Galoisgruppen verallgemeinerter biquadratischer Polynome

Klassische Algebra und ihre Computerimplementierung

Hausarbeit
im Rahmen der Ersten Staatsprüfung für das
Lehramt an Gymnasien/Lehramt an berufsbildenden Schulen;
vorgelegt von
Werner Neumann.

Betreuer: Prof. Dr. P. Schroth
Technische Universität Carolo-Wilhelmina zu Braunschweig

Braunschweig, den 14.12.1999.

Inhaltsverzeichnis

1 Einleitung **2**

2 Grundlagen **5**
2.1 Vom Allgemeinen zum Speziellen 5
2.2 Reine Gleichungen 7
2.3 Galoisgruppen der Kreisteilungspolynome 9
2.4 Primitive $(p-1)$-te Einheitswurzeln vs. primitive Wurzeln modulo p 12

3 Die Galoisgruppen **14**
3.1 Möglicher Grad des Zerfällungskörpers 14
3.2 Galoisgruppen der Ebene 1 16
3.3 Galoisgruppen der Ebene 2 20
3.4 Galoisgruppen der Ebene 3 32
3.5 Zusammenfassung 40

4 Wann treten welche Gruppen auf? **42**
4.1 Einfache Radikalerweiterungen 42
4.2 Strukturanalyse 47
4.3 Bestimmung der Galoisgruppen 51

5 Sein oder nicht sein? – Existenzfragen **53**
5.1 Irreduzibilitätskriterien 53
5.2 Konstruktion bestimmter Polynome 55

6 Computerimplementierung **59**
6.1 Die Prozedur `galbi(p,a,b)` 59
6.2 Die Prozedur `groupSelect(p,a,b)` 60
6.3 Galoisgruppen vs. Permutationsgruppen 64
6.4 Berechnung der Galoisgruppen 65
6.5 Das Listing 69

7 Ausblick **80**

Literatur **81**

1 Einleitung

Gegen Ende des 18. Jahrhunderts wurde die Algebra in der Mathematik eher stiefmütterlich behandelt. Kaum jemand vermochte zu erahnen, welch schier unerschöpflicher Reichtum an Ideenvielfalt und Anwendungsmöglichkeiten sich in unterschiedlichsten Bereichen hinter dieser Disziplin verbirgt. Es waren Pioniere wie Gauss, Abel und nicht zuletzt auch Galois, die mit ihren Ideen wichtige Grundlagen, erste Erkenntnisse und weitere Richtungen vorgaben. Sie erkannten das Potential der Algebra und formten aus ihr eine Disziplin, die nur einhundert Jahre später zu einer der wichtigsten und vielfältigsten der gesamten Mathematik gehörte. Das Wesen der Algebra ist heute nicht nur in Bereichen wie Geometrie, Zahlentheorie und der Analysis vertreten, sondern sie entwickelte ebenso eigene und fruchtbare Zweige.

Eine faszinierende, anziehende Kraft strahlt die Algebra nicht zuletzt dadurch aus, daß es ihr gelang, jahrtausendealte, unlösbar geglaubte Probleme scheinbar "en passant" aufzudecken. Hierzu gehören unter anderem die Quadratur des Kreises, die Dreiteilung eines Winkels und die Volumenverdopplung eines Würfels.

Die Theorie des Evariste Galois (1811-1832) gilt als eine der wichtigsten und grundlegendsten der modernen Algebra. Er betrachtete endliche, normale und separable Körpererweiterungen K' eines Grundkörpers K. Eine endliche Erweiterung ist stets algebraisch, eine normale Erweiterung hingegen liegt vor, wenn es sich um den Zerfällungskörper eines Polynoms $f(x) \in K[x]$ handelt.

Zentrales Element dieser Theorie ist die Galoisgruppe $G(K' \mid K)$. Sie besteht aus all denjenigen Automorphismen $\phi : K' \longrightarrow K'$, die den Grundkörper K elementweise fest lassen.

Faßt man K' als Zerfällungskörper eines Polynoms $f(x) \in K[x]$ auf, so zeichnen sich die Elemente der Galoisgruppe dadurch aus, daß es zu je zwei Wurzeln ω_1, ω_2 eines beliebigen irreduziblen Faktors von $f(x)$ einen Automorphismus $\sigma \in G(K' \mid K)$ gibt, der ω_1 in ω_2 überführt. Als zentrale Ergebnisse der Galoistheorie gelten die Aussagen über die Struktur des Zwischenkörperverbandes der Körpererweiterung K' über K. Im einzelnen heißt dies:

Satz 1.1 (Hauptsatz der Galoistheorie)
Es sei K' eine endliche, normale, separable Körpererweiterung des Grundkörpers K vom Grad n. Dann gelten:

(i) Zu jedem Zwischenkörper L mit $K \subseteq\mid L \subseteq\mid K'$ gehört eine Untergruppe g der Galoisgruppe $G(K' \mid K)$, und zwar die Gesamtheit derjenigen Automorphismen von K', die alle Elemente von L festlassen.

(ii) L ist durch g eindeutig bestimmt durch die Gesamtheit derjenigen Elemente von K', die die Substitutionen von g gestatten, das

heißt bei ihnen invariant bleiben.

(iii) Zu jeder Untergruppe g von $G(K' \mid K)$ existiert ein Körper L, der zu g in der erwähnten Beziehung steht.

(iv) Die Ordnung von g ist gleich dem Grad von K' über L; der Index von g in $G(K' \mid K)$ ist gleich dem Grad von L über K.

(v) L ist genau dann normal über K, wenn g ein Normalteiler in $G(K' \mid K)$ ist.

(vi) Gilt $K \subseteq\mid L_1 \subseteq\mid L_2 \subseteq\mid K'$, so ist die zu L_1 gehörende Gruppe g_1 Obergruppe der zu L_2 gehörenden Gruppe g_2 und umgekehrt.

Beweis: (i) – (iv): vgl. [2] S. 171f. (v): vgl. [2] S. 175. (vi): vgl. [2] S. 173.

Die vorliegende Arbeit ist als Anwendung dieser Theorie anzusehen. Betrachtet werden hierzu verallgemeinerte biquadratische Polynome der Form

$$x^{2p} + ax^p + b \in \mathbb{Q}[x]\,, \tag{1.1}$$

worin p eine ungerade Primzahl ist. Gegenstand der Arbeit sind die Galoisgruppen des Zerfällungskörpers Z_f über dem Grundkörper $\mathbb{Q}$ und ihre Berechnung. Zwar existieren hierzu allgemeine Verfahren (s. [7]), diese sind aber zumeist nur von theoretischem Interesse und stoßen sehr rasch an praktische Grenzen. Zur individuellen Analyse der betrachteten Polynome werden daher spezifische Eigenschaften herausgearbeitet.

In Kapitel 2 werden hierzu algebraische und zahlentheoretische Grundlagen gelegt und die Problemstellung verdeutlicht. Hierin kommt an einigen Stellen bereits der Nutzen der Primeigenschaft des Parameters p zum Ausdruck.

Kapitel 3 befaßt sich mit der Bestimmung und Charakterisierung der Gruppen bis auf Isomorphie. Hierzu werden überdies die Elementeordnungen berechnet, denn stimmen in zwei Gruppen jeweils die Anzahlen der Elemente gleicher Ordnungen nicht überein, so sind die Gruppen nicht isomorph zueinander. Allerdings kann im allgemeinen nicht umgekehrt geschlossen werden, wie auch an einem Beispiel ersichtlich wird. Es zeigt sich, daß in Abhängigkeit von p jeweils 8 bzw. 9 paarweise nichtisomorphe Galoisgruppen existieren, die in entsprechenden Klassen zusammengefaßt werden.

Aufbauend auf diesen Ergebnissen wird in Kapitel 4 ein Verfahren hergeleitet, das es gestattet, die Galoisgruppe eines Polynoms der Form (1.1) in drei Schritten zu bestimmen.

Um aufzuzeigen, daß die angestellten Berechnungen nicht auf Sand gebaut sind, wird in Kapitel 5 bewiesen, daß sämtliche betrachteten

Gruppen auch tatsächlich als Galoisgruppen auftreten. Hierzu werden Methoden zur Erzeugung entsprechender Polynome hergeleitet.

In Kapitel 6 erfolgt schließlich die praktische Umsetzung der Ergebnisse. Es wird unter dem Computeralgebrasystem *Maple V, Release 4* eine Prozedur erzeugt, die die Berechnung der Galoisgruppe unter Vorgabe der Parameter a, b und p durchführt. Hierzu wird speziell auf die Möglichkeiten von *Maple* eingegangen und das Verfahren entsprechend angepaßt.

Im Verlaufe der Betrachtungen haben sich einige Ergebnisse herauskristallisiert, die mit der ursprünglichen Fragestellung nur mittelbar in Beziehung stehen.

In Kapitel 2.4 werden primitive Wurzeln modulo p näher beleuchtet, denen in der Zahlentheorie oft ein mystischer Charakter anhaftet. Es zeigt sich aber, daß diese nichts anderes sind, als die Nullstellen des $(p-1)$-ten Kreisteilungspolynoms über $\mathbb{Q}$ modulo p.

Die Betrachtungen des Kapitel 4.1 zeigen relativ übersichtliche Strukturen einfacher Radikalerweiterungen auf. Diese bieten die Grundlage für das angesprochene Verfahren zur Bestimmung der Galoisgruppe und ermöglichen seine sinnvolle praktische Umsetzung.

2 Grundlagen

Die Struktur der Galoisgruppe eines Polynoms basiert auf der Struktur seines Zerfällungskörpers. Im folgenden Kapitel werden auf der Grundlage allgemeiner Betrachtungen Möglichkeiten zur Zerlegung der Polynome (1.1) untersucht und die dafür notwendigen algebraischen und zahlentheoretischen Grundlagen bereitgestellt.

2.1 Vom Allgemeinen zum Speziellen

Ein Oberkörper L eines Körpers K kann stets als Vektorraum über K aufgefaßt werden. Man definiert den Grad eines Oberkörpers $K \subseteq| L$ durch

$$[L : K] := \mathrm{Dim}_K L\,.$$

Satz 2.1 (Gradformel)
Es seien K, L und M Körper. Dann gilt:

$$K \subseteq| L \subseteq| M \Longrightarrow [M : K] = [M : L] \cdot [L : K]\,.$$

Beweis: vgl. [1], S. 177.

Es sei $h(x) \in K[x]$ und α ein algebraisches Element über K. Gelten die Eigenschaften

1. $h(x)$ ist normiert
2. α ist Nullstelle von $h(x)$
3. Ist $g(x) \in K[x]$ und $\mathrm{Grad}\, g(x) < \mathrm{Grad}\, h(x)$, so gilt $g(\alpha) \neq 0$,

so wird $h(x)$ mit $\mathrm{Irr}(\alpha, K)$ bezeichnet. Hierzu gilt:

Satz 2.2 *Sei α algebraisch über K. Dann gilt:*

(i) *Es gibt genau ein Polynom $Irr(\alpha, K)$*
(ii) *$Irr(\alpha, K)$ ist irreduzibel*
(iii) *Ist $g(x) \in K[x]$ mit $g(\alpha) = 0$, so gilt: $Irr(\alpha, K) \,|\, g(x)$ in $K[x]$.*

Sei $Grad\, Irr(\alpha, K) = n \in \mathbb{N}^*$. Dann gilt:

(iv) $[K[\alpha] : K] = n$
(v) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ *ist eine Basis von $K[\alpha]$ über K*
(vi) $K[\alpha] = K(\alpha)$

Beweis: (i),(ii) vgl. [1] S. 106. (iii): vgl. [1] S. 179 f. (iv) ist eine unmittelbare Folge aus (iv). (v): vgl. [2] S. 120. (vi): vgl. [1] S. 180.

Das Polynom $\mathrm{Irr}(\alpha, K)$ wird als irreduzibles Polynom von α über K

bezeichnet. Offenbar folgt aus dem vorangehenden Satz, daß ein normiertes, irreduzibles Polynom aus $K[x]$, das α zur Nullstelle hat, gleich $\mathrm{Irr}(\alpha, K)$ ist.

Der Zerfällungskörper Z_f eines Polynoms $f(x) \in K[x]$ entsteht durch sukzessive Adjunktion der Nullstellen von f an den Grundkörper K.

Ein Automorphismus der Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ bildet Elemente, die nicht im Grundkörper enthalten sind, stets auf Konjugierte ab. Zwei Elemente α und β heißen genau dann konjugiert zueinander, wenn gilt: $\mathrm{Irr}(\alpha, K) = \mathrm{Irr}(\beta, K)$. Für die Anzahl paarweise verschiedener Automorphismen und damit der Ordnung der Galoisgruppe gilt:

$$\mathrm{Ord}\, G(Z_f \,|\, K) = [Z_f : K]\,.$$

Basierend auf diesen allgemeinen Grundlagen lassen sich für das Ausgangsproblem folgende Fragen formulieren:

- Wie sehen die Nullstellen der Polynome (1.1) aus?
- Welchen Grad kann der Zerfällungskörper über $\mathbb{Q}$ besitzen?
- Wie und wann können derartige Polynome zerfallen?

Im folgenden sei $f(x)$ stets ein Polynom der Form (1.1), also

$$f(x) = x^{2p} + ax^p + b \in \mathbb{Q}[x]\,.$$

Hierin und in allen weiteren Verwendungen bezeichne, falls nicht anders deklariert, $p \in \mathbb{N}$ eine ungerade Primzahl.

Die Nullstellen von $f(x)$ lassen sich mit Hilfe der Lösungsformel für quadratische Gleichungen ermitteln und über das Vorzeichen der Quadratwurzel in zwei Klassen unterteilen:

$$\alpha = \sqrt[p]{-\frac{a}{2} + \sqrt{\frac{a^2}{4} - b}} \qquad \beta = \sqrt[p]{-\frac{a}{2} - \sqrt{\frac{a^2}{4} - b}}\,. \tag{2.1}$$

Darin sei

$$\sqrt{d} := \sqrt{\frac{a^2}{4} - b}$$

für α und β gleich gewählt.

Allgemein wird mit $\sqrt[n]{c}$ stets eine beliebige Nullstelle des Polynoms $x^n - c \in K[x]$ bezeichnet. Im wesentlichen wird diese Symbolik aber für den Fall der Irreduzibilität von $x^n - c$ über dem Grundkörper K verwendet.

Offenbar gilt

$$\sqrt{d} = \alpha^p + \frac{a}{2} = -\left(\beta^p + \frac{a}{2}\right) \in Z_f$$

und daraus folgt

$$\mathbb{Q}[\sqrt{d}] \subseteq | \; Z_f \; .$$

Es existieren sowohl für α, als auch für β maximal p paarweise verschiedene Wurzeln. Der Zerfällungskörper entsteht durch sukzessive Adjunktion dieser Wurzeln an $\mathbb{Q}$. Durch Adjunktion von $\sqrt{d}$ an $\mathbb{Q}$ zerfällt $f(x)$ mindestens in die Faktoren

$$f(x) = (x^p - \alpha^p)(x^p - \beta^p) \in \mathbb{Q}[\sqrt{d}][x] \, . \tag{2.2}$$

Diese Darstellung führt dazu, die oben formulierten Fragen auf Polynome der Form $x^p - c \in K[x]$ zu übertragen.

2.2 Reine Gleichungen

Gleichungen der Form $x^n - c = 0$ mit $n > 0$ werden als reine Gleichungen bezeichnet. Um ihre Lösungen zu bestimmen, sei zunächst der Spezialfall $x^n - 1 \in K[x]$ betrachtet. Die Nullstellen dieses Polynoms heißen n-te Einheitswurzeln, ihre Menge $E_n(K)$ bildet eine multiplikative Gruppe (vgl. [2], S. 127). Elemente, deren Potenzen die gesamte Gruppe erzeugen heißen primitive n-te Einheitswurzeln.

Zwischen den Lösungen einer reinen Gleichung und den Einheitswurzeln besteht folgende Beziehung:

Satz 2.3 *Sei ω_0 eine beliebige Nullstelle von $x^n - c \in K[x]$. Dann gilt für jede Nullstelle ω:*

$$\exists \xi \in E_n(K) : \omega = \xi \cdot \omega_0 \, .$$

Beweis: Es seien zwei Nullstellen ω_0 und ω von $x^n - c \in K[x]$ vorgegeben. Dann ist

$$\omega_0^n = \omega^n = c \, .$$

Daraus folgt

$$\frac{\omega^n}{\omega_0^n} = \left(\frac{\omega}{\omega_0}\right)^n = 1 \, ,$$

und damit ist $\frac{\omega}{\omega_0} = \xi$ eine n-te Einheitswurzel.

Man erhält also die Gesamtheit aller Lösungen einer reinen Gleichung durch Multiplikation einer beliebigen Lösung mit den n-ten Einheitswurzeln. Ist das Polynom $x^n - c \in K[x]$ mit $n > 1$ irreduzibel, so nennt man jede seiner Nullstellen Radikal und bezeichnet sie mit $\sqrt[n]{c}$. Ist $n = p$ eine Primzahl, so spricht man von p-Radikalen. Zwei Radikale eines Polynoms sind algebraisch gleichwertig im Sinne von

$$K\left[\left(\sqrt[n]{c}\right)_1\right] \cong K\left[\left(\sqrt[n]{c}\right)_2\right] \, ,$$

wobei sogar von K-Isomorphie ausgegangen werden kann. Zur Erkennung von Radikalen gilt folgendes Kriterium:

Satz 2.4 *Ist $x^n - c \in K[x]$ reduzibel, dann gibt es einen Teiler $d \mid n$, $d < n$, sodaß c^d die n-te Potenz eines Grundkörperelementes ist.*

Beweis: Sei zunächst $x^n - c \in K[x]$ reduzibel. Dann existieren Polynome $g(x), h(x) \in K[x]$ mit $\mathrm{Grad}\, g(x), \mathrm{Grad}\, h(x) \geq 1$, für die gilt:

$$x^n - c = g(x) \cdot h(x)\,.$$

Nach Satz 2.3 ist jede Nullstelle von $x^n - c$ durch ein Produkt einer beliebigen Nullstelle ω, sowie einer n-ten Einheitswurzel ξ darstellbar. Damit zerfällt das Polynom in seinem Zerfällungskörper zu

$$x^n - c = \prod_{j=0}^{n-1} (x - \xi_j \cdot \omega)\,.$$

Es muß dann zum Beispiel $g(x)$ ein Produkt von $m < n$ Faktoren $x - \xi_j\omega$ sein. Das heißt aber, daß für das absolute Glied $\pm a_0$ von $g(x)$ eine n-te Einheitswurzel ξ existiert, sodaß gilt:

$$a_0 = \xi \cdot \omega^m\,, \quad \text{also} \quad a_0^n = \omega^{mn} = (\omega^n)^m = c^m\,.$$

Es sei $\mathrm{ggT}(m, n) = d < n$. Da $\mathbb{Z}$ ein euklidischer Ring ist, finden sich ganze Zahlen c_0, c_1 mit $d = c_0 m + c_1 n$. Somit folgt insgesamt

$$c^d = c^{c_0 m} \cdot c^{c_1 n} = (c^m)^{c_0} \cdot (c^{c_1})^n = (a_0^n)^{c_0} \cdot (c^{c_1})^n = (a_0^{c_0} \cdot c^{c_1})^n\,,$$

das heißt, c^d ist die n-te Potenz des Grundkörperelementes $(a_0^{c_0} \cdot c^{c_1})$.

Bei der Analyse der Polynome (1.1) werden zu einem Großteil reine Polynome vom Primzahlgrad im Mittelpunkt stehen. Diese werden daher im folgenden speziell untersucht. Die Frage, ob ein p-Radikal vorliegt, läßt sich wie folgt beantworten:

Satz 2.5 *Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $x^p - c \in K[x]$ genau dann reduzibel, wenn c die p-te Potenz eines Grundkörperelementes ist. Anders formuliert: $x^p - c \in K[x]$ ist entweder irreduzibel, oder es existiert eine Nullstelle in K.*

Beweis: Die Hinlänglichkeit der Reduzibilität folgt direkt aus dem vorangehenden Satz. Ist umgekehrt $c = r^p$ mit $r \in K$, so läßt sich ein Linearfaktor abspalten:

$$x^p - c = x^p - r^p = (x - r)(x^{p-1} + rx^{p-2} + \cdots + r^{p-2}x^1 + r^{p-1})\,.$$

Damit ist aber x^p–c reduzibel in $K[x]$ und besitzt in K eine Nullstelle.

Schließlich läßt sich über speziellen Körpern folgendes behaupten:

Satz 2.6 *Der Körper K enthalte alle p-ten Einheitswurzeln. Dann ist $x^p - c$ in $K[x]$ entweder irreduzibel oder zerfällt vollständig in Linearfaktoren.*

Beweis: Ist $x^p - c \in K[x]$ reduzibel, so existiert nach dem soeben Gezeigten eine Nullstelle in K.

Nach Voraussetzung enthält K alle p-ten Einheitswurzeln, sodaß insgesamt mit Satz 2.3 sämtliche Nullstellen von $x^p - c$ in K enthalten sind und damit das Polynom vollständig in Linearfaktoren zerfällt.

2.3 Galoisgruppen der Kreisteilungspolynome

Es seien noch einmal die m-ten Einheistwurzeln Gegenstand der Betrachtungen, speziell im Fall $K = \mathbb{Q}$.

Nach dem Fundamentalsatz der Algebra, zerfällt $x^m - 1$ in $\mathbb{C}[x]$ vollständig in Linearfaktoren:

$$x^m - 1 = (x - \xi_1)(x - \xi_2) \dots (x - \xi_m) \,.$$

Dabei stellen die paarweise verschiedenen komplexen Nullstellen

$$\xi_j = e^{\frac{j}{m} 2\pi i} \qquad 1 \leq j \leq m \tag{2.3}$$

die Gesamtheit aller m-ten Einheitswurzeln über $\mathbb{Q}$ dar. Diese beschreiben in der komplexen Zahlenebene die Eckpunkte eines regelmässigen m-Ecks, das dem Einheitskreis einbeschrieben ist und einen Eckpunkt in 1 besitzt. Die primitiven m-ten Einheitswurzeln sind genau diejenigen ξ_j, für die j und m teilerfremd sind. Es läßt sich dann die multiplikative Gruppe der m-ten Einheitswurzeln durch die Potenzen einer beliebigen primitiven m-ten Einheitswurzel ξ_j erzeugen. Das Polynom

$$\Phi_m(x) = \prod_{\substack{1 \leq j \leq m \\ \mathrm{ggT}(j,m) = 1}} (x - \xi_j)$$

mit den primitiven m-ten Einheitswurzeln als Nullstellen heißt m-tes Kreisteilungspolynom.

Satz 2.7 *Es sei $m \in \mathbb{N}^*$. Dann gilt gilt:*

(i) $\mathit{Grad}\, \Phi_m(x) = \varphi(m)$
(ii) $\Phi_m(x) \in \mathbb{Z}[x]$
(iii) $\Phi_m(x)$ *ist irreduzibel über* $\mathbb{Q}$
(iv) $x^m - 1 = \prod_{d|m} \Phi_d(x)$.

Beweis: vgl. [1], S. 161f.

Mit den Bezeichnungen (2.1) und dem Satz 2.3 läßt sich nun die erste

in Kapitel 2.1 gestellte Frage beantworten: Mit einer primitiven p-ten Einheitswurzel ζ_p über $\mathbb{Q}$ ist die Gesamtheit aller Nullstellen von (1.1) gegeben durch

$$\alpha,\, \zeta_p\alpha,\, \ldots,\, \zeta_p^{p-1}\alpha,\, \beta,\, \zeta_p\beta,\, \ldots,\, \zeta_p^{p-1}\beta\,. \tag{2.4}$$

Welche Struktur besitzt die Galoisgruppe des Polynoms x^m-1 über $\mathbb{Q}$? Der Zerfällungskörper Z_{x^m-1} läßt sich durch Adjunktion einer primitiven m-ten Einheitswurzel ζ_m an $\mathbb{Q}$ realisieren:

$$Z_{x^m-1} = Z_{\Phi_m} = \mathbb{Q}[\zeta_m]\,.$$

Dieser Körper heißt m-ter Kreisteilungskörper. Die Automorphismen σ der Galoisgruppe $G(Z_{\Phi_m}\,|\,\mathbb{Q})$ sind festgelegt durch $\sigma(\zeta_m)$. Ihre Anzahl beträgt

$$|\; G(Z_{\Phi_m}\,|\,\mathbb{Q})\;| = [Z_{\Phi_m} : \mathbb{Q}] = \varphi(m)\,.$$

Mögliche Automorphismen sind gegeben durch

$$\sigma(\zeta_m) \in \{\zeta_m^j \mid \mathrm{ggT}(j,m) = 1 \;\wedge\; 1 \le j \le m\}\,.$$

Da dieses aber genau $\varphi(m)$ verschiedene Möglichkeiten sind, treten all diese in der Galoisgruppe auf:

$$G(Z_{\Phi_m}\,|\,\mathbb{Q}) = \{\sigma_j \mid \sigma_j(\zeta_m) = \zeta_m^j \;\wedge\; \mathrm{ggT}(j,m) = 1 \;\wedge\; 1 \le j \le m\}\,.$$

Für die Verknüpfung zweier Automorphismen gilt

$$(\sigma_i \circ \sigma_j)\,(\zeta_m) = \sigma_i(\zeta_m^j) = (\sigma_i(\zeta_m))^j = \zeta_m^{i\cdot j} = \zeta_m^k = \sigma_k(\zeta_m)$$

mit

$$i \cdot j \equiv k \bmod m\,.$$

So läßt sich die Analyse der Gruppenstruktur auf die Multiplikation modulo m zurückführen. Da die Menge der Automorphismen eine Gruppe darstellt, bildet die Menge

$$M_m = \{j \mid \mathrm{ggT}(j,m) = 1 \;\wedge\; 1 \le j \le m\}$$

eine multiplikative Gruppe der Ordnung $\varphi(m)$. Diese ist vermöge

$$\Psi : (M_m, \cdot) \longrightarrow G(Z_{\Phi_m}\,|\,\mathbb{Q}); \quad j \mapsto \sigma_j$$

isomorph zu $G(Z_{\Phi_m}\,|\,\mathbb{Q})$.

Ein Element $\delta \in M_m$ der Ordnung $\mathrm{Ord}_{M_m}\delta = \varphi(m)$ bezeichnet man als primitive Wurzel modulo m.

Satz 2.8 *Primitive Wurzeln modulo m existieren genau für die Moduln $1, 2, 4, p^r, 2p^r$, mit $p \in \mathbb{N}$ ungerade Primzahl und $r \in \mathbb{N}$.*

Beweis: vgl. [4], S. 64f.

Primitive Wurzeln modulo m erzeugen mit ihren Potenzen die Gruppe $(M_m, \cdot)$. Gruppen, die einelementig erzeugbar sind, heißen zyklisch. Sie besitzen spezifische Eigenschaften:

Satz 2.9 *Sei G eine endliche zyklische Gruppe der Ordnung n. Dann gilt:*

(i) $G \cong \mathbb{Z}_n$
(ii) *Jede Untergruppe U von G ist zyklisch*

Für jeden natürlichen Teiler $d \,|\, n$ gilt:

(iii) *Es existiert genau eine Untergruppe der Ordnung d von G*
(iv) *Es existieren genau $\varphi(d)$ Elemente der Ordnung d in G.*

Beweis: (i) – (iii): vgl. [1], S. 38ff.
(iv): Sei $\mathrm{Ord}_{\mathbf{Z}_m} n = d \mid m$. Dann gilt:

$$d \cdot n \equiv 0 \mod m \quad \Longleftrightarrow \quad d \equiv 0 \mod \frac{m}{\mathrm{ggT}(m,n)} .$$

Da $d > 0$ die kleinste Zahl ist, die diese Kongruenz erfüllt, folgt

$$d = \frac{m}{\mathrm{ggT}(m,n)} , \quad \text{also} \quad \mathrm{ggT}(m,n) = \frac{m}{d} .$$

Damit ist

$$1 = \mathrm{ggT}\left(\frac{m}{\mathrm{ggT}(m,n)}, \frac{n}{\mathrm{ggT}(m,n)}\right) = \mathrm{ggT}\left(d, d \cdot \frac{n}{m}\right) .$$

Da $\frac{n}{m} < 1$, lassen sich bei vorgegebenem m und d genau $\varphi(d)$ verschiedene n finden, die diese Gleichung erfüllen.

An dieser Stelle werden zwei Folgerungen aus (iv) notiert: Da die Ordnung d eines jeden Gruppenelementes stets Teiler der Gruppenordnung n ist, folgt unmittelbar die Identität

$$\sum_{d|n} \varphi(d) = n . \tag{2.5}$$

Auch die Frage nach der Anzahl primitiver Wurzeln modulo m für entsprechende Moduln ist direkt zu beantworten: sie beträgt $\varphi(\varphi(m))$.

Verknüpft man die Sätze 2.8 und 2.9, so ergibt sich für die Galoisgruppen der Kreisteilungspolynome der

Satz 2.10 *Ist m eine Zahl aus $1, 2, 4, p^r, 2p^r$, mit $p \in \mathbb{N}$ ungerade Primzahl und $r \in \mathbb{N}$, so ist die Galoisgruppe $G(Z_{\Phi_m} \mid \mathbb{Q})$ zyklisch. Speziell gilt im Fall $m = p$ Primzahl: $G(Z_{\Phi_p} | \mathbb{Q}) \cong \mathbb{Z}_p^*$.*

Beweis: Zunächst ist $(M_m, \cdot) \cong G(Z_{\Phi_m} | \mathbb{Q})$. Nach Satz 2.8 gibt es eine primitive Wurzel modulo m. Damit ist die Gruppe $(M_m, \cdot)$ zyklisch.

Ist $m = p$ eine Primzahl, so besteht M_p aus allen Zahlen von 1 bis $p - 1$, also $(M_p, \cdot) = \mathbb{Z}_p^* \cong G(Z_{\Phi_p} | \mathbb{Q})$.

2.4 Primitive $(p-1)$-te Einheitswurzeln vs. primitive Wurzeln modulo p

Die im vorigen Abschnitt eingeführten primitiven Einheitswurzeln und primitiven Wurzeln modulo m scheinen zunächst nicht viel gemeinsam zu haben.

Stellt man aber die primitiven $(p-1)$-ten Einheitswurzeln den primitive Wurzeln modulo p gegenüber, so ist für beide erst die $(p-1)$-te Potenz das neutrale Element der Multiplikation.

Um diese Ähnlichkeit weiter analysieren zu können, werden zunächst folgende Ergebnisse aus der Zahlentheorie herangezogen:

Satz 2.11 *Sei $f(x) = c_n x^n + \ldots + c_1 x + c_0 \in \mathbb{Z}[x]$ und $p \in \mathbb{N}$ eine Primzahl mit $p \nmid c_n$. Dann besitzt die Kongruenz $f(x) \equiv 0 \, mod p$ höchstens n modulo p inkongruente Lösungen.*

Beweis: vgl. [4], S. 59f.

Satz 2.12 (multiplikative Möbiussche Umkehrformel)
Die Möbiusfunktion $\mu : \mathbb{N}^* \longrightarrow \mathbb{N}$ ist definiert durch

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 \cdot \ldots \cdot p_k \\ & \text{mit verschiedenen Primzahlen } p_1, \ldots, p_k \in \mathbb{N} \\ 0 & \text{sonst}. \end{cases}$$

Seien $f, F : \mathbb{N}^* \longrightarrow \mathbb{N}$. Dann gilt:

$$\forall n \in \mathbb{N}^* : F(n) = \prod_{d|n} f(d) \quad \Longleftrightarrow \quad \forall n \in \mathbb{N}^* : f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}.$$

Beweis: vgl. [5], S. 181.

Daraus folgt sofort

Satz 2.13 *Für alle $n \in \mathbb{N}^*$ gilt:*

$$\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} .$$

Beweis: Die Formel ergibt sich durch Anwendung der Möbiusschen Umkehrformel auf Satz 2.7 (iv).

Mit Hilfe dieser Sätze folgt nun abschließend in bezug auf die primitiven Wurzeln modulo p:

Satz 2.14 *Die primitiven Wurzeln modulo p sind gegeben durch die Lösungen der Kongruenz $\Phi_{p-1}(x) \equiv 0 \, mod \, p$.*

Beweis: Satz 2.13 ergibt für das $(p-1)$-te Kreisteilungspolynom

$$\Phi_{p-1}(x) = (x^{p-1} - 1) \cdot \prod_{1 \neq d \mid p-1} \left(x^{\frac{p-1}{d}} - 1 \right)^{\mu(d)} .$$

Nach Satz 2.7 (ii) ist dies ein Polynom mit ganzzahligen Koeffizienten. Betrachtet man es modulo p, so ist jede Zahl von $1, 2, \ldots, p-1$ nach Fermat eine Nullstelle des isolierten Faktors.

Eine primitive Wurzel δ modulo p ist für alle anderen Faktoren stets keine Nullstelle:

$$\forall \, 1 \neq d \, | \, p-1 : \quad \delta^{\frac{p-1}{d}} \not\equiv 1 \mod p .$$

Mit $\mathbb{Z}_p[x]$ liegt ein Integritätsbereich vor. Stellt man sich den Faktor $(x^{p-1} - 1)$ in Linearfaktoren zerlegt vor, so können diejenigen, deren Nullstelle die primitiven Wurzeln modulo p sind, nicht durch das anschließende Produkt herausgekürzt werden. Damit bleiben die nach Satz 2.8 $\varphi(\varphi(p)) = \varphi(p-1)$ primitiven Wurzeln modulo p als Nullstellen modulo p von $\Phi_{p-1}(x)$ erhalten.

Nach Satz 2.7 (i) ist aber $\operatorname{Grad} \Phi_{p-1}(x) = \varphi(p-1)$, sodaß es mit Satz 2.11 höchstens $\varphi(p-1)$ modulo p inkongruente Nullstellen geben kann. Damit kann die Kongruenz $\Phi_{p-1}(x) \equiv 0 \mod p$ außer den primitiven Wurzeln modulo p keine weiteren Lösungen besitzen.

3 Die Galoisgruppen

Aufbauend auf den Grundlagen lassen sich nun die noch offenen Fragen aus Kapitel 2.1 beantworten und die Galoisgruppen der Polynome (1.1) bestimmen.

Eine Gruppe ist bis auf Isomorphie festgelegt durch Angabe einer Basis und der Verknüpfungen der Basiselemente miteinander. Ziel wird es sein, die Gruppen konkret anzugeben, das heißt ihre Elemente aufzuzählen, daraus eine Basis und die Verknüpfung ihrer Elemente abzuleiten, um so ihre Strukturen zu entschlüsseln. Einen ersten Einblick hierin gestatten bereits die Nullstellen (2.1) von $f(x)$. Unter Verwendung von Satz 2.5 gibt es ein α bzw. β, daß durch Radikale darstellbar ist. Aus Sicht der Galoistheorie bedeutet dies, daß die Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ auflösbar ist. (vgl. [2] S. 186f.)

Zunächst soll nun eine Antwort auf die zweite Frage aus Kapitel 2.1 gefunden werden.

3.1 Möglicher Grad des Zerfällungskörpers

Anhand der Nullstellen (2.4) ist ersichtlich, daß sich der Zerfällungskörper Z_f durch Adjunktion zweier Nullstellen α und β, sowie, falls eine der beiden von Null verschieden ist, einer zusätzlichen primitiven p-ten Einheiswurzel ζ erzeugen läßt:

$$Z_f = \mathbb{Q}[\sqrt{d}, \zeta, \alpha, \beta]\,.$$

Verschwinden sowohl α als auch β, so ist Null eine $(2p)$-fache Nullstelle von $f(x)$, das dann die Koeffizienten $a=b=0$ besitzt und bereits in $\mathbb{Q}$ vollständig zerfällt:

$$[Z_f : \mathbb{Q}] = 1\,.$$

Andernfalls ist die Adjunktion einer primitiven p-ten Einheitswurzel ζ stets notwendig. Diese ist nach (2.3) nicht rational und ergibt mit Satz 2.7 (i) den Grad

$$[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1\,.$$

Daraus ist ersichtlich, daß die Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ dann und nur dann die Einheitsgruppe ist, wenn $a = b = 0$. Diese triviale Gruppe erfordert keine weitere Untersuchung und wird daher aus der Analyse des folgenden Kapitels ausgeklammert.

Ansonsten läßt sich der Grad $[Z_f : \mathbb{Q}]$ des Zerfällungskörpers über $\mathbb{Q}$ schrittweise ermitteln: Mit den Bezeichnungen aus (2.1) wurde in Kapitel 2.1 bereits festgestellt, daß das Polynom $f(x)$ über $\mathbb{Q}[\sqrt{d}]$ zerfällt:

$$f(x) = (x^p - \alpha^p)(x^p - \beta^p) \in \mathbb{Q}[\sqrt{d}][x]\,.$$

Der Grad $[\mathbb{Q}[\sqrt{d},\zeta] : \mathbb{Q}[\zeta]]$ ist nach Satz 2.6 abhängig von der Irreduzibilität des Polynoms $x^2 - d$ in $\mathbb{Q}[\zeta][x]$. Mit Satz 2.5 bedeutet dies

$$[\mathbb{Q}[\sqrt{d},\zeta] : \mathbb{Q}[\zeta]] = \begin{cases} 1 & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \\ 2 & \text{falls } \sqrt{d} \notin \mathbb{Q}[\zeta]\,. \end{cases}$$

Über $\mathbb{Q}[\sqrt{d},\zeta]$ ist das Polynom $x^p - \alpha^p$ bzw. $x^p - \beta^p$ nach Satz 2.6 entweder irreduzibel oder zerfällt vollständig in Linearfaktoren. Sollte der erste Fall eintreten, so läßt sich der zweite durch Adjunktion einer Nullstelle α bzw. β realisieren. Dies bedeutet jeweils eine Körpererweiterung vom Grad p:

$$[Z_f : \mathbb{Q}[\sqrt{d},\zeta]] = \begin{cases} p^2 & \alpha \notin \mathbb{Q}[\sqrt{d},\zeta] \wedge \beta \notin \mathbb{Q}[\sqrt{d},\zeta,\alpha] \\ 1 & \alpha \in \mathbb{Q}[\sqrt{d},\zeta] \wedge \beta \in \mathbb{Q}[\sqrt{d},\zeta] \\ p & \text{sonst}\,. \end{cases}$$

Zusammenfassend ergibt sich mit Hilfe der Gradformel:

$$[Z_f : \mathbb{Q}] = [Z_f : \mathbb{Q}[\sqrt{d},\zeta]] \cdot [\mathbb{Q}[\sqrt{d},\zeta] : \mathbb{Q}[\zeta]] \cdot [\mathbb{Q}[\zeta] : \mathbb{Q}]\,.$$

und damit insgesamt:

$$[Z_f : \mathbb{Q}] \in \{1,\ p-1,\ 2(p-1),\ p(p-1),\ 2p(p-1),\ p^2(p-1),\ 2p^2(p-1)\}\,.$$

Hierdurch werden lediglich die möglichen Grade aufgezeigt. Es ist noch nicht gesichert, ob derartige Zerfällungskörper als solche überhaupt auftreten. Diese Frage wird teilweise beim Auffinden der Galoisgruppen mitbeantwortet, vollständig gesichert wird die Existenz in Kapitel 5.

Damit die Automorphismen der Galoisgruppe konkret berechnet werden können, muß eine Zerlegung von $f(x)$ in irreduzible Faktoren und damit konjugierte Elemente bekannt sein. Als Leitfaden hierzu wird die Unterscheidung von $\sqrt{d}$ in drei Fallebenen dienen:

$$\sqrt{d} \begin{cases} \in \mathbb{Q} & \text{Ebene 1} \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} & \text{Ebene 2} \\ \notin \mathbb{Q}[\zeta] & \text{Ebene 3}\,. \end{cases}$$

Die Untersuchung dieser Fälle kann als spiralförmig bezeichnet werden, da gewisse Rechentechniken und –methoden auf den einzelnen Ebenen in ähnlicher Form zurückkehren.

Es wird zunächst $\mathbb{Q}[\sqrt{d},\zeta]$ konstruiert, um Satz 2.6 anwenden zu können. Auf dieser Grundlage läßt sich dann die dritte Frage aus Kapitel 2.1 nach den unterschiedlichen Zerfällungsmöglichkeiten von $f(x)$ beantworten und die Galoisgruppe bestimmen.

3.2 Galoisgruppen der Ebene 1

Ist $\sqrt{d} \in \mathbb{Q}$, so zerfällt $f(x)$ bereits in $\mathbb{Q}[x]$ zu

$$f(x) = (x^p - \alpha^p)(x^p - \beta^p)\,.$$

Wie bereits erwähnt ist eine primitive p-te Einheitswurzel ζ über $\mathbb{Q}$ nicht rational und erzeugt bei Adjunktion eine Körpererweiterung $\mathbb{Q}[\zeta]$ vom Grad $p-1$ über $\mathbb{Q}$.

Fall 1:
Sind bereits Nullstellen α und β in $\mathbb{Q}[\zeta]$ enthalten, so zerfällt $f(x)$ nach Satz 2.6 hierüber bereits vollständig in Linearfaktoren. Dies ist zum Beispiel der Fall für das Polynom

$$x^{2p}+2x^p+1 = (x^p+1)(x^p+1) = (x+1)^2(x+\zeta)^2\ldots(x+\zeta^{p-1})^2 \in \mathbb{Q}[\zeta]$$

mit $\alpha = \beta = \sqrt[p]{-1}$.

Damit stellt bereits $\mathbb{Q}[\zeta]$ den Zerfällungskörper dar. Die Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ ist nach Satz 2.10 zyklisch und gegeben durch

$$G(Z_f\,|\,\mathbb{Q}) = G(Z_{\Phi_p}\,|\,\mathbb{Q}) \cong \mathbb{Z}_p^*\,.$$

Diese hat die Ordnung $p-1$ und besitzt nach Satz 2.9 (iv) zu jedem Teiler d von $p-1$ genau $\varphi(d)$ Elemente der Ordnung d.

Fall 2:
Eine zweite Möglichkeit besteht darin, daß mindestens eines der Polynome $x^p-\alpha^p$ und $x^p-\beta^p$ in $\mathbb{Q}[\zeta]$ irreduzibel ist, und die Adjunktion einer Nullstelle $\gamma \in \{\alpha,\beta\}$ bereits zum Zerfällungskörper führt. Beispiele dafür sind die Polynome

$$\begin{aligned} x^{2p} - x^p - 2 &= (x^p+1)(x^p-2) \\ &= (x+1)(x+\zeta)\ldots(x+\zeta^{p-1})(x^p-2) \\ x^{2p} + 2x^p - 8 &= (x^p-2)(x^p+4)\,, \end{aligned}$$

deren Zerfällungskörper durch $Z_f = \mathbb{Q}[\zeta, \sqrt[p]{2}]$ gegeben ist.

Der Grad eines solchen Zerfällungskörpers über $\mathbb{Q}$ und damit die Ordnung der Galoisgruppe beträgt

$$[Z_f : \mathbb{Q}] = \mid G(Z_f\,|\,\mathbb{Q}) \mid = p\,(p-1)\,.$$

Es gibt also $p\,(p-1)$ verschiedene Automorphismen σ, die den Grundkörper $\mathbb{Q}$ elementweise festlassen. Diese sind festgelegt durch ihre Bilder $\sigma(\zeta)$ und $\sigma(\gamma)$. Die Konjugierten von ζ sind die primitiven p-ten Einheitswurzeln über $\mathbb{Q}$. Die Konjugierten von γ sind die Nullstellen des nach Voraussetzung irreduziblen Polynoms $x^p - \gamma^p \in \mathbb{Q}[\zeta][x]$.

Mit Satz 2.3 ist damit ein möglicher Automorphismus $\sigma \in G(Z_f \mid \mathbb{Q})$ festgelegt durch

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1, \ldots, p-1\} \\ \gamma \mapsto \zeta^{\mu}\gamma & \mu \in \{0, \ldots, p-1\}\,. \end{cases} \tag{3.1}$$

Dies sind aber genau $p\,(p-1)$ paarweise verschiedene Automorphismen, und damit bildet ihre Gesamtheit mit der Verknüpfung "$\circ$" die gesuchte Galoisgruppe.

Welche Ordnungen besitzen die einzelnen Elemente? Betrachtet man einen beliebigen Automorphismus σ der Form (3.1), so sind seine Potenzen gekennzeichnet durch

$$\begin{aligned} \sigma : &\quad \begin{cases} \zeta \mapsto \zeta^{\nu} \\ \gamma \mapsto \zeta^{\mu}\gamma \end{cases} \\ \sigma^2 : &\quad \begin{cases} \zeta \mapsto \zeta^{(\nu^2)} \\ \gamma \mapsto \zeta^{\mu\nu+\mu}\gamma = \zeta^{\mu(\nu+1)}\gamma \end{cases} \\ &\quad \vdots \\ \sigma^n : &\quad \begin{cases} \zeta \mapsto \zeta^{(\nu^n)} \\ \gamma \mapsto \zeta^{\mu(\nu^{n-1}+\nu^{n-2}+\ldots+\nu+1)}\gamma\,. \end{cases} \end{aligned}$$

Es stellt sich die Frage, welche Potenz σ^n die Identität ergibt. Es muß gelten:

$$\nu^n \equiv 1 \mod p \quad \wedge \quad \mu(\nu^{n-1} + \nu^{n-2} + \ldots + \nu + 1) \equiv 0 \mod p\,.$$

Dann ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma$ das kleinste $n > 0$, das diese Kongruenzen erfüllt.

Für den Fall $\nu \neq 1$ impliziert die erste Bedingung die zweite:

$$\nu^n \equiv 1 \bmod p \implies \nu^{n-1}+\nu^{n-2}+\ldots+\nu+1 = \frac{\nu^n - 1}{\nu - 1} \equiv \frac{1-1}{\nu-1} \equiv 0 \bmod p.$$

Damit ist die Ordnung n unabhängig von μ und wird allein durch ν bestimmt: $n = \mathrm{Ord}_{\mathbb{Z}_p^*}\nu$.

Zu jedem ν existieren genau p verschiedene Automorphismen in $G(Z_f \mid \mathbb{Q})$. Nach Satz 2.10 ist $\mathbb{Z}_p^*$ zyklisch, sodaß mit Satz 2.9 (iv) geschlossen werden kann, daß es in $G(Z_f \mid \mathbb{Q})$ zu jedem $d \mid p-1$ mindestens $p \cdot \varphi(d)$ Elemente der Ordnung d gibt. Der Fall $d = 1$ ist hiervon ausgenommen, da $\nu \neq 1$ vorausgesetzt ist.

Ist $\nu = 1$, so ist

$$\mu(\nu^{n-1} + \nu^{n-2} + \ldots + \nu + 1) = \mu \cdot n \equiv 0 \mod p\,,$$

also

$$\mu \equiv 0 \mod p \quad \vee \quad n \equiv 0 \mod p\,.$$

Im ersten Fall ist der Automorphismus die Identität und besitzt damit die Ordnung $n = 1$. Für $\mu \neq 0$ ergibt sich im zweiten Fall die Ordnung

als kleinstes $n > 0$, das die Kongruenz $n \equiv 0 \bmod p$ erfüllt, also $n = p$. Automorphismen dieser Ordnung gibt es $p - 1$ verschiedene.

Insgesamt besitzt $G(Z_f \,|\, \mathbb{Q})$ im betrachteten Fall Elemente folgender Ordnung:

$$\begin{array}{rrll} & 1 & \text{Element der Ordnung} & 1 \\ \forall\, 1 \neq d \,|\, p-1 : & p \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ & p-1 & \text{Elemente der Ordnung} & p\,. \end{array}$$

Hieraus folgt zunächst, daß die Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ nicht zyklisch sein kann. Zu ihrer Erzeugung sind daher mindestens zwei Elemente erforderlich. Eine Basis ist bereits gegeben durch $\sigma, \tau \in G(Z_f \,|\, \mathbb{Q})$ mit

$$\begin{aligned} \sigma : & \begin{cases} \zeta \mapsto \zeta \\ \gamma \mapsto \zeta\gamma \end{cases} , \quad \mathrm{Ord}_{G(Z_f|\mathbb{Q})}\sigma = p \\ \tau : & \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \gamma \mapsto \gamma \end{cases} , \quad \mathrm{Ord}_{G(Z_f|\mathbb{Q})}\tau = p-1\,, \end{aligned}$$

wobei δ eine primitive Wurzel modulo p ist. Dann ist jeder Automorphismus ϕ der Form (3.1) darstellbar durch

$$\phi = \sigma^{\mu} \circ \tau^{\overline{\nu}}\,.$$

Dabei ist $\overline{\nu}$ eine Lösung der Kongruenz

$$\delta^{\overline{\nu}} \equiv \nu \mod p\,.$$

Diese existiert immer, da δ eine primitive Wurzel modulo p ist und ihre Potenzen sämtliche Zahlen $0, 1, \ldots, p-1$ ausschöpfen. Primitive Wurzeln modulo p und Lösungen obiger Kongruenz werden im Verlaufe der Untersuchung desöfteren auftauchen. Von daher seien im folgenden mit δ und $\overline{\nu}$ stets derartige Werte bezeichnet.

Die Verknüpfung obiger Basiselemente ist gegeben durch

$$\sigma \circ \tau = \tau \circ \sigma^{\delta^{-1}} : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \gamma \mapsto \zeta\gamma \end{cases}$$

mit dem multiplikativen Inversen $\delta^{-1} \in \mathbb{Z}_p^*$. Dieses ist ebenfalls eine primitive Wurzel modulo p, denn es gilt

$$(\delta^{-1})^n \equiv \delta^{-n} \equiv 1 \mod p \quad \Longleftrightarrow \quad 1 \equiv \delta^n \mod p \qquad (3.2)$$

und damit $\mathrm{Ord}_{\mathbb{Z}_p^*}\delta^{-1} = \mathrm{Ord}_{\mathbb{Z}_p^*}\delta = p - 1$.

So läßt sich die Gruppe nun allgemein mit einer beliebigen primitiven Wurzel δ modulo p charakterisieren durch

$$\Lambda_p := \langle \sigma, \tau \rangle; \quad |\,\Lambda_p\,| = p\,(p-1)$$
$$\mathrm{Ord}_{\Lambda_p}\sigma = p\,; \quad \mathrm{Ord}_{\Lambda_p}\tau = p-1; \quad \sigma \circ \tau = \tau \circ \sigma^{\delta}\,.$$

Λ_p ist nach den Voraussetzungen stets die Galoisgruppe eines irreduziblen Polynoms $x^p - c \in \mathbb{Q}[x]$. Sie wird sich in bezug auf die Polynome (1.1) als wichtiges Grundelement weiterer Galoisgruppen erweisen.

Fall 3:
Als letzter Fall ist schließlich derjenige zu betrachten, bei dem sowohl $x^p - \alpha^p$ als auch $x^p - \beta^p$ über $\mathbb{Q}[\zeta]$ irreduzibel sind und die Adjunktion einer Nullstelle noch nicht den Zerfällungskörper Z_f liefert. Dieser wird erst durch sukzessive Erweiterung von $\mathbb{Q}[\zeta]$ mit α und β jeweils vom Grad p konstruiert:

$$Z_f = \mathbb{Q}[\zeta, \alpha, \beta] \,.$$

Als Beispiel hierfür sei das Polynom

$$x^{2p} - 5x^p + 6 = (x^p - 2)(x^p - 3)$$

mit $Z_f = \mathbb{Q}[\zeta, \sqrt[p]{2}, \sqrt[p]{3}]$ genannt.

Der Grad eines solchen Zerfällungskörpers über $\mathbb{Q}$ und damit die Anzahl der Automorphismen der Galoisgruppe beträgt

$$[Z_f : \mathbb{Q}] = \mid G(Z_f \,|\, \mathbb{Q}) \mid = p^2(p-1) \,.$$

Aufbauend auf den Ergebnissen des vorherigen Falles läßt sich ein Automorphismus σ der Form (3.1) auf Z_f fortsetzen und ist dann von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1, 2, \ldots, p-1\} \\ \alpha \mapsto \zeta^{\mu}\alpha & \mu \in \{0, 1, \ldots, p-1\} \\ \beta \mapsto \zeta^{\kappa}\beta & \kappa \in \{0, 1, \ldots, p-1\} \,. \end{cases} \tag{3.3}$$

Die so beschriebenen $p^2(p-1)$ verschiedenen Automorphismen bilden mit der Verknüpfung "$\circ$" die Galoisgruppe. Ihre Ordnungen lassen sich völlig analog zum Fall 2 bestimmen, worin lediglich zu berücksichtigen ist, daß zu jedem ν genau p^2 verschiedene Automorphismen existieren. Damit besitzt $G(Z_f \,|\, \mathbb{Q})$ im betrachteten Fall Elemente folgender Ordnung:

$$\begin{array}{rrll} & 1 & \text{Element der Ordnung} & 1 \\ \forall\ 1 \neq d \,|\, p-1 : & p^2 \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ & p^2 - 1 & \text{Elemente der Ordnung} & p \,. \end{array}$$

Ein Erzeugendensystem der Gruppe ist gegeben durch die Elemente $\sigma_1, \sigma_2, \tau \in G(Z_f \,|\, \mathbb{Q})$ mit

$$\sigma_1 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \\ \beta \mapsto \beta \end{cases} \quad ; \quad \sigma_2 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \alpha \\ \beta \mapsto \zeta\beta \end{cases} \quad ; \quad \tau : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \alpha \mapsto \alpha \\ \beta \mapsto \beta \end{cases} \,.$$

Jeder Automorphismus ϕ der Form (3.3) läßt sich dann darstellen als

$$\phi = \sigma_1^{\mu} \circ \sigma_2^{\kappa} \circ \tau^{\overline{\nu}} .$$

Es liegt sogar eine Basis vor, denn entfernt man σ_1 oder σ_2, so bleibt eine Basis der Λ_p zurück, die somit als echte Untergruppe auftritt. Auch τ läßt sich nicht durch σ_1 und σ_2 erzeugen:

$$\forall\, \nu, \mu \in \mathbb{N} :\ \tau \neq \sigma_1^{\nu} \circ \sigma_2^{\mu} = \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta^{\nu} \alpha \\ \beta \mapsto \zeta^{\mu} \beta \, . \end{cases}$$

Die Verknüpfung der Basiselemente ist analog zur Λ_p gegeben durch

$$\begin{aligned} \sigma_{1,2} \circ \tau &= \tau \circ \sigma_{1,2}^{\delta^{-1}} \\ \sigma_1 \circ \sigma_2 &= \sigma_2 \circ \sigma_1 \, , \end{aligned}$$

Somit läßt sich mit Blick auf (3.2) die Galoisgruppe mit Hilfe einer beliebigen primitiven Wurzel δ modulo p allgemein charakterisieren als

$$\begin{gathered} \Lambda_{p^2} := \langle \sigma_1, \sigma_2, \tau \rangle ; \quad |\, \Lambda_{p^2} \,| = p^2(p-1) \\ \mathrm{Ord}_{\Lambda_{p^2}} \sigma_1 = \mathrm{Ord}_{\Lambda_{p^2}} \sigma_2 = p \, ; \quad \mathrm{Ord}_{\Lambda_p} \tau = p - 1 ; \\ \sigma_{1,2} \circ \tau = \tau \circ \sigma_{1,2}^{\delta}, \quad \sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1 \, . \end{gathered}$$

Es sind nun für den Fall $\sqrt{d} \in \mathbb{Q}$ sämtliche Zerfällungsmöglichkeiten von $f(x)$ untersucht. Damit ist in der Ebene 1 stets eine der Gruppen

$$\mathbb{Z}_p^*, \quad \Lambda_p, \quad \Lambda_{p^2}$$

isomorph zur Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$.

3.3 Galoisgruppen der Ebene 2

Zunächst steht die Frage im Raum, welcher Gestalt $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$ sein muß. Für die betrachtete Wurzel muß gelten:

$$\mathbb{Q} \subset |\, \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q}[\zeta]$$

und damit

$$[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2 \, .$$

Nach Satz 2.10 ist die Galoisgruppe $G(\mathbb{Q}[\zeta] \,|\, \mathbb{Q})$ zyklisch. Sie besitzt die Ordnung $p-1$ und nach Satz 2.9 (iii) zu jedem Teiler d von $p-1$ genau eine zyklische Untergruppe der Ordnung d.

Aus der Galoistheorie erhält man damit für $d = \frac{p-1}{2}$ einen eindeutigen Zwischenkörper vom Grad 2 über $\mathbb{Q}$.

Satz 3.1 *Für jede ungerade Primzahl p ist der eindeutige quadratische Teilkörper von $\mathbb{Q}[\zeta]$ gegeben durch*

$$\mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right] .$$

Beweis: Mit $n := \frac{p-1}{2} \in \mathbb{N}$ läßt sich folgende Hilfsgröße konstruieren:

$$\Delta := \zeta^{-\frac{n(n+1)}{2}} \cdot \prod_{j=1}^{n}(1-\zeta^{2j}) \ \in \mathbb{Q}[\zeta] .$$

Für das Quadrat gilt

$$\begin{aligned}
\Delta^2 &= \zeta^{-n(n+1)} \cdot \textstyle\prod_{j=1}^{n}(1-\zeta^{2j})(1-\zeta^{2j}) \\
&= \zeta^{-n(n+1)} \cdot \textstyle\prod_{j=1}^{n}(1-\zeta^{2j}) \cdot (-\zeta^{2j}) \cdot (-\zeta^{p-2j}+1) \\
&= (-1)^n \cdot \textstyle\prod_{j=1}^{n}(1-\zeta^{2j})(1-\zeta^{p-2j}) \\
&= (-1)^n \cdot \textstyle\prod_{j=1}^{p-1}(1-\zeta^{j}) \\
&= (-1)^n \cdot \Phi_p(1) .
\end{aligned}$$

Mit Satz 2.13 gilt

$$\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+1 \quad \Longrightarrow \quad \Phi_p(1) = p .$$

Somit ergibt sich

$$\Delta^2 = (-1)^n p \ \in \mathbb{Q} \quad \Longrightarrow \quad \Delta = \pm\sqrt{(-1)^n p} \ \notin \mathbb{Q} ,$$

also

$$\mathrm{Irr}(\Delta, \mathbb{Q}) = x^2 - \Delta^2 \in \mathbb{Q}[x] .$$

Damit folgt insgesamt, daß

$$\mathbb{Q}[\Delta] = \mathbb{Q}[\sqrt{(-1)^{\frac{p-1}{2}}p}] \subseteq| \ \mathbb{Q}[\zeta]$$

mit

$$[\mathbb{Q}[\sqrt{(-1)^{\frac{p-1}{2}}p}] : \mathbb{Q}] = 2$$

der gesuchte Teilkörper ist.

Mit Hilfe dieses Satzes gilt unter Verwendung von $p^* = (-1)^{\frac{p-1}{2}}p$:

$$\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{p^*}] .$$

Daraus folgt mit $c_0, c_1 \in \mathbb{Q}$:

$$\sqrt{d} = c_1\sqrt{p^*} + c_0 \ ,$$

also

$$d = c_1^2 p^* + 2c_1 c_0 \sqrt{p^*} + c_0^2 \in \mathbb{Q}\,.$$

Dies bedeutet aber, daß der Wurzelterm des Ausdrucks verschwinden muß, also

$$c_0 = 0 \quad \vee \quad c_1 = 0\,.$$

Für den Fall $c_1 = 0$ wäre aber $\sqrt{d} \in \mathbb{Q}$, was gegen die Voraussetzung spricht. Damit gilt $c_0 = 0$ und insgesamt

$$\sqrt{d} \in \mathbb{Q}[\zeta] \quad \Longleftrightarrow \quad \exists\, c_0 \in \mathbb{Q} \,:\, d = \frac{a^2}{4} - b = c_0^2 p^*\,. \tag{3.4}$$

Die Koeffizienten der auf dieser Ebene betrachteten Polynome $f(x)$ sind damit abhängig von der Primzahl p — allgemeine Beispiele für die im folgenden betrachteten Zerfällungsmöglichkeiten lassen sich damit nicht wie im vorherigen Kapitel angeben.

Die Existenz derartiger Polynome soll aus diesem Grund nicht anhand von Beispielen gesichert werden. Vielmehr sei diesbezüglich auf Kapitel 5 verwiesen, in dem die Konstruktion derartiger Polynome beschrieben wird.

Welche Zerfällungskörper können nun auftreten und welche Galoisgruppen lassen sich daraus ableiten? Unter der gegebenen Voraussetzung $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$ zerfällt $f(x)$ in $\mathbb{Q}[\zeta]$ zu

$$f(x) = (x^p - \alpha^p)(x^p - \beta^p)\,.$$

Somit ist eine analoge Voraussetzung zur Analyse der Ebene 1 geschaffen. Es bietet sich daher eine sich daran anlehnende Untersuchung der Galoisgruppen an.

Fall 1:
Zerfällt $f(x)$ bereits in $\mathbb{Q}[\zeta]$ vollständig in Linearfaktoren, so ist dies mit den Sätzen 2.6 und 2.5 gleichwertig dazu, daß, sowohl α als auch β in $\mathbb{Q}[\zeta]$ enthalten sind. Die Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ ist dann nach Satz 2.10 gegeben durch

$$G(Z_f \,|\, \mathbb{Q}) = G(Z_{\Phi_p} \,|\, \mathbb{Q}) \cong \mathbb{Z}_p^*\,.$$

Fall 2:
Als nächstes sei angenommen, daß mindestens eine der Nullstellen α und β nicht in $\mathbb{Q}[\zeta]$ enthalten ist, aber die Adjunktion eines $\gamma \in \{\alpha, \beta\}$ bereits zum Zerfällungskörper führt.

Der Grad einer solchen Körpererweiterung und damit die Ordnung der Galoisgruppe beträgt

$$[Z_f : \mathbb{Q}] = \mid G(Z_f \,|\, \mathbb{Q}) \mid = p\,(p-1)\,.$$

Damit gibt es $p\,(p-1)$ verschiedene Automorphismen σ, die den Grundkörper $\mathbb{Q}$ punktweise festlassen. Diese sind eindeutig festgelegt durch ihre Bilder $\sigma(\zeta)$ und $\sigma(\gamma)$. Wie aber sehen die Konjugierten von γ über $\mathbb{Q}$ aus? Anders gefragt: Was ist $\mathrm{Irr}(\gamma, \mathbb{Q})$? Mit der Gradformel gilt zunächst

$$\begin{aligned} & [\mathbb{Q}[\zeta] : \mathbb{Q}] && = [\mathbb{Q}[\zeta] : \mathbb{Q}[\sqrt{d}]] \cdot [\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] \\ \Longrightarrow \quad & p-1 && = [\mathbb{Q}[\zeta] : \mathbb{Q}[\sqrt{d}]] \cdot 2 \\ \Longrightarrow \quad & [\mathbb{Q}[\zeta] : \mathbb{Q}[\sqrt{d}]] && = \frac{p-1}{2} \\ \Longrightarrow \quad & [\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}[\gamma]] && \leq \frac{p-1}{2}, \quad \text{da } \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{Q}[\gamma]\,. \end{aligned}$$

Damit folgt aber erneut mit Hilfe der Gradformel

$$\underbrace{[\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}]}_{=p\,(p-1)} = \underbrace{[\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}[\gamma]]}_{\leq \frac{p-1}{2}} \cdot [\mathbb{Q}[\gamma] : \mathbb{Q}]$$

und somit

$$[\mathbb{Q}[\gamma] : \mathbb{Q}] \geq 2p\,.$$

Damit besitzt $\mathrm{Irr}(\gamma, \mathbb{Q})$ mindestens den Grad $2p$. Nun ist aber γ eine Nullstelle des Polynoms $f(x) \in \mathbb{Q}[x]$ vom Grad $2p$. Also gilt:

$$f(x) = \mathrm{Irr}(\gamma, \mathbb{Q})\,.$$

Allgemeiner ist für die Ebene 2 sogar gezeigt: Falls $f(x)$ über $\mathbb{Q}[\zeta]$ nicht vollständig in Linearfaktoren zerfällt, so ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$.

Damit sind die Konjugierten von γ gegeben durch (2.4), also sämtliche Nullstellen von $f(x)$. Der Zerfällungskörper Z_f läßt sich nun charakterisieren als

$$Z_f = \mathbb{Q}[\zeta, \gamma] = \mathbb{Q}[\zeta, \alpha] = \mathbb{Q}[\zeta, \beta]\,.$$

Ein Automorphismus σ der Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ ist damit von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1, 2, \ldots, p-1\} \\ \alpha \mapsto \zeta^{\mu}\gamma & \mu \in \{0, 1, \ldots, p-1\}\,,\ \gamma \in \{\alpha, \beta\}\,. \end{cases} \tag{3.5}$$

Dies sind aber insgesamt $2p\,(p-1)$ Möglichkeiten. Da es aber nur $p\,(p-1)$ verschiedene Automorphismen gibt, stellt sich die Frage, wie diese herauszufiltern sind. Alsdann wäre zu klären, wie die Potenzen σ^n aussehen, um die Ordnung $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma$ berechnen zu können. All diese Probleme lassen sich relativ übersichtlich lösen, wenn man eine weitere Fallunterscheidung vornimmt. Es gilt

$$\alpha^p \cdot \beta^p = b \quad \text{und damit} \quad \sqrt[p]{b} = \alpha \cdot \beta \in Z_f\,.$$

Nun gibt es zwei Möglichkeiten: Entweder liegt eine p-te Wurzel aus b bereits in $\mathbb{Q}$, oder nicht. Mit Satz 2.5 formuliert bedeutet dies: Entweder ist $x^p - b \in \mathbb{Q}[x]$ reduzibel oder nicht.

Nimmt man den zweiten Fall an, so ist $Z_{x^p-b} \subseteq| \; Z_f$, da $\zeta, \sqrt[p]{b} \in Z_f$. Damit ist nach der Galoistheorie $G(Z_{x^p-b} \,|\, \mathbb{Q})$ eine Untergruppe von $G(Z_f \,|\, \mathbb{Q})$. In Kapitel 3.2 wurde bereits gezeigt, daß die Galoisgruppe eines irreduziblen Polynoms $x^p - c \in \mathbb{Q}[x]$ stets isomorph ist zur Λ_p, also ist

$$G(Z_{x^p-b} \,|\, \mathbb{Q}) \cong \Lambda_p \,.$$

Da aber

$$\mathrm{Ord}\, G(Z_f \,|\, \mathbb{Q}) = p\,(p-1) = \mathrm{Ord}\Lambda_p \,,$$

folgt ingesamt

$$G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_p \,.$$

Der erste Fall erfordert eine genauere Untersuchung. Der Schlüssel zur Frage, wie sich aus den durch (3.5) beschriebenen Möglichkeiten die $p\,(p-1)$ Automorphismen $\sigma \in G(Z_f \,|\, \mathbb{Q})$ herausfiltern lassen, ist das Bild $\sigma(\sqrt{d})$, denn $\sigma(\alpha)$ und $\sigma(\zeta)$ sind überdies miteinander verknüpft. Es gilt zum einen

$$\sigma(\sqrt{d}) = \sigma(\alpha^p + \frac{a}{2}) = (\sigma(\alpha))^p + \frac{a}{2} = \begin{cases} \alpha^p + \frac{a}{2} = \sqrt{d} \\ \beta^p + \frac{a}{2} = -\sqrt{d} \end{cases}$$

und damit

$$\sigma(\sqrt{d}) = \begin{cases} \sqrt{d}\,, & \text{falls } \sigma(\alpha) = \zeta^\mu \alpha \\ -\sqrt{d}\,, & \text{falls } \sigma(\alpha) = \zeta^\mu \beta \,. \end{cases} \tag{3.6}$$

Desweiteren folgt aus der Galoistheorie, daß $G(\mathbb{Q}[\zeta] \,|\, \mathbb{Q}[\sqrt{d}])$ eine Untergruppe der zyklischen Gruppe $G(\mathbb{Q}[\zeta] \,|\, \mathbb{Q})$ ist. Sie ist nach Satz 2.9 ebenfalls zyklisch und besitzt die Ordnung

$$\mathrm{Ord}\; G(\mathbb{Q}[\zeta] \,|\, \mathbb{Q}[\sqrt{d}]) = \frac{[\mathbb{Q}[\zeta] : \mathbb{Q}]}{[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}]} = \frac{p-1}{2} \,.$$

Es gibt also $\frac{p-1}{2}$ verschiedene Automorphismen τ auf $\mathbb{Q}[\zeta]$, die den Teilkörper $\mathbb{Q}[\sqrt{d}]$ elementweise fest lassen. Mit dem soeben Gezeigten und Satz 2.9 (iv) sind dies aber alle $\tau \in G(\mathbb{Q}[\zeta] \,|\, \mathbb{Q})$, deren Ordnung ein Teiler von $\frac{p-1}{2}$ ist. Hierzu gilt mit der in Kapitel 2.3 betrachteten Isomorphie:

$$\tau(\zeta) = \zeta^\nu \,,\; \nu \in \{1, 2, \ldots, p-1\} \quad \Longleftrightarrow \quad \mathrm{Ord}_{G(\mathbb{Q}[\zeta]|\mathbb{Q})}\, \tau = \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \,.$$

Daraus folgt insgesamt:

$$\tau(\sqrt{d}) = \sqrt{d} \quad \Longleftrightarrow \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \mid \frac{p-1}{2} \,.$$

Dieses Konzept läßt sich auf die Automorphismen σ übertragen, da $\mathbb{Q}[\zeta]$ ein Teilkörper von Z_f ist. Es folgt dann

$$\sigma(\sqrt{d}) = \sqrt{d} \quad \Longleftrightarrow \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \mid \frac{p-1}{2}\,.$$

Damit läßt sich nun insgesamt die Verbindung von $\sigma(\alpha)$ über $\sigma(\sqrt{d})$ aufschlüsseln, wenn σ in der Form (3.5) angenommen wird:

$$\sigma(\sqrt{d}) = \left\{ \begin{array}{rcl} \sqrt{d} & \Longleftrightarrow & \sigma(\alpha) = \zeta^\mu \alpha \quad \wedge \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \mid \frac{p-1}{2} \\ -\sqrt{d} & \Longleftrightarrow & \sigma(\alpha) = \zeta^\mu \beta \quad \wedge \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \not\mid \frac{p-1}{2}\,. \end{array} \right.$$

Mit den Kombinationsmöglichkeiten von μ und ν sind somit insgesamt $2 \cdot p \cdot \frac{p-1}{2} = p\,(p-1)$ verschiedene, also alle Automorphismen der gesuchten Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ erfaßt.

Um die Potenzen von σ berechnen zu können, ist noch die Voraussetzung auszunutzen, daß eine rationale p-te Wurzel aus b existiert. Es gibt dann mit Blick auf (2.4) gewisse Nullstellen α und β mit

$$\alpha \cdot \beta = \sqrt[p]{b} =: r \in \mathbb{Q}\,, \quad \text{also} \quad \beta = \frac{r}{\alpha}\,. \tag{3.7}$$

Damit läßt sich die Gesamtheit aller Automorphismen $\sigma \in G(Z_f \,|\, \mathbb{Q})$ in der Form

$$\sigma : \left\{ \begin{array}{ll} \zeta \mapsto \zeta^\nu & \nu \in \{1, 2, \ldots, p-1\} \\ \alpha \mapsto \left\{ \begin{array}{ll} \zeta^\mu \alpha & \text{falls} \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \mid \frac{p-1}{2} \\ \zeta^\mu \frac{r}{\alpha} & \text{falls} \quad \mathrm{Ord}_{\mathbb{Z}_p^*}\, \nu \not\mid \frac{p-1}{2} \end{array} \right. & \mu \in \{0, 1, \ldots, p-1\} \end{array} \right.$$

schreiben. Daraus seien nun die Automorphismen $\sigma, \tau \in G(Z_f \,|\, \mathbb{Q})$ mit

$$\sigma : \left\{ \begin{array}{l} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \end{array} \right. \quad ; \qquad \tau : \left\{ \begin{array}{l} \zeta \mapsto \zeta^\delta \\ \alpha \mapsto \frac{r}{\alpha} \end{array} \right.$$

Gegenstand der Betrachtungen.

σ ist in dieser Form bekannt aus der Analyse der Ebene 1, Fall 2, seine Ordnung beträgt p. Für τ bildet erst die $(p-1)$-te Potenz ζ auf sich selbst ab. Gleichzeitig bleibt dann aber auch α fest, da $p-1$ gerade ist, sodaß τ die Ordnung $p-1$ besitzt.

Betrachtet man nun die Produkte $\sigma^\mu \circ \tau^\nu$ mit $\mu \in \{1, 2, \ldots, p\}$ und $\nu \in \{1, 2, \ldots, p-1\}$, so sind diese paarweise verschieden. Dies ist zum einen darin begründet, daß das Bild von ζ allein durch die Potenz τ^ν festgelegt ist. Durchläuft nämlich ν die Zahlen $1, 2, \ldots, p-1$, so taucht jedes der Bilder $\zeta, \zeta^2, \ldots \zeta^{p-1}$ genau einmal auf, da δ eine primitive Wurzel modulo p ist. Auf der anderen Seite wird allein durch μ die Potenz von ζ in $\sigma^\mu(\alpha)$ festgelegt.

Insgesamt stellen die betrachteten Produkte genau $p\,(p-1)$ paarweise verschiedene Automorphismen dar und damit die gesamte Gruppe $G(Z_f \mid \mathbb{Q})$. Somit bilden σ und τ eine Basis von $G(Z_f \mid \mathbb{Q})$. Ihre Verknüpfung ist gegeben durch

$$\sigma \circ \tau = \tau \circ \sigma^{-\delta^{-1}} : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \alpha \mapsto \frac{r}{\zeta\alpha}\,. \end{cases}$$

Interessant ist hierbei die Untersuchung von $-\delta^{-1}$, denn es gilt

$$(-\delta^{-1})^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot \delta^{-\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \mod p$$

und damit

$$(-\delta^{-1})^{\frac{p-1}{2}} \equiv \begin{cases} 1 \mod p & \text{für} \quad p \equiv -1 \mod 4 \\ -1 \mod p & \phantom{\text{für}} \quad p \equiv 1 \mod 4\,. \end{cases}$$

Im zweiten Fall ist $-\delta^{-1}$ wieder eine primitive Wurzel modulo p. Dann folgt aber erneut

$$G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_p\,.$$

Somit haben die bisher durchgeführten Betrachtungen lediglich die Erkenntnis geliefert, daß die gesuchten Galoisgruppen stets isomorph sind zur Λ_p.

Die einzige Frage, die in diesem Fall abschließend beantwortet werden muß, ist, welche Galoisgruppe vorliegt, wenn eine rationale p-te Wurzel aus b existiert und wenn $p \equiv -1 \bmod 4$ ist.

Betrachtet man Automorphismen $\sigma \in G(Z_f \,|\, \mathbb{Q})$ der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \mathrm{Ord}_{\mathbb{Z}_p^*}\nu \mid \frac{p-1}{2} \\ \alpha \mapsto \zeta^{\mu}\alpha & \mu \in \{0, 1, \ldots, p-1\}\,, \end{cases}$$

so wurde ihre Ordnung bereits in Kapitel 3.2 bestimmt: für $\nu \neq 1$ gibt es zu jedem $d \mid \frac{p-1}{2}$ mit $d \neq 1$ genau $p \cdot \varphi(d)$ Automorphismen der Ordnung d. Für $\nu = 1$ gibt es einen Automorphismus der Ordnung 1 und $p-1$ Automorphismen der Ordnung p.

Sei nun $\sigma \in G(Z_f \,|\, \mathbb{Q})$ von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \mathrm{Ord}_{\mathbb{Z}_p^*}\nu \nmid \frac{p-1}{2} \\ \alpha \mapsto \zeta^{\mu}\frac{r}{\alpha} & \mu \in \{0, 1, \ldots, p-1\}\,. \end{cases}$$

Ungerade Potenzen von σ bilden α stets reziprok ab im Sinne von $\sigma(\alpha) = \zeta^{\kappa}\frac{r}{\alpha}$. Dieses muß stets ungleich α sein, da sonst $\alpha^2 \in \mathbb{Q}[\zeta]$, was aber nicht sein kann, da dann folgt

$$\alpha = \frac{(\alpha^2)^{\frac{p+1}{2}}}{\alpha^p} \in \mathbb{Q}[\zeta]\,,$$

was nach Voraussetzung falsch ist. Somit ist die Ordnung von σ in jedem Fall gerade. Entsprechende Potenzen sind gegeben durch

$$\begin{aligned}
\sigma^2 &: \begin{cases} \zeta \mapsto \zeta^{(\nu^2)} \\ \alpha \mapsto \zeta^{\mu\nu-\mu}\alpha = \zeta^{\mu(\nu-1)}\alpha \end{cases} \\
\sigma^4 &: \begin{cases} \zeta \mapsto \zeta^{(\nu^4)} \\ \alpha \mapsto \zeta^{\nu^2\mu(\nu-1)+\mu(\nu-1)}\alpha = \zeta^{\mu(\nu^3-\nu^2+\nu-1)}\alpha \end{cases} \\
&\vdots \\
\sigma^{2n} &: \begin{cases} \zeta \mapsto \zeta^{(\nu^{2n})} \\ \alpha \mapsto \zeta^{\mu(\nu^{2n-1}-\nu^{2n-2}\pm\ldots+\nu-1)}\alpha\,. \end{cases}
\end{aligned}$$

Damit σ^{2n} die Identität ergibt, muß gelten:

$$\nu^{2n} \equiv 1 \mod p \quad \wedge \quad \mu(\nu^{2n-1} - \nu^{2n-2} \pm \ldots + \nu - 1) \equiv 0 \mod p\,.$$

Dann ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma = 2n$ mit dem kleinsten $n > 0$, das diese Kongruenzen erfüllt.

Für den Fall $\nu \neq p-1$ ergibt sich die zweite Bedingung aus der ersten, denn mit $\nu^{2n} \equiv 1 \bmod p$ folgt

$$\nu^{2n-1} - \nu^{2n-2} \pm \ldots + \nu - 1 = \frac{\nu^{2n}-1}{\nu+1} \equiv \frac{1-1}{\nu+1} \equiv 0 \mod p\,.$$

Damit ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma$ allein durch ν bestimmt. Nun muß aber die Ordnung $\mathrm{Ord}_{\mathbb{Z}_p^*}\nu$ ein gerader Teiler von $p-1$ sein, denn sonst würde sie auch $\frac{p-1}{2}$ teilen, was nach Voraussetzung nicht der Fall ist. Daraus folgt, daß $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma = \mathrm{Ord}_{\mathbb{Z}_p^*}\nu$, womit wieder geschlossen werden kann, daß zu jedem betrachteten ν mit $\mathrm{Ord}_{\mathbb{Z}_p^*}\nu = d$ genau $p \cdot \varphi(d)$ Automorphismen der Ordnung d existieren.

Die Elementeordnungen sind bis hierher also mit denen der Λ_p identisch. Zu untersuchen bleibt noch der Fall $\nu = p-1$. Hierin gilt zunächst $\mathrm{Ord}_{\mathbb{Z}_p^*}\nu = 2$, da $(p-1)^2 \equiv (-1)^2 \equiv 1 \bmod p$. Weiter ist

$$\sigma^{2n} : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta^{\mu((-1)^{2n-1}-(-1)^{2n-2}\pm\ldots+(-1)-1)}\alpha = \zeta^{-2n\mu}\alpha \end{cases}$$

genau dann die Identität, wenn gilt:

$$-2n\mu \equiv 0 \mod p\,.$$

Dies ist der Fall, wenn zum einen $\mu = 0$ und damit die Ordnung $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma = 2$ ist. Zum anderen wird die Bedingung für $n \equiv 0 \bmod p$ erfüllt. Das kleinste $n > 0$, das diese Kongruenz zu einer wahren Aussage macht, ist $n = p$, sodaß folgt: $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma = 2p$. Derartige Elementeordnungen gibt es in der Λ_p nicht, sodaß sich in der sich immer feiner verästelnden Fallunterscheidung zu guter letzt doch noch eine

Gruppe finden ließ, die bisher noch nicht auftrat. Sie tritt nur auf für Primzahlen p mit $p \equiv -1 \bmod 4$ und besitzt Elemente folgender Ordnung:

$$\begin{array}{rrll} & 1 & \text{Element der Ordnung} & 1 \\ & 1 & \text{Element der Ordnung} & 2 \\ \forall\, d \,|\, p-1,\, d \notin \{1,2\}: & p\cdot\varphi(d) & \text{Elemente der Ordnung} & d \\ & p-1 & \text{Elemente der Ordnung} & p \\ & p-1 & \text{Elemente der Ordnung} & 2p\,. \end{array}$$

Die allgemeine Charakterisierung erfolgt mit einer primitiven Wurzel δ modulo p durch

$$\widetilde{\Lambda}_p := \langle \sigma, \tau \rangle; \quad |\,\widetilde{\Lambda}_p\,| = p\,(p-1)$$
$$\mathrm{Ord}_{\widetilde{\Lambda}_p}\sigma = p\,; \quad \mathrm{Ord}_{\widetilde{\Lambda}_p}\tau = p-1; \quad \sigma\circ\tau = \tau\circ\sigma^{-\delta}\,.$$

Diese Gruppe ist in fast allen Fällen nicht kommutativ und damit nicht zyklisch, sodaß die Basis mindestens zweielementig sein muß. Als einzige Ausnahme ist dabei der Fall $p=3$ herauszustellen, denn es gilt

$$\widetilde{\Lambda}_3 \cong \mathbb{Z}_6\,.$$

Diese Gruppe ist im Gegensatz zu allen anderen $\widetilde{\Lambda}_p$ nicht nur kommutativ, sondern sogar zyklisch und läßt sich damit einelementig erzeugen.

Fall 3:
Als letzter Fall ist schließlich analog zur Ebene 1 zu betrachten, daß sowohl $x^p - \alpha^p$ als auch $x^p - \beta^p$ über $\mathbb{Q}[\zeta]$ irreduzibel sind und der Zerfällungskörper erst durch Adjunktion zweier Nullstellen α und β erzeugt wird. Dies beinhaltet jeweils eine Körpererweiterung vom Grad p und liefert insgesamt

$$[Z_f : \mathbb{Q}] = |\,G(Z_f\,|\,\mathbb{Q})\,| = p^2(p-1)\,.$$

Ein Automorphismus σ der Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ ist dann festgelegt durch seine Bilder $\sigma(\zeta)$, $\sigma(\alpha)$ und $\sigma(\beta)$. Aufbauend auf den Ergebnissen des vorherigen Falls ist σ von der Form

$$\sigma: \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1,2,\ldots,p-1\} \\ \alpha \mapsto \begin{cases} \zeta^{\mu}\alpha & \text{falls } \mathrm{Ord}_{\mathbb{Z}_p^*}\,\nu \mid \frac{p-1}{2} \\ \zeta^{\mu}\beta & \text{falls } \mathrm{Ord}_{\mathbb{Z}_p^*}\,\nu \not\mid \frac{p-1}{2} \end{cases} & \mu \in \{0,1,\ldots,p-1\} \\ \beta \mapsto \begin{cases} \zeta^{\kappa}\beta & \text{falls } \mathrm{Ord}_{\mathbb{Z}_p^*}\,\nu \mid \frac{p-1}{2} \\ \zeta^{\kappa}\alpha & \text{falls } \mathrm{Ord}_{\mathbb{Z}_p^*}\,\nu \not\mid \frac{p-1}{2} \end{cases} & \kappa \in \{0,1,\ldots,p-1\}\,. \end{cases} \tag{3.8}$$

Bei festem ν lassen sich so p^2 verschiedene Möglichkeiten realisieren. Damit stellt (3.8) insgesamt $p^2(p-1)$ paarweise verschiedene, Automorphismen und damit die gesamte Galoisgruppe dar.

Hieraus betrachtet werden nun σ_1, σ_2, τ mit

$$\sigma_1 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \\ \beta \mapsto \beta \end{cases} ; \quad \sigma_2 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \alpha \\ \beta \mapsto \zeta\beta \end{cases} ; \quad \tau : \begin{cases} \zeta \mapsto \zeta^\delta \\ \alpha \mapsto \beta \\ \beta \mapsto \alpha \end{cases} .$$

Die Automorphismen σ_1 und σ_2 besitzen jeweils die Ordnung p. Bei τ bildet erst die $(p-1)$-te Potenz ζ auf sich selbst ab. Da $p-1$ gerade ist, bleiben dann auch α und β fest, sodaß τ die Ordnung $p-1$ besitzt. Ein beliebiges ϕ der Form (3.8) läßt sich stets durch ein Produkt der Potenzen von σ_1, σ_2 und τ ausdrücken:

$$\phi = \begin{cases} \sigma_2^\kappa \circ \sigma_1^\mu \circ \tau^{\overline{\nu}} & \text{falls } \overline{\nu} \text{ gerade} \\ \sigma_1^\kappa \circ \sigma_2^\mu \circ \tau^{\overline{\nu}} & \text{falls } \overline{\nu} \text{ ungerade} . \end{cases}$$

Damit ist durch $\{\sigma_1, \sigma_2, \tau\}$ ein Erzeugendensystem der Galoisgruppe gegeben. Es gilt

$$\sigma_1 \circ \tau = \tau \circ \sigma_2^{\delta^{-1}} : \begin{cases} \zeta \mapsto \zeta^\delta \\ \alpha \mapsto \beta \\ \beta \mapsto \zeta\alpha \end{cases} ; \quad \sigma_2 \circ \tau = \tau \circ \sigma_1^{\delta^{-1}} : \begin{cases} \zeta \mapsto \zeta^\delta \\ \alpha \mapsto \zeta\beta \\ \beta \mapsto \alpha \end{cases} ,$$

womit die Galoisgruppe nicht kommutativ und damit nicht einelemtig erzeugbar ist. Eine zweielementige Basis läßt sich aus dem gegebenen Erzeugendensystem ableiten. Es ist

$$\sigma_2 \circ \tau = \tau \circ \sigma_1^{\delta^{-1}} , \quad \text{also} \quad \sigma_2 = \tau \circ \sigma_1^{\delta^{-1}} \circ \tau^{-1}$$

und damit

$$\begin{aligned} \sigma_1 \circ \tau &= \tau \circ \sigma_2^{\delta^{-1}} \\ &= \tau \circ (\tau \circ \sigma_1^{\delta^{-1}} \circ \tau^{-1})^{\delta^{-1}} \\ &= \tau \circ (\tau \circ (\sigma_1^{\delta^{-1}})^{\delta^{-1}} \circ \tau^{-1}) \\ &= \tau^2 \circ \sigma_1^{\delta^{-2}} \circ \tau^{-1} . \end{aligned}$$

Mit dieser Verknüpfung bilden σ_1 und τ eine Basis von $G(Z_f \mid \mathbb{Q})$. Somit läßt sich nun die betrachtete Gruppe mit einer beliebigen primitiven Wurzel δ modulo p charakterisieren als:

$$\widetilde{\Lambda}_{p^2} := \langle \sigma, \tau \rangle ; \quad |\widetilde{\Lambda}_{p^2}| = p^2(p-1)$$

$$\mathrm{Ord}_{\widetilde{\Lambda}_{p^2}} \sigma = p ; \quad \mathrm{Ord}_{\widetilde{\Lambda}_{p^2}} \tau = p-1 ; \quad \sigma \circ \tau = \tau^2 \circ \sigma^{\delta^2} \circ \tau^{-1} .$$

Welcher Ordnung sind dann die einzelnen Elemente dieser Gruppe? Automorphismen σ der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^\nu & \mathrm{Ord}_{\mathbb{Z}_p^*} \nu \mid \frac{p-1}{2} \\ \alpha \mapsto \zeta^\mu \alpha & \mu \in \{0, 1, \ldots, p-1\} \\ \beta \mapsto \zeta^\kappa \beta & \kappa \in \{0, 1, \ldots, p-1\} \end{cases}$$

traten bereits in der Ebene 1, Fall 3 auf. Für $\nu = 1$ existiert ein Automorphismus der Ordnung 1 und $p^2 - 1$ Automorphismen der Ordnung p. Ist $\nu \neq 1$, so ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\sigma = \mathrm{Ord}_{\mathbb{Z}_p^*}\nu$. Da μ und κ beliebig kombiniert werden können, gibt es mit Blick auf Satz 2.9 zu jedem Teiler d von $\frac{p-1}{2}$ genau $p^2 \cdot \varphi(d)$ Automorphismen der Ordnung d.

Ist $\sigma \in G(Z_f\,|\,\mathbb{Q})$ von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \mathrm{Ord}_{\mathbb{Z}_p^*}\nu \nmid \frac{p-1}{2} \\ \alpha \mapsto \zeta^{\mu}\beta & \mu \in \{0, 1, \ldots, p-1\} \\ \beta \mapsto \zeta^{\kappa}\alpha & \kappa \in \{0, 1, \ldots, p-1\}\,, \end{cases}$$

so muß seine Ordnung gerade sein, da $\alpha \neq \beta$. Entsprechende Potenzen sind gegeben durch

$$\sigma^2 : \begin{cases} \zeta \mapsto \zeta^{(\nu^2)} \\ \alpha \mapsto \zeta^{\nu\mu+\kappa}\alpha \\ \beta \mapsto \zeta^{\nu\kappa+\mu}\beta \end{cases}$$

$$\sigma^4 : \begin{cases} \zeta \mapsto \zeta^{(\nu^4)} \\ \alpha \mapsto \zeta^{\nu^3\mu+\nu^2\kappa+\nu\mu+\kappa}\alpha = \zeta^{(\nu\mu+\kappa)(\nu^2+1)}\alpha \\ \beta \mapsto \zeta^{\nu^3\kappa+\nu^2\mu+\nu\kappa+\mu}\beta = \zeta^{(\nu\kappa+\mu)(\nu^2+1)}\beta \end{cases}$$

$$\vdots$$

$$\sigma^{2n} : \begin{cases} \zeta \mapsto \zeta^{(\nu^{2n})} \\ \alpha \mapsto \zeta^{(\nu\mu+\kappa)(\nu^{2n-2}+\nu^{2n-4}+\ldots+\nu^2+1)}\alpha \\ \beta \mapsto \zeta^{(\nu\kappa+\mu)(\nu^{2n-2}+\nu^{2n-4}+\ldots+\nu^2+1)}\beta\,. \end{cases}$$

Damit σ^{2n} die Identität darstellt, muß gelten:

$$\nu^{2n} \equiv 1 \bmod p \quad \wedge \quad (\nu\mu+\kappa)\sum_{j=0}^{n-1}\nu^{2j} \equiv (\nu\kappa+\mu)\sum_{j=0}^{n-1}\nu^{2j} \equiv 0 \bmod p\,.$$

Dann ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\,\sigma = 2n$ mit dem kleinsten $n > 0$, das diese Kongruenzen erfüllt.

Für $\nu \notin \{1, p-1\}$ impliziert die erste Bedingung die zweite, denn mit $\nu^{2n} \equiv 1 \bmod p$ folgt

$$\nu^{2n-2} + \nu^{2n-4} + \ldots + \nu^2 + 1 \equiv \frac{\nu^{2n}-1}{\nu^2-1} \equiv \frac{1-1}{\nu^2-1} \equiv 0 \mod p\,.$$

Damit tritt eine Situation wie bei der Untersuchung von Fall 2 ein, sodaß analog geschlossen werden kann, daß es zu jedem betrachteten ν mit $\mathrm{Ord}_{\mathbb{Z}_p^*}\nu = d$ in der Galoisgruppe genau $p^2 \cdot \varphi(d)$ Elemente der Ordnung d gibt.

Es bleiben nun noch die Automorphismenordnungen für $\nu = p-1$ zu untersuchen. Aus Fall 2 ist bekannt: $\mathrm{Ord}_{\mathbb{Z}_p^*}\nu = 2$. Gilt $2 \,|\, \frac{p-1}{2}$, das heißt $p \equiv 1 \bmod 4$, so ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\sigma$ bereits oben ermittelt worden.

Damit stehen hierfür die Elementeordnungen der Galoisgruppe bereits fest:

$$\begin{array}{rll} 1 & \text{Element der Ordnung} & 1 \\ \forall\ 1 \neq d \,|\, p-1: \ p^2 \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ p^2 - 1 & \text{Elemente der Ordnung} & p\,. \end{array}$$

Dies sind aber dieselben Ordnungen, wie sie auch in der Λ_{p^2} zu finden sind. Dennoch ist die $\widetilde{\Lambda}_{p^2}$ nicht isomorph zur Λ_{p^2}! Denn betrachtet man zwei beliebige Automorphismen $\sigma, \tau \in \Lambda_{p^2}$ der Form (3.3) mit $\mathrm{Ord}_{\Lambda_{p^2}}\sigma = p$ und $\mathrm{Ord}_{\Lambda_{p^2}}\tau = p-1$, so ist

$$\sigma : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta^{\mu_1}\alpha \\ \beta \mapsto \zeta^{\kappa_1}\beta \end{cases} ; \quad \tau : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \alpha \mapsto \zeta^{\mu_2}\alpha \\ \beta \mapsto \zeta^{\kappa_2}\beta \end{cases} .$$

Dann gilt aber stets

$$\sigma \circ \tau = \tau \circ \sigma^{\delta^{-1}} : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \alpha \mapsto \zeta^{\mu_1+\mu_2}\alpha \\ \beta \mapsto \zeta^{\kappa_1+\kappa_2}\beta \end{cases} .$$

Diese Struktur müßte sich insbesondere auch in obiger Basis der $\widetilde{\Lambda}_{p^2}$ wiederfinden, was nicht der Fall ist.

Es bleibt noch zu untersuchen, welche Elementeordnungen für den Fall $p \equiv -1 \bmod 4$ bei Automorphismen $\sigma \in G(Z_f \,|\, \mathbb{Q})$ der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{p-1} = \zeta^{-1} & \\ \alpha \mapsto \zeta^{\mu}\beta & \mu \in \{0, 1, \ldots, p-1\} \\ \beta \mapsto \zeta^{\kappa}\alpha & \kappa \in \{0, 1, \ldots, p-1\} \end{cases}$$

auftreten. Die $2n$-te Potenz

$$\sigma^{2n} : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta^{(-\mu+\kappa)((-1)^{2n-2}+(-1)^{2n-4}+\ldots+(-1)^2+1)}\alpha = \zeta^{(-\mu+\kappa)n}\alpha \\ \beta \mapsto \zeta^{(-\kappa+\mu)((-1)^{2n-2}+(-1)^{2n-4}+\ldots+(-1)^2+1)}\beta = \zeta^{(-\kappa+\mu)n}\beta \end{cases}$$

ist genau dann die Identität, wenn

$$\mu \equiv \kappa \mod p \quad \vee \quad n \equiv 0 \mod p\,.$$

Für die betrachteten μ und κ wird die erste Kongruenz genau dann erfüllt, wenn sie gleich sind, was durch p verschiedene Belegungen realisierbar ist. Die Ordnung der Automorphismen ist dann jeweils 2. Sind μ und κ verschieden, so ist das kleinste $n > 0$, daß die zweite Kongruenz erfüllt gegeben durch $n = p$. Insgesamt besteht die Galoisgruppe

für den Fall $p \equiv -1 \bmod 4$ aus Elementen folgender Ordnung:

$$\begin{array}{rll} 1 & \text{Element der Ordnung} & 1 \\ p & \text{Elemente der Ordnung} & 2 \\ \forall\, d \,|\, p-1,\, d \notin \{1,2\}:\ p^2 \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ p^2-1 & \text{Elemente der Ordnung} & p \\ p^2-p & \text{Elemente der Ordnung} & 2p\,. \end{array}$$

Hierin zeigt sich, daß die $\widetilde{\Lambda}_{p^2}$ im Gegensatz zu den bisher diskutierten Gruppen keine einheitlichen Anzahlen an Elementen gleicher Ordnung besitzt, sondern diese abhängig davon ist, ob $\frac{p-1}{2}$ gerade oder ungerade ist. Auch wurde hier ein Beispiel dafür gefunden, daß Gruppen, deren Elemente gleiche Ordnungen besitzen, keinesfalls isomorph sein müssen.

Damit ist die Analyse der Ebene 2 abgeschlossen. Für den Fall $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$ tritt somit stets eine der folgenden Gruppen als Galoisgruppe von $f(x)$ auf:

$$\mathbb{Z}_p^*, \quad \Lambda_p, \quad \widetilde{\Lambda}_p, \quad \widetilde{\Lambda}_{p^2}\,.$$

Die Ergebnisse dieses Kapitels wurden allesamt aus vielschichtigen Fallunterscheidungen gewonnen, die die Untersuchung im Vergleich zur ersten Ebene ungleich aufwendiger gestalteten. Diese Ergebnisse und Methoden sind aber keineswegs nur für diese Ebene gültig, sondern werden sich auch in der Analyse der letzten Ebene als hilfreich erweisen.

3.4 Galoisgruppen der Ebene 3

Es wird nun der Fall $\sqrt{d} \notin \mathbb{Q}[\zeta]$ betrachtet. Wie in den zwei Ebenen zuvor sollen auch hier die Voraussetzungen für Satz 2.6 geschaffen werden. Da nach Voraussetzung $\sqrt{d} \notin \mathbb{Q}[\zeta]$, wohl aber $\sqrt{d} \in Z_f$, so ist die Adjunktion dieser Wurzel notwendig. Der Grad der so entstandene Körpererweiterung $\mathbb{Q}[\zeta, \sqrt{d}]$ ergibt sich unter Verwendung der Gradformel zu

$$[\mathbb{Q}[\zeta, \sqrt{d}] : \mathbb{Q}] = [\mathbb{Q}[\zeta, \sqrt{d}] : \mathbb{Q}[\zeta]] \cdot [\mathbb{Q}[\zeta] : \mathbb{Q}] = 2(p-1)\,.$$

Es kann nun analog zu den Ebenen 1 und 2 untersucht werden, wie auf dieser Grundlage das Polynom $f(x)$ weiter zerfallen kann und welche weiteren Adjunktionen gegebenenfalls notwendig sind.

Fall 1:
Eine Möglichkeit besteht darin, daß $f(x)$ bereits in $Z_f = \mathbb{Q}[\zeta, \sqrt{d}]$ vollständig in Linearfaktoren zerfällt. Ein Beispiel für derartige Polynome

ist

$$x^{2p}-2^p = (x^p-\sqrt{2}^p)(x^p+\sqrt{2}^p) = \prod_{j=1}^{p}(x-\zeta^j\sqrt{2})(x+\zeta^j\sqrt{2}) \in \mathbb{Q}[\zeta,\sqrt{2^p}]\,.$$

Die $2(p-1)$ verschiedene Automorphismen $\sigma \in G(Z_f\,|\,\mathbb{Q})$ sind festgelegt durch ihre Bilder $\sigma(\zeta)$ und $\sigma(\sqrt{d})$ und daher von der Form

$$\sigma : \left\{ \begin{array}{ll} \zeta & \mapsto \zeta^\nu \\ \sqrt{d} & \mapsto \pm\sqrt{d} \end{array} \right. \quad \nu \in \{1,2,\ldots,p-1\} \quad . \tag{3.9}$$

Hierdurch werden bereits genau $2(p-1)$ verschiedene Möglichkeiten und damit sämtliche Elemente der Galoisgruppe beschrieben.

Die Bilder $\sigma(\zeta)$ und $\sigma(\sqrt{d})$ beeinflussen sich, im Gegensatz zu den meisten bisherigen Gruppen, beim Potenzieren von σ nicht gegenseitig. Dies läßt vermuten, daß es sich bei der Galoisgruppe um ein direkten Produkt zweier Untergruppen handelt. Um dieses nachzuweisen, wird folgendes notwendige und hinreichende Kriterium aus der Gruppentheorie herangezogen:

Satz 3.2 *Genau dann ist eine Gruppe G das direkte Produkt zweier Untergruppen U und V, wenn gilt:*

(i) *Für das Komplexprodukt UV gilt: $UV = G$*
(ii) *$U \cap V = \{e\}$*
(iii) *U und V sind Normalteiler von G.*

Beweis: vgl. [1], S.43f.

Die Untergruppen seien gegeben durch $U = \langle\lambda\rangle$ und $V = \langle\tau\rangle$ mit

$$\lambda : \left\{ \begin{array}{ll} \zeta & \mapsto \zeta \\ \sqrt{d} & \mapsto -\sqrt{d} \end{array} \right. , \quad \tau : \left\{ \begin{array}{ll} \zeta & \mapsto \zeta^\delta \\ \sqrt{d} & \mapsto \sqrt{d} \end{array} \right. .$$

Zunächst erkennt man unmittelbar, daß zum einen Ord $U = 2$ und damit $U \cong \mathbb{Z}_2$, zum anderen Ord $V = p-1$, sowie $V \cong \mathbb{Z}_p^*$. Ferner enthält der Schnitt von U und V offenbar nur die Identität.

Auch ist jedes ϕ der Form (3.9) durch ein Produkt der Potenzen von λ und τ darstellbar:

$$\tau^\nu \circ \lambda^\kappa = \lambda^\kappa \circ \tau^\nu = \phi : \left\{ \begin{array}{ll} \zeta & \mapsto \zeta^\nu \\ \sqrt{d} & \mapsto (-1)^\kappa\sqrt{d} \end{array} \right. .$$

Damit bildet das Komplexprodukt UV die gesamte Gruppe. Mehr noch: Die Automorphismen λ und τ bilden eine Basis und kommutieren miteinander. Damit ist die Galoisgruppe abelsch und jede Untergruppe, insbesondere U und V ein Normalteiler.

Es sind somit alle drei Kriterien des Satzes 3.2 erfüllt, sodaß insgesamt folgt:

$$G(Z_f \,|\, \mathbb{Q}) = U \times V \cong \mathbb{Z}_2 \times \mathbb{Z}_p^* \,.$$

Die Ordnung eines Elementes $\phi = \lambda^\kappa \circ \tau^\nu \in U \times V$ ist dann festgelegt durch

$$\mathrm{Ord}_{U\times V}\, \phi = \mathrm{kgV}(\mathrm{Ord}_U\, \lambda^\kappa, \mathrm{Ord}_V\, \tau^\nu) \,.$$

Die Elementeordnungen der $\mathbb{Z}_2$ und der $\mathbb{Z}_p^*$ sind durch Satz 2.9 (iv) bekannt und liefern insgesamt für ihr direktes Produkt:

$$\begin{array}{lrll} \forall\, d \,|\, p-1,\ 2 \,|\, d: & 2\varphi(d) & \text{Elemente der Ordnung} & d \\ \forall\, d \,|\, p-1,\ 2 \not| \, d: & \varphi(d) & \text{Elemente der Ordnung} & d \\ \forall\, d \,|\, p-1,\ 2 \not| \, d: & \varphi(d) & \text{Elemente der Ordnung} & 2d \,. \end{array}$$

Fall 2:
Als zweiter Fall ist wieder zu betrachten, wenn mindestens eines der Polynome $x^p - \alpha^p$ und $x^p - \beta^p$ über $\mathbb{Q}[\zeta, \sqrt{d}]$ irreduzibel ist, aber die Adjunktion eines $\gamma \in \{\alpha, \beta\}$ bereits zum Zerfällungskörper führt. Dessen Grad und damit die Ordnung der Galoisgruppe ist dann

$$[Z_f : \mathbb{Q}] = [\mathbb{Q}[\zeta, \sqrt{d}, \gamma] : \mathbb{Q}[\zeta, \sqrt{d}]] \cdot [\mathbb{Q}[\zeta, \sqrt{d}] : \mathbb{Q}] = p \cdot 2(p-1) \,.$$

Da $\mathbb{Q}[\sqrt{d}]$ ein Teilkörper von $\mathbb{Q}[\gamma]$ ist, läßt sich der Zerfällungskörper einfacher durch $Z_f = \mathbb{Q}[\zeta, \gamma]$ charakterisieren. Dann ist aber mit Hilfe der Gradformel

$$\begin{array}{lll} & [Q[\zeta, \gamma] : \mathbb{Q}] & = [\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}[\zeta]] \cdot [\mathbb{Q}[\zeta] : \mathbb{Q}] \\ \Longrightarrow & 2p\,(p-1) & = [\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}[\zeta]] \cdot (p-1) \\ \Longrightarrow & [\mathbb{Q}[\zeta, \gamma] : \mathbb{Q}[\zeta]] & = 2p \\ \Longrightarrow & [\mathbb{Q}[\gamma] : \mathbb{Q}] & \geq 2p \,. \end{array}$$

Hier gilt sogar die Gleichheit, denn γ ist eine Nullstelle von $f(x)$, dessen Grad $2p$ beträgt, also $\mathrm{Irr}(\gamma, \mathbb{Q}) = f(x)$. Damit gilt analog zum Fall 2 der Ebene 2: Zerfällt $f(x)$ über $\mathbb{Q}[\zeta]$ nicht vollständig in Linearfaktoren, so ist es irreduzibel über $\mathbb{Q}$.

Da es keine Rolle spielt, welche Nullstelle des irreduziblen Polynoms adjungiert wird, ist der Zerfällungskörper gegeben durch

$$Z_f = \mathbb{Q}[\zeta, \gamma] = \mathbb{Q}[\zeta, \alpha] = \mathbb{Q}[\zeta, \beta] \,.$$

Die Galoisgruppe läßt sich nun sehr übersichtlich berechnen, wenn man die Fallunterscheidung der Ebene 2, Fall 2 aufgreift: Entweder existiert eine rationale p-te Wurzel aus b, oder nicht. Mit Satz 2.5 formuliert: Entweder ist $x^p - b$ über $\mathbb{Q}$ reduzibel, oder nicht.

Nimmt man zunächst letzteres an, so ist $x^p - b$ aber auch irreduzibel über $\mathbb{Q}[\zeta, \sqrt{d}]$, denn andernfalls ist nach Satz 2.6 bereits

$\sqrt[p]{b} \in \mathbb{Q}[\zeta, \sqrt{d}]$. Dann folgt aber unter Verwendung der Gradformel:

$$\begin{array}{rcl} & [\mathbb{Q}[\sqrt[p]{b}] : \mathbb{Q}] \mid [\mathbb{Q}[\zeta, \sqrt{d}] : Q] \\ \Longleftrightarrow & p \mid 2(p-1) \\ \Longleftrightarrow & p \mid 2 \,, \end{array}$$

was nicht sein kann, da p eine ungerade Primzahl ist.

Somit ist nun der Grad $[\mathbb{Q}[\zeta, \sqrt{d}, \sqrt[p]{b}] : \mathbb{Q}] = 2p\,(p-1) = [Z_f : \mathbb{Q}]$. Zudem ist $\zeta, \sqrt{d}, \sqrt[p]{b} \in Z_f$, woraus insgesamt folgt:

$$Z_f = \mathbb{Q}[\zeta, \sqrt{d}, \sqrt[p]{b}] \,.$$

Auf dieser Grundlage sind Automorphismen $\sigma \in G(Z_f \mid \mathbb{Q})$ von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1, 2, \ldots, p-1\} \\ \sqrt[p]{b} \mapsto \zeta^{\mu} \sqrt[p]{b} & \mu \in \{0, 1, \ldots, p-1\} \\ \sqrt{d} \mapsto \pm\sqrt{d} \,. \end{cases} \tag{3.10}$$

Da hiermit genau $2p\,(p-1)$ verschiedene Möglichkeiten beschrieben sind, stellt (3.10) die gesamte Galoisgruppe dar.

Die Bilder $\sigma(\zeta)$ und $\sigma(\sqrt[p]{b})$ auf der einen Seite und $\sigma(\sqrt{d})$ auf der anderen Seite beeinflussen sich beim Potenzieren von σ nicht gegenseitig, sodaß die Idee aus Fall 1 aufgegriffen werden kann: Handelt es sich bei der Galoisgruppe um ein direktes Produkt zweier Untergruppen? Betrachtet hierzu werden die Untergruppen $U = \langle\lambda\rangle$ und $V = \langle\sigma, \tau\rangle$, gegeben durch

$$\lambda : \begin{cases} \zeta \mapsto \zeta \\ \sqrt[p]{b} \mapsto \sqrt[p]{b} \\ \sqrt{d} \mapsto -\sqrt{d} \end{cases} \quad ; \quad \sigma : \begin{cases} \zeta \mapsto \zeta \\ \sqrt[p]{b} \mapsto \zeta \sqrt[p]{b} \\ \sqrt{d} \mapsto \sqrt{d} \end{cases} \quad ; \quad \tau : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \sqrt[p]{b} \mapsto \sqrt[p]{b} \\ \sqrt{d} \mapsto \sqrt{d} \end{cases} \,.$$

Es ist $\mathrm{Ord}_{G(Z_f|\mathbb{Q})}\lambda = 2$ und damit $U \cong \mathbb{Z}_2$. Die Automorphismen σ und τ besitzen die Ordnungen p bzw. $p-1$. Da zudem $\sigma \circ \tau = \tau \circ \sigma^{\delta^{-1}}$, folgt mit Blick auf (3.2): $V \cong \Lambda_p$.

Man erkennt unmittelbar, daß der Schnitt der beiden Gruppen U und V lediglich aus der Identität besteht.

Weiter ist jedes ϕ der Form (3.10) darstellbar durch

$$\lambda^{\kappa} \circ \sigma^{\mu} \circ \tau^{\overline{\nu}} = \phi : \begin{cases} \zeta \mapsto \zeta^{\nu} \\ \sqrt[p]{b} \mapsto \zeta^{\mu} \sqrt[p]{b} \\ \sqrt{d} \mapsto (-1)^{\kappa} \sqrt{d} \,, \end{cases}$$

womit gezeigt ist, daß das Komplexprodukt UV die gesamte Gruppe darstellt.

Um Satz 3.2 anwenden zu können, ist noch zu zeigen, daß U und V Normalteiler der Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ sind. Betrachtet aus der Perspektive der Galoistheorie ist gleichbedeutend dazu, daß die Fixkörper von U und V normal über $\mathbb{Q}$ sind.

Für den Fixkörper F_U der Gruppe U gilt

$$[F_U : \mathbb{Q}] = \frac{[Z_f : \mathbb{Q}]}{\operatorname{Ord} U} = \frac{2p\,(p-1)}{2} = p\,(p-1)\,.$$

Offenbar bleiben ζ und $\sqrt[p]{b}$ unter U fest. Da $\mathbb{Q}[\zeta, \sqrt[p]{b}]$ nach Voraussetzung den Grad $p\,(p-1)$ über $\mathbb{Q}$ besitzt, ist dies der gesuchte Fixkörper. Dieser aber stellt den Zerfällungskörper von $x^p - b \in \mathbb{Q}[x]$ dar und ist damit normal über $\mathbb{Q}$.

Analog besitzt der Fixkörper F_V der Gruppe V den Grad

$$[F_V : \mathbb{Q}] = \frac{[Z_f : \mathbb{Q}]}{\operatorname{Ord} V} = \frac{2p\,(p-1)}{p\,(p-1)} = 2\,.$$

Da zum einen $\sqrt{d}$ unter den Automorphismen von V fest bleibt, zum andern nach Voraussetzung $[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2$, ist $F_V = \mathbb{Q}[\sqrt{d}]$. Dieser kann als Zerfällungskörper von $x^2 - d \in \mathbb{Q}[x]$ aufgefaßt werden und ist damit ebenfalls normal über $\mathbb{Q}$.

So sind nun insgesamt alle drei Kriterien des Satz 3.2 erfüllt, und es ergibt sich für die gesuchte Galoisgruppe im betrachteten Fall

$$G(Z_f\,|\,\mathbb{Q}) = U \times V \cong \mathbb{Z}_2 \times \Lambda_p\,.$$

Existiert eine rationale p-te Wurzel aus b, so läßt sich der Zerfällungskörper nicht in der oben betrachteten alternativen Form wiedergeben. Legt man ohne Einschränkung als Zerfällungskörper $\mathbb{Q}[\zeta, \alpha]$ zugrunde, so sind damit die Automorphismen $\sigma \in G(Z_f\,|\,\mathbb{Q})$ festgelegt durch $\sigma(\zeta)$ und $\sigma(\alpha)$. Schaut man auf (3.7) zurück, so sind sie von der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} & \nu \in \{1, 2, \ldots, p-1\} \\ \alpha \mapsto \begin{cases} \zeta^{\mu}\alpha \\ \zeta^{\mu}\frac{r}{\alpha} \end{cases} & \mu \in \{0, 1, \ldots, p-1\}\,. \end{cases} \tag{3.11}$$

Hiermit sind $2p\,(p-1)$ Möglichkeiten und damit genau die Automorphismen der Galoisgruppe beschrieben. Es zeigt sich, daß diese isomorph zu der durch (3.10) beschriebenen Gruppe ist, denn sie besitzt zum einen dieselbe Ordnung, zum andern eine strukturell identische Basis. Diese ist analog zu der oben diskutierten Basis $\{\lambda, \sigma, \tau\}$ gegeben durch $\{\lambda^*, \sigma^*, \tau^*\}$ mit

$$\lambda^* : \begin{cases} \zeta \mapsto \zeta^{-1} \\ \alpha \mapsto \frac{r}{\alpha} \end{cases} \quad ; \quad \sigma^* : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \end{cases} \quad ; \quad \tau^* : \begin{cases} \zeta \mapsto \zeta^{\delta} \\ \alpha \mapsto \alpha \end{cases} \quad .$$

Die Automorphismen σ^* und τ^* wurden bereits in der Ebene 1, Fall 2 diskutiert, sie bilden die Basis einer Λ_p. Der Automorphismus λ^* besitzt die Ordnung 2 und kann nicht durch σ^* und τ^* erzeugt werden, er kommutiert aber mit ihnen:

$$\tau^* \circ \lambda^* = \lambda^* \circ \tau^* : \begin{cases} \zeta \mapsto \zeta^{-\delta} \\ \alpha \mapsto \frac{r}{\alpha} \end{cases} \quad \text{und} \quad \sigma^* \circ \lambda^* = \lambda^* \circ \sigma^* : \begin{cases} \zeta \mapsto \zeta^{-1} \\ \alpha \mapsto \frac{r}{\zeta\alpha} \end{cases} .$$

Damit ist die oben behauptete Gruppenisomorphie bewiesen. Insgesamt ist nun gezeigt, daß die Galoisgruppe im betrachteten Fall dieser Ebene stets isomorph ist zur $\mathbb{Z}_2 \times \Lambda_p$. Welche Ordnungen besitzen die Elemente dieser Gruppe? Sei $(\phi_1, \phi_2) \in \mathbb{Z}_2 \times \Lambda_p$, so gilt

$$\mathrm{Ord}_{\mathbb{Z}_2 \times \Lambda_p}(\phi_1, \phi_2) = \mathrm{kgV}(\mathrm{Ord}_{\mathbb{Z}_2}\, \phi_1, \mathrm{Ord}_{\Lambda_p}\, \phi_2) .$$

Da die Elementeordnungen der Gruppen $\mathbb{Z}_2$ und Λ_p bekannt sind, besitzt ihr direktes Produkt

	1	Element der Ordnung	1
	$2p+1$	Elemente der Ordnung	2
$\forall\, d \mid p-1,\ d \notin \{1,2\},\ 2 \mid d:$	$2p \cdot \varphi(d)$	Elemente der Ordnung	d
$\forall\, d \mid p-1,\ d \notin \{1,2\},\ 2 \nmid d:$	$p \cdot \varphi(d)$	Elemente der Ordnung	d
$\forall\, d \mid p-1,\ d \notin \{1,2\},\ 2 \nmid d:$	$p \cdot \varphi(d)$	Elemente der Ordnung	$2d$
	$p-1$	Elemente der Ordnung	p
	$p-1$	Elemente der Ordnung	$2p$.

Fall 3:
Es verbleibt der Fall, bei dem Z_f erst durch Adjunktion beider Nullstellen α und β an $\mathbb{Q}[\zeta, \sqrt{d}]$ erzeugt wird. Die damit einhergehende Körpererweiterung jeweils vom Grad p ergibt mit Hilfe der Gradformel:

$$[Z_f : \mathbb{Q}] = p^2 \cdot\ 2(p-1) .$$

Dabei läßt sich der Zerfällungskörper schreiben als

$$Z_f = \mathbb{Q}[\zeta, \alpha, \beta] ,$$

da die Adjunktion einer Nullstelle bereits die Adjunktion von $\sqrt{d}$ einschließt. Ein Automorphismus $\sigma \in G(Z_f \mid \mathbb{Q})$ bildet dann α und β auf gewisse Nullstellen von $f(x)$ ab. Wird α auf $\zeta^\mu\alpha$ abgebildet, so bedeutet dies mit (3.6), daß $\sqrt{d}$ unter σ fest bleibt. Daraus folgt, daß dann β auf $\zeta^\kappa\beta$ abgebildet werden muß. Ist aber $\sigma(\alpha) = \zeta^\mu\beta$, so wird $\sqrt{d}$ auf $-\sqrt{d}$ abgebildet, woraus folgt, daß das Bild von β unter σ von der Form $\zeta^\kappa\alpha$ sein muß. Durch diese Einschränkung besitzt σ die Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^\nu & \nu \in \{1, 2, \ldots, p-1\} \\ \alpha \mapsto \begin{cases} \zeta^\mu\alpha \\ \zeta^\mu\beta \end{cases} & \mu \in \{0, 1, \ldots, p-1\} \\ \beta \mapsto \begin{cases} \zeta^\kappa\beta \\ \zeta^\kappa\alpha \end{cases} \text{ falls } \begin{matrix} \alpha \mapsto \zeta^\mu\alpha \\ \alpha \mapsto \zeta^\mu\beta \end{matrix} & \kappa \in \{0, 1, \ldots, p-1\} . \end{cases} \tag{3.12}$$

Hierdurch werden genau $2p^2(p-1)$ verschiedene Möglichkeiten beschrieben, also genau soviele, wie es auch Automorphismen gibt. Damit stellt (3.12) genau die Elemente der Galoisgruppe dar. Welche Ordnungen besitzen ihre Elemente? Betrachtet man nur die Automorphismen $\sigma \in G(Z_f \,|\mathbb{Q})$ der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} \\ \alpha \mapsto \zeta^{\mu}\alpha \\ \beta \mapsto \zeta^{\kappa}\beta\,, \end{cases}$$

so stellt ihre Gesamtheit gerade die in der Ebene 1, Fall 3 diskutierte Gruppe Λ_{p^2} dar, deren Elementeprdnungen dort berechnet wurden:

$$\begin{array}{rrll} & 1 & \text{Element der Ordnung} & 1 \\ \forall\, 1 \neq d \,|\, p-1: & p^2 \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ & p^2-1 & \text{Elemente der Ordnung} & p\,. \end{array}$$

Automorphismen der Form

$$\sigma : \begin{cases} \zeta \mapsto \zeta^{\nu} \\ \alpha \mapsto \zeta^{\mu}\beta \\ \beta \mapsto \zeta^{\kappa}\alpha \end{cases}$$

treten, allerdings unter Einschränkung bezüglich ν, bereits in der Ebene 2, Fall 3 auf. Für $\nu \notin \{1, p-1\}$ wurde gezeigt, daß es zu jedem $d = \mathrm{Ord}_{\mathbb{Z}_p^*}\nu$ genau $p^2 \cdot \varphi(d)$ Elemente der Ordnung d gibt. Dies ist hier für die betrachteten ν mit Satz 2.9 (iv) zu jedem natürlichen Teiler $d \notin \{1, 2\}$ von $p-1$ der Fall, da $\mathrm{Ord}_{\mathbb{Z}_p^*}1 = 1$ und $\mathrm{Ord}_{\mathbb{Z}_p^*}(p-1) = 2$. Für $\nu = p-1$ wurde gezeigt, daß es genau p Automorphismen der Ordnung 2 und $p^2 - p$ Automorphismen der Ordnung $2p$ gibt.

Somit bleibt noch der Fall $\nu = 1$ zu untersuchen. Auch hier muß die Automorphismenordnung wieder gerade sein, da sonst α und β nicht auf sich abgebildet werden können. Benutzt man die allgemeine Darstellung aus Ebene 2, Fall 3, so ist die $(2n)$-te Potenz gegeben durch

$$\sigma^{2n} : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta^{(\mu+\kappa)(1^{2n-2}+1^{2n-4}+\ldots+1^2+1)}\alpha = \zeta^{(\mu+\kappa)n}\alpha \\ \beta \mapsto \zeta^{(\kappa+\mu)(1^{2n-2}+1^{2n-4}+\ldots+1^2+1)}\beta = \zeta^{(\kappa+\mu)n}\beta\,. \end{cases}$$

Diese ist genau dann die Identität, wenn

$$\nu \equiv -\kappa \bmod p \quad \vee \quad n \equiv 0 \bmod p\,.$$

Die Automorphismenordnung ist dann das kleinste $2n > 0$, das diese Bedingung erfüllt. Für die betrachteten μ und κ ist die erste Kongruenz genau dann wahr, wenn $\mu = -\kappa$. Es gibt genau p verschiedene derartige Automorphismen, ihre Ordnung beträgt 2. Alle weiteren $p^2 - p$

Automorphismen besitzen die Ordnung $2p$, da $n=p$ das kleinste $n>0$ ist, das die zweite Kongruenz erfüllt.

Damit sind nun sämtliche Automorphismenordnungen bekannt. Es gibt in der betrachteten Galoisgruppe

$$\begin{array}{rll} 1 & \text{Element der Ordnung} & 1 \\ p^2+2p & \text{Elemente der Ordnung} & 2 \\ \forall\, d \,|\, p-1,\, d \notin \{1,2\} : p^2 \cdot \varphi(d) & \text{Elemente der Ordnung} & d \\ p^2-1 & \text{Elemente der Ordnung} & p \\ 2p\,(p-1) & \text{Elemente der Ordnung} & 2p\,. \end{array}$$

Damit zeigt sich, daß eine ähnliche Struktur wie in den ersten zwei Fällen dieser Ebene nicht auftritt. Eine etwaige Vermutung, die gesuchte Galoisgruppe sei isomorph zur $\mathbb{Z}_2 \times \Lambda_{p^2}$ erweist sich mit diesen Elementeordnungen als falsch.

Ein Erzeugendensystem der Gruppe ist gegeben durch $\{\sigma_1, \sigma_2, \tau, \lambda\}$ mit

$$\sigma_1 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \\ \beta \mapsto \beta \end{cases} ; \qquad \sigma_2 : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \alpha \\ \beta \mapsto \zeta\beta \end{cases} ;$$

$$\tau : \begin{cases} \zeta \mapsto \zeta^\delta \\ \alpha \mapsto \alpha \\ \beta \mapsto \beta \end{cases} ; \qquad \lambda : \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \beta \\ \beta \mapsto \alpha \end{cases} .$$

Jedes $\phi \in G(Z_f \,|\, \mathbb{Q})$ der Form

$$\phi : \begin{cases} \zeta \mapsto \zeta^\nu \\ \alpha \mapsto \zeta^\mu \alpha \\ \beta \mapsto \zeta^\kappa \beta \end{cases}$$

ist dann darstellbar durch $\phi = \sigma_1^\mu \circ \sigma_2^\kappa \circ \tau^{\overline{\nu}}$. Ein Automorphismus ϕ der Form

$$\phi : \begin{cases} \zeta \mapsto \zeta^\nu \\ \alpha \mapsto \zeta^\mu \beta \\ \beta \mapsto \zeta^\kappa \alpha \end{cases}$$

läßt sich analog schreiben als $\phi = \lambda \circ \sigma_1^\mu \circ \sigma_2^\kappa \circ \tau^{\overline{\nu}}$.

Die Verknüpfungsstruktur dieses Erzeugendensystems zeigt sich durch

$$\sigma_1 \circ \lambda = \lambda \circ \sigma_2 \qquad \sigma_{1,2} \circ \tau = \tau \circ \sigma_{1,2}^{\delta^{-1}} .$$

Die Automorphismen λ und τ kommutieren miteinander. Nun läßt sich einer der Automorphismen σ_1, σ_2 aus dem Erzeugendensystem eliminieren, zum Beispiel durch

$$\sigma_2 = \lambda \circ \sigma_1 \circ \lambda^{-1} = \lambda \circ \sigma_1 \circ \lambda\,.$$

Welche Verknüpfungsstruktur zeigt sich dann zwischen σ_1 und λ? Zwar kommutieren sie nicht direkt miteinander, es gilt aber

$$(\sigma_1 \circ \lambda)^2 = (\lambda \circ \sigma_1)^2 = \begin{cases} \zeta \mapsto \zeta \\ \alpha \mapsto \zeta\alpha \\ \beta \mapsto \zeta\beta \end{cases}$$

und damit

$$\sigma_1 \circ \lambda = (\lambda \circ \sigma_1)^2 \circ (\lambda \circ \sigma_1^{-1}) .$$

Das verbleibende System $\{\lambda, \sigma_1, \tau\}$ stellt eine Basis dar: Denn entfernt man λ aus dieser Menge, so verbleibt eine Basis der Λ_p, die aufgrund ihrer Ordnung nicht die Gruppe sein kann. Bleibt σ_1 unberücksichtigt, so ist $\langle \lambda, \tau \rangle$ eine zu $\mathbb{Z}_2 \times \mathbb{Z}_p^*$ isomorphe Gruppe, die bereits in Fall 1 dieser Ebene diskutiert wurde und deren Ordnung ebenfalls zu klein ist. Schließlich kann auch auf τ nicht verzichtet werden, denn unter allen Produkten, die aus Potenzen von λ und σ_1 gebildet werden, wird ζ nur auf sich selbst abgebildet.

Die Galoisgruppe ist damit vollständig erfaßt, sie läßt sich nun allgemein mit einer primitiven Wurzel δ modulo p charakterisieren:

$$\Lambda_{2p^2} := \langle \sigma, \tau, \lambda \rangle; \quad |\Lambda_{2p^2}| = 2p^2(p-1)$$

$$\mathrm{Ord}_{\Lambda_{2p^2}} \sigma = p ; \quad \mathrm{Ord}_{\Lambda_{2p^2}} \tau = p-1 ; \quad \mathrm{Ord}_{\Lambda_{2p^2}} \lambda = 2$$

$$\sigma \circ \lambda = (\lambda \circ \sigma)^2 \circ (\lambda \circ \sigma^{-1}) ; \quad \tau \circ \lambda = \lambda \circ \tau ; \quad \sigma \circ \tau = \tau \circ \sigma^{\delta} .$$

Somit sind nun sämtliche mögliche Gruppen dieser Ebene analysiert. Insgesamt ergibt sich, daß die Galoisgruppe des Polynoms $f(x)$ für den Fall $\sqrt{d} \notin \mathbb{Q}[\zeta]$ stets zu einer der Gruppen

$$\mathbb{Z}_2 \times \mathbb{Z}_p^* , \quad \mathbb{Z}_2 \times \Lambda_p , \quad \Lambda_{2p^2}$$

isomorph ist.

3.5 Zusammenfassung

In den Kapiteln 3.1 bis 3.4 wurden sämtliche, bis auf Isomorphie verschiedene, mögliche Galoisgruppen der Polynome (1.1) berechnet.

Zusammenfassend werden sie hier noch einmal kurz ihrer Ordnung nach aufgelistet und charakterisiert. Dabei bedeute δ wieder eine beliebige primitive Wurzel modulo p. Die Verknüpfung kommutierender Basiselemente wird nicht explizit aufgeführt.

$id = \langle 1 \rangle$: $\mathrm{Ord}\, id = 1 ;\ \mathrm{Ord}_{id} 1 = 1$

$\mathbb{Z}_p^* = \langle \tau \rangle$: $\mathrm{Ord}\, \mathbb{Z}_p^* = p-1 ; \mathrm{Ord}_{\mathbb{Z}_p^*} \tau = p-1$

$$\Lambda_p = \langle \sigma, \tau \rangle \quad : \quad \begin{array}{c} \operatorname{Ord} \Lambda_p = p\,(p-1) \\ \operatorname{Ord}_{\Lambda_p} \sigma = p\,;\ \operatorname{Ord}_{\Lambda_p} \tau = p-1 \\ \sigma \circ \tau = \tau \circ \sigma^{\delta} \end{array}$$

$$\widetilde{\Lambda}_p = \langle \sigma, \tau \rangle \quad : \quad \begin{array}{c} \operatorname{Ord} \widetilde{\Lambda}_p = p\,(p-1) \\ \operatorname{Ord}_{\widetilde{\Lambda}_p} \sigma = p\,;\ \operatorname{Ord}_{\widetilde{\Lambda}_p} \tau = p-1 \\ \sigma \circ \tau = \tau \circ \sigma^{-\delta} \end{array}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_p^* = \langle \sigma, \lambda \rangle \quad : \quad \begin{array}{c} \operatorname{Ord}\ \mathbb{Z}_2 \times \mathbb{Z}_p^* = 2(p-1) \\ \operatorname{Ord}_{\mathbb{Z}_2 \times \mathbb{Z}_p^*} \sigma = p\,;\ \operatorname{Ord}_{\mathbb{Z}_2 \times \mathbb{Z}_p^*} \lambda = 2 \end{array}$$

$$\mathbb{Z}_2 \times \Lambda_p = \langle \sigma, \tau, \lambda \rangle \, : \quad \begin{array}{c} \operatorname{Ord}\ \mathbb{Z}_2 \times \Lambda_p = 2p\,(p-1) \\ \operatorname{Ord}_{\mathbb{Z}_2 \times \Lambda_p} \sigma = p\,;\ \operatorname{Ord}_{\mathbb{Z}_2 \times \Lambda_p} \tau = p-1 \\ \operatorname{Ord}_{\mathbb{Z}_2 \times \Lambda_p} \lambda = 2 \\ \sigma \circ \tau = \tau \circ \sigma^{\delta} \end{array}$$

$$\Lambda_{p^2} = \langle \sigma_1, \sigma_2, \tau \rangle \quad : \quad \begin{array}{c} \operatorname{Ord}\ \Lambda_{p^2} = p^2(p-1) \\ \operatorname{Ord}_{\Lambda_{p^2}} \sigma_{1,2} = p\,;\ \operatorname{Ord}_{\Lambda_{p^2}} \tau = p-1 \\ \sigma_{1,2} \circ \tau = \tau \circ \sigma_{1,2}^{\delta} \end{array}$$

$$\widetilde{\Lambda}_{p^2} = \langle \sigma, \tau \rangle \quad : \quad \begin{array}{c} \operatorname{Ord}\ \widetilde{\Lambda}_{p^2} = p^2(p-1) \\ \operatorname{Ord}_{\widetilde{\Lambda}_{p^2}} \sigma = p\,;\ \operatorname{Ord}_{\widetilde{\Lambda}_{p^2}} \tau = p-1 \\ \sigma \circ \tau = \tau^2 \circ \sigma^{\delta^2} \circ \tau^{-1} \end{array}$$

$$\Lambda_{2p^2} = \langle \sigma, \tau, \lambda \rangle \quad : \quad \begin{array}{c} \operatorname{Ord}\ \Lambda_{2p^2} = 2p^2(p-1) \\ \operatorname{Ord}_{\Lambda_{2p^2}} \sigma = p\,;\ \operatorname{Ord}_{\Lambda_{2p^2}} \tau = p-1; \\ \operatorname{Ord}_{\Lambda_{2p^2}} \lambda = 2 \\ \sigma \circ \tau = \tau \circ \sigma^{\delta}; \\ \sigma \circ \lambda = (\lambda \circ \sigma)^2 \circ (\lambda \circ \sigma^{-1}) \quad . \end{array}$$

4 Wann treten welche Gruppen auf?

In jeder der in Kapitel 3 diskutierten Ebene wurde unterschieden, ob die Adjunktion der Nullstellen α oder β erforderlich ist; genauer gesagt: ob α bzw. β p-Radikale der Körper $\mathbb{Q}[\zeta, \sqrt{d}]$ bzw. $\mathbb{Q}[\zeta, \sqrt{d}, \gamma]$ mit $\gamma \in \{\alpha, \beta\}$ sind.

In Anlehnung an diese Vorgehensweise stellt sich bezüglich des Zusammenhangs zwischen einem Polynom $f(x)$ der Form (1.1) und seinem Zerfällungskörper die Frage, welche Radikale eines Grundkörpers K sich in einer einfachen Radikalerweiterung $K[\sqrt[n]{c}]$ befinden. Diese Strukturfrage läßt sich sehr überschaubar beantworten und darauf aufbauend schließlich vollständig analysieren, unter welchen Voraussetzungen $f(x)$ eine bestimmte Galoisgruppe besitzt.

4.1 Einfache Radikalerweiterungen

Bevor auf die spezifischen Eigenschaften einfacher Radikalerweiterungen eingegangen wird, werden kurz einige Begriffe der Linearen Algebra auf die Körpertheorie übertragen: Sei $K[\gamma]$ eine einfache algebraische Erweiterung des Grundkörpers K vom Grad n. Das irreduzible Polynom von γ über K ist dann von der Form

$$\mathrm{Irr}(\gamma, K) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]\,.$$

Nach den Grundlagen aus Kapitel 2 kann $K[\gamma]$ als Vektorraum über K aufgefaßt werden, eine Basis ist nach Satz 2.2 durch $\{1, \gamma, \ldots, \gamma^{n-1}\}$ gegeben. Jedes Element $v \in K[\gamma]$ ist dann mit Koeffizienten aus K darstellbar in der Form

$$v = c_1 + c_2\gamma + \ldots + c_n\gamma^{n-1}.$$

Durch γ wird folgende Abbildung induziert:

$$\phi_\gamma : K[\gamma] \longrightarrow K[\gamma];\ v \mapsto \gamma v\,.$$

Diese stellt eine lineare Transformation von $K[\gamma]$ auf sich selbst dar, denn es gilt:

$$\begin{aligned}\phi_\gamma(v+w) = \gamma(v+w) = \gamma v + \gamma w = \phi_\gamma(v) + \phi_\gamma(w)\\ \phi_\gamma(cv) = \gamma(cv) = c\cdot(\gamma v) = c\cdot\phi_\gamma(v)\,.\end{aligned}$$

Die zugehörige Transformationsmatrix $T_{\phi_\gamma} = (c_{ji})$ ist gegeben durch die Koeffizienten der Bilder der Basiselemente :

$$\phi_\gamma(\gamma^{i-1}) = \sum_{j=1}^{n} c_{ji}\gamma^{j-1}\,, \quad i = 1, 2, \ldots, n\,.$$

Mittels $\mathrm{Irr}(\gamma, K)$ entsteht dann folgendes System:

$$\begin{array}{lcl}
\phi_\gamma(1) & = & \gamma \\
\phi_\gamma(\gamma) & = & \gamma^2 \\
 & \vdots & \ddots \\
\phi_\gamma(\gamma^{n-2}) & = & \gamma^{n-1} \\
\phi_\gamma(\gamma^{n-1}) & = & -a_0 - a_1\gamma - a_2\gamma^2 - \ldots - a_{n-1}\gamma^{n-1} \quad .
\end{array}$$

Die Spur einer quadratischen Matrix ist definiert durch die Summe ihrer Hauptdiagonalelemente. Betrachtet man obiges Gleichungssystem, so sind bis auf die letzte Zeile alle Koeffizienten der Hauptdiagonalen gleich Null. Es gilt daher:

$$Sp\,(T_{\phi_\gamma}) := \sum_{j=1}^{n} c_{jj} = -a_{n-1}\,.$$

Sind $A = (a_{ij})$ und $B = (b_{ij})$ zwei (n×n)-Matritzen, so ist die Spur ihrer Produkte gegeben durch

$$Sp\,(A \cdot B) = \sum_{i,j=1,2,\ldots,n} a_{ij} \cdot b_{ji} = Sp\,(B \cdot A)\,.$$

Damit folgt insbesondere für zwei (n×n)-Matritzen S und T, von denen mindestens S regulär sei:

$$Sp\,(S \cdot T \cdot S^{-1}) = Sp\,(S^{-1} \cdot S \cdot T) = Sp\,(T)\,.$$

Aus der Linearen Algebra ist bekannt, daß eine lineare Transformationsmatrix T beim Wechsel der Basis mittels einer geeigneten regulären Matrix S übergeht in die Form

$$T' = S \cdot T \cdot S^{-1}\,.$$

Daraus folgt aber insgesamt, daß sich beim Übergang zu einer anderen Basis die Spur nicht ändert.

Diese Theorie bietet nun die Grundlage dafür, folgende Aussage über die Struktur einer einfachen p-radikalischen Körpererweiterung zu treffen:

Satz 4.1 *Sei K ein Körper der Charakteristik q und $p \in \mathbb{N}$ eine davon verschiedene Primzahl. Ferner seien $x^p - r, x^p - s \in K[x]$ irreduzibel. Dann sind gleichwertig:*

(i) $\sqrt[p]{s} \in K[\sqrt[p]{r}]$

(ii) $K[\sqrt[p]{s}] = K[\sqrt[p]{r}]$

(iii) $\exists\, c \in K, \nu \in \{1, 2, \ldots, p-1\} : \sqrt[p]{s} = c \cdot \sqrt[p]{r}^{\,\nu}$.

Beweis: Die Behauptung wird durch Kreisschluß gezeigt:

$(iii) \Rightarrow (i)$:
Diese Richtung folgt unmittelbar, denn es gilt: $\sqrt[p]{s} = c \cdot \sqrt[p]{r}^{\,\nu} \in K[\sqrt[p]{r}]$.

$(i) \Rightarrow (ii)$:
Nach Voraussetzung ist $K[\sqrt[p]{s}]$ ein Teilkörper von $K[\sqrt[p]{r}]$. Da aber

$$[K[\sqrt[p]{r}] : K] = [K[\sqrt[p]{s}] : K] = p\,,$$

folgt sofort die Gleichheit der beiden Körper.

$(ii) \Rightarrow (iii)$:
Aus der vorausgesetzten Gleichheit folgt mit Satz 2.2 zunächst, daß $B_1 = \{1, \sqrt[p]{s}, \ldots, \sqrt[p]{s}^{\,p-1}\}$ und $B_2 = \{1, \sqrt[p]{r}, \ldots, \sqrt[p]{r}^{\,p-1}\}$ zwei Basen ein und desselben Körpers sind.

Überträgt man die eingangs beschriebene Theorie auf die vorliegende Situation, so folgt mit $\mathrm{Irr}(\sqrt[p]{s}, K) = x^p - s$:

$$Sp\,(T_{\phi\,\sqrt[p]{s}}) = 0\,.$$

Da $\sqrt[p]{s} \in K[\sqrt[p]{r}]$, existieren Koeffizienten in K, sodaß gilt:

$$\sqrt[p]{s} = c_0 + c_1\sqrt[p]{r} + \ldots + c_{n-1}\sqrt[p]{r}^{\,p-1}\,.$$

Damit kann die Transformationsmatrix $T_{\phi\,\sqrt[p]{s}}$ bezüglich der Basis B_2 aus den Koeffizienten des Gleichungssystems abgelesen werden, in dem $\phi_{\sqrt[p]{s}}$ auf die Basiselemente angewendet wird:

$$\begin{array}{lll}
\phi_{\sqrt[p]{s}}\,(1) & = \sqrt[p]{s} & = \quad c_0 + c_1\sqrt[p]{r} + \ldots + \; c_{p-2}\sqrt[p]{r}^{\,p-2} + c_{p-1}\sqrt[p]{r}^{\,p-1} \\
\phi_{\sqrt[p]{s}}\,(\sqrt[p]{r}) & = \sqrt[p]{s}\sqrt[p]{r} & = c_{p-1}r + c_0\sqrt[p]{r} + \ldots + \; c_{p-3}\sqrt[p]{r}^{\,p-2} + c_{p-2}\sqrt[p]{r}^{\,p-1} \\
 & \vdots & \vdots \\
\phi_{\sqrt[p]{s}}\,(\sqrt[p]{r}^{\,p-1}) & = \sqrt[p]{s}\sqrt[p]{r}^{\,p-1} & = \quad c_1 r + c_2\sqrt[p]{r} + \ldots + c_{p-1}r\sqrt[p]{r}^{\,p-2} + \quad c_0\sqrt[p]{r}^{\,p-1}.
\end{array}$$

Insbesondere folgt daraus für die Spur

$$Sp\,(T_{\phi\,\sqrt[p]{s}}) = p \cdot c_0\,.$$

Nun wurde aber gezeigt, daß die Spurabbildung basisunabhängig ist. Somit gilt insgesamt

$$0 = p \cdot c_0\,.$$

Da nach Voraussetzung p ungleich der Charakteristik des Körpers ist, folgt notwendigerweise $c_0 = 0$.

Damit besitzt jedes p-Radikal $\sqrt[p]{s} \in K[\sqrt[p]{r}]$ des Grundkörpers K eine Basisdarstellung durch B_2, deren absolutes Glied verschwindet:

$$\sqrt[p]{s} = c_1\sqrt[p]{r} + \ldots + c_{n-1}\sqrt[p]{r}^{\,p-1}\,.$$

Es sei nun angenommen, daß diese Summendarstellung aus mehr als einem von Null verschiedenen Summanden besteht:

$$\sqrt[p]{s} = \sum_{j=1}^{n} c_{\nu_j} \sqrt[p]{r}^{\nu_j} .$$

Darin sei $n > 1$, die Koeffizienten c_{ν_j} ungleich Null und die Indizes ν_j der Größe nach geordnet: $1 \leq \nu_1 < \nu_2 < \ldots < \nu_n \leq p-1$.

Aus der rechten Seite der Gleichung läßt sich nun $\sqrt[p]{r}^{\nu_1}$ aus der Summe herausziehen und durch Division auf die linke Seite bringen:

$$\omega := \frac{\sqrt[p]{s}}{\sqrt[p]{r}^{\nu_1}} = c_{\nu_1} + c_{\nu_2} \sqrt[p]{r}^{\nu_2 - \nu_1} + \ldots + c_{\nu_n} \sqrt[p]{r}^{\nu_n - \nu_1} .$$

Hierdurch ist dann die Basisdarstellung einer Nullstelle des Polynoms $x^p - \frac{s}{r^{\nu_1}} \in K[x]$ bezüglich B_2 gegeben. Damit ist $K[\omega]$ ein Teilkörper von $K[\sqrt[p]{r}]$. Es gilt mit Hilfe der Gradformel

$$p = [K[\sqrt[p]{r}] : K] = [K[\sqrt[p]{r}] : K[\omega]] \cdot [K[\omega] : K] ,$$

das heißt, das $[K[\omega] : K]$ ein natürlicher Teiler von p sein muß:

$$[K[\omega] : K] \in \{1, p\} .$$

Ist der Grad gleich 1, so wäre $\omega \in K$, was obiger Darstellung widerspricht. Also folgt, daß das irreduzible Polynom von ω über K den Grad p besitzt. Da ω eine Nullstelle von $x^p - \frac{s}{r^{\nu_1}} \in K[x]$ ist, muß dieses Polynom irreduzibel sein. Das bedeutet aber, daß ω ein p-Radikal über K ist und nach dem oben Gezeigten ein verschwindendes absolutes Glied in seiner Basisdarstellung bezüglich B_2 besitzen muß. Da dies mit $c_{\nu_1} \neq 0$ nicht der Fall ist, ist die oben gemachte Annahme zum Widerspruch geführt, es kann keine echte Summendarstellung von $\sqrt[p]{s}$ durch B_2 geben. Somit folgt nun schließlich, daß die Linearkombination von $\sqrt[p]{s}$ durch B_2 aus genau einem Summanden besteht:

$$\sqrt[p]{s} = c \sqrt[p]{r}^{\nu} .$$

Damit ist die Behauptung (iii) bewiesen.

Diese sehr übersichtliche Struktur der einfachen radikalischen Körpererweiterung vom Primzahlgrad läßt sich auch auf Erweiterungen beliebigen Grades über speziellen Körpern anwenden. Auf dem Weg dorthin soll zunächst die Zwischenkörperstruktur einer derartigen Erweiterung näher beleuchtet werden.

Satz 4.2 *Sei $K[\sqrt[n]{r}]$ eine einfache Radikalerweiterung des Körpers K, der alle n-ten Einheitswurzeln enthalte. Dann gibt es zu jedem $m \,|\, n$ genau einen Zwischenkörper L mit $K \subseteq| \; L \subseteq| \; K[\sqrt[n]{r}]$ vom Grad m über K. Dieser ist gegeben mit einer geeigneten m-ten Wurzel aus r durch $L = K[\sqrt[m]{r}]$.*

Beweis: Mit einem Teiler m von n und $k = \frac{n}{m}$ gilt:

$$(\sqrt[n]{r}^{\,k})^m - r = \sqrt[n]{r}^{\,n} - r = 0\,.$$

Damit ist $\sqrt[n]{r}^{\,k}$ Nullstelle des Polynoms $x^m - r \in K[x]$. Da $x^n - r \in K[x]$ als irreduzibel vorausgesetzt ist, gilt dies erst recht für $x^m - r$. Es existiert daher eine Wurzel $\sqrt[m]{r} := \sqrt[n]{r}^{\,k} \in K[\sqrt[n]{r}]$ mit

$$K \subseteq\mid K[\sqrt[m]{r}] \subseteq\mid K[\sqrt[n]{r}]$$

und

$$[K[\sqrt[m]{r}] : K] = m\,.$$

Sei nun L ein beliebiger Zwischenkörper $K \subseteq\mid L \subseteq\mid K[\sqrt[n]{r}]$ vom Grad m über K. Dann gilt zunächst:

$$K[\sqrt[n]{r}] = L[\sqrt[n]{r}]\,.$$

Mit $d = n$ existiert ein $d \in \mathbb{N}^*$, für das gilt: $\sqrt[n]{r}^{\,d} \in L$ und $d \mid n$. Setzt man d' als das Minimum aller d, so ist $\sqrt[n]{r}$ eine Nullstelle von $x^{d'} - \sqrt[n]{r}^{\,d'} \in L[x]$. Dann ist $d' = 1$ genau für den Fall $L = K[\sqrt[n]{r}]$. Andernfalls ist $d' > 1$. Hierzu werde angenommen, daß $x^{d'} - \sqrt[n]{r}^{\,d'}$ reduzibel ist über L. Dann folgt mit Satz 2.4:

$$\exists\, t \,|\, d', t < d'\ \exists\, s \in L:\ \sqrt[n]{r}^{\,td'} = s^{d'}$$

Unter Verwendung von Satz 2.3 ist damit

$$s = \xi\, \sqrt[n]{r}^{\,t} \in L$$

mit einem $\xi \in \mathrm{E}_{d'}(K) \subseteq \mathrm{E}_n(K)$, das nach Voraussetzung in K enthalten ist. Dann ist aber

$$\sqrt[n]{r}^{\,t} \in L\,,$$

was nach Konstruktion von d' nicht möglich ist. Somit ist die Annahme zum Widerspruch geführt und gezeigt, daß das Polynom $x^{d'} - \sqrt[n]{r}^{\,d'}$ in $L[x]$ irreduzibel ist. Es ist also

$$Irr(\sqrt[n]{r}, L) = x^{d'} - \sqrt[n]{r}^{\,d'}\,.$$

Mit Hilfe der Gradformel läßt sich dann schließen:

$$\begin{aligned} [L[\sqrt[n]{r}] : K] &= [L[\sqrt[n]{r}] : L] \cdot [L : K] \\ \Longrightarrow \qquad n &= d' \cdot m \\ \Longrightarrow \qquad d' &= \tfrac{n}{m} = k\,, \end{aligned}$$

und damit $\sqrt[n]{r}^{\,k} = \sqrt[m]{r} \in L$. Das bedeutet aber insgesamt, daß L und $K[\sqrt[m]{r}]$ gleich sind.

Diese Struktur des Zwischenkörperverbandes gestattet nun schließlich mit Satz 4.1 das Erfassen von Radikalen einer beliebigen einfachen Radikalerweiterung über speziellen Körpern.

Satz 4.3 *Sei $K[\sqrt[n]{r}]$ eine einfache Radikalerweiterung des Körpers K, der alle n-ten Einheitswurzeln enthalte. Ferner sei $x^m - s \in K[x]$ irreduzibel und $m \in \mathbb{N}$ mit $m \mid n$ nicht durch die Charakteristik von K teilbar. Dann gilt mit einer geeigneten m-ten Wurzel aus r:*

$$\sqrt[m]{s} \in K[\sqrt[n]{r}] \iff \exists\, c \in K[x],\ \nu \in \{1, 2, \ldots, m-1\} :\ \sqrt[m]{s} = c \cdot \sqrt[m]{r}^{\nu}.$$

Beweis: "$\Longleftarrow$": Es folgt unmittelbar $\sqrt[m]{s} = c \cdot \sqrt[m]{r}^{\nu} = c \cdot \sqrt[n]{r}^{\frac{n}{m}\nu} \in K[\sqrt[n]{r}]$.

"$\Longrightarrow$": Der Beweis wird induktiv über die Primfaktorzerlegung von m geführt.

Sei zu Beginn p ein Primteiler von m. Dann ist $\sqrt[m]{s}^{\frac{m}{p}}$ Nullstelle von $x^p - s$, das irreduzibel sein muß, da dies bereits für $x^m - s$ gilt. Mit Satz 4.1 und 4.2 gilt dann:

$$\exists\, c \in K,\ \nu \in \{1, 2, \ldots, p-1\} :\ \sqrt[m]{s}^{\frac{m}{p}} = c \cdot \sqrt[n]{r}^{\frac{n}{p}\nu}.$$

Im Induktionsschluß gelte für ein $k \mid m$, $k < m$ die Darstellung:

$$\exists\, c \in K,\ \nu \in \{1, 2, \ldots, p-1\} :\ \sqrt[m]{s}^{\frac{m}{k}} = c \cdot \sqrt[n]{r}^{\frac{n}{k}\nu}.$$

Sei q ein Primteiler von $\frac{m}{k}$. Dann sind $\sqrt[m]{s}^{\frac{m}{qk}}$ und $\sqrt[q]{c} \cdot \sqrt[n]{r}^{\frac{n\nu}{qk}}$ Nullstellen von

$$x^q - \sqrt[m]{s}^{\frac{m}{k}}.$$

Mit den Sätzen 2.5, sowie 4.1 und 4.2 folgt weiter:

$$\exists\, c' \in K,\ \mu \in \{0, 1, \ldots, p-1\} :\ \sqrt[q]{c} = c' \cdot \sqrt[n]{r}^{\frac{n\mu}{q}},$$

Also insgesamt mit Blick auf Satz 2.3:

$$\sqrt[m]{s}^{\frac{m}{qk}} = \xi \cdot c' \cdot \sqrt[n]{r}^{\frac{n\mu}{q}} \cdot \sqrt[n]{r}^{\frac{n\nu}{qk}} = \xi \cdot c' \cdot \sqrt[n]{r}^{\frac{n}{qk}(k\mu+\nu)} = \xi \cdot c' \cdot \sqrt[qk]{r}^{(k\mu+\nu)}.$$

Hierin ist $\xi \in \mathrm{E}_q(K) \subseteq \mathrm{E}_n(K)$ ein Grundkörperelement. Damit läßt sich die rechte Seite der Gleichung in der geforderten Darstellung schreiben, womit der Induktionsschluß gelungen ist.

Die allgemeinen Aussagen dieses Kapitels, insbesondere die des Satzes 4.1 spielen eine wichtige Rolle bei der Antwort auf die Frage, unter welchen Bedingungen ein Polynom $f(x)$ der Form (1.1) eine gewisse Galoisgruppe besitzt.

4.2 Strukturanalyse

Es wird nun untersucht, welcher Zusammenhang zwischen den Koeffizienten a und b der Polynome $f(x)$ einerseits und den möglichen Zerfällungskörpern Z_f und damit den Galoisgruppen $G(Z_f \mid \mathbb{Q})$ andererseits besteht.

Es sei $\mathbb{Q}'$ ein beliebiger Erweiterungskörper von $\mathbb{Q}$ und ζ eine primitive p-te Einheitswurzel.

Ist $x^p - c$ irreduzibel in $\mathbb{Q}'[\zeta][x]$, so muß es dies auch in $\mathbb{Q}'[x]$ sein. Ist umgekehrt das Polynom $x^p - c$ irreduzibel über $\mathbb{Q}'$, so kann in $\mathbb{Q}'[\zeta]$ keine seiner Nullstellen enthalten sein, da mit Satz 2.7 (i) gilt:

$$[\mathbb{Q}'[\zeta] : \mathbb{Q}'] \leq p - 1 < p = [\mathbb{Q}'[\sqrt[p]{c}] : \mathbb{Q}'] \,.$$

Somit kann $x^p - c$ über $\mathbb{Q}'[\zeta]$ nicht vollständig zerfallen und ist nach Satz 2.6 irreduzibel. Es gilt also insgesamt für alle $c \in \mathbb{Q}'$:

$$\begin{array}{rl} & x^p - c \text{ irreduzibel über } \mathbb{Q}' \\ \Longleftrightarrow & x^p - c \text{ irreduzibel über } \mathbb{Q}'[\zeta] \,. \end{array} \tag{4.1}$$

Sei nun eine beliebige p-te Wurzel ω des absoluten Gliedes b von $f(x)$ in $\mathbb{Q}'$ enthalten. Dann findet sich in Anlehnung an (3.7) unter Vorgabe einer konkreten Nullstelle α bzw. β mit Blick auf (2.1) ein β bzw. α mit

$$\alpha \cdot \beta = \omega \,.$$

Sind diese Nullstellen beide von Null verschieden, so folgt

$$\alpha \in \mathbb{Q}'[\beta] \;\wedge\; \beta \in \mathbb{Q}'[\alpha] \,. \tag{4.2}$$

Neben ω sei nun auch $\sqrt{d} \in \mathbb{Q}'$. Darüber hinaus seien zunächst α und β ungleich Null.

Ist das $x^p - \alpha^p$ reduzibel über $\mathbb{Q}'$, so besitzt dieses Polynom nach Satz 2.5 eine Nullstelle in $\mathbb{Q}'$. Ohne Einschränkung werde diese mit α im Sinne von (2.1) bezeichnet. Mit (4.2) folgt dann, daß auch eine Nullstelle β in $\mathbb{Q}'[\alpha] = \mathbb{Q}'$ enthalten und damit auch $x^p - \beta^p \in \mathbb{Q}'[x]$ reduzibel ist. Die umgekehrte Richtung folgt analog. Insgesamt gilt:

$$x^p - \alpha^p \text{ reduzibel über } \mathbb{Q}' \quad \Longleftrightarrow \quad x^p - \beta^p \text{ reduzibel über } \mathbb{Q}' \,.$$

Daraus folgt schließlich mit (4.1) und unter Verwendung von Satz 2.6 für jedes $\gamma \in \{\alpha, \beta\}$, sowie einer primitiven p-ten Einheitswurzel ζ:

$$x^p - \gamma^p \in \mathbb{Q}'[x] \left\{ \begin{array}{l} \text{reduzibel} \\ \text{irreduzibel} \end{array} \right. \quad \Longrightarrow \quad Z_f = \left\{ \begin{array}{l} \mathbb{Q}'[\zeta] \\ \mathbb{Q}'[\zeta, \gamma] \,. \end{array} \right. \tag{4.3}$$

Dieses gilt in eingeschränkter Form auch, wenn entweder α oder β gleich Null ist. Der Zerfällungskörper ist dann in gleicher Weise einzig durch das nichtverschwindende $\gamma \in \{\alpha, \beta\}$ bestimmt.

Fall 1:
Es sei nun vorausgesetzt, daß eine rationale p-te Wurzel aus b existiert, oder mit Satz 2.5 formuliert: b ist die p-te Potenz einer rationalen Zahl r. Dann zerfällt $f(x)$ über $\mathbb{Q}' := \mathbb{Q}[\sqrt{d}]$ mindestens in die Faktoren

$$(x^p - \alpha^p)(x^p - \beta^p) \in \mathbb{Q}'[x] \,.$$

Verknüpft man die Charakterisierung (4.3) des Zerfällungskörpers mit den Ergebnissen aus Kapitel 3, so folgt insgesamt mit einem beliebigen von Null verschiedenen $\gamma \in \{\alpha, \beta\}$:

$$\begin{array}{l} x^p - \gamma^p \text{ reduzibel über } \mathbb{Q}' \\ \Longrightarrow \quad G(Z_f \,|\, \mathbb{Q}) \cong \left\{ \begin{array}{ll} \mathbb{Z}_p^* & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \\ \mathbb{Z}_2 \times \mathbb{Z}_p^* & \text{falls } \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. ; \end{array}$$

$$\begin{array}{l} x^p - \gamma^p \text{ irreduzibel über } \mathbb{Q}' \\ \Longrightarrow \quad G(Z_f \,|\, \mathbb{Q}) \cong \left\{ \begin{array}{ll} \Lambda_p & \sqrt{d} \in \mathbb{Q} \\ \Lambda_p & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \ \wedge \ p \equiv \ 1 \mod 4 \\ \widetilde{\Lambda}_p & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \ \wedge \ p \equiv -1 \mod 4 \\ \mathbb{Z}_2 \times \Lambda_p & \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. . \end{array}$$

Fall 2:
Sei nun $x^p - b \in \mathbb{Q}[x]$ irreduzibel, sowie $\mathbb{Q}' := \mathbb{Q}[\sqrt[p]{b}, \sqrt{d}]$. Dann sind sowohl α als auch β ungleich Null, da sonst $\alpha^p \cdot \beta^p = b = 0$.

Zudem kann $\mathbb{Q}'$ als einfache Radikalerweiterung von $\mathbb{Q}[\sqrt{d}]$ aufgefaßt werden, denn es gilt:

$$[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] \leq 2 < p = [\mathbb{Q}[\sqrt[p]{b}] : \mathbb{Q}] \ , \quad \text{also} \quad \sqrt[p]{b} \notin \mathbb{Q}[\sqrt{d}] \, ,$$

und mit Satz 2.5 die Irreduzibilität von $x^p - b$ über $\mathbb{Q}[\sqrt{d}]$.

Unter Verwendung von (4.1) und Satz 2.7 (i), sowie der Charakterisierung (4.3) läßt sich dann über die Gradformel $[Z_f : \mathbb{Q}]$ berechnen und mit den Ergebnissen aus Kapitel 3 die Galoisgruppe $G(Z_f \mid \mathbb{Q})$ herleiten: Sei $\gamma \in \{\alpha, \beta\}$, dann gilt:

$$\begin{array}{l} x^p - \gamma^p \text{ reduzibel über } \mathbb{Q}' \\ \Longrightarrow \quad [Z_f : \mathbb{Q}] \ = \left\{ \begin{array}{ll} p \cdot (p-1) & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \\ 2p \cdot (p-1) & \text{falls } \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. \\ \Longrightarrow \quad G(Z_f \,|\, \mathbb{Q}) \cong \left\{ \begin{array}{ll} \Lambda_p & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \\ \mathbb{Z}_2 \times \Lambda_p & \text{falls } \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. ; \end{array}$$

$$\begin{array}{l} x^p - \gamma^p \text{ irreduzibel über } \mathbb{Q}' \\ \Longrightarrow \quad [Z_f : \mathbb{Q}] \ = \left\{ \begin{array}{ll} p^2 \cdot (p-1) & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \\ 2p^2 \cdot (p-1) & \text{falls } \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. \\ \Longrightarrow \quad G(Z_f \,|\, \mathbb{Q}) \cong \left\{ \begin{array}{ll} \Lambda_{p^2} & \sqrt{d} \in \mathbb{Q} \\ \widetilde{\Lambda}_{p^2} & \text{falls } \sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \\ \Lambda_{2p^2} & \sqrt{d} \notin \mathbb{Q}[\zeta] \end{array} \right. . \end{array}$$

Um die Irreduzibilität von $x^p - \gamma^p$ über $\mathbb{Q}'$ festzustellen, ist im allgemeinen erheblicher Rechenaufwand nötig. Daher soll es nun das Ziel

sein, dieses Irreduzibilitätskriterium analog zum Fall 1 auf $\mathbb{Q}[\sqrt{d}]$, also einer höchstens quadratischen Erweiterung von $\mathbb{Q}$ zu übertragen.

Es sei $x^p - \gamma^p$ reduzibel in $\mathbb{Q}'[x]$, das heißt mit Satz 2.5, es besitzt eine Nullstelle in $\mathbb{Q}'$. Diese werde ohne Einschränkung mit γ bezeichnet. Ist $x^p - \gamma^p$ auch reduzibel über $\mathbb{Q}[\sqrt{d}]$, folgt sogar $\gamma \in \mathbb{Q}[\sqrt{d}]$. Dann gibt es mit $\sqrt[p]{b}^{\,0} := 1$ ein $c \cdot \sqrt[p]{b}^{\,0} = \gamma \in \mathbb{Q}[\sqrt{d}]$. Ist aber $x^p - \gamma^p$ irreduzibel über $\mathbb{Q}[\sqrt{d}]$, so läßt sich Satz 4.1 anwenden. Verbunden mit dem zuvor Gezeigten gilt dann insgesamt:

$$\exists\, c \in \mathbb{Q}[\sqrt{d}],\ \nu \in \{0, 2, \ldots, p-1\} :\ \gamma = c \cdot \sqrt[p]{b}^{\,\nu}\,.$$

Mit Satz 2.5 folgt dann sofort

$$\frac{\gamma^p}{b^\nu} = c^p \quad \text{also} \quad x^p - \frac{\gamma^p}{b^\nu} \in \mathbb{Q}[\sqrt{d}][x] \ \text{ reduzibel.}$$

Ist umgekehrt $x^p - \frac{\gamma^p}{b^\nu}$ reduzibel über $\mathbb{Q}[\sqrt{d}]$, so gilt erneut mit Satz 2.5:

$$\exists\, c \in \mathbb{Q}[\sqrt{d}] :\ c^p = \frac{\gamma^p}{b^\nu}\,.$$

Dann ist

$$\gamma^p = c^p \cdot \left(\sqrt[p]{b}^{\,p}\right)^\nu = \left(c \cdot \sqrt[p]{b}^{\,\nu}\right)^p$$

mit

$$c \cdot \sqrt[p]{b}^{\,\nu} \in \mathbb{Q}'\,,$$

woraus sofort die Reduzibilität von $x^p - \gamma^p$ in $\mathbb{Q}'[x]$ folgt.

Insgesamt ist nun gezeigt, daß ein $\nu \in \{0, 1, \ldots, p-1\}$ existiert, sodaß gilt:

$$x^p - \gamma^p \text{ reduzibel über } \mathbb{Q}' \quad \Longleftrightarrow \quad x^p - \frac{\gamma^p}{b^\nu} \text{ reduzibel über } \mathbb{Q}[\sqrt{d}]\,.$$

Damit ist das oben formulierte Ziel erreicht. Darüber hinaus läßt sich für den Fall $\sqrt{d} \notin \mathbb{Q}$ das ν exakt bestimmen:

Es sei $x^p - \alpha^p$ und damit auch $x^p - \beta^p$ reduzibel in $\mathbb{Q}'[x]$. Einerseits liegen dann nach Satz 2.5 Nullstellen α, β in $\mathbb{Q}'$, andererseits gilt mit den Ergebnissen von oben $G(Z_f \mid \mathbb{Q}) \cong \Lambda_p$ oder $G(Z_f \mid \mathbb{Q}) \cong \mathbb{Z}_2 \times \Lambda_p$. Dies führt mit $\sqrt{d} \notin \mathbb{Q}$ zum Fall 2 der Kapitel 3.3 und 3.4. Daraus ist bekannt, daß $\mathrm{Irr}(\alpha, \mathbb{Q}) = f(x)$. Galoistheoretisch betrachtet heißt dies, daß ein Automorphismus $\sigma \in G(Z_f \mid \mathbb{Q})$ existiert, der α auf β abbildet. Weiter folgt

$$[\mathbb{Q}[\sqrt{d}] : \mathbb{Q}] = 2 < 2p = [\mathbb{Q}[\alpha] : \mathbb{Q}]\,, \quad \text{also} \quad \alpha \notin \mathbb{Q}[\sqrt{d}]\,.$$

Nach Satz 2.5 ist daher $x^p - \alpha^p \in \mathbb{Q}[\sqrt{d}][x]$ irreduzibel und somit, wie oben gezeigt, α von der Form

$$\alpha = \left(c_0 + c_1\sqrt{d}\right) \cdot \sqrt[p]{b}^{\,\nu} \in \mathbb{Q}'$$

für gewisse Koeffizienten $c_0, c_1 \in \mathbb{Q}$, sowie einem $\nu \in \{1, 2, \ldots, p-1\}$. Damit ist dann

$$\sigma(\alpha) = \left(c_0 + c_1 \cdot \sigma(\sqrt{d})\right) \cdot \left(\sigma(\sqrt[p]{b})\right)^{\nu} = \beta \in \mathbb{Q}' \,.$$

Mit Blick auf (3.6), sowie der Irreduzibilität von $x^p - b$ in $\mathbb{Q}[x]$ folgt

$$\sigma(\alpha) = \left(c_0 - c_1\sqrt{d}\right) \cdot \left(\zeta^{\mu}\sqrt[p]{b}\right)^{\nu} \in \mathbb{Q}' \,,$$

mit einem $\mu \in \{0, 1, \ldots, p-1\}$. Dieses muß aber gleich Null sein, da andernfalls die primitive p-te Einheitswurzel $\zeta^{\mu\nu}$ in $\mathbb{Q}'$ enthalten ist, womit $Z_f = \mathbb{Q}'$ gilt, was nicht möglich ist, da $[\mathbb{Q}' : \mathbb{Q}] \in \{p,\, 2p\}$. Daher folgt insgesamt

$$\beta = \left(c_0 - c_1\sqrt{d}\right) \cdot \sqrt[p]{b}^{\,\nu} \in \mathbb{Q}' \,.$$

Desweiteren ist

$$\alpha \cdot \beta = (c_0 + c_1\sqrt{d})(c_0 - c_1\sqrt{d}) \cdot \sqrt[p]{b}^{\,2\nu} = \underbrace{(c_0^2 - c_1^2 d)}_{\in \mathbb{Q}} \cdot \sqrt[p]{b}^{\,2\nu} \stackrel{!}{=} \sqrt[p]{b}$$

und daher

$$2\nu \equiv 1 \bmod p \,.$$

Das einzige $\nu \in \{1, 2, \ldots, p-1\}$, das diese Kongruenz erfüllt ist $\nu = \frac{p+1}{2}$. Damit folgt einerseits

$$\alpha = (c_0 + c_1\sqrt{d}) \cdot \sqrt[p]{b}^{\,\frac{p+1}{2}} \;; \quad \beta = (c_0 - c_1\sqrt{d}) \cdot \sqrt[p]{b}^{\,\frac{p+1}{2}}$$

und bezüglich der Ausgangsfrage für den Fall $\sqrt{d} \notin \mathbb{Q}$, daß das Gruppenkriterium wie folgt auf $\mathbb{Q}[\sqrt{d}]$ übertragen werden kann:

$$x^p - \gamma^p \text{ reduzibel über } \mathbb{Q}' \quad \Longleftrightarrow \quad x^p - \frac{\gamma^p}{b^{\frac{p+1}{2}}} \text{ reduzibel über } \mathbb{Q}[\sqrt{d}] \,.$$

Es sind nun abschließend sämtliche Zerfällungsmöglichkeiten diskutiert und der eingangs angestrebte Zusammenhang zwischen den Koeffizienten von $f(x)$ und den Galoisgruppen $G(Z_f \,|\, \mathbb{Q})$ hergestellt.

4.3 Bestimmung der Galoisgruppen

Trägt man die Ergebnisse der Strukturanalyse zusammen, so kann ein Polynom $f(x)$ der Form (1.1) über drei Kriterien K_1, K_2, K_3 mit seiner Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ verknüpft werden. Zum einen ist unabhängig voneinander folgendes zu prüfen:

$$K_1 \,:\, \sqrt{d} \begin{cases} \in \mathbb{Q} \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \\ \notin \mathbb{Q}[\zeta] \end{cases} \;; \quad K_2 \,:\, x^p - b \in \mathbb{Q}[x] \begin{cases} \text{reduzibel} \\ \text{irreduzibel} \end{cases} .$$

Darauf aufbauend ist schließlich zu untersuchen:

$$K_3(\gamma,\nu)\ :\ x^p-\frac{\gamma^p}{b^\nu}\in\mathbb{Q}[\sqrt{d}][x]\left\{\begin{array}{l}\text{reduzibel}\\ \text{irreduzibel}\end{array}\right. .$$

Hierin ist $\gamma\in\{\alpha,\beta\}$ ungleich Null. Für ν sind in Abhängigkeit von K_2 und K_1 folgende Werte einzusetzen:

$$x^p-b\in\mathbb{Q}[x]\left\{\begin{array}{ll}\text{reduzibel} & \Longrightarrow\ \nu=0\\ \text{irreduzibel}\ \wedge\ \sqrt{d}\ \left\{\begin{array}{ll}\in\mathbb{Q} & \Longrightarrow\ \nu=0,1,\ldots,p-1\\ \notin\mathbb{Q} & \Longrightarrow\ \nu=\frac{p+1}{2}\end{array}\right. & \end{array}\right. .$$

Hierbei liefert das Kriterium K_3 genau dann Irreduzibilität, wenn das entsprechende Polynom für alle in Frage kommenden ν irreduzibel ist.

Anhand der Ergebnisse dieser drei Kriterien ist dann die Galoisgruppe bis auf Isomorphie mit den Resultaten aus Kapitel 3 eindeutig festgelegt. Im folgenden wird dieser Zusammenhang kurz veranschaulicht:

K_1	K_2	K_3	$G(Z_f\,\vert\,\mathbb{Q})\cong\ldots$
$\sqrt{d}\in\mathbb{Q}$	reduzibel	reduzibel	$\mathbb{Z}_p^*$
$\sqrt{d}\in\mathbb{Q}$	reduzibel	irreduzibel	Λ_p
$\sqrt{d}\in\mathbb{Q}$	irreduzibel	reduzibel	Λ_p
$\sqrt{d}\in\mathbb{Q}$	irreduzibel	irreduzibel	Λ_{p^2}
$\sqrt{d}\in\mathbb{Q}[\zeta]\setminus\mathbb{Q}$	reduzibel	reduzibel	$\mathbb{Z}_p^*$
$\sqrt{d}\notin\mathbb{Q}[\zeta]$	reduzibel	reduzibel	$\mathbb{Z}_2\times\mathbb{Z}_p^*$
$\sqrt{d}\in\mathbb{Q}[\zeta]\setminus\mathbb{Q}$	irreduzibel	reduzibel	Λ_p
$\sqrt{d}\notin\mathbb{Q}[\zeta]$	irreduzibel	reduzibel	$\mathbb{Z}_2\times\Lambda_p$
$\sqrt{d}\in\mathbb{Q}[\zeta]\setminus\mathbb{Q}$	reduzibel	irreduzibel	Λ_p falls $p\equiv\ 1\mod 4$
$\sqrt{d}\in\mathbb{Q}[\zeta]\setminus\mathbb{Q}$	reduzibel	irreduzibel	$\widetilde{\Lambda}_p$ falls $p\equiv -1\mod 4$
$\sqrt{d}\notin\mathbb{Q}[\zeta]$	reduzibel	irreduzibel	$\mathbb{Z}_2\times\Lambda_p$
$\sqrt{d}\in\mathbb{Q}[\zeta]\setminus\mathbb{Q}$	irreduzibel	irreduzibel	$\widetilde{\Lambda}_{p^2}$
$\sqrt{d}\notin\mathbb{Q}[\zeta]$	irreduzibel	irreduzibel	Λ_{2p^2}

Tabelle 1

5 Sein oder nicht sein? – Existenzfragen

Tabelle 1 ist dahingehend vollständig, als sie sämtliche möglichen Resultate der Kriterien K_1, K_2 und K_3 erfaßt. Mit keinem Wort wurde jedoch auf die Frage eingegangen, ob all diese Ergebnisse überhaupt auftreten können. Dazu werden diese nun nacheinander untersucht und daraus Verfahren zur Erzeugung von Polynomen $f(x)$ mit einer gewissen Galoisgruppe $G(Z_f\,|\,\mathbb{Q})$ hergeleitet, sodaß zusätzlich die noch offenen Existenzfragen aus Kapitel 3 beantwortet werden können.

5.1 Irreduzibilitätskriterien

Das Wesen der Kriterien K_1, K_2 und K_3 liegt in der Frage nach der Irreduzibilität gewisser Polynome

$$x^p - c \in \mathbb{Q}[x] \text{ bzw. } \mathbb{Q}[\sqrt{d}][x]\,,$$

worin $p \in \mathbb{N}$ eine bestimmte Primzahl ist. Im folgenden werden hierfür Kriterien hergeleitet, die es gestatten, der Antwort ein wenig näher zu kommen.

Bei Reduzibilität liegt nach Satz 2.5 eine Nullstelle des Polynoms im Grundkörper. Eben durch Vorgabe einer solchen Nullstelle lassen sich derartige Polynome auch erzeugen.

Wie verhält es sich jedoch mit der Irreduzibilität? Betrachtet man Polynome $x^p - c \in \mathbb{Q}[x]$, worin $c = \frac{n}{m}$ mit $m \neq 0, n \in \mathbb{Z}$ vollständig gekürzt sei, so ist dieses Polynom genau dann irreduzibel über $\mathbb{Q}$, wenn n oder m keine p-te Potenz in $\mathbb{Z}$ ist, das heißt, es gibt eine Primzahl, deren höchstmöglicher Exponent in der Primfaktorzerlegung von n oder m nicht durch p teilbar ist.

Im allgemeinen ist jedoch $\mathbb{Z}[\sqrt{d}]$ mit einer beliebigen $\sqrt{d} \notin \mathbb{Q}$ kein Gaußscher Ring, sodaß diese Argumentation dort nicht greift. Ziel ist es nun, ein hinreichendes Kriterium für die Irreduzibilität spezieller Polynome $x^p - c$ über $\mathbb{Q}[\sqrt{d}]$ herzuleiten. Dem werden zunächst einige allgemeine Bemerkungen vorangestellt:

Ist $x^p - c \in \mathbb{Q}[\sqrt{d}][x]$ reduzibel, so sichert Satz 2.5 die Existenz eines $s = s_0 + s_1\sqrt{d}$ mit $s^p = c = c_0 + c_1\sqrt{d}$. Nun kann $\mathbb{Q}[\sqrt{d}]$ als Zerfällungskörper von $x^2 - d \in \mathbb{Q}[x]$ aufgefaßt werden und ist damit normal über $\mathbb{Q}$. Daher existiert die Galoisgruppe und darin ein Automorphismus σ, der $\sqrt{d}$ auf $-\sqrt{d}$ abbildet. Dann gilt:

$$\overline{c} = c_0 - c_1\sqrt{d} = \sigma(c) = \sigma(s^p) = (\sigma(s))^p = \left(s_0 - s_1\sqrt{d}\right)^p = \overline{s}^p\,.$$

Wendet man σ noch einmal an, so folgt insgesamt:

$$c = s^p \quad \Longleftrightarrow \quad \overline{c} = \overline{s}^p\,. \tag{5.1}$$

Somit liegt nun folgende Situation vor:

$$(x-s)\,|\,(x^p-c) \text{ und } (x-\overline{s})\,|\,(x^p-\overline{c}) \text{ in } \mathbb{Q}[\sqrt{d}][x]\,.$$

Multipliziert man beide Ausdrücke, so gilt auch

$$(x^2-2s_0x+s_0^2-s_1^2d)\mid(x^{2p}-2c_0x^p+c_0^2-c_1^2d) \text{ in } \mathbb{Q}[x]\,, \qquad (5.2)$$

womit gezeigt ist, daß $x^{2p}-2c_0x^p+c_0^2+c_1^2d$ reduzibel ist über $\mathbb{Q}$. Mit $c_1\neq 0$ läßt sich auch umgekehrt schließen, denn wenn x^p-c und damit auch $x^p-\overline{c}$ irreduzibel sind über $\mathbb{Q}[\sqrt{d}]$, so muß es ihr Produkt auch über $\mathbb{Q}$ sein, da beide Faktoren nicht in $\mathbb{Q}[x]$ enthalten sind und weitere Zerlegungen nach Voraussetzung nicht möglich sind. Damit ist gezeigt:

$$\begin{aligned} & x^p-(c_0+c_1\sqrt{d}) \quad \text{irreduzibel über } \mathbb{Q}[\sqrt{d}] \\ \Longleftrightarrow\ & x^{2p}-2c_0x^p+c_0^2-c_1^2d \quad \text{irreduzibel über } \mathbb{Q}\,. \end{aligned} \qquad (5.3)$$

Auf die soeben hergeleiteten Eigenschaften wird im Verlaufe dieses und des folgenden Kapitels noch zurückgegriffen.

Nun aber zu den angekündigten Spezifizierungen von $x^p-c\in\mathbb{Q}[\sqrt{d}]$: Darin sei zum einen $d=\frac{a^2}{4}-b\in\mathbb{Z}$ und $p\,|\,d$, zum anderen $c=c_0+c_1\sqrt{d}$ aus $\mathbb{Z}[\sqrt{d}]$. Ferner sei vorausgesetzt, daß in der Primfaktorzerlegung von d verschiedene Primzahlen höchstens in erster Potenz auftreten.

Ist nun x^p-c reduzibel über $\mathbb{Q}[\sqrt{d}]$, so überträgt sich diese Eigenschaft gemäß (5.2) auf $x^{2p}-2c_0x^p+c_0^2-c_1^2d\in\mathbb{Z}[x]$ über $\mathbb{Q}$. Aus der Algebra ist bekannt, daß diese Reduzibilität dann sogar über $\mathbb{Z}$ gilt (vgl. [1] S. 155). Damit folgt:

$$2s_0\in\mathbb{Z}\ \wedge\ s_0^2-s_1^2d\in\mathbb{Z} \quad\Longrightarrow\quad (2s_1)^2d\in\mathbb{Z}\,.$$

Da d quadratfrei ist, gilt $2s_1\in\mathbb{Z}$ und somit

$$2s=2s_0+2s_1\sqrt{d}\in\mathbb{Z}[\sqrt{d}][x]\,.$$

Mit $(2s_0+2s_1\sqrt{d})^p=(2s)^p=2^pc=2^pc_0+2^pc_1\sqrt{d}$ folgt unter Verwendung des binomischen Lehrsatzes:

$$2^pc_1=\sum_{j=0}^{\frac{p-1}{2}}\underbrace{\binom{p}{2j+1}(2s_0)^{p-2j-1}(2s_1)^{2j+1}d^j}_{\in\mathbb{Z}}\,.$$

Da $p\,|\,d$ vorausgesetzt ist, folgt mit $\binom{p}{1}=p$ insgesamt $p\,|\,2^pc_1$, und für ungerade Primzahlen p:

$$c_1\equiv 0 \bmod p\,. \qquad (5.4)$$

Wird dieses notwendige Kriterium verletzt, so folgt sofort die Irreduzibilität von x^p-c über $\mathbb{Q}[\sqrt{d}]$.

Aufbauend auf diesen Grundlagen lassen sich nun Polynome $f(x)$ mit gewissen Galoisgruppen $G(Z_f\,|\,\mathbb{Q})$ erzeugen.

5.2 Konstruktion bestimmter Polynome

Ein Polynom der Form (1.1) läßt sich durch seine Koeffizienten $a, b \in \mathbb{Q}$, aber auch durch zwei Werte $\alpha^p, \beta^p \in \mathbb{Q}[\sqrt{d}]$ eindeutig charakterisieren:

$$f(x) = x^{2p} + ax^p + b = (x^p - \alpha^p)(x^p - \beta^p)\,.$$

Sind α und β vorgegeben, so sind sie genau dann die Nullstellen eines Polynoms $f(x)$, wenn

$$\alpha^p \cdot \beta^p = b \in \mathbb{Q} \quad \wedge \quad \alpha^p + \beta^p = -a \in \mathbb{Q}\,.$$

Bei der Ermittlung der Galoisgruppe spielt nach den Ergebnissen aus Kapitel 4.3 neben b auch der Wert $d = \frac{a^2}{4} - b = \frac{1}{4}(\alpha^p - \beta^p)^2$ eine wichtige Rolle.

Fall 1:
Es werden zunächst die Möglichkeiten aus Tabelle 1 für $\sqrt{d} \in \mathbb{Q}$ untersucht. Dabei stehen aus Gründen der Übersichtlichkeit $s \neq 0$ und r für beliebige rationale Zahlen, die keine p-ten Potenzen sind.

Für $G(Z_f \mid \mathbb{Q}) \cong \mathbb{Z}_p^*$ ist dann notwendig und hinreichend, wenn gilt: $b = r^p$ und $\alpha^p = s^p$. Das zugehörige Polynom ist dann

$$f(x) = x^{2p} - \left(s^p + \left(\frac{r}{s}\right)^p\right) x^p + r^p\,.$$

Für $G(Z_f \mid \mathbb{Q}) \cong \Lambda_p$ bieten sich zwei Möglichkeiten an. Setzt man zum einen $b = r^p$, also K_2 reduzibel, so liefert K_3 die geforderte Irreduzibilität genau dann, wenn $\alpha^p = s$. Es gilt dann

$$f(x) = x^{2p} - \left(s + \frac{r^p}{s}\right) x^p + r^p\,.$$

Gibt man $b = r$ vor, so verlangt K_3 die Reduzibilität von $x^p - \frac{\alpha^p}{b^\nu}$ über $\mathbb{Q}$ für ein $\nu \in \{0, 1, \ldots, p-1\}$. Mit den Sätzen 4.1 und 2.5 ist dies genau dann der Fall, wenn

$$\exists c \in \mathbb{Q} \,:\, \alpha^p = c^p b^\nu\,.$$

Damit ergibt sich für $\alpha^p = s^p r^\nu$ mit einem beliebigen ν das gesuchte Polynom

$$f(x) = x^{2p} - \left(s^p r^\nu + \frac{r}{s^p r^\nu}\right) x^p + r\,.$$

Damit $G(Z_f \mid \mathbb{Q}) \cong \Lambda_{p^2}$, muß zum einen $b = r$, und zum anderen $x^p - \frac{\alpha^p}{r^\nu}$ für alle $\nu \in \{0, 1, \ldots, p-1\}$ irreduzibel über $\mathbb{Q}$ sein. Dies läßt sich zum Beispiel für ein zu $r \in \mathbb{Z}$ teilerfremdes $\alpha^p = s \in \mathbb{Z}$ erreichen. Das Polynom ist dann von der Form

$$f(x) = x^{2p} - \left(s + \frac{r}{s}\right) x^p + r\,.$$

Fall 2:
Es sei nun $\sqrt{d} \notin \mathbb{Q}$, sowie zunächst Reduzibilität in K_3 vorausgesetzt.

Ist b eine rationale p-te Potenz, so fordert K_3 die Existenz zweier Nullstellen $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$, die gemäß (5.1) von der Form

$$\alpha = c_0 + c_1\sqrt{d}, \quad \beta = c_0 - c_1\sqrt{d} \tag{5.5}$$

mit gewissen Koeffizienten $c_0, c_1 \in \mathbb{Q}$ sein müssen.

Dieses notwendige Kriterium ist im allgemeinen noch nicht hinreichend. Zwar ist mit beliebigen Werte $c_0, c_1, d' \in \mathbb{Q}$ mit $\sqrt{d'} \notin \mathbb{Q}$ durch analoge α und β ein Polynom der Form (1.1) festgelegt, da

$$\begin{aligned} & \alpha^p \cdot \beta^p \;\; = (c_0^2 - c_1^2 d')^p \in \mathbb{Q} \\ \wedge \;\; & \alpha^p + \beta^p = 2 \cdot \Big(c_0^p + \tbinom{p}{2} c_0^{p-2} c_1^2 \; d' + \ldots + \tbinom{p}{p-1} c_0 \; c_1^{p-1} \; d'^{\frac{p-1}{2}} \Big) \in \mathbb{Q} \,, \end{aligned}$$

allerdings folgt damit lediglich $\mathbb{Q}[\sqrt{d}] \subseteq\mid \mathbb{Q}[\sqrt{d'}]$. In der Regel liegt aber die geforderte Gleichheit der Körper vor, zum Beispiel für $c_0 = 0$ und $c_1 \neq 0$, sodaß sich unter Verwendung von (3.4) auf diese Weise Polynome mit folgenden Galoisgruppen erzeugen lassen:

$$G(Z_f \,|\, \mathbb{Q}) \cong \begin{cases} \mathbb{Z}_p^* & \text{falls } \; \exists c \in \mathbb{Q} : \; d' = (-1)^{\frac{p-1}{2}} c^2 p \\ \mathbb{Z}_2 \times \mathbb{Z}_p^* & \text{sonst} \,. \end{cases}$$

Ist b keine p-te Potenz in $\mathbb{Q}$, so gilt durch die vorausgesetzte Reduzibilität von K_3 mit den Ergebnissen aus Kapitel 4.2:

$$\alpha = (c_0 + c_1\sqrt{d}) \cdot \sqrt[p]{b}^{\,\frac{p+1}{2}} \,; \quad \beta = (c_0 - c_1\sqrt{d}) \cdot \sqrt[p]{b}^{\,\frac{p+1}{2}} \tag{5.6}$$

für gewisse Koeffizienten $c_0, c_1 \in \mathbb{Q}$. Gibt man umgekehrt derartige Werte $c_0, c_1, b', d' \in \mathbb{Q}$ mit $x^p - b', x^2 - d'$ irreduzibel in $\mathbb{Q}[x]$ vor, so wird durch α und β mit

$$\begin{aligned} & \alpha^p \cdot \beta^p \;\; = b'^{p+1} \cdot (c_0^2 - c_1^2 d')^p \in \mathbb{Q} \\ \wedge \;\; & \alpha^p + \beta^p = 2 \cdot b'^{\frac{p+1}{2}} \cdot \Big(c_0^p + \tbinom{p}{2} c_0^{p-2} c_1^2 \; d' + \ldots + \tbinom{p}{p-1} c_0 \; c_1^{p-1} \; d'^{\frac{p-1}{2}} \Big) \in \mathbb{Q} \end{aligned}$$

ein Polynom $f(x)$ erzeugt. Es gilt dann jedoch analog zu oben lediglich $\mathbb{Q}[\zeta, \sqrt[p]{b}, \sqrt{d}] \;\subseteq\mid\; \mathbb{Q}[\zeta, \sqrt[p]{b'}, \sqrt{d'}]$. Die geforderte Gleichheit liegt aber auch hier in den meisten Fällen vor, unter anderem für $c_0 = 0, c_1 \neq 0$. Es folgt dann mit (3.4):

$$G(Z_f \,|\, \mathbb{Q}) \cong \begin{cases} \Lambda_p & \text{falls } \; \exists c \in \mathbb{Q} : \; d' = (-1)^{\frac{p-1}{2}} c^2 p \\ \mathbb{Z}_2 \times \Lambda_p & \text{sonst} \,. \end{cases}$$

Fall 3:
Es verbleibt noch die Untersuchung für $\sqrt{d} \notin \mathbb{Q}$, wenn K_3 Irreduzibilität liefert. Um letzteres sichern zu können, soll auf (5.4) zurückgegriffen werden.

Sei zunächst $b = r^p$ eine rationale p-te Potenz und damit das Polynom in K_2 als reduzibel vorausgesetzt. Mit einem ganzzahligem $d' = p \cdot q_1 \cdot \ldots \cdot q_n$, worin $p, q_1, \ldots, q_n$ paarweise verschiedene Primzahlen sind, gelte $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$. Nach Satz 4.1 ist dies gleichwertig zu

$$\exists\, c \in \mathbb{Q} : d = c^2 d' = \left(\frac{a}{2}\right)^2 - r^p \,.$$

Da $p-1$ gerade ist, findet sich für jedes rationale Quadrat s^2 ein $t = \frac{s}{r^{\frac{p-1}{2}}} \in \mathbb{Q}$, sodaß

$$s^2 = t^2 r^{p-1} \,.$$

Daher existieren $u, v \in \mathbb{Q}$ mit

$$\begin{aligned} d = u^2 r^{p-1} d' &= v^2 r^{p-1} - r^p \\ \Longrightarrow \qquad u^2 d' &= v^2 - r \\ \Longrightarrow \qquad r &= v^2 - u^2 d' \,. \end{aligned}$$

Umgekehrt ist hiermit für beliebige $u, v \in \mathbb{Q}^*$ sowohl $\sqrt{d} \notin \mathbb{Q}$ als auch $b = r^p$. Darüber hinaus fordert K_3 die Irreduzibilität von

$$x^p - \alpha^p = x^p - \left(\pm v r^{\frac{p-1}{2}} + u r^{\frac{p-1}{2}} \sqrt{d'}\right)$$

über $\mathbb{Q}[\sqrt{d'}]$. Sind u und v ganzzahlig, so greift (5.4):

$$u r^{\frac{p-1}{2}} \equiv u v^{p-1} \not\equiv 0 \bmod p \,,$$

und damit

$$u \not\equiv 0 \bmod p \quad \wedge \quad v \not\equiv 0 \bmod p \,.$$

Man erhält so die geforderte Irreduzibilität durch Vorgabe zweier Werte $u, v \in \mathbb{Z}^*$, die nicht durch p teilbar sind. Es ergibt sich dann das Polynom

$$f(x) = x^{2p} \pm 2v(v^2 - u^2 d')^{\frac{p-1}{2}} x^p + (v^2 - u^2 d')^p \,.$$

Unter Verwendung von (3.4) folgt dann in Abhängigkeit von d':

$$G(Z_f \,|\, \mathbb{Q}) \cong \begin{cases} \Lambda_p & \text{falls} \quad d' = p \quad \wedge \quad p \equiv 1 \mod 4 \\ \widetilde{\Lambda}_p & \text{falls} \quad d' = -p \quad \wedge \quad p \equiv -1 \mod 4 \\ \mathbb{Z}_2 \times \Lambda_p & \text{sonst} \,. \end{cases}$$

Es sei nun $x^p - b$ irreduzibel über $\mathbb{Q}$ und d' wie zuvor angesetzt. Mit zwei Werten $u, v \in \mathbb{Z}$ seien

$$\alpha^p = u + v\sqrt{d'}, \quad \beta^p = u - v\sqrt{d'} \in \mathbb{Z}[\sqrt{d'}][x]$$

und damit

$$b = u^2 - v^2 d',\ a = -2u \in \mathbb{Z} \,.$$

Daher sind u und v so zu wählen, daß b keine p-te Potenz in $\mathbb{Q}$ ist. Dies ist bei beliebigen Werten in der Regel der Fall, im allgemeinen zum Beispiel für $u = v \neq \mid 1 - d' \mid$ ungleich einer rationalen p-ten Potenz. Mit Satz 4.1 folgt $\mathbb{Q}[\sqrt{d'}] = \mathbb{Q}[\sqrt{d}]$, sodaß die durch K_3 geforderte Irreduzibilität von

$$x^p - \frac{\alpha^p}{b^{\frac{p+1}{2}}} \in \mathbb{Q}[\sqrt{d}][x]$$

gleichwertig in $\mathbb{Q}[\sqrt{d'}][x]$ auf

$$x^p - b^p \cdot \frac{\alpha^p}{b^{\frac{p+1}{2}}} = x^p - b^{\frac{p-1}{2}} \cdot \left(u + v\sqrt{d'}\right) \in \mathbb{Z}[\sqrt{d'}][x]$$

übertragen werden kann. Dies läßt sich nach (5.4) realisieren für

$$b^{\frac{p-1}{2}} v = (u^2 - v^2 d')^{\frac{p-1}{2}} v \not\equiv 0 \bmod p\,.$$

Daraus folgt mit $p \mid d'$:

$$u^{p-1} v \not\equiv 0 \bmod p\ ,$$

das heißt

$$u \not\equiv 0 \bmod p \quad \wedge \quad v \not\equiv 0 \bmod p\,.$$

So ergibt sich schließlich für zwei zu p teilerfremden Zahlen $u, v \in \mathbb{Z}^*$, für die $u^2 - v^2 d'$ keine rationale p-te Potenz ist, ein Polynom

$$f(x) = x^{2p} - 2ux^p + u^2 - v^2 d'\ ,$$

für das mit Blick auf (3.4) gilt:

$$G(Z_f \mid \mathbb{Q}) \cong \begin{cases} \tilde{\Lambda}_{p^2} & \text{falls } d' = (-1)^{\frac{p-1}{2}} p \\ \Lambda_{2p^2} & \text{sonst}\,. \end{cases}$$

Es sind nun sämtliche möglichen Resultate der Kriterien K_1, K_2 und K_3 aus Tabelle 1 untersucht. Anhand der Konstruktion zugehöriger Polynome ist damit nicht nur gezeigt, daß all diese Fälle auftreten, sondern auch die Existenz sämtlicher in Kapitel 3 diskutierter Galoisgruppen bewiesen.

6 Computerimplementierung

Die Ergebnisse des letzten Kapitels haben gezeigt, daß das vorgestellte Verfahren zur Bestimmung der Galoisgruppe neben seiner Vollständigkeit keine überflüssigen Fälle beinhaltet. Im folgenden wird gezeigt, wie sich dieses Verfahren nebst Berechnung der Galoisgruppen in Form von Permutationsgruppen unter *Maple V, Release 4* installieren läßt. Die nachstehende Abbildung gibt dazu einen Überblick über die Programmstruktur. Ihr kann die Hierarchie der Prozeduren entnommen werden:

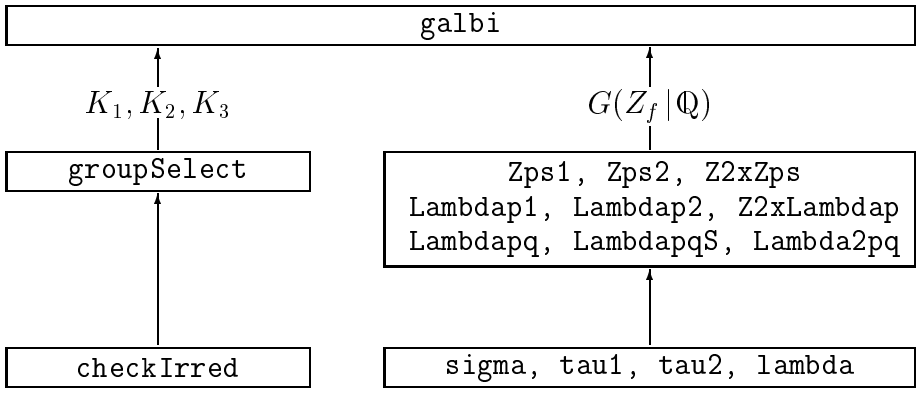

Abbildung 1 : Programmstruktur

Das Listing hierzu befindet sich am Ende dieses Kapitels.

6.1 Die Prozedur `galbi(p,a,b)`

`galbi(p,a,b)`wird von außen durch den Benutzer unter Übergabe der Parameter a, b und p des Polynoms $f(x)$ aufgerufen. Sie kann als Schaltzentrale interpretiert werden, die den Aufruf der weiteren Prozeduren steuert und entspricht in grober Form den Algorithmus zur Bestimmung der Galoisgruppe:

Zunächst wird untersucht, ob p eine gerade Primzahl ist und ob als Galoisgruppe die Einheitsgruppe vorliegt. Ist beides nicht der Fall, so werden durch `groupSelect` die Ergebnisse der Kriterien K_1, K_2, K_3 bestimmt und in der Variablen K wie folgt hinterlegt:

$$\sqrt{d} \quad \begin{cases} = 0 \\ \in \mathbb{Q}^* \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \ \wedge \ p \equiv -1 \bmod 4 \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} \ \wedge \ p \equiv 1 \bmod 4 \\ \notin \mathbb{Q}[\zeta] \end{cases} \quad \Longrightarrow \quad K[1] = \begin{cases} 0 \\ 2 \\ 1 \\ 3 \\ 4 \end{cases}$$

$$K_2, K_3 \begin{cases} \text{reduzibel} \\ \text{irreduzibel} \end{cases} \quad \Longrightarrow \quad K[2], K[3] = \begin{cases} 0 \\ 1\,. \end{cases}$$

Darin sei ζ eine primitive p-te Einheitswurzel über $\mathbb{Q}$.

Unter Verwendung dieser Ergebnisse ist mit Blick auf Tabelle 1 die zugehörige Galoisgruppe bis auf Isomorphie festgelegt. Ihre exakte Berechnung als Permutationsgruppe erfolgt darauf aufbauend in den entsprechenden Prozeduren. Schließlich folgt die Ausgabe der Gruppe nach folgendem Muster:

$$\text{Gruppenordnung}, \text{Kommutativität}, \{\text{Basis}\}$$

Ist die Gruppe kommutativ, so wird dieses durch ein + zum Ausdruck gebracht, ansonsten tritt ein − auf.

6.2 Die Prozedur `groupSelect(p,a,b)`

Die Untersuchung von K_1, K_2, K_3 in `groupSelect(p,a,b)` basiert auf der in *Maple V, Release 4* implementierten Prozedur `irreduc(p)`, die die Irreduzibilität eines Polynoms

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

über $\mathbb{Q}[a_0, a_1, \ldots, a_n]$ bestimmt. Die Ergebnisse aller drei Kriterien werden als Liste zurückgegeben.

Das Ergebnis von K_1 wird mit Hilfe von (3.4) wie folgt bestimmt:

$$\sqrt{d} \begin{cases} = 0 & \iff d = 0 \\ \in \mathbb{Q} & \iff x^2 - d \text{ reduzibel über } \mathbb{Q} \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} & \iff x^2 - \frac{d}{(-1)^{\frac{p-1}{2}} \cdot p} \text{ reduzibel über } \mathbb{Q}\,. \end{cases}$$

Tritt keiner dieser Fälle ein, so gilt $\sqrt{d} \notin \mathbb{Q}[\zeta]$.

Für die Bestimmung von K_3 ist im Fall, daß $\sqrt{d}$ rational ist, zu beachten, daß $\gamma^p \in \{\alpha^p, \beta^p\}$ von Null verschieden sein muß. Zu seiner Berechnung wird folgende Eigenschaft herangezogen: Für ungerade Primzahlen $p \in \mathbb{N}$ gilt in beliebigen Körpern K:

$$\omega \text{ Nullstelle von } x^p - r \in K[x] \iff -\omega \text{ Nullstelle von } x^p + r \in K[x]\,.$$

Mit Satz 2.5 folgt daraus:

$$x^p - r \text{ irreduzibel in } K[x] \iff x^p + r \text{ irreduzibel in } K[x]\,.$$

Damit spielt das Vorzeichen bei der Frage nach der Irreduzibilität reiner Polynome von ungeradem Primzahlgrad keine Rolle. In K_3 kann daher der Wert

$$\gamma^p = \frac{|a|}{2} + \sqrt{d} \in \{\pm\alpha^p, \pm\beta^p\}$$

verwendet werden. Dieser ist stets von Null verschieden, da zum einen der Fall $a = b = 0$ in `galbi` zuvor ausgeklammert wurde, und zum

anderen *Maple* für reellwertige $\sqrt{d}$ stets mit der nichtnegativen Wurzel arbeitet.

Die Kriterien K_2 und K_3 lassen sich mit `irreduc` wörtlich unter *Maple* implementieren. Man stellt aber sehr schnell fest, daß dies nicht praktikabel ist, da die Rechenzeiten schon für relativ kleine Primzahlen (> 100) sehr groß werden können. Dies hat folgende Ursachen:

- `irreduc` benötigt deutlich mehr Zeit in komplexen Erweiterungen von $\mathbb{Q}$, als in reellen Erweiterungen.
- Der Ausdruck in K_3 wächst mit den Primzahlen exponentiell und erschwert so die Auswertung durch `irreduc`.

Ist $x^p - c$ aus $\mathbb{Q}[x]$, so nutzt *Maple* die einfache Struktur der reinen Polynome und beantwortet mit geringem Zeitaufwand die Frage nach der Irreduzibilität. Damit beziehen sich die angeführten Probleme auf das Kriterium K_3 für den Fall, daß $\sqrt{d}$ nicht rational ist. Der zweiten Ursache kann dadurch beigekommen werden, daß K_3 auf die Frage nach der Irreduzibilität von

$$x^p - \left(\frac{\alpha}{\beta}\right)^p \in \mathbb{Q}[\sqrt{d}][x]$$

übertragen wird. Dies ist aus folgenden Gründen gleichwertig zum ursprünglichen Kriterium: ist dieses Polynom reduzibel, so gilt mit

$$\left(\frac{\alpha}{\beta}\right)^p = \frac{\alpha^{2p}}{b}\,,$$

daß auch

$$x^p - \left(\frac{\alpha^{2p}}{b}\right)^{\frac{p+1}{2}} = x^p - (\alpha^p)^p\,\frac{\alpha^p}{b^{\frac{p+1}{2}}} \in \mathbb{Q}[\sqrt{d}][x]$$

reduzibel ist. Dies läßt sich vereinfachen, indem die p-ten Potenzen $(\alpha^p)^p$ und gegebenenfalls auch b entfernt werden. Es verbleibt dann das Polynom aus K_3. Liefert umgekehrt K_3 Reduzibilität, so kann mit den Strukturen (5.5) und (5.6) sofort abgelesen werden, daß dann auch $x^p - \frac{\alpha^p}{\beta^p}$ reduzibel ist über $\mathbb{Q}[\sqrt{d}]$.

Hierauf aufbauend kann auch dem ersten Problem entgegengewirkt werden. Ziel dazu ist es nun, die nichtrationale Quadratwurzel aus d aus den Betrachtungen zu eliminieren. Dies gelingt auf zweierlei Arten: Zum einen kann die Frage nach Irreduzibilität gleichwertig auf ein Polynom mit rationalen Koeffizienten übertragen werden. Hierzu wird auf (5.3) zurückgegriffen. Es folgt dann:

$$\begin{aligned} & x^p - \left(\tfrac{\alpha}{\beta}\right)^p = x^p - \tfrac{(\alpha^p)^2}{b} && \text{irreduzibel über } \mathbb{Q}[\sqrt{d}] \\ \Longleftrightarrow\quad & x^{2p} - \left(\tfrac{a^2}{b} - 2\right) x^p + 1 && \text{irreduzibel über } \mathbb{Q}\,. \end{aligned}$$

Bei reellwertigen Erweiterungen $\mathbb{Q}[\sqrt{d}]$ ist keine Veränderung des Zeitaufwandes zu erkennen, obwohl die sehr einfache Struktur der reinen Polynome verloren geht. Gleichwohl ist dieser aber nun unabhängig davon, ob $\sqrt{d}$ komplexwertig ist, dennoch immer noch merklich höher als im Fall $\sqrt{d} \in \mathbb{Q}$.

Um aus diesen Gründen `irreduc` zu entlasten, wird diesem Befehl der "Filter" `checkIrred` vorangeschaltet, der deutlich schneller arbeitet. Hierin wird folgende Überlegung ausgenutzt: Ist das Polynom

$$x^{2p} - \left(\frac{a^2}{b} - 2\right) x^p + 1 = \left(x^p - \left(\frac{\alpha}{\beta}\right)^p\right) \cdot \left(x^p - \left(\frac{\beta}{\alpha}\right)^p\right)$$

reduzibel über $\mathbb{Q}$, so ist dies durch (5.1) und (5.3) gleichbedeutend damit, daß die Polynome

$$x^p - \left(\frac{\alpha}{\beta}\right)^p \,,\; x^p - \left(\frac{\beta}{\alpha}\right)^p$$

reduzibel sind über $\mathbb{Q}[\sqrt{d}]$. Nun läßt sich $\sqrt{d}$ dadurch beseitigen, daß diese Polynome unter einem gewissen Modul q, wobei $q \in \mathbb{N}$ eine Primzahl sei, betrachtet wird. Ist nämlich d quadratischer Rest modulo q, das heißt, die Kongruenz $x^2 - d \equiv 0$ modulo q ist lösbar, so gilt:

$$x^p - \left(\frac{\alpha}{\beta}\right)^p \,,\; x^p - \left(\frac{\beta}{\alpha}\right)^p \in \mathbb{Z}_q[x] \,.$$

Ein derartiges Polynom besitzt nun wieder eine sehr einfache Struktur und kann von *Maple* mittels der Prozedur `Irreduc mod q` merklich schnell gegenüber anderen Polynomen auf Irreduzibilität überprüft werden. Ist das Polynom irreduzibel über $\mathbb{Z}_q$, so muß es dies auch über $\mathbb{Q}$ sein, denn andernfalls ließe sich ein Linearfaktor in $\mathbb{Q}[x]$ abspalten und diese Zerlegung würde auch in $\mathbb{Z}_q[x]$ existieren. Allerdings gilt die Umkehrung im allgemeinen nicht. In aller Regel und bei beliebiger Wahl der Koeffizienten a und b liegt aber Irreduzibilität vor, sodaß diese Überlegung eine große Anzahl an Polynomen im Vorfeld abfangen kann und vor der zeitintensiven Prozedur `irreduc` schützt. Bei der Umsetztung in `checkIrred` stellen sich die Fragen, wieviele und welche Moduln q anzuwenden sind. Letzterem hilft der folgende

Satz 6.1 *Es sei $q \in \mathbb{N}$ eine Primzahl mit $q \geq m \in \mathbb{N}$. Dann gilt: Durchläuft c die Zahlen $1, 2, \ldots, q-1$, so nehmen die Potenzen c^m genau $\frac{q-1}{ggT(m,q-1)}$ paarweise inkongruente Werte an.*

Beweis: Bezeichne n den $\mathrm{ggT}(m, q-1)$ und n' seinen Komplementärteiler bezüglich m. Ferner sei $\overline{c}^{\,m}$ eine beliebige aber fest gewählte m-te Potenz einer Zahl $\overline{c} \in \{1, 2, \ldots, q-1\}$. Dann gilt zunächst

$$c^m \equiv \overline{c}^{\,m} \bmod q \quad \Longleftrightarrow \quad \left(\left(c \cdot \overline{c}^{\,-1}\right)^n\right)^{n'} \equiv 1 \bmod q \,.$$

Da n' und $q-1=\varphi(q)$ teilerfremd sind, folgt äquivalent:

$$\left(c\cdot\overline{c}^{-1}\right)^n \equiv 1 \bmod q\,.$$

Diese Kongruenz wird durch genau die $r\in\mathbb{Z}_p^*$ erfüllt, deren Ordnung $d=\mathrm{Ord}_{\mathbb{Z}_p^*}r$ ein Teiler von $n\leq\varphi(p)$ ist. Zu jedem d gibt es rückblickend auf Satz 2.9 genau $\varphi(d)$ Elemente dieser Ordnung. Zieht man noch (2.5) hinzu, so gibt es insgesamt n modulo q paarweise inkongruente Werte für r. Diese seien mit $r_1, r_2, \ldots, r_n$ bezeichnet. Daraus folgt nun insgesamt:

$$c^m \equiv \overline{c}^m \bmod q \quad\Longleftrightarrow\quad \exists\nu\in\{1,2,\ldots,n\}:\ c\equiv r_\nu\cdot\overline{c} \bmod q\,.$$

Hierdurch zerfällt $\{1,2,\ldots,q-1\}$ in genau $\frac{q-1}{n}$ paarweise disjunkte Teilmengen, die jeweils dadurch gekennzeichnet sind, daß die m-ten Potenzen ihrer Elemente kongruent modulo q sind. Gleichzeitig sind aber die m-ten Potenzen von Elementen verschiedener Teilmengen paarweise inkongruent modulo q.

Somit ist gezeigt, daß die m-ten Potenzen der Zahlen $1,2,\ldots,q-1$ genau $\frac{q-1}{n}$ paarweise modulo q inkongruente Werte liefern.

Will man die Irreduzibilität von $x^p-c\in\mathbb{Z}_q[x]$ zeigen, so ist dies mit Satz 2.5 gleichwertig dazu, daß c keine p-te Potenz in $\mathbb{Z}_q$ ist. Sind p und $q-1$ teilerfremd, so ist c nach dem soeben Gezeigten stets eine p-te Potenz in $\mathbb{Z}_q$. Da p eine Primzahl ist, bleibt als Alternative nur $\mathrm{ggT}(p,q-1)=p$, das heißt $p\mid q-1$. Daher werden in `checkIrred` nur derartige Moduln q herangezogen. Ihre Existenz wird durch den Primzahlsatz von Dirichlet (vgl. [5] S. 176ff.) gesichert. Bei der Berechnung von q ist zusätzlich zu beachten, daß der Koeffizient $\frac{a^2}{b}-2$ modulo q existiert, ein Aspekt, der einen Modul gerade bei sehr kleinen Primzahlen unbrauchbar machen kann.

Die Anzahl dieser Moduln ist ein Maß für die Sicherheit, mit der ein irreduzibles Polynom $x^p-c\in\mathbb{Z}_q[x]$ von `checkIrred` erfaßt wird. Aus der Zahlentheorie ist bekannt, daß sich in $\{1,2,\ldots,q-1\}$ genausoviele quadratische Reste, wie Nichtreste modulo q befinden (vgl. [5] S. 91). Weiter wird die Irreduzibilität aber erst dann festgestellt, wenn c nicht kongruent zu einer der $\frac{q-1}{p}$ verschiedenen p-ten Potenzen modulo q ist. Eine durchschnittliche Anzahl an Moduln ist folgenden Tests mit jeweils 10000 zufällig ausgewählten, irreduziblen Polynomen der Form $x^{2p}-\left(\frac{a^2}{b}-2\right)x^p+1$ zu entnehmen:

p:	3	5	7	11	...	59	...	101	...	251	...	401
$\#q$:	3.24	2.63	2.37	2.28		2.03		2.02		2.02		2.02

Aus diesen Werten ist ersichtlich, daß durch die maximal 30 Moduln in `checkIrred` verhältnismäßig oft Irreduzibilität nachgewiesen wird.

Allerdings kann nicht garantiert werden, daß sich gewisse irreduzible Polynome dieses Zugriffs verweigern, sodaß schließlich doch auf `irreduc` zurückgegriffen werden muß. Dies ist erst recht bei Reduzibilität der Fall, wobei der "verlorene" Zeitaufwand durch `checkIrred` relativ gering ist.

6.3 Galoisgruppen vs. Permutationsgruppen

In Tabelle 1 ist die Galoisgruppe $G(Z_f \,|\, \mathbb{Q})$ bis auf Isomorphie festgelegt. Was aber bedeutet konkret die Galoisgruppe einer Gleichung?

Es sei K ein beliebiger Körper und $p\,(x) \in K[x]$ ein Polynom n-ten Grades ohne mehrfache Wurzeln $\omega_1, \omega_2, \ldots, \omega_n$. Diese erzeugen nach Satz 2.2 (v) den Zerfällungskörper Z_p. Jedes $\sigma \in G(Z_p \,|\, K)$ ist eindeutig durch die Bilder aller ω_j festgelegt, genauer: jedes σ permutiert die Elemente ω_j. Daher kann $G(Z_p \mid K)$ als Permutationsgruppe einer Menge von n Elementen aufgefaßt werden. Vereinfachend betrachtet man die Galoisgruppe als Permutationsgruppe der Indizes j der ω_j, die die Elemente $1, 2, \ldots, n$ permutiert.

Hieraus lassen sich weitere Informationen über das zugrundeliegende Polynom ableiten. Sei $q(x)$ ein in K irreduzibler Faktor von $p\,(x)$. Bei geeigneter Umnumerierung sind $\omega_1, \omega_2, \ldots, \omega_m$ seine Nullstellen. Nun permutiert einerseits jedes $\sigma \in G(Z_p \,|\, K)$ diese Wurzeln nur unter sich, auf der anderen Seite existiert aber auch zu je zwei Nullstellen ein Automorphismus, der beide ineinander überführt. Eine deratig abgeschlossene Teilmenge wird als Transitivitätsgebiet bezeichnet.

Es ist ersichtlich, daß damit die Zahlen $1, 2, \ldots, n$ durch $G(Z_p \,|\, K)$ in elementfremde Transitivitätsgebiete zerlegt werden. Diese stehen umkehrbar eindeutig in Beziehung zu der Zerlegung von $p\,(x)$ in irreduzible Faktoren über K.

Davon ausgehend stellen sich bezogen auf $f(x)$ folgende Fragen:

- Wieviel paarweise verschiedene Nullstellen besitzt $f(x)$?
- Welchen Effekt besitzen die Elemente aus $G(Z_f \mid \mathbb{Q})$ auf diese Wurzeln?

Die erste Frage läßt sich direkt beantworten unter dem Gesichtspunkt, wann sind zwei Nullstellen gleich? Mit Blick auf die Nullstellen (2.4) gilt für verschiedene $\nu, \mu \in \{0, 1, \ldots, p-1\}$ zum einen

$$\zeta_p^{\nu}\alpha = \zeta_p^{\mu}\alpha \quad \Longleftrightarrow \quad \alpha\left(\zeta_p^{\nu} - \zeta_p^{\mu}\right) = 0 \quad \Longleftrightarrow \quad \alpha = 0$$

und damit notwendigerweise $b = 0$. Umgekehrt liegt für $b = 0$ das Polynom $f(x) = x^p(x^p - a)$ mit der mindestens p-fachen Nullstelle 0 vor. Andererseits gilt

$$\zeta_p^{\nu}\alpha = \zeta_p^{\mu}\beta\,,$$

und damit

$$\alpha^p = \beta^p \;, \qquad \text{das heißt} \qquad d = \frac{a^2}{4} - b = 0 \;.$$

Umgekehrt läßt sich so im Fall $d = 0$ für jedes $\zeta^\nu\alpha$ ein identisches $\zeta^\mu\beta$ finden. Insgesamt besitzt $f(x)$ daher folgende Anzahl paarweise verschiedener Nullstellen:

$$\left.\begin{array}{cl} 1 & \text{falls} \quad b = 0 \;\wedge\; a = 0 \\ p+1 & \text{falls} \quad b = 0 \;\wedge\; a \neq 0 \\ p & \text{falls} \quad b \neq 0 \;\wedge\; d = 0 \\ 2p & \text{falls} \quad b \neq 0 \;\wedge\; d \neq 0 \,. \end{array}\right\} \Longrightarrow \sqrt{d} \in \mathbb{Q}$$

Die zweite Frage erfordert eine individuelle Untersuchung. Für jeden in Tabelle 1 auftretenden Fall ist in Kapitel 3 eine Basis der Galoisgruppe vorzufinden. Davon ausgehend kann teils direkt, teils mit Hilfe von Strukturergebnissen aus Kapitel 4 und 5 der Effekt der Basiselemente auf die Nullstellen (2.4) bestimmt werden. Durch geeignete Numerierung der paarweise verschiedenen Nullstellen kann so die Basis in Form von Permutationen in Zykeldarstellung übersetzt werden.

6.4 Berechnung der Galoisgruppen

Aus `galbi` ist ersichtlich, welche Prozedur in Abhängigkeit der Kriterien K_1, K_2, K_3 für die Berechnung von $G(Z_f \,|\, \mathbb{Q})$ als Permuationsgruppe verantwortlich ist. Sie funktionieren derart, daß sie den Effekt der in Kapitel 3 diskutierten Basen auf die Nullstellen (2.4) bestimmen. Ihnen zur Seite stehen diverse Hilfsprozeduren, in denen gewisse Basiselemente berechnet werden und als Produkt elementfremder Zyklen ausgegeben werden. Für letzteres steht die Prozedur `permout(perm)` zur Verfügung, die eine übergebene Liste als String zurückgibt.

Die weiteren Hilfsprozeduren übersetzen typische Elemente der Basen in Permutationen. Ihnen zugrunde liegt die Numerierung der Nullstellen (2.4) mit einer primitiven p-ten Einheitswurzel ζ in Form von

$$n \leftrightarrow \zeta^n\alpha \,, \quad p+n \leftrightarrow \zeta^n\beta \;; \quad n = 1, 2, \ldots, p \,. \tag{6.1}$$

Nicht selten treten Automorphismen σ auf, die gewisse Nullstellen zyklisch permutieren. Hierzu dient die Prozedur `_sigma(p,s)`, die einen Zykel der Form

$$\left.\begin{array}{l} (s, s+1, \ldots, s+(p-1)) \\ (s, s-1, \ldots, s-(p-1)) \end{array}\right. \quad \begin{array}{ll} \text{falls} & s > 0 \\ & s < 0 \end{array}$$

zurückgibt.

Zur Berechnung eines $\tau \in G(Z_f \,|\, \mathbb{Q})$ mit $\tau(\zeta) = \zeta^\nu$, das α und β entweder vertauscht oder festläßt dienen die Prozeduren `_tau1(p,nu,s)`

und `_tau2(p,nu)`. In `_tau1` werden Zyklen berechnet, in denen der Effekt von τ auf die ersten bzw. letzten p Nullstellen zum Ausdruck kommt. Dies setzt voraus, daß $\sqrt{d}$ unter τ festbleibt. Mit (3.6) folgt dann:

$$\tau : \zeta^n\alpha \mapsto \zeta^{\nu n}\alpha \ , \quad \text{und damit} \quad n \to \nu n \ (\mathrm{mod}\ p) \ ; \quad n = 1, 2, \ldots, p \, .$$

Hierbei bezeichne $\nu n \ (\mathrm{mod}\ p)$ die kleinste Zahl $m \in \{0, 1, \ldots, p-1\}$ mit $m \equiv \nu n \bmod p$. Durch den Parameter s wird festgelegt, ob der Effekt von τ auf die Nullstellen $\alpha\zeta^\nu$ $(s{=}0)$ oder $\beta\zeta^\nu$ $(s{=}p)$ berechnet wird.

`_tau2` berücksichtigt den Fall $\tau(\sqrt{d}) = -\sqrt{d}$. Gemäß (3.6) werden so die Nullstellen wie folgt abgebildet:

$$\tau : \left\{ \begin{array}{lcl} \zeta^n\alpha \mapsto \zeta^{\nu n}\beta & \Longrightarrow & n \to \nu n \ (\mathrm{mod}\ p) + p \\ \zeta^n\beta \mapsto \zeta^{\nu n}\alpha & \Longrightarrow & n + p \to \nu n \ (\mathrm{mod}\ p) \end{array} \right. ; \ n = 1, 2, \ldots, p \, .$$

Ein Automorphismus $\lambda \in G(Z_f \,|\, \mathbb{Q})$ mit $\lambda(\sqrt{d}) = -\sqrt{d}$, der ζ festläßt, wird mit Blick auf (3.6) in `_lambda(p)` berechnet:

$$\lambda : \left\{ \begin{array}{lcl} \zeta^n\alpha \mapsto \zeta^n\beta & \Longrightarrow & n \to n + p \\ \zeta^n\beta \mapsto \zeta^n\alpha & \Longrightarrow & n + p \to n \end{array} \right. ; \quad n = 1, 2, \ldots, p \, .$$

Damit besteht λ aus einem Produkt p elementfremder Transpositionen.

Aufbauend auf den Hilfsprozeduren lassen sich die Galoisgruppen sehr übersichtlich berechnen. All dies geschieht in den folgenden Prozeduren, denen ebenfalls die Numerierung (6.1) der Nullstellen zugrunde liegt.

`_Zps1(p,s)`, `_Zps2(p)`, `_Z2xZps(p)`:

Ist $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_p^*$ so ist dies gleichwertig dazu, daß der Zerfällungskörper Z_f bereits durch $\mathbb{Q}[\zeta]$ gegeben ist. Die Galoisgruppe ist dann einelementig erzeugbar vermöge

$$\tau : \zeta \mapsto \zeta^\delta \, ,$$

worin δ eine primitive Wurzel modulo p ist. Ihre Berechnung als Permutationsgruppe erfolgt in Abhängigkeit von $\sqrt{d}$ in folgenden Prozeduren:

$$\sqrt{d} \left\{ \begin{array}{lcl} \in \mathbb{Q} & : & \texttt{\_Zps1} \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} & : & \texttt{\_Zps2} \end{array} \right. .$$

Gilt $\sqrt{d} \in \mathbb{Q}$, so gibt es Nullstellen α, β in $\mathbb{Q}$, die unter τ festbleiben. Die Bilder der weiteren Nullstellen sind unter Verwendung von (3.6) gegeben durch

$$\zeta\gamma \overset{\tau}{\mapsto} \zeta^\delta\gamma \overset{\tau}{\mapsto} \zeta^{\delta^2}\gamma \overset{\tau}{\mapsto} \cdots \overset{\tau}{\mapsto} \zeta^{\delta^{p-1}}\gamma = \zeta\gamma \ ; \quad \gamma \in \{\alpha, \beta\} \, .$$

Hierbei schöpfen die Potenzen von δ sämtliche Zahlen von 1 bis $p-1$ aus. Die so entstehende zyklische Permutation wird durch `_tau1` berechnet.

Zu berücksichtigen ist die Anzahl der paarweise verschiedenen, nichtrationalen Nullstellen. Gesteuert werden kann dies über den Parameter s. Dieser ist genau dann Null, wenn entweder b oder d verschwindet. Die Anzahl beträgt dann statt $2(p-1)$ lediglich $p-1$.

Ist $\sqrt{d}$ in $\mathbb{Q}[\zeta] \setminus \mathbb{Q}$, so wurde in Kapitel 3.2 gezeigt, daß dann $\tau(\sqrt{d}) = -\sqrt{d}$. Mit (3.6) folgt

$$\zeta^{\mu}\alpha \ \stackrel{\tau}{\mapsto} \zeta^{\delta\mu}\beta \ , \quad \zeta^{\mu}\beta \ \stackrel{\tau}{\mapsto} \zeta^{\delta\mu}\alpha \, .$$

Da $p-1$ gerade ist, kann der Effekt auf die $2p$ Nullstellen durch zwei Zyklen der Länge $p-1$, sowie einer zusätzlichen Transposition wiedergegeben werden. Hierzu wird die Prozedur `_tau2` herangezogen.

Gilt $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_p^*$, so wird `_Z2xZps` aufgerufen. Obiger Basis ist dann ein Automorphismus λ mit $\lambda(\sqrt{d}) = -\sqrt{d}$ hinzuzufügen, der ζ festläßt. Der bereits vorhandene Automorphismus τ wird vermöge $\tau(\sqrt{d}) = \sqrt{d}$ auf Z_f fortgesetzt und in der Prozedur `_tau1` berechnet. Dabei kann von $2p$ paarweise verschiedenen Nullstellen ausgegangen werden, da $\sqrt{d} \notin \mathbb{Q}[\zeta]$.

`_Lambdap1(p,s,t)`, `_Lambdap2(p,s)`, `_Z2xLambdap(p,s)`:

Diese Prozeduren werden herangezogen, wenn $G(Z_f \,|\, \mathbb{Q})$ isomorph zu einer der Gruppen Λ_p, $\widetilde{\Lambda}_p$, $\mathbb{Z}_2 \times \Lambda_p$ ist. Welche im konkreten Fall aufgerufen wird, hängt von $\sqrt{d}$ ab:

$$\sqrt{d} \begin{cases} \in \mathbb{Q} & : \ \texttt{\_Lambdap1} \\ \in \mathbb{Q}[\zeta] \setminus \mathbb{Q} & : \ \texttt{\_Lambdap2} \\ \notin \mathbb{Q}[\zeta] & : \ \texttt{\_Z2xLambdap} \end{cases} .$$

Der Zerfällungskörper ist in allen Fällen durch $Z_f = \mathbb{Q}[\zeta, \gamma, \sqrt{d}]$ bestimmt. Darin ist γ eine nichtverschwindende Nullstelle von $f(x)$. Eine Basis der Galoisgruppe ist gegeben durch einen analog zu oben diskutierten Automorphismus τ, der γ festläßt, sowie einem Automorphismus σ, der durch $\sigma(\gamma) = \zeta\gamma$ festgelegt ist und der ζ und $\sqrt{d}$ als Fixpunkte besitzt. Ist $\sqrt{d} \notin \mathbb{Q}[\zeta]$, so ist der Basis ein λ mit $\lambda(\sqrt{d}) = -\sqrt{d}$ hinzuzufügen, unter dem ζ und γ festbleiben.

Der Automorphismus τ läßt sich analog zu oben durch die Prozeduren `_tau2`, falls $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$, bzw. `_tau1` in allen anderen Fällen berechnen.

Besondere Aufmerksamkeit muß dem Automorphismus σ in bezug auf die Fallunterscheidung des Kriteriums K_2 zukommen. Ist b eine rationale p-te Potenz r^p, so wurde in Kapitel 4.2 gezeigt, daß es dann Nullstellen α und β gibt mit

$$\alpha \cdot \beta = r \, .$$

Ist hingegen $x^p - b$ irreduzibel über $\mathbb{Q}$, so wurde gezeigt, daß es dann Nullstellen der Gestalt

$$\alpha = c_1 \sqrt[p]{b}^{\,\nu} \; ; \; \beta = c_2 \sqrt[p]{b}^{\,\mu}$$

gibt, mit gewissen Koeffizienten $c_1, c_2 \in \mathbb{Q}[\sqrt{d}]$, die unter σ festbleiben. Sei ohne Einschränkung $\alpha \neq 0$. Dann ist der Effekt von σ auf die Nullstellen (2.4) gegeben durch:

$$\alpha \overset{\sigma}{\mapsto} \zeta\alpha \;\wedge\; x^p - b \in \mathbb{Q}[x] \begin{cases} \text{irreduzibel} \implies \sqrt[p]{b} \overset{\sigma}{\mapsto} \zeta \sqrt[p]{b} \implies \beta \overset{\sigma}{\mapsto} \zeta\beta \\ \text{reduzibel} \quad \implies \beta = \frac{r}{\alpha} \qquad \implies \beta \overset{\sigma}{\mapsto} \zeta^{-1}\beta. \end{cases}$$

Damit permutiert σ die $\zeta^\mu\beta$ im ersten Fall in genau umgekehrter Richtung als im zweiten.

In `_Lambdap1` ist die Anzahl der paarweise verschiedenen, nichtverschwindenden Nullstellen von $f(x)$ zu berücksichtigen, die durch den Parameter s zum Ausdruck kommt. Ist dieser gleich Null, so liegen statt $2p$ lediglich p verschiedene Nullstellen vor. Durch den Parameter t, der das Ergebnis des Kriteriums K_2 beinhaltet, wird unterschieden, in welcher Reihenfolge σ die $\zeta^\mu\beta$ permutiert.

Analoge Rechnungen, bei denen von $2p$ verschiedenen Nullstellen ausgegangen werden kann, werden in den Prozeduren `_Lambdap2` und `_Z2xLambdap` durchgeführt. Letztere fügt darüber hinaus den oben angesprochenen Automorphismus λ hinzu, der in `_lambda` berechnet wird.

Eine Ausnahme stellt in `_Lambdap2` der Fall $p = 3$ dar, falls b eine rationale p-te Potenz ist. In Kapitel 3.3 wurde gezeigt, daß dann $G(Z_f\,|\,\mathbb{Q}) \cong Z_6$ eine zyklische Gruppe ist. Bei geeigneter Numerierung der Nullstellen (2.4) ist dann eine Basis durch den Zykel (1 2 3 4 5 6) gegeben.

`_Lambdapq(p)`, `_LambdapqS(p)`, `_Lambda2pq(p)`:

Es fehlt noch die Berechnung der Galoisgruppen für den Fall, daß K_2 und K_3 Irreduzibilität liefern. Diese erfolgt in den nachstehenden Prozeduren:

$$G(Z_f\,|\,\mathbb{Q}) \cong \begin{cases} \Lambda_{p^2} & : \texttt{\_Lambdapq} \\ \widetilde{\Lambda}_{p^2} & : \texttt{\_LambdapqS} \\ \Lambda_{2p^2} & : \texttt{\_Lambda2pq} \end{cases} .$$

Basen dieser Gruppen sind jeweils dem Fall 3 der Kapitel 3.2 bis 3.4 zu entnehmen. Der Effekt ihrer Elemente auf die Nullstellen (2.4) kann direkt abgelesen und in den entsprechenden Prozeduren übersetzt werden.

6.5 Das Listing

```
************************************************************
```
`galbi` ist die zentrale Prozedur, die vom Benutzer zur Berechnung der Galoisgruppen aufgerufen wird.
```
************************************************************

galbi := proc(p:prime, a:rational, b:rational)

  local K;

  *** Test auf ungerade Primzahl ***

  if p=2 then ERROR(‘Nur Primzahlen > 2 !‘):
  fi:

  *** Test auf Einheitsgruppe ***

  if a=0 and b=0 then RETURN(‘1,+,{id}‘);
  fi:

  *** Bestimmung und Berechnung der Galoisgruppe ***

  K:=groupSelect(p,a,b):

  if K[2]+K[3]=0 then
     if K[1] = 4 then          _Z2xZps(p):
     elif type(K[1],odd) then _Zps2(p):
     else                      _Zps1(p, b*K[1]):
     fi:
  elif K[2]+K[3]=1 then
     if K[1] = 4 then          _Z2xLambdap(p, K[2]):
     elif type(K[1],odd) then _Lambdap2(p, K[1]+K[2]):
     else                      _Lambdap1(p, b*K[1], K[2]):
     fi:
  else
     if K[1] = 4 then          _Lambda2pq(p):
     elif type(K[1],odd) then _LambdapqS(p):
     else                      _Lambdapq(p):
     fi:
  fi:

  end:
```

```
************************************************
```
`groupSelect` bestimmt die Ergebnisse von K_1, K_2 und K_3.
```
************************************************

groupSelect := proc(p:prime, a:rational, b:rational)

  local d, gamma, k1, k2, k3, x, j:

  *** Berechnung von d und Bestimmung von K2 ***

  d :=a^2/4-b:
  if irreduc(x^p-b) then k2:=1:
  else                   k2:=0:
  fi:

  *** Bestimmung von K3 in Abhaengigkeit von sqrt(d) ***

  k3:=1:
  if not irreduc(x^2-d) then
     k1:=2*signum(d):
     gamma:=abs(a)/2+sqrt(d):
     for j from 0 to k2*(p-1) do
        if not irreduc(x^p-gamma/b^j) then
           k3:=0:
           break:
        fi:
     od:

  else
     j:=mods(p,4):
     if not irreduc(x^2-d/(j*p)) then k1:=j+2:
     else k1:=4:
     fi:
     gamma:=a^2/b-2:
     if not (checkIrred(p,gamma)
        or irreduc(x^(2*p)+gamma*x^p+1)) then
        k3:=0:
     fi:
  fi:

  *** Rueckgabe der Ergebnisse ***

  RETURN([k1,k2,k3]):

  end:
```

```
**********************************************************
```
`checkIrred` untersucht ein Polynom der Form $x^{2p}+cx^p+1$. Der Wert "true" sichert die Irreduzibilität, "false" hingegen sagt gar nichts aus.
```
**********************************************************

checkIrred:=proc(p:prime, c:rational)

  local f, n, j, q;

  *** n = Nenner von c ***

  if nops(c)=2 then n:=op(2,c):
  else n:=1:
  fi:

  *** Testen auf Irreduzibilitaet mit max. 30 Moduln ***

  q:=1:
  for j from 1 to 30 do

  *** Berechnung des naechstgroesseren Modul ***

     q:=eval(q)+p:
     while not type(q,prime) or modp(n,q)=0 do
        q:=eval(q)+p:
     od:

  *** Test, ob d quadr. Rest mod q und ob K3 irred. ***

     f:=Factors(x^2+c*x+1) mod q:
     if nops(f[2])=2
        and Irreduc(subs(x=x^p,f[2][1][1])) mod q then
        RETURN(true):
     fi:
  od:

  RETURN(false);

  end:
```

```
*********************************************************
```
_Zps1 berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_p^*$ und $\sqrt{d} \in \mathbb{Q}$.
```
*********************************************************

_Zps1:=proc(p:prime, s:integer)

  local d, bas;

  *** Berechnung des "Basisstamms" ***

  d  :=numtheory[primroot](p):
  bas:=_tau1(p,d,0):

  *** diesen "verdoppeln", falls 2p-2 versch. Nullst. ***

  if not s=0 then
     bas:=cat(bas, _tau1(p,d,p)):
  fi:

  RETURN(p-1, `+ , { `.bas.` }`):

  end:



*********************************************************
```
_Zps2 berechnet $G(Z_f \,|\, \mathbb{Q})$, falls $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_p^*$ und $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$.
```
*********************************************************

_Zps2:=proc(p:prime)

  local d, bas;

  *** Berechnung der Basis ***

  d  :=numtheory[primroot](p):
  bas:=_tau2(p,d):

  RETURN(p-1,`+ , { `.bas.` }`):

  end:
```

```
*****************************************************
```
_Z2xZps berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_p^*$.
```
*****************************************************

_Z2xZps:=proc(p:prime)

  local bas;

  *** Berechnung der Basis ***

  bas:=cat(_lambda(p), `, `, _sigma(p,1), _sigma(p,p+1)):

  RETURN(2*(p-1), `+ , { `.bas.` }`):

  end:



*******************************************************
```
_Lambdap1 berechnet $G(Z_f \,|\, \mathbb{Q})$, falls $G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_p$ und $\sqrt{d} \in \mathbb{Q}$.
```
*******************************************************

_Lambdap1:=proc(p:prime, s:integer, t:integer)

  local d, bas;

  *** Berechnung der Basis in Abhaengigkeit der Anzahl
      paarweise versch. Nullst. (s), sowie K2 (t) ***

  d  :=numtheory[primroot](p):
  if s=0 then
     bas:=cat(_tau1(p,d,0), `, `, _sigma(p,1)):
  else
     bas:=cat(_tau1(p,d,0), _tau1(p,d,p), `, `, _sigma(p,1)):
     if t=1 then bas:=cat(bas, _sigma(p,p+1)):
     else        bas:=cat(bas, _sigma(p,-2*p)):
     fi:
  fi:

  RETURN(p*(p-1),`- , { `.bas.` }`):

  end:
```

```
************************************************
```
_Lambdap2 berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_p$ und $\sqrt{d} \in \mathbb{Q}[\zeta] \setminus \mathbb{Q}$.
```
************************************************
_Lambdap2:=proc(p:prime, t:integer)

  local bas, d;

  *** Sonderfall p=3 und K2 red ***

  if p=3 and t=1 then
     RETURN(6, `+ , { (1 2 3 4 5 6) }`);

  *** Sonst Basis in Abhaengigkeit von K2 berechnen ***

  else
     d:=numtheory[primroot](p):
     bas:=cat(_tau2(p,d), `, `, _sigma(p,1)):
     if type(t,even) then bas:=cat(bas, _sigma(p,p+1)):
     else                 bas:=cat(bas, _sigma(p,-2*p)):
     fi:
     RETURN(p*(p-1),`- , { `.bas.` }`):
  fi:

  end:
```
****
```
_Z2xLambdap1 berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \mathbb{Z}_2 \times \Lambda_p$.
```
****
_Z2xLambdap:=proc(p:prime, t:integer)

  local d, bas;

  *** Berechnung der Basis abhaengig von K2 (t) ***

  d :=numtheory[primroot](p):
  bas:=cat(_tau1(p,d,0), _tau1(p,d,p), `, `):
  bas:=cat(bas,_lambda(p), `, `, _sigma(p,1)):
  if t=1 then bas:=cat(bas, _sigma(p,p+1)):
  else   bas:=cat(bas, _sigma(p,-2*p)):
  fi:

  RETURN(2*p*(p-1),`- , { `.bas.` }`):

  end:
```
```

```
*************************************************
```
_Lambdapqp berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_{p^2}$
```
*************************************************

_Lambdapq:=proc(p:prime)

  local d, bas;

  *** Berechnung der Basis ***

  d  :=numtheory[primroot](p):
  bas:=cat(_sigma(p,1), ` ,`, _sigma(p,p+1), `, `):
  bas:=cat(bas, _tau1(p,d,0), _tau1(p,d,p)):

  RETURN(p^2*(p-1),`- , { `.bas.` }`):

  end:
```

```
*************************************************
```
_LambdapqS berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \widetilde{\Lambda}_{p^2}$.
```
*************************************************

_LambdapqS:=proc(p:prime)

  local bas, d;

  *** Berechnung der Basis ***

  d:=numtheory[primroot](p):
  bas:=cat(_sigma(p,1),` ,`, _tau2(p,d)):

  RETURN(p^2*(p-1),`- , { `.bas.` }`):

  end:
```

```
 ***************************************************
```
_Lambda2pq berechnet die Galoisgruppe, falls $G(Z_f \,|\, \mathbb{Q}) \cong \Lambda_{2p^2}$.
```
***************************************************

_Lambda2pq:=proc(p:prime)

  local d, bas;

  *** Berechnung der Basis ***

  d  :=numtheory[primroot](p):
  bas:=cat(_sigma(p,1), ` ,`, _lambda(p), ` ,`):
  bas:=cat(bas, _tau1(p,d,0), _tau1(p,d,p)):

  RETURN(2*p^2*(p-1),`- , { `.bas.` }`):

  end:



***********************************************
```
_sigma, _lambda, _tau1, _tau2 sind die Hilfsprozeduren
zur Berechnung der Zykeln
```
***********************************************

_sigma:=proc(p:prime, s:integer)

  RETURN(permout([seq(abs(s)+signum(s)*n, n=0..p-1)])):

  end:


_lambda:=proc(p:integer)

  RETURN(seq(permout([n,n+p]), n=1..p)):

  end:
```

```
_tau1:=proc(p:prime, d:integer, s:integer)

  local n, q, zyk, tau;

  *** tau und q initialisieren ***

  tau:=``:
  q:={seq(n, n=1..p-1)}:

  *** Solange Zahlen unberuecksichtigt sind, werden
      ausgehend von der kleinsten ... ***

  while nops(q)>0 do:
     zyk:=[q[1]]:

  *** ... alle weiteren bestimmt, bis der Zykel
      geschlossen ist ***

     while not modp(zyk[-1]*d-zyk[1],p)=0 do:
        zyk:=[op(zyk), modp(zyk[-1]*d, p)]:
     od:

  *** Zykelelemente von q abziehen und Zykel tau
      zufuegen ***

     q:=q minus {op(zyk)}:
     tau:=cat(tau, permout(zyk+[seq(s, n=1..nops(zyk))])):
  od:

  RETURN(tau):

  end:
```

```
_tau2:=proc(p:prime, d:integer)

  local n, q, zyk, tau;

  *** tau und q initialisieren ***

  tau:=``:
  q:={seq(n, n=1..p)}:

  *** Solange Zahlen unberuecksichtigt sind, werden
      ausgehend von der kleinsten ... ***

  while nops(q)>0 do:
     zyk:=[q[1], modp(q[1]*d,p)+(1+iquo(q[1],p))*p]:

  *** ... alle weiteren bestimmt, bis der Zykel
      geschlossen ist ***

     while not modp(zyk[-1]*d-zyk[1],p)=0 do
        zyk:=[op(zyk), modp(zyk[-1]*d,p)]:
        zyk:=[op(zyk), modp(zyk[-1]*d,p)+p]:
     od:

  *** Zykelelemente von q abziehen und Zykel tau
      zufuegen ***

     q:=q minus {op(zyk)}:
     tau:=cat(tau, permout(zyk)):
  od:

  RETURN(tau);

  end:
```

```
 ************************************************
permout gibt eine Liste als Zykel in Form eines String zurück.
************************************************

permout:=proc(liste:list)

  local perm, j;

  *** Nacheinander die Elemente der Liste lesen ***

  perm:=`(`:
  for j from 1 to nops(liste) do
     perm:=cat(perm, ` `, liste[j]):
  od:

  RETURN(cat(perm,` )`)):
```

7 Ausblick

Ausgehend von der ursprünglichen Problemstellung kann zurückblikkend festgestellt werden, daß die gesuchten Galoisgruppen der Polynome (1.1) nicht nur charakterisiert und klassifiziert wurden, sondern darauf aufbauend auch ein Verfahren zur Berechnung der Gruppe hergeleitet und praktisch umgesetzt wurde. Hieran anschließend lassen sich weiterführende und vertiefendere Fragestellungen formulieren.

Zunächst kann die ursprüngliche Problemstellung auf Polynome der Form $x^{2n} + ax^n + b \in \mathbb{Q}[x]$ für beliebige $n \in \mathbb{N}$. Denkbar ist auch eine analoge Betrachtung der behandelten Problemstellung über verschiedenen Grundkörpern. Hierbei kann die vorliegende Arbeit unter Umständen als Grundlage dienen, die entweder direkt zur Anwendung kommt oder aber gewisse Methoden zur Problemorientierung bereitstellt. Dies könnte bedeuten, daß über die Primfaktorzerlegung von n ein Zugang zu gewissen Untergruppen der Galoisgruppe ermöglicht wird. Dazu könnten die Gruppen, die im Rahmen dieser Arbeit diskutiert wurden, von Nutzen sein.

Allgemein ließe sich auch die Untersuchung der Galoisgruppen weiter vertiefen. Fragen nach der Untergruppenstruktur, speziell den Normalteilern hinsichtlich der bekannten Auflösbarkeit bieten sich an.

Ein weiterer diskussionsfähiger Aspekt ist das vorgestellte Verfahren zur Berechnung der Galoisgruppe hinsichtlich seiner computertechnischen Optimierung. Hierbei steht in erster Linie der Rechenaufwand im Vordergrund, zu dessen Verringerung bereits einige Möglichkeiten umgesetzt wurden. Erdenklich ist auch eine Realisierung des Verfahrens unter weiteren Computeralgebrasystemen bzw. Programmiersprachen.

Literatur

[1] B. Hornfeck: *Algebra,* 3. Auflage, Walter de Gruyter, Berlin, New York 1976.

[2] B.L. van der Waerden: *Algebra I,* 8. Auflage, Springer–Verlag, Berlin, Heidelberg, New York 1971.

[3] F. Lorenz: *Einführung in die Algebra I,* B.I.-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1987.

[4] I. Niven, H.S. Zuckerman: *Einführung in die Zahlentheorie I,* B.I.-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1976.

[5] H. Hasse: *Vorlesungen über Zahlentheorie,* 2. Auflage, Springer–Verlag, Berlin, Göttingen, Heidelberg, New York, 1964.

[6] E. Artin: *Galoissche Theorie,* 2. Auflage, Verlag Harri Deutsch, Zürich, Frankfurt a. M. 1965.

[7] T. Aßelmeyer: *Die erste Grenze der Lösbarkeit,* Logos–Verlag, Berlin, 1996.

[8] A.N. Kolmogorov, A.P. Yushkevich: *Mathematics of the 19th Century,* Birkhäuser Verlag, Basel, Boston, Berlin, 1992.

Ich versichere, daß die vorliegende Arbeit ohne fremde Hilfe angefertigt wurde, und daß ich außer der von mir angegebenen Literatur keine weitere benutzt habe. Die wörtlich übernommenen Stellen sind als solche gekennzeichnet. Die Arbeit ist gemäß den alten Rechtschreibregeln verfaßt.

Braunschweig, den 14.12.1999.

(Werner Neumann)