mathcal{P} \in \mathbb{F}_{q^{\deg(\mathcal{P})}}$ nicht nur aus Linearfaktoren besteht. Über $K = \mathbb{Q}$ genügt in den meisten Fällen die Rekonstruktion der zwei Koeffizienten von $\gamma''_{\sigma,(k',l')}$, um alle der nicht ganzalgebraischen Nullstellen herauszufiltern. Somit ist die Verwendung der heuristischen Schranken in beiden Fällen sehr effektiv. In einem zweiten Durchlauf liften wir die restlichen Nullstellen dann zu der aktuellen Präzision l bzw. k, l Präzision.

(iii) Bemerkung 3.40 *(iii)* und *(iv)* gelten im Funktionenkörperfall analog.

Kapitel 5

Erweiterungen des Verfahrens von Stauduhar

Ziel dieses Kapitel ist es, Erweiterungen des Verfahrens von Stauduhar zu beschreiben, so daß daraus ein speziell für größere Grade effizientes Verfahren resultiert. Die Hauptprobleme der relativen Resolventenmethode ergeben sich aus den ersten Abstiegen, ausgehend von der symmetrischen Gruppe S_n bzw. der alternierenden Gruppe A_n. Die Indizes der maximalen transitiven Untergruppen dieser beiden Gruppen werden für wachsendes n besonders groß. Für $n = 16, \ldots, 23$ erhalten wir zum Beispiel unter den maximalen imprimitiven und primitiven Untergruppen von S_n und A_n die maximalen Indizes

$[S_{16} : 16T_{1947}] = 2627625$	$[A_{16} : 16T^+_{1942}] = 2627625$ $[A_{16} : 16T^+_{1906}] = 32432400$
$[S_{17} : 17T_5] = 1307674368000$	$[A_{17} : 17T^+_8] = 10897286400$
$[S_{18} : 18T_{962}] = 190590400$ $[S_{18} : 18T_{468}] = 1307674368000$	$[A_{18} : 18T^+_{959}] = 190590400$ $[A_{18} : 18T^+_{377}] = 1307674368000$
$[S_{19} : 19T_6] = 355687428096000$	$[A_{19} : 19T^+_5] = 355687428096000$
$[S_{20} : 20T_{1101}] = 2546168625$ $[S_{20} : 20T_{362}] = 355687428096000$	$[A_{20} : 20T^+_{1090}] = 2546168625$ $[A_{20} : 20T^+_{272}] = 355687428096000$
$[S_{21} : 21T_{152}] = 36212176000$ $[S_{21} : 21T_{20}] = 152056375511040000$	$[A_{21} : 21T^+_{150}] = 36212176000$ $[A_{21} : 21T^+_{33}] = 10137091700736000$
$[S_{22} : 22T_{53}] = 13749310575$ $[S_{22} : 22T_{41}] = 1267136462592000$	$[A_{22} : 22T^+_{51}] = 13749310575$ $[A_{22} : 22T^+_{38}] = 1267136462592000$
$[S_{23} : 23T_4] = 51090942171709440000$	$[A_{23} : 23T^+_5] = 1267136462592000.$

Allgemein gilt, daß die Gruppenindizes exponentiell in n wachsen. Für n gerade

erhalten wir zum Beispiel

$$[S_n : (S_{\frac{n}{2}} \wr S_2)] = \frac{n!}{2(\frac{n}{2})!(\frac{n}{2})!} \text{ und } [S_n : (S_2 \wr S_{\frac{n}{2}})] = \frac{n!}{2^{\frac{n}{2}}(\frac{n}{2})!}.$$

Darüber hinaus ist für eine Primzahl p die transitive Permutationsgruppe $\mathrm{PSL}_2(p)$ Untergruppe von A_{p+1} mit Index $[A_{p+1} : \mathrm{PSL}_2(p)] = (p-2)!$, und für $p \neq 2, 3, 11, 23$ ist $\mathrm{PSL}_2(p)$ maximal in A_{p+1}.

Für Indizes dieser Größenordnung scheint eine effiziente Galoisgruppenberechnung mit den bisherigen Methoden wenig aussichtsreich. Dies liegt an mehreren Punkten: Ein erstes Problem ergibt sich bei der Berechnung der Nebenklassenrepräsentantensysteme. Hier ist es ratsam, daß der zugrundeliegende Algorithmus nicht alle Nebenklassenrepräsentanten auf einmal erzeugt, sondern einen nach dem anderen, um eine Berechnung des Nebenklassenrepräsentantensystems überhaupt zu ermöglichen. Wesentlich gravierender wirkt sich jedoch auf das Laufzeitverhalten die Auswertung der $[\,G : H\,]$ vielen Konjugierten eines G-relativen H-invarianten Polynoms für $G = S_n$ oder $G = A_n$ aus. Darüber hinaus stellt der Verifikationsschritt beim Inklusionstest ein weiteres Problem dar. Um zu beweisen, daß eine Nullstellenapproximation in der Maximalordnung eines algebraischen Zahl- bzw. Funktionenkörpers liegt, müssen die Nullstellenapproximationen bis zu einer Schranke k bzw. l geliftet werden, die linear vom Index abhängt. In Kapitel 3 hatten wir zum Beispiel gesehen, daß im Zahlkörperfall k so gewählt werden muß, daß

$$p^k > \max\left\{ \prod_{j=1}^{m} (2M_j)^{[G:H]},\ 2^{\frac{m^2}{2}} (A^2 + A)^m \prod_{j=1}^{m} W_j \right\}.$$

gilt. Da die letzten beiden angesprochenen Punkte für eine effektive Gestaltung der relativen Resolventenmethode am problematischsten erscheinen, gehen wir in den folgenden Abschnitten speziell darauf ein.

5.1 Erweiterung mittels Teilkörpern

Die bisherigen Ausführungen haben gezeigt, daß die ersten Abstiege besonders zeitkritisch sind. Daher wäre es generell wünschenswert, diese durch Berechnung geeigneter Zusatzinformationen zu überspringen und den Einstiegspunkt für das bisherige Verfahren in das Untergruppengitter möglichst nahe der tatsächlichen Galoisgruppe zu wählen. Als Voraussetzung für einen solchen Quereinstieg muß gewährleistet werden, daß die Galoisgruppe $\mathcal{G}(f, K)$ Untergruppe der als Einstiegspunkt gewählten Gruppe G ist, und zwar als Permutationsgruppe der ge-

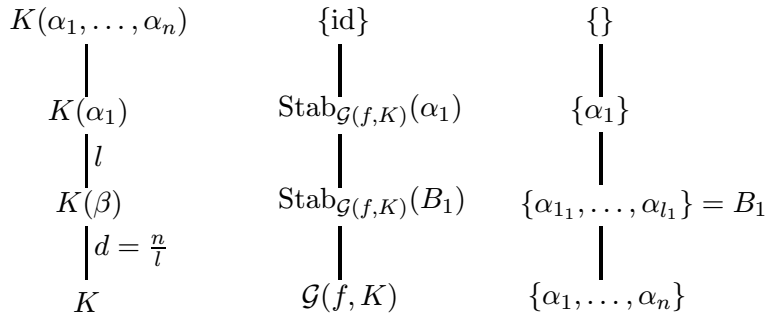
wählten Anordnung der Nullstellen von f. Eine solche Vorgehensweise läßt sich für imprimitive transitive Galoisgruppen realisieren:

Sei zunächst wieder R ein Integritätsring mit Eins, der ganzabgeschlossen in seinem Quotientenkörper K ist, und $f(x) \in R[x]$ ein normiertes, separables, irreduzibles Polynom vom Grad n. Da die Galoisgruppe $\mathcal{G}(f,K)$ transitiv auf der Menge der Nullstellen $\alpha = \alpha_1, \ldots, \alpha_n \in N(f,K)$ von f operiert, ist eine Unterteilung in imprimitive und primitive Gruppen möglich. Diese Eigenschaften von $\mathcal{G}(f,K)$ wurden bisher weitgehend unberücksichtigt gelassen. Wäre es möglich, ausgehend von dem Polynom f, nähere Informationen über die Blocksysteme der Galoisgruppe zu erhalten, so können diese einerseits dazu genutzt werden, die Menge der in Frage kommenden Permutationsgruppen einzuschränken. Andererseits läßt sich nach dem Satz von Krasner und Kaloujnine (vgl. Satz 1.10) eine transitive imprimitive Permutationsgruppe mit einem nichttrivialen Blocksystem, welches aus d Blöcken der Länge l besteht, in ein Kranzprodukt der Form $S_l \wr S_d$ einbetten. Sind zusätzliche Informationen über die Operation innerhalb bzw. auf den Blöcken bekannt, so ist es möglich, die jeweilige Komponente des Kranzproduktes durch eine entsprechende transitive Untergruppe von S_l bzw. S_d zu ersetzen. Sind mehrere Blocksysteme vorhanden, so liegt die imprimitive Permutationsgruppe im Schnitt der zugehörigen Kranzprodukte. Somit stellt sich nun die Frage, wie wir für ein gegebenes Polynom $f(x) \in R[x]$ diese Informationen erhalten. Dazu erinnern wir an den Zusammenhang zwischen Teilkörpern von $K(\alpha)$ und Blöcken von $\mathcal{G}(f,K)$.

5.1. Satz. *Sei $f \in K[x]$ normiert, irreduzibel und separabel vom Grad n und α eine Nullstelle von f. Dann existiert eine Bijektion zwischen den Teilkörpern von $K(\alpha)$ vom Grad d und den Blöcken B der Länge l von $\mathcal{G}(f,K)$, die α enthalten. Zusätzlich gilt $n = d\,l$.*

Beweis. Analog wie Beweis zu Satz 4.11 in Klüners, [41]. □

Unter Beachtung von Satz 1.4 illustriert das folgende Diagramm unsere Situation:



Die Teilkörper von $K(\alpha)$ sind also genau die Fixkörper der Stabilisatoren der Blöcke B von $\mathcal{G}(f,K)$, die α enthalten. Jeder Teilkörper kann durch ein Paar von Polynomen $(m,w) \in R[x] \times K[x]$ dargestellt werden, wobei m das Minimalpolynom eines primitiven Elements β eines Teilköpers und w ein Polynom vom Grad kleiner n mit $w(\alpha) = \beta$ ist. Das Polynom w wird aufgrund seiner Eigenschaft auch als Einbettungspolynom bezeichnet. Wir spezialisieren den Sachverhalt aus Satz 5.1 im Hinblick auf unsere geplante Anwendung:

5.2. Satz. *Seien $E_1 = K(\beta)$ und $E_2 = K(\alpha)$ mit $K \subseteq E_1 \subseteq E_2$ und $m(x), f(x) \in R[x]$ die zugehörigen Minimalpolynome. Sei $w(x) \in K[x]$ mit $w(\alpha) = \beta$. Die Konjugierten von α und β werden mit $\alpha_1, \ldots, \alpha_n \in N(f,K)$ und $\beta_1, \ldots, \beta_d \in N(m,K)$ bezeichnet. Setze $B_i = \{\, \alpha_j \mid w(\alpha_j) = \beta_i \,\}$. Dann gilt:*

(i) Die B_i liefern ein zu E_1 gehöriges Blocksystem der Galoisgruppe $\mathcal{G}(f,K)$ der Länge d. Es gilt $n = |\, B_i \,| \, d$ für $1 \leq i \leq d$.

(ii) Die Galoisgruppe der Erweiterung E_1/K ist, aufgefaßt als Permutationsgruppe der $\beta_1, \ldots, \beta_d$, äquivalent zur Permutationsdarstellung von $\mathcal{G}(f,K)$ auf der Menge $B_1, \ldots, B_d$ unter der Abbildung $\theta : \beta_i \longmapsto B_i$.

Beweis. (i) Sei $\sigma \in \mathcal{G}(f,K)$ mit $\sigma(\beta_i) = \beta_k$ und $\gamma \in B_i$. Dann gelten die folgenden Äquivalenzen:

$$\begin{aligned} \gamma \in B_i &\Leftrightarrow w(\gamma) = \beta_i \\ &\Leftrightarrow \sigma(w(\gamma)) = w(\sigma(\gamma)) = \beta_k \\ &\Leftrightarrow \sigma(\gamma) \in B_k. \end{aligned}$$

Aus den obigen Äquivalenzen und der Transitivität von $\mathcal{G}(f,K)$ folgt $n = |\, B_i \,| \, d$ für $1 \leq i \leq d$.

(ii) Die Gruppe $\mathcal{G}(m,K)$ ist äquivalent zu der Permutationsdarstellung der Gruppe $\mathcal{G}(f,K)$ bezüglich der B_i unter der Abbildung $\theta : \beta_i \longmapsto B_i$, weil $K(\beta_i) = Fix(K(\alpha_1, \ldots, \alpha_n), \mathrm{Stab}_{\mathcal{G}(f,K)}(B_i))$ gilt und somit dann $\mathcal{G}(m,K) \cong \mathcal{G}(f,K)/\cap_{i=1}^{d} \mathrm{Stab}_{\mathcal{G}(f,K)}(B_i)$ folgt. □

Damit können wir nun einen allgemeinen Algorithmus zur Galoisgruppenberechnung mittels Teilkörperberechnung angeben. Im Anschluß gehen wir dann speziell auf die von uns betrachteten Körper aus Kapitel 3 und Kapitel 4 ein.

5.3. Algorithmus. *(Galoisgruppenberechnung mittels Teilkörperberechnung)*

Eingabe: *Ein normiertes, irreduzibles, separables Polynom $f \in R[x]$ vom Grad n.*

Ausgabe: *Gruppe $T \in \mathcal{L}$ und Nullstellenanordnung, so daß $\mathcal{G}(f,K) \leq T$.*

1. *(Schritte aus Algorithmus 2.20) Durchlaufe die Schritte 1 bis 5 von Algorithmus 2.20.*

2. *(Teilkörperberechnung) Berechne Minimalpolynome* $m_1, \ldots, m_r$ *der Teilkörper von* $K(\alpha)$*, (*α *ist Nullstelle von* f*), und Einbettungspolynome* $w_1, \ldots, w_r$ *mit Hilfe des Teilkörperalgorithmus.*

3. *(Primitivität?) Ist* $r = 0$*, so ist* $\mathcal{G}(f, K)$ *eine primitive Permutationsgruppe. Ausgabe von* $T \leftarrow G$ *und Nullstellenanordnung* $\alpha_1, \ldots, \alpha_n$*. Terminiere. Sonst setze* $i \leftarrow 1$*.*

4. *(Schleife über die* m_i*) Für jedes* $i \leq r$ *mache:*

5. *(Nullstellen in Blöcken) Setze* $d_i \leftarrow Grad\ m_i$ *und* $l_i \leftarrow n/d_i$*. Die Galoisgruppe besitzt ein Blocksystem* $\mathcal{B}_i = \{B_1, \ldots, B_{d_i}\}$ *mit Blöcken der Länge* l_i*. Berechne Nullstellenaufteilung der Nullstellen von* f *auf die Blöcke* $B_1, \ldots, B_{d_i}$ *mit Hilfe des Einbettungspolynoms* w_i *nach Satz 5.2.*

6. *(Kranzprodukt) Bilde* $U_i = S_{l_i} \wr S_{d_i}$ *und bestimme Permutation* $\sigma \in S_n$*, die das Blocksystem von* U_i *auf das Blocksystem* $\mathcal{B}_i$ *abbildet.*

7. *(Konjugiere Kranzprodukt) Setze* $U_i \leftarrow \sigma U_i \sigma^{-1}$*. Nun gilt* $\mathcal{G}(f, K) \leq U_i$*.*

8. *(Nächstes* m_i*?) Ist* $i < r$*, so setze* $i \leftarrow i + 1$ *und wiederhole ab Schritt 4.*

9. *(Schnittbildung) Setze* $G \leftarrow G \cap \bigcap_{i=1}^{r} U_i$*.*

10. *(Identifikation) Identifiziere* G *mit* $T \in \mathcal{L}$*. Bestimme Permutation* τ*, so daß* $G = \tau T \tau^{-1}$ *gilt.*

11. *(Nullstellenanordnung anpassen) Setze* $\alpha_i \leftarrow \alpha_{\tau(i)}$*. Nun gilt* $\mathcal{G}(f, K) \leq T$*. Ausgabe von* T *und Nullstellenanordnung* $\alpha_1, \ldots, \alpha_n$*. Terminiere.*

5.4. Bemerkung. (i) Nach Satz 5.2 (ii) entspricht die Operation der Galoisgruppe $\mathcal{G}(f, K)$ auf den Blöcken $B_1, \ldots, B_{d_i}$ der Operation der Galoisgruppe der Minimalpolynome m_i, die die Teilkörper erzeugen, auf deren Nullstellen. Folglich läßt sich $\mathcal{G}(f, K)$ in ein Kranzprodukt der Form $S_{l_i} \wr \mathcal{G}(m_i, K)$ einbetten und wir können Algorithmus 5.3 erweitern: Durch Berechnung der Galoisgruppe $\mathcal{G}(m_i, K)$ als Permutationsgruppe der Nullstellen $\beta_1, \ldots, \beta_{d_i} \in N(m_i, K)$ in Schritt 5 und Umnumerierung der Blöcke B_i bezüglich des Isomorphismus $\theta : \beta_i \longmapsto B_i$ aus Satz 5.2 (ii), können wir in Schritt 6 $U_i = S_{l_i} \wr \mathcal{G}(m_i, K)$ setzen und somit noch bessere Annäherungen an die eigentliche Galoisgruppe $\mathcal{G}(f, K)$ erhalten.

(*ii*) Ähnliche Verbesserungen lassen sich durch Berechnung der relativen Galoisgruppe $\mathcal{G}(m_\alpha, K(\beta))$ des Minimalpolynoms von α über $K(\beta)$ erhalten. In diesem Fall kann $U_i = \mathcal{G}(m_\alpha, K(\beta)) \wr S_{d_i}$ verwendet werden.

Wichtigster Bestandteil des obigen Verfahrens ist das Vorhandensein eines Algorithmus zur Berechnung von Teilkörpern. Für Zahlkörper $F(\alpha)$ mit $F = \mathbb{Q}$ und rationale Funktionenkörper in einer Variablen über $\mathbb{Q}$ sind Algorithmen zur Berechnung von Teilkörpern (vgl. Klüners, [42], [43]) im Computeralgebrasystem KASH [38] implementiert, die uns Minimalpolynome und Einbettungspolynome in der gewünschten Form berechnen. Den Teilkörperalgorithmus für Zahlkörper der Form $F(\alpha)$ mit $F = \mathbb{Q}$ haben wir mit den in Kapitel 3 beschriebenen Methoden auf relative Zahlkörper $F(\alpha)$ mit $F = \mathbb{Q}(\delta)$ (δ wie in Sektion 3.1) erweitert und ebenfalls in dem Computeralgebrasystem KASH [38] implementiert. Somit konnte die Erweiterung der relativen Resolventenmethode mittels Teilkörperberechnung für diese Körper durchgeführt werden. Die Erweiterung von Algorithmus 5.3 durch Berechnung der Galoisgruppen der Teilkörper (Bemerkung 5.4 (*i*)) wird in unserer Implementierung für Grade $n > 12$ verwendet. Testdurchläufe haben gezeigt, daß bei Gruppen kleinerer Ordnung mit mehreren Blocksystemen der Einstieg an höherer Stelle und Durchlauf des Untergruppengitters meistens effizienter ist, als entsprechend viele Galoisgruppen der Teilkörper zu berechnen.

Wir merken an, daß Algorithmus 5.3 prinzipiell auch durchgeführt werden kann, wenn R nicht ganzabgeschlossen in seinem Quotientenkörper ist. Ist dies der Fall, so muß im Schritt 1 getestet werden, ob $\mathrm{disc}(f)$ Quadrat eines Elements in $Cl(R, K)$ ist. Implementationstechnisch wird überprüft, ob $\mathrm{disc}(f)$ Quadrat eines Elements in K ist, wenn $Cl(R, K)$ nicht explizit bekannt ist. Existiert nämlich ein Element in K mit dieser Eigenschaft, so muß es in $Cl(R, K)$ liegen. Dies ist von Bedeutung, wenn man im relativen Zahl- bzw. Funktionenkörperfall bezüglich Ordnungen arbeitet, die nicht maximal sind. Um für die in Kapitel 3 und Kapitel 4 betrachteten Körper eine Aufteilung der approximierten Nullstellen in Blöcke (Schritt 5 aus Algorithmus 5.3) konkret durchführen zu können, benötigen wir Aussagen über die Nenner der Einbettungspolynome.

5.5. Satz. *Sei $F = \mathbb{Q}(\delta)$ ein algebraischer Zahlkörper mit Minimalpolynom $h(x) \in \mathbb{Z}[x]$, $\mathfrak{o}$ eine Ordnung von F und $f(x) \in \mathfrak{o}[x]$ ein normiertes, irreduzibles Polynom vom Grad n mit Nullstelle $\alpha \in N(f, F)$. Sei $F(\beta)$ ein Teilkörper von $F(\alpha)$ mit einem über $\mathbb{Z}$ ganzalgebraischen Element β und einem Einbettungspolynom $w(x) \in F[x]$ vom Grad kleiner n mit $w(\alpha) = \beta$. Dann folgt $w(x) \in \mathfrak{o}_{(d)}[x]$ für $d := \mathrm{disc}(\mathfrak{o})\mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$.*

Beweis. Nach Neukirch [62], Kapitel I, §2, Satz 2.9 gilt $\mathfrak{o}_F \subseteq \mathfrak{o}_{(d)}$ und $\mathfrak{o}_{F(\alpha)} \subseteq \mathfrak{o}_F[\alpha]_{(d)}$. Da β ganzalgebraisch über $\mathbb{Z}$ ist, folgt $\beta \in \mathfrak{o}_{F(\alpha)} \subseteq \mathfrak{o}_{(d)}[\alpha]$, und somit

$w(x) \in \mathfrak{o}_{(d)}[x]$. □

An dieser Stelle zeigt sich nun, warum wir in Abschnitt 3.2 bei der Wahl des Primideals für die darunterliegende Primzahl $p \nmid \mathrm{disc}(\mathfrak{o})\mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$ gefordert hatten. Sei nun die Situation wie in Bemerkung 3.11 gegeben, d.h. seien $p \in \tilde{\mathfrak{p}} \subset \mathfrak{o}$ das unverzweigte Primideal vom Grad eins mit $p \nmid \mathrm{disc}(\mathfrak{o})\mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$ und $\mathbb{Z}[\rho]$ wie in Diagramm (3.12). Mit $\tilde{f}, \tilde{m} \in \mathbb{Z}[x]$ bezeichnen wir Approximationen von $f \in \mathfrak{o}[x]$ und $m \in \mathfrak{o}_{(d)}[x]$ mit $f - \tilde{f} \equiv 0 \bmod \tilde{\mathfrak{p}}$ und $m - \tilde{m} \equiv 0 \bmod \tilde{\mathfrak{p}}\mathfrak{o}_{(d)}$. Die Nenner der Koeffizienten des Polynoms $w \in \mathfrak{o}_{(d)}[x]$ lassen sich aufgrund unserer Voraussetzungen an die Primzahl p nach dem obigen Satz modulo $\tilde{\mathfrak{p}}\mathfrak{o}_{(d)}$ invertieren, und wir können das Polynom w durch ein Polynom $\tilde{w}$ in $\mathbb{Z}[x]$ mit $w - \tilde{w} \equiv 0 \bmod \tilde{\mathfrak{p}}\mathfrak{o}_{(d)}$ approximieren. Wurde das Primideal $\tilde{\mathfrak{p}}$ so gewählt, daß $\mathrm{disc}(m) \notin \tilde{\mathfrak{p}}\mathfrak{o}_{(d)}$ für die Diskriminante des Minimalpolynoms $m(x) \in \mathfrak{o}_{(d)}[x]$ des Teilkörpers $F(\beta)$ gilt, so sind die approximierten Nullstellen von $\tilde{m}$ und von $\tilde{f}$ im Restklassenkörper $\mathbb{Z}[\rho]/p\mathbb{Z}[\rho]$ verschieden. Die Nullstellenapproximationen von $\tilde{m} \bmod p\mathbb{Z}[\rho]$ erhalten wir dann durch Auswertung von $\tilde{w} \bmod p\mathbb{Z}[\rho]$ an den Nullstellenapproximationen von $\tilde{f} \bmod p\mathbb{Z}[\rho]$ und die Aufteilung in Blöcke erfolgt ebenfalls mittels des Polynoms $\tilde{w} \bmod p\mathbb{Z}[\rho]$.

Analoge Aussagen gelten auch im Funktionenkörperfall.

5.6. Satz. *Sei $F = K(t, \delta)$, $K \in \{\mathbb{F}_q, \mathbb{Q}\}$ ein algebraischer Funktionenkörper mit Minimalpolynom $h(t, x) \in R[t][x]$, $R \in \{\mathbb{F}_q, \mathbb{Z}\}$. Sei $f(x) \in R[t, \delta][x]$ normiert, irreduzibel und separabel vom Grad n mit Nullstelle $\alpha \in N(f, F)$. Darüber hinaus sei $F(\beta)$ ein Teilkörper von $F(\alpha)$ mit einem über $R[t]$ ganzalgebraischen Element β und einem Einbettungspolynom $w(x) \in F[x]$ vom Grad kleiner n mit $w(\alpha) = \beta$. Dann folgt $w(x) \in R[t]_{(d(t))}[\delta][x]$ für $d(t) := \mathrm{disc}(h)\mathrm{N}_{F/K(t)}(\mathrm{disc}(f))$.*

Genauso wie nach Satz 1.14 die Galoisgruppe $\mathcal{G}(\bar{f}, \bar{F}_{\mathcal{P}})$ Untergruppe der Galoisgruppe $\mathcal{G}(f, F)$ ist, erhalten wir für die Teilkörper von $F(\alpha)$: Ist $F(\beta)$ ein Teilkörper von $F(\alpha)$ mit Minimalpolynom $m \in F[x]$, so ist der von einer Nullstelle von $\bar{m} \in \bar{F}_{\mathcal{P}}[x]$ mit $\bar{m} := m \bmod \mathcal{P}$ erzeugte Körper Teilkörper von $\bar{F}_{\mathcal{P}}(\bar{\alpha})$. Die Umkehrung dieser Aussage gilt nicht. Nach Wahl der Stelle $\mathcal{P}$ im Fall $F = \mathbb{Q}(t, \delta)$ (vgl. Bemerkung 4.56) sind die Voraussetzungen von Satz 5.5 für $\bar{F}_{\mathcal{P}} = \mathbb{Q}(\bar{\delta}_1), \bar{h} \in \mathbb{Z}[x], \bar{f} \in \mathbb{Z}[\bar{\delta}_1][x]$ und $\bar{w} \in F[x]$ mit $\bar{w} := w \bmod \mathcal{P}$ erfüllt. Somit können wir die Routinen des Zahlkörperfalls auf die spezialisierten Minimalpolynome der Teilkörper von $\mathbb{Q}(t, \delta)(\alpha)$ anwenden, um eine Aufteilung der Nullstellenapproximationen in Blöcke zu erhalten. Im Funktionenkörperfall über endlichen Körpern erfolgt die Vorgehensweise dagegen analog zum Zahlkörperfall. Wir vermerken somit:

5.7. Bemerkung. Im Zahlkörperfall muß zusätzlich bei der Wahl des Primideals $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ beachtet werden, daß $\mathrm{disc}(m) \notin \tilde{\mathfrak{p}}\mathfrak{o}_{(d)}$ für das erzeugende Polynom jedes Teilkörpers $F(\beta)$ von $F(\alpha)$ gilt. Dies kann durch Wahl einer Primzahl p mit $p \nmid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(m))$ erreicht werden. Analog wählt man im Funktionenkörperfall ein normiertes Primpolynom $p(t) \in R[t]$, $R \in \{\mathbb{F}_q, \mathbb{Z}\}$, welches zusätzlich zu den Bedingungen aus (4.34) bzw. (4.56) nicht die Norm $\mathrm{N}_{F/K(t)}(\mathrm{disc}(m))$, $K \in \{\mathbb{F}_q, \mathbb{Q}\}$ teilt. Darüber hinaus sind im Fall $F = \mathbb{Q}(t, \delta)$ für die Primzahl p, bezüglich derer die Einbettung von $N(\bar{f}, \bar{F}_{\mathcal{P}})$ nach $\mathbb{Q}_p(\rho)$ (vgl. (4.39)) realisiert wird, die gleichen Kriterien wie im Zahlkörperfall zu beachten.

5.2 Verkürzte Nebenklassenrepräsentantensysteme

Im vorherigen Kapitel haben wir eine Verbesserung des Verfahrens von Stauduhar für imprimitive Gruppen dargestellt, welche die Probleme für diese Gruppen im wesentlichen löst. Somit verbleiben die primitiven Gruppen. Im folgenden beschreiben wir eine von den Eigenschaften der Permutationsgruppe unabhängige Lösung für das Problem großer Nebenklassenvertretersysteme und großer Schranken für das Lifting der $\mathfrak{p}$-adischen bzw. $\mathcal{P}$-adischen Nullstellenapproximationen. Die Methoden lassen sich also allgemein für primitive als auch imprimitive Gruppen anwenden. Für große Grade n (≥ 11) erhält man die besten Ergebnisse, wenn die Methoden aus diesem und dem nächsten Abschnitt miteinander kombiniert werden.

Sei nun wieder die Situation wie in Abschnitt 5.1 gegeben. Wir beginnen mit der Definition von verkürzten Nebenklassenrepräsentantensystemen. Sei $f \in R[x]$ normiert, irreduzibel und separabel mit Nullstellen $\alpha_1, \ldots, \alpha_n \in N(f, K)$. Wir betrachten die Galoisgruppe von f als Permutationsgruppe der Nullstellen und nehmen an, daß wir eine transitive Permutationsgruppe $G \leq S_n$ mit $\mathcal{G}(f, K) \leq G$ kennen. Für eine maximale transitive Untergruppe H von G müssen wir im Verfahren von Stauduhar $\mathcal{G}(f, K) \leq \sigma H \sigma^{-1}$ für jeden Nebenklassenrepräsentanten $\sigma \in G//H$ testen. Ist zusätzlich eine Permutationsgruppe U mit $U \leq \mathcal{G}(f, K)$ bekannt, so sind Verbesserungen möglich, da wir uns auf die $\sigma \in G//H$ beschränken können, für die $U \leq \sigma H \sigma^{-1}$ gilt.

5.8. Definition. Sei $H < G \leq S_n$ und U eine Untergruppe von $\mathcal{G}(f, K) \leq G$ bezüglich der gewählten Anordnung der Nullstellen des Polynoms $f \in R[x]$. Dann nennen wir die Menge

$$(G/H)_U := \{\, \sigma H \in G/H \mid U \leq \sigma H \sigma^{-1} \,\}$$

ein verkürztes System von Nebenklassen von H in G bezüglich U. Mit $(G//H)_U$ bezeichnen wir das zugehörige vollständige Nebenklassenrepräsentantensystem von $(G/H)_U$.

Eine Permutationsgruppe U mit dieser Eigenschaft kann auf verschiedene Weisen erhalten werden:

Wir gehen wie im Kapitel 3 und Kapitel 4 vor. Sei nun R nicht nur ganzabgeschlossen in K, sondern ein Dedekindring und $\mathcal{K}$ eine Vervollständigung von K bezüglich eines nichttrivialen Absolutbetrages. Darüber hinaus sei die Erweiterung des Zerfällungskörpers $N(f,\mathcal{K})$ über $\mathcal{K}$ für nicht-archimedische Beträge unverzweigt. Wir betrachten die Nullstellen $\alpha_1,\ldots,\ \alpha_n$ von f und den Zerfällungskörper $N(f,K)$ eingebettet in $N(f,\mathcal{K})$. Nach Lorenz [53], §12, Satz 1 ist $\mathcal{G}(f,\mathcal{K})$ eine Untergruppe von $\mathcal{G}(f,K)$ bezüglich der Operation auf den Nullstellen α_i, $(1 \leq i \leq n)$. Wurde $\mathcal{K}$ durch Vervollständigung mittels eines Primideals $0 \neq \mathfrak{p} \subset R$ mit $\mathrm{disc}(f) \notin \mathfrak{p}$ erhalten, so können wir modulo $\mathfrak{p}$ reduzieren und erhalten $N(\bar{f},R/\mathfrak{p}) \cong Cl(\mathcal{R},N(f,\mathcal{K}))/\mathfrak{p}\,Cl(\mathcal{R},N(f,\mathcal{K}))$, wobei $\mathcal{R}$ die Vervollständigung von R bezüglich $\mathfrak{p}$ bezeichne. Die Reduktionsabbildung von $Cl(\mathcal{R},N(f,\mathcal{K})) \to N(\bar{f},R/\mathfrak{p})$ bezeichnen wir ebenfalls mit $\bar{\cdot}$. Nach Lorenz [52], §24, Satz 3 ist dann $\mathcal{G}(f,\mathcal{K}) = \mathcal{G}(\bar{f},R/\mathfrak{p})$ unter der Ziffernzuordnung $\alpha_i \mapsto \bar{\alpha}_i$ für $1 \leq i \leq n$. Um Untergruppen von $\mathcal{G}(f,K)$ zu erhalten, können wir also $\mathcal{G}(f,\mathcal{K})$ oder $\mathcal{G}(\bar{f},R/\mathfrak{p})$ bestimmen.

Wir bemerken den folgenden allgemeinen Sachverhalt (vgl. Korollar 1.15): Ist $f \in R[x]$ ein separables Polynom mit Faktorisierung $f = \prod_{j=1}^{u} f_j$ in $\mathcal{K}[x]$ und $\mathcal{G}(f,\mathcal{K})$ zyklisch mit Erzeuger τ, so besitzt τ den Zykeltyp $(\deg(f_1),\ldots,\deg(f_u))$. Ist $\mathcal{K} = \mathbb{R}$, so ist $N(f,\mathcal{K}) = \mathbb{R}$ oder $N(f,\mathcal{K}) = \mathbb{C}$, abhängig davon, ob f komplexe Nullstellen hat oder nicht. Die Galoisgruppe von $\mathbb{C}/\mathbb{R}$ wird von der komplexen Konjugation erzeugt, so daß $\mathcal{G}(f,\mathbb{R})$ den Erzeuger $((\alpha_1),\ldots,(\alpha_{r_1}),(\alpha_{r_1},\alpha_{r_1+r_2}),\ldots,(\alpha_{r_1+r_2},\alpha_{r_1+2r_2}))$ besitzt. Ist $\mathcal{K} = \mathbb{Q}_p$ (dann $q := p$) oder $\mathcal{K} = \mathbb{F}_q((\pi))$, so ist der Erzeuger von $\mathcal{G}(f,\mathcal{K})$ der Frobenius-Automorphismus, welcher die Zykel $(\alpha_{i_1},\ldots,\alpha_{i_{\deg(f_j)}})$ enthält, wobei $\bar{\alpha}_{i_j}^{q} = \bar{\alpha}_{i_{j+1}}$ gilt. Wie bereits gesehen, hat der Frobenius-Automorphismus damit die Ordnung $\mathrm{kgV}(\deg(f_1),\ldots,\deg(f_u))$. Für $\mathcal{K} = \mathbb{Q}(\bar{\delta}_1)((\pi))$ wie in Kapitel 4 ist der Restklassenkörper $\mathbb{Q}(\bar{\delta}_1)$, und wir wenden die Methode mittels einer weiteren Reduktion für $\bar{f}$ statt f erneut an.

Obwohl die Gruppe U sehr klein ist, lassen sich auf diesem Weg große Einschränkungen der zu testenden Nebenklassenrepräsentanten und damit große Laufzeitbeschleunigungen erreichen.

5.9. Beispiel. Sei H die Gruppe $\mathrm{PSL}_2(p)$, welche maximal in $G := A_{p+1}$ für $p \neq 2,3,11,23$ ist. Für den Index von H in G gilt $[\,G:H\,] = (p-2)!$. Wird U von einem Element der Ordnung p erzeugt, so folgt $|(G//H)_U| = 1$ (vgl. [30]).

Hier zeigt sich ein weiterer Vorteil der Verwendung $\mathfrak{p}$-adischer bzw. $\mathcal{P}$-adischer Nullstellenapproximationen. Haben wir ein Primideal $\mathfrak{p}$ bzw. eine Stelle $\mathcal{P}$ gewählt, für die sich das zugehörige Nebenklassenrepräsentantensystem nicht reduzieren läßt, so sind wir in der Lage, ein anderes Primideal oder eine andere Stelle zu wählen. Im komplexen Fall ist dies dagegen nicht möglich. Insbesondere ergeben sich für total reelle Polynome grundsätzlich keine Verbesserungen.

5.10. Satz. *Es gelten die Voraussetzungen von Satz 2.4. Gibt es $\sigma_1, \sigma_2 \in G//H$ mit $\sigma_1 \neq \sigma_2$, so daß $(\sigma_1 F)(\alpha_1, \ldots, \alpha_n) \in R$ und $(\sigma_1 F)(\alpha_1, \ldots, \alpha_n) \neq (\sigma_2 F)(\alpha_1, \ldots, \alpha_n)$ gilt, so folgt $\mathcal{G}(f, K) \lneqq G$.*

Beweis. Wir nehmen an, daß $\mathcal{G}(f, K) = G$ gilt. Da $\mathrm{Stab}_G(F) = H$ folgt, daß $\tilde{\gamma} := F(\alpha_1, \ldots, \alpha_n)$ ein Element des Fixkörpers $Fix(N(f, K), H)$ ist. Deshalb erhalten wir für das charakteristische Polynom $char_{\tilde{\gamma}}(X)$ von $\tilde{\gamma}$ bezüglich der Erweiterung $Fix(N(f, K), H)/K$:

$$\begin{aligned} char_{\tilde{\gamma}}(X) &= \prod_{\sigma \in G//H} (X - \sigma F(\alpha_1, \ldots, \alpha_n)) \\ &= R_{(G,H,F)}(X). \end{aligned}$$

Die Annahme $\mathcal{G}(f, K) = G$ geht hier bei der ersten Gleichung ein. Andererseits gilt

$$char_{\tilde{\gamma}}(X) = (m_{\tilde{\gamma}}(X))^l \text{ für ein } l \in \mathbb{Z}_{>0},$$

wobei mit $m_{\tilde{\gamma}}(X)$ das Minimalpolynom von $\tilde{\gamma}$ über K bezeichnet sei. Da $(X - \gamma) \mid char_{\tilde{\gamma}}(X) = (m_{\tilde{\gamma}}(X))^l$ in $R[X]$ folgt, daß $char_{\tilde{\gamma}}(X) = (X - \gamma)^{[G:H]}$ ist im Widerspruch zur Voraussetzung, daß es eine Nullstelle von $R_{(G,H,F)}(X)$ gibt, welche von γ verschieden ist. Somit folgt $\mathcal{G}(f, K) \lneqq G$. □

5.11. Bemerkung. In der Situation von Satz 5.10 folgt nicht, daß $\mathcal{G}(f, K) \leq H$ gilt.

Satz 5.10 läßt sich in der Praxis folgendermaßen anwenden: Man betrachtet alle maximalen Untergruppen der Permutationsgruppe G mittels verkürzter Nebenklassenrepäsentantensysteme. Ist nur ein Abstieg in eine dieser Untergruppen möglich, so ist dieser Abstieg bewiesen, wenn die Voraussetzung von Satz 5.10 für diese Untergruppe zutrifft. Für die uns interessierenden primitiven Gruppen vom Grad $9 \leq n \leq 23$ haben wir den Vorteil, daß es in den meisten Fällen überhaupt nur eine maximale Untergruppe in der S_n bzw. A_n gibt.

Wir nehmen nun an, daß $U = \langle \tau \rangle \leq \mathcal{G}(f, K)$ gilt. Eine unmittelbar einsichtige, wenngleich auch recht unpraktische Methode zur Berechnung eines verkürzten

Nebenklassenrepräsentantensystems wäre, zuerst alle Nebenklassenrepräsentanten $\sigma \in G//H$ zu erzeugen und dann die herauszufiltern, welche der Bedingung $\tau \in \sigma H \sigma^{-1}$ genügen. Deshalb suchen wir nach anderen Möglichkeiten einer effizienten Berechnung von verkürzten Nebenklassenrepräsentantensystemen. Der folgende Algorithmus stellt eine große Verbesserung gegenüber der eben beschriebenen Vorgehensweise dar. Wir verwenden hierfür etwas mehr Gruppentheorie. Für eine Permutationsgruppe G und eine Permutation $\tau \in S_n$ sei mit $C_G(\tau) := \{ \sigma \in G \mid \sigma\tau = \tau\sigma \}$ der Zentralisator von τ in G bezeichnet.

5.12. Algorithmus. *(Verkürztes Nebenklassenrepräsentantensystem)*

Eingabe: $U \leq H < G \leq S_n$ *mit* $U = \langle \tau \rangle$.

Ausgabe: $(G//H)_U$.

1. *(Konjugationsklassen) Berechne die Menge $\mathcal{C}$ der H-Konjugationsklassen von H, welche denselben Zykeltyp wie τ haben.*
2. *(Existiert $\sigma \in G$ mit $\sigma^{-1}\tau\sigma \in C$?) Für jedes $C \in \mathcal{C}$ berechne eine Permutation $\sigma \in G$ mit $\sigma^{-1}\tau\sigma \in C$, falls eine solche Permutation existiert. Die Menge aller σ bezeichnen wir mit $\mathcal{R}$.*
3. *(Nebenklassenrepräsentantensysteme der Zentralisatoren) Für jedes $\sigma \in \mathcal{R}$ berechne die Menge $A_\sigma := C_G(\tau)//C_{\sigma H \sigma^{-1}}(\tau)$.*
4. *(Ende) Ausgabe von $\{ a\sigma \mid \sigma \in \mathcal{R},\, a \in A_\sigma \} = (G//H)_U$.*

Beweis. Die Korrektheit des Algorithmus erhalten wir aus den folgenden Überlegungen:

1. Für $\sigma \in G$ ist $\langle \tau \rangle \leq \sigma H \sigma^{-1}$ äquivalent zu $\sigma^{-1}\tau\sigma \in H$. Folglich liegt $\sigma^{-1}\tau\sigma \in H$ in einem $C \in \mathcal{C}$.
2. Sei $\sigma \in \mathcal{R}$ mit $\sigma^{-1}\tau\sigma \in C$. Für $\tilde{\sigma} \in G$ folgt, daß
$$\begin{aligned} \tilde{\sigma}^{-1}\tau\tilde{\sigma} \in C &\iff \text{es existiert } \rho \in H : \tilde{\sigma}^{-1}\tau\tilde{\sigma} = \rho^{-1}\sigma^{-1}\tau\sigma\rho \\ &\iff \tilde{\sigma} \in C_G(\tau)\sigma H. \end{aligned}$$
Dann gilt $\{ \sigma \in G \mid \sigma^{-1}\tau\sigma \in H \} = \dot{\cup}_{\sigma \in \mathcal{R}} C_G(\tau)\sigma H$ mit $\mathcal{R}$ wie in Algorithmus 5.12.
3. Da $C_G(\tau) = \dot{\cup}_{a \in A_\sigma} a C_{\sigma H \sigma^{-1}}(\tau)$ für jedes $\sigma \in \mathcal{R}$ und $C_{\sigma H \sigma^{-1}}(\tau)\sigma H = \sigma H$ erhalten wir $\dot{\cup}_{\sigma \in \mathcal{R}} C_G(\tau)\sigma H = \dot{\cup}_{\sigma \in \mathcal{R}} (\dot{\cup}_{a \in A_\sigma} a\sigma H)$. Die letzte Vereinigung ist disjunkt, da
$$\begin{aligned} a_1\sigma H = a_2\sigma H &\iff a_2^{-1}a_1 \in C_G(\tau) \cap \sigma H \sigma^{-1} \\ &\iff a_2^{-1}a_1 \in C_{\sigma H \sigma^{-1}}(\tau), \end{aligned}$$
was nach der Wahl von A_σ nicht möglich ist.

□

5.3 Verifikation von Inklusionstests mit großem Index

Bisher haben wir das Problem von großen Nebenklassenrepräsentantensystemen durch die Betrachtung von verkürzten Nebenklassenrepräsentantensystemen gelöst. Um bewiesene Ergebnisse zu erhalten, müssen wir aber die $\mathfrak{p}$-adischen bzw. $\mathcal{P}$-adischen Approximationen bis zu einer Schranke k bzw. l liften, die linear von Index $[\,G:H\,]$ abhängt (in Satz 5.10 müssen wir $(\sigma_1 F)(\alpha_1,\ldots,\alpha_n) \in R$ beweisen). Aus Effizienzgründen wäre es wünschenswert, das Liften zur Nullstellenpräzision für Gruppenpaare G, H mit sehr großem Index zu vermeiden. Dies kann grob gesagt auf folgende Art und Weise gemacht werden:

1. Berechne die Galoisgruppe des Polynoms $f \in R[x]$ mit der Methode von Stauduhar unter Verwendung von verkürzten Nebenklassenrepräsentantensystemen und heuristischen Schranken k' bzw. l' für das Lifting. Diese Vorgehensweise führt zu einem unbewiesenen Ergebnis.

2. Beweise oder widerlege das Ergebnis aus 1. unter Verwendung der absoluten Resolventenmethode.

Da das Verfahren von Stauduhar neben der Galoisgruppe auch die Operation der Gruppe auf den Nullstellen bestimmt, kann man bei der absoluten Resolventenmethode den umgekehrten Weg gehen: Anstatt r-set Resolventen zu faktorisieren, können wir die vermuteten Faktoren direkt berechnen, und der Beweisschritt besteht darin, zu testen, ob die berechneten Faktoren in $R[X]$ sind. Um auf Inklusion in der richtigen Konjugierten einer Untergruppe schließen zu können, benötigen wir außerdem die nächste Proposition und das darauffolgende Korollar:

5.13. Proposition. *Sei $G \leq S_n$ eine Permutationsgruppe und $F \in R[x_1,\ldots,x_n]$ ein Polynom und $\mathcal{O} := Orb_G(F)$. Bezeichne $\tau : G \longrightarrow S_{|\mathcal{O}|}$ die Permutationsdarstellung, welche durch Operation von G auf der Menge $\mathcal{O}$ gegeben ist. Dann gilt:*

(i) Die Gruppe $\tau(G)$ ist transitiv.

(ii) Die Operation auf der Menge $\mathcal{O}$ ist äquivalent zur Operation von G auf der Menge der linken Nebenklassen $G/\mathrm{Stab}_G(F)$.

(iii) $\mathrm{Kern}\,\tau = \bigcap_{\sigma\in G//\mathrm{Stab}_G(F)} \sigma\mathrm{Stab}_G(F)\sigma^{-1}$.

Beweis. (i) $\tau(G)$ operiert transitiv auf $\mathcal{O}$, wenn $\mathcal{O}$ nur aus einer Bahn unter den Permutationen von $\tau(G)$ besteht. Dies ist aber aufgrund der Definition von $\mathcal{O}$ der Fall. (ii) Folgt direkt aus dem Bahnensatz 1.2, vgl. auch Satz 2.21. (iii) Sei $g \in \mathrm{Kern}\,\tau$. Mittels (ii) erhalten wir $g\sigma\mathrm{Stab}_G(F) = \sigma\mathrm{Stab}_G(F)$ für alle $\sigma \in G//\mathrm{Stab}_G(F)$. Dies ist aber äquivalent zu $g \in \bigcap_{\sigma\in G//\mathrm{Stab}_G(F)} \sigma\mathrm{Stab}_G(F)\sigma^{-1}$. □

5.14. Korollar. *Sei* $F = x_1 \cdots x_r \in R[x_1, \ldots, x_n]$ *für* $r \leq n-1$ *und* $\mathcal{O} = Orb_{S_n}(F)$. *Dann ist die Permutationsdarstellung* $\tau : S_n \longrightarrow S_{|\mathcal{O}|}$ *treu.*

Beweis. Nach Proposition 5.13 gilt

$$\operatorname{Kern}\tau = \bigcap_{\sigma \in S_n // \operatorname{Stab}_{S_n}(F)} \sigma \operatorname{Stab}_{S_n}(F) \sigma^{-1}. \tag{5.15}$$

Die Untergruppe $\operatorname{Stab}_{S_n}(F) = S_r \times S_{n-r}$ fixiert das Polynom $F = x_1 \cdots x_r$ bzw. die r-elementige Teilmenge $\{1, \ldots, r\}$, und für jedes $\sigma \in S_n // \operatorname{Stab}_{S_n}(F)$ wird σF bzw. die r-elementige Teilmenge $\{\sigma(1), \ldots, \sigma(r)\}$ von $\sigma \operatorname{Stab}_{S_n}(F) \sigma^{-1}$ fixiert. Treten die Stabilisatoren aller r-elementigen Teilmengen der Menge $\{1, \ldots, n\}$ auf der rechten Seite von Gleichung (5.15) auf, so muß $\operatorname{Kern}\tau$ die Identität sein. Dies ist aber der Fall, da nach dem Bahnensatz 1.2 eine Bijektion zwischen der Menge der linken Nebenklassen von $\operatorname{Stab}_{S_n}(F)$ in S_n und der Bahn $\mathcal{O} = Orb_{S_n}(F)$ existiert. □

Damit ist die Voraussetzung von Korollar 2.7 an die Treue der Permutationsdarstellung erfüllt. Sei nun zum Beispiel H eine maximale transitive Untergruppe von G und $r \in \mathbb{Z}_{>0}$, so daß die Bahnen der r-elementigen Teilmengen von $\{1, \ldots, n\}$ bezüglich der Permutationen von H und G verschieden sind. Es gelte außerdem $\mathcal{G}(f, K) \leq G$. Damit sind auch die weiteren Voraussetzungen von Korollar 2.7 erfüllt. Ist der Inklusionsschritt zwischen G und H nicht bewiesen, so folgt nach Korollar 2.7 aus der Existenz eines echten Faktors der r-set Resolvente $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)}$ in $R[X]$, daß die Galoisgruppe in H enthalten ist. Sei nun eine Kette von Gruppeninklusionen $H_i < H_{i-1} < \cdots < H_1 < G$, $(i \in \mathbb{Z}_{>2})$ gegeben, bei der nur der erste Inklusionsschritt nicht bewiesen ist, aber alle anderen Inklusionen nach dem Verfahren von Stauduhar unter der Annahme, daß $\mathcal{G}(f, K) \leq H_1$ gilt, bewiesen sind. Aus dem Beweis von $\mathcal{G}(f, K) \leq H_1$ folgt dann $\mathcal{G}(f, K) = H_i$. Hier ist es meistens geschickter, eine r-set Resolvente zu wählen, welche die Gruppen G und H_i unterscheidet, anstelle der Gruppen G und H_1. Wie man anhand der Tabellen aus dem Anhang erkennt, kann man nämlich die Gruppen G und H_i oftmals schon durch Wahl eines wesentlich kleineren r unterscheiden, d.h. es brauchen nur Faktoren kleineren Grads einer r-set Resolvente kleineren Grads berechnet werden. Korollar 2.7 kann nun nicht direkt angewendet werden, da zwar die Orbitlängen verschieden sind, aber H_i nicht mehr maximal in G ist. Anhand von Satz 2.6 (ii) folgt aus der Existenz eines echten Faktors der r-set Resolvente in $R[X]$ und der Treue der Permutationsdarstellung, daß die Galoisgruppe zumindest Untergruppe von $\operatorname{Stab}_G(Orb_{H_i}(F))$ für geeignetes $F \in R[x_1, \ldots, x_n]$ wie zum Beispiel in Korollar 5.14 ist. Gilt nun $\operatorname{Stab}_G(Orb_{H_i}(F)) \leq H_1$, so ist das Ergebnis $\mathcal{G}(f, K) = H_i$ bewiesen. Mit den eben beschriebenen Methoden können wir also

im Nachhinein zeigen, daß der Inklusionstest unter Verwendung der heuristischen Schranken korrekt war.

In unserer Implementierung verwenden wir diese Methode für die Grade $n > 9$. Anstatt der Nullstellenpräzision benutzen wir im Zahlkörperfall eine heuristische Präzision von

$$k' = \max\{\ \min\{\ 10 \sum_{j=1}^{m} \log_p(2M_j),\ [\,G\!:\!H\,] \sum_{j=1}^{m} \log_p(2M_j)\ \},\ m \log_p(2^{\frac{m}{2}}(A^2+A)) + \sum_{j=1}^{m} \log_p(W_j)\ \} \tag{5.16}$$

und im Funktionenkörperfall

$$l' = \max\{\ \min\{-10 \sum_{j=1}^{s} \deg(P_j)M_j,\ -[\,G\!:\!H\,] \sum_{j=1}^{s} \deg(P_j)M_j\},\ s'(3A \min_{1\le j\le s}\{e_j\} - \min_{1\le j\le s}\{W_j\})\ \}. \tag{5.17}$$

In den folgenden Algorithmen wird der Verifikationsschritt für die Körper aus Kapitel 3 und Kapitel 4 beschrieben:

5.18. Algorithmus. *(Verifikation von Inklusionstests mit großem Index - Zahlkörperfall.)*

Eingabe: *Eine transitive Permutationsgruppe $G \le S_n$ mit $\mathcal{G}(f,F) \le G$, eine transitive Untergruppe $H < G$ und $r \in \mathbb{Z}_{>0}$, so daß die Bahnen der r-elementigen Teilmengen von $\{1,\dots,n\}$ bezüglich der Permutationen von H und G verschieden sind. Ein normiertes irreduzibles Polynom $f \in \mathfrak{o}[x]$ vom Grad n, wobei $\mathfrak{o}$ eine Ordnung des Zahlkörpers $F/\mathbb{Q}$, $[F:\mathbb{Q}] = m$ sei. Ein unverzweigtes Primideal $p \in \tilde{\mathfrak{p}} \subset \mathfrak{o}$ vom Grad eins wie in Bemerkung 3.11, so daß die r-set Resolvente modulo $\tilde{\mathfrak{p}}$ separabel ist. Nullstellenapproximationen $\alpha^*_{1,(\tilde{k})},\dots,\alpha^*_{n,(\tilde{k})} \in \mathbb{Z}[\rho]$ von $\iota_{\mathfrak{p}}(f) \in \mathbb{Z}_p[x]$ für $\tilde{k} \in \mathbb{Z}_{>0}$.*

Ausgabe: $\mathcal{G}(f,F) \ne H$ *oder* $\mathcal{G}(f,F) \le \mathrm{Stab}_G(\mathcal{O}) \lneqq G$.

1. *(Initialisierung)* $S := \{U \subseteq \{\alpha^*_{1,(\tilde{k})},\dots,\alpha^*_{n,(\tilde{k})}\} \mid |U| = r\}$.
2. *(Bahnberechnung) Berechne eine Bahn $\mathcal{O}$ von S unter den Permutationen von H, welche keine Bahn unter den Permutationen von G ist.*
3. *(r-set Resolvente) Für* $F(x_1,\dots,x_n) = x_1 \cdots x_r \in \mathbb{Z}[x_1,\dots,x_n]$ *berechne* $T(X) := R_{(S_n,S_r\times S_{n-r},F)}(X) \in \mathfrak{o}[X]$ *nach Algorithmus* P *aus Casperson, McKay [10] mittels der Koeffizienten von* $f \in \mathfrak{o}[x]$.

4. *(Faktor der Resolvente modulo $p\mathbb{Z}[\rho]$) Berechne $q_1 \in \mathbb{Z}[X]$ mit*

$$q_1 \equiv \prod_{U \in \mathcal{O}} (X - \prod_{\alpha^*_{i,(\tilde{k})} \in U} \alpha^*_{i,(\tilde{k})}) \bmod p\mathbb{Z}[\rho].$$

Existiert kein solches $q_1 \in \mathbb{Z}[X]$, dann Ausgabe $\mathcal{G}(f, F) \neq H$.

5. *(Kofaktor modulo $\tilde{\mathfrak{p}}$) Berechne $q_2 \in \mathbb{Z}[X]$ mit $T \equiv q_1 q_2 \bmod \tilde{\mathfrak{p}}$. Nach Voraussetzung an $\tilde{\mathfrak{p}}$ sind q_1, q_2 koprim modulo $\tilde{\mathfrak{p}}$.*

6. *(Koeffizientenschranke) Berechne obere Schranken M_j, $(1 \leq j \leq m)$ für die Größe der Konjugierten der Koeffizienten der Faktoren von $T(X) \in \mathfrak{o}[X]$ und $k \in \mathbb{Z}_{>0}$ mit $p^k > 2M_1$ im Fall $F = \mathbb{Q}$ bzw. $p^k > 2^{m^2/2} d_S^2 (A^2 + A)^m \prod_{j=1}^m W_j$ für $F \neq \mathbb{Q}$, wobei $d_S \in \mathbb{Z}_{>0}$ und $A, W_j \in \mathbb{R}$ wie in Kapitel 3.4.*

7. *(Hensel-Lifting) Berechne $\tilde{T} \in \mathbb{Z}[X]$ mit $\tilde{T} \equiv T \bmod \tilde{\mathfrak{p}}^k$. Lifte $\tilde{T} \equiv q_1 q_2 \bmod p\mathbb{Z}$ zu $\tilde{T} \equiv \tilde{q}_1 \tilde{q}_2 \bmod p^k\mathbb{Z}$, wobei die Koeffizienten von $\tilde{q}_1, \tilde{q}_2 \in \mathbb{Z}[X]$ in $[-(p^k - 1)/2, p^k/2]$ sind.*

8. *(Rekonstruktion) Ist $F = \mathbb{Q}$, so teste, ob der Absolutbetrag jedes Koeffizienten von $\tilde{q}_1$ kleiner gleich M_1 ist. Ist dies der Fall, so setze $Q_1 = \tilde{q}_1 \in \mathbb{Z}[X]$, ansonsten Ausgabe von $\mathcal{G}(f, F) \neq H$. Gilt $F \neq \mathbb{Q}$ rekonstruiere jeden Koeffizienten von $\tilde{q}_1 \in \mathbb{Z}[X]$ mittels des in Kapitel 3.4 beschriebenen Verfahrens zu $Q_1 \in \mathfrak{o}_F[X]$. Ist dies nicht möglich, so Ausgabe von $\mathcal{G}(f, F) \neq H$.*

9. *(Teilt Faktor Q_1 die Resolvente?) Teste, ob Q_1 zu einem echten Faktor von T in $\mathfrak{o}_F[X]$ korrespondiert. In diesem Fall Ausgabe von $\mathcal{G}(f, F) \leq \mathrm{Stab}_G(\mathcal{O}) \lneqq G$. Ansonsten Ausgabe von $\mathcal{G}(f, F) \neq H$.*

In Schritt 6 von Algorithmus 5.18 lassen sich wohlbekannte Schranken über die Größe der Koeffizienten der Faktoren von $T(X) \in \mathfrak{o}[X]$ verwenden, wie man sie bei Faktorisierungsalgorithmen findet (vgl. z.B. von zur Gathen, Gerhard [85], Corollary 6.33, Schranke von Mignotte für $F = \mathbb{Q}$ und Beauzamy [3], Pohst [67] für algebraische Zahlkörper). In unserer Implementierung benutzen wir das Resultat aus Beauzamy [3]:

5.19. Proposition. *Sei F ein algebraischer Zahlkörper mit Maximalordnung $\mathfrak{o}_F$ und $f(x) = \sum_{i=0}^n a_i x^i \in \mathfrak{o}_F[x]$ ein normiertes Polynom. Ist $g(x) = \sum_{r=0}^m b_r x^r \in \mathfrak{o}_F[x]$ normiert und ein Teiler von f in $\mathfrak{o}_F[x]$, so sind die Konjugierten der Koeffizienten von g beschränkt durch*

$$|b_r^{(j)}| \leq \frac{3^{\frac{3}{4}} 3^{\frac{n}{2}}}{2\sqrt{\pi}\sqrt{n}} \left(\sum_{i=0}^n \binom{n}{i}^{-1} |a_i^{(j)}|^2 \right)^{\frac{1}{2}}, \ (1 \leq j \leq r_1 + 2r_2).$$

Speziell für $\mathfrak{o}_F = \mathbb{Z}$ verwenden wir die einfacher zu berechnende obere Schranke $|b_r| \leq 2^m(n+1)^{\frac{1}{2}} \max_{0\leq i\leq n}\{|a_i|\}$ für die Absolutbeträge der Koeffizienten des Faktors.

5.20. Algorithmus. *(Verifikation von Inklusionstests mit großem Index - Funktionenkörperfall $F = K(t,\delta)$, $K \in \{\mathbb{F}_q, \mathbb{Q}\}$.)*

Eingabe: *Eine transitive Permutationsgruppe $G \leq S_n$ mit $\mathcal{G}(f,F) \leq G$, eine transitive Untergruppe $H < G$ und $r \in \mathbb{Z}_{>0}$, so daß die Bahnen der r-elementigen Teilmengen von $\{1,\ldots,n\}$ bezüglich der Permutationen von H und G verschieden sind. Ein in x normiertes, separables irreduzibles Polynom $f \in R[t,\delta][x] \subset F[x]$, $R \in \{\mathbb{F}_q, \mathbb{Z}\}$ vom Grad n, wobei $[F : K(t)] = m$ ist. Eine Stelle $\mathcal{P} \in \mathbb{P}(F)$ mit Primelement $p(t) = t - t_0 \in R[t_0][t]$, welche den Bedingungen (4.34) bzw. (4.56) genügt, so daß die r-set Resolvente modulo $\mathcal{P}$ separabel ist.*

$K = \mathbb{F}_q$: Nullstellenapproximationen $\alpha'_{1,(\tilde{l})},\ldots,\alpha'_{n,(\tilde{l})} \in \mathbb{F}_{q^{\deg(\mathcal{P})d}}[\pi]$ von $\iota_{\mathcal{P}}(f) \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[[\pi]][x]$ für $\tilde{l} \in \mathbb{Z}_{>0}$.

$K = \mathbb{Q}$: Nullstellenapproximationen $\alpha''_{1,(\tilde{k},\tilde{l})},\ldots,\alpha''_{n,(\tilde{k},\tilde{l})} \in \mathbb{Z}[\rho][\pi]$ von $(\psi \circ \iota_{\mathcal{P}})(f) \in \mathbb{Z}_p[[\pi]][x]$ für $\tilde{k},\tilde{l} \in \mathbb{Z}_{>0}$. Ein Primideal $p \in \tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$ der Gleichungsordnung des Restklassenkörpers $\bar{F}_{\mathcal{P}} = \mathbb{Q}(\bar{\delta}_1)$, wie in Algorithmus 4.59, so daß die spezialisierte r-set Resolvente über $\mathbb{Z}[\bar{\delta}_1]$ modulo $\tilde{\mathfrak{p}}$ separabel ist.

Ausgabe: $\mathcal{G}(f,F) \neq H$ *oder* $\mathcal{G}(f,F) \leq \mathrm{Stab}_G(\mathcal{O}) \lneq G$.

1. *(Initialisierung) $K = \mathbb{F}_q$: Setze $S := \{U \subseteq \{\alpha'_{1,(\tilde{l})},\ldots,\alpha'_{n,(\tilde{l})}\} \mid |U| = r\}$.*

   $K = \mathbb{Q}$: Setze $S := \{U \subseteq \{\alpha''_{1,(\tilde{k},\tilde{l})},\ldots,\alpha''_{n,(\tilde{k},\tilde{l})}\} \mid |U| = r\}$.

2. *(Bahnberechnung) Berechne eine Bahn $\mathcal{O}$ von S unter den Permutationen von H, welche keine Bahn unter den Permutationen von G ist.*

3. *(r-set Resolvente) Für $F(x_1,\ldots,x_n) = x_1\cdots x_r \in R[x_1,\ldots,x_n]$ berechne $T(X) := R_{(S_n,S_r\times S_{n-r},F)}(X) \in R[t,\delta][X]$ für $K = \mathbb{Q}$ nach Algorithmus* P *aus Casperson, McKay [10] und für $K = \mathbb{F}_q$ nach Algorithmus 2.23.*

4. *(Faktor der Resolvente des Restklassenkörpers) $K = \mathbb{F}_q$: Berechne $\bar{Q}_1 \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[X] = \mathfrak{o}_{\bar{F}_{\mathcal{P}}}[X]$ für $\bar{F}_{\mathcal{P}} = \mathbb{F}_{q^{\deg(\mathcal{P})}}$ mit*

$$\bar{Q}_1 \equiv \prod_{U\in\mathcal{O}} (X - \prod_{\alpha'_{i,(\tilde{l})}\in U} \alpha'_{i,(\tilde{l})}) \bmod \pi\mathbb{F}_{q^{\deg(\mathcal{P})d}}[\pi].$$

Existiert kein solches $\bar{Q}_1 \in \mathbb{F}_{q^{\deg(\mathcal{P})}}[X]$*, dann Ausgabe* $\mathcal{G}(f,F) \neq H$*.*

$K = \mathbb{Q}$ *: Berechne* $\bar{T} \in \mathbb{Z}[\bar{\delta}_1][X]$ *mit* $\bar{T} \equiv T \bmod \mathcal{P}$ *und* $\alpha^*_{i,(\tilde{k})} \in \mathbb{Z}[\rho]$ *mit* $\alpha^*_{i,(\tilde{k})} \equiv \alpha''_{i,(\tilde{k},\tilde{l})} \bmod \pi\mathbb{Z}[\rho][\pi]$ *für* $1 \leq i \leq n$*. Wende Schritt* $4-9$ *aus Algorithmus 5.18 auf* $\alpha^*_{1,(\tilde{k})} \ldots, \alpha^*_{n,(\tilde{k})} \in \mathbb{Z}[\rho]$*, Gleichungsordnung* $\mathbb{Z}[\bar{\delta}_1]$*, Primideal* $\tilde{\mathfrak{p}}$ *und* $\bar{T} \in \mathbb{Z}[\bar{\delta}_1][X]$ *an. Erhalte entweder* $\bar{Q}_1 \in \mathfrak{o}_{\bar{F}_\mathcal{P}}[X]$ *oder Ausgabe* $\mathcal{G}(f,F) \neq H$*.*

5. *(Kofaktor modulo* $\mathcal{P}$*) Berechne* $\bar{Q}_2 \in \mathfrak{o}_{\bar{F}_\mathcal{P}}[X]$ *mit* $\bar{T} = \bar{Q}_1\bar{Q}_2$ *in* $\mathfrak{o}_{\bar{F}_\mathcal{P}}[X]$*. Nach Voraussetzung an* $\mathcal{P}$ *sind* $\bar{Q}_1, \bar{Q}_2$ *koprim modulo* $\mathcal{P}$*.*

6. *(Gradschranke) Berechne untere Schranken* M_j*,* $(1 \leq j \leq s)$ *der Bewertungen* ν_j *der Koeffizienten der Faktoren von* $T(X) \in R[t,\delta][X]$ *und* $l \in \mathbb{Z}_{>0}$ *mit* $l > -2M_1$ *im Fall* $F = K(t)$ *bzw.* $l > s'(3A\min_{1\leq j\leq s}\{e_j\} - \min_{1\leq j\leq s}\{W_j\})$ *für* $F \neq K(t)$*, wobei* $A, W_j \in \mathbb{Q}$ *wie in* (4.76)*,* (4.77) *und* $s' \in \mathbb{Z}_{>0}$ *aus Bezeichnung 4.83.*

7. *(Hensel-Lifting) Berechne* $\tilde{T} \in \bar{F}_\mathcal{P}[\pi][X]$ *mit* $\tilde{T} \equiv \iota_\mathcal{P}(T) \bmod \pi^l\bar{F}_\mathcal{P}[[\pi]]$*. Lifte* $\tilde{T} \equiv \bar{Q}_1\bar{Q}_2 \bmod \pi\bar{F}_\mathcal{P}[\pi]$ *zu* $\bar{T} \equiv \tilde{Q}_1\tilde{Q}_2 \bmod \pi^l\bar{F}_\mathcal{P}[\pi]$*, wobei die Koeffizienten von* $\tilde{Q}_1, \tilde{Q}_2$ *einen Grad bezüglich* π *haben, der kleiner als* l *ist.*

8. *(Rekonstruktion) Ist* $F = K(t)$*, so setze* $Q_1 = \tilde{Q}_1(t - t_0, X)$*. Ist* $Q_1 \notin K(t)[X]$*, so Ausgabe von* $\mathcal{G}(f,F) \neq H$*. Ist* $F \neq K(t)$*, so rekonstruiere jeden Koeffizienten von* $\tilde{Q}_1 \in \bar{F}_\mathcal{P}[\pi][X]$ *mittels des in Kapitel 4 beschriebenen Verfahrens zu* $Q_1 \in \mathfrak{o}_F[X]$*. Ist dies nicht möglich, so Ausgabe von* $\mathcal{G}(f,F) \neq H$*.*

9. *(Teilt Faktor* Q_1 *die Resolvente?) Teste, ob* Q_1 *zu einem echten Faktor von* T *in* $\mathfrak{o}_F[X]$ *korrespondiert. In diesem Fall Ausgabe von* $\mathcal{G}(f,F) \leq \mathrm{Stab}_G(\mathcal{O}) \lneqq G$*. Ansonsten Ausgabe von* $\mathcal{G}(f,F) \neq H$*.*

In Schritt 6 erhalten wir mittels des folgenden Satzes Schranken für die Grade der Koeffizienten der möglichen Faktoren von $T(X) \in R[t,\delta][X]$:

5.21. Proposition. *Sei* $F/K(t)$*,* $K \in \{\mathbb{Q}, \mathbb{F}_q\}$ *ein algebraischer Funktionenkörper mit Maximalordnung* $\mathfrak{o}_F$ *und* $f(x) = \sum_{i=0}^n a_i x^i \in \mathfrak{o}_F[x]$ *ein normiertes Polynom. Ist* $g(x) = \sum_{r=0}^m b_r x^r \in \mathfrak{o}_F[x]$ *normiert und ein Teiler von* f *in* $\mathfrak{o}_F[x]$*, so gilt für die Bewertungen* ν_j*,* $(1 \leq j \leq s)$*, welche zu den unendlichen Stellen aus* $\mathbb{P}_\infty(F)$ *korrespondieren, der Koeffizienten von* g*:*

$$\nu_j(b_{r-k}) \geq k \min_{1\leq i\leq n}\left\{\frac{\nu_j(a_{n-i})}{i}\right\},\ (1 \leq j \leq s, 1 \leq k \leq r).$$

Beweis. Nach Lorenz [52], §23, Satz 5 existiert eine Fortsetzung der Bewertung ν_j, $(1 \leq j \leq s)$ auf den Zerfällungskörper $N(f,F)$ von f. Diese wollen wir ebenfalls mit ν_j bezeichnen. Die Nullstellen von f seien mit $\alpha_1, \ldots, \alpha_n \in N(f,F)$ bezeichnet. Durch Darstellung der Koeffizienten von $g \in \mathfrak{o}_F[x]$ als elementarsymmetrische Funktionen der Nullstellen von $f \in \mathfrak{o}_F[x]$ folgt aus Satz 4.112

$$\begin{aligned} \nu_j(b_{r-k}) &= \nu_j\Big(\sum_{1\leq l_1<\cdots<l_k\leq r} \alpha_{l_1}\cdots\alpha_{l_k}\Big) \\ &\geq k \min_{1\leq i\leq n}\{\nu_j(\alpha_i)\} = k \min_{1\leq i\leq n}\left\{\tfrac{\nu_j(a_{n-i})}{i}\right\}. \end{aligned}$$

□

5.22. Beispiel. (*i*) Sei $G = 12T_{300}^{+} = A_{12}$ mit maximaler transitiver Untergruppe $H = 12T_{295}^{+} = M_{12}$, und es gelte $H \leq \mathcal{G}(f,F) \leq G$. Anhand der Tabellen aus dem Anhang können wir für $r = 6$ die Gruppen H und G unterscheiden. Somit impliziert die Ausgabe $\mathcal{G}(f,F) \leq \mathrm{Stab}_G(\mathcal{O}) \lneqq G$ von Algorithmus 5.18 bzw. 5.20 unter Verwendung von Korollar 2.7, daß $\mathcal{G}(f,F) = H$ gelten muß.

(*ii*) Sei $G = 15T_{103}^{+}$ und $H = 15T_{20}^{+}$ und $\mathcal{G}(f,F)$ in der Menge der Gruppen $\{15T_{20}^{+}, 15T_{28}^{+}, 15T_{47}^{+}, 15T_{72}^{+}, 15T_{103}^{+}\}$ enthalten. Aus den Tabellen aus dem Anhang folgt, daß eine 2-set Resolvente genügt, um die Gruppen G und H zu unterscheiden. Als 2-set Resolvente wählen wir $R_{(S_{15},S_2\times S_{13},F)}$ für $F = x_1x_4$. In diesem Fall ist H keine maximale Untergruppe von G, sondern es liegt die folgende Situation vor: $15T_{20}^{+} < 15T_{28}^{+} < 15T_{47}^{+} < 15T_{72}^{+} < 15T_{103}^{+}$. Der einzige Inklusionstest, welcher nicht bewiesen ist, ist der Abstieg von $15T_{103}^{+}$ nach $15T_{72}^{+}$. Die restlichen Abstiege sind nach dem Verfahren von Stauduhar unter der Annahme, daß der erste Abstieg bewiesen ist, korrekt. Liefert Algorithmus 5.18 bzw. 5.20 die Ausgabe $\mathcal{G}(f,F) \leq \mathrm{Stab}_G(Orb_H(F)) \lneqq G = 15T_{103}^{+}$, so folgt aus $\mathrm{Stab}_G(Orb_H(F)) \leq 15T_{72}^{+}$, daß $H = \mathcal{G}(f,F)$ gilt. Wie Beispiel 2.24 zeigt, hätten wir unter Verwendung der absoluten Resolventenmethode alleine eine r-set Resolvente mit $r = 4$ wählen müssen, um zwischen den Gruppen $15T_{20}^{+}$ und $15T_{28}^{+}$ zu unterscheiden.

5.4 Der gesamte Algorithmus

In diesem Abschnitt geben wir abschließend einen Gesamtüberblick über den entwickelten Algorithmus zur Galoisgruppenberechnung für algebraische Zahl- und Funktionenkörper. Dabei werden alle bisher behandelten Methoden eingeordnet.

Ein kritischer Punkt im Algorithmus ist die Wahl des Primideals $\mathfrak{p}$ bzw. der Stelle $\mathcal{P}$ für die Berechnung der $\mathfrak{p}$-adischen ($\mathcal{P}$-adischen) Vervollständigung. Betrachten wir zunächst den Zahlkörperfall: Sei $\mathfrak{o}$ eine beliebige Ordnung des algebraischen Zahlkörpers F, $f \in \mathfrak{o}[x]$ ein normiertes, irreduzibles Polynom und $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ ein unverzweigtes Primideal vom Grad eins, so daß für die Primzahl

$p \in \tilde{\mathfrak{p}}$ gilt $p \nmid \mathrm{disc}(\mathfrak{o})\mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$. Wir faktorisieren $f \equiv f_1 \cdots f_u \bmod \tilde{\mathfrak{p}}$ und definieren $d_{\tilde{\mathfrak{p}}} := \mathrm{kgV}(\deg(f_1), \ldots, \deg(f_u))$. Haben wir ein Primideal $p \in \tilde{\mathfrak{p}}$ mit $p \nmid \mathrm{disc}(\mathfrak{o})\mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(f))$ fixiert, so gibt es keine mehrfachen Nullstellen modulo $\tilde{\mathfrak{p}}$. Deshalb genügt es, die Nullstellen in der $\tilde{\mathfrak{p}}$-adischen Vervollständigung modulo $\tilde{\mathfrak{p}}$ zu berechnen, da sie bereits im Restklassenkörper verschieden sind. Werden die Nullstellen mit einer größeren Präzision benötigt, so können wir diese mittels Newton-Lifting (vgl. Sektion 1.4) erhalten. Wir verwenden wieder die Notationen aus Algorithmus 2.20.

5.23. Algorithmus. *(Galoisgruppenberechnung - Algebraische Zahlkörper)*

Eingabe: *Ein normiertes, irreduzibles Polynom f vom Grad n mit Koeffizienten in einer Ordnung $\mathfrak{o}$ eines algebraischen Zahlkörpers F.*

Ausgabe: *Die Galoisgruppe von f, inklusive der zugehörigen Nullstellenanordnung.*

1. *(Grad von f?) Ist $n = 2$, so terminiere mit Ausgabe von $\mathcal{G}(f, F) \leftarrow S_2$ und einer beliebigen Nullstellenanordnung.*

2. *(Diskriminante?) Ist $\mathrm{disc}(f)$ kein Quadrat in F, setze $G \leftarrow S_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_u$. Andernfalls setze $G \leftarrow A_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_g$. Ist $n = 3$, so terminiere mit Ausgabe von $\mathcal{G}(f, F) \leftarrow G$ und einer beliebigen Nullstellenanordnung.*

3. *(Faktorisierung $\bmod \tilde{\mathfrak{p}}$) Faktorisiere das Polynom f modulo einiger Primideale $\tilde{\mathfrak{p}}$ mit $\mathrm{disc}(f) \notin \tilde{\mathfrak{p}}$ und setze $\mathcal{L}_z \leftarrow \{$ Menge aller Gruppen in $\mathcal{L}$, die mindestens ein Element der gegebenen Zykeltypen enthalten $\}$ (Korollar 1.15).*

4. *(Galoisgruppe gefunden?) Ist $\tilde{\mathcal{L}} \cap \mathcal{L}_z = \{T\}$, so terminiere mit Ausgabe von $\mathcal{G}(f, F) \leftarrow T$ und einer beliebigen Nullstellenanordnung.*

5. *(Teilkörper) Berechne die Teilkörper des Körpers $F(\alpha)$ für eine Nullstelle $\alpha \in N(f, F)$ von f.*

6. *Gibt es nicht-triviale Teilkörper, so gehe zu Schritt 6.1, ansonsten gehe zu Schritt 6.2.*

   6.1 *(Galoisgruppe imprimitiv) Eliminiere alle Gruppen in $\mathcal{L}_z$, die kein Blocksystem der berechneten Gestalt haben. Wähle ein Primideal $p \in \tilde{\mathfrak{p}} \subset \mathfrak{o}$, so daß $p \nmid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(m))$ für jedes Minimalpolynom m eines Teilkörpers von $F(\alpha)$ gilt (Bemerkung 5.7) und $d_{\tilde{\mathfrak{p}}}$ klein ist. Berechne Nullstellen $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \bmod p\mathbb{Z}[\rho]$ mittels Algorithmus 3.10*

(vgl. Bemerkung 3.11). Wende Algorithmus 5.3 an, um $T \in \mathcal{L}$ mit $\mathcal{G}(f,F) \leq T$ zu berechnen. Setze $G \leftarrow T$.

6.2 (Galoisgruppe primitiv) Eliminiere alle imprimitiven Gruppen der Menge $\mathcal{L}_z$. Liegt aufgrund der möglichen, verbleibenden Gruppen die Vermutung nahe, daß zur Berechnung von $\mathcal{G}(f,F)$ ein Abstieg $\tilde{H} < \tilde{G}$ mit großem Gruppenindex durchlaufen werden muß, so berechne eine geeignete r-set Resolvente $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)}$, welche anschließend für den Beweis des unbewiesenen Schritts (Algorithmus 5.18) benötigt wird. Wähle ein Primideal $\tilde{\mathfrak{p}} \subset \mathfrak{o}$ mit den folgenden Eigenschaften:

(1) $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)} \bmod \tilde{\mathfrak{p}}$ ist separabel.

(2) $d_{\tilde{\mathfrak{p}}}$ ist klein.

(3) $[C_G(\tau) : C_H(\tau)]$ ist klein, wobei τ der korrespondierende Frobenius-Automorphismus ist.

Berechne Nullstellen $\alpha^*_{1,(k)}, \ldots, \alpha^*_{n,(k)} \bmod p\mathbb{Z}[\rho]$ unter Benutzung von Algorithmus 3.10 (vgl. Bemerkung 3.11).

7. (Durchlaufe das Untergruppengitter) Wende für alle maximalen Untergruppen H von G, welche in $\mathcal{L}_z$ enthalten sind, die $\tilde{\mathfrak{p}}$-adische Version des Stauduhar Algorithmus an (Sektion 3.3, Sektion 3.4, vgl. auch Schritt 6-15 von Algorithmus 2.20). Ist $[\,G:H\,] > 2000$, so verwende eine heuristische Präzision (vgl. (5.16)). Ist $\mathcal{G}(f,F) \leq H$, so setze $G \leftarrow H$ und gehe zu Schritt 7.

8. (Ergebnis nicht bewiesen?) Gibt es in Schritt 7 einen unbewiesenen Abstieg, so wende Algorithmus 5.18 an, um diesen Schritt zu verifizieren. Ist der nichtbewiesene Abstieg $\tilde{H} < \tilde{G}$ falsch, so eliminiere $\tilde{H}$ in $\mathcal{L}_z$, setze $G \leftarrow \tilde{G}$, ordne die Nullstellen wie vor dem unbewiesenen Abstieg an und gehe zu Schritt 7. Sind alle Abstiege im Untergruppengitter korrekt, so terminiere mit Ausgabe von G und aktueller Nullstellenanordnung.

In der Praxis hat es sich als nützlich erweisen, die Faktorisierung des Polynoms f modulo $\tilde{\mathfrak{p}}$ für Primideale $p \in \tilde{\mathfrak{p}} \subset \mathfrak{o}$ mit $p \leq 100$ durchzuführen. Testdurchläufe bestätigen, daß in der Regel nach den ersten $20 - 25$ Primidealen eine sehr gute Annäherung von unten an die eigentliche Galoisgruppe stattgefunden hat. Wie wir schon in den Algorithmen 2.20 und 5.3 gesehen haben, wird die Anordnung der Nullstellen in Schritt 6 und 7 geändert. Es kann sein, daß die r-set Resolvente $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)}$, welche in Schritt 6.2 berechnet wird, nicht separabel ist. In diesem Fall wenden wir eine geeignete Tschirnhauentransformation (meistens sind Transformationen der Art $h(x) = x + 1$ ausreichend, vgl. auch Satz 2.16) auf das Polynom f an. Außerdem muß in Schritt 6.2 *(2)*, *(3)* ein guter Kompromiß

zwischen dem korrespondierenden Grad des $\tilde{\mathfrak{p}}$-adischen Körpers und der Anzahl der verkürzten Nebenklassenrepräsentanten gefunden werden. In der Regel korrespondieren Frobenius-Automorphismen von größerem Grad nämlich zu kleineren verkürzten Nebenklassenrepräsentantensystemen.

Kommen wir nun zum Funktionenkörperfall. Analog wie im Zahlkörperfall wählen wir für ein normiertes, irreduzibles, separables Polynom $f \in R[t,\delta][x] \subset F[x] = K(t,\delta)[x] = K(t)[x]/h(t,x)K(t)[x]$ ein normiertes Primpolynom $p(t) = t - t_0 \in R[t_0]$ mit $p(t) \nmid \mathrm{disc}(h)\mathrm{N}_{F/K(t)}(\mathrm{disc}(f))$. Bezeichnet $\boldsymbol{\mathcal{P}} \in \mathbb{P}(F)$ die zu $p(t)$ gehörige unverzweigte Stelle so faktorisieren wir $f \equiv f_1 \cdots f_u \bmod \tilde{\boldsymbol{\mathcal{P}}}$ und definieren $d_{\boldsymbol{\mathcal{P}}} := \mathrm{kgV}(\deg(f_1), \ldots, \deg(f_u))$.

5.24. Algorithmus. *(Galoisgruppenberechnung-Algebraische Funktionenkörper)*

Eingabe: *Ein in x normiertes, irreduzibles, separables Polynom $f(x) \in R[t,\delta][x] \subset F[x] = K(t,\delta)[x]$ vom Grad n ($R \in \{\mathbb{F}_q, \mathbb{Q}, \}$, $K := \mathrm{Quot}(R)$).*

Ausgabe: *Die Galoisgruppe von f, inklusive der zugehörigen Nullstellenanordnung.*

1. *(Grad von f?) Ist $n = 2$, so terminiere mit Ausgabe von $\mathcal{G}(f,F) \leftarrow S_2$ und einer beliebigen Nullstellenanordnung.*

2. *(Diskriminante?) Ist $\mathrm{char}(F) = 2$ oder $\mathrm{disc}(f)$ kein Quadrat in F, setze $G \leftarrow S_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_u$. Andernfalls setze $G \leftarrow A_n$ und $\tilde{\mathcal{L}} \leftarrow \mathcal{L}_g$ (Satz 2.11). Ist $n = 3$ und $\mathrm{char}(F) \neq 2$, so terminiere mit Ausgabe von $\mathcal{G}(f,F) \leftarrow G$ und einer beliebigen Nullstellenanordnung.*

3. *(Faktorisierung $\bmod \boldsymbol{\mathcal{P}}$) $K = \mathbb{F}_q$: Faktorisiere das Polynom f modulo einiger Stellen $\boldsymbol{\mathcal{P}} \in \mathbb{P}(F)$ mit $\mathrm{disc}(f) \notin \boldsymbol{\mathcal{P}}$ und setze $\mathcal{L}_z \leftarrow \{$ Menge aller Gruppen in $\mathcal{L}$, die mindestens ein Element der gegebenen Zykeltypen enthalten $\}$ (Korollar 1.15).*

   $K = \mathbb{Q}$: Bestimme Stellen $\boldsymbol{\mathcal{P}} \in \mathbb{P}(F)$, für die das Polynom $\bar{f} := f \bmod \boldsymbol{\mathcal{P}} \in \mathbb{Z}[\bar{\delta}_1][x]$ irreduzibel ist, und wende Schritt 3 aus Algorithmus 5.23 auf die Polynome $\bar{f}$ an. Setze $\mathcal{L}_z \leftarrow \{$ Menge aller Gruppen in $\mathcal{L}$, die mindestens ein Element der gegebenen Zykeltypen enthalten $\}$ (Korollar 1.15).

4. *(Galoisgruppe gefunden?) Ist $\mathrm{char}(F) \neq 2$ und $\tilde{\mathcal{L}} \cap \mathcal{L}_z = \{T\}$, so terminiere mit Ausgabe von $\mathcal{G}(f,F) \leftarrow T$ und einer beliebigen Nullstellenanordnung.*

5. *(Teilkörper) Berechne die Teilkörper des Körpers $F(\alpha)$ für eine Nullstelle $\alpha \in N(f,F)$ von f.*

6. Gibt es nicht-triviale Teilkörper, so gehe zu Schritt 6.1, ansonsten gehe zu Schritt 6.2.

6.1 (Galoisgruppe imprimitiv) Eliminiere alle Gruppen in $\mathcal{L}_z$, die kein Blocksystem der berechneten Gestalt haben.

$K = \mathbb{F}_q$: Wähle ein normiertes Primpolynom $p(t) \in \mathbb{F}_q[t]$ minimalen Grades, so daß $p(t) \nmid \mathrm{N}_{F/\mathbb{Q}}(\mathrm{disc}(m))$ für jedes Minimalpolynom m eines Teilkörpers von $F(\alpha)$ gilt (Bemerkung 5.7) und für die zu $p(t)$ gehörige Stelle $\mathcal{P} \in \mathbb{P}(F)$ die Zahl $d_{\mathcal{P}}$ klein ist. Berechne Nullstellen $\alpha'_{1,(l)}, \ldots, \alpha'_{n,(k,l)} \bmod \pi\mathbb{F}_{q^{\deg(\mathcal{P})d_{\mathcal{P}}}}$ mittels Algorithmus 4.57.

$K = \mathbb{Q}$: Wähle ein normiertes Primpolynom $p(t) = t - t_0 \in \mathbb{Z}[t]$, welches den Bedingungen aus Bemerkung 4.56 genügt und für das zusätzlich $p(t) \nmid \mathrm{N}_{F/K(t)}(\mathrm{disc}(m))$ für jedes Minimalpolynom m eines Teilkörpers von $F(\alpha)$ gilt (Bemerkung 5.7). Dann ist die zu $p(t)$ gehörige Stelle $\mathcal{P} \in \mathbb{P}(F)$ vom Grad $m = [F : \mathbb{Q}(t)]$ und $\bar{f} \bmod \mathcal{P}$ ist irreduzibel über dem Restklassenkörper $\bar{F}_{\mathcal{P}}$ (Satz 4.53). Wähle ein Primideal $\tilde{p} \in \mathbb{Z}[\bar{\delta}_1]$ wie in Algorithmus 5.23 Schritt 6.1. Berechne Nullstellen $\alpha''_{1,(k,l)}, \ldots, \alpha''_{n,(k,l)} \bmod p\mathbb{Z}[\rho] + \pi\mathbb{Z}[\rho]$ mittels Algorithmus 4.59.

Wende Algorithmus 5.3 an, um $T \in \mathcal{L}$ mit $\mathcal{G}(f, F) \leq T$ zu berechnen. Setze $G \leftarrow T$.

6.2 (Galoisgruppe primitiv) Eliminiere alle imprimitiven Gruppen der Menge $\mathcal{L}_z$. Liegt aufgrund der möglichen, verbleibenden Gruppen die Vermutung nahe, daß zur Berechnung von $\mathcal{G}(f, F)$ ein Abstieg $\tilde{H} < \tilde{G}$ mit großem Gruppenindex durchlaufen werden muß, so berechne eine geeignete r-set Resolvente $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)}$, welche anschließend für den Beweis des unbewiesenen Schritts (Algorithmus 5.18) benötigt wird. Wähle ein normiertes Primpolynom $p(t) \in R[t]$ bzw. die zugehörige Stelle $\mathcal{P} \in \mathbb{P}(F)$ mit den folgenden Eigenschaften:

$K = \mathbb{F}_q$:

(1) $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)} \bmod \mathcal{P}$ ist separabel.

(2) $d_{\mathcal{P}}$ ist klein.

(3) $[C_G(\tau) : C_H(\tau)]$ ist klein, wobei τ der korrespondierende Frobenius-Automorphismus ist.

Berechne Nullstellen $\alpha'_{1,(l)}, \ldots, \alpha'_{n,(k,l)} \bmod \pi\mathbb{F}_{q^{\deg(\mathcal{P})d_{\mathcal{P}}}}$ mittels Algorithmus 4.57.

$K = \mathbb{Q}$:

(1) Das Primpolynom $p(t) = t - t_0 \in \mathbb{Z}[t]$ erfüllt die Bedingungen aus Bemerkung 4.56.

(2) $R_{(S_n, S_r \times S_{n-r}, x_1 \cdots x_r)} \bmod \mathcal{P}$ ist separabel.

(3) Wähle ein Primideal $\tilde{\mathfrak{p}} \subset \mathbb{Z}[\bar{\delta}_1]$, welches die Kriterien 6.2 (1)-(3) aus Algorithmus 5.23 erfüllt.

Berechne Nullstellen $\alpha''_{1,(k,l)}, \ldots, \alpha''_{n,(k,l)} \bmod p\mathbb{Z}[\rho] + \pi\mathbb{Z}[\rho]$ mittels Algorithmus 4.59.

7. *(Durchlaufe das Untergruppengitter) Wende für alle maximalen Untergruppen H von G, welche in $\mathcal{L}_z$ enthalten sind, die $\mathcal{P}$-adische Version des Stauduhar Algorithmus an (Sektion 4.3, vgl. auch Schritt 6-15 von Algorithmus 2.20). Ist $[\, G : H \,] > 2000$, so verwende eine heuristische Präzision (vgl. (5.17), (5.16)). Ist $\mathcal{G}(f, F) \leq H$, so setze $G \leftarrow H$ und gehe zu Schritt 7.*

8. *(Ergebnis nicht bewiesen?) Gibt es in Schritt 7 einen unbewiesenen Abstieg, so wende Algorithmus 5.20 an, um diesen Schritt zu verifizieren. Ist der nichtbewiesene Abstieg $\tilde{H} < \tilde{G}$ falsch, so eliminiere $\tilde{H}$ in $\mathcal{L}_z$, setze $G \leftarrow \tilde{G}$, ordne die Nullstellen wie vor dem unbewiesenen Abstieg an und gehe zu Schritt 7. Sind alle Abstiege im Untergruppengitter korrekt, so terminiere mit Ausgabe von G und aktueller Nullstellenanordnung.*

Auch wenn wir bei der Beschreibung der Theorie und der Verfahren immer eine Unterteilung nach Zahl- bzw. Funktionenkörpern gewählt haben, so bringt doch der Gesamtüberblick über den entwickelten Algorithmus die Verwandtschaft der algebraischen Zahlkörper und der globalen Funktionenkörper deutlich zum Ausdruck. Unsere Implementation verwendet in der Tat generische Algorithmen, sogar unter Einbeziehung der Funktionenkörper über $\mathbb{Q}$, wobei für Zahlkörper bzw. Funktionenkörper spezifische Routinen über eine einheitliche Schnittstelle aufgerufen werden.

Kapitel 6

Berechnung der Daten

In diesem Kapitel geben wir nähere Informationen zur Berechnung der erforderlichen Daten für das Verfahren von Stauduhar an. In Abschnitt 2.1.4 haben wir gesehen, daß die Kenntnis der transitiven Permutationsgruppen des jeweiligen Grades eine Grundvoraussetzung für diese Methode darstellt. Darüber hinaus gehören die Bestimmung des Untergruppengitters, die Berechnung G-relativer H-invarianter Polynome und Nebenklassenrepräsentantensysteme $G//H$ für alle auftretenden Gruppenpaare zu den Kerndaten des Verfahrens. Zur Anwendung des van der Waerden-Kriteriums müssen außerdem zu allen Gruppen $G \neq S_n$ die auftretenden Zykeltypen, gegebenenfalls mit Häufigkeiten, berechnet werden.

Bis Grad 15 wurden die transitiven Permutationsgruppen von Butler, McKay [8, 7] und Royle [73] klassifiziert. Hulpke [36] hat diese Arbeit in seiner Dissertation bis Grad 31 fortgeführt. In den Computeralgebrasystemen MAGMA [5, 16] und GAP [54] sind die von ihm bestimmten Vertreter der S_n-Konjugationsklassen für die Grade $n \leq 23$ gespeichert, welche wir als Grundlage für unsere Berechnungen verwendet haben. Ebenfalls in Butler, McKay [8] findet man eine Liste der auftretenden Zykeltypen mit Häufigkeiten der transitiven Permutationsgruppen bis zum Grad 11. Für größere Grade ≤ 23 haben wir derartige Listen durch Berechnung der Konjugationsklassen der Elemente der betreffenden Permutationsgruppen mittels MAGMA [5, 16] erstellt. Die restlichen relevanten Daten gibt Stauduhar [78] in dem Artikel, in dem er sein Verfahren zur Galoisgruppenberechnung von irreduziblen Polynomen über $\mathbb{Q}$ vorstellt, bis Grad 7 an. Der Unterschied zu den von uns berechneten Daten ergibt sich in der Behandlung der geraden Gruppen. Stauduhar nimmt keine Unterteilung der Untergruppengitter in gerade und ungerade Gruppen vor, sondern schließt aus einer Inklusion $\mathcal{G}(f, \mathbb{Q}) \leq G$ in einer ungeraden Gruppe G mittels der Diskriminante $\mathrm{disc}(f)$, ob $\mathcal{G}(f, \mathbb{Q}) \leq G \cap A_n$ gilt. Dadurch brauchen für eine Reihe von Gruppenpaaren $H, G \leq A_n$ keine gesonderten Daten berechnet werden, für die Anzahl der zu betrachtenden Inklusionen

ergibt sich aber kein Unterschied. Wir hingegen bestimmen erst, ob es sich bei der Galoisgruppe um eine gerade oder ungerade Permutationsgruppe handelt (außer im Fall $\mathrm{char}(K) = 2$), und durchlaufen anschließend das Untergruppengitter der geraden oder ungeraden Gruppen.

Olivier und Eichenlaub [23, 22] haben die Arbeit von Stauduhar zur Berechnung der Galoisgruppe irreduzibler ganzrationaler Polynome f für die Grade $8 \leq n \leq 11$ fortgesetzt. Sie verwenden im Gegensatz zu unseren Daten die Erzeuger der Permutationsgruppen aus Butler, McKay [8]. Für $12 \leq n \leq 23$ haben wir mittels des Computeralgebrasysteme MAGMA [5, 16] als erste einen vollständigen Datensatz für das Verfahren von Stauduhar berechnet und implementiert. Die besondere Schwierigkeit für große Grade liegt zum einen an der wachsenden Anzahl der Gruppen (bei Grad 16 gibt es zum Beispiel 1954 transitive Gruppen und 8238 Gruppenpaare), aber auch an der wachsenden Gruppenordnung der zu betrachtenden Gruppen. Vielfach erwiesen sich bestehende Algorithmen für die Datensätze aufgrund der großen Grade als nicht mehr praktikabel. Insbesondere zur Berechnung der Invarianten entwickeln wir neue Lösungsmethoden, um ein effizientes Programm zur Berechnung von Galoisgruppen zu erhalten.

6.1 Berechnung G-relativer H-invarianter Polynome

Für ein beliebiges Gruppenpaar $H < G \leq S_n$ haben wir die Existenz eines Polynoms $F \in K[x_1, \ldots, x_n]$ mit $\mathrm{Stab}_G(F) = H$ in 2.1.1 bewiesen. In diesem Abschnitt möchten wir diese Aussage konstruktiv belegen und darüber hinaus Algorithmen angeben, die uns G-relative H-invariante Polynome mit besonders günstigen Eigenschaften konstruieren.

6.1. Lemma. *Für $H < G \leq S_n$ und $\tilde{F}(x_1, \ldots, x_n) = x_1^1 x_2^2 \cdots x_{n-1}^{n-1}$ sei*

$$F(x_1, \ldots, x_n) := \sum_{\sigma \in H} \sigma \tilde{F}.$$

Dann gilt $\mathrm{Stab}_G(F) = H$.

Beweis. Für $\tau \in H$ gilt $\tau(F) = F$, da mit $\sigma \in H$ auch $\tau\sigma$ ganz H durchläuft, weil H eine endliche Gruppe ist. Ist nun $\tau \notin H$, so zeigen wir, daß $\tau(F) \neq F$ gilt: Da $\tilde{F}(x_1, \ldots, x_n) = x_1^1 x_2^2 \cdots x_{n-1}^{n-1}$ nur von der Identität invariant gelassen wird, gilt für zwei beliebige Permutationen $\tau_1, \tau_2 \in S_n$ mit $\tau_1 \neq \tau_2$, daß $\tau_1(\tilde{F}) \neq \tau_2(\tilde{F})$ ist. Somit sind alle Elemente der Menge $M := \{\sigma(\tilde{F}) \,|\, \sigma \in H\}$ verschieden und $\sigma(\tilde{F}) \notin M$ für $\sigma \in S_n \backslash H$. □

Allgemeiner erhalten wir für maximale Untergruppen H von G (vgl. [29], Satz 4.1.1):

6.2. Satz. *Seien $H < G \leq S_n$, H maximale Untergruppe von G und $m = x_1^{e_1} \cdots x_n^{e_n}$, $(e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0})$ ein Monom, für das $|\operatorname{Orb}_H(m)| \neq |\operatorname{Orb}_G(m)|$ gilt. Dann ist*

$$F(x_1, \ldots, x_n) = \sum_{\tilde{m} \in \operatorname{Orb}_H(m)} \tilde{m}$$

ein G-relatives H-invariantes Polynom.

G-relative H-invariante Polynome ergeben sich also zum Beispiel als Bahnsummen von geeigneten Monomen. Die Polynome aus Lemma 6.1 sind in der Praxis aufgrund der großen Anzahl von durchzuführenden Multiplikationen nicht sehr effizient. Die Wahl eines G-relativen H-invarianten Polynoms mit kleinstmöglichem Totalgrad hat aber große Auswirkungen auf das Laufzeitverhalten des Programms: Multiplikationen sind sehr teuer, so daß Berechnungen extrem beschleunigt werden können, wenn wir die Anzahl der auszuführenden Multiplikationen minimieren. Auf der anderen Seite sparen wir durch Wahl einer Resolvente, deren Konjugierte betraglich kleinere komplexe Nullstellen haben, auch beim Lifting wegen geringerer $\mathfrak{p}$-adischer Präzision Zeit (vgl. Satz 3.33, Satz 4.91). Analoges gilt für die Schranke bezüglich der Gradbewertung für das Lifting im Funktionenkörperfall (vgl. Satz 4.91, Satz 4.97 und Proposition 4.116). Unser Ziel ist es daher, Invarianten mit kleinstmöglichem Totalgrad und minimaler Anzahl von Monomen zu finden. Unsere bisherigen Methoden in [29] (vgl. Algorithmen 4.1.2, 4.1.3) zur Berechnung derartiger Invarianten stützten sich vor allem auf Satz 6.2. Dort hatten wir sukzessive die Menge aller Monome m vom Grad $d = 2, 3, \ldots$ bestehend aus $k = d, d-1, \ldots, 2$ Variablen bestimmt und $|\operatorname{Orb}_G(m)|$ mit $|\operatorname{Orb}_H(m)|$ verglichen, um eine Invariante mit kleinstmöglichem Totalgrad und minimaler Anzahl von Monomen zu garantieren. Schon bei Grad 12 erwies sich eine derartige Vorgehensweise nicht mehr uneingeschränkt praktikabel, so daß wir für manche Gruppenpaare eine randomisierte Variante dieses Algorithmus gewählt hatten, bei der die Minimalität der Invariante aber nicht mehr garantiert war. Im folgenden beschreiben wir einen wesentlich schnelleren, effektiveren Algorithmus mit den gewünschten Eigenschaften. Dieser Algorithmus hat darüber hinaus den besonderen Vorteil, daß Invarianten zur Laufzeit berechnet werden können und nicht mehr in umfangreichen Tabellen gespeichert werden müssen.

Sei $V := K[x_1, \ldots, x_n]$. Wir können den Polynomring V in

$$V = \bigoplus_{d=0}^{\infty} V_d,$$

zerlegen, wobei mit V_d die homogenen Komponenten vom Grad d bezeichnet werden. Dies hat eine Zerlegung des Invariantenringes $V^H := \{g \in V \mid \sigma(g) = g \text{ für alle } \sigma \in H\}$ zur Folge:

$$V^H = \bigoplus_{d=0}^{\infty} V_d^H.$$

V_d ist ein K-Vektorraum der Dimension $\binom{n+d-1}{n-1}$, da es genau so viele über K linear unabhängige Monome vom Grad d gibt.

6.3. Definition. Unter der Hilbert Reihe von V^H verstehen wir die formale Potenzreihe

$$h(V^H, t) := \sum_{d=0}^{\infty} \dim_K(V_d^H) \cdot t^d \in \mathbb{Z}[[t]].$$

In unserem Fall gilt somit $h(V,t) = \sum_{d=0}^{\infty} \binom{n+d-1}{n-1} t^d$. Da wir nur maximale Untergruppen H von G betrachten, entspricht der kleinstmögliche Totalgrad d eines G-relativen H-invarianten Polynoms dem kleinsten Exponenten von t, so daß die zugehörigen Koeffizienten der Reihen $h(V^H, t)$ und $h(V^G, t)$ verschieden sind.

6.4. Algorithmus. *(Berechnung G-relativer H-invarianter Polynome)*

Eingabe: *Eine Permutationsgruppe $G \leq S_n$, $(n \geq 3)$ und eine maximale transitive Untergruppe H von G.*

Ausgabe: *Ein homogenes Polynom $F \in K[x_1, \ldots, x_n]$ minimalen Grades $d \leq \frac{n(n-1)}{2}$ mit $\mathrm{Stab}_G(F) = H$.*

1. *(Hilbertreihen) Berechne die Hilbertreihen $h(V^H, t)$ und $h(V^G, t)$ und den kleinsten Exponenten d von t, so daß die zugehörigen Koeffizienten verschieden sind.*

2. *(Invarianten vom Grad d) Berechne alle homogenen Invarianten bezüglich H vom Grad d.*

3. *(G-relative Invarianten) Entferne alle Invarianten, welche nicht G-relativ sind.*

4. *(Ende) Gebe Invariante F mit kleinster Anzahl von Monomen zurück.*

6.5. Bemerkung. Nach Lemma 6.1 ist das Polynom $F(x_1, \ldots, x_n) := \sum_{\sigma \in H} \sigma(x_1^1 x_2^2 \cdot \cdots x_{n-1}^{n-1})$ für alle transitiven Gruppenpaare $H < G$ ein G-relatives H-invariantes Polynom, und wir können als obere Schranke für den Grad d des homogenen Polynoms $\sum_{i=1}^{n-1} i = n(n-1)/2$ in Algorithmus 6.4 angeben. Diese Schranke wird

für das Gruppenpaar $G = S_n$ und $H = A_n$ auch wirklich angenommen. Das Polynom

$$F(x_1, \ldots, x_n) = \sum_{\sigma \in A_n} \sigma(x_1^1 x_2^2 \cdots x_{n-1}^{n-1}) \tag{6.6}$$

ist ein S_n-relatives A_n-invariantes Polynom mit kleinstmöglichem Totalgrad. Gilt $\mathrm{char}(K) = 2$, so können wir anstelle des Diskriminantenkriteriums (vgl. Satz 2.11 (iii)) die Resolvente $R_{(S_n,A_n,F)}$ verwenden, um festzustellen, ob $\mathcal{G}(f, K) = S_n$ oder $\mathcal{G}(f, K) = A_n$ gilt. Wir bemerken allerdings, daß in dieser Invariante F in n exponentiell viele Terme aufsummiert werden.

Für die Schritte 1 und 2 in Algorithmus 6.4 verwenden wir Algorithmen des Invariantenpaketes in MAGMA (vgl. Kemper, Steel [39]). Hierbei ist Schritt 2 am kostspieligsten. Der Anwendungsbereich von Schritt 2 beschränkt sich bei derzeitigen Speicherkapazitäten für die betrachteten Permutationsgruppen vom Grad n auf Größenordnungen $\binom{n+d-1}{n-1} \approx 2500000$. Damit lassen sich für Grade $n \geq 12$ mittels Algorithmus 6.4 nicht zu allen Gruppenpaaren Invarianten berechnen. Auch stellt sich heraus, daß die Invarianten, die wir mit Algorithmus 6.4 erhalten, nicht immer am günstigsten für das Laufzeitverhalten unseres Programms sind. Betrachten wir zum Beispiel die maximale Untergruppe $18T_{981} = S_9 \wr S_2$ von S_{18}, welche bezüglich der Vertreter der S_{18}-Konjugationsklassen aus [5, 16] das Blocksystem $\mathcal{B} = \{\{1,2,3,4,5,6,7,8,9\},\{10,\ 11,12,13,14,15,16,17,18\}\}$ besitzt. Die Berechnung des speziellen S_{18}-relativen $18T_{981}$-invarianten Polynoms $(x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_8+x_9)(x_{10}+x_{11}+x_{12}+x_{13}+x_{14}+x_{15}+x_{16}+x_{17}+x_{18})$ ist schneller als die Berechnung des Polynoms $\sum_{i=1}^{9}\sum_{j=10}^{18} x_i x_j$, welches wir mit Algorithmus 6.4 gefunden haben. Dies liegt vor allem daran, daß die Gruppenstruktur der betrachteten Gruppenpaare bisher weitgehend außer acht gelassen wurde. Im folgenden geben wir eine Reihe von Sätzen an, mit Hilfe derer Invarianten erhalten werden können, die für das Laufzeitverhalten des Algorithmus wesentlich günstiger sind.

Beginnen wir mit zwei Ergebnissen über Kranzprodukte aus Eichenlaub [22], Abschnitt 1.1.2 und Abschnitt 2.1.2, Proposition 3. Der erste Satz beschränkt sich auf Kranzprodukte der Form $G = S_l \wr S_m$, wobei durch Betrachtung der Stabilisatoren symmetrischer Polynome Untergruppen klassifiziert werden. Die symmetrischen Polynome dienen dann umgekehrt als Invarianten dieser Gruppenpaare. Seien

$$d_k := \prod_{1 \leq i < j \leq l} (x_{i,k} - x_{j,k}), \quad (1 \leq k \leq m) \ \text{ und } \ D := \prod_{1 \leq i < j \leq m} (y_i - y_j) \tag{6.7}$$

mit $y_j := \sum_{i=1}^{l} x_{i,j}$, $(1 \leq j \leq m)$. Darüber hinaus bezeichnen wir mit $s_k, (1 \leq k \leq m)$ die k-te elementarsymmetrische Funktion in m Variablen.

6.8. Satz. *Sei* $\mathrm{char}(K) \neq 2$ *und* $l, m \geq 2$. *Die Gruppe* $S_l \wr_\Gamma S_m$ *mit* $\Gamma := \{1, \ldots, m\}$ *hat mindestens drei Untergruppen von Index* 2*: Die Stabilisatoren von* $s_m(d_1, \ldots, d_m)$, $D(y_1, \ldots, y_m)$ *(das ist* $S_l \wr_\Gamma A_m$*) und* $D(y_1, \ldots, y_m)s_m(d_1, \ldots, d_m)$. *Außerdem hat* $S_l \wr_\Gamma S_m$ *jeweils eine Untergruppe vom Index* 2^{m-1} *und eine Untergruppe vom Index* 2^m*, (diese ist* $A_l \wr_\Gamma S_m$*), welche die Stabilisatoren von* $s_2(d_1, \ldots, d_m)$ *bzw.* $s_1(d_1, \ldots, d_m)$ *sind.*

6.9. Beispiel. Die imprimitive Gruppe $22T_{57}$ ist das Kranzprodukt $S_{11} \wr S_2$. Diese Gruppe hat bei Identifizierung von $\{1, \ldots, 11\} \times \{1, 2\}$ mit $\{1, \ldots, 22\}$ bezüglich der Erzeuger in MAGMA [5, 16] das Blocksystem $\{\{1, \ldots, 11\}, \{12, \ldots, 22\}\}$. Mit unseren bisherigen Mitteln hatten wir für den Abstieg von $22T_{57}$ in die maximale Untergruppe $22T_{56}$ das invariante Polynom

$$F = \sum_{\tilde{m} \in \mathrm{Orb}_{22T_{56}}(m)} \tilde{m}$$

mit $m = x_1^{10}x_2^9x_3^8x_4^7x_5^6x_6^5x_7^4x_8^3x_9^2x_{10}x_{12}^{10}x_{13}^9x_{14}^8x_{15}^7x_{16}^6x_{17}^5x_{18}^4x_{19}^3x_{20}^2x_{21}$ gefunden, dessen Auswertung uns $109 \cdot 796675461120000$ Multiplikationen kostet. Mit Hilfe des letzten Satzes können wir nachrechnen, daß im Fall $\mathrm{char}(K) \neq 2$

$$\mathrm{Stab}_{S_{11} \wr S_2}(Ds_2) = 22T_{56}$$

ist, wobei $D = y_1 - y_2 = (x_1 + \cdots + x_{11}) - (x_{12} + \cdots + x_{22})$ und $s_2 = d_1d_2$ mit $d_1 = \prod_{1 \leq i < j \leq 11}(x_i - x_j)$ und $d_2 = \prod_{12 \leq i < j \leq 22}(x_i - x_j)$ sind. Für dieses invariante Polynom benötigen wir gerade einmal 110 Multiplikationen.

Nach Proposition 1.9 sind maximale transitive imprimitive Permutationsgruppen Kranzprodukte der Form $S_l \wr_\Gamma S_m$. Da diese Gruppen beim Verfahren von Stauduhar die Nahtstelle zwischen der S_n bzw. A_n und den kleineren imprimitiven Gruppen bilden, werden sie besonders oft frequentiert. Daher ist es sehr wichtig, diese Übergänge effektiv zu gestalten. Mit Hilfe des letzten Satzes konnten viele ungünstige Invarianten ersetzt, und damit das Galoisgruppenprogramm insbesondere für Grade $n > 12$ erst lauffähig gemacht werden.

Wir geben für die Grade $14 \leq n \leq 22$ eine vollständige Übersicht der Gruppen, die wir als Stabilisatoren der Polynome Ds_m, s_m, D, s_1, s_2 aus Satz 6.8 identifiziert haben (vgl. auch [29] für $6 \leq n \leq 12$).

$\underline{n = 14}$: Maximale Kranzprodukte in S_{14} sind $14T_{61} = \sigma(S_7 \wr S_2)\sigma^{-1}$ mit $\sigma = (2, 3, 5, 9)(4, 7, 13, 6, 11)$ und $14T_{57} = \sigma(S_2 \wr S_7)\sigma^{-1}$ mit $\sigma = (2, 8, 14, 6, 12, 4, 10)$.
$G = 14T_{61}$: $\mathrm{Stab}_G(Ds_2) = 14T_{59}^+$, $\mathrm{Stab}_G(s_2) = 14T_{60}$, $\mathrm{Stab}_G(D) = \sigma(S_7 \times S_7)\sigma^{-1}$ mit $\sigma = (2, 3, 5, 9)(4, 7, 13, 6, 11)$ ist intransitiv, $\mathrm{Stab}_G(s_1) = 14T_{58} = \sigma(A_7 \wr S_2)\sigma^{-1}$ mit $\sigma = (2, 3, 5, 9)(4, 7, 13, 6, 11)$.

$G = 14T_{57}$: $\mathrm{Stab}_G(Ds_7) = 14T_{54}$, $\mathrm{Stab}_G(s_7) = 14T_{55}^+$, $\mathrm{Stab}_G(D) = 14T_{56} = \sigma(S_2 \wr A_7)\sigma^{-1}$ mit $\sigma = (2,8,14,6,12,4,10)$, $\mathrm{Stab}_G(s_2) = 14T_{49}$, $\mathrm{Stab}_G(s_1)$ ist intransitiv.

$\underline{n = 15}$: Maximale Kranzprodukte in S_{15} sind $15T_{102} = \sigma(S_5 \wr S_3)\sigma^{-1}$ mit $\sigma = (2,4,10,12)(3,7)(5,13)(8,9,15)$ und $15T_{93} = \sigma(S_3 \wr S_5)\sigma^{-1}$ mit $\sigma = (2,6,14,3,11,5,9,12,15,8)$.

$G = 15T_{102}$: $\mathrm{Stab}_G(Ds_3) = 15T_{99}^+$, $\mathrm{Stab}_G(s_3) = 15T_{100}$, $\mathrm{Stab}_G(D) = 15T_{101} = \sigma(S_5 \wr A_3)\sigma^{-1}$ mit $\sigma = (2,4,10,15,8,9,12)(3,7)(5,13)$, $\mathrm{Stab}_G(s_2) = 15T_{97}$, $\mathrm{Stab}_G(s_1) = 15T_{96} = \sigma(A_5 \wr S_3)\sigma^{-1}$ mit $\sigma = (2,4,10,12)(3,7)(5,13)(8,9,15)$.

$G = 15T_{93}$: $\mathrm{Stab}_G(Ds_5) = 15T_{89}^+$, $\mathrm{Stab}_G(s_5) = 15T_{91}$, $\mathrm{Stab}_G(D) = 15T_{90} = \sigma(S_3 \wr A_5)\sigma^{-1}$ mit $\sigma = (2,6,14,3,11,5,9,12,15,8)$, $\mathrm{Stab}_G(s_2) = 15T_{83}$, $\mathrm{Stab}_G(s_1) = 15T_{78} = \sigma(A_3 \wr S_5)\sigma^{-1}$ mit $\sigma = (2,11,5,14,8)(3,6,9,12,15)$.

$\underline{n = 16}$: Maximale Kranzprodukte in S_{16} sind $16T_{1952} = S_8 \wr S_2, 16T_{1948} = S_2 \wr S_8$ und $16T_{1947} = S_4 \wr S_4$.

$G = 16T_{1952}$: $\mathrm{Stab}_G(Ds_2) = 16T_{1950}$, $\mathrm{Stab}_G(s_2) = 16T_{1951}^+$, $\mathrm{Stab}_G(D) = S_8 \times S_8$ ist intransitiv, $\mathrm{Stab}_G(s_1) = 16T_{1949}^+ = A_8 \wr S_2$.

$G = 16T_{1948}$: $\mathrm{Stab}_G(Ds_8) = 16T_{1946}$, $\mathrm{Stab}_G(s_8) = 16T_{1945}^+$, $\mathrm{Stab}_G(D) = 16T_{1944} = S_2 \wr A_8$, $\mathrm{Stab}_G(s_2) = 16T_{1873}^+$, $\mathrm{Stab}_G(s_1)$ ist intransitiv.

$G = 16T_{1947}$: $\mathrm{Stab}_G(Ds_4) = 16T_{1943}$, $\mathrm{Stab}_G(s_4) = 16T_{1942}^+$, $\mathrm{Stab}_G(D) = 16T_{1941} = S_4 \wr A_4$, $\mathrm{Stab}_G(s_2) = \sigma 16T_{1929}\sigma^{-1}$ mit $\sigma = (11,12)(15,16)$, $\mathrm{Stab}_G(s_1) = \sigma 16T_{1918}\sigma^{-1} = A_4 \wr S_4$ mit $\sigma = (7,8)(15,16)$.

$\underline{n = 18}$: Maximale Kranzprodukte in S_{18} sind $18T_{981} = S_9 \wr S_2, 18T_{968} = S_2 \wr S_9$, $18T_{977} = S_6 \wr S_3$ und $18T_{962} = S_3 \wr S_6$.

$G = 18T_{981}$: $\mathrm{Stab}_G(Ds_2) = 18T_{979}^+$, $\mathrm{Stab}_G(s_2) = 18T_{980}$, $\mathrm{Stab}_G(D) = S_9 \times S_9$ ist intransitiv, $\mathrm{Stab}_G(s_1) = 18T_{978} = A_9 \wr S_2$.

$G = 18T_{968}$: $\mathrm{Stab}_G(Ds_9) = 18T_{965}$, $\mathrm{Stab}_G(s_9) = 18T_{964}^+$, $\mathrm{Stab}_G(D) = 18T_{966} = S_2 \wr A_9$, $\mathrm{Stab}_G(s_2) = \sigma T18_{913}\sigma^{-1}$ mit $\sigma = (3,4)(9,10)(11,12)$, $\mathrm{Stab}_G(s_1)$ ist intransitiv.

$G = 18T_{977}$: $\mathrm{Stab}_G(Ds_3) = 18T_{975}$, $\mathrm{Stab}_G(s_3) = 18T_{976}^+$, $\mathrm{Stab}_G(D) = 18T_{974} = S_6 \wr A_3$, $\mathrm{Stab}_G(s_2) = 18T_{972}$, $\mathrm{Stab}_G(s_1) = 18T_{971} = A_6 \wr S_3$.

$G = 18T_{962}$: $\mathrm{Stab}_G(Ds_6) = 18T_{959}^+$, $\mathrm{Stab}_G(s_6) = 18T_{961}$, $\mathrm{Stab}_G(D) = 18T_{960} = S_3 \wr A_6$, $\mathrm{Stab}_G(s_2) = \sigma 18T_{925}\sigma^{-1}$ mit $\sigma = (5,6)(8,9)(17,18)$, $\mathrm{Stab}_G(s_1) = \sigma 18T_{898}\sigma^{-1} = A_3 \wr S_6$ mit $\sigma = (5,6)(14,15)$.

$\underline{n = 20}$: Maximale Kranzprodukte in S_{20} sind $20T_{1115} = S_{10} \wr S_2$, $20T_{1110} = S_2 \wr S_{10}$, $20T_{1111} = S_5 \wr S_4$ und $20T_{1101} = S_4 \wr S_5$.

$G = 20T_{1115}$: $\mathrm{Stab}_G(Ds_2) = 20T_{1113}$, $\mathrm{Stab}_G(s_2) = 20T_{1114}^+$, $\mathrm{Stab}_G(D) = S_{10} \times S_{10}$ ist intransitiv, $\mathrm{Stab}_G(s_1) = A_{10} \wr S_2 = \sigma 20T_{1112}^+\sigma^{-1}$ mit $\sigma = (19,20)$.

$G = 20T_{1110}$: $\mathrm{Stab}_G(Ds_{10}) = 20T_{1104}$, $\mathrm{Stab}_G(s_{10}) = 20T^+_{1105}$, $\mathrm{Stab}_G(D) = 20T_{1106} = S_2 \wr A_{10}$, $\mathrm{Stab}_G(s_2) = \sigma 20T^+_{1021}\sigma^{-1}$ mit $\sigma = (9,10)(13,14)(17,18)$, $\mathrm{Stab}_G(s_1)$ ist intransitiv.

$G = 20T_{1111}$: $\mathrm{Stab}_G(Ds_4) = 20T^+_{1109}$, $\mathrm{Stab}_G(s_4) = 20T_{1108}$, $\mathrm{Stab}_G(D) = 20T_{1107} = S_5 \wr A_4$, $\mathrm{Stab}_G(s_2) = \sigma 20T_{1092}\sigma^{-1}$ mit $\sigma = (9,10)(14,15)(19,20)$, $\mathrm{Stab}_G(s_1) = A_5 \wr S_4 = \sigma 20T_{1078}\sigma^{-1}$ mit $\sigma = (9,10)$.

$G = 20T_{1101}$: $\mathrm{Stab}_G(Ds_5) = 20T_{1091}$, $\mathrm{Stab}_G(s_5) = 20T^+_{1090}$, $\mathrm{Stab}_G(D) = 20T_{1089} = S_4 \wr A_5$, $\mathrm{Stab}_G(s_2) = \sigma 20T_{1054}\sigma^{-1}$ mit $\sigma = (11,12)(19,20)$, $\mathrm{Stab}_G(s_1) = A_4 \wr S_5 = \sigma 20T^+_{1048}\sigma^{-1}$ mit $\sigma = (7,8)(15,16)(19,20)$.

$\underline{n = 21}$: Maximale Kranzprodukte in S_{21} sind $21T_{162} = S_7 \wr S_3$ und $21T_{152} = S_3 \wr S_7$.

$G = 21T_{162}$: $\mathrm{Stab}_G(Ds_2) = 21T^+_{161}$, $\mathrm{Stab}_G(s_2) = 21T_{160}$, $\mathrm{Stab}_G(D) = 21T_{159} = S_7 \wr A_3$, $\mathrm{Stab}_G(s_1) = A_7 \wr S_3 = \sigma 21T_{156}\sigma^{-1}$ mit $\sigma = (13,14)(20,21)$.

$G = 21T_{152}$: $\mathrm{Stab}_G(Ds_{11}) = 21T^+_{150}$, $\mathrm{Stab}_G(s_{11}) = 21T_{149}$, $\mathrm{Stab}_G(D) = 21T_{151} = S_3 \wr A_7$ $\mathrm{Stab}_G(s_2) = \sigma 21T_{144}\sigma^{-1}$ mit $\sigma = (17,18)(20,21)$, $\mathrm{Stab}_G(s_1) = A_3 \wr S_7 = \sigma 21T_{139}\sigma^{-1}$ mit $\sigma = (8,9)(11,12)(14,15)(17,18)$.

$\underline{n = 22}$: Maximale Kranzprodukte in S_{22} sind $22T_{57} = S_{11} \wr S_2$ und $22T_{53} = S_2 \wr S_{11}$

$G = 22T_{57}$: $\mathrm{Stab}_G(Ds_2) = 22T^+_{55}$, $\mathrm{Stab}_G(D) = S_{11} \times S_{11}$ ist intransitiv, $\mathrm{Stab}_G(s_2) = 22T_{56}$, $\mathrm{Stab}_G(s_1) = A_{11} \wr S_2 = 22T_{54}$.

$G = 22T_{53}$: $\mathrm{Stab}_G(Ds_{11}) = 22T_{50}$, $\mathrm{Stab}_G(s_{11}) = 22T^+_{51}$, $\mathrm{Stab}_G(D) = 22T_{52} = S_2 \wr A_{11}$, $\mathrm{Stab}_G(s_2) = \sigma 22T_{47}\sigma^{-1}$ mit $\sigma = (3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(17,18)(19,20)$, $\mathrm{Stab}_G(s_1)$ ist intransitiv.

6.10. Bemerkung. Die Polynome aus Satz 6.8 lassen sich auch als Invarianten für viele andere Gruppenpaare verwenden, bei denen die Gruppe G kein Kranzprodukt ist (vgl. Tabelle 6.1).

Der zweite Satz zeigt, daß sich invariante Polynome zwischen Kranzprodukten mittels Invarianten der einzelnen Komponenten der Kranzprodukte konstruieren lassen.

6.11. Satz. *Seien $G \le G' \le S_\Lambda$ und $H \le H' \le S_\Gamma$ transitive Gruppen mit $\Lambda := \{1,\dots,l\}$ und $\Gamma := \{1,\dots,m\}$. Wir setzen $y_j := \sum_{\lambda=1}^{l} x_{\lambda,j}$ und $F_j := F(x_{1,j},\dots,x_{l,j})$ für $j = 1,\dots,m$, wobei F ein G'-relatives G-invariantes Polynom ist. Weiterhin sei E ein H'-relatives H-invariantes Polynom. Dann ist*

$$F_1 + F_2 + \cdots + F_m + E(y_1,\dots,y_m)$$

ein $G' \wr_\Gamma H'$-relatives $G \wr_\Gamma H$-invariantes Polynom.

6.12. Bemerkung. Gilt im obigen Satz $G = G'$, so liefert bereits $E(y_1, \ldots, y_m)$ ein $G' \wr_\Gamma H'$-relatives $G \wr_\Gamma H$-invariantes Polynom. Analog genügt für $H = H'$ ein Polynom $F_1 + \ldots + F_m$.

6.13. Beispiel. Betrachten wir die Gruppen $G = 20T_{1055} = S_4 \wr D(5)$ und $H = 20T_{1050} = S_4 \wr C(5)$. Der Algorithmus braucht für den Abstieg mit der bisherigen Methode 160 Multiplikationen. Identifiziert man nach Bemerkung 1.8 die Menge $\{1,2,3,4\} \times \{1,2,3,4,5\}$ mit $\{1, \ldots, 20\}$, so erhält man bezüglich der Vertreter der S_{20}-Konjugationsklassen in [5, 16] für G und H das Blocksystem $\mathcal{B} = \{\{1,2,3,4\}, \{5,6,7,8\}, \{9,10,11,12\}, \{13,14,15,16\}, \{17,18,19,20\}\}$. Nach Bemerkung 6.12 ist $E(y_1, y_2, y_3, y_4, y_5)$ mit $y_j = x_{4j-3} + x_{4j-2} + x_{4j-1} + x_{4j}$, $(1 \leq j \leq 5)$ ein G-relatives H-invariantes Polynom, falls E ein $D(5)$-relatives $C(5)$-invariantes Polynom ist. Mittels Algorithmus 6.4 erhalten wir

$$\begin{aligned} E &= y_1^2 y_2 + y_2^2 y_3 + y_3^2 y_4 + y_4^2 y_5 + y_5^2 y_1 \\ &= y_1(y_1 y_2 + y_5^2) + y_3(y_2^2 + y_3 y_4) + y_4^2 y_5. \end{aligned}$$

Für dieses invariante Polynom benötigen wir nur noch 8 Multiplikationen.

Die folgenden Sätze stellen eine Verallgemeinerung von Satz 6.11 und Bemerkung 6.12 dar, da sich die Aussagen nun nicht mehr nur auf Kranzprodukte beschränken, sondern allgemein für transitive, imprimitive Gruppen gelten.

6.14. Satz. *Seien $H < G < S_n$ transitive, imprimitive Permutationsgruppen, H maximale Untergruppe von G und $\mathcal{B} := \{B_1, \ldots, B_m\}$ ein Blocksystem der Gruppe G, so daß die Permutationsdarstellung $G|_\mathcal{B} \leq S_\Gamma$, $\Gamma := \{1, \ldots, m\}$ von G und die Permutationsdarstellung $H|_\mathcal{B} \leq S_\Gamma$ von H auf den Blöcken von $\mathcal{B}$ verschieden sind. Wir setzen $y_j := \sum_{i \in B_j} x_i$, $(B_j \in \mathcal{B})$ für $j = 1, \ldots, m$. Ist E ein $G|_\mathcal{B}$-relatives $H|_\mathcal{B}$-invariantes Polynom, so ist $E(y_1, \ldots, y_m)$ ein G-relatives H-invariantes Polynom.*

Beweis. Die Gruppe H operiert genau so auf den y_j, $(1 \leq j \leq m)$, wie sie auf den Blöcken $B_j \in \mathcal{B}$ operiert, d.h. $H|_{\{y_1,\ldots,y_m\}} = H|_\mathcal{B}$. Da E ein bezüglich dieser Operationen invariantes Polynom ist, wird $E(y_1, \ldots, y_m)$ von H stabilisiert. Das Polynom $E(y_1, \ldots, y_m)$ wird aber auch nur von den Permutationen aus H stabilisiert, aufgrund der folgenden Überlegungen: Da E ein $G|_\mathcal{B}$-relatives $H|_\mathcal{B}$-invariantes Polynom ist, existiert $\bar{\sigma} \in G|_\mathcal{B} \backslash H|_\mathcal{B}$ mit $\bar{\sigma}(E) \neq E$. Damit folgt für das Urbild $\sigma \in G \backslash H$ von $\bar{\sigma}$ bezüglich der Permutationsdarstellung auf $\mathcal{B}$, daß $\sigma(E(y_1, \ldots, y_m)) \neq E(y_1, \ldots, y_m)$ gilt, da die Variablenmengen der y_j, $(1 \leq j \leq m)$ algebraisch unabhängig sind. Somit ist $H \leq \mathrm{Stab}_G(E(y_1, \ldots, y_m)) \lneq G$ und da H maximal in G ist, folgt $H = \mathrm{Stab}_G(E(y_1, \ldots, y_m))$. □

6.15. Beispiel. Das $20T_{1039}$-relative $20T_{1029}$-invariante Monomsummenpolynom erfordert bei seiner Auswertung $15 \cdot 460800$ Multiplikationen. Die Permutationsgruppe $G = 20T_{1039}$ hat bezüglich der Repräsentanten der S_{20}-Konjugationsklassen in MAGMA [5, 16] die Blocksysteme $\mathcal{B}_1 := \{\{1,2,5,6,9,10,13,14,17,18\},\{3,4,7,8,11,12,15,16,19,20\}\}$ und $\mathcal{B}_2 := \{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{9,10\},\{11,12\},\{13,14\},\{15,16\},\{17,18\},\{19,20\}\}$. Für die Permutationsdarstellung von G und H bezüglich $\mathcal{B}_2$ erhalten wir die Gruppen $G|_{\mathcal{B}_2} = \sigma S_5 \wr S_2 \sigma^{-1} = \tau 10T_{43}\tau^{-1}$ mit $\sigma = (1,2,4,6)(5,9)$, $\tau = (1,2)(4,5)(6,7) \in S_{10}$ und $H|_{\mathcal{B}_2} = \tau 10T_{41}\tau^{-1}$, während die Permutationsdarstellung von $\mathrm{Stab}_G(B_i)$ bzw. $\mathrm{Stab}_H(B_i)$ bezüglich eines fest gewählten Blockes $B_i \in \mathcal{B}_2$ in beiden Fällen die symmetrische Gruppe S_2 ist. Durch Nachrechnen erhalten wir mittels Anwendung von Satz 6.8, daß im Fall $\mathrm{char}(K) \neq 2$ der Stabilisator $\mathrm{Stab}_G(\sigma(s_2))$ des Polynom $\sigma(s_2) = \sigma(d_1)\sigma(d_2) \in K[x_1,\ldots,x_{10}]$ mit $d_1 = \prod_{1\le i<j\le 5}(x_{2i-1} - x_{2j-1})$ und $d_2 = \prod_{1\le i<j\le 5}(x_{2i} - x_{2j})$ die Gruppe $H|_{\mathcal{B}_2}$ ist. Somit ist $\sigma(s_2)$ ein $G|_{\mathcal{B}_2}$-relatives $H|_{\mathcal{B}_2}$-invariantes Polynom. Setzen wir $y_j := x_{2j-1} + x_{2j}$ für $1 \le j \le 10$, so ist das Polynom

$$\sigma(s_2)(y_1,\ldots,y_{10}) = \prod_{1\le i<j\le 5}(y_{\sigma(2i-1)} - y_{\sigma(2j-1)}) \prod_{1\le i<j\le 5}(y_{\sigma(2i)} - y_{\sigma(2j-1)})$$

für $\mathrm{char}(K) \neq 2$ ein G-relatives H-invariantes Polynom. Für diese Invariante benötigen wir nur noch 19 Multiplikationen.

6.16. Satz. *Seien $H < G < S_n$ transitive, imprimitive Permutationsgruppen, H maximale Untergruppe von G und $B_i \in \mathcal{B} := \{B_1,\ldots,B_m\}$, $|B_i| = l$ ein Block eines Blocksystems $\mathcal{B}$ der Gruppe G, so daß die Permutationsdarstellung von* $\mathrm{Stab}_G(B_i)$ *und* $\mathrm{Stab}_H(B_i)$ *auf der Menge B_i verschieden ist. Wir bezeichnen die Permutationsdarstellung von* $\mathrm{Stab}_G(B_i)$ *bzw.* $\mathrm{Stab}_H(B_i)$ *auf der Menge B_i mit* $\mathrm{Stab}_G(B_i)|_{B_i}$ *und* $\mathrm{Stab}_H(B_i)|_{B_i}$. *Ist $\{\sigma_1,\ldots,\sigma_m\}$ ein vollständiges System von linken Nebenklassen von* $\mathrm{Stab}_H(B_i)$ *in H und $F(x_{i_1},\ldots,x_{i_l}) \in K[x_{i_1},\ldots,x_{i_l}]$ für $i_1,\ldots,i_l \in B_i$ ein* $\mathrm{Stab}_G(B_i)|_{B_i}$*-relatives* $\mathrm{Stab}_H(B_i)|_{B_i}$*-invariantes Polynom, so ist $\sigma_1(F) + \cdots + \sigma_m(F)$ ein G-relatives H-invariantes Polynom.*

Beweis. Sei o.B.d.A $\sigma_1 = \mathrm{id}$. Die Menge $\{\sigma_1(F),\ldots,\sigma_m(F)\}$ ist algebraisch unabhängig, da die Variablenmengen in den Polynomen $\sigma_j(F)$, $(1 \le j \le m)$ disjunkt sind, und es gilt $\mathrm{Orb}_H(F) = \{\sigma_1(F),\ldots,\sigma_m(F)\}$, da $\tau_1\mathrm{Stab}_H(B_i) = \tau_2\mathrm{Stab}_H(B_i) \Leftrightarrow \tau_1 F = \tau_2 F$ für $\tau_1,\tau_2 \in H$ ist. Somit ist das Polynom $F_H := \sigma_1(F) + \cdots + \sigma_m(F)$ H-invariant. Zu zeigen bleibt, daß $\mathrm{Stab}_G(F_H) = H$ ist. Nach Voraussetzung ist $H = \cup_{j=1}^m \sigma_j \mathrm{Stab}_H(B_i)$ und $\mathcal{B} = \{\sigma_1(B_i),\ldots,\sigma_m(B_i)\}$ nach Huppert [37], Kapitel II, Satz 1.2. Da $\mathcal{B}$ ebenfalls Blocksystem von G ist, folgt $[G : \mathrm{Stab}_G(B_i)] = [H : \mathrm{Stab}_H(B_i)] = m$ und aus $\sigma_j^{-1}\sigma_k \notin \mathrm{Stab}_G(B_i)$, $j \neq k$ erhalten wir somit $G = \cup_{j=1}^m \sigma_j \mathrm{Stab}_G(B_i)$. Sei nun $\bar{\tau} \in \mathrm{Stab}_G(B_i)|_{B_i} \backslash \mathrm{Stab}_H(B_i)|_{B_i}$.

Bezeichne $\tau \in \mathrm{Stab}_G(B_i)\backslash\mathrm{Stab}_H(B_i)$ das Urbild von $\bar{\tau}$ bezüglich der Permutationsdarstellung von $\mathrm{Stab}_G(B_i)$ auf B_i, so gilt $\tau(F) \neq F$ und $\tau(F)$ ist algebraisch unabhängig von $\tau\sigma_2(F), \ldots, \tau\sigma_m(F)$ (disjunkte Variablenmengen). Es folgt $\tau(F_H) \neq F$ und $H \leq \mathrm{Stab}_G(F_H) \lneqq G$. Da H maximal in G ist, erhalten wir $\mathrm{Stab}_G(F_H) = H$. □

6.17. Bemerkung. Gelten die Voraussetzungen von Satz 6.14, so ist $H_{\mathcal{B}}$ maximale transitive Untergruppe von $G_{\mathcal{B}}$. Analog erhalten wir im Fall von Satz 6.16, daß $\mathrm{Stab}_H(B_i)|_{B_i}$ maximale transitive Untergruppe von $\mathrm{Stab}_G(B_i)|_{B_i}$ ist.

6.18. Beispiel. Betrachten wir die Gruppen $G = 16T^+_{1951}$ und $H = 16T^+_{1949}$. Verwenden wir eine Invariante, die als Bahnsumme von Monomen dargestellt ist, so brauchen wir für diesen Abstieg $27 \cdot 40320$ Multiplikationen. Bezüglich der Vertreter der S_{16}-Konjugationsklassen in MAGMA [5, 16] ist $\mathcal{B} = \{\{1,2,3,4,5,6,7,8\}, \{9,10,11,12,13,14,15,16\}\}$ ein Blocksystem von G. Sei $B_1 := \{1,2,3,4,5,6,7,8\}$. Es gilt $\mathrm{Stab}_G(B_1)|_{B_1} = S_8$, $\mathrm{Stab}_H(B_1)|_{B_1} = A_8$ und $G|_{\mathcal{B}} = H|_{\mathcal{B}} = S_2$. Nach Bemerkung 2.11 ist für $\mathrm{char}(K) \neq 2$ das Polynom $F = \prod_{1 \leq i < j \leq 8}(x_i - x_j)$ ein S_8-relatives A_8-invariantes Polynom. Als Nebenklassenrepräsentantensystem von $\mathrm{Stab}_H(B_1)$ in H erhalten wir $\sigma_1 = \mathrm{id}$ und $\sigma_2 = (1,16,6,14,2,10)(3,11,8,13,7,15,5,9,4,12)$. Somit ist

$$F + \sigma_2 F$$

für $\mathrm{char}(K) \neq 2$ ein G-relatives H-invariantes Polynom, für daß wir nur noch 54 Multiplikationen benötigen.

6.19. Bemerkung. Seien wieder $H < G < S_n$ transitive, imprimitive Permutationsgruppen und H maximal in G. Stimmen die Permutationsdarstellungen von G und H auf allen nichttrivialen Blocksystemen überein und sind auch die Permutationsdarstellungen von $\mathrm{Stab}_G(B_i)$ und $\mathrm{Stab}_H(B_i)$ auf den Blöcken B_i der nichttrivialen Blocksysteme gleich, so bietet sich die folgende Strategie an, um eine günstigere Invariante zu finden: Ist $\mathcal{B}$ ein nichttriviales Blocksystem von G und $B_i \in \mathcal{B}$ ein festgewählter Block, so suchen wir nach einem transitiven Gruppenpaar $K_1 < K_2 \leq \mathrm{Stab}_G(B_i)|_{B_i}$ (in unseren Anwendungen beschränken wir uns auf Gruppenpaare K_1, K_2, wobei K_1 maximal in K_2 ist) und einem K_2-relativen K_1-invarianten Polynom Y_1, so daß die Permutationsdarstellung $G|_{\mathcal{O}}$ von G auf $\mathcal{O} := Orb_G(Y_1)$ verschieden von der Permutationsdarstellung $H|_{\mathcal{O}}$ ist. Die Gruppe $H|_{\mathcal{O}}$ ist dann maximale transitive Untergruppe der Gruppe $G|_{\mathcal{O}}$, da $Orb_G(Y_1) = Orb_H(Y_1)$ gilt und H nach Voraussetzung maximale Untergruppe von G ist. Ist F ein $G|_{\mathcal{O}}$-relatives $H|_{\mathcal{O}}$-invariantes Polynom, so testen wir, ob $F(Y_1, \ldots, Y_{|\mathcal{O}|})$ ein G-relatives H-invariantes Polynom ist. Das Problem im Vergleich zu den vorherigen Sätzen ist, daß die $Y_1, \ldots, Y_{|\mathcal{O}|}$ nicht unbedingt algebraisch unabhängig sind, und somit das Polynom $F(Y_1, \ldots, Y_{|\mathcal{O}|})$ zwar H-invariant,

aber eventuell nicht G-relativ ist. Ist letzteres der Fall, läßt sich durch geeignete Tschirnhausentransformation der Y_j ein G-relatives H-invariantes Polynom der Form $F(h(Y_1),\ldots,h(Y_{|\mathcal{O}|}))$, $h \in K[X]$ erhalten (vgl. Bemerkung 2.15 und Satz 2.16).

Mit der eben beschriebenen Vorgehensweise konnten für fast 300 Gruppenpaare der Grade $16-22$ bessere Invarianten gefunden werden. Wir geben ein Beispiel.

6.20. Beispiel. Betrachten wir die Gruppen $G = 16T^+_{1937}$ und $H = 16^+_{1917}$. Mit unseren bisherigen Mitteln hatten wir für den Abstieg von G in die maximale Untergruppe H das invariante Polynom $F = \sum_{\tilde{m}\in \mathrm{Orb}_H(m)} \tilde{m}$ mit $m = x_1^3x_2^2x_3x_5^3x_6^2x_7$ gefunden, dessen Auswertung uns $11 \cdot 1728$ Multiplikationen kostet. Bezüglich der Vertreter der S_{16}-Konjugationsklassen aus [5, 16] hat die Gruppe G das Blocksystem $\mathcal{B} = \{\{1,2,3,4\},\{5,6,7,8\},\{9,10,11,12\},\{13,14,15,16\}\}$, und es gilt sowohl $G|_{\mathcal{B}} = H|_{\mathcal{B}} = A_4$, als auch $\mathrm{Stab}_G(B_i)|_{B_i} = \mathrm{Stab}_H(B_i)|_{B_i} = S_4$ für $B_i \in \mathcal{B}$. Sei nun $B_i = \{9,10,11,12\}$ fixiert und $K_2 = S_4$ und $K_1 = D(4)$ (auf den Ziffern von B_i). Da die Gruppe $D(4)$ im Gegensatz zu S_4 imprimitiv mit Blocksystem $\{\{9,11\},\{10,12\}\}$ ist, ist $Y_1 = (x_9 + x_{11})(x_{10} + x_{12})$ ein S_4-relatives $D(4)$-invariantes Polynom. Es gilt $\mathcal{O} := \mathrm{Orb}_G(Y_1) = \{Y_1,\ldots,Y_{12}\}$ mit

$$
\begin{array}{lll}
Y_2 = (x_9 + x_{12})(x_{10} + x_{11}) & Y_3 = (x_1 + x_2)(x_3 + x_4) & Y_4 = (x_5 + x_8)(x_6 + x_7) \\
Y_5 = (x_1 + x_4)(x_2 + x_3) & Y_6 = (x_5 + x_6)(x_7 + x_8) & Y_7 = (x_5 + x_7)(x_6 + x_8) \\
Y_8 = (x_{13} + x_{12})(x_{14} + x_{15}) & Y_9 = (x_{13} + x_{12})(x_{14} + x_{16}) & Y_{10} = (x_{13} + x_{14})(x_{15} + x_{16}) \\
Y_{11} = (x_9 + x_{10})(x_{11} + x_{12}) & Y_{12} = (x_1 + x_3)(x_2 + x_4) &
\end{array}
$$

Die Permutationsdarstellung $G|_{\mathcal{O}}$ ist isomorph zur Gruppe $\sigma 12T^+_{271}\sigma^{-1}$ mit $\sigma = (2,3,8,6,5)(7,9,11,10,12)$, während die Permutationsdarstellung $H|_{\mathcal{O}}$ isomorph zu $\sigma 12T^+_{234}\sigma^{-1}$ ist. Für $\mathrm{char}(K) \neq 2$ ist das Polynom $F = s_2(\sigma(d_1),\ldots,\sigma(d_4))$ für $d_k = (x_k - x_{k+4})(x_k - x_{k+8})(x_{k+4} - x_{k+8})$, $(1 \leq k \leq 4)$ ein $\sigma 12T^+_{271}\sigma^{-1}$-relatives $\sigma 12T^+_{234}\sigma^{-1}$-invariantes Polynom. Durch Nachrechnen verifizieren wir, daß $F(Y_1,\ldots,Y_{12})$ im Fall $\mathrm{char}(K) \neq 2$ ein G-relatives H-invariantes Polynom, für daß wir weniger als 30 Multiplikationen benötigen.

Der folgende Satz (vgl. Eichenlaub [22], Abschnitt 2.1.2, Proposition 2) beschäftigt sich mit Untergruppen der Gruppe G vom Index 2. Im wesentlichen geht es darum, aus bereits bekannten G-relativen H-invarianten Polynomen F mit $[\,G:H\,] = 2$ Invarianten für andere Untergruppen von G vom Index 2 zu konstruieren. Dabei werden die bekannten Invarianten so abgeändert, daß die zugehörige Resolvente von der Form $X^2 - F^2(\alpha_1,\ldots,\alpha_n)$ ist, wobei mit α_i, $(1 \leq i \leq n)$ wieder die Nullstellen des Polynoms f bezeichnet seien.

6.21. Satz. *Sei* $\mathrm{char}(K) \neq 2$. *Die Permutationsgruppe G habe die Untergruppen H_1 und H_2 vom Index* 2. *Seien $F_i, (i = 1,2)$ G-relative H_i-invariante Polynome,*

für die $\sigma_i F_i = -F_i$, $(\sigma_i \in G\backslash H_i)$ gelte. Dann ist $H_1+H_2 := (H_1\cap H_2)\cup((G\backslash H_1)\cap (G\backslash H_2))$ ebenfalls eine Untergruppe von G, und F_1F_2 ist ein G-relatives H_1+H_2-invariantes Polynom.

6.22. Bemerkung. (i) Die Bedingung $\sigma_i F_i = -F_i$, $(\sigma_i \in G\backslash H_i)$ stellt keine Einschränkung dar, da F_i durch die Invariante $F_i' = F_i - \sigma_i F_i$, $\sigma_i \in G\backslash H_i$ ersetzt werden kann.
(ii) Für $H_1 \neq H_2 \neq G$ ist $H_1 + H_2$ Untergruppe vom Index 2. Darüber hinaus ist die Operation + assoziativ und kommutativ mit neutralem Element G, d.h. $H + G = H$ für alle Untergruppen H vom Index 2. Außerdem gilt $H + H = G$.

6.23. Beispiel. Das $20T_{1055}$ -relative $20T_{1051}$ -invariante Monomsummenpolynom erfordert bei seiner Auswertung $32 \cdot 39813120$ Multiplikationen. Die Permutationsgruppe $20T_{1055}$ hat die Untergruppen $20T_{1051}$, $20T_{1050}$, $20T^+_{1049}$ vom Index 2. Durch direktes Nachrechnen läßt sich verifizieren, daß $20T_{1051} = 20T_{1050} + 20T^+_{1049}$ gilt. Beginnen wir mit dem $20T_{1055}$-relativen $20T_{1050}$-invarianten Polynom. In Beispiel 6.13 hatten wir das Polynom $E = y_1(y_1\ y_2 + y_5^2) + y_3(y_2^2 + y_3y_4) + y_4^2y_5$ als Invariante gefunden. Die Bilder dieses Polynoms unter den Permutationen von $20T_{1055}$ sind E und $\sigma E = y_1(y_1y_5+y_2^2)+y_4(y_5^2+y_3y_4)+y_3^2y_2$, $(\sigma \in 20T_{1055}\backslash 20T_{1050})$. Somit ist das Polynom

$$\begin{aligned} E - \sigma E &= y_1(y_2 - y_5)(y_1 - y_2 - y_5) + y_3(y_4 - y_2)(y_3 - y_2 - y_5) + \\ &\quad y_4y_5(y_4 - y_5) \end{aligned}$$

ein $20T_{1055}$-relatives $20T_{1050}$-invariantes Polynom, welches den Voraussetzungen von Satz 6.21 genügt. Nun gilt es, eine Invariante für den Abstieg von $20T_{1055}$ nach $20T^+_{1049}$ zu finden. Nach Bemerkung 2.12 (i) ist generell für einen Abstieg zwischen ungeraden und geraden Gruppen und $\mathrm{char}(K) \neq 2$ das Polynom $\prod_{1\le i<j\le 20}(x_i - x_j)$ eine Invariante. Mittels Satzes 6.8 läßt sich aber für $\mathrm{char}(K) \neq 2$ ein $20T_{1055}$-relatives $20T^+_{1049}$-invariantes Polynom mit weniger Multiplikationen finden. Durch Nachrechnen erhält man $\mathrm{Stab}_{20T_{1055}}(s_5) = 20T^+_{1049}$ mit

$$s_5 = \prod_{1\le k\le 5} \prod_{4k-3\le i<j\le 4k} (x_i - x_j).$$

Außerdem gilt $\sigma(s_5) = -s_5$ für $\sigma \in 20T_{1055}\backslash 20T^+_{1049}$, womit die Voraussetzungen von Satz 6.21 erfüllt sind. Multiplikation der einzelnen Polynome liefert das $20T_{1055}$-relative $20T_{1051}$-invariante Polynom

$$(E - \sigma E)s_5$$

für das wir weniger als 40 Multiplikationen benötigen.

Abschließend geben wir eine Übersicht über die Anzahl der gefundenen Gruppenpaare, die auf die vorgestellten Methoden für Körper K mit $\mathrm{char}(K) \neq 2$ zutreffen. Tabelle 6.1 beinhaltet für jeden Grad n mit $3 \leq n \leq 23$ die folgenden Informationen: Die Anzahl der transitiven Permutationsgruppen des jeweiligen Grades in Spalte 2. In Spalte 3 steht die Gesamtanzahl transitiver Gruppenpaare G, H des Grades n, wobei H maximal in G ist. Die restlichen Spalten besagen für wieviele der Gruppenpaare aus Spalte 3 mit den entsprechenden Methoden Invarianten gefunden werden konnten. Dabei sind natürlich Mehrfachnennungen möglich. Speziell bei der Methode nach Satz 6.21 muß für die Implementierung geprüft werden, ob die erhaltene Invariante die beste Wahl darstellt.

Grad	Anzahl transitive Gruppen	Anzahl Gruppen-paare	Methode Satz 6.8	Methode Satz 6.14, Satz 6.16	Methode Satz 6.21
3	2	1	0	0	0
4	5	5	2	0	0
5	5	5	0	0	0
6	16	28	16	6	6
7	7	8	0	0	0
8	50	104	77	59	25
9	34	65	43	20	17
10	45	87	51	34	16
11	8	9	0	0	0
12	301	890	698	635	266
13	9	10	0	0	0
14	63	133	73	60	9
15	104	259	164	138	66
16	1954	8238	4605	6685	5502
17	10	12	0	0	0
18	983	3500	2407	2719	1120
19	8	10	0	0	0
20	1117	3726	2184	2715	1526
21	164	428	228	222	72
22	59	122	71	58	9
23	7	8	0	0	0

Tabelle 6.1: Methoden zur Invariantenberechnung

Wir beenden diesen Abschnitt mit einer Zusammenfassung des Algorithmus zur Invariantenberechnung, wie wir ihn in unserem Programm verwenden. Dabei soll vor allem noch einmal die Rekursivität der besprochenen Methoden dargestellt werden, die letztendlich die Effektivität und Flexibilität des Algorithmus aus-

macht. Die oben angeführten Beispiele belegen, daß ohne diesen Algorithmus die Galoisgruppenberechnung in größeren Graden unmöglich wäre.
Die Implementierung hängt natürlich entscheidend von dem Vorhandensein entsprechender gruppen- und invariantentheoretischer Routinen ab. Ohne diese mußten in früheren Implementierungen speziell konstruierte Invarianten für einzelne Gruppenpaare per Hand eingegeben werden.

6.24. Algorithmus. *(Berechnung G-relativer H-invarianter Polynome unter Beachtung der Gruppenstruktur)*

Eingabe: *Eine Permutationsgruppe $G \leq S_n$, $(n > 2)$ und eine maximale transitive Untergruppe H von G.*

Ausgabe: *G-relatives H-invariantes Polynom $F \in K[x_1, \ldots, x_n]$.*

1. *(G, H primitiv?) Sind G, H primitiv, so setze im Fall $\mathrm{char}(K) \neq 2$, G ungerade und H gerade Permutationsgruppe $F \leftarrow \prod_{1 \leq i < j \leq n}(x_i - x_j)$ und terminiere, ansonsten gehe zu Schritt 7.*

2. *(Blocksysteme) Berechne nichttriviale Blocksysteme $\mathcal{B}_G, \mathcal{B}_H$ von G bzw. H.*

3. *(Methode Satz 6.8: D, s_1, s_m, s_2, Ds_m ist Invariante?) Ist $\mathrm{char}(K) = 2$, so gehe zu Schritt 4, ansonsten zu Schritt 3.1.*

   3.1 *Existiert $\mathcal{B} \in \mathcal{B}_H \backslash \mathcal{B}_G$, so setze $F \leftarrow \prod_{B_i \in \mathcal{B}} \sum_{i \in B_i} x_i$. Terminiere.*

   3.2 *Für alle $\mathcal{B} \in \mathcal{B}_G = \mathcal{B}_H$ mache:*

      3.2.1 *Setze $m \leftarrow |\mathcal{B}|$, $l \leftarrow |B_i|$, $B_i \in \mathcal{B}$, $y_i \leftarrow \sum_{k \in B_i} x_k$, $(1 \leq i \leq m)$ und $d_k \leftarrow \prod_{1 \leq i < j \leq l}(x_{b_i} - x_{b_j})$ für $B_k = \{b_1, \ldots, b_l\}$, $(1 \leq k \leq m)$.*

      3.2.2 *Ist $D(y_1, \ldots, y_m)$ G-relativ H-inv., setze $F \leftarrow D$. Terminiere.*

      3.2.3 *Ist $s_1(d_1, \ldots, d_m)$ G-relativ H-inv., setze $F \leftarrow s_1$. Terminiere.*

      3.2.4 *Ist $s_m(d_1, \ldots, d_m)$ G-relativ H-inv., setze $F \leftarrow s_m$. Terminiere.*

      3.2.5 *Ist $s_2(d_1, \ldots, d_m)$ G-relativ H-inv., setze $F \leftarrow s_2$. Terminiere.*

      3.2.6 *Ist $D(y_1, \ldots, y_m)s_m(d_1, \ldots, d_m)$ G-relativ H-invariant, setze $F \leftarrow Ds_m$. Terminiere.*

4. *(Methode Satz 6.14, 6.16: $H|_{\mathcal{B}} \lneqq G|_{\mathcal{B}}$ oder $\mathrm{Stab}_H(B_i)|_{B_i} \lneqq \mathrm{Stab}_G(B_i)|_{B_i}$?)*

   4.1 *Für alle $\mathcal{B} \in \mathcal{B}_G = \mathcal{B}_H$ mache:*

      4.1.1 *Berechne Permutationsdarstellung $G|_{\mathcal{B}}$, $H|_{\mathcal{B}}$.*

      4.1.2 *Gilt $H|_{\mathcal{B}} \lneqq G|_{\mathcal{B}}$, setze $y_i \leftarrow \sum_{k \in B_i} x_k$, $(1 \leq i \leq |\mathcal{B}|)$, rufe Algorithmus 6.24 für $G|_{\mathcal{B}}$, $H|_{\mathcal{B}}$ auf. Erhalte $G|_{\mathcal{B}}$-relatives $H|_{\mathcal{B}}$-invariantes Polynom E. Setze $F \leftarrow E(y_1, \ldots, y_{|\mathcal{B}|})$. Terminiere.*

4.1.3 Berechne Permutationsdarstellung $\mathrm{Stab}_G(B_i)|_{B_i}$, $\mathrm{Stab}_H(B_i)|_{B_i}$ *für beliebigen, fest gewählten Block* $B_i \in \mathcal{B}$.

4.1.4 Gilt $\mathrm{Stab}_H(B_i)|_{B_i} \lneqq \mathrm{Stab}_G(B_i)|_{B_i}$, *so rufe Algorithmus 6.24 für* $\mathrm{Stab}_G(B_i)|_{B_i}$, $\mathrm{Stab}_H(B_i)|_{B_i}$ *auf. Erhalte* $\mathrm{Stab}_G(B_i)|_{B_i}$*-relatives* $\mathrm{Stab}_H(B_i)|_{B_i}$*-invariantes Polynom* $\tilde{F}$. *Berechne Nebenklassenrepr.* $C \leftarrow H//\mathrm{Stab}_H(B_i)$. *Setze* $F \leftarrow \sum_{\sigma\in C} \sigma(\tilde{F})$. *Terminiere.*

5. *(Methode Satz 6.21:* $H = H_1 + H_2$ *mit* $[G:H] = [G:H_1] = [G:H_2] = 2$ *?) Ist* $\mathrm{char}(K) = 2$, *so gehe zu Schritt 6, ansonsten zu Schritt 5.1.*

   5.1 Sind H_1, H_2 *gespeichert mit* $H = H_1 + H_2$, *so rufe Algorithmus 6.24 für* G, H_1 *und* G, H_2 *auf, und erhalte* G*-relative* H_i*-invariante Polynome* F_i, $(i = 1, 2)$. *Ansonsten gehe zu Schritt 6.*

   5.2 Ist $\sigma_i F_i \neq -F_i$ *für* $\sigma_i \in G\backslash H_i$, *setze* $F_i \leftarrow F_i - \sigma_i F_i\,(i = 1, 2)$. *Setze* $F \leftarrow F_1 F_2$. *Terminiere.*

6. *(Methode Bem. 6.19: Gruppenpaar* $K_1 < K_2$ *gespeichert mit* $H|_{\mathrm{Orb}_G(Y_1)} \lneqq G|_{\mathrm{Orb}_G(Y_1)}$ *für* K_2*-relatives* K_1*-invariantes Polynom* Y_1*)*

   6.1 Sind K_1, K_2 *gespeichert mit* $H|_{\mathrm{Orb}_H(Y_1)} \lneqq G|_{\mathrm{Orb}_G(Y_1)}$, *so rufe Algorithmus 6.24 für* K_2, K_1 *auf, und erhalte* K_2*-relatives* K_1*-invariantes Polynome* Y_1. *Ansonsten gehe zu Schritt 7.*

   6.2 Berechne $\mathcal{O} \leftarrow \mathrm{Orb}_G(Y_1) = \{Y_1, \ldots, Y_{|\mathcal{O}|}\}$ *und* $H|_{\mathcal{O}}$, $G|_{\mathcal{O}}$.

   6.3 Rufe Algorithmus 6.24 für $G|_{\mathcal{O}}, H|_{\mathcal{O}}$ *auf. Erhalte* $G|_{\mathcal{O}}$*-relatives* $H|_{\mathcal{O}}$*-invariantes Polynom* F. *Setze* $F \leftarrow F(Y_1, \ldots, Y_{|\mathcal{O}|})$. *Terminiere.*

7. *(Methode Satz 6.2: Monom* m *gespeichert mit* $|\mathrm{Orb}_H(m)| \neq |\mathrm{Orb}_G(m)|$ *?)*

   7.1 Sind für G, H *Monom* m *mit* $|\mathrm{Orb}_H(m)| \neq |\mathrm{Orb}_G(m)|$ *gespeichert, so setze* $F \leftarrow \sum_{\tilde{m}\in\mathrm{Orb}_H(m)} \tilde{m}$ *und terminiere. Ansonsten gehe zu Schritt 8.*

8. *(Methode Algorithmus 6.4)*

   8.1 Rufe Algorithmus 6.4 für G, H *auf. Erhalte* G*-relatives* H*-invariantes Polynom* F. *Terminiere.*

6.2 Maximale Konjugationsklassen

Die algorithmischen Möglichkeiten zur Berechnung von Konjugationsklassen von (maximalen) Untergruppen einer endlichen Permutationsgruppe haben sich innerhalb der letzten 5 Jahre dramatisch verbessert. Bis vor nicht allzu langer Zeit

basierte der einzig realisierbare Ansatz zu diesem Problem auf der zyklischen Erweiterungsmethode, welche zuerst von Neubüser 1960 (vgl. [61]) vorgestellt wurde. Die Idee dieser Methode ist, neue Untergruppen als zyklische Erweiterungen bekannter Untergruppen zu konstruieren. Ausgangspunkt dieses Algorithmus ist die Bestimmung aller zyklischen Untergruppen von Primzahlordnung, welche die erste Ebene im Untergruppengitter bilden. Untergruppen G der nächsten Ebene werden aus Untergruppen H der vorhergehenden Ebene mit $G =< H, \sigma >$ gebildet, wobei $H \lhd G$ ist. Ohne weitere Zusatzinformationen können auf diese Art und Weise nur auflösbare Gruppen erreicht werden. Die nicht auflösbaren Untergruppen lassen sich ähnlich konstruieren, benötigen aber die perfekten Gruppen als erste Ebene. Dieses Verfahren ist im allgemeinen schnell für Gruppen der Ordnung 1000 und hat passable Laufzeiten für viele Gruppen bis zur Ordnung 10000. Cannon, Cox, Holt stellen in ihrem Artikel "Computing the Subgroups of a Permutation Group" (2001) [9] ein neues Verfahren zur Berechnung der Konjugationsklassen von Untergruppen von Permutationsgruppen dar, welches in MAGMA [5, 16] implementiert ist. Im Gegensatz zur zyklischen Erweiterungsmethode werden, ausgehend von der gegebenen Gruppe G, nach unten hin die Konjugationsklassen der Untergruppen bestimmt. Dies geschieht durch Berechnung einer Kompositionsreihe $\mathrm{id} = N_0 \lhd N_1 \lhd \cdots \lhd N_r \lhd G$ mit abelschen Faktoren, bei der G/N_r nur triviale auflösbare Normalteiler hat. Anschließend werden die Konjugationsklassen der größeren Faktorgruppe G/N_{i-1} aus der Faktorgruppe G/N_i bestimmt, wobei dafür (insbesondere für die nicht auflösbaren Gruppen) Datenbanken für perfekte und einfache Gruppen notwendig sind.

Während wir vor einigen Jahren noch mehrere Wochen zur Bestimmung der maximalen Konjugationsklassen für Grad 12 (auf mehreren Rechnern gleichzeitig) benötigen, haben sich während der Implementierung der Grade $13 \leq n \leq 23$ die Berechnungszeiten auf wenige Tage verringert, wobei die Bestimmung maximaler Untergruppen auf Gruppen G mit $|G/N_r| \leq 216000$ beschränkt war. Da die symmetrische Gruppe S_n und die alternierende Gruppe A_n für $n \geq 5$ nicht auflösbar sind, folgt schon für $n = 9$, daß $|S_9/N_r| = |S_9/\mathrm{id}| > 216000$ ist ($G/N_r = \mathrm{id}$ genau dann, wenn G auflösbar ist). Für diese Gruppen aber lassen sich die maximalen Konjugationsklassen per Hand bestimmen. Die dafür relevante Hauptaussage ist die folgende (vgl. Dixon, Mortimer [20], Abschnitt 8.5):

6.25. Satz. *Die maximalen Untergruppen G der Gruppen S_n lassen sich im wesentlichen in drei Klassen aufteilen. Sie sind entweder*

(i) intransitiv: G ist der Mengenstabilisator einer Menge der Länge m mit $1 \leq m < n/2$ und somit isomorph zu $S_m \times S_{n-m}$.

(ii) imprimitiv: G ist der Stabilisator einer Partition der Menge $\{1, 2, \ldots, n\}$

in m gleiche Teile der Länge k mit $1 < m < n$ und somit isomorph zum Kranzprodukt $S_k \wr S_m$.

(iii) primitiv: $G = A_n$ oder eine echte primitive Untergruppe der S_n.

Die maximalen imprimitiven Gruppen der symmetrischen Gruppe S_n lassen sich leicht finden. Für die Grade $13 \leq n \leq 23$ sind dies die auf Seite 134f. aufgeführten Kranzprodukte. Es ist klar, daß für $G = S_n$ zu einer maximalen Untergruppe H nur eine Konjugationsklasse existiert. Die maximalen imprimitiven Untergruppen der alternierenden Gruppe A_n erhält man bis auf eine Ausnahme ($8T_{39}^{+} = S_2 \wr S_4 \cap A_8 < AGL(3,2) < A_8$) durch Schnitte mit den maximalen imprimitiven Gruppen der S_n, also durch Schnitte mit den entsprechenden Kranzprodukten. Im „ATLAS of finite groups“ [17] findet man für $n \leq 12$ die maximalen primitiven Gruppen der S_n und A_n. Ansonsten geben Liebeck, Praeger, Saxl [50] eine vollständige Klassifikation der maximalen Untergruppen der endlichen alternierenden und symmetrischen Gruppen, mittels derer wir die folgende Tabelle erhalten haben. Dabei sind auch die Artikel von Kleidman, Liebeck [40] und der Artikel von Buekenhout, Leemans [6], in dem die primitiven Gruppen vom Grad ≤ 50 aufgelistet sind, sehr hilfreich.

Grad	S_n	A_n
13	$13T_6 \cong AGL(1,13)$	$13T_7^{+} \cong PSL(3,3)$ $13T_5^{+} \cong A_{13} \cap AGL(1,13)$
14	$14T_{39} \cong PGL(2,13)$	$14T_{30}^{+} \cong PSL(2,13)$
15		$15T_{72}^{+} \cong PSL(4,2)$
16		$16T_{1906}^{+} \cong AGL(4,2)$
17	$17T_5 \cong AGL(1,17)$	$17T_8^{+} \cong P\Gamma L(2,16)$
18	$18T_{468} \cong PGL(2,17)$	$18T_{377}^{+} \cong PSL(2,17)$
19	$19T_6 \cong AGL(1,19)$	$19T_5^{+} \cong A_{19} \cap AGL(1,19)$
20	$20T_{362} \cong PGL(2,19)$	$20T_{272}^{+} \cong PSL(2,19)$
21	$21T_{103} \cong P\Gamma L(3,4)$ $21T_{85} \cong P\Sigma L(3,4)$ $21T_{38} \cong A_7$ $21T_{20} \cong PGL(2,7)$	$21T_{91}^{+} \cong PGL(3,4)$ $21T_{67}^{+} \cong PSL(3,4)$ $21T_{33}^{+} \cong A_7$
22	$22T_{41} \cong M(22):2$	$22T_{38}^{+} \cong M(22)$
23	$23T_4 \cong AGL(1,23)$	$23T_5^{+} \cong M(23)$

Tabelle 6.2: Maximale primitive Untergruppen der S_n und A_n, $(13 \leq n \leq 23)$

Mittels Korollars 2.10 können wir durch Berechnung der Normalisatoren $N_{S_n}(H)$ der maximalen Untergruppen H von A_n ermitteln, wieviele A_n-Konjugationsklassen es gibt. Bis auf die Gruppen $H = 13T_7^{+}$,$15T_{72}^{+}$,$16T_{1906}^{+}$ und $17T_8^{+}$ gilt $N_{S_n}(H) \neq$

H. Für die eben genannten Gruppen ist also $N_{S_n}(H) = H$, und es gibt in A_n zwei Klassen maximaler Untergruppen, die isomorph zur entsprechenden Gruppe H sind. Wenn wir die Gruppe H mit einem Element aus S_n konjugieren, welches nicht in A_n liegt, so müssen wir die andere Klasse treffen, da $\sigma H\sigma^{-1} = \tau H\tau^{-1}$, $(\sigma \in A_n, \tau \in S_n \backslash A_n)$ genau dann, wenn $\sigma^{-1}\tau \in N_{S_n}(H)$ ist. Somit müssen wir nun für alle Gruppen außer S_n, A_n Repräsentanten der Konjugationsklassen aller maximalen Untergruppen finden. Insgesamt sind 3817 Gruppen der Grade $13 \leq n \leq 23$ auflösbar d.h. es gibt eine Kompositionsreihe mit Faktoren, die zyklisch von Primzahlordnung sind und die Berechnung der maximalen G-Konjugationsklassen bereitet keine Probleme. Für 162 von den restlichen 661 nicht auflösbaren Gruppen G gilt $|G/N_r| > 216000$ (ausgenommen S_n und A_n). Für diese Permutationsgruppen verdanken wir John Cannon die Berechnung der maximalen G-Konjugationsklassen. Inzwischen wurde die MAGMA Implementierung dieses Algorithmus nochmals um Größenordnungen verbessert. Mit dem neuen MAGMA Release 2.9 (Mai 2002) lassen sich die gesamten Untergruppengitter der Grade $3 \leq n \leq 23$ in weniger als zwei Minuten bestimmen, so daß diese Daten künftig auch zur Laufzeit berechnet werden können und nicht mehr wie in der aktuellen Galoisgruppenimplementierung gespeichert werden müssen. Hat man Repräsentanten für jede Konjugationsklasse einer maximalen Untergruppe gefunden, so wird wie in Sektion 2.1.4 beschrieben fortgefahren. Dabei werden in unserer Implementierung die Permutationen $\varrho_{i,j} \in S_n$ und die Menge der Permutationen $\mathcal{P}(G, T_i, H_{i,j})$ aus Sektion 2.1.4 gespeichert. Somit verbleibt für einen vollständigen Datensatz nur noch die Berechnung der Nebenklassenrepräsentanten, die in unserer Implementierung zur Laufzeit erfolgt und dank des in MAGMA [5, 16] verwendeten Algorithmus auch für große Indizes unproblematisch ist.

Kapitel 7

Beispiele

Wir betrachten nun Beispiele für die Berechnung von Galoisgruppen von algebraischen Zahlkörpern und algebraischen Funktionenkörpern über $\mathbb{Q}$ und endlichen Körpern. Unsere Implementation des Algorithmus zur Galoisgruppenberechnung beschränkt sich im Funktionenkörperfall auf absolute Funktionenkörper über $\mathbb{Q}$ und endliche Körper der Charakteristik ungleich 2. Die Algorithmen sind in den Computeralgebrasystemen KASH [38] und MAGMA [5, 16] implementiert. Alle gemessenen Laufzeiten wurden auf einem 1.5 GHz Intel Pentium Prozessor unter Linux ermittelt und beinhalten alle Berechnungen, um ein bewiesenes Ergebnis zu erhalten. Wir haben insgesamt mehr als 100 000 Polynome der Grade 3 bis 23 getestet. Die Laufzeit des Algorithmus hängt für die betrachteten Körper von der Größe der Koeffizienten und der Galoisgruppe ab. Darüber hinaus hängt sie natürlich auch von der Anzahl der durchzuführenden Tschirnhausentransformationen ab, die in unseren Beispielen meistens mit der Größe der Koeffizienten zunimmt.

7.1 Galoisgruppen über algebraischen Zahlkörpern

7.1.1 Galoisgruppen über $\mathbb{Q}$ bis zum Grad 15

Wir beginnen mit einem Vergleich des in der Diplomarbeit der Autorin [29] entwickelten Verfahrens, welches ebenfalls auf der Methode von Stauduhar beruht. Dort wurden Galoisgruppen für jede Gruppe vom Grad $7-11$ und mehrere Gruppen vom Grad 12 berechnet und mit anderen Verfahren [2, 54, 76] verglichen. Dabei stellte sich heraus, daß die Methoden in [29] überlegen waren. Ein großer Nachteil der damaligen Implementation bestand jedoch in der Verwendung komplexer

Approximationen der Nullstellen des Eingabepolynoms, welches in der Regel zu korrekten, aber nicht bewiesen Ergebnissen führte. Im folgenden vergleichen wir die Beispiele vom Grad 11 und 12 aus [29] (alt) mit den in der Arbeit präsentierten Methoden (neu).

Grad 11

Gruppe	Polynom	Laufzeit	
		alt	neu
$11T_1^+$	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6 - 56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	29.35s	0.96s
$11T_2$	$x^{11} - x^{10} + 5x^9 - 4x^8 + 10x^7 - 6x^6 + 11x^5 - 7x^4 + 9x^3 - 4x^2 + 2x + 1$	3595.65s	0.51s
$11T_3^+$	$x^{11} - 33x^9 + 396x^7 - 2079x^5 + 4455x^3 - 2673x - 243$	29.13s	0.72s
$11T_4$	$x^{11} - 2$	3601.13s	0.41s
$11T_5^+$	$x^{11} + 44x^9 - 1133x^8 + 3597x^7 + 18161x^6 - 105215x^5 + 74514x^4 + 690767x^3 - 1435929x^2 + 138600x + 53994$	38.69s	0.59s
$11T_6^+$	$x^{11} - x^{10} - 121x^9 + 65x^8 + 5345x^7 - 481x^6 - 96739x^5 - 23689x^4 + 413690x^3 - 493810x^2 + 26910x - 856170$	38.11s	15.76s
$11T_7^+$	$x^{11} - 132x - 120$	0.02s	0.04s
$11T_8$	$x^{11} - x - 1$	0.02s	0.04s

Grad 12

Gruppe	Polynom	Laufzeit	
		alt	neu
$12T_1$	$x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$	5.66s	0.32s
$12T_3^+$	$x^{12} - 3x^{10} + 2x^8 + x^6 + 2x^4 - 3x^2 + 1$	2.13s	0.20s
$12T_9^+$	$x^{12} + 2x^{10} + 2x^8 - x^6 + 4x^4 - x^2 + 1$	5.01s	0.34s
$12T_{15}$	$x^{12} - 12x^{10} + 54x^8 - 112x^6 + 105x^4 - 36x^2 + 27$	1.23s	0.17s
$12T_{25}^+$	$x^{12} - 2x^{11} + 2x^{10} + 2x^9 - 4x^8 + 3x^6 - 4x^4 + 2x^3 + 2x^2 - 2x + 1$	5.33s	0.49s
$12T_{39}$	$x^{12} - 5x^3 + 5$	3.33s	0.32s
$12T_{44}$	$x^{12} - 6x^6 - 10x^3 - 6$	5.65s	0.28s
$12T_{52}$	$x^{12} - 6x^{10} - 9x^8 - 36x^6 + 223x^4 - 214x^2 - 23$	11.03s	0.50s
$12T_{58}^+$	$x^{12} + 2x^{10} - 10x^8 - 20x^6 - 5x^4 + 4x^2 + 1$	4.33s	0.34s
$12T_{62}^+$	$x^{12} - 10x^{10} + 32x^8 - 32x^6 - 59x^4 + 198x^2 + 196$	4.31s	0.45s
$12T_{74}^+$	$x^{12} - 3x^{10} - 3x^8 + 4x^6 + 2x^4 - x^2 + 1$	9.31s	0.43s
$12T_{89}^+$	$x^{12} - 18x^8 - 9x^4 + 9$	7.68s	1.23s
$12T_{106}^+$	$x^{12} + 12x^{11} + 60x^{10} + 160x^9 + 240x^8 + 192x^7 + 64x^6 + 3$	1.20s	0.14s

Gruppe	Polynom	Laufzeit	
		alt	neu
$12T_{117}^{+}$	$x^{12}+4x^9+2x^6-4x^3-2$	11.34s	0.56s
$12T_{135}$	$x^{12}-36x^8+24x^6+108x^4-144x^2+48$	5.04s	0.26s
$12T_{156}$	$x^{12}-10x^6-8x^3-1$	3.62s	0.39s
$12T_{161}^{+}$	$x^{12}-x^8+2x^6+x^4+2x^2+1$	9.11s	0.32s
$12T_{166}^{+}$	$x^{12}+18x^{10}+135x^8+348x^6+63x^4-512x^3-270x^2+729$	11.23s	0.76s
$12T_{174}^{+}$	$x^{12}-8x^9-36x^8-48x^7+8x^6+144x^5+273x^4+248x^3+72x^2-96t-32$	7.17s	0.38s
$12T_{178}$	$x^{12}-10x^6-4x^3-1$	10.43s	0.41s
$12T_{180}^{+}$	$x^{12}+4x^{10}+6x^8+6x^6+5x^4+6x^2+1$	8.41s	0.52s
$12T_{191}^{+}$	$x^{12}+x^{10}+2x^8-x^6+2x^4-3x^2+1$	4.11s	0.33s
$12T_{203}^{+}$	$x^{12}-x^{10}-x^4+x^2+1$	3.13s	0.31s
$12T_{213}$	$x^{12}+12x^3+27$	2.43s	0.37s
$12T_{222}$	$x^{12}+x^{10}-x^8-5x^6-5x^4-3x^2-1$	1.83s	0.55s
$12T_{236}^{+}$	$x^{12}+2x^{10}+2x^8-3x^6-3x^4+x^2+1$	2.46s	0.23s
$12T_{249}^{+}$	$x^{12}+12x^{10}-24x^7-184x^6-72x^5+309x^4-32x^3+360x^2+80$	4.00s	0.60s
$12T_{258}$	$x^{12}-4x^3-2$	3.06s	0.36s
$12T_{260}$	$x^{12}-2x^8+x^6+x^4-x^2-1$	2.56s	0.40s
$12T_{270}$	$x^{12}+4x^8-6x^6+6x^4-2x^2+8$	3.67s	0.33s
$12T_{277}^{+}$	$x^{12}+3x^6+3x^2+4$	2.70s	0.51s
$12T_{285}^{+}$	$x^{12}+2x^6+3x^4+4x^2+1$	1.50s	0.44s
$12T_{289}$	$x^{12}-27x^8+36x^7+15x^6-54x^5-45x^4+208x^3-216x^2+96x-16$	1.61s	1.00s
$12T_{291}$	$x^{12}+12x^9-9x^8+64x^3-144x^2+108x-27$	1.83s	0.99s
$12T_{293}$	$x^{12}+x^{10}+x^6-3x^2-1$	1.34s	0.35s
$12T_{295}^{+}$	$x^{12}+75x^8+750x^6-5625x^4-23250x^2-30000x+50625$	94.34s	72.82s
$12T_{299}$	$x^{12}+4x^7+4x^2+2$	2.16s	0.15s

Die Beispiele belegen die großen Fortschritte insbesondere bei den primitiven Gruppen. Hierzu werden wir im Anschluß an die folgenden Tabellen noch genauere Informationen liefern. Bei den imprimitiven Gruppen führen neben der Verwendung der $\mathfrak{p}$-adischen Arithmetik (vgl. Sektion 7.1.2) insbesondere die systematisch konstruierten G-relativen H-invarianten Polynome zu den erhaltenen Laufzeitverbesserungen.

In den folgenden Beispieltabellen wurden für jede Gruppe der Grade $12-15$ Galoisgruppenberechnungen durchgeführt. Als Beispiele haben wir alle Polynome der Datenbank von Klüners, Malle [45] (dies sind momentan 52710 Polynome für diese Grade) verwendet. Wir geben neben der Anzahl der vorhandenen Polynome (Polynome) für eine bestimmte Gruppe jeweils die Durchschnittslaufzeit (Zeit) in

Sekunden an.

Grad 12

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$12T_1$	45	0.37s	$12T_{36}$	360	0.53s	$12T_{71}^+$	10	0.64s
$12T_2^+$	156	0.43s	$12T_{37}^+$	246	0.58s	$12T_{72}$	13	0.51s
$12T_3^+$	732	0.33s	$12T_{38}$	38	0.37s	$12T_{73}$	19	0.49s
$12T_4^+$	140	0.24s	$12T_{39}$	46	0.39s	$12T_{74}^+$	70	0.37s
$12T_5$	32	0.39s	$12T_{40}^+$	132	0.44s	$12T_{75}^+$	84	0.36s
$12T_6^+$	348	0.39s	$12T_{41}$	107	0.38s	$12T_{76}^+$	99	0.41s
$12T_7^+$	312	0.36s	$12T_{42}$	134	0.34s	$12T_{77}^+$	373	0.25s
$12T_8$	451	0.20s	$12T_{43}^+$	18	0.15s	$12T_{78}$	304	0.43s
$12T_9^+$	451	0.35s	$12T_{44}$	36	0.32s	$12T_{79}$	92	0.35s
$12T_{10}^+$	765	0.40s	$12T_{45}$	31	0.26s	$12T_{80}$	81	0.37s
$12T_{11}$	132	0.37s	$12T_{46}^+$	10	0.59s	$12T_{81}$	125	0.29s
$12T_{12}$	74	0.36s	$12T_{47}^+$	12	0.44s	$12T_{82}$	132	0.37s
$12T_{13}$	99	0.38s	$12T_{48}^+$	1271	0.42s	$12T_{83}$	33	0.16s
$12T_{14}$	170	0.37s	$12T_{49}$	177	0.54s	$12T_{84}^+$	41	0.62s
$12T_{15}$	162	0.21s	$12T_{50}$	194	0.39s	$12T_{85}^+$	14	0.77s
$12T_{16}^+$	184	0.29s	$12T_{51}$	84	0.39s	$12T_{86}$	264	0.36s
$12T_{17}$	81	0.35s	$12T_{52}$	83	0.46s	$12T_{87}^+$	104	0.44s
$12T_{18}^+$	118	0.43s	$12T_{53}$	113	0.36s	$12T_{88}$	236	0.41s
$12T_{19}$	55	0.40s	$12T_{54}$	46	0.40s	$12T_{89}^+$	37	0.56s
$12T_{20}^+$	46	0.28s	$12T_{55}^+$	28	0.37s	$12T_{90}^+$	506	0.49s
$12T_{21}^+$	691	0.23s	$12T_{56}^+$	935	0.39s	$12T_{91}^+$	34	0.45s
$12T_{22}$	635	0.44s	$12T_{57}^+$	24	0.43s	$12T_{92}$	183	0.43s
$12T_{23}^+$	1218	0.41s	$12T_{58}^+$	99	0.32s	$12T_{93}$	285	0.44s
$12T_{24}^+$	1155	0.38s	$12T_{59}$	115	0.38s	$12T_{94}$	71	0.39s
$12T_{25}^+$	355	0.42s	$12T_{60}^+$	15	0.45s	$12T_{95}^+$	77	0.33s
$12T_{26}^+$	211	0.56s	$12T_{61}$	80	0.38s	$12T_{96}$	23	0.45s
$12T_{27}$	19	0.55s	$12T_{62}^+$	35	0.37s	$12T_{97}^+$	33	0.45s
$12T_{28}$	335	0.19s	$12T_{63}^+$	17	0.39s	$12T_{98}$	59	0.57s
$12T_{29}$	43	0.36s	$12T_{64}$	17	0.43s	$12T_{99}$	28	0.48s
$12T_{30}$	20	0.39s	$12T_{65}^+$	23	0.44s	$12T_{100}$	289	0.40s
$12T_{31}^+$	14	0.42s	$12T_{66}$	350	0.43s	$12T_{101}^+$	705	0.41s
$12T_{32}^+$	240	0.39s	$12T_{67}^+$	136	0.39s	$12T_{102}$	15	0.46s
$12T_{33}^+$	35	0.43s	$12T_{68}^+$	288	0.37s	$12T_{103}^+$	591	0.39s
$12T_{34}^+$	333	0.49s	$12T_{69}^+$	139	0.32s	$12T_{104}$	76	0.49s
$12T_{35}$	401	0.22s	$12T_{70}^+$	34	0.61s	$12T_{105}$	17	0.38s

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$12T_{106}^{+}$	186	0.21s	$12T_{145}$	18	0.41s	$12T_{184}^{+}$	140	0.37s
$12T_{107}$	6	0.36s	$12T_{146}$	54	0.44s	$12T_{185}$	180	0.53s
$12T_{108}^{+}$	260	0.32s	$12T_{147}$	45	0.59s	$12T_{186}$	133	0.38s
$12T_{109}^{+}$	293	0.29s	$12T_{148}$	165	0.51s	$12T_{187}^{+}$	265	0.39s
$12T_{110}$	293	0.46s	$12T_{149}$	136	0.62s	$12T_{188}$	372	0.40s
$12T_{111}$	256	0.44s	$12T_{150}$	67	0.49s	$12T_{189}$	171	0.41s
$12T_{112}^{+}$	135	0.49s	$12T_{151}$	37	0.73s	$12T_{190}$	99	0.39s
$12T_{113}^{+}$	144	0.39s	$12T_{152}$	72	0.50s	$12T_{191}^{+}$	115	0.44s
$12T_{114}$	200	0.49s	$12T_{153}$	47	0.43s	$12T_{192}$	22	0.47s
$12T_{115}$	143	0.46s	$12T_{154}$	50	0.45s	$12T_{193}$	300	0.26s
$12T_{116}$	30	0.45s	$12T_{155}$	111	0.32s	$12T_{194}^{+}$	27	0.46s
$12T_{117}^{+}$	35	0.75s	$12T_{156}$	81	0.44s	$12T_{195}^{+}$	259	0.52s
$12T_{118}$	20	0.49s	$12T_{157}^{+}$	22	1.04s	$12T_{196}$	33	0.50s
$12T_{119}$	40	0.45s	$12T_{158}^{+}$	102	0.45s	$12T_{197}$	58	0.42s
$12T_{120}$	23	0.51s	$12T_{159}$	16	0.39s	$12T_{198}$	67	0.39s
$12T_{121}$	27	0.43s	$12T_{160}$	39	0.43s	$12T_{199}^{+}$	143	0.44s
$12T_{122}^{+}$	5	0.53s	$12T_{161}^{+}$	98	0.45s	$12T_{200}$	102	0.47s
$12T_{123}^{+}$	181	0.43s	$12T_{162}^{+}$	75	0.38s	$12T_{201}$	73	0.54s
$12T_{124}$	29	0.50s	$12T_{163}^{+}$	131	0.37s	$12T_{202}^{+}$	54	0.61s
$12T_{125}$	348	0.22s	$12T_{164}^{+}$	22	0.50s	$12T_{203}^{+}$	166	0.45s
$12T_{126}^{+}$	115	0.36s	$12T_{165}$	122	0.57s	$12T_{204}$	38	0.54s
$12T_{127}$	24	0.53s	$12T_{166}^{+}$	28	0.64s	$12T_{205}$	9	0.45s
$12T_{128}^{+}$	68	0.52s	$12T_{167}$	37	0.36s	$12T_{206}^{+}$	63	0.51s
$12T_{129}$	75	0.54s	$12T_{168}^{+}$	42	0.70s	$12T_{207}$	50	0.85s
$12T_{130}^{+}$	21	0.61s	$12T_{169}$	15	0.42s	$12T_{208}$	268	0.38s
$12T_{131}$	43	0.46s	$12T_{170}$	37	0.45s	$12T_{209}$	38	0.55s
$12T_{132}^{+}$	36	0.49s	$12T_{171}^{+}$	74	0.48s	$12T_{210}^{+}$	56	0.53s
$12T_{133}^{+}$	20	0.40s	$12T_{172}^{+}$	63	0.48s	$12T_{211}$	41	0.43s
$12T_{134}$	186	0.46s	$12T_{173}^{+}$	66	0.56s	$12T_{212}^{+}$	72	0.69s
$12T_{135}$	192	0.34s	$12T_{174}^{+}$	38	0.43s	$12T_{213}$	91	0.47s
$12T_{136}^{+}$	325	0.44s	$12T_{175}$	48	0.42s	$12T_{214}^{+}$	96	0.51s
$12T_{137}$	308	0.39s	$12T_{176}^{+}$	40	0.44s	$12T_{215}^{+}$	66	0.47s
$12T_{138}^{+}$	124	0.62s	$12T_{177}$	50	0.56s	$12T_{216}^{+}$	160	0.54s
$12T_{139}^{+}$	372	0.48s	$12T_{178}$	26	0.46s	$12T_{217}$	60	0.45s
$12T_{140}$	212	0.46s	$12T_{179}^{+}$	16	16.58s	$12T_{218}$	45	6.85s
$12T_{141}$	142	0.43s	$12T_{180}^{+}$	74	0.38s	$12T_{219}^{+}$	150	0.39s
$12T_{142}$	259	0.48s	$12T_{181}^{+}$	8	2.76s	$12T_{220}^{+}$	60	2.34s
$12T_{143}$	138	0.66s	$12T_{182}^{+}$	14	1.65s	$12T_{221}$	147	0.56s
$12T_{144}^{+}$	151	0.38s	$12T_{183}^{+}$	65	0.59s	$12T_{222}$	810	0.54s

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$12T_{223}$	54	0.54s	$12T_{250}$	609	0.27s	$12T^{+}_{277}$	104	0.49s
$12T_{224}$	386	0.42s	$12T_{251}$	38	0.52s	$12T_{278}$	21	1.01s
$12T_{225}$	69	0.52s	$12T^{+}_{252}$	73	0.47s	$12T^{+}_{279}$	11	1.06s
$12T^{+}_{226}$	303	0.32s	$12T_{253}$	88	0.54s	$12T_{280}$	254	0.51s
$12T_{227}$	520	0.39s	$12T_{254}$	44	0.96s	$12T_{281}$	42	0.45s
$12T^{+}_{228}$	26	0.89s	$12T_{255}$	342	0.47s	$12T^{+}_{282}$	33	0.35s
$12T^{+}_{229}$	31	0.39s	$12T_{256}$	34	0.49s	$12T_{283}$	81	0.49s
$12T^{+}_{230}$	109	0.36s	$12T^{+}_{257}$	115	0.43s	$12T^{+}_{284}$	46	0.59s
$12T_{231}$	56	0.58s	$12T_{258}$	120	0.49s	$12T^{+}_{285}$	677	0.54s
$12T^{+}_{232}$	38	0.90s	$12T^{+}_{259}$	54	1.76s	$12T_{286}$	187	0.47s
$12T_{233}$	36	0.53s	$12T_{260}$	282	0.32s	$12T_{287}$	169	0.64s
$12T^{+}_{234}$	54	0.53s	$12T_{261}$	89	0.28s	$12T_{288}$	35	0.81s
$12T_{235}$	69	0.48s	$12T_{262}$	34	0.59s	$12T_{289}$	54	0.25s
$12T^{+}_{236}$	205	0.36s	$12T_{263}$	107	0.66s	$12T^{+}_{290}$	73	0.30s
$12T_{237}$	76	0.41s	$12T_{264}$	135	0.47s	$12T_{291}$	67	0.49s
$12T_{238}$	15	0.47s	$12T^{+}_{265}$	32	0.48s	$12T_{292}$	13	0.48s
$12T_{239}$	68	0.54s	$12T^{+}_{266}$	66	0.39s	$12T_{293}$	1151	0.41s
$12T_{240}$	363	0.36s	$12T_{267}$	224	0.46s	$12T_{294}$	51	0.29s
$12T_{241}$	89	0.42s	$12T_{268}$	75	0.50s	$12T^{+}_{295}$	28	122.79s
$12T^{+}_{242}$	63	0.45s	$12T^{+}_{269}$	21	0.56s	$12T^{+}_{296}$	11	0.59s
$12T^{+}_{243}$	68	0.51s	$12T_{270}$	315	0.48s	$12T^{+}_{297}$	26	0.35s
$12T^{+}_{244}$	47	0.56s	$12T^{+}_{271}$	87	0.59s	$12T_{298}$	31	0.77s
$12T_{245}$	19	0.88s	$12T^{+}_{272}$	5	70.75s	$12T_{299}$	74	0.29s
$12T_{246}$	17	0.54s	$12T_{273}$	45	0.49s	$12T^{+}_{300}$	38	0.14s
$12T_{247}$	48	0.59s	$12T_{274}$	144	0.34s	$12T_{301}$	87	0.15s
$12T_{248}$	51	0.47s	$12T^{+}_{275}$	12	0.56s			
$12T^{+}_{249}$	51	0.59s	$12T_{276}$	46	0.46s			

Grad 13

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$13T^{+}_{1}$	2	2.31s	$13T_{4}$	2	2.20s	$13T^{+}_{7}$	15	1.63s
$13T^{+}_{2}$	4	2.04s	$13T^{+}_{5}$	12	0.88s	$13T^{+}_{8}$	7	0.10s
$13T^{+}_{3}$	1	0.49s	$13T_{6}$	3	1.75s	$13T_{9}$	202	0.18s

Grad 14

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$14T_{1}$	39	1.17s	$14T_{3}$	59	0.58s	$14T_{5}$	36	0.36s
$14T_{2}$	2	1.60s	$14T_{4}$	11	0.59s	$14T^{+}_{6}$	5	0.90s

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$14T_7$	69	0.54s	$14T_{26}$	2	1.40s	$14T_{45}$	72	0.64s
$14T_8$	4	4.21s	$14T_{27}$	126	1.06s	$14T_{46}$	11	0.77s
$14T_9$	40	0.76s	$14T_{28}^+$	112	0.45s	$14T_{47}$	79	0.44s
$14T_{10}^+$	3	0.79s	$14T_{29}$	53	0.83s	$14T_{48}$	161	0.93s
$14T_{11}^+$	30	0.65s	$14T_{30}^+$	7	1.46s	$14T_{49}$	102	0.31s
$14T_{12}^+$	2	0.55s	$14T_{31}$	4	1.34s	$14T_{50}^+$	390	0.40s
$14T_{13}$	6	0.71s	$14T_{32}$	65	0.64s	$14T_{51}$	883	0.51s
$14T_{14}$	22	1.06s	$14T_{33}^+$	61	1.10s	$14T_{52}$	8	1.19s
$14T_{15}$	2	1.40s	$14T_{34}^+$	112	0.66s	$14T_{53}^+$	221	0.32s
$14T_{16}$	20	0.96s	$14T_{35}^+$	57	0.44s	$14T_{54}$	104	0.81s
$14T_{17}$	39	0.89s	$14T_{36}^+$	3	1.13s	$14T_{55}^+$	156	0.34s
$14T_{18}$	80	0.69s	$14T_{37}$	7	0.93s	$14T_{56}$	165	0.45s
$14T_{19}$	82	0.35s	$14T_{38}$	189	0.56s	$14T_{57}$	445	0.74s
$14T_{20}$	4	0.87s	$14T_{39}$	16	3.44s	$14T_{58}$	37	0.65s
$14T_{21}^+$	23	0.92s	$14T_{40}$	27	1.15s	$14T_{59}^+$	12	0.34s
$14T_{22}^+$	2	0.80s	$14T_{41}^+$	84	0.57s	$14T_{60}$	16	0.65s
$14T_{23}^+$	4	0.46s	$14T_{42}$	214	4.31s	$14T_{61}$	101	0.36s
$14T_{24}$	19	0.55s	$14T_{43}$	266	0.78s	$14T_{62}^+$	5	0.31s
$14T_{25}$	5	1.66s	$14T_{44}$	146	0.41s	$14T_{63}$	28	0.25s

Grad 15

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$15T_1^+$	30	0.35s	$15T_{17}^+$	3	1.96s	$15T_{33}$	12	0.57s
$15T_2$	14	0.61s	$15T_{18}$	5	1.57s	$15T_{34}^+$	40	0.71s
$15T_3^+$	45	0.45s	$15T_{19}$	12	1.55s	$15T_{35}$	8	0.85s
$15T_4$	40	0.39s	$15T_{20}^+$	2	1.55s	$15T_{36}^+$	22	0.45s
$15T_5^+$	3	0.59s	$15T_{21}^+$	3	0.99s	$15T_{37}^+$	2	1.82s
$15T_6^+$	13	0.34s	$15T_{22}^+$	11	0.35s	$15T_{38}$	55	1.64s
$15T_7$	36	0.34s	$15T_{23}$	25	0.32s	$15T_{39}^+$	2	1.33s
$15T_8$	41	0.42s	$15T_{24}$	63	0.40s	$15T_{40}$	6	1.19s
$15T_9^+$	2	1.10s	$15T_{25}^+$	4	1.19s	$15T_{41}$	31	0.95s
$15T_{10}^+$	2	0.67s	$15T_{26}^+$	1	0.77s	$15T_{42}^+$	10	0.70s
$15T_{11}$	36	0.33s	$15T_{27}$	32	1.49s	$15T_{43}$	25	0.70s
$15T_{12}^+$	3	0.77s	$15T_{28}^+$	9	1.01s	$15T_{44}$	43	0.61s
$15T_{13}$	6	1.09s	$15T_{29}$	7	0.25s	$15T_{45}$	21	0.84s
$15T_{14}$	2	1.53s	$15T_{30}^+$	6	0.76s	$15T_{46}^+$	107	0.66s
$15T_{15}^+$	5	0.89s	$15T_{31}$	2	9.48s	$15T_{47}^+$	2	7.15s
$15T_{16}^+$	42	0.30s	$15T_{32}$	19	1.15s	$15T_{48}$	4	4.06s

Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit	Gruppe	Polynome	Zeit
$15T_{49}$	113	1.84s	$15T_{68}$	130	1.15s	$15T_{87}$	118	0.43s
$15T_{50}^{+}$	29	1.21s	$15T_{69}^{+}$	88	0.60s	$15T_{88}^{+}$	46	0.37s
$15T_{51}$	3	2.36s	$15T_{70}$	12	0.81s	$15T_{89}^{+}$	39	0.30s
$15T_{52}$	25	0.73s	$15T_{71}^{+}$	27	0.34s	$15T_{90}$	134	0.55s
$15T_{53}^{+}$	11	0.59s	$15T_{72}^{+}$	4	3.76s	$15T_{91}$	75	0.68s
$15T_{54}^{+}$	7	0.58s	$15T_{73}^{+}$	4	3.86s	$15T_{92}^{+}$	18	0.97s
$15T_{55}$	88	0.75s	$15T_{74}$	26	3.29s	$15T_{93}$	140	0.44s
$15T_{56}$	92	0.72s	$15T_{75}$	136	4.13s	$15T_{94}^{+}$	37	0.74s
$15T_{57}^{+}$	2	7.86s	$15T_{76}$	87	0.90s	$15T_{95}$	57	0.92s
$15T_{58}^{+}$	5	3.66s	$15T_{77}^{+}$	10	0.69s	$15T_{96}$	40	0.65s
$15T_{59}$	72	1.28s	$15T_{78}$	167	0.65s	$15T_{97}$	102	0.73s
$15T_{60}$	41	0.90s	$15T_{79}$	44	0.83s	$15T_{98}^{+}$	42	0.46s
$15T_{61}$	19	0.91s	$15T_{80}^{+}$	5	0.54s	$15T_{99}^{+}$	58	0.43s
$15T_{62}^{+}$	10	0.70s	$15T_{81}$	37	0.35s	$15T_{100}$	112	0.73s
$15T_{63}$	47	0.71s	$15T_{82}$	239	2.71s	$15T_{101}$	85	0.48s
$15T_{64}$	99	0.72s	$15T_{83}$	87	0.61s	$15T_{102}$	103	0.39s
$15T_{65}$	3	27.35s	$15T_{84}^{+}$	34	0.50s	$15T_{103}^{+}$	1	0.29s
$15T_{66}$	5	10.50s	$15T_{85}$	18	0.65s	$15T_{104}$	49	0.26s
$15T_{67}^{+}$	8	3.90s	$15T_{86}$	103	0.54s			

Für alle primitiven Gruppen der Grade 14 und 15 (außer A_{14}, S_{14}, A_{15} und S_{15}) und alle Beispiele mit mehr als 3 Sekunden Durchschnittslaufzeit geben wir nun mehr Details an. In der folgenden Tabelle bezeichnet der Eintrag „Teilkörper“ die Durchschnittslaufzeit des Algorithmus 5.3, welcher die Teilkörperberechnung beinhaltet. Für die primitiven Gruppen geben wir die Durchschnittslaufzeit für die Berechnung der Resolvente und der notwendigen Transformationen an. Die Spalte „Faktoren“ beinhaltet die Durchschnittslaufzeit, um die Faktoren der Resolvente zu finden. In der Spalte „Stauduhar“ geben wir die Durchschnittslaufzeit für die Berechnung aller Inklusionstests an. Die Spalte „Gesamt“ gibt dann schließlich die Durchschnittslaufzeit in Sekunden an. Bei Betrachtung der primitiven Gruppen stellt man fest, daß der Verifikationsschritt mittels der absoluten Resolvente nicht kritisch ist. Am zeitaufwendigsten ist die Gruppe $M_{12} = 12T_{295}^{+}$, da in diesem Fall eine Resolvente vom Grad 924 benötigt wird. Wir bemerken, daß die Koeffizienten der Polynome der Galoisgruppen $15T_{65}$ und $15T_{66}$ sehr groß im Vergleich zu den Koeffizienten der anderen Polynome sind.

Gruppe	Teilkörper	Resolvente	Stauduhar	Faktoren	Gesamt
$12T_{179}^{+}$	0.01s	3.72s	1.59s	11.26s	16.58s
$12T_{218}$	0.01s	1.66s	0.82s	4.36s	6.85s

Gruppe	Teilkörper	Resolvente	Stauduhar	Faktoren	Gesamt
$12T_{272}^{+}$	0.01s	16.86s	0.58s	53.30s	70.75s
$12T_{295}^{+}$	0.01s	42.27s	0.41s	80.10s	122.79s
$14T_{8}$	0.22s		3.99s		4.21s
$14T_{30}^{+}$	0.01s	0.20s	1.17s	0.08s	1.46s
$14T_{39}$	0.01s	0.62s	1.35s	1.46s	3.44s
$14T_{42}$	0.13s		4.18s		4.31s
$15T_{20}^{+}$	0.12s	0.18s	1.22s	0.03s	1.55s
$15T_{28}^{+}$	0.11s	0.36s	0.49s	0.05s	1.01s
$15T_{31}$	0.25s		9.23s		9.48s
$15T_{47}^{+}$	0.02s	2.43s	1.00s	3.70s	7.15s
$15T_{48}$	0.20s		3.86s		4.06s
$15T_{57}^{+}$	0.38s		7.48s		7.86s
$15T_{58}^{+}$	0.20s		3.46s		3.66s
$15T_{65}$	0.89s		26.46s		27.35s
$15T_{66}$	0.37s		10.13s		10.50s
$15T_{67}^{+}$	0.11s		3.79s		3.90s
$15T_{72}^{+}$	0.01s	1.24s	0.42s	2.09s	3.76s
$15T_{73}^{+}$	0.19s		3.67s		3.86s
$15T_{74}$	0.14s		3.15s		3.29s
$15T_{75}$	0.12s		4.01s		4.13s

Tabelle 7.1: Durchschnittslaufzeiten spezieller Galoisgruppen vom Grad $12 \leq n \leq 15$

Die obigen Beispiele belegen die Effizienz unseres Algorithmus. Für die Gruppe $13T_6$, $13T_5^+$, $14T_{39}$ und $14T_{30}^+$ ist der Index $[\,G : H\,] = 39916800$. Ohne die Anwendung von verkürzten Nebenklassen wäre eine vollständige Durchführung des ursprünglichen Stauduhar Algorithmus nicht möglich gewesen.

7.1.2 Komplexe Approximationen

Ein Vorteil der $\mathfrak{p}$-adischen Version des Verfahrens von Stauduhar ist, daß dieser Algorithmus in polynomieller Laufzeit in der Größe der Koeffizienten des Ausgangspolynoms ist (vgl. Sektion 7.1.4). Unter den Beispielpolynomen der Gruppe $15T_{65}$ aus Tabelle 7.1 befindet sich auch das Polynom f aus Klüners, Malle [44]. Dieses Polynom hat sehr große Koeffizienten und der $\mathfrak{p}$-adische Algorithmus benötigt 5.56s zur Berechnung der Galoisgruppe. Zum Vergleich haben wir denselben Algorithmus mit dem Polynom f (mit Teilkörperberechnung) ausgeführt, aber komplexe Approximation der Nullstellen verwendet. Die folgende Tabelle stellt die Laufzeiten und die erhaltenen Ergebnisse bezüglich der verwen-

deten Präzision dar:

Präzision	Ergebnis	Zeit
100	$15T_{82}$	2.19s
200	$15T_{82}$	4.05s
300	$15T_{82}$	7.00s
400	$15T_{65}$	48.65s

Wie auch bei der $\mathfrak{p}$-adischen Variante sind im komplexen Fall Abschätzungen bezüglich der verwendeten Präzision der Nullstellen unerläßlich. In unserem Beispiel ist eine Präzision von knapp 400 Stellen die kleinste Präzision mittels derer ein korrektes Ergebnis erhalten werden kann. Wird eine Präzision verwendet, die ein bewiesenes Ergebnis liefert, so wird sich die Laufzeit noch einmal verschlechtern.

7.1.3 Galoisgruppen über $\mathbb{Q}$ vom Grad $16 \leq n \leq 23$

Wir kommen nun zu den Gruppen der Grade $16 - 23$. Bis heute ist die Frage, ob jede endliche Gruppe als Galoisgruppe einer Galoiserweiterung über $\mathbb{Q}$ auftritt, noch nicht gelöst und weit weniger ist in Richtung expliziter Konstruktionen bekannt. Die letzten veröffentlichten Ergebnisse für Permutationsgruppen bis zum Grad 11 stammen von Eichenlaub [22] bzw. Malle, Matzat [55] und wurden von Klüners, Malle [44, 45] bis zum Grad 15 fortgeführt. Vollständige Beispieltabellen für alle der 4302 Gruppen der Grade $16 - 23$ sind zum jetzigen Zeitpunkt noch nicht vorhanden. Dank der Programme, die zur Erstellung der Polynome aus Klüners, Malle [44] geschrieben worden sind und die uns von Jürgen Klüners zur Verfügung gestellt wurden, konnten wir für ca. ein Fünftel der Gruppen vom Grad $16 - 23$ Polynome konstruieren und mit unserem Programm verifizieren. Wie auch bei den Graden < 15 erfordert die Berechnung einer primitiven Galoisgruppe, welche nicht die symmetrische oder alternierende Gruppe ist, in Abhängigkeit der Koeffizientengröße den größeren Zeitaufwand. In diesem Sinne können wir sie nutzen, um einen gewissen Eindruck über die zu erwartenden Laufzeiten zu erhalten. In den folgenden Beispieltabellen geben wir für fast alle primitiven Gruppen (außer S_n, A_n, $(16 \leq n \leq 23)$) neben einem Polynom wieder nähere Details zur Galoisgruppenberechnung an. Dabei entsprechen die Einträge der folgenden Tabelle wieder den Einträgen aus Tabelle 7.1. Auf Angabe von Beispielpolynomen mit symmetrischer und alternierender Galoisgruppe verzichten wir an dieser Stelle, da sie für beliebigen Grade leicht aus den Polynomen in Matzat [57], Kapitel II, §3, Satz 1 und Satz 2 erhalten werden können. Die Polynome der Gruppen $18T_{377}^{+} = PSL(2,17)$, $18T_{468} = PGL(2,17)$,

$20T^+_{272} = PSL(2,19)$, $20T_{362} = PGL(2,19)$, $21T_{85} = P\Sigma L(3,4)$, $22T^+_{38} = M(22)$ und $22T_{41} = M(22) : 2$ sind durch geeignete Spezialisierung der Polynome aus „Table 10“ in Malle, Matzat [55] entstanden. In den Tabellen 7.2 bzw. 7.3 fehlen noch Beispielpolynome und Zeiten zu den primitiven Gruppen $16T^+_{1329}$, $16T^+_{1508}$, $16T^+_{1753}$, $17T^+_4$, $17T^+_6$, $17T^+_7$, $21T^+_{91}$, $21T_{103}$ und $23T^+_5$.

Gruppe	Teilkörper	Resolvente	Stauduhar	Faktoren	Gesamt
$16T^+_{178}$	0.01s	0.08s	1.75s	0.06s	2.00s
$16T^+_{415}$	0.00s	0.07s	5.15s	0.06s	5.54s
$16T^+_{447}$	0.00s	4.45s	1.65s	5.80s	12.35s
$16T^+_{708}$	0.31s	0.14s	2.66s	0.07s	3.34s
$16T^+_{711}$	0.03s	0.38s	3.36s	0.06s	4.23s
$16T^+_{777}$	0.00s	2.60s	1.85s	3.47s	7.99s
$16T^+_{1030}$	0.12s	0.32s	2.05s	0.11s	2.79s
$16T^+_{1034}$	0.13s	0.14s	4.90s	0.12s	5.63s
$16T^+_{1079}$	0.00s	15.65s	2.03s	40.57s	58.44s
$16T^+_{1080}$	0.01s	21.39s	2.40s	54.71s	78.74s
$16T^+_{1081}$	0.00s	0.08s	4.28s	0.06s	4.67s
$16T^+_{1294}$	0.14s	0.22s	2.70s	0.09s	3.25s
$16T^+_{1328}$	0.00s	0.06s	1.45s	0.11s	1.72s
$16T^+_{1653}$	0.00s	4.75s	2.55s	9.19s	16.66s
$16T^+_{1654}$	0.00s	4.85s	2.59s	9.32s	16.98s
$16T^+_{1840}$	0.01s	1459.76s	2.98s	1363.43s	2826.77s
$16T^+_{1906}$	0.01s	709.78s	1.27s	619.15s	1330.80s
$17T_1$	0.00s	0.05s	15.32s	0.09s	15.53s
$17T_2$	0.00s	0.02s	17.15s	0.24s	17.43s
$17T_3$	0.00s	0.06s	7.97s	0.23s	8.30s
$17T_5$	0.00s	1.70s	7.82s	3.79s	13.35s
$17T_8$	0.00s	243.38s	2.34s	137.65s	383.37s
$18T^+_{377}$	0.01s	0.02s	4.62s	42.81s	47.54s
$18T_{468}$	0.04s	0.02s	12.54s	2109.56s	2122.23s
$19T^+_1$	0.00s	0.07s	12.91s	0.37s	13.35s
$19T_2$	0.00s	0.10s	14.84s	0.25s	15.25s
$19T^+_3$	0.00s	0.27s	31.02s	4.20s	36.52s
$19T_4$	0.00s	0.05s	4.22s	1.45s	5.83s
$19T^+_5$	0.00s	15.78s	2.25s	14.61s	33.51s
$19T_6$	0.00s	5.09s	4.01s	5.48s	14.62s
$20T^+_{272}$	0.01s	12746.06s	48.62s	4088.47s	16883.30s
$20T_{362}$	0.24s	16713.51s	97.72s	3493.96s	19637.22s

Gruppe	Teilkörper	Resolvente	Stauduhar	Faktoren	Gesamt
$21T_{20}$	0.02s	0.03s	3.30s	0.96s	4.36s
$21T_{33}^{+}$	0.01s	0.02s	7.34s	0.24s	7.70s
$21T_{38}$	0.01s	0.01s	3.84s	0.92s	5.19s
$21T_{67}^{+}$	0.03s	50.48s	24.94s	60.92s	136.75s
$21T_{85}$	0.02s	48.43s	16.91s	67.08s	132.33s
$22T_{38}^{+}$	0.01s	26698.90s	371.95s	7549.79s	34620.76s
$22T_{41}$	0.01s	27079.11s	362.78s	7930.13s	35372.12s
$23T_{1}^{+}$	0.00s	0.07s	73.94s	0.20s	74.26s
$23T_{2}$	0.00s	0.18s	67.02s	0.54s	68.40s
$23T_{3}^{+}$	0.00s	53.14s	71.48s	39.29s	165.89s
$23T_{4}$	0.00s	41.51s	17.92s	22.29s	81.32s

Tabelle 7.2: Laufzeiten primitiver Galoisgruppen vom Grad $16 \leq n \leq 23$

Am zeitaufwendigsten sind die primitiven Gruppen $16T_{1840}^{+}$,$16T_{1906}^{+}$,$18T_{468}$, $20T_{272}^{+}$, $20T_{362}$, $22T_{38}^{+}$ und $22T_{41}$, da in diesen Fällen für den Verifikationsschritt Resolventen vom Grad $1820, 1820, 3060, 4845, 4845, 7315$ und 7315 berechnet werden. Alle Gruppen bis auf die Ausnahme $16T_{1840}^{+} < 16T_{1906}^{+}$ sind maximale Untergruppe der symmetrischen bzw. alternierenden Gruppen des jeweiligen Grades, und die auftretenden Indizes liegen in der Größenordnung zwischen 32 432 400 und 1 267 136 462 592 000. Ohne die Verwendung heuristischer Präzisionen mit anschließendem Verifikationsschritt und geeigneter verkürzter Nebenklassenrepräsentantensysteme wäre die Berechnung von Galoisgruppen für diese Grade nicht realisierbar gewesen.

Gruppe	Polynom
$16T_{178}^{+}$	$x^{16} - 2x^{15} + 2x^{14} - 24x^{13} + 2x^{12} + 44x^{11} + 156x^{10} + 316x^{9} + 10x^{8} - 444x^{7} - 280x^{6} + 196x^{5} + 368x^{4} + 244x^{3} + 92x^{2} + 20x + 2$
$16T_{415}^{+}$	$x^{16} + 2x^{15} - 6x^{14} - 12x^{13} - 2x^{12} + 40x^{10} + 40x^{9} - 42x^{8} - 16x^{7} - 44x^{6} + 36x^{5} - 8x^{4} - 40x^{3} + 68x^{2} + 8x - 26$
$16T_{447}^{+}$	$x^{16} + 2x^{15} - 428x^{14} - 1320x^{13} + 62092x^{12} + 220480x^{11} - 3633464x^{10} - 12204344x^{9} + 81935950x^{8} + 175605868x^{7} - 729549480x^{6} - 168712188x^{5} + 1147884592x^{4} + 3407876x^{3} - 91633952x^{2} - 2724436x + 1022790$
$16T_{708}^{+}$	$x^{16} + 14x^{14} + 70x^{12} + 8x^{11} + 148x^{10} + 28x^{9} - 65x^{8} + 152x^{7} - 394x^{6} + 140x^{5} - 286x^{4} + 64x^{3} - 120x^{2} + 48x + 24$
$16T_{711}^{+}$	$x^{16} + 2x^{15} - 12x^{14} - 26x^{13} + 62x^{12} + 150x^{11} - 168x^{10} - 498x^{9} + 182x^{8} + 958x^{7} + 168x^{6} - 950x^{5} - 674x^{4} + 150x^{3} + 424x^{2} + 258x + 63$
$16T_{777}^{+}$	$x^{16} - 4x^{15} + 84x^{14} - 312x^{13} + 1772x^{12} - 8068x^{11} + 13120x^{10} - 9672x^{9} + 33312x^{8} - 70872x^{7} + 33240x^{6} - 76720x^{5} + 126632x^{4} + 191736x^{3} + 4528x^{2} + 298880x + 249844$
$16T_{1030}^{+}$	$x^{16} - 32x^{13} - 36x^{12} - 32x^{10} - 1152x^{9} - 738x^{8} + 1024x^{7} + 1728x^{6} - 288x^{5} - 11732x^{4} + 18432x^{3} + 57312x^{2} + 17728x - 16407$
$16T_{1034}^{+}$	$x^{16} + 48x^{13} - 36x^{12} + 768x^{10} - 720x^{9} + 486x^{8} + 4096x^{7} - 2304x^{6} + 1296x^{5} + 10140x^{4} + 11664x + 6561$

Gruppe	Polynom
$16T^{+}_{1079}$	$x^{16}+18840x^{14}-1010720x^{13}+312110700x^{12}-27117617472x^{11}+$ $2219634811080x^{10}-161576368979040x^{9}+2793940132293270x^{8}-$ $18024624182058880x^{7}-9618274408724881560x^{6}+$ $7566888899638397064 00x^{5}+4646824208859805372300x^{4}+$ $6720780436935533899440 00x^{3}+1074473172808969432187358 00x^{2}-$ $1311833950255129117457623200x+47782253424673367928813926 25$
$16T^{+}_{1080}$	$x^{16}-278504x^{14}+4495904x^{13}+35894567564x^{12}-560260338112x^{11}-$ $2683616784278648x^{10}+24775247844842592x^{9}+125835481316837727606x^{8}+$ $10249838184005802124 8x^{7}-3676473556941820824655256x^{6}-$ $3158371119049519692956547 2x^{5}+6454356883663995264090265943 6x^{4}+$ $7204979284437251474729102869 12x^{3}-6245911133598857228278383044386 64x^{2}$ $-5055061367156053973957915496410976x+$ $2577379107449322293816895144560000785$
$16T^{+}_{1081}$	$x^{16}+4x^{15}+16x^{14}+48x^{13}+84x^{12}+120x^{11}-32x^{10}-728x^{9}-2072x^{8}-4464x^{7}-$ $7224x^{6}-8160x^{5}-6768x^{4}-3696x^{3}-384x^{2}+288x+36$
$16T^{+}_{1294}$	$x^{16}-32x^{13}-16x^{12}+224x^{10}+768x^{9}-1536x^{8}+3072x^{7}-10496x^{6}+1024x^{5}+$ $21248x^{4}-16384x^{3}+1024x^{2}+1024$
$16T^{+}_{1328}$	$x^{16}+8x^{14}+64x^{13}-580x^{12}+9856x^{11}-44552x^{10}+37568x^{9}-56794x^{8}+564992x^{7}-$ $1636680x^{6}+3480000x^{5}-1768068x^{4}-6872448x^{3}+12834760x^{2}-7947456x+$ 1645345
$16T^{+}_{1653}$	$x^{16}+4x^{15}-8x^{14}+3884x^{13}+94608x^{12}+1075116x^{11}+7437864x^{10}+33734804x^{9}+$ $102015730x^{8}+210616252x^{7}+370344280x^{6}+921794612x^{5}+2659199064x^{4}+$ $5295173364x^{3}+6417291816x^{2}+4089179564x+1183124709$
$16T^{+}_{1654}$	$x^{16}+20x^{14}+476x^{13}-4680x^{12}+40460x^{11}+217332x^{10}-3937108x^{9}+8907656x^{8}+$ $49358904x^{7}-262355464x^{6}+187920768x^{5}+3363851176x^{4}-6827119432x^{3}-$ $25449731720x^{2}+31852690296x+87558819124$
$16T^{+}_{1840}$	$x^{16}-4x^{15}+16596x^{14}-19712x^{13}+92248392x^{12}+7980853800x^{11}+$ $156114759192x^{10}+4901995788144x^{9}-5594815507338488x^{8}-$ $4652187946155204 64x^{7}+4704063661831912528x^{6}+$ $1530953000298707686400x^{5}+4314978199110541730 4992x^{4}-$ $4879738552914281335631 04x^{3}-3799743337321897868403766 4x^{2}-$ $4400535187427610741243333 76x+2357294354003301810244956 32$
$16T^{+}_{1906}$	$x^{16}-8x^{15}+760x^{14}-4008x^{13}+155272x^{12}-2340624x^{11}-8613624x^{10}-$ $651189744x^{9}+5863459792x^{8}+169071887136x^{7}-1143545120576x^{6}-$ $17921045986944x^{5}+321311519145968x^{4}-425938176021312x^{3}-$ $13067657144938816x^{2}+20122298096102 40x+176258317442080000$
$17T_{1}$	$x^{17}-x^{16}-48x^{15}+105x^{14}+763x^{13}-2579x^{12}-3653x^{11}+23311x^{10}-11031x^{9}-$ $74838x^{8}+107759x^{7}+50288x^{6}-198615x^{5}+102976x^{4}+58507x^{3}-75722x^{2}+$ $25763x-2837$
$17T_{2}$	$x^{17}-5253x^{15}+124321x^{14}+5648726x^{13}-269027142x^{12}+2991583500x^{11}+$ $26806727882x^{10}-834242860956x^{9}+4681414706866x^{8}+31121584356393x^{7}-$ $480423093241596x^{6}+1933229407742391x^{5}-1317311078775634x^{4}-$ $7838914559012256x^{3}+10790602892187624x^{2}+5862324729078675x-$ 9856487818137825

Gruppe	Polynom
$17T_3$	$x^{17} + 4x^{16} - 476x^{15} - 3026x^{14} + 82996x^{13} + 736812x^{12} - 6121180x^{11} - 80531352x^{10} + 108448584x^9 + 4267795762x^8 + 9723361580x^7 - 95353221324x^6 - 524744382701x^5 + 7660737412x^4 + 6800548404356x^3 + 21491689501032x^2 + 27480501953536x + 12878683864992$
$17T_5$	$x^{17} - 2$
$17T_8$	$x^{17} - 5x^{16} + 40x^{15} - 140x^{14} + 610x^{13} - 1622x^{12} + 4870x^{11} - 10220x^{10} + 22720x^9 - 38080x^8 + 63500x^7 - 84100x^6 + 102200x^5 - 102400x^4 + 83000x^3 - 55864x^2 + 24080x - 9400$
$18T_{377}^+$	$x^{18} + 3x^{17} - 204x^{16} - 544x^{15} + 16932x^{14} + 43248x^{13} - 724064x^{12} - 1906176x^{11} + 17083776x^{10} + 51262208x^9 - 254053440x^8 - 859163136x^7 + 3555026944x^6 + 9831324672x^5 - 51900237312x^4 - 76531486720x^3 + 325226526720x^2 + 305883789312x - 874955762688$
$18T_{468}$	$x^{18} - 43x^{17} + 765x^{16} - 7905x^{15} + 51476x^{14} - 220507x^{13} + 640577x^{12} - 1308439x^{11} + 1971184x^{10} - 2269823x^9 + 2048483x^8 - 1470551x^7 + 843625x^6 - 383656x^5 + 135422x^4 - 36346x^3 + 7412x^2 - 1080x + 81$
$19T_1^+$	$x^{19} + 2x^{18} - 360x^{17} - 456x^{16} + 48704x^{15} + 35968x^{14} - 3275776x^{13} - 617216x^{12} + 121344768x^{11} - 46136320x^{10} - 2524246016x^9 + 2361833472x^8 + 28074385408x^7 - 41149440000x^6 - 142722891776x^5 + 293282676736x^4 + 170402512896x^3 - 671847809024x^2 + 407226810368x - 61681958912$
$19T_2$	$x^{19} - 38x^{17} + 703x^{15} + 228x^{14} - 7239x^{13} - 6384x^{12} + 39159x^{11} + 64068x^{10} - 78147x^9 - 263112x^8 - 144818x^7 + 236892x^6 + 532855x^5 + 695400x^4 + 696844x^3 + 445968x^2 + 229824x + 110592$
$19T_3^+$	siehe unten
$19T_4$	siehe unten
$19T_5^+$	$x^{19} - 95x^{17} + 3800x^{15} - 83125x^{13} + 1080625x^{11} - 8490625x^9 + 39187500x^7 - 97968750x^5 + 111328125x^3 - 37109375x - 8734375$
$19T_6$	$x^{19} - 2$
$20T_{272}^+$	$x^{20} + 8x^{19} + 380x^{18} - 18050x^{16} - 3800x^{15} + 484500x^{14} + 19000x^{13} - 6709375x^{12} + 380000x^{11} + 57475000x^{10} - 4275000x^9 - 330125000x^8 + 14250000x^7 + 1330000000x^6 + 47500000x^5 - 3443750000x^4 - 475000000x^3 + 4750000000x^2 + 1500000000x + 125000000$
$20T_{362}$	$x^{20} + 103x^{19} + 4332x^{18} + 92302x^{17} + 1079276x^{16} + 7322695x^{15} + 33549364x^{14} + 112366931x^{13} + 288461667x^{12} + 583212030x^{11} + 943165130x^{10} + 1228576727x^9 + 1289766664x^8 + 1085616908x^7 + 724933790x^6 + 377817280x^5 + 150061392x^4 + 43811264x^3 + 8860384x^2 + 1109760x + 65025$
$21T_{20}$	$x^{21} - 1260x^{19} + 336x^{18} + 612710x^{17} - 249760x^{16} - 144140255x^{15} + 76921009x^{14} + 17018423534x^{13} - 17961229132x^{12} - 967153165139x^{11} + 3335024018998x^{10} + 21099297327472x^9 - 293200794043654x^8 + 108073560459819x^7 + 6904732733968811x^6 - 26132997546433526x^5 - 9149724649985605x^4 + 47137704927150283 6x^3 - 67255696964157599 1x^2 - 491828483010376883x + 9484047376918067631$
$21T_{33}^+$	$x^{21} + 21x^{18} - 252x^{15} - 171x^{14} - 98x^{12} + 1722x^{11} + 5047x^9 - 3024x^8 - 2601x^7 - 3087x^6 - 18081x^5 + 6489x^4 - 45276x^3 + 38514x^2 - 2898x + 67255$
$21T_{38}$	$x^{21} - 25x^{15} - 57x^{14} - 53x^9 - 30x^8 - 289x^7 - 27x^3 + 27x^2 - 9x + 1$

Gruppe	Polynom
$21T_{67}^{+}$	$x^{21}+8x^{20}+65x^{19}+555x^{18}+3682x^{17}+22572x^{16}+126444x^{15}+594616x^{14}+2309393x^{13}+7356020x^{12}+18806423x^{11}+37461659x^{10}+54612777x^{9}+45885418x^{8}-17628635x^{7}-129364885x^{6}-221678886x^{5}-223266960x^{4}-144690656x^{3}-59424208x^{2}-13938272x-1375360$
$21T_{85}$	$x^{21}+6x^{20}-32x^{19}-220x^{18}-71x^{17}+902x^{16}+5320x^{15}+32524x^{14}+54335x^{13}-52730x^{12}-451160x^{11}-2325392x^{10}-6659517x^{9}-11243466x^{8}-15644640x^{7}-4239088x^{6}+54407188x^{5}+141705136x^{4}+265754960x^{3}+413258960x^{2}+333108324x+162458072$
$22T_{38}^{+}$	$x^{22}+11x^{21}+55x^{20}+198x^{19}+297x^{18}-1320x^{17}-7920x^{16}-25080x^{15}-51546x^{14}+62854x^{13}+723074x^{12}+2293168x^{11}+5508426x^{10}+9506640x^{9}+5161068x^{8}-12278376x^{7}-21394791x^{6}-8240265x^{5}+4581423x^{4}+4441338x^{3}+1659933x^{2}+323136x+25164$
$22T_{41}$	$x^{22}+11x^{21}+77x^{20}+418x^{19}+1639x^{18}+4939x^{17}+10549x^{16}+6050x^{15}-57178x^{14}-317768x^{13}-1067770x^{12}-2443414x^{11}-3781129x^{10}-2295337x^{9}+11831105x^{8}+50994834x^{7}+129210323x^{6}+254905167x^{5}+388599915x^{4}+468051848x^{3}+448498072x^{2}+323729604x+160810076$
$23T_{1}^{+}$	$x^{23}+x^{22}-22x^{21}-21x^{20}+210x^{19}+190x^{18}-1140x^{17}-969x^{16}+3876x^{15}+3060x^{14}-8568x^{13}-6188x^{12}+12376x^{11}+8008x^{10}-11440x^{9}-6435x^{8}+6435x^{7}+3003x^{6}-2002x^{5}-715x^{4}+286x^{3}+66x^{2}-12x-1$
$23T_{2}$	$x^{23}-23x^{21}-69x^{20}-69x^{19}-2162x^{18}-7636x^{17}-11891x^{16}-46552x^{15}-28612x^{14}+118519x^{13}-1702989x^{12}-7119949x^{11}-75095x^{10}+35218037x^{9}-14349654x^{8}-404963944x^{7}-1069251462x^{6}-1257791271x^{5}-453896191x^{4}+485249653x^{3}+443818028x^{2}-130082411x-240490609$
$23T_{3}^{+}$	$x^{23}-46x^{21}+920x^{19}-10488x^{17}+75072x^{15}-350336x^{13}+1071616x^{11}-2104960x^{9}+2525952x^{7}-1683968x^{5}+518144x^{3}-47104x-5760$
$23T_{4}$	$x^{23}-2$

Tabelle 7.3: Polynome vom Grad $16 \leq n \leq 23$ mit primitiver Galoisgruppe

Für die Gruppen $19T_{3}^{+}$ und $19T_{4}$ haben wir in Tabelle 7.3 die folgenden Polynome verwendet:

$$x^{19}-195282x^{18}-413937194090x^{17}-29556485377441393x^{16}+27378474671058793486043x^{15}+2064004808001283840636289243x^{14}-74031381104310849679954461839326 4x^{13}-350819734127598142677617308309622103 12x^{12}+90590105518423686218575794115384166301201 90x^{11}+85365555708590555178972401810142012589594215842x^{10}-40837735671186150116152570811594231754610182689222726x^{9}+11820651862729925427068695147167359398496200817800696894 68x^{8}+11109420619309289194569641067729006086545050106986443224924286x^{7}-84623772556662134437669569621472049216762305074983807985069536020 4x^{6}+87765074999889796186147309445432329015646075940173766817081543622876 91x^{5}+21995900024221800056841127928642494006867913389198279289531675513805239820x^{4}-37139195503602777967457547284584487825264748210833827039073532806721297516776 4x^{3}-13545209883701982656104028572775193378160097565167028475302803028930169105084995 33x^{2}-11932401480323459045690113937975825411579964904848531391082940330356697702334635858 15x-55160674206854352470260739668378304980486402782859928517046247533229410950141230053101$$

$$x^{19}+2071x^{18}+1995703x^{17}+31371964x^{16}+178421356718x^{15}+150337270992734x^{14}-130607704604525331x^{13}-947315565068689 3 58x^{12}+22060334755525384121837x^{11}-52002079214610837431137 05x^{10}-506055822157996585579643 37x^{9}+11362398095630193582601341 2504x^{8}+69240538657110940522042110403 72x^{7}-95805043403483015840693420193 5749x^{6}-22732574655121594262783224205308937 8x^{5}-21046433469175261783073300527107404203x^{4}-11052704532816542093258397213288110685 55x^{3}-36475261981399309192423693020574032576898x^{2}-66283312522888106022140444366599707232 7213x-49021262521819787112423849607352577260405 11$$

7.1.4 Koeffizientengröße

Im folgenden vergleichen wir den Zusammenhang zwischen der Größe der Koeffizienten des Eingabepolynoms, der benötigten Präzision und der zugehörigen Laufzeit. Dazu betrachten wir die Polynome

$$\begin{aligned} f_1(x) &= x^{16} - 64x^{15} + 1584x^{14} - 97280x^{13} + 1529800x^{12} - 17476992x^{11} + \\ &\quad 165412880x^{10} - 1379458976x^9 + 8077549480x^8 - 50320055264x^7 + \\ &\quad 169393873584x^6 - 820626424032x^5 + 277207213424x^4 - \\ &\quad 2334240536480x^3 - 6287712726880x^2 + 3461448217920x + \\ &\quad 7730427713806 \in \mathbb{Q}[x] \end{aligned}$$

und

$$\begin{aligned} f_2(x) &= x^{16} - 272x^{15} + 40536x^{14} - 2437104x^{13} + 66417884x^{12} - 764172432x^{11} + \\ &\quad 4025091176x^{10} - 34363617264x^9 + 730844666694x^8 - 6940738781872x^7 + \\ &\quad 40375367651176x^6 - 262826782246224x^5 + 1562689790645212x^4 - \\ &\quad 6239079270902704x^3 + 76886070471562584x^2 - 421956103099634384x + \\ &\quad 1379654645298816129 \in \mathbb{Q}[x] \end{aligned}$$

mit imprimitiver ($16T_{144}$) bzw. primitiver ($16T^{+}_{178}$) Galoisgruppe. Wir verändern die Eingabepolynome f_1, f_2 durch Transformationen der Form $f_i(x) \mapsto a_n^{n-1} f_i(r \cdot x/a_n)$, $(r \in \mathbb{Z}_{>0})$, wobei $f_i(r \cdot x) = \sum_{i=0}^{n} a_i (r \cdot x)^i$, $(i = 1, 2)$ sei. Beide Polynome sind so gewählt, daß während der Galoisgruppenberechnung keine Tschirnhausentransformationen auftreten. In der nachfolgenden Tabelle entspricht der Wert p der Primzahl bezüglich der die p-adischen Berechnungen durchgeführt werden und k ist die maximale Präzision, d.h. der maximale Exponent von p^k während einer Galoisgruppenberechnung. Alle anderen Einträge entsprechen den Einträgen in Tabelle 7.1.

Polynom	r	p	k	Laufzeit				
				Teilk.	Res.	Stau.	Fak.	Gesamt
f_1	1	23	173	0.28s		0.94s		2.18s
f_1	5	23	1030	3.83s		6.26s		13.59s
f_1	10	23	1400	5.45s		10.09s		21.80s
f_1	100	23	2627	21.17s		37.91s		86.32s
f_1	1000	23	3854	60.03s		86.91s		223.36s
f_1	10000	23	5081	98.01s		148.53s		404.51s
f_1	100000	23	6308	192.52s		241.80s		695.61s
f_2	1	17	91	0.02s	0.14s	2.79s	0.24s	3.31s
f_2	5	17	432	0.78s	1.56s	13.24s	5.66s	22.61s
f_2	10	17	579	1.66s	2.44s	22.97s	7.39s	34.72s
f_2	100	17	1067	8.86s	10.87s	76.02s	21.28s	117.38s

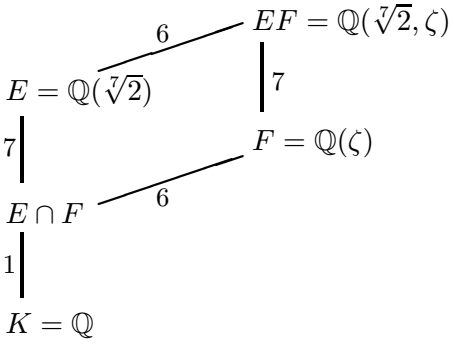
Polynom	r	p	k	Laufzeit				
				Teilk.	Res.	Stau.	Fak.	Gesamt
f_2	1000	17	1554	25.93s	30.07s	147.40s	43.50s	248.17s
f_2	10000	17	2042	54.46s	60.37s	249.44s	57.41s	432.21s
f_2	100000	17	2529	90.99s	98.89s	412.71s	76.07s	680.23s

Für festen Grad und konstante Galoisgruppe lassen die Daten einen ungefähr quadratischen Zusammenhang zwischen der Präzision und der Laufzeit erkennen. Wegen des linearen Zusammenhangs zwischen der Präzision und dem Logarithmus des größten Nullstellenbetrags und weil der größte Nullstellenbetrag linear durch den größten Koeffizientenbetrag beschränkt wird, ist die Laufzeit ungefähr quadratisch durch den Logarithmus des größten Koeffizientenbetrags des Eingabepolynoms beschränkt. Die Effizienz des Verfahrens bei großen Koeffizienten wird somit im wesentlichen von der zugrundeliegenden Integerarithmetik bestimmt.

7.1.5 Erweiterung des Grundkörpers $K = \mathbb{Q}$

Wir wenden uns nun einfachen algebraischen Zahlkörpern als Grundkörpern zu. Laufzeitvergleiche sind in diesem Fall nicht möglich, da uns nur für spezielle (relativ-abelsche) Körper Verfahren (vgl. Klüners [42]) bekannt sind. Eine erste natürliche Fragestellung ist die Frage nach dem Verhalten der Galoisgruppe eines Polynoms bei Erweiterung des Grundkörpers K. Allgemein gilt für separable Polynome $f \in K[x]$, daß $\mathcal{G}(f, F)$ für einen Erweiterungskörper F von K als Untergruppe von $\mathcal{G}(f, K)$ aufgefaßt werden kann. Wir geben ein Beispiel:

Sei $f(x) = x^7 - 2 \in \mathbb{Q}[x]$ und $F = \mathbb{Q}(\zeta)$, wobei ζ siebte primitive Einheitswurzel sei. Wir betrachten das folgenden Diagramm:



Es gilt $C(7) = \mathcal{G}(f, F) \leq \mathcal{G}(f, \mathbb{Q}) = F_{42}(7)$. Wäre die Erweiterung $E/\mathbb{Q}$ galoissch, so erhielte man nach dem Verschiebungssatz der Galoisschen Theorie (vgl. Lang [48], Chapter VI, Theorem 1.12), daß $G(EF/F) \cong G(E/E \cap F)$ ist. Da in

unserem Beispiel $\sqrt[7]{2}$ reell und ζ komplex ist, gilt $E \cap F = \mathbb{Q}$, und es würde $\mathcal{G}(f, F) \cong G(EF/F) \cong G(E/\mathbb{Q}) \cong \mathcal{G}(f, \mathbb{Q})$ folgen.

Wir betrachten nun unsere Implementation unter den folgenden Gesichtspunkten:

(i) Laufzeitverhalten bei wachsendem Grad m des Grundkörpers mit Maximal- und Gleichungsordnung als Koeffizientenordnung,

(ii) Vergleich des Rekonstruktionsalgorithmus aus [25] bei wachsendem Grad m des Grundkörpers bzw. wachsender Koeffizientengröße mit unserem Rekonstruktionsalgorithmus.

Sei $E = \mathbb{Q}(\rho_m)$ mit Minimalpolynom $g(x) = x^m - 3 \in \mathbb{Z}[x]$, $(m \in \mathbb{Z}_{\geq 2})$. Um als Grundkörper einen Zahlkörper F_m zu erhalten, dessen Gleichungsordnung und Maximalordnung $\mathfrak{o}_F$ verschieden sind, betrachten wir für bestimmte $m \in \mathbb{Z}_{\geq 2}$ den Zahlkörper F_m, der von dem Minimalpolynom des Elements $2\rho_m + 1$ erzeugt wird. Als Relativpolynom über F_m beschränken wir uns auf die einfachste Variante, nämlich auf ein Polynom mit Koeffizienten in $\mathbb{Z}$. Hierzu wählen wir das Kreisteilungspolynom $\phi_{11} = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 \in \mathbb{Z}[x]$, dessen Galoisgruppe über den betrachteten Körpern die zyklische Gruppe $C(10)$ ist. In der folgenden Tabelle bezeichnet m den Grad des Grundkörpers, $p \in \mathfrak{p}$ die Primzahl des für die Berechnung gewählten Primideals $\mathfrak{p}$ und k die maximale Präzision, d.h. den größten auftretenden Exponenten von p^k bei der Galoisgruppenberechnung. Die Einträge Teilkörper, Stauduhar und Gesamt entsprechen den Einträgen in Tabelle 7.1. Hinzu kommen die Zeiten, die während einer Galoisgruppenberechnung für LLL-Berechnung, Gittererzeugung und Rekonstruktion verwendet werden. Zur LLL-Berechnung werden auch die LLL-Zeiten gemessen, die innerhalb der Teilkörperberechnung und bei der Galoisgruppenberechnung der Teilkörper stattfinden. Die Gittererzeugung umfaßt neben der Aufstellung des Teilgitters $\Lambda'_{\gamma^*_{(k,1)},(k)} \subset \mathbb{R}^{m+1}$ von $\Lambda_{\gamma^*_{\sigma,(k,1)},(k)}$ auch eine initiale LLL-Rekonstruktion (vgl. Bemerkung 3.40 (*iii*)). Beim Rekonstruktionsschritt wird die Zeit für Algorithmus 3.38 gemessen, wobei die Berechnung für das Teilgitter $\Lambda'_{\gamma^*_{(k,1)},(k)}$ aber entfällt. Für festes $m \in \mathbb{Z}_{\geq 2}$ führen wir die Berechnungen jeweils mit Maximalordnung $\mathfrak{o}_{F_m}$ und Gleichungsordnung als Koeffizientenordnung durch.

m	p	k	Koeffizienten-ordnung	Laufzeit					
				Teilk.	Stau.	Reko.	Gitter	LLL	Gesamt
5	23	58	$\mathfrak{o}_{F_m}$	0.38s	0.20s	0.01s	0.02s	0.03s	0.71s
5	23	74	$\mathbb{Z}[2\rho_m + 1]$	0.40s	0.21s	0.01s	0.02s	0.04s	0.76s
10	23	146	$\mathfrak{o}_{F_m}$	1.31s	0.55s	0.03s	0.15s	0.40s	2.15s
10	23	191	$\mathbb{Z}[2\rho_m + 1]$	1.59s	0.72s	0.05s	0.21s	0.64s	2.59s
15	23	269	$\mathfrak{o}_{F_m}$	4.66s	1.86s	0.20s	1.02s	2.72s	6.98s

m	p	k	Koeffizienten-ordnung	Laufzeit					
				Teilk.	Stau.	Reko.	Gitter	LLL	Gesamt
15	23	349	$\mathbb{Z}[2\rho_m+1]$	6.38s	2.91s	0.24s	1.47s	4.58s	9.90s
20	23	422	$\mathfrak{o}_{F_m}$	16.81s	6.50s	0.56s	4.74s	12.74s	24.25s
20	23	546	$\mathbb{Z}[2\rho_m+1]$	26.30s	12.00s	0.99s	7.84s	23.73s	40.32s
25	23	605	$\mathfrak{o}_{F_m}$	51.02s	21.18s	1.61s	17.67s	48.32s	73.83s
25	23	784	$\mathbb{Z}[2\rho_m+1]$	90.30s	39.93s	3.19s	29.07s	90.04s	132.08s

Die folgende Tabelle umfaßt die gleichen Beispiele wie in der letzten Tabelle, aber unter Verwendung des Rekonstruktionsalgorithmus aus [25].

m	p	k	Koeffizienten-ordnung	Laufzeit		
				Teilk.	Stau.	Gesamt
5	23	41	$\mathfrak{o}_{F_m}$	0.40s	0.18s	0.77s
5	23	77	$\mathbb{Z}[2\rho_m+1]$	0.41s	0.21s	0.82s
10	23	135	$\mathfrak{o}_{F_m}$	1.34s	0.58s	2.21s
10	23	221	$\mathbb{Z}[2\rho_m+1]$	1.66s	0.88s	2.83s
15	23	308	$\mathfrak{o}_{F_m}$	4.73s	2.65s	7.84s
15	23	452	$\mathbb{Z}[2\rho_m+1]$	6.45s	4.70s	11.86s
20	23	580	$\mathfrak{o}_{F_m}$	16.98s	14.40s	32.30s
20	23	792	$\mathbb{Z}[2\rho_m+1]$	26.25s	26.03s	53.57s
25	23	963	$\mathfrak{o}_{F_m}$	51.51s	74.14s	127.30s
25	23	1259	$\mathbb{Z}[2\rho_m+1]$	89.61s	127.56s	219.06s

Im folgenden vergleichen wir die beiden Verfahren bei wachsender Koeffizientengröße. Dabei verändern wir das Polynom ϕ_{11} durch Transformationen der Form wie in Sektion 7.1.4 mittels des Parameters $r \in \mathbb{Z}_{>0}$. Für die ersten drei Zeilen der nachfolgenden Tabelle wurde unser Rekonstruktionsalgorithmus verwendet, während für die darauffolgenden drei Zeilen der Algorithmus aus [25] eingesetzt wurde.

m	r	k	Koeffizienten-ordnung	Laufzeit		
				Teilk.	Stau.	Gesamt
5	5	520	$\mathfrak{o}_{F_m}$	3.32s	1.36s	4.89s
5	10	719	$\mathfrak{o}_{F_m}$	7.16s	1.48s	9.01s
5	50	1181	$\mathfrak{o}_{F_m}$	17.46s	2.95s	20.87s
5	5	306	$\mathfrak{o}_{F_m}$	3.31s	1.18s	4.72s
5	10	425	$\mathfrak{o}_{F_m}$	7.19s	1.19s	8.82s
5	50	702	$\mathfrak{o}_{F_m}$	17.39s	1.93s	19.65s

Die gewonnen Laufzeiten bestätigen somit die theoretischen Aussagen aus Sektion 3.5.

7.2 Galoisgruppen über $\mathbb{Q}(t)$

Sei K ein Körper der Charakteristik Null. Haben wir ein Polynom f über der transzendenten Erweiterung $K(t)$ gegeben, so folgt nach dem Hilbertschen Irreduzibilitätssatz (vgl. Matzat [57], Kapitel IV,§1, Satz 1), daß es unendlich viele $t_0 \in K$ gibt, so daß $\mathcal{G}(f(t,x),K(t)) \cong \mathcal{G}(f(t_0,x),K)$ ist. Ist das spezialisierte Polynom irreduzibel über K, so kann die Galoisgruppe aber durchaus verschieden von der Galoisgruppe über $K(t)$ sein, wie die folgenden Beispiele zeigen:

(i) Sei $f(t,x) = x^4 - 2x^2 + t$. Es gilt $\mathcal{G}(f,K(t)) = D(4)$. Ist $t_0 = a^2 \in K$ ein Quadrat eines Elements $a \in K$, so folgt $\mathrm{disc}(f(t_0,x)) = 256t_0^3 - 512t_0^2 + 256t_0 = 2^8a^2(a-1)^2(a+1)^2$ und $\mathcal{G}(f(t_0,x),K)$ ist die Kleinsche Vierergruppe $E(4) = C(2) \times C(2)$.

(ii) Seien $g, h \in K[x]$ irreduzible Polynome mit nicht isomorphen Galoisgruppen. Wir definieren

$$f(t,x) := tg(x) + (1-t)h(x) \in K(t)[x].$$

Das Polynom $f(t,x)$ ist irreduzibel über $K(t)$, aber Spezializierung von t zu 0 und 1 liefert über K irreduzible Polynome mit nichtisomorphen Galoisgruppen.

Speziell aus (i) folgt, daß es unendlich viele Ausnahmewerte $t_0 \in K$ geben kann, so daß die Gruppen $\mathcal{G}(f(t,x),K(t))$ und $\mathcal{G}(f(t_0,x),K)$ nicht isomorph zueinander sind. Dennoch gilt in jedem Fall für die Galoisgruppe des spezialisierten Polynoms nach dem van der Waerden-Kriterium (vgl. Satz 1.14) der folgende Zusammenhang: $\mathcal{G}(f(t_0,x),K) \leq \mathcal{G}(f,K(t))$.

Wir vergleichen nun unseren Algorithmus mit dem einzigen anderen implementierten Verfahren für diese Körper. Es handelt sich dabei um die absolute Resolventenmethode in MAPLE [76] für Polynome über $\mathbb{Q}(t_1,\ldots,t_r)$, $(r \in \mathbb{Z}_{>0})$ bis zum Grad 8. Bei unserem Vergleich beschränken wir uns auf Polynome vom Grad 8, wobei diese aus der Datenbank von Klüners, Malle [45] stammen. Hierbei sind die Beispielpolynome der fast-einfachen Gruppen aus dieser Datenbank dem Buch von Malle, Matzat [55] entnommen. Berechnungen, die eine Laufzeit von mehr als 2 Tagen benötigt haben, wurden nach dieser Zeit abgebrochen.

Gruppe	Polynom	KASH	MAPLE
$8T_1$	$x^8+(-4t^4-4)x^6+(8t^6+2t^4+8t^2+2)x^4+(-4t^8-4t^6-4t^4-4t^2)x^2+t^8+t^4$	8.72s	20.78s
$8T_2^+$	$x^8-t^2x^7+(-7t^2-12)x^6+(t^4-3t^2)x^5+(2t^4+6t^2+38)x^4+(t^4-3t^2)x^3+(-7t^2-12)x^2-t^2x+1$	2.19s	13.85s

Gruppe	Polynom	KASH	MAPLE
$8T_3^+$	$x^8-2tx^6+(5t^2+2)x^4+(-8t^3+14t)x^2+4t^4+4t^2+1$	2.72s	2.74s
$8T_4^+$	$x^8+(16t-12)x^6+(-32t+38)x^4+(16t-12)x^2+1$	0.48s	1.88s
$8T_5^+$	$x^8+(-4t^4-12t^2-8)x^6+(6t^8+32t^6+58t^4+40t^2+8)x^4+(-4t^{12}-28t^{10}-76t^8-100t^6-64t^4-16t^2)x^2+t^{16}+8t^{14}+26t^{12}+44t^{10}+41t^8+20t^6+4t^4$	1.83s	76.87s
$8T_6$	$x^8+8x^6+(32t^2+4)x^4+(32t^4+16t^2)x^2+8t^6+12t^4$	1.76s	3.13s
$8T_7$	$x^8+tx^7-28x^6-7tx^5+70x^4+7tx^3-28x^2-tx+1$	2.91s	3.95s
$8T_8$	$x^8+(-4t^4-40t^2-64)x^6+(8t^6+72t^4+48t^2-128)x^4+(-4t^8-24t^6+96t^4+256t^2)x^2-9t^8-90t^6-144t^4$	8.13s	1726.60s
$8T_9^+$	$x^8+tx^6+(2t-1)x^4+tx^2+1$	0.52s	1.23s
$8T_{10}^+$	$x^8+(2t^4+20t^2+18)x^6+(2t^8+48t^6+316t^4+432t^2+162)x^4+(2t^{12}+52t^{10}+494t^8+2136t^6+4446t^4+4212t^2+1458)x^2+t^{16}+32t^{14}+412t^{12}+2784t^{10}+10854t^8+25056t^6+33372t^4+23328t^2+6561$	3.91s	57.10s
$8T_{11}^+$	$x^8+4tx^6+5t^2x^4+2t^3x^2+1$	0.73s	3.34s
$8T_{12}^+$	$x^8-22tx^6+135t^2x^4-150t^3x^2+t^4$	0.60s	4.32s
$8T_{13}^+$	$x^8+18tx^6+(81t^2+2)x^4+(108t^3+2t)x^2+1$	0.54s	1.91s
$8T_{14}^+$	$x^8-36x^6+486x^4+(3t^2+3996)x^2+6561$	0.66s	>2 Tage
$8T_{15}$	$x^8+8x^6+20x^4+16x^2+t+4$	0.82s	11.27s
$8T_{16}$	$x^8+(-128t^{12}-576t^{10}-648t^8)x^6+(4608t^{24}+41472t^{22}+139968t^{20}+209952t^{18}+118098t^{16})x^4+11943936t^{46}+235892736t^{44}+2070033408t^{42}+10593338112t^{40}+34839854784t^{38}+76365945936t^{36}+111557968956t^{34}+104732672193t^{32}+57338232372t^{30}+13947137604t^{28}$	276.63s	16109.23s
$8T_{17}$	$x^8-tx^7-11x^6+7tx^5+36x^4-7tx^3-11x^2+tx+1$	1.34s	3.52s
$8T_{18}^+$	$x^8+tx^6+tx^2+1$	0.59s	2.76s
$8T_{19}^+$	$x^8+(-t^4-2t^2-1)x^6+(2t^6+4t^4+4t^2+2)x^4+(-t^8-3t^6-3t^4-t^2)x^2+t^8+2t^6+t^4$	1.31s	44.31s
$8T_{20}^+$	$x^8+24x^7+220x^6+936x^5+1734x^4+936x^3+(-4096t^6-4096t^4+220)x^2+24x+1$	1.96s	62.12s
$8T_{21}$	$x^8+(2t^2-2)x^6+(3t^4-t^2)x^4+(2t^6+2t^4)x^2+t^8+t^6$	2.96s	7.19s
$8T_{22}^+$	$x^8+(-4t^2+4)x^6+(6t^4-4t^3-14t^2+4t+8)x^4+(-4t^6+8t^5+8t^4-16t^3-4t^2+8t)x^2+t^8+-4t^7+2t^6+8t^5-7t^4-4t^3+4t^2$	1.09s	25.71s
$8T_{23}$	$x^8+6x^4-tx^2-3$	0.60s	6.68s
$8T_{24}^+$	$x^8+6tx^4-16tx^2+9t^2$	0.38s	1.92s
$8T_{25}^+$	siehe unten	1747.22s	>2 Tage
$8T_{26}$	x^8-2x^4+t+1	0.65s	1.49s

Gruppe	Polynom	KASH	MAPLE
$8T_{27}$	$x^8+tx^7-2x^6+2tx^5-5x^4+2tx^3-2x^2+tx+1$	0.94s	5.04s
$8T_{28}$	$x^8+(2t^2+2)x^6+(t^4+4t^2+3)x^4+(2t^4+4t^2+2)x^2+t^4+t^2$	9.62s	2.09s
$8T_{29}^+$	$x^8-4tx^6+(6t^2-t-2)x^4+(-4t^3+4t)x^2+t^4+-2t^2+1$	0.62s	14.46s
$8T_{30}$	$x^8-8x^6+(-4t^2+8)x^4+(16t^2+32)x^2+4t^4+12t^2$	3.70s	105.57s
$8T_{31}$	$x^8+(t^2-1)x^7+(4t^4+8t^2+4)x^6+(4t^6+4t^4-4t^2-4)x^5+(7t^8+28t^6+42t^4+28t^2+7)x^4+(4t^{10}+12t^8+8t^6-8t^4-12t^2-4)x^3+(4t^{12}+24t^{10}+60t^8+80t^6+60t^4+24t^2+4)x^2+(t^{14}+5t^{12}+9t^{10}+5t^8-5t^6-9t^4-5t^2-1)x+t^{16}+8t^{14}+28t^{12}+56t^{10}+70t^8+56t^6+28t^4+8t^2+1$	6.19s	79.92s
$8T_{32}^+$	$x^8-8x^6+18x^4+t^2$	0.62s	2.44s
$8T_{33}^+$	$x^8+4x^5+3x^4+4/3/(t^2+1/3)x^2+2/(t^2+1/3)x+3/4/(t^2+1/3)$	1.61s	>2 Tage
$8T_{34}^+$	$x^8+4x^5+3x^4+12t^2x^2+18t^2x+27/4t^2$	0.510	>2 Tage
$8T_{35}$	$x^8+2x^6+x^4+t$	0.31s	1.15s
$8T_{36}^+$	$x^8+tx^7+(t^2+108)x^6+(t^3+108t+216)x^5+(t^4+108t^2+216t+4374)x^4+(t^5+108t^3+216t^2+4374t+13608)x^3+(t^6+108t^4+216t^3+4374t^2+13608t+99468)x^2+(t^7+108t^5+216t^4+4374t^3+13608t^2+99468t+215784)x+t^8+108t^6+216t^5+4374t^4+13608t^3+99468t^2+215784t+998001$	5.71s	25907.97s
$8T_{37}^+$	$x^8+6x^7+(147t^2+3024)x^2+(126t^2+2592)x+756t^2+15552$	0.85s	334.19s
$8T_{38}$	$x^8-4x^6+t^2+27$	0.62s	1.39s
$8T_{39}^+$	x^8+tx^2+1	0.37s	0.89s
$8T_{40}$	$x^8-8x^6+18x^4-27t$	0.46s	8.44s
$8T_{41}^+$	$x^8-8x^6+24x^4+(4t-32)x^2-12tx+9t+16$	0.49s	>2 Tage
$8T_{42}^+$	$x^8-12x^6+54x^4+(12t^2-108)x^2-36t^2x+27t^2+81$	0.73s	216.45s
$8T_{43}$	$x^8-x^7+7x^6-tx+t$	17.19s	397.10s
$8T_{44}$	x^8+tx^7+tx+1	0.35s	0.84s
$8T_{45}^+$	$x^8-12x^6+54x^4+(4t-108)x^2-12tx+9t+81$	0.35s	0.70s
$8T_{46}$	$x^8-8x^5+6x^4-16t^2x^2+24t^2x-9t^2$	1.49s	1.16s
$8T_{47}$	$x^8-16tx^2+24tx-9t$	0.31s	0.68s
$8T_{48}^+$	$x^8-3x^7+2x^6-4x^5+(-t+8)x^4+tx^3+tx-t$	0.78s	709.54s
$8T_{49}^+$	$x^8-8x^7+t^2+823543$	0.07s	0.06s
$8T_{50}$	x^8+x+t	0.09s	0.04s

Das Polynom der Gruppe $8T_{25}$ ist

$$x^8+(4t^8-8t^7+36t^6-16t^5-8t^4+108t^3+20t^2-232t-148)x^6+(-16t^{10}-16t^9-32t^8-112t^7-240t^6-128t^5-208t^4-128t^3+496t^2+1408t+576)x^5+(6t^{16}-24t^{15}+108t^{14}-160t^{13}+462t^{12}+172t^{11}+44t^{10}+3884t^9+1112t^8+2464t^7+14194t^6+11068t^5+534t^4+16964t^3+19324t^2+7880t+2094)x^4+(-32t^{18}+32t^{17}+96t^{16}-2112t^{15}+4384t^{14}-9216t^{13}-6080t^{12}+6048t^{11}-41920t^{10}-53600t^9-18176t^8-154752t^7-206080t^6-120992t^5-287872t^4-421952t^3-228064t^2-60096t-10816)x^3+(4t^{24}-24t^{23}+108t^{22}-208t^{21}+404t^{20}+140t^{19}+672t^{18}+1328t^{17}+13748t^{16}-11884t^{15}+72032t^{14}+65976t^{13}+27500t^{12}+378184t^{11}+581884t^{10}+312788t^9+1223224t^8+2155284t^7+$$

$1593108t^6 + 1900208t^5 + 3109708t^4 + 2334852t^3 + 668860t^2 + 39816t - 3236)x^2 + (-16t^{26} + 48t^{25} - 128t^{24} - 464t^{23} + 1024t^{22} - 2832t^{21} - 8208t^{20} + 5136t^{19} - 20256t^{18} - 119040t^{17} + 21024t^{16} - 233040t^{15} - 693184t^{14} - 443200t^{13} - 1165360t^{12} - 3144656t^{11} - 2836048t^{10} - 4073008t^9 - 8512192t^8 - 8488560t^7 - 6844256t^6 - 10234656t^5 - 10429744t^4 - 4210112t^3 - 162064t^2 + 275520t + 47872)x + t^{32} - 8t^{31} + 36t^{30} - 64t^{29} - 66t^{28} + 844t^{27} - 1928t^{26} + 1084t^{25} + 8809t^{24} - 19396t^{23} + 12686t^{22} + 75864t^{21} - 105422t^{20} + 31492t^{19} + 563002t^{18} - 292592t^{17} - 21216t^{16} + 2543836t^{15} + 916580t^{14} - 451716t^{13} + 7199811t^{12} + 8121352t^{11} + 1864046t^{10} + 10723596t^9 + 20080301t^8 + 11096812t^7 + 8379910t^6 + 15685188t^5 + 11438\,158t^4 + 1590828t^3 - 1093228t^2 - 372392t - 30567.$

Zum Abschluß dieses Abschnitts betrachten wir noch einige Galoisgruppen zu Polynomen mit größeren Graden. Die Beispielpolynome bis zum Grad 15 haben wir wieder der Datenbank von Klüners, Malle [45] entnommen.

Gruppe	Polynom	Laufzeit
$12T_9^+$	$x^{12} + 6x^{10} + (64t - 44)x^9 + (48t - 27)x^8 + (-120t - 36)x^7 + (1024t^2 - 1344t + 456)x^6 + (1536t^2 - 3144t + 1080)x^5 + (6144t^2 - 6720t - 1548)x^4 + (5504t^2 - 3312t - 3488)x^3 + (10752t^2 + 48t + 864)x^2 + (4704t^2 - 8544t + 3840)x + 5488t^2 - 7088t + 1600$	36.44s
$12T_{17}$	$x^{12} - 36x^{10} + 486x^8 + (864t^2 - 2052)x^6 + (-15552t^2 - 8991)x^4 + (69984t^2 + 69984)x^2 + 186624t^4 + 186624t^2$	17.02s
$12T_{163}^+$	$x^{12} - 24x^{10} + 144x^8 + 8tx^6 + 48tx^4 + 16t^2$	3.89s
$14T_7$	$x^{14} - 2tx^7 - 49tx^6 - 196tx^5 - 294tx^4 - 210tx^3 - 77tx^2 - 14tx + t^2 - t$	5.74s
$15T_{92}^+$	$x^{15} + (450t^2 + 135)x^{11} + (-360t^2 - 108)x^{10} + (50625t^4 + 29250t^2 + 4200)x^7 + (-81000t^4 - 46800t^2 - 6720)x^6 + (32400t^4 + 18720t^2 + 2688)x^5 + (309375t^4 + 217500t^2 + 38000)x^3 + (-742500t^4 - 522000t^2 - 91200)x^2 + (594000t^4 + 417600t^2 + 72960)x - 158400t^4 - 111360t^2 - 19456$	35.15s
$15T_{102}$	$x^{15} - 125tx^3 + 300tx^2 - 240tx + 64t$	1.46s
$18T_{45}$	$x^{18} - t$	7.54s
$21T_{15}$	$x^{21} + 21tx^{10} + 385tx^9 + 2079tx^8 + 5148tx^7 + 7007tx^6 + 5733tx^5 + 2940tx^4 + 952tx^3 + 189tx^2 + 21tx - t^2 + t$	12.15s

7.3 Galoisgruppen über $\mathbb{F}_q(t)$

Analog zur Spezialisierung d.h. Reduktion des Funktionenkörpers $\mathbb{Q}(t)$ nach einer Stelle $\boldsymbol{p}$ mit Primelement $t - t_0$ können wir auch nach einem Primideal des Konstantenkörpers reduzieren. Ist also $f \in \mathbb{Z}[t][x]$ ein in x normiertes Polynom und

bezeichne ϕ die durch den kanonischen Epimorphismus $\mathbb{Z} \to \mathbb{F}_p$ induzierte Abbildung auf die Polynomringe $\mathbb{Z}[t][x]$ und $\mathbb{F}_p[t][x]$, wobei die Primzahl p so gewählt sei, daß $\phi(f)$ separabel ist, so folgt aus dem Waerden-Kriterium (vgl. Satz 1.14) für $R = \mathbb{Z}[t]$ und $\mathfrak{p} = p\mathbb{Z}[t]$, daß $\mathcal{G}(\phi(f), \mathbb{F}_p(t)) \leq \mathcal{G}(\phi(f), \mathbb{Q}(t))$ gilt. Für einen Erweiterungskörper $\mathbb{F}_q$ von $\mathbb{F}_p$ ergibt sich dann $\mathcal{G}(\phi(f), \mathbb{F}_q(t)) \leq \mathcal{G}(\phi(f), \mathbb{F}_p(t)) \leq \mathcal{G}(\phi(f), \mathbb{Q}(t))$. Ähnlich dem Hilbertschen Irreduzibilitätssatz gilt auch bei Reduktion nach einem Primideal des Konstantenkörpers ein Irreduzibilitätssatz: Es gibt nur endlich viele Primzahlen $p \in \mathbb{Z}$, so daß das Polynom $\phi(f)$ über $\mathbb{F}_p(t)$ reduzibel oder auch nur inseparabel wird (vgl. Eichler [24], Kapitel III, §6). Sind $f, \phi(f)$ irreduzibel und $\phi(f)$ separabel, so sind die zugehörigen Galoisgruppen auch hier nicht notwendigerweise isomorph. Wir geben ein Beispiel für eine echte Inklusion: Für eine Primzahl p sei $f(t, x) := x^p - t \in \mathbb{Z}[t][x]$, welches nach dem Irreduzibilitätskriterium von Eisenstein irreduzibel ist. Dann ist $\mathcal{G}(\phi(f), \mathbb{F}_q(t))$ für eine Primzahlpotenz $q \in \mathbb{Z}_{>0}$ eine echte Untergruppe von $\mathcal{G}(f, \mathbb{Q}(t))$, wenn p ein Teiler von $q - 1$ ist: Zunächst einmal ist das Polynom $\phi(f) \in \mathbb{F}_q(t)[x]$ separabel, da die Ableitung px^{p-1} von $\phi(f)$ für $p \mid q - 1$ verschieden von Null ist. Außerdem enthält der Körper $\mathbb{F}_q$ alle p-ten Einheitswurzeln, was bewirkt, daß für eine Nullstelle α von $\phi(f)$ der Körper $\mathbb{F}_q(t, \alpha)$ normal über $\mathbb{F}_q$ ist. Über $\mathbb{Q}(t)$ ist dies dagegen nicht der Fall. Für $p = 3$ und $q = 7$ erhalten wir zum Beispiel $A_3 = \mathcal{G}(\phi(f), \mathbb{F}_7(t)) < \mathcal{G}(f, \mathbb{Q}(t)) = S_3$.

Andere Verfahren zur Galoisgruppenberechnung über $\mathbb{F}_q(t)$ sind uns nicht bekannt, so daß wir keine Laufzeitvergleiche angeben können. Zum Abschluß berechnen wir die Galoisgruppen der Beispiele über $\mathbb{Q}(t)$ über den Funktionenkörpern $\mathbb{F}_3(t), \mathbb{F}_7(t)$ und $\mathbb{F}_{1009}(t)$. Befindet sich in der folgenden Tabelle in einer Spalte der Eintrag „–“, so ist das Polynom über dem Funktionenkörper des entsprechenden endlichen Körpers nicht irreduzibel oder nicht separabel.

Gruppe	Laufzeit					
über $\mathbb{Q}(t)$	Gruppe	$\mathbb{F}_3(t)$	Gruppe	$\mathbb{F}_7(t)$	Gruppe	$\mathbb{F}_{1009}(t)$
$8T_1$	$8T_1$	0.34s	$8T_1$	0.35s	$8T_1$	2.34s
$8T_2^+$	–	–	$8T_2^+$	0.19s	$8T_2^+$	1.44s
$8T_3^+$	$8T_3^+$	0.18s	$8T_3^+$	0.13s	$8T_3^+$	0.95s
$8T_4^+$	$8T_4^+$	0.12s	$8T_4^+$	0.14s	$8T_4^+$	0.90s
$8T_5^+$	$8T_5^+$	0.49s	$8T_5^+$	0.30s	$8T_5^+$	3.34s
$8T_6$	$8T_6$	0.16s	$8T_6$	0.15s	$8T_6$	2.17s
$8T_7$	$8T_7$	0.11s	$8T_1$	0.10s	$8T_1$	1.66s
$8T_8$	–	–	$8T_8$	0.37s	$8T_1$	3.40s
$8T_9^+$	$8T_9^+$	0.18s	$8T_9^+$	0.15s	$8T_9^+$	1.74s
$8T_{10}^+$	$8T_2^+$	0.36s	$8T_{10}^+$	0.26s	$8T_{10}^+$	4.47s
$8T_{11}^+$	$8T_{11}^+$	0.15s	$8T_4^+$	0.16s	$8T_4^+$	1.86s

Gruppe	Laufzeit					
über $\mathbb{Q}(t)$	Gruppe	$\mathbb{F}_3(t)$	Gruppe	$\mathbb{F}_7(t)$	Gruppe	$\mathbb{F}_{1009}(t)$
$8T_{12}^{+}$	–	–	–	–	–	–
$8T_{13}^{+}$	$8T_{13}^{+}$	0.11s	$8T_{13}^{+}$	0.12s	$8T_{13}^{+}$	1.85s
$8T_{14}^{+}$	–	–	$8T_{14}^{+}$	0.10s	$8T_{14}^{+}$	1.89s
$8T_{15}$	$8T_{15}$	0.13s	$8T_{6}$	0.15s	$8T_{6}$	2.00s
$8T_{16}$	–	–	$8T_{16}$	0.95s	$8T_{16}$	7.43s
$8T_{17}$	$8T_{11}^{+}$	0.21s	$8T_{17}$	0.13s	$8T_{17}$	0.99s
$8T_{18}^{+}$	$8T_{18}^{+}$	0.13s	$8T_{18}^{+}$	0.13s	$8T_{18}^{+}$	0.86s
$8T_{19}^{+}$	$8T_{19}^{+}$	0.24s	$8T_{19}^{+}$	0.28s	$8T_{19}^{+}$	3.78s
$8T_{20}^{+}$	–	–	$8T_{20}^{+}$	0.19s	$8T_{20}^{+}$	1.07s
$8T_{21}$	–	–	$8T_{21}$	0.14s	$8T_{21}$	1.17s
$8T_{22}^{+}$	$8T_{11}^{+}$	0.21s	$8T_{22}^{+}$	0.23s	$8T_{22}^{+}$	1.71s
$8T_{23}$	–	–	$8T_{12}^{+}$	0.25s	$8T_{12}^{+}$	1.55s
$8T_{24}^{+}$	–	–	$8T_{24}^{+}$	0.11s	$8T_{24}^{+}$	0.75s
$8T_{25}^{+}$	$8T_{25}^{+}$	0.73s	$8T_{25}^{+}$	2.31s	$8T_{25}^{+}$	5.52s
$8T_{26}$	$8T_{26}$	0.08s	$8T_{26}$	0.07s	$8T_{17}$	0.96s
$8T_{27}$	$8T_{20}^{+}$	0.21s	$8T_{27}$	0.12s	$8T_{27}$	1.02s
$8T_{28}$	$8T_{28}$	0.14s	$8T_{28}$	0.14s	$8T_{28}$	2.75s
$8T_{29}^{+}$	$8T_{29}^{+}$	0.16s	$8T_{29}^{+}$	0.16s	$8T_{29}^{+}$	1.03s
$8T_{30}$	$8T_{10}^{+}$	0.15s	$8T_{30}$	0.23s	$8T_{30}$	1.14s
$8T_{31}$	$8T_{5}^{+}$	0.24s	$8T_{11}^{+}$	0.20s	$8T_{31}$	1.35s
$8T_{32}^{+}$	$8T_{12}^{+}$	0.16s	$8T_{32}^{+}$	0.16s	$8T_{32}^{+}$	2.93s
$8T_{33}^{+}$	–	–	$8T_{33}^{+}$	0.12s	$8T_{33}^{+}$	1.46s
$8T_{34}^{+}$	–	–	$8T_{34}^{+}$	0.10s	$8T_{34}^{+}$	0.79s
$8T_{35}$	$8T_{35}$	0.08s	$8T_{35}$	0.07s	$8T_{28}$	0.65s
$8T_{36}^{+}$	–	–	$8T_{36}^{+}$	0.23s	$8T_{36}^{+}$	1.49s
$8T_{37}^{+}$	–	–	–	–	$8T_{37}^{+}$	0.80s
$8T_{38}$	$8T_{12}^{+}$	0.16s	$8T_{38}$	0.15s	$8T_{38}$	1.52s
$8T_{39}^{+}$	$8T_{12}^{+}$	0.12s	$8T_{39}^{+}$	0.13s	$8T_{39}^{+}$	1.32s
$8T_{40}$	–	–	$8T_{40}$	0.10s	$8T_{40}$	1.03s
$8T_{41}^{+}$	$8T_{14}^{+}$	0.10s	$8T_{41}^{+}$	0.09s	$8T_{41}^{+}$	0.77s
$8T_{42}^{+}$	–	–	–	–	–	–
$8T_{43}$	$8T_{43}$	0.24s	–	–	$8T_{43}$	2.41s
$8T_{44}$	$8T_{44}$	0.87s	$8T_{6}$	0.13s	$8T_{44}$	3.68s
$8T_{45}^{+}$	–	–	$8T_{42}^{+}$	0.16s	$8T_{42}^{+}$	1.01s
$8T_{46}$	–	–	$8T_{46}$	0.10s	$8T_{46}$	0.79s
$8T_{47}$	–	–	$8T_{47}$	0.07s	$8T_{47}$	0.94s
$8T_{48}^{+}$	$8T_{48}^{+}$	0.14s	–	–	$8T_{48}^{+}$	1.4s
$8T_{49}^{+}$	$8T_{49}^{+}$	0.03s	$8T_{49}^{+}$	0.16s	$8T_{49}^{+}$	1.23s
$8T_{50}$	$8T_{50}$	0.05s	$8T_{50}$	0.05s	$8T_{50}$	0.75s

Gruppe	Laufzeit					
über $\mathbb{Q}(t)$	Gruppe	$\mathbb{F}_3(t)$	Gruppe	$\mathbb{F}_7(t)$	Gruppe	$\mathbb{F}_{1009}(t)$
$12T_9^+$	–	–	$12T_9^+$	2.63s	$12T_9^+$	9.56s
$12T_{17}$	–	–	$12T_{17}$	7.53s	$12T_{17}$	35.70s
$12T_{163}^+$	–	–	$12T_{126}^+$	1.23s	$12T_{126}^+$	3.56s
$14T_7$	$14T_7$	16.25s	–	–	$14T_1$	13.79s
$15T_{92}^+$	–	–	$15T_{92}^+$	163915.80s	$15T_{92}^+$	217812.31s
$15T_{102}$	–	–	$15T_{101}$	52128.98s	$15T_{101}$	106030.59s
$18T_{45}$	–	–	$18T_{14}$	29385.57s	$18T_{45}$	83277.12s

Die außerordentlich langen Laufzeiten der Gruppen $15T_{92}^+, 15T_{102}$ und $18T_{45}$ kommen dadurch zustande, daß für Funktionenkörper über endlichen Körpern zum jetzigen Zeitpunkt noch kein Teilkörperalgorithmus implementiert ist. Dies bedeutet zum Beispiel, daß bei der Berechnung der Galoisgruppe des Polynoms f (mit $\mathcal{G}(f, \mathbb{Q}(t) = 15T_{102})$, über $\mathbb{F}_7(t)$ bzw. $\mathbb{F}_{1009}(t)$ zunächst ein Abstieg von der Gruppe S_{15} in das Kranzprodukt $15T_{102} = S_5 \wr S_3$ gemacht werden muß, welcher die Auswertung von 126 126 Nebenklassenrepräsentanten erfordert. Hinzu kommt beim Inklusionstest das Liften von Nullstellen bis zu einer Präzision von $l = 378\,378$ für $l \in \mathbb{Z}_{>0}$ wie in Bemerkung 4.109. Deshalb haben wir auf die Berechnung der Galoisgruppen der Grade $21 - 23$ verzichtet, da in diesen Fällen mit Indizes der Größenordnung $66\,512\,160 - 51\,090\,942\,171\,709\,440\,000$ gearbeitet werden muß.

Symbolverzeichnis

Wir vereinbaren die folgenden Bezeichnungen, falls sie nicht im Zusammenhang erklärt werden:

$\lvert\cdot\rvert$	Betrag eines Körpers	11
$\lvert\cdot\rvert_q$, $\lvert\cdot\rvert_{\mathcal{P}}$	Normierter, diskreter Betrag zum Bewertungsideal q bzw. $\mathcal{P}$	12, 62
$\lvert\cdot\rvert_{\mathfrak{p}}$	Normierter, diskreter Betrag zum Primideal $\mathfrak{p}$	36
$\lvert\cdot\rvert_i$	Betrag zur Bewertung ν_i, $(1 \leq i \leq s)$	64
$\lvert\cdot\rvert_j$	Archimedischer Betrag des algebraischen Zahlkörpers $F, (1 \leq j \leq m)$	36
$\lvert\cdot\rvert_{t^{-\frac{1}{k}}}$	Betrag zur Bewertung $\nu_{t^{-\frac{1}{k}}}$	63
$[\,\lvert\cdot\rvert_p\,]$	Stelle eines Körpers bezüglich des Betrags $\lvert\cdot\rvert_p$	11
$\lVert\cdot\rVert$	Euklidische Norm eines Vektors im $\mathbb{R}^m$ bzw. mit der euklidischen Norm verträgliche Matrixnorm für Matrizen im $\mathbb{R}^{m\times m}$	46
$\lVert\cdot\rVert_{T_2}$	Norm des Funktionenkörpers F/K	65
$\lVert\cdot\rVert_\infty$	Maximumnorm eines Polynoms aus $\mathbb{C}[\pi]$	83
$\lVert\cdot\rVert_{\infty,(l)}$	Maximum der Beträge der ersten l Koeffizienten einer Reihe aus $\mathbb{C}[[\pi]]$	83
$\lVert\cdot\rVert_{t^{-\frac{1}{k}}}$	Norm des m-dimensionalen Raums $E((t^{-\frac{1}{k}}))^m$ über dem Körper $E((t^{-\frac{1}{k}}))$	66
$.^{(j)}$	j-te Konjugierte	35, 64
$.^{tr}$	Transponierter Vektor bzw. Matrix	46
$<\cdot,\cdot>$	Skalarprodukt auf dem $\mathbb{Q}$-Vektorraum des algebraischen Zahlkörpers F	35
$\alpha_1, \ldots, \alpha_n$	Nullstellen des Polynoms $f \in K[x]$ in $N(f, K)$	7, 15
$\alpha_{j,1}, \ldots, \alpha_{j,n}$	Nullstellen des Polynoms $f^{(j)} \in \mathbb{C}[x]$, $(1 \leq j \leq m)$ in $\mathbb{C}$	44
$\alpha_1^*, \ldots, \alpha_n^*$	Nullstellen des Polynoms $\iota_{\mathfrak{p}}(f) \in \mathbb{Z}_p[x]$ in $\mathbb{Z}_p[\rho]$	39
$\alpha_{1,(k)}^*, \ldots, \alpha_{n,(k)}^*$	Approximationen von $\alpha_1^*, \ldots, \alpha_n^*$ mod $p^k\mathbb{Z}_p[\rho]$ in $\mathbb{Z}[\rho]$	41

$\bar{\alpha}$	Nullstelle des Polynoms $\bar{f} \in \bar{F}_{\mathcal{P}}[x]$ in $\bar{F}_{\mathcal{P}}[x]/\bar{f}(x)\bar{F}_{\mathcal{P}}[x]$	74
$\bar{\alpha}_1, \ldots, \bar{\alpha}_n$	Nullstellen des Polynoms $\bar{f} \in \bar{F}_{\mathcal{P}}[x]$ in $N(\bar{f}, \bar{F}_{\mathcal{P}})$	72
$\bar{\alpha}^*_{1,(k)}, \ldots, \bar{\alpha}^*_{n,(k)}$	Approximationen der Nullstellen des Polynoms $\psi(\bar{f}) \bmod p^k\mathbb{Z}_p[\rho]$ in $\mathbb{Z}[\rho]$	80
α'	Nullstelle von $\iota_{\mathcal{P}}(f) \in R[t_0]_{(\mathrm{disc}(\bar{h}_1))}[\bar{\delta}_1][[\pi]][x]$ in $R[t_0, \bar{\delta}_1]_{(\mathrm{disc}(\bar{h}_1)\mathrm{disc}(\bar{f}))}[\bar{\alpha}][[\pi]]$	74
$\alpha'_1, \ldots, \alpha'_n$	Nullstellen des Polynoms $\iota_{\mathcal{P}}(f) \in \mathbb{F}_q[t_0, \bar{\delta}_1][[\pi]][x]$ in $\mathbb{F}_{q^{\deg(\mathcal{P})d}}[[\pi]]$	74
$\alpha'_{1,(l)}, \ldots, \alpha'_{n,(l)}$	Approximationen von $\alpha'_1, \ldots, \alpha'_n \bmod \pi^l\mathbb{F}_{q^{\deg(\mathcal{P})\,d}}[[\pi]]$ in $\mathbb{F}_{q^{\deg(\mathcal{P})\,d}}[\pi]$	79
$\alpha''_1, \ldots, \alpha''_n$	Nullstellen des Polynoms $\psi \circ \iota_{\mathcal{P}}(f) \in \mathbb{Z}_p[\rho][[\pi]][x]$ in $\mathbb{Z}_p[\rho][[\pi]]$	74
$\alpha''_{1,(k,l)}, \ldots, \alpha''_{n,(k,l)}$	Approximationen von $\alpha''_1, \ldots, \alpha''_n \bmod p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$ in $\mathbb{Z}[\rho][\pi]$	80
A	Schranke $A \in \mathbb{R}$ bzw. $A \in \mathbb{Q}$	46, 87
$A_{\bar{F}_{\mathcal{P}},\nu}$	Schranke $A_{\bar{F}_{\mathcal{P}},\nu} \in \mathbb{R}$, $(0 \le \nu \le l-1)$	84
$A_{\bar{F}_{\mathcal{P}}}$	Maximum der $A_{\bar{F}_{\mathcal{P}},\nu}$, $(0 \le \nu \le l-1)$	95
$Abb(\Gamma, G)$	Gruppe aller Abbildungen der Menge Γ in die Menge G	4
b	Grad der Erweiterung E/K	63
$B \subseteq \Omega$, $B_\gamma \subseteq \Lambda \times \Gamma$	Block (Imprimitivitätsgebiet) einer Permutationsgruppe (G, Ω) bzw. $(G, \Lambda \times \Gamma)$	3, 5
$B(k)$, $B(l)$	Schranke $B : \mathbb{Z}_{>0} \to \mathbb{R}$	47, 90
$\mathcal{B}$	Blocksystem einer Permutationsgruppe	3
$\mathcal{B}_0$, $\mathcal{B}_\infty$	Triviale Blocksysteme einer Permutationsgruppe	3
c	$\lvert\cdot\rvert = c^{-\nu(\cdot)}$	11, 62
$char_a$	Charakteristisches Polynom des Elements a	71
$\mathrm{char}(K)$	Charakteristik des Körpers K	9
$C_G(\tau)$	Zentralisator von τ in der Gruppe G	115
$Cl(R, S)$	Ring der über R ganzalgebraischen Elemente von S	12
$\mathcal{C}_{S_n}(G, H)$	Menge $\{\, \tau H \tau^{-1} \mid \tau \in S_n \text{ und } \tau H \tau^{-1} < G \,\}$ für Permutationsgruppen $H < G \le S_n$	21
d, $d_{\tilde{\mathfrak{p}}}$, $d_{\mathcal{P}}$	$\mathrm{kgV}\{\deg(\tilde{f}_1), \ldots, \deg(\tilde{f}_u)\}$ bzw. $\mathrm{kgV}\{\deg(\bar{f}_1), \ldots, \deg(\bar{f}_u)\}$	38,41,74, 79,123,125
d_k	Polynom $\prod_{1 \le i < j \le l}(x_{i,k} - x_{j,k})$, $(1 \le k \le m)$	133
$\deg(f)$	Grad des Polynoms f	30

$\deg(\mathcal{P})$	Grad einer Stelle $\mathcal{P}$	62
$\mathrm{disc}(f)$	Diskriminante des Polynoms f	9
$\mathrm{disc}(\mathfrak{o})$	Diskriminante einer Ordnung des algebraischen Zahlkörpers F	42, 55
δ	Nullstelle des Polynoms $h(x) \in \mathbb{Z}[x]$ in $\mathbb{Q}[x]/h(x)\,\mathbb{Q}[x]$ bzw. Nullstelle des Polynoms $h(t,x) \in R[t][x]$ in $K(t)[x]/h(t,x)K(t)[x]$	35, 61
$\delta_1, \ldots, \delta_m$	Nullstellen des Polynoms $h(t,x) \in K(t)[x]$	72
$\delta^{(1)}, \ldots, \delta^{(m)}$	Konjugierte von δ	35, 64
$\delta^{(1,1)}, \ldots, \delta^{(s,m_s)}$	Konjugierte von δ	64
$\bar{\delta}_1, \ldots, \bar{\delta}_m$	Nullstellen des Polynoms $\bar{h}(x) \in \overline{K(t)}_p[x]$	72
$\bar{\delta}_1^*$	Nullstelle des Polynom $\psi(\bar{h}_1) \in \mathbb{Z}_p[x]$ in $\mathbb{Z}_p$	74
$\bar{\delta}_{1,(k)}^*$	Approximation von $\bar{\delta}_1^*$ mod $p^k\mathbb{Z}_p[\rho]$ in $\mathbb{Z}[\rho]$	80
δ_1'	Nullstelle des Polynoms $\iota_{\mathcal{P}}(h(t,x)) = h_{\mathcal{P}}(\pi,x) \in \bar{F}_{\mathcal{P}}((\pi))[x]$	73, 83
D	Polynom $D := \prod_{1\le i<j\le m}(y_i - y_j)$	133
e	$\mathrm{kgV}(e_1, \ldots, e_s)$	64
e_i	Verzweigungsindex der Stelle $\mathcal{P}_i$ über $\mathfrak{p}_\infty$, $(1 \le i \le s)$	64
e_i'	Verzweigungsindex der Stelle $\mathcal{P}_i'$ über $\mathfrak{p}_\infty'$, $(1 \le i \le s')$	90
$e(\mathfrak{p}\|p)$	Verzweigungsindex des Primideals $\mathfrak{p}$ über $p\mathbb{Z}$	36
$e(\mathcal{P}\|\mathfrak{p})$	Verzweigungsindex des Bewertungsideals $\mathcal{P}$ über $\mathfrak{p}$	12
E	Algebraischer Zahlkörper bzw. endliche Körpererweiterung von K	35, 63
$\mathcal{E}$	Vervollständigung des Körpers E bezüglich eines Betrags (Bewertung, Stelle, „geeigneten“ Primideals) von E	38
$E((t^{-\frac{1}{k}}))$	Körper der Puiseuxreihen mit endlichem Hauptteil in der Variablen $t^{-\frac{1}{k}}$	63
f	Polynom, dessen Galoisgruppe berechnet werden soll	15, 37, 69
$\tilde{f}$	Approximation $\tilde{f} \equiv f$ mod $\mathfrak{p}^k$ in $\mathbb{Z}[x]$	40, 41
$\bar{f}$	f mod $\mathcal{P} \in \bar{F}_{\mathcal{P}}[x]$, $\bar{f} \equiv \bar{f}_1 \cdots \bar{f}_u$ mod $\mathcal{P}$	72
$f_{\mathcal{P}}$	Bild des Polynoms f bezüglich der Abbildung $\iota_{\mathcal{P}}$	73
$f(\mathfrak{p}\|p)$	Trägheitsgrad des Primideals $\mathfrak{p}$ über $p\mathbb{Z}$	36
$f(\mathcal{P}\|\mathfrak{p})$	Trägheitsgrad des Bewertungsideals $\mathcal{P}$ über $\mathfrak{p}$	12
F	Algebraischer Zahlkörper	35

F/K	Algebraischer Funktionenkörper	61
F'/K'	Konstantenkörpererweiterung von F/K	62
$F(x_1,\ldots,x_n)$	G-relatives H-invariantes Polynom für Permutationsgruppen $H < G \leq S_n$	17
$Fix(E,H)$	Fixkörper der Gruppe H im Körper E	7
$\bar{F}_{\mathcal{P}}$	Restklassenkörper von F bezüglich der Stelle $\mathcal{P}$, welcher mit $K(t_0,\bar{\delta}_1)$ identifiziert wird	72
$\mathcal{F}$	Vervollständigung des Körpers F bezüglich eines Betrags (Bewertung, Stelle, „geeigneten“ Primideals) von F	12
$\mathcal{F}_i$	Vervollständigung des Körpers F/K bezüglich der Stelle $\mathcal{P}_i$, $(1 \leq i \leq s)$ von F/K	64
γ, γ_σ	Nullstelle der Resolvente $R_{G,H,F)}$ in $Cl(\mathfrak{o}_F, N(f,F))$	44
$\gamma^*, \gamma^*_\sigma$	Nullstelle der Resolvente $\iota_{\mathfrak{p}}(R_{G,H,F)})$ in $\mathbb{Z}_p[\rho]$	44
$\gamma^*_{(k)}, \gamma^*_{\sigma,(k)}$	Approximation von γ^* bzw. γ^*_σ mod $p^k\mathbb{Z}_p[\rho]$ in $\mathbb{Z}[\rho]$	44
$\gamma^*_{(k,i)}$	i-ter Koeffizient von $\gamma^*_{(k)} = \sum_{i=1}^{d} \gamma^*_{(k,i)}\rho^{i-1} \in \mathbb{Z}[\rho]$, $d := [\,\mathbb{Q}(\rho):\mathbb{Q}\,]$	44
γ', γ'_σ	Nullstelle der Resolvente $\iota_{\mathcal{P}}(R_{G,H,F)}) \in \bar{F}_{\mathcal{P}}[[\pi]]$ in $N(\bar{f},\bar{F}_{\mathcal{P}})[[\pi]]$	82
$\gamma'_{(l)}, \gamma'_{\sigma,(l)}$	Approximation vom Grad $l-1$ von γ' bzw. γ'_σ mod $\pi^l\bar{F}_{\mathcal{P}}[[\pi]]$ in $\bar{F}_{\mathcal{P}}[\pi]$	82
$\gamma'', \gamma''_\sigma$	Nullstelle der Resolvente $(\psi\circ\iota_{\mathcal{P}})(R_{G,H,F)})$ in $\mathbb{Z}_p[\rho][[\pi]]$	82
$\gamma''_{(k,l)}, \gamma''_{\sigma,(k,l)}$	Approximationen vom Grad $l-1$ von γ'' bzw. γ''_σ mod $p^k\mathbb{Z}_p[\rho][[\pi]] + \pi^l\mathbb{Z}_p[\rho][[\pi]]$ in $\mathbb{Z}[\rho][\pi]$	82
$\gamma'^{[j]}, \gamma'^{[j]}_\sigma$	Nullstelle $F(\phi_{j,1}(\alpha'),\ldots,\phi_{j,n}(\alpha'))$ der Resolvente in $\mathbb{C}[[\pi]]$	82
$\gamma'^{[j]}_{(l)}, \gamma'^{[j]}_{\sigma,(l)}$	Approximation vom Grad $l-1$ von $\gamma'^{[j]}$ mod $\pi^l\mathbb{C}[[\pi]]$ bzw. $\gamma'^{[j]}_\sigma$ mod $\pi^l\mathbb{C}[[\pi]]$ in $\mathbb{C}[\pi]$	82
G	Permutationsgruppe $G \leq S_n$	16
$G\|_{\mathcal{B}}$	Permutationsdarstellung der Gruppe G auf dem Blocksystem $\mathcal{B}$	137
(G,Ω)	Permutationsgruppe G, die auf der Menge Ω operiert	2
$(G//H)_U$	Verkürztes Nebenklassenrepräsentantensystem bezüglich der Permutationsgruppe U	113, 115
$G \wr_\Gamma H$	Kranzprodukt der Gruppen G und H bezüglich der Menge Γ	4
$G(E/F)$	Galoisgruppe der Körpererweiterung E/F	7
$G(f,K)$	Galoisgruppe der Körpererweiterung $N(f,K)/K$	7

$\mathcal{G}(f,K)$	Zu $G(f,K)$ isomorphe Permutationsgruppe	7
h	Erzeugendes Polynom des algebraischen Zahlkörpers F bzw. des Funktionenkörpers F/K	35, 61
$h(V^H,t)$	Hilbert-Reihe von V^H	132
$\bar{h}$	$\bar{h} := h \bmod p\mathbb{Z} \in \mathbb{F}_p[x]$ bzw. $\bar{h} := h \bmod \mathfrak{p} \in \overline{K(t)}_p[x]$	36, 63, 72
$h_{\mathcal{P}}$	Bild des Polynoms h bezüglich der Abbildung $\iota_{\mathcal{P}}$	73
${}^h f$	Das aus f durch Tschirnhausentransformation mittels des Polynoms $h \in K[x]$ hervorgegangene Polynom	25
H	Permutationsgruppe $H \leq S_n$	16
Im	Imaginärteil einer komplexen Zahl	46
$\iota_{\mathfrak{p}}$	Bewertungserhaltender Monomorphismus des algebraischen Zahlkörpers F nach $\mathbb{Q}_p$	39
$\iota_{\mathcal{P}}$	Bewertungserhaltender Monomorphismus des algebraischen Funktionenkörpers F/K nach $\bar{F}_{\mathcal{P}}((\pi))$	73
k	Präzision	41, 80
k'	Heuristische Präzision	53, 103
$K(t)$	Funktionenkörper $K(t)$, $K \in \{\mathbb{F}_q, \mathbb{Q}\}$	61
$K^\times$	Einheitengruppe des Körpers K	11
$\tilde{K}$	Exakter Konstantenkörper von F/K	61
$\bar{K}_{\mathfrak{q}}$	Restklassenkörper des Körpers K bezüglich des Bewertungsideals $\mathfrak{q}$	11
$\overline{K(t)}_p$	Restklassenkörper des Körpers $K(t)$ bezüglich der Stelle p; welcher mit dem Körper $K(t_0)$ identifiziert wird	63, 72
$K(s_1,\ldots,s_n)$	Körper der rationalen symmetrischen Funktionen	16
l	Präzision	80
l'	Heuristische Präzision	103
$\mathcal{L}$	Liste der Vertreter der S_n-Konjugationsklassen transitiver Gruppen	27
$\mathcal{L}_G$	Menge aller $T \in \mathcal{L}$ für die eine Permutation $\varrho \in S_n$ existiert mit $\varrho T \varrho^{-1} \in \mathcal{R}_G(G)$	27
$\mathcal{L}_u$	Menge der ungeraden Gruppen in $\mathcal{L}$	28,123,125
$\mathcal{L}_g$	Menge der geraden Gruppen in $\mathcal{L}$	28,123,125
$\mathcal{L}_z$	Menge der noch möglichen Galoisgruppen in $\mathcal{L}$	28,123,125
$\Lambda_{\gamma^*_{(k,1)},(k)}$	Gitter der Dimension $m+1$ im $\mathbb{R}^{m+1}$	46
$\Lambda'_{\gamma^*_{(k,1)},(k)}$	Teilgitter von $\Lambda_{\gamma^*_{(k,1)},(k)}$, welches nur aus den Relationen der $\omega^*_{i,(k)} \in \mathbb{Z}$, $(1 \leq i \leq m)$ besteht	46

$\Lambda_{\gamma'_{(l)},(l)}$	$\bar{F}_{\mathcal{P}}[\pi]$-Gitter der Dimension $m+1$ im $\bar{F}_{\mathcal{P}}((\pi^{-1}))^{m+1}$	87
$\Lambda'_{\gamma'_{(l)},(l)}$	Teilgitter von $\Lambda_{\gamma'_{(l)},(l)}$, welches nur aus den Relationen der $\omega'_{i,(l)}$, $(1 \leq i \leq m)$ besteht	87
m	Grad der Erweiterung $F/\mathbb{Q}$ bzw. Grad der Erweiterung $F/K(t)$	35, 61
m_α	Minimalpolynom des Elements α	25
μ	Minkowskiabbildung $\mu : F \longrightarrow \mathbb{R}^m$ bzw. $\mu : F \longrightarrow E((t^{-\frac{1}{e}}))^m$	46, 87
M_j	Reelle obere Schranke der Absolutbeträge der komplexen Nullstellen von $R^{(j)}_{(G,H,F)}$, $(1 \leq j \leq m)$	46
$M_{\bar{F}_{\mathcal{P}},j,\nu}$	Reelle obere Schranke von $\lvert g_{j,\nu}\rvert$, $\gamma'^{[j]}_{(l)} = \sum_{\nu=0}^{l-1} g_{j,\nu}\pi^\nu \in \mathbb{C}[\pi]$	84
$M^{[j]}_{\bar{F}_{\mathcal{P}},(l)}$	Polynom vom Grad $l-1$ aus $\mathbb{R}[\pi]$ mit Koeffizienten $M_{\bar{F}_{\mathcal{P}},j,\nu}$	85
$\mathrm{N}_{F/\mathbb{Q}}(a)$	Norm des Elements $a \in F$ über dem Körper $\mathbb{Q}$	37
$\mathrm{N}(\mathfrak{p})$	Norm des Primideals $\mathfrak{p}$	9
$N(g,Q)$	Zerfällungskörper des Polynoms $g(x) \in Q[x]$ über dem Körper Q	12
$N_G(H)$	Normalisator der Gruppe H in G	3
ν	Exponentielle, surjektive Bewertung $K \longrightarrow \mathbb{R} \cup \{\infty\}$	11
ν_p	Normierte, diskrete Bewertung $\mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Primideals $p\mathbb{Z}$ bzw. normierte, diskrete Bewertung der Vervollständigung $\mathbb{Q}_p$ von $\mathbb{Q}$ bzgl. $p\mathbb{Z}$ und deren Fortsetzung auf $\mathbb{Q}_p(\rho)$	40
$\nu_{\mathfrak{p}}$	Normierte, diskrete Bewertung $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Primideals $\mathfrak{p}$ bzw. deren Fortsetzung auf $N(f,F)$	36, 39
$\nu_{\mathfrak{P}}$	Normierte, diskrete Bewertung $E \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Primideals $\mathfrak{P}$ bzw. normierte, diskrete Bewertung der Vervollständigung $\mathcal{E}$ von E bzgl. $\mathfrak{P}$.	38
$\nu_{\mathfrak{q}}$	Normierte, diskrete Bewertung $K \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathfrak{q}$	12
$\nu_{\mathcal{P}}$	Normierte, diskrete Bewertung $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathcal{P}$ und deren Fortsetzung auf $N(f,F)$ bzw. normierte, diskrete Bewertung der Vervollständigung $\mathcal{F}$ von F bzgl. $\mathcal{P}$	62, 70
ν_π	Normierte, diskrete Bewertung $\bar{F}_{\mathcal{P}}((\pi)) \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\pi\bar{F}_{\mathcal{P}}[[\pi]]$ und deren Fortsetzung auf $N(\bar{f},\bar{F}_{\mathcal{P}})((\pi))$	70, 73, 81

ν_i	Normierte, diskrete Bewertung $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathcal{P}_i$, $(1 \leq i \leq s)$ bzw. normierte, diskrete Bewertung der Vervollständigung $\mathcal{F}_i$ von F bzgl. $\mathcal{P}_i$	64
ν'_i	Normierte, diskrete Bewertung $F' := F\bar{F}_{\mathcal{P}} \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathcal{P}'_i$, $(1 \leq i \leq s')$	90
ν_∞	Normierte, diskrete Bewertung $K(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathfrak{p}_\infty$	62
ν'_∞	Normierte, diskrete Bewertung $\bar{F}_{\mathcal{P}}(t) \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $\mathfrak{p}'_\infty$	90
$\nu_{t^{-\frac{1}{k}}}$	Normierte, diskrete Bewertung $E((t^{-\frac{1}{k}})) \longrightarrow \mathbb{Z} \cup \{\infty\}$ des Bewertungsideals $t^{-\frac{1}{k}}E[[t^{-\frac{1}{k}}]]$	63
$\mathfrak{o}$	Ordnung des algebraischen Zahlkörpers F	36
$\mathfrak{o}_F$	Ring der ganzalgebraischen Zahlen des Körpers F bzw. des Körpers F/K	36
$\omega_1, \ldots, \omega_m$	Ganzheitsbasis von $\mathfrak{o}_F$	43, 62
$\omega^*_{1,(k)}, \ldots, \omega^*_{m,(k)}$	Approximationen der Ganzheitsbasis von $\mathfrak{o}_F$ in $\mathbb{Z}$	45
$\omega'_{1,(l)}, \ldots, \omega'_{m,(l)}$	Approximationen der Ganzheitsbasis von $\mathfrak{o}_F$ in $\bar{F}_{\mathcal{P}}[\pi]$	85
$\varpi_1, \ldots, \varpi_m$	Ganzheitsbasis der Ordnung $\mathfrak{o}$	54
$\mathcal{O}_\mathfrak{q}, \mathcal{O}_\mathcal{P}$	Diskreter Bewertungsring eines Körpers mit Bewertungsideal $\mathfrak{q}$ bzw. Bewertungsideal $\mathcal{P}$	12, 62
$\mathrm{Orb}_G(\omega)$	Bahn eines Elements $\omega \in \Omega$ unter den Permutationen der Gruppe (G, Ω)	2
$\mathrm{Orb}_G(F)$	Bahn des Polynoms $F(x_1, \ldots, x_n)$ unter den Permutationen der Gruppe G, wobei G auf der Menge $\{x_1, \ldots, x_n\}$ durch Permutation der Indizes operiert	20
$\mathrm{Orb}_G(H)$	Bahn der Permutationsgruppe H unter den Permutationen der Gruppe G, wobei G auf der Menge H durch Konjugation operiert	22
p	Primzahl $p \in \mathbb{Z}_{>0}$	36
$p(t)$	Primpolynom aus $K[t]$	63
π	Primelement der Stelle $\mathcal{P}$	70
$\mathfrak{p}, \tilde{\mathfrak{p}}, \mathfrak{P}$	Primideale eines Rings	8
$\mathfrak{p}, \mathfrak{q}, \mathcal{P}$	Bewertungsideale (Stellen) diskreter Bewertungsringe eines Körpers	12
$\mathfrak{p}_\infty$	Bewertungsideal zu t^{-1} in $K(t)$	62
$\mathfrak{p}'_\infty$	Bewertungsideal zu t^{-1} in $\bar{F}_{\mathcal{P}}(t)$	90

ψ	Ringmonomorphismus	70
$\mathbb{P}(K)$	Menge der Bewertungsideale aller diskreten Bewertungsringe des Körpers K	12
$\mathbb{P}(F)_\infty = \{\mathcal{P}_1, \ldots, \mathcal{P}_s\}$	Menge der Stellen von F/K über $\mathfrak{p}_\infty$	62
$\mathbb{P}(F')_\infty = \{\mathcal{P}'_1, \ldots, \mathcal{P}'_{s'}\}$	Menge der Stellen von F'/K, $(F' = F\bar{F}_\mathcal{P})$ über $\mathfrak{p}'_\infty$	90
$\mathcal{P}(G, T_i, H_{i,j})$	Menge von Permutationen aus $N_{S_n}(G)$	28
q	Elementanzahl des endlichen Körpers $\mathbb{F}_q$ der Charakteristik p	61
$\mathbb{Q}_p$	Körper der p-adischen Zahlen	37
$\mathrm{Quot}(R)$	Quotientenkörper des Integritätsrings R	12
r_1, r_2	Signatur des algebraischen Zahlkörpers F	35
R	Integritätsring	15
$R_{(G,H,F)}$	G-relatives H-invariantes Resolventenpolynom	17
Re	Realteil einer komplexen Zahl	46
$Res_y(h, f)$	Resultante der Polynome h, f bezüglich der Variablen y	78
$\mathcal{R}_{N_{S_n}(G)}(G)$	Vertretersystem der $N_{S_n}(G)$-Konjugationsklassen maximaler transitiver Untergruppen von G	27
$\mathcal{R}_G(G, T_i)$	Menge der $H \in \mathcal{R}_G(G)$ vom transitiven Gruppentyp wie $T_i \in \mathcal{L}$	27
s	Anzahl der Stellen in $\mathbb{P}_\infty(F)$ über $\mathfrak{p}_\infty$	64
s'	Anzahl der Stellen in $\mathbb{P}_\infty(F')$ über $\mathfrak{p}'_\infty$	90
$s_i(x_1, \ldots, x_n)$	i-te elementarsymmetrische Funktion in den Unbestimmten $x_1, \ldots, x_n$	16
$S_{(d)}$	Lokalisierung des Integritätsrings S nach $\{d^i \mid i \in \mathbb{Z}\}$	70
S_Ω	Symmetrische Permutationsgruppe der Menge Ω	1
$\mathbb{S}(K)$	Menge aller Stellen des Körpers K	11
$\mathbb{S}(K)_{norm.diskr.}$	Menge aller normierten diskreten Stellen des Körpers K	12
$\mathrm{Stab}_G(\omega)$	(Punkt-) Stabilisator eines Elements $\omega \in \Omega$ unter den Permutationen der Gruppe (G, Ω)	2
$\mathrm{Stab}_G(B)$	Mengenstabilisator des Blocks $B \subseteq \Omega$ unter den Permutationen der Gruppe (G, Ω)	3

$\mathrm{Stab}_G(B)\vert_B$	Permutationsdarstellung der Permutationsgruppe $\mathrm{Stab}_G(B)$ auf der Menge B	138
$\mathrm{Stab}_G(F)$	Stabilisator des Polynoms $F(x_1, \ldots, x_n)$ unter den Permutationen der Gruppe G	17
t_0	Nullstelle des Primpolynoms $p(t)$	72
$T_2(x)$	T_2-Norm des Elements x eines algebraischen Zahlkörpers	35
$u_{1,(k)}, \ldots, u_{m+1,(k)}$	Basisvektoren des Gitters $\Lambda_{\gamma^*_{(k,1)},(k)}$	45
$u_{1,(l)}, \ldots, u_{m+1,(l)}$	Basisvektoren des Gitters $\Lambda_{\gamma'_{(l)},(l)}$	87
V	Polynomring $K[x_1, \ldots, x_n]$ über dem Körper K	132
V_d	K-Vektorraum der homogenen Komponenten vom Grad d in V	132
V^H	Invariantenring bezüglich der Gruppe H	132
V_d^H	K-Vektorraum der homogenen Komponenten vom Grad d in V^H	132
W_j	Schranke $W_j \in \mathbb{R}$, $(1 \leq j \leq m)$ bzw. $W_j \in \mathbb{Q}$, $(1 \leq j \leq s)$	46, 88
$W_{\bar{F}_\mathcal{P},j}$	Schranke $W_{\bar{F}_\mathcal{P},j} \in \mathbb{R}$, $(1 \leq j \leq m)$	84
y_j	Polynom $\sum_{i=1}^{l} x_{i,j}$, $(1 \leq j \leq m)$	133
$\mathbb{Z}_p$	Ring der ganzen p-adischen Zahlen	37

Anhang

Im folgenden geben wir Partitionstabellen für die primitiven Permutationsgruppen der Grade 12 bis 23 an, wie wir sie für den Verifikationsschritt 5.3 verwenden. Für eine primitive Permutationsgruppe der folgenden Tabellen bedeutet die Bezeichnung $110^3, 132^2, 330$, daß die zugehörige r-set Resolvente in drei Faktoren der Grade 110, zwei Faktoren der Grade 132 und einen Faktoren vom Grad 330 zerfällt. Da eine r-set Resolvente eine absolute Resolvente bezüglich der intransitiven Gruppen $H = S_r \times S_{n-r}$, $(1 \leq r \leq \lfloor n/2 \rfloor)$ ist, bedeutet dies nichts anderes, als daß die Bahnlängen der Operation der primitiven Permutationsgruppe auf den Nebenklassen von S_n/H den Werten $110^3, 132^2, 330$ entsprechen. Da S_n-relative $S_1 \times S_{n-1}$-invariante Resolventen irreduzibel vom Grad n sind, werden durch diese Polynome im Hinblick auf unsere Anwendung keine Informationen erhalten. Folglich haben wir 1-set Resolventen nicht mit in die Tabellen aufgenommen. Die Notation der Permutationsgruppen setzt sich aus einer Ziffer n für den Grad, dem Buchstaben T, welcher für transitiv steht, und einer Nummer zusammen, die man für den jeweiligen Grad in Conway et al. [18] (bis Grad 15) oder den Computeralgebrasystemen GAP [54] bzw. MAGMA [5, 16] entnimmt. Falls es sich um eine gerade Gruppe handelt, wird dies zusätzlich mit einem „ + “-Exponenten vermerkt. Entsprechende Partitionstabellen für die Grade 8 bis 11 lassen sich zum Beispiel in Eichenlaub [22] finden.

Grad 12

$\mathcal{G}(f, F)$	2-set	3-set	4-set	5-set	6-set
$12T_{301}$	66	220	495	792	924
$12T^+_{300}$	66	220	495	792	924
$12T^+_{295}$	66	220	495	792	$132, 792$
$12T^+_{272}$	66	220	$165, 330$	$132, 660$	$22, 110, 792$
$12T_{218}$	66	220	$165, 330$	$132, 660$	$110, 220, 264, 330$
$12T^+_{179}$	66	220	$165, 330$	$132, 660$	$110^3, 132^2, 330$

Grad 13

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set
$13T_9$	78	286	715	1287	1716
$13T_8^+$	78	286	715	1287	1716
$13T_7^+$	78	$52, 234$	$13, 234, 468$	$117, 468, 702$	$78, 234, 468, 936$
$13T_6$	78	$52, 78, 156$	$39, 52, 78^2, 156^3$	$39, 78^2, 156^7$	$26, 52, 78^3, 156^9$
$13T_5^+$	39^2	$26^2, 39^2, 78^2$	$26^2, 39^5, 78^6$	$39^5, 78^{14}$	$13^2, 26^2, 39^6, 78^{18}$
$13T_4$	26^3	$26^3, 52^4$	$13^3, 26^6, 52^{10}$	$13^3, 26^6, 52^{21}$	$26^{10}, 52^{28}$
$13T_3^+$	39^2	$13^4, 39^6$	$13^4, 39^{17}$	39^{33}	$13^6, 39^{42}$
$13T_2^+$	13^6	$13^6, 26^8$	$13^{15}, 26^{20}$	$13^{15}, 26^{42}$	$13^{20}, 26^{56}$
$13T_1^+$	13^6	13^{22}	13^{55}	13^{99}	13^{132}

Grad 14

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$14T_{63}$	91	364	1001	2002	3003	3432
$14T_{62}^+$	91	364	1001	2002	3003	3432
$14T_{39}$	91	364	$182, 273, 546$	$364, 546, 1092$	$91, 182, 546, 1092^2$	$156, 364, 728, 1092^2$
$14T_{30}^+$	91	182^2	$91^2, 273, 546$	$182^2, 546^3$	$91^3, 546^3, 1092$	$78^2, 182^2, 364^2, 546^4$

Grad 15

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$15T_{104}$	105	455	1365	3003	5005	6435
$15T_{103}^+$	105	455	1365	3003	5005	6435
$15T_{72}^+$	105	$35, 420$	$105, 420, 840$	$168, 315, 840, 1680$	$105, 280, 420, 1680, 2520$	$15, 120, 420, 840, 2520^2$
$15T_{47}^+$	105	$35, 420$	$105, 210, 420, 630$	$42, 126, 315, 420, 840, 1260$	$70, 105, 210, 420^2, 1260, 2520$	$15, 120, 420, 630^2, 840, 1260^3$

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$15T_{28}^{+}$	$45, 60$	$15, 20, 60, 180^2$	$30, 45, 60^2, 90, 180^2, 360^2$	$6, 45, 60, 72, 90^2, 120, 180^2, 360^6$	$10, 15, 60^3, 90^2, 120, 180^3, 360^9, 720$	$15, 60, 90^2, 120^2, 180^9, 360^6, 720^3$
$15T_{20}^{+}$	$45, 60$	$15, 20, 60, 180^2$	$30, 45, 60^2, 90, 180^4, 360$	$6, 36^2, 45, 60, 90^2, 120, 180^6, 360^4$	$10, 15, 60^5, 90^2, 180^7, 360^9$	$15, 60, 90^2, 120^2, 180^{15}, 360^9$

Grad 16

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set
$16T_{1954}$	120	560	1820	4368	8008	11440	12870
$16T_{1953}^{+}$	120	560	1820	4368	8008	11440	12870
$16T_{1906}^{+}$	120	560	140, 1680	1680, 2688	$448, 840, 6720$	$240, 4480, 6720$	$30, 840, 1920, 10080$
$16T_{1840}^{+}$	120	560	140, 1680	$672, 1680, 2016$	$112, 336, 840, 6720$	$240, 1120, 3360, 6720$	$30, 840, 1920, 5040^2$
$16T_{1753}^{+}$	120	240, 320	60, 80, 240, 1440	$96, 720, 960, 1152, 1440$	$16, 120, 192, 240, 720, 960, 2880^2$	$160, 240, 960^2, 1440, 1920, 2880^2$	$30, 360, 480, 720^2, 1440^2, 1920, 5760$
$16T_{1654}^{+}$	120	240, 320	60, 80, 240, 1440	$96, 576^2, 720, 960, 1440$	$16, 96^2, 120, 240, 720, 960, 2880^2$	$160, 240, 960^4, 1440, 2880^2$	$30, 360, 480, 720^2, 1440^2, 1920, 2880^2$
$16T_{1653}^{+}$	120	80, 480	20, 120, 720, 960	$240, 288, 960, 1440^2$	$48, 160, 240, 360, 480, 960, 2880^2$	$160, 240, 480, 960^2, 1440^2, 2880^2$	$30, 120, 720^3, 1440^2, 1920, 2880^2$
$16T_{1508}^{+}$	120	80, 480	20, 120, 720, 960	$240, 288, 960, 1440^2$	$48, 160, 240, 360, 480, 960, 1440^2, 2880$	$160, 240, 480, 960^2, 1440^4, 2880$	$30, 120, 720^3, 960^2, 1440^2, 2880^2$

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set
$16T^{+}_{1329}$	120	80, 160, 320	20, 40, 80, 240, 480, 960	96, 192, 240, 480^2, 960^3	16, 32, 80, 120, 160^2, 240, 480, 960^5, 1920	160^2, 240, 320^2, 480^2, 640, 960^7, 1920	30, 120, 240^3, 480^5, 960^4, 1920^3
$16T^{+}_{1328}$	40, 80	160^2, 240	40^2, 60, 80, 160, 480^3	16, 80, 160, 192, 240, 320, 480^3, 960^2	16, 40, 80, 160, 192, 240^4, 320, 480^3, 960^5	80, 160^3, 240^2, 320, 480^3, 960^9	10, 20, 80, 120, 160, 240^4, 320^3, 480^8, 960^3, 1920^2
$16T^{+}_{1294}$	48, 72	32, 96, 144, 288	8, 24, 36, 72, 96, 144, 288^3, 576	96^2, 144^3, 288^3, 576^5	16, 48, 72, 96^2, 144^4, 192, 288^4, 576^8, 1152	16, 96^3, 144^2, 192, 288^5, 576^{12}, 1152^2	12, 18, 48, 72, 144^5, 192, 288^{11}, 576^7, 1152^4
$16T^{+}_{1081}$	40, 80	160^2, 240	40^2, 60, 80, 160, 480^3	16, 80, 96^2, 160, 240, 320, 480^5, 960	16, 40, 80, 96^2, 160, 240^4, 320, 480^5, 960^4	80, 160^3, 240^2, 320, 480^{11}, 960^5	10, 20, 80, 120, 160, 240^4, 320^3, 480^{12}, 960^5
$16T^{+}_{1080}$	120	80, 160^3	20, 40^3, 240^3, 960	96^3, 240, 480^6, 960	16^3, 80^3, 120^3, 160, 480^7, 960^4	160^4, 240, 320^3, 480^{12}, 960^4	30, 120, 240^9, 480^6, 960^8
$16T^{+}_{1079}$	120	80, 480	20, 120, 240, 480, 960	48, 240^2, 480^2, 960^3	48, 120, 160, 240^2, 480^3,960^6	160, 240^3, 480^4, 960^9	30, 120, 240^3, 480^5, 960^{10}
$16T^{+}_{1034}$	48, 72	32, 48^2, 144, 288	8, 12^2, 36, 72, 96, 144, 288^5	96^2, 144^5, 288^8, 576^2	16, 48^3, 72, 96^3, 144^6, 288^9, 576^7	16, 48^2, 96^4, 144^4, 288^{16}, 576^{10}	12, 18, 48, 72^3, 144^8, 192, 288^{17}, 576^{11}

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set
$16T^+_{1030}$	48, 72	32, 96, 144, 428	$8, 24, 36, 72, 96, 144, 288^3, 576$	$96^2, 144^3, 288^7, 576^3$	$16, 48, 72, 96^4, 144^4, 288^6, 576^9$	$16, 96^5, 144^2, 288^{11}, 576^{13}$	$12, 18, 48, 72, 144^5, 192, 288^{15}, 576^{13}$
$16T^+_{777}$	120	$80, 240^2$	$20, 60^2, 240^3, 480^2$	$48, 240^6, 480^6$	$48, 80^2, 120^3, 240^7, 480^{12}$	$80^2, 240^{11}, 480^{18}$	$30, 120^3, 240^{12}, 480^{20}$
$16T^+_{711}$	40, 80	$80, 160^3$	$20, 40^3, 80, 160^4, 320^3$	$16, 32, 80^2, 160^8, 320^9$	$16, 32, 40, 80^5, 160^{11}, 320^{18}$	$80^3, 160^{16}, 320^{27}$	$10, 20, 40, 80^6, 160^{17}, 320^{30}$
$16T^+_{708}$	48, 72	$32, 48^2, 144, 288$	$8, 12^2, 36, 72, 96, 144^3, 288^4$	$96^2, 144^7, 288^{11}$	$16, 48^3, 72^3, 96^3, 144^9, 288^{21}$	$16, 48^2, 96^4, 144^{10}, 288^{33}$	$12, 18, 48, 72^3, 96^2, 144^{14}, 288^{36}$
$16T^+_{447}$	120	$80, 240^2$	$20, 60^2, 240^7$	$48, 240^{18}$	$48, 80^2, 120^7, 240^{29}$	$80^2, 240^{47}$	$30, 120^7, 240^{50}$
$16T^+_{415}$	40^3	80^7	$20^7, 80^9, 160^6$	$16^3, 80^{18}, 160^{18}$	$16^3, 40^9, 80^{23}, 160^{36}$	$80^{35}, 160^{54}$	$10^3, 40^9, 80^{36}, 160^{60}$
$16T^+_{178}$	40^3	80^7	$20^7, 80^{21}$	$16^3, 80^{54}$	$16^3, 40^{21}, 80^{89}$	80^{143}	$10^3, 40^{21}, 80^{150}$

Grad 17

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set
$17T_{10}$	136	680	2380	6188	12376	19448	24310
$17T^+_9$	136	680	2380	6188	12376	19448	24310
$17T^+_8$	136	680	340, 2040	68, 2040, 4080	816, 1360, 2040, 8160	$408, 2720, 4080^2, 8160$	$510, 1360, 2040, 4080, 8160^2$
$17T^+_7$	136	680	$340, 1020^2$	$68, 1020^2, 4080$	$680^2, 816, 2040, 4080^2$	$408, 1360^2, 2040^2, 4080^3$	$510, 680^2, 2040, 4080^5$

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set
$17T_6^+$	136	680	340, 1020^2	$68, 1020^2$, 4080	680^2, 816, 2040^5	$408, 1360^2$, 2040^6, 4080	$510, 680^2$, 2040^5, 4080^3
$17T_5$	136	136, 272^2	$68, 136^3$, 272^7	$68, 136^3$, 272^{21}	136^7, 272^{42}	136^7, 272^{68}	$34, 68$, $136^8, 272^{85}$
$17T_4^+$	68^2	68^2, 136^4	$34^2, 68^6$, 136^{14}	$34^2, 68^6$, 136^{42}	68^{14}, 136^{84}	68^{14}, 136^{136}	$17^2, 34^2$, $68^{16}, 136^{170}$
$17T_3^+$	34^4	34^4, 68^8	$17^4, 34^{12}$, 68^{28}	$17^4, 34^{12}$, 68^{84}	34^{28}, 68^{168}	$34^{28}, 68^{272}$	$17^6, 34^{32}$, 68^{340}
$17T_2^+$	17^8	17^8, 34^{16}	$17^{28}, 34^{56}$	17^{28}, 34^{168}	17^{56}, 34^{336}	$17^{56}, 34^{544}$	$17^{70}, 34^{680}$
$17T_1^+$	17^8	17^{40}	17^{140}	17^{364}	17^{728}	17^{1144}	17^{1430}

Grad 18

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set	9-set
$18T_{983}$	153	816	3060	8568	18564	31824	43758	48620
$18T_{982}^+$	153	816	3060	8568	18564	31824	43758	48620
$18T_{468}$	153	816	612, 1224^2	1224, 2448^3	204, 408, 816, 1224^2, 2448^4, 4896	2448^7, 4896^3	306, 612, 1224^3, 2448^8, 4896^4	272, 612, 816, 1224, 1632, 2448^6, 4896^6
$18T_{377}^+$	153	408^2	306^2, 1224^2	612^2, 1224^6	$102^2, 408$, $612^2, 816$, 1224^5, 2448^4	1224^{14}, 2448^6	153^2, 612^3, 1224^{10}, 2448^{12}	$136^2, 306^2$, $408^2, 612^2$, 816^2, 1224^{12}, 2448^{12}

Grad 19

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set	9-set
$19T_8$	171	969	3876	11628	27132	50388	75582	92378
$19T_7^+$	171	969	3876	11628	27132	50388	75582	92378

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set	8-set	9-set
$19T_6$	171	114, 171, 342^2	114, 171^4, 342^9	171^4, 342^{32}	$57, 114^2$, 171^9, 342^{74}	$57, 114^2$, 171^9, 342^{142}	171^{14}, 342^{214}	$38, 114^3$, 171^{14}, 342^{262}
$19T_5^+$	171	57^2, 171^5	57^2, 171^{22}	171^{68}	57^5, 171^{157}	57^5, 171^{293}	171^{442}	$19^2, 57^6$, 171^{538}
$19T_4$	57^3	38^3, 57^3, 114^6	38^3, 57^{12}, 114^{27}	57^{12}, 114^{96}	$19^3, 38^6$, 57^{27}, 114^{222}	$19^3, 38^6$, 57^{27}, 114^{426}	57^{42}, 114^{642}	$38^{10}, 57^{42}$, 114^{786}
$19T_3^+$	57^3	19^6, 57^{15}	19^6, 57^{66}	57^{204}	19^{15}, 57^{471}	19^{15}, 57^{879}	57^{1326}	19^{20}, 57^{1614}
$19T_2$	19^9	19^9, 38^{21}	19^{36}, 38^{84}	19^{36}, 38^{288}	19^{84}, 38^{672}	19^{84}, 38^{1284}	19^{126}, 38^{1926}	19^{126}, 38^{2368}
$19T_1^+$	19^9	19^{51}	19^{204}	19^{612}	19^{1428}	19^{2652}	19^{3978}	19^{4862}

Grad 20

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$20T_{1117}$	190	1140	4845	15504	38760	77520
$20T_{1116}^+$	190	1140	4845	15504	38760	77520
$20T_{362}$	190	1140	$570, 855$, 1710^2	$684, 1140$, $3420^2, 6840$	$570, 1140^2$, $1710^3, 3420^5$, 6840^2	$1140, 2280^2$, $3420^9, 6840^6$
$20T_{272}^+$	190	1140	$285^2, 855$, 1710^2	$684, 1140$, 3420^4	$570^3, 1140$, $1710^9, 3420^6$	1140^5, 3420^{21}

$\mathcal{G}(f,F)$	8-set	9-set	10-set
$20T_{1117}$	125970	167960	184756
$20T_{1116}^+$	125970	167960	184756
$20T_{362}$	$285, 570, 855, 1140$, $1710^4, 3420^{12}, 6840^{11}$	$380, 1140, 2280$, $3420^{12}, 6840^{18}$	$342, 684, 760, 1710^5$, $2280^3, 3420^{17}, 6840^{16}$
$20T_{272}^+$	$285, 570^3, 855^3, 1710^{13}$, 3420^{29}	$380, 1140^3, 3420^{48}$	$342^3, 380^2, 1140^6$, $1710^{23}, 3420^{40}$

Grad 21

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$21T_{164}$	210	1330	5985	20349	54264	116280
$21T_{163}^{+}$	210	1330	5985	20349	54264	116280
$21T_{103}$	210	210, 1120	105, 2520, 3360	21, 1008, 1680, 7560, 10080	168, 336, 2520^2, 3360, 10080, 15120, 20160	360, 1680, 2520^2, 3360, 10080, 15120, 20160, 30240^2
$21T_{91}^{+}$	210	210, 1120	105, 2520, 3360	21, 1008, 1680, 7560, 10080	168, 336, 2520^2, 3360, 10080, 15120, 20160	360, 1680, 2520^2, 3360, 10080, 15120, 20160, 30240^2
$21T_{85}$	210	210, 1120	105, 840, 1680, 3360	21, 336, 672, 1680, 2520, 5040, 10080	56, 112, 336, 840, 1680, 2520, 3360, 5040, 10080^2, 20160	120, 240, 840, 1680^2, 2520, 3360, 5040, 6720, 10080^4, $13440, 20160^2$
$21T_{67}^{+}$	210	210, 1120	105, 840^3, 3360	$21, 336^3$, 1680, 2520^3, 10080	56^3, 336, 840^3, 2520, 3360, 5040^3, 10080, 20160	120^3, 840^3, 1680, 2520, 3360, 5040^3, 6720^3, 10080^7
$21T_{38}$	105^2	35, 105, 140, 420, 630	105^2, $210, 315, 420^2$, 630, 1260^3	$42, 105^2$, $210, 252, 315, 420^2$, $630^2, 840, 1260^7$; 2520^3	$7, 35, 70, 140, 210^2, 252, 315^2$; $420^4, 630^3$, $840^3, 1260^{11}$, $2520^9, 5040^2$	$105^3, 210^2$, 315, 360, $420^4, 630^5$, $840^2, 1260^{20}$, $2520^{21}, 5040^6$
$21T_{33}^{+}$	105^2	35, 105, 140, 420, 630	105^2, $210, 315, 420^2$, 630, 1260^3	$42, 105^2$, $210, 252, 315, 420^2$, $630^2, 840, 1260^9$, 2520^2	$7, 35, 70, 140, 210^2, 252, 315^2, 420^8$, $630^3, 840, 1260^{13}$; 2520^{12}	$105^3, 210^2$, 315, 360, $420^4, 630^5$, $840^2, 1260^{32}$, 2520^{27}
$21T_{20}$	42, 84^2	$14, 28, 56^2, 84^2$; 168^4, 336	$21, 42^2$, 84^4, 168^{15}, 336^9	$21, 42^2$, $84^5, 168^{36}$, 336^{41}	$14, 28^3, 42$, $56^4, 84^9$, $112^2, 168^{57}$, 336^{129}	$24, 42^2, 84^{13}$, $168^{97}, 336^{294}$

$\mathcal{G}(f,F)$	8-set	9-set	10-set
$21T_{164}$	203490	293930	352716
$21T_{163}^{+}$	203490	293930	352716
$21T_{103}$	$210, 1680, 2520, 5040, 7560, 10080^3, 15120, 20160, 30240^2, 60480$	$210, 280, 1120, 2520^2, 10080^3, 15120, 20160^3, 30240^4, 60480$	$1008, 2520, 3360^2, 3780, 5040, 6048, 10080^3, 15120, 20160^2, 30240^2, 60480^3$
$21T_{91}^{+}$	$210, 1680, 2520, 5040, 7560, 10080^3, 15120, 20160, 30240^2, 60480$	$210, 280, 1120, 2520^2, 10080^3, 15120, 20160^3, 30240^4, 60480$	$1008, 2520, 3360^2, 3780, 5040, 6048, 10080^3, 15120, 20160^2, 30240^4, 60480^2$
$21T_{85}$	$210, 1680^2, 2520^2, 3360^3, 5040^2, 6720^2, 10080^4, 20160^4, 40320$	$210, 280, 840, 1120, 1680, 2520, 3360^2, 5040, 6720^2, 10080^6, 20160^8, 40320$	$336, 672, 1260, 1680, 2016, 2520^2, 3360^4, 4032, 5040, 6720^2, 10080^5, 13440, 20160^8, 40320^2$
$21T_{67}^{+}$	$210, 1680^4, 2520^4, 3360^6, 5040^3, 10080^7, 20160^4$	$210, 280, 840^3, 1120, 2520, 3360^6, 5040^3, 10080^{13}, 20160^6$	$336^3, 1260^3, 1680^3, 2016^3, 2520, 3360^5, 5040^3, 6720^3, 10080^{14}, 20160^7$
$21T_{38}$	$105^2, 210^2, 315^2, 420^6, 630^7, 840^3, 1260^{25}, 2520^{36}, 5040^{14}$	$35, 70, 105^2, 140, 210^2, 315, 420^8, 630^8, 840^7, 1260^{27}, 2520^{49}, 5040^{24}$	$21^2, 210^2, 315^2, 420^8, 504, 630^{10}, 840^3, 1260^{31}, 2520^{59}, 5040^{30}$
$21T_{33}^{+}$	$105^2, 210^2, 315^2, 420^6, 630^7, 840^3, 1260^{45}, 2520^{54}$	$35, 70, 105^2, 140, 210^2, 315, 420^{16}, 630^8, 840^3, 1260^{47}, 2520^{87}$	$21^2, 210^2, 252^2, 315^2, 420^8, 630^{10}, 840^3, 1260^{61}, 2520^{104}$
$21T_{20}$	$21^2, 42^2, 84^{15}, 168^{133}, 336^{535}$	$14, 21^2, 28^3, 42, 56^7, 84^{13}, 112^4, 168^{161}, 336^{788}$	$42^2, 84^{20}, 168^{183}, 336^{953}$

Grad 22

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$22T_{59}$	231	1540	7315	26334	74613	170544
$22T_{58}^{+}$	231	1540	7315	26334	74613	170544

Grad 22

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$22T_{41}$	231	1540	1155, 6160	462, 7392, 18480	77, 2464, 7392, 9240, 55440	352, 1232, 2640, 36960, 55440, 73920
$22T_{38}^{+}$	231	1540	1155, 6160	$462, 3696^2$, 18480	$77, 1232^2, 7392$, 9240, 55440	$176^2, 1232$, $2640, 18480^2$, 55440, 73920

$\mathcal{G}(f,F)$	8-set	9-set	10-set	11-set
$22T_{59}$	319770	497420	646646	705432
$22T_{58}^{+}$	319770	497420	646646	705432
$22T_{41}$	330, 5280, 9240, $27720, 36960^2$, 55440, 147840	4620, 6160, 18480, 24640, 36960, 73920, 110880, 221760	616, 2310, 6160, 14784, 18480, 22176, 27720, 73920, 110880, 147840, 221760	$1344, 7392^2$, 18480, 27720, $73920^3, 88704$, 110880, 221760
$22T_{38}^{+}$	$330, 2640^2, 9240$, $27720, 36960^2$, $55440, 73920^2$	4620, 6160, $18480^3, 24640$, $36960^2, 110880$, 221760	616, 2310, 6160, $7392^2, 18480$, 22176, 27720, $73920^3, 110880$, 221760	$672^2, 7392^2$, $9240^2, 27720$, $36960^2, 44352^2$, $73920^2, 110880^3$

Grad 23

$\mathcal{G}(f,F)$	2-set	3-set	4-set	5-set	6-set	7-set
$23T_7$	253	1771	8855	33649	100947	245157
$23T_6^{+}$	253	1771	8855	33649	100947	245157
$23T_5^{+}$	253	1771	8855	5313, 28336	1771, 14168, 85008	253, 4048, 28336,212520
$23T_4$	253	$253, 506^3$	$253^5, 506^{15}$	$253^5, 506^{64}$	$253^{15}, 506^{192}$	$253^{15}, 506^{477}$
$23T_3^{+}$	253	253^7	253^{35}	253^{133}	253^{399}	253^{969}
$23T_2$	23^{11}	$23^{11}, 46^{33}$	$23^{55}, 46^{165}$	$23^{55}, 46^{704}$	$23^{165}, 46^{2112}$	$23^{165}, 46^{5247}$
$23T_1^{+}$	23^{11}	23^{77}	23^{385}	23^{1463}	23^{4389}	23^{10659}

$\mathcal{G}(f,F)$	8-set	9-set	10-set	11-set
$23T_7$	490314	817190	1144066	1352078
$23T_6^+$	490314	817190	1144066	1352078
$23T_5^+$	$506, 4048, 60720, 212520^2$	$7590, 30360, 70840, 283360, 425040$	$14168, 53130, 85008, 141680, 850080$	$1288, 15456, 17710, 170016, 212520, 425040, 510048$
$23T_4$	$253^{30}, 506^{954}$	$253^{30}, 506^{1600}$	$253^{42}, 506^{2240}$	$46, 253^{42}, 506^{2651}$
$23T_3^+$	253^{1938}	253^{3230}	253^{4522}	$23^2, 253^{5344}$
$23T_2$	$23^{330}, 46^{10494}$	$23^{330}, 46^{17600}$	$23^{462}, 46^{24640}$	$23^{462}, 46^{29162}$
$23T_1^+$	23^{21318}	23^{35530}	23^{49742}	23^{58786}

Literaturverzeichnis

[1] H. Anai, M. Noro and K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials*, Algorithms in Algebraic Geometry and Applications, MEGA '94, Progress in Mathematics 143, Birkhäuser Verlag, 1996, pp. 29–50.

[2] C. Batut, D. Bernadi, H. Cohen, and M. Olivier, Pari-GP, Version 1.39.13, 1996.

[3] B. Beauzamy, *Products of polynomials and a priori estimates for coefficients in polynomial decompositions: a sharp result*, J. Symbolic Comput. **13** (1992), 463–472.

[4] E. H. Berwick, *On Soluble Sextic equations*, Proc. London Math. Soc (2) **29** (1929), 1–28.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24, 3/4** (1997), 235–265.

[6] F. Buekenhout and D. Leemans, *On the list of finite primitive permutation groups of degree* ≤ 50, J. Symbolic Comput. **22** (1996), no. 2, 215–225.

[7] G. Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Comput. **16** (1993), no. 5, 413–422.

[8] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.

[9] J. J. Cannon, B. C. Cox, and D. F. Holt, *Computing the subgroups of a permutation group*, J. Symbolic Comput. **31** (2001), no. 1-2, 149–161, Computational algebra and number theory (Milwaukee, WI, 1996).

[10] D. Casperson and J. McKay, *Symmetric functions, m-sets, and Galois groups*, Math. Comput. **63** (1994), 749–757.

[11] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, American Mathematical Society, New York, 1951.

[12] H. Cohen, *A Course in Computational Algebraic Number Theory*, 3rd corr. printing, GTM 138, Springer-Verlag, Berlin - Heidelberg - New York, 1996.

[13] P. M. Cohn, *Algebraic Numbers and Algebraic Functions*, Chapman & Hall, London, 1991.

[14] A. Colin, *Formal computation of Galois groups with relative resolvents*, Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995), Springer, Berlin, 1995, pp. 169–182.

[15] A. Colin, *Théorie des invariants effective. Applications à la théorie de Galois et à la résolution des systèmes algébriques. Implanatation en Axiom*, Thèse, École Polytechnique, 1997.

[16] Computational algebra group, Magma, `http://www.maths.usyd.edu.au:8000/u/magma/`, 2002.

[17] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985, Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[18] J. H. Conway, A. Hulpke, and J. McKay, *On Transitive Permutation Groups*, LMS J. Comp. Math. **1** (1998), 1–8.

[19] H. Darmon and D. Ford, *Computational Verification of M_{11} and M_{12} as Galois Groups over $\mathbb{Q}$*, Comm. Algebra **17** (1989), no. 12, 2941–2943.

[20] J. D. Dixon and B. Mortimer, *Permutation groups*, Springer-Verlag, Berlin - Heidelberg - New York, 1996.

[21] D. Duval, *Rational Puiseux expansions*, Compositio mathematica **70** (1989), 119–154.

[22] Y. Eichenlaub, *Problèmes effectifs de théorie de Galois en degrés 8 à 11*, Thèse, Université Bordeaux 1, 1996.

[23] Y. Eichenlaub and M. Olivier, *Computation of Galois groups for polynomials with degree up to eleven*, Preprint, Université Bordeaux I, 1995.

[24] M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser Verlag, Basel, 1963.

[25] C. Fieker and C. Friedrichs, *On Reconstruction of Algebraic Numbers*, Proceedings of the Fourth Symposium on Algorithmic Number Theory, ANTS-IV (W. Bosma, ed.), LNCS 1838, Springer-Verlag, Berlin-Heidelberg-New York, 2000, pp. 285–296.

[26] D. J. Ford and J. McKay, *Computation of Galois Groups from Polynomials over the Rationals*, L.N. Pure Appl. Math. **113** (1989), 145–150.

[27] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin - Heidelberg - New York, 1986.

[28] M. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge University Press, Cambridge, 1991.

[29] K. Geißler, *Zur Berechnung von Galoisgruppen*, Diplomarbeit, Technische Universität Berlin, 1997.

[30] K. Geißler and J. Klüners, *Galois group computation for rational polynomials*, J. Symbolic Comput. **30** (2000), no. 6, 653–674, Algorithmic methods in Galois theory.

[31] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. **43** (1983), no. 2-3, 289–307.

[32] L. J. Goldstein, *A Generalization of the Siegel-Walfisz Theorem*, Transactions of the American Mathematical Society **149** (1970), 417–429.

[33] G. Hanrot and F. Morain, *Solvability by radicals from a practical point of view*, submitted to J. Symbolic Comput., 2002.

[34] F. Heß, *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*, Dissertation, Technische Universität Berlin, 1999.

[35] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445.

[36] A. Hulpke, *Konstruktion transitiver Permutationsgruppen. (Construction of transitive permutation groups).*, Ph.D. thesis, Aachener Beiträge zur Mathematik. 18. Aachen: Verlag der Augustinus-Buchhandlung. Aachen: RWTH, 159 p. , 1996.

[37] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin - Heidelberg - New York, 1967.

[38] Kant-Gruppe, KASH, `http://www.math.tu-berlin.de/~kant`, 2002.

[39] G. Kemper and A. Steel, *Some algorithms in invariant theory of finite groups*, Proceedings of the Euroconference on Computational Methods for Representations of Groups and Algebras (Basel) (P. Dräxler, G.O. Michler, and C. M. Ringel, eds.), Progress in Mathematics, Birkhäuser Verlag, 1999.

[40] P. B. Kleidman and M. W. Liebeck, *A survey of the maximal subgroups of the finite simple groups*, Geom. Dedicata **25** (1988), no. 1-3, 375–389, Geometries and groups (Noordwijkerhout, 1986).

[41] J. Klüners, *Über die Berechnung von Teilkörpern algebraischer Zahlkörper*, Diplomarbeit, Technische Universität Berlin, 1995.

[42] J. Klüners, *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, Dissertation, Technische Universität Berlin, 1997.

[43] J. Klüners, *Algorithms for Function Fields*, to appear in Exp. Math., 2002.

[44] J. Klüners and G. Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. (2000), 675–716.

[45] J. Klüners and G. Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196 (electronic).

[46] M. Krasner and L. Kaloujnine, *Produit complet des groupes de permutations et probléme d'extension de groupes II*, Acta Sci. Math.(Szeged) **14** (1951), 39–66.

[47] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296.

[48] S. Lang, *Algebra. 3. ed.*, Reading, MA: Addison Wesley. xv, 906 p. , 1993.

[49] A. K. Lenstra, *Factoring polynomials over algebraic number fields*, LNCS **144** (1982), 32–39.

[50] M. W. Liebeck, C. E. Praeger, and J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups*, J. Algebra **111** (1987), no. 2, 365–383.

[51] R. Loos, *Computing in algebraic extensions*, Computer Algebra, Springer-Verlag, Vienna, New York, 1983, pp. 173–187.

[52] F. Lorenz, *Einführung in die Algebra, Teil II*, BI-Wissenschaftsverlag, Mannheim - Wien - Zürich, 1990.

[53] F. Lorenz, *Einführung in die Algebra, Teil I*, BI-Wissenschaftsverlag, Mannheim - Wien - Zürich, 1992.

[54] M. Schönert et al:, Gap 3.4, patchlevel 3, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1995.

[55] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer-Verlag, Berlin, 1999.

[56] T. Mattman and J. McKay, *Computation of Galois groups over function fields*, Math.Comput. **66** (1997), 823–831.

[57] B. H. Matzat, *Konstruktive Galoistheorie*, Springer-Verlag, Berlin, 1987.

[58] J. McKay and L. Soicher, *Computing Galois Groups over the Rationals*, J. Number Th. **20** (1985), 273–281.

[59] K. Meyberg, *Algebra, Teil 2*, Carl Hanser Verlag, München Wien, 1976.

[60] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, PWN, Polish Scientific Publishers, Warszawa, 1990.

[61] J. Neubüser, *Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten electronischen Dualmaschine*, Numer. Math. **2** (1960), 280–292.

[62] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin - Heidelberg - New York, 1992.

[63] M. Noro and T. Shimoyama, Risa/Asir, Computer Systems Laboratories, Fujitsu Laboratories Limited, 1999.

[64] J. Oesterlé, *Versions effectives du théoremè de Chebotarev sous l'hypothèse de Rieman généralisée*, Astérisque **61** (1979), 165–167.

[65] A. N. Parshin and I. R. Shafarevich (eds.), *Number Theory II*, Encyclopedia of Mathematical Scienes, vol. 62, Springer-Verlag, Berlin - Heidelberg - New York, 1991.

[66] S. Paulus, *Lattice basis reduction in function fields*, Proceedings of the Third Symposium on Algorithmic Number Theory, ANTS-III (Portland, Oregon) (J. Buhler, ed.), LNCS 1423, Springer-Verlag, Berlin - Heidelberg - New York, 1998, pp. 567–575.

[67] M. E. Pohst, *Factoring polynomials over global fields*, submitted to J. Symbolic Comput.

[68] M. E. Pohst, *Computational algebraic number theory*, DMV-Seminar 21, Birkhäuser Verlag, Basel, 1993.

[69] M. E. Pohst and M. Schörnig, *On integral basis reduction in global function fields*, Proceedings of the Second Symposium on Algorithmic Number Theory, ANTS-II (Talence, France) (H. Cohen, ed.), LNCS 1122, Springer-Verlag, Berlin - Heidelberg - New York, 1996, pp. 273–282.

[70] M. E. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopaedia of mathematics and its applications, Cambridge University Press, 1989.

[71] X.-F. Roblot, *Algorithmes de factorisation dans les corps de nombres et applications de la conjecture de Stark à la construction des corpes de classes de rayon*, Thèse, Université Bordeaux 1, 1997.

[72] J. Rotman, *Galois Theory*, Springer-Verlag, Berlin - Heidelberg - New York, 1990.

[73] G. F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268.

[74] M. Rybowicz and B. Lenzinger, *On the implementation of a p-adic method for computing Galois groups*, Preprint, University of Waterloo, 1998.

[75] M. Schörnig, *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern*, Dissertation, Technische Universität Berlin, 1996.

[76] Waterloo Maple Software, Maple V Release 5.1, `ttp://www.maplesoft.com`, 1998.

[77] L. Soicher, *The computation of Galois groups*, Master's thesis, Concordia University, Montreal, 1981.

[78] R. P. Stauduhar, *The Determination of Galois Groups*, Math. Comp. **27** (1973), 981–996.

[79] G. W. Stewart, *Introduction To Matrix Computations*, Academic Press, London, 1973.

[80] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin - Heidelberg - New York, 1993.

[81] N. Tschebotarev, *Grundzüge der Galois'schen Theorie*, P. Noordhoff, Groningen, 1950, Übersetzt und bearbeitet von H. Schwerdtfeger.

[82] F. Stummel und K. Hainer, *Praktische Mathematik*, B.G. Teubner, Stuttgart, 1993.

[83] B. L. van der Waerden, *Algebra I*, Springer-Verlag, Berlin - Heidelberg - New York, 1960.

[84] H. Völklein, *Groups as Galois Groups, An introduction*, Cambridge University Press, Cambridge, 1996.

[85] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999.

[86] R. J. Walker, *Algebraic Curves*, Springer-Verlag, Berlin - Heidelberg - New York, 1978.

[87] H. Wielandt, *Finite Permutation Groups*, Academic Press, London, 1968.

[88] K. Yokoyama, *A modular method for computing the Galois group of polynomials*, MEGA '96 (A. Cohen and M.-F. Roy, eds.), vol. 117-118, J. Pure Appl. Algebra, 1997, pp. 617–636.

Zusammenfassung

Sei F ein algebraischer Zahlkörper oder ein algebraischer Funktionenkörper über $\mathbb{Q}$ oder einem endlichen Körper.

In dieser Arbeit beschreiben wir einen effizienten Algorithmus zur Berechnung der Galoisgruppe eines normierten, irreduziblen und separablen Polynoms f vom Grad $n \leq 23$ über F. Unser Ansatz ist frei von Approximationsfehlern und liefert bewiesene Ergebnisse bei schnellen Laufzeiten. Grundlage des Algorithmus ist das Verfahren von Stauduhar und die Verwendung von p-adischen Approximationen der Nullstellen des Polynoms f.

Für die Berechnungen wird der Zerfällungskörper des Polynoms f in einer geeigneten unverzweigten p-adischen Erweiterung approximiert. Einer der Schwerpunkte dieser Arbeit bildet die Entwicklung von Algorithmen zur Nullstellenberechnung in diesen Erweiterungen und zur Rekonstruktion von algebraischen Elementen aus einer p-adischen Approximation. Für die Rekonstruktionsalgorithmen werden Techniken verwendet, die auf Gittern basieren. Ferner werden Schranken für die Präzision hergeleitet, um die Korrektheit der Ergebnisse zu garantieren. Speziell im Funktionenkörperfall über $\mathbb{Q}$ wird dabei auf die Ergebnisse des Restklassenkörpers (Zahlkörperfall) zurückgegriffen.

Das ursprüngliche Verfahren von Stauduhar wird in vielerlei Hinsicht erweitert, um es speziell für große Grade effizient zu machen. Wir zeigen, wie man durch Berechnung von Teilkörpern des Körpers $F(\alpha)$, wobei α eine Nullstelle von f ist, auf Blocksysteme der Galoisgruppe schließen kann. Somit wird es möglich, die Galoisgruppe in geeignete Kranzprodukte einzubetten und die Einstiegspunkte im Verfahren von Stauduhar variabel zu halten. Weiter wird eine Kombination des Verfahrens mit der absoluten Resolventenmethode vorgestellt, mittels derer die Verwendung extrem großer p-adischer Präzisionen umgangen werden kann. Dadurch wird die Berechnung von primitiven Galoisgruppen höheren Grads überhaupt erst ermöglicht. Darüber hinaus wird der Frobenius-Automorphismus des zugehörigen p-adischen Körpers gewinnbringend eingesetzt, da er Erzeuger einer Untergruppe der Galoisgruppe ist. Durch ihn lassen sich sogenannte verkürzte Nebenklassenrepräsentantensysteme berechnen, die für die zeitkritischen Stellen im Verfahren von Stauduhar enorme Verbesserungen darstellen.

Wir beschreiben Berechnungsmethoden der Daten, die für das Verfahren von Stauduhar notwendig sind, und geben Algorithmen an, mittels derer speziell optimierte Invarianten bestimmt werden können. Diese führen zu weiteren erheblichen Verbesserungen für das Laufzeitverhalten der Galoisgruppenberechnung.

Den Abschluß bilden eine Vielzahl illustrativer Beispiele, die die Leistungsfähigkeit und die Anwendbarkeit des Verfahrens belegen.