Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe

Habilitationsschrift

Jürgen Klüners
Fachbereich für Mathematik und Informatik
Universität Kassel

Kassel, im April 2005

Inhaltsverzeichnis

Kapitel 1

Einleitung

In dieser Arbeit sind wir an der Dichte algebraischer Zahlkörper mit vorgegebener Galoisgruppe G interessiert. Wir betrachten hierzu für einen gegebenen Zahlkörper k die Zählfunktion

$$Z(k, G; x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, \mathcal{N}(d_{K/k}) \leq x\}|,$$

welche die Anzahl der Erweiterungen K/k mit Galoisgruppe G (innerhalb einer festgelegten algebraischen Hülle $\bar{\mathbb{Q}}$) zählt, wobei die Norm der Diskriminante durch $x \in \mathbb{R}$ nach oben beschränkt ist. Es ist wohlbekannt, dass diese Anzahl endlich ist, da es nur endlich viele Zahlkörper mit beschränkter Diskriminante und festem Grad gibt.

In zwei Arbeiten [23, 24] vermutet Gunter Malle, wie sich diese Zählfunktionen für $x \to \infty$ verhalten sollten. Dabei gibt er für jeden Zahlkörper k und jede Gruppe G zwei Konstanten $a(G)$ und $b(k, G)$ an und vermutet, dass eine weitere (von k und G abhängige) Konstante $c(k, G)$ existiert mit:

$$Z(k, G; x) \sim c(k, G) x^{a(G)} \log(x)^{b(k,G)}.$$

Zu diesem Zeitpunkt war die Richtigkeit der Vermutung für alle abelschen Gruppen G und Zahlkörper k durch die Arbeit von David Wright [33] bekannt. Bereits deutlich früher konnten Harold Davenport und Hans Arnold Heilbronn die Asymptotik für die Gruppe S_3 bestimmen. Deutlich später bestimmten Henri Cohen, Francisco Diaz y Diaz und Michel Olivier [6] die Asymptotik für $G = D_4$.

In den letzten Jahren hat Manjul Bhargava die Methoden verallgemeinert, die zur Bestimmung der Asymptotik von S_3–Erweiterungen führten, und hat die entsprechenden Asymptotiken für die Gruppen S_4 und S_5 angekündigt. Wir verweisen hier den interessierten Leser auf die Übersichtsartikel [3, 2].

Wir merken an, dass die dort verwendeten Methoden total unabhängig von den in dieser Arbeit verwendeten Methoden sind.

Dies sind sämtliche endliche Gruppen, für die eine asymptotische Aussage bekannt war.

In einer gemeinsamen Arbeit mit Gunter Malle [19] haben wir einige „gute“ obere und untere Abschätzungen für nilpotente Gruppen bewiesen. Z.B. zeigen wir in dieser Arbeit für Galoiserweiterungen mit nilpotenter Galoisgruppe G und alle Zahlkörper k, dass für alle $\epsilon > 0$ stets positive Konstanten $c_1(k,G), c_2(k,G,\epsilon)$ existieren mit:

$$c_1(k,G)x^{a(G)} \leq Z(k,G;x) \leq c_2(k,G,\epsilon)x^{a(G)+\epsilon} \text{ für } x \text{ groß genug,}$$

wobei $a(G)$ gerade die oben vermutete Konstante ist. Als weiteren wichtigen Hauptsatz können wir in [19] unter schwachen Voraussetzungen zeigen, dass für Kranzprodukte $G = Z_2 \wr H$ stets positive Konstanten $c_1(k,G), c_2(k,G,\epsilon)$ existieren mit:

$$c_1(k,G)x^{a(G)} \leq Z(k,G;x) \leq c_2(k,G,\epsilon)x^{a(G)+\epsilon} \text{ für } x \text{ groß genug}$$

(wobei in diesem Fall $a(G) = 1$ gilt). Dieses Beispiel liefert also nicht–symmetrische Gruppen, deren zugehörige Zählfunktion lineare Asymptotik hat.

Da die nilpotenten Gruppen auch in dieser Arbeit eine wichtige Rolle spielen, geben wir hier eine kurze Zusammenfassung der Hauptideen in [19]. Dort reduzieren wir unser Problem auf das Studium von zentralen Einbettungsproblemen mit Kern Z_ℓ, wobei Z_ℓ die zyklische Gruppe mit Ordnung $\ell \in \mathbb{P}$ ist. Durch Hinzufügen der ℓ–ten Einheitswurzeln können wir Kummertheorie verwenden und erhalten sogenannte Brauer–Einbettungsprobleme. Hier verwenden wir starke Sätze, welche alle Lösungen angeben, sobald wir eine kennen. In einem abschließenden Schritt müssen wir dann wieder zu unserem ursprünglichen Problem zurückkehren, d.h. die ℓ–ten Einheitswurzeln wieder loswerden.

Wir werden in dieser Arbeit einen mehr gruppentheoretischen Zugang verwenden, um alle Lösungen eines geeigneten Einbettungsproblems zu parametrisieren. Dabei werden wir für Einbettungsprobleme mit abelschem Kern eine explizite Beschreibung aller Lösungskörper angeben, sobald wir einen kennen. Mit Hilfe dieser Reduktion können wir die Kummertheorie, d.h. das Hinzufügen und Entfernen der ℓ–ten Einheitswurzeln einsparen.

Wir werden für sogenannte verallgemeinerte Quaternionengruppen $G = Q_{4m}$ und Kranzprodukte der Form $G = Z_2 \wr H$ unter schwachen Voraussetzungen an H (z.B. H nilpotent oder H regulär und es existiert K/k mit $\mathrm{Gal}(K/k) =$

H) obige Vermutung beweisen, d.h. für alle Zahlkörper k und diese Gruppen G gilt (Sätze 3.29 und 7.6):

$$Z(k, G; x) \sim c(k, G) x^{a(G)}.$$

Für allgemeine nilpotente Gruppen G beweisen wir in Satz 4.25 eine obere Abschätzung der Form:

$$Z(k, G; x) \leq c(k, G) x^{a(G)} \log(x)^{d(G)},$$

wobei $c(k, G) > 0$ und $d(G) \geq b(k, G)$ gilt. Damit wird das x^{ϵ}, welches wir in [19] erhalten hatten, durch das genauere $\log(x)^{d(G)}$ ersetzt. Zusätzlich gilt diese obere Schranke auch für nicht normale Erweiterungen.

Die in dieser Arbeit entwickelten Methoden können im Prinzip auch auf allgemeine auflösbare Gruppen angewendet werden. Hier stellt sich jedoch heraus, dass gute obere Schranken unserer Zählfunktionen an der fehlenden Kenntnis von guten Abschätzungen für die ℓ–Ränge von Klassengruppen scheitern. Der einfachste Fall von nicht nilpotenten auflösbaren Gruppen sind Diedergruppen der Ordnung 2ℓ, wobei ℓ eine ungerade Primzahl ist. In diesem Fall stellt sich heraus, dass der ℓ–Rang der Klassengruppe quadratischer Zahlkörper eine wesentliche Rolle spielt. In der Cohen–Lenstra–Heuristik (Vermutung 6.6) werden präzise Vermutungen geäußert, wie sich diese ℓ–Ränge im Schnitt verhalten sollen. Unter der Annahme einer schwachen Form der Cohen–Lenstra–Heuristik können wir für diese Diedergruppen die korrekte obere Schranke (Satz 6.9) zeigen, d.h. es existieren $c_1(k, D_\ell), c_2(k, D_\ell) > 0$ mit:

$$c_1(k, D_\ell) x^{a(D_\ell)} \leq Z(k, D_\ell; x) \leq c_2(k, D_\ell) x^{a(D_\ell)}$$

für x groß genug. Dabei können wir die untere Schranke unkonditionell beweisen (Satz 6.4). Zusätzlich zeigen wir, dass eine Verletzung der Asymptotik–Vermutung für Diedergruppen zur Folge hat, dass die Cohen–Lenstra–Heuristik falsch ist.

Allerdings geben wir in dieser Arbeit auch ein Gegenbeispiel zur Asymptotik–Vermutung an. So zeigen wir für die Zählfunktion $Z(\mathbb{Q}, Z_3 \wr Z_2; x)$, dass sie für alle c stärker als $cx^{a(G)} \log(x)^{b(k,G)}$ wächst. Dieses Beispiel entsteht durch ein unglückliches Zusammenspiel von abelschen Teilerweiterungen, die in einem „kritischen“ Kreisteilungskörper liegen. Wenn wir die analogen Fragestellungen für globale Funktionenkörper untersuchen, so ist es recht natürlich nur geometrische Erweiterungen zu betrachten, also solche, die zu keiner Konstantenerweiterung führen. Auf diese Weise können dann Teilkörper von Kreisteilungskörpern nicht auftreten. Unter einer nicht bewiesenen Heuristik können dann Jordan Ellenberg und Akshay Venkatesh [14] zeigen, dass wir

für alle globalen Funktionenkörper k der Charakteristik p und alle Gruppen G mit $p \nmid |G|$ Konstanten $c_1(k,G) > 0, c_2(k,G)$ finden mit:

$$c_1(k,G)x^{a(G)}\log(x)^{b(k,G)} \leq Z(k,G;x) \leq c_2(k,G)x^{a(G)}\log(x)^{b(k,G)}$$

für x groß genug. Dies zeigt, dass obige Vermutung trotz der hier gefundenen Gegenbeispiele der Wahrheit schon sehr nahe kommt.

Die Arbeit ist wie folgt organisiert. Nach dieser Einleitung stellen wir im zweiten Kapitel die Asymptotik–Vermutung vor. Hierzu erweitern wir den Begriff Galoisgruppe auf nicht normale Erweiterungen. Weiterhin stellen wir einfache Grundlagen wie Diskriminantenrelationen, Dirichletreihen und Taubersätze vor. Zum Abschluss dieses Kapitels geben wir eine Kurzeinführung in die Klassenkörpertheorie. Diese werden wir benötigen, um die Anzahl der Z_ℓ–Erweiterungen abzuschätzen, die höchstens oder sogar genau in einer vorgegebenen Menge von Primidealen verzweigt ist.

Im dritten Kapitel untersuchen wir die Asymptotik unserer Zählfunktion für zyklische Gruppen. Da wir später bei den nilpotenten Gruppen einen induktiven Ansatz verfolgen, müssen wir diese Zählfunktionen besonders gut verstehen. Hier halten wir uns am Anfang sehr nahe an die Arbeit [6], in welcher quadratische Erweiterungen untersucht werden. Es wird sich später herausstellen, dass wir Variationen unserer Zählfunktion brauchen werden. Z.B. möchten wir für eine vorgegebene endliche Menge von Primidealen nur die Körpererweiterungen berücksichtigen, die nicht in diesen Primidealen verzweigen. Im Prinzip liegen in der zitierten Arbeit alle Methoden vor, um diese Asymptotiken zu bestimmen. Leider wurden aber diese Rechnungen nicht durchgeführt, so dass wir dies in unserer Arbeit nachholen müssen. Zum Abschluss dieses Kapitels beweisen wir die exakte Asymptotik der Zählfunktion für Kranzprodukte der Form $Z_2 \wr H$, wobei wir wie oben bereits erwähnt etwas über H voraussetzen müssen. Die hier benutzten Methoden verallgemeinern die Methoden aus [6], in der die exakte Asymptotik der Zählfunktion von D_4 bestimmt wurde.

Im nächsten Kapitel führen wir die bereits angekündigte gruppentheoretische Reduktion durch. Sei hierzu

$$1 \to A \to G \to H \to 1$$

eine exakte Sequenz von Gruppen, wobei A abelsch sein soll. Dann zeigen wir in Satz 4.7, dass $G \times_H G \cong G \times_H (A \rtimes H)$ gilt. Nehmen wir nun an, dass K/k eine Körpererweiterung mit Galoisgruppe H ist und L_1/K und L_2/K zwei Lösungen des zugehörigen Einbettungsproblems sind, für welche zusätzlich $L_1 \cap L_2 = K$ gilt. Dann bedeutet obige Isomorphie, dass die Körpererweiterung L_1L_2/K einen Zwischenkörper L_3 besitzt mit $\mathrm{Gal}(L_3/k) =$

$A \rtimes H$. Umgekehrt führt die Kenntnis von Körpern L_1, L_3 mit $\mathrm{Gal}(L_1/k) = G$ und $\mathrm{Gal}(L_3/k) = A \rtimes H$ zu einem Zwischenkörper $K \leq L_2 \leq L_1 L_3$ mit $\mathrm{Gal}(L_2) = G$. Auf diese Weise können wir alle Lösungskörper unseres gegebenen Einbettungsproblems auf das Finden einer Lösung und das Finden aller Lösungen des zugehörigen zerfallenden Einbettungsproblems reduzieren. Besonders einfach stellt sich die Situation dar, wenn wir zusätzlich annehmen, dass $A = Z_\ell$ die zyklische Gruppe mit ℓ Elementen ist und diese im Zentrum von G liegt. Dann ist obiges semidirektes Produkt sogar direkt und wir müssen lediglich Z_ℓ–Erweiterungen des Grundkörpers parametrisieren. Wir zeichnen einen Lösungskörper als speziell aus und wollen ihn mit minimaler Verzweigung wählen. Hierzu müssen wir geeignete zyklische Erweiterungen des Grundkörpers bestimmen, welche bestimmte Verzweigungsbedingungen erfüllen. Zur Lösung dieses Problems verwenden wir dann Methoden aus der Kummer– und Klassenkörpertheorie. Zum Abschluss dieses Kapitels beweisen wir in Satz 4.25 die oben erwähnte obere Abschätzung für die Asymptotik der Zählfunktion nilpotenter Gruppen.

Im fünften Kapitel präsentieren wir das bereits erwähnte Gegenbeispiel. Weitere Beispiele zeigen, dass es nicht so einfach ist eine korrigierte Vermutung aufzustellen. Im darauf folgenden Kapitel beweisen wir die bereits oben erwähnten Ergebnisse für Diedergruppen (Sätze 6.4 und 6.9). Der Zusammenhang zur Cohen–Lenstra–Heuristik zeigt, dass die Asymptotik der Zählfunktion auflösbarer Gruppen ein bekanntermaßen schweres Problem darstellt (siehe Anmerkungen nach Vermutung 6.6).

Im letzten Kapitel beweisen wir dann die angekündigten Ergebnisse über die verallgemeinerten Quaternionengruppen G (Satz 7.6). Hier benutzen wir die Ergebnisse aus Kapitel 4. Die exakte Asymptotik erhalten wir durch das Studium der zu unserer Zählfunktion assoziierten Dirichletreihe. So können wir zeigen, dass diese Dirichletreihen an der Stelle $a(G)$ einen einfachen Pol und eine meromorphe Fortsetzung nach links besitzen. Durch Anwendung eines geeigneten Taubersatzes erhalten wir dann die gewünschte Asymptotik. Für diese Abschätzungen benötigen wir die Ergebnisse aus Kapitel 3. Insbesondere die Zählfunktionen quadratischer Erweiterungen mit lokalen Vorgaben spielen eine wesentliche Rolle.

Verwendete Begriffe und Notationen haben wir im Index und im Symbolverzeichnis am Ende dieser Arbeit zusammengefasst.

Ich danke allen meinen jetzigen und ehemaligen Kollegen für die Unterstützung in den vergangenen Jahren. Mein besonderer Dank gilt Prof. Dr. Gunter Malle, der mich auf dieses Thema gestoßen hat und immer als Diskussionspartner zur Verfügung stand. Widmen möchte ich diese Arbeit meinen Eltern, die mir zu jeder Zeit einen Rückhalt geboten haben.

Kapitel 2

Grundlagen

In diesem Kapitel sammeln wir einfache Grundlagen und Notationen. Außerdem stellen wir die Asymptotikvermutung und einfache Folgerungen hieraus vor. In dieser Arbeit bezeichne k stets einen algebraischen Zahlkörper, d.h. eine endliche Erweiterung von $\mathbb{Q}$.

2.1 Galoisgruppen

Im Folgenden sei $G \leq S_n$ stets eine transitive Untergruppe der symmetrischen Gruppe auf n Punkten. Für eine endliche Erweiterung K/k vom Grad n mit $K = k(\alpha)$ bezeichnen wir mit $\mathrm{Gal}(K/k)$ die Galoisgruppe $\mathrm{Gal}(m_\alpha)$, welche auf den Nullstellen $\alpha = \alpha_1, \ldots, \alpha_n$ des Minimalpolynoms $m_\alpha \in \mathbb{Q}[x]$ von α operiert. Wir weisen ausdrücklich darauf hin, dass wir mit dieser Notation auch einer nicht normalen Erweiterung eine Galoisgruppe zuordnen. Hierbei macht es einen Unterschied, ob eine Körpererweiterung die Galoisgruppe S_3 hat (Körpergrad 3) oder ob sie die gruppentheoretisch isomorphe Galoisgruppe $S_3(6)$ besitzt, welches die nicht abelsche transitive Untergruppe der Ordnung 6 von S_6 ist (Körpergrad 6). Hierbei deutet die Notation (6) in $S_3(6)$ an, dass die Gruppe auf 6 Punkten operieren soll. Wir merken an, dass wir in vielen Situationen vorkommende Gruppen implizit als transitive Permutationsgruppen auffassen.

2.2 Diskriminantenrelationen

Wir bezeichnen mit $d_{K/k}$ die Relativdiskriminante einer Körpererweiterung, welche ein Ideal der Maximalordnung $\mathcal{O}_k$ des Körpers k ist. Die Menge

der Primideale von $\mathcal{O}_k$ bezeichnen wir mit $\mathbb{P}(k)$. Den Körpergrad von K/k bezeichnen wir mit $[K : k]$. Für ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ bezeichnen wir mit $\mathcal{N}_{K/k}(\mathfrak{a}) \subseteq \mathcal{O}_k$ seine Norm, welche wieder ein Ideal ist. Weiterhin bezeichnen $\mathcal{N}(\mathfrak{a}) := |\mathcal{O}_k/\mathfrak{a}|$ die Absolutnorm eines Ideals $\mathfrak{a} \subseteq \mathcal{O}_k$ und $d_k := \mathcal{N}(d_{k/\mathbb{Q}})$ die Absolutdiskriminante von k. In dieser Arbeit wird es von zentraler Bedeutung sein die Diskriminanten von Körpertürmen zu kontrollieren. Die einfachste Version einer solchen Relation erhalten wir im folgenden Lemma (z.B. [28, Prop. 4.9]).

Lemma 2.1
Es seien $L/K/k$ endliche Körpererweiterungen. Dann gelten:

$$d_{L/k} = d_{K/k}^{[L:K]} \mathcal{N}_{K/k}(d_{L/K}),$$

$$d_L = d_K^{[L:K]} \mathcal{N}_{K/\mathbb{Q}}(d_{L/K}).$$

Unsere Beispiele sind nicht immer reine Körpertürme wie im obigen Lemma. Es seien hierzu N/k eine normale Erweiterung von Zahlkörpern mit Galoisgruppe G und $H_1, \ldots, H_r \leq G$. Wir bezeichnen mit $K_i := N^{H_i}$ die Fixkörper von H_i, d.h. die maximalen Teilkörper von N, welche unter H_i elementweise invariant bleiben. Unser Ziel wird es sein Relationen zwischen den Diskriminanten dieser Körper zu finden. Wir verwenden im Folgenden die Notationen von [31, VI.3]. Hierzu sei s_{G/H_i} der Permutationscharakter der Permutationsdarstellung von G auf den Links–Nebenklassen G/H_i. Der folgende Satz ist eine direkte Konsequenz von Proposition 6 und Corollary 1 in [31, VI.3].

Satz 2.2
Für $a_i \in \mathbb{Z}$ gelte die folgende Relation:

$$\sum_{i=1}^{r} a_i s_{G/H_i} = 0.$$

Dann erhalten wir

$$\prod_{i=1}^{r} d_{K_i/k}^{a_i} = (1).$$

Wir merken an, dass additive Relationen zwischen Permutationscharakteren auch die entsprechenden multiplikativen Relationen zwischen den Dedekindschen Zetafunktionen ergeben ([4, 21]). Dies ist aber für unsere Arbeit nicht von Bedeutung.

Im Folgenden behandeln wir Beispiele, die im weiteren Verlauf von großer Bedeutung sind. Dabei bezeichnet E die triviale Gruppe. Das folgende Lemma ist eine direkte Konsequenz aus Satz 2.2, wobei Z_ℓ stets die zyklische Gruppe mit ℓ Elementen bezeichnet und ℓ eine Primzahl ist.

Lemma 2.3
Es sei $G = Z_\ell \times Z_\ell$. Dann besitzt G genau $\ell+1$ Untergruppen H_i, $1 \leq i \leq \ell+1$, der Ordnung ℓ. Weiterhin gilt die Relation:

$$s_{G/H_1} + \ldots + s_{G/H_{\ell+1}} = \ell s_{G/G} + s_{G/E}.$$

Für $\mathrm{Gal}(N/k) = G$ gilt daher mit obigen Bezeichnungen:

$$d_{N/k} = d_{K_1/k} \cdots d_{K_{\ell+1}/k}.$$

Mit Hilfe dieses Lemmas können wir sehr viel über das Verzweigungsverhalten solcher Erweiterungen lernen. Im Folgenden bezeichne $v_\mathfrak{p}(\mathfrak{a})$ die (exponentielle) $\mathfrak{p}$–Bewertung von $\mathfrak{a}$, d.h. $v_\mathfrak{p}(\mathfrak{a}) = j$, wenn $\mathfrak{p}^j \mid\mid \mathfrak{a}$, d.h. $\mathfrak{p}^j \mid \mathfrak{a}$ und $\mathfrak{p}^{j+1} \nmid \mathfrak{a}$.

Lemma 2.4
Es seien N/k eine Erweiterung mit Galoisgruppe $Z_\ell \times Z_\ell$ und $\mathfrak{p} \in \mathbb{P}(k)$ ein zahm verzweigtes Ideal. Dann gelten:

(1) $v_\mathfrak{p}(d_{N/k}) = \ell(\ell-1)$.

(2) *$\mathfrak{p}$ ist genau in ℓ Teilkörpern von N/k vom Grad ℓ verzweigt. In jedem solchen Teilkörper K gilt:* $v_\mathfrak{p}(d_{K/k}) = \ell - 1$.

Beweis
Da N/k galoissch ist, gilt $\mathfrak{p}\mathcal{O}_N = (\mathfrak{P}_1 \ldots \mathfrak{P}_s)^\ell$ für Primideale $\mathfrak{P}_i \trianglelefteq \mathcal{O}_N$ und ein geeignetes $s \in \mathbb{N}$. Der Exponent ist ℓ, da die Trägheitsgruppe von zahm verzweigten Primidealen immer zyklisch ist. Alle Primideale $\mathfrak{P}_i$ haben denselben Trägheitsgrad f. Daher gilt für die lokale Erweiterung $N_{\mathfrak{P}_i}/k_\mathfrak{p}$: $d_{N_{\mathfrak{P}_i}/k_\mathfrak{p}} = \mathfrak{p}^{(\ell-1)f}$. Da $\ell^2 = \ell f s$ gilt, folgt somit: $v_\mathfrak{p}(d_{N/k}) = \ell(\ell-1)$. Für eine in $\mathfrak{p}$ zahm verzweigte Z_ℓ–Erweiterung K/k gilt natürlich $v_\mathfrak{p}(d_{K/k}) = \ell - 1$. Nach Lemma 2.3 muss das Produkt der Diskriminanten der Teilkörper gleich der Diskriminante $d_{N/k}$ sein. Da $v_\mathfrak{p}(d_{N/k}) = (\ell-1)\ell$ ist, sind genau ℓ Teilkörper in $\mathfrak{p}$ verzweigt. □

Leider stimmt obiges Lemma nicht mehr für wild verzweigte Primideale. Dies zeigt z.B. die Erweiterung $N = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hier gilt: $v_2(d_{N/\mathbb{Q}}) = 8$. Zwei der drei quadratischen Teilkörper haben 2–Bewertung 3, während der verbleibende 2–Bewertung 2 hat. Immerhin können wir folgendes zeigen:

Lemma 2.5
Es sei N/k eine Erweiterung mit Galoisgruppe $Z_\ell \times Z_\ell$ und $\mathfrak{p} \in \mathbb{P}(k)$ sei ein wild verzweigtes Ideal, welches in einem Zwischenkörper K vom Grad ℓ unverzweigt ist. Dann ist $\mathfrak{p}$ genau in ℓ Teilkörpern vom Grad ℓ verzweigt. Für alle diese Körper ist die $\mathfrak{p}$–Bewertung der Diskriminante gleich.

Beweis
Es sei K_1/k ein solcher in $\mathfrak{p}$ verzweigter Körper. Da K/k in $\mathfrak{p}$ unverzweigt ist, ist auch K_1K/K_1 an den über $\mathfrak{p}$ liegenden Stellen unverzweigt. Nach Lemma 2.1 gilt daher: $v_\mathfrak{p}(d_{N/k}) = \ell v_\mathfrak{p}(d_{K_1/k})$. Dies gilt für alle in $\mathfrak{p}$ verzweigten Grad ℓ–Teilkörper. Daher folgt die Behauptung. □

Eine weitere Anwendung für Satz 2.2 bilden sogenannte Frobeniusgruppen. Als Spezialfall stellen wir im folgenden Beispiel Diedergruppen vor.

Beispiel 2.6
Für eine Primzahl $\ell > 2$ sei $D_\ell = \langle a, x \mid a^\ell = 1 = x^2, x^{-1}ax = a^{-1}\rangle$ die Diedergruppe mit 2ℓ Elementen. Mit $F := \langle a\rangle$ und $H := \langle x\rangle$ erhalten wir folgende Relation (z.B. [18, Theorem 4]) von Permutationscharakteren:

$$2s_{G/G} + s_{G/E} = 2s_{G/H} + s_{G/F}.$$

Sei N/k galoissch mit Galoisgruppe D_ℓ. Dann bezeichnen wir mit K/k bzw. M/k Zwischenkörper vom Grad ℓ bzw. 2 über k. Wir erhalten mit Lemma 2.1 und Satz 2.2 die folgenden Relationen:

$$d_{N/k} = d_{M/k}^\ell \mathcal{N}_{M/k}(d_{N/M}) \text{ und } d_{N/k} = d_{K/k}^2 d_{M/k}$$

und damit

$$d_{K/k} = d_{M/k}^d \mathcal{N}_{M/k}(d_{N/M})^{1/2} \text{ für } d = \frac{\ell - 1}{2}.$$

2.3 Semidirekte und Kranzprodukte

In diesem Abschnitt definieren wir semidirekte und Kranzprodukte. Insbesondere die Kranzprodukte werden eine wichtige Rolle in dieser Arbeit haben. Wir bezeichnen mit $U \trianglelefteq G$ einen Normalteiler von G sowie mit $H \leq G$ eine Untergruppe.

Definition 2.7
Eine Gruppe G heißt semidirektes Produkt von U mit H ($G = U \rtimes H$), falls $U \trianglelefteq G$ und $H \leq G$ existieren mit $G = UH$ sowie $U \cap H = 1$. Eine Gruppe H mit diesen Eigenschaften heißt Komplement von U in G.

Ein typisches Beispiel für semidirekte Produkte sind Diedergruppen $D_n = Z_n \rtimes Z_2$. Das folgende Lemma zur Charakterisierung von semidirekten Produkten ist wohlbekannt.

Lemma 2.8
Es seien G eine Gruppe mit Normalteiler U sowie $\kappa : G \to H$ ein Epimorphismus mit Kern U. Dann ist G genau dann ein semidirektes Produkt von U mit H, wenn es einen Gruppenhomomorphismus $s : H \to G$ gibt mit: $\kappa \circ s = \mathrm{id}_H$.

Beweis
Es sei s gegeben. Dann gilt wegen der Exaktheit der Sequenz $1 \to U \to G \to H \to 1$, dass $s(H)$ ein Komplement zu U ist. Für ein Komplement H' von U ist $\kappa_{|H'}$ ein Isomorphismus zwischen H und H'. □

Wir bezeichnen mit $\mathrm{Aut}(U)$ die Automorphismengruppe einer Gruppe U. Aus Gruppen U, H sowie einem Homomorphismus $\Psi : H \to \mathrm{Aut}(U)$ können wir eine Gruppe G definieren, die ein semidirektes Produkt von U mit H ist:

$$G := \{(u,h) \mid u \in U, h \in H\} \text{ mit } (u_1,h_1)(u_2,h_2) = (u_1\Psi(h_1)(u_2), h_1h_2).$$

Die Gruppeneigenschaften erhalten wir durch Nachrechnen. Wir definieren $U^* := \{(u,1) \mid u \in U\}$ und $H^* := \{(1,h) \mid h \in H\}$. Damit erhalten wir $H \cong H^*$ sowie $U \cong U^*$. Weiterhin erfüllen diese Gruppen gerade die Eigenschaften in Definition 2.7.

Das Kranzprodukt ist ein spezielles semidirektes Produkt. Es seien hierzu $H_1 \leq S_m$ und $H_2 \leq S_d$ zwei transitive Gruppen sowie $n = md$. Dann ist das Kranzprodukt $G = H_1 \wr H_2 \cong H_1^d \rtimes H_2 \leq S_n$ ein semidirektes Produkt, wobei $H_2 \leq S_d$ gerade die d Kopien von H_1 vertauscht (Dies definiert $\Psi : H \to \mathrm{Aut}(H_1^d)$). Für eine genaue Definition des Kranzprodukts verweisen wir auf [12, S. 46]. Wir wollen hier lediglich auf eine wichtige körpertheoretische Interpretation hinweisen. Hierzu seien $L/K/k$ Körpererweiterungen mit $\mathrm{Gal}(L/K) = H_1$ und $\mathrm{Gal}(K/k) = H_2$. Dann ist $H_1 \wr H_2$ die größte Galoisgruppe, die für L/k auftreten kann.

2.4 Die Zählfunktion

Wir erinnern noch einmal an unsere Definition von Galoisgruppen nicht normaler Erweiterungen in Abschnitt 2.1. Für eine positive reelle Zahl x, einem Zahlkörper k und einer transitiven Gruppe $G \leq S_n$ definieren wir:

$$Z(k,G;x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, \mathcal{N}(d_{K/k}) \leq x\}|.$$

Dabei zählen wir die Körpererweiterungen K/k in einem fest gewählten algebraischen Abschluss $\bar{k}$ von k. Hierbei werden isomorphe aber nicht identische Körper mehrfach gezählt. Falls wir Körper nur bis auf Isomorphie zählen wollen, so ändern sich die Zahlen um eine Konstante, die nur von der Gruppe $G \leq S_n$ abhängt. Da es nur endlich viele Körper mit beschränkter Diskriminante und festem Grad gibt [5, Anwendung von Theorem 6.4.2], ist $Z(k, G; x)$ stets eine endliche Zahl. Wir sind im Folgenden daran interessiert, wie sich $Z(k, G; x)$ bei festem k und G für $x \to \infty$ verhält.

Für zwei reellwertige Funktionen f und g seien f und g *asymptotisch äquivalent* ($f \sim g$), falls $\lim_{x\to\infty} f(x)/g(x) = 1$ gilt. Weiterhin sagen wir $f = O(g)$, falls $\limsup_{x\to\infty} f(x)/g(x) < \infty$ gilt. Analog sei $f = o(g)$, falls $\limsup_{x\to\infty} f(x)/g(x) = 0$ gilt. Weiterhin werden wir später die Notation $x >> 0$ verwenden für x groß genug. Eine sehr allgemeine Vermutung besagt (siehe Vermutung 2.12)

$$Z(k, G; x) \sim c(k, G) x^{\alpha(k,G)} \log(x)^{\beta(k,G)},$$

wobei α, β, c Konstanten sind, die von k und G abhängen. Dies ist bereits für abelsche Gruppen G bekannt [33]. Wir werden darauf aber später noch genauer eingehen.

2.5 Die Konstanten a und b

In zwei Arbeiten [23, 24] hat Gunter Malle Vermutungen aufgestellt, wie sich die Konstanten α und β aus dem vorherigen Abschnitt in Abhängigkeit von k und G verhalten sollen. Auf den ersten Blick überraschend hierbei ist, dass die Konstante α nur von G abhängen soll und damit vom Grundkörper k unabhängig ist. Im Folgenden werden wir diese Konstanten explizit beschreiben. Es sei $G \leq S_n$ eine nicht triviale transitive Untergruppe, die auf $\{1, \ldots, n\}$ operiert. Für $\sigma \in G$ bezeichnet

$$\mathrm{ind}(\sigma) := n - \text{ Anzahl der Bahnen von } \sigma \text{ auf } \{1, \ldots, n\}$$

den *Index* von σ. Nun definieren wir:

Definition 2.9

$$\mathrm{ind}(G) := \min\{\mathrm{ind}(\sigma) \mid 1 \neq \sigma \in G\},$$

$$a(G) := \mathrm{ind}(G)^{-1}.$$

Aufgrund der Definition ist sofort klar, dass stets $1/(n-1) \leq a(G) \leq 1$ gilt.
Die Definition der Konstante b ist etwas komplizierter. Hierzu merken wir an, dass mit g auch alle Elemente der Konjugationsklasse C von g denselben Index haben, da dieser nur vom Zykeltyp des Elements abhängig ist. Wir brauchen nun eine Verallgemeinerung des Begriffs Konjugationsklasse.

Definition 2.10
Es sei $G_k := \mathrm{Gal}(\bar{k}/k)$ die absolute Galoisgruppe von k, wobei $\bar{k}$ den algebraischen Abschluss bezeichnet. Dann operiert G_k auf den Konjugationsklassen von G via der Operation auf den Spalten der Charaktertafel. Die Bahnen unter dieser Operation heißen k–Konjugationsklassen von G.

Es ist leicht einzusehen, dass Elemente einer k–Konjugationsklasse denselben Zykeltyp und damit denselben Index haben. Daher macht folgende Definition Sinn.

Definition 2.11

$$b(k,G) := |\{C \mid C \text{ ist } k\text{–Konjugationsklasse mit Index } \mathrm{ind}(G)\}| - 1.$$

Da es stets mindestens eine k–Konjugationsklasse von minimalem Index gibt, gilt $b(k,G) \geq 0$. Die Vermutung von Gunter Malle [24] lautet nun:

Vermutung 2.12
Es seien $G \leq S_n$ transitiv und k ein algebraischer Zahlkörper. Dann existiert eine Konstante $c(k,G) > 0$ mit

$$Z(k,G;x) \sim c(k,G)x^{a(G)} \log(x)^{b(k,G)},$$

wobei $a(G)$ und $b(k,G)$ wie in den Definitionen 2.9 und 2.11 definiert sind.

Wie bereits in der Einleitung erwähnt, geben wir in Kapitel 5 Gegenbeispiele zu dieser Vermutung an. Exakter sollte also diese Vermutung lauten: „Für welche Gruppen G und Zahlkörper k gilt…“. Alle mit der Konstruktion in Kapitel 5 entstehenden Gegenbeispiele haben gemeinsam, dass $b(k,G) \neq b(\mathbb{Q},G)$ für geeignete Zahlkörper k ist. Dabei stellt sich in diesen Beispielen heraus, dass ein höherer log–Faktor als vermutet auftritt.

Wie bereits in der Einleitung angemerkt, wurde diese Vermutung für abelsche Gruppen bereits 1989 von David Wright [33] mit einer anderen Interpretation von $a(G)$ und $b(k,G)$ bewiesen.

2.6 Folgerungen aus der Vermutung

Die meisten Anmerkungen dieses Abschnitts stammen aus [23, 24]. Sollte die Vermutung für einen Zahlkörper k und eine Gruppe G stimmen, so hat dies zur Folge, dass es unendlich viele Körpererweiterungen K/k mit dieser Galoisgruppe gibt. Insbesondere hätte in diesem Fall das inverse Galois–Problem über diesem Zahlkörper und für diese Gruppe eine positive Antwort. Für auflösbare Gruppen ist bekannt, dass sie über jedem Zahlkörper als Galoisgruppe auftreten (Satz von Shafarevich, siehe z.B. [30]). Für nicht auflösbare Gruppen ist momentan nicht bekannt, ob jede Gruppe z.B. über $k = \mathbb{Q}$ als Galoisgruppe auftaucht. Beispielsweise weiß man keine Antwort für die sporadische (Mathieu–)Gruppe M_{23}.

Schauen wir uns im Folgenden die Konstanten $a(G)$ und $b(k, G)$ an. Als erstes ist klar, dass $\mathrm{ind}(\sigma) = \mathrm{ind}(G)$ nur für Elemente von Primzahlordnung gelten kann. Wir haben schon erwähnt, dass stets $1/(n-1) \leq a(G) \leq 1$ gilt. Der Fall $a(G) = 1/(n-1)$ kann nur auftreten, wenn G neben der Identität nur n–Zykel enthält. Letzteres ist genau dann möglich, wenn n eine Primzahl und G die zyklische Gruppe mit n Elementen ist. Der andere Extremfall ($a(G) = 1$) bedeutet, dass die Gruppe G eine Transposition enthält. Dies ist z.B. der Fall, wenn $G = S_n$ in natürlicher Darstellung ist. Wir benötigen zuerst eine Definition.

Definition 2.13
Es sei $G \leq S_n$ eine transitive Gruppe, die auf $\Omega = \{1, \ldots, n\}$ operiert. Dann heißt $\Delta \subseteq \Omega$ ein Block von G, falls $\Delta^g \cap \Delta \in \{\Delta, \emptyset\}$ für alle $g \in G$ gilt. Falls G nur einelementige Blöcke bzw. den Block Ω besitzt, so nennen wir G primitiv. Andernfalls heißt G imprimitiv.

Wir merken an, dass eine Körpererweiterung K/k genau dann nicht triviale Zwischenkörper besitzt, wenn $\mathrm{Gal}(K/k)$ imprimitiv ist.

Lemma 2.14
Es sei $G \leq S_n$ eine transitive Gruppe, die eine Transposition enthält. Dann gelten:

(1) Alle Transpositionen in G sind konjugiert, d.h. $b(k, G) = 0$ für alle Zahlkörper k.

(2) $G = S_m \wr H$ für $1 \neq m$, $m \mid n$ und $H \leq S_{n/m}$ transitiv.

Beweis
Der erste Teil wird in [24, Lemma 2.2] bewiesen. Falls G primitiv ist, so

ist die zweite Aussage in [12, Theorem 3.3A] bewiesen. Sei nun $\tau = (i, j)$ eine Transposition und B ein minimaler (nicht trivialer) Block, der i enthält. Dann gilt $\tau(i) = j \in B$, da τ die anderen Elemente in B fixiert. Somit enthält $G|_B$ eine Transposition und operiert auf $G|_B$ primitiv. Damit operiert $G|_B$ auf B wie $S_{|B|}$. Für einen beliebigen zu B konjugierten Block $\tilde{B}$ können wir durch Konjugation von τ eine Transposition in $G|_{\tilde{B}}$ finden. Wir erhalten somit $n/|B|$ verschiedene Kopien der $S_{|B|}$. Damit ist $G \cong S_{|B|} \wr H$, wobei H das Bild des natürlichen Homomorphismus $\varphi : G \to S_{n/|B|}$ ist, welcher die konjugierten Blöcke zu B permutiert. □

Wir können zwei Folgerungen aus diesem Lemma ziehen. Als erstes erwarten wir maximal lineares Wachstum für eine Gruppe G, d.h. es soll stets $Z(k, G; x) = O(x)$ gelten. Weiterhin gibt es für nicht prime n andere Gruppen als S_n, welche lineares Wachstum haben sollten. Im Fall $n = 4$ ist dies z.B. für die Gruppe $G = D_4 = Z_2 \wr Z_2$ (siehe [1, 6]) bewiesen.

Wir bezeichnen mit

$$Z(k, n; x) := |\{K/k \mid [K : k] = n, \mathcal{N}(d_{K/k}) \leq x\}|$$

die Anzahl der Zahlkörper vom Grad n mit beschränkter Diskriminante. Aus Vermutung 2.12 und Lemma 2.14 erhalten wir die folgende Vermutung:

Vermutung 2.15
Für alle $n > 1$ existiert eine Konstante $c(k, n) > 0$ mit

$$Z(k, n; x) \sim c(k, n)x.$$

Weiterhin gilt:

$$c(k, n) = \sum_{G \leq S_n, a(G)=1} c(k, G),$$

wobei die Summe über transitive nicht isomorphe Untergruppen der S_n geht.

Wir werden später sehen (Satz 3.29), dass wir für $2 \mid n$ stets imprimitive Gruppen $G \leq S_n$ finden können mit $Z(k, G; x) \sim c(k, G)x$ für $x >> 0$ für ein $c(k, G) > 0$. Dies ist ein wenig überraschend, da momentan solche Asymptotiken für symmetrische Gruppen S_n selbst noch nicht bekannt sind.

2.7 Dirichletreihen und Taubersätze

In diesem Abschnitt wollen wir einige Eigenschaften von sogenannten Dirichletreihen herleiten. Insbesondere werden wir eine Version eines Taubersatzes

angeben. Wir bezeichnen für eine komplexe Zahl s mit $\Re(s)$ bzw. $\Im(s)$ den *Real– bzw. Imaginärteil.* Die Beweise der folgenden Aussagen können z.B. in [27, Seite 100f] oder [22, Seite 155ff] nachgelesen werden.

Definition 2.16
Eine Reihe der Form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ mit } a_n \in \mathbb{C}, s \in \mathbb{C} \tag{2.1}$$

heißt Dirichlet–Reihe.

Wir erhalten folgende grundlegende Aussage.

Satz 2.17

(1) Falls die Dirichlet–Reihe (2.1) *für einen Punkt $s_0 \in \mathbb{C}$ konvergent ist, so konvergiert sie lokal gleichmäßig für alle s mit $\Re(s) > \Re(s_0)$.*

(2) Falls die Dirichlet–Reihe für einen Punkt $s_0 \in \mathbb{C}$ absolut konvergent ist, so konvergiert sie absolut und gleichmäßig für alle s mit $\Re(s) \geq \Re(s_0)$.

In beiden Fällen definiert die Summe eine analytische Funktion für $\Re(s) > \Re(s_0)$ (bzw. für $\Re(s) \geq \Re(s_0)$).

Die kleinste reelle Zahl t, so dass die Dirichlet–Reihe für alle s mit $\Re(s) > t$ konvergiert, heißt *Konvergenzabzisse.* Wir sind im Folgenden mehr an der Summationsfunktion

$$A(x) := \sum_{n \leq x} a_n$$

interessiert. Wir erhalten folgende Abschätzung:

Lemma 2.18
Falls Konstanten C und $t > 0$ existieren mit

$$A(x) = \sum_{n \leq x} a_n \leq Cx^t \text{ für alle } x >> 0,$$

so ist die Konvergenzabzisse von (2.1) *kleiner oder gleich t.*

Wir kommen nun zu einer Version eines Taubersatzes, die für unsere Anwendungen geeignet ist. Diese Version basiert auf der Originalarbeit [11] und wird in [27, Seite 121] bewiesen.

Satz 2.19 (Taubersatz von Delange)
Es sei

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

eine für $\Re(s) > a > 0$ konvergente Dirichletreihe mit reellen $a_n \geq 0$. Weiterhin gelte im Konvergenzbereich für ein positives$w \in \mathbb{R}$

$$f(s) = \frac{g(s)}{(s-a)^w} + h(s),$$

wobei g und h in der Halbebene $\Re(s) \geq a$ analytische Funktionen mit $g(a) \neq 0$ sind. Dann gilt für $x \to \infty$:

$$\sum_{n \leq x} a_n = \left(\frac{g(a)}{a\Gamma(w)} + o(1) \right) x^a \log(x)^{w-1},$$

wobei Γ die Gamma–Funktion bezeichnet. Dies ist äquivalent zu

$$\sum_{n \leq x} a_n \sim \frac{g(a)}{a\Gamma(w)} x^a \log(x)^{w-1}.$$

Wir merken an, dass es wichtig ist, dass alle a_n nicht negative reelle Zahlen sind. Im selben Abschnitt in [27] wird noch eine andere Version bewiesen, in der $\log(\log(x))$–Faktoren in der Asymptotik auftreten. Diese werden wir aber nicht benötigen. Der Vorteil dieser Version eines Taubersatzes ist es, dass er nicht nur für Pole erster Ordnung anwendbar ist. Weiterhin werden keine Voraussetzungen an die Größe der Funktionswerte von g oder h gestellt. Wir merken an, dass für ganzzahlige w der Wert $\frac{g(a)}{\Gamma(w)}$ aus der Laurentreihen–Entwicklung der Funktion f abgelesen werden kann. Beispielsweise lässt sich die Riemannsche Zetafunktion $\zeta(s) = 1/(s-1) + h(s)$ schreiben, wobei $h(s)$ analytisch für $\Re(s) > 0$ ist.

2.8 Einfache Abschätzungen

In diesem Abschnitt sammeln wir einige Abschätzungen für Summen, die wir später benötigen werden. Hierzu seien k ein Zahlkörper und $\mathcal{O}_k$ die zugehörige Maximalordnung. Für ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_k$ bezeichnen wir mit $\omega(\mathfrak{a})$ die Anzahl der verschiedenen Primideale, die $\mathfrak{a}$ teilen. Weiterhin bezeichnen wir mit $t_k(\mathfrak{a})$ die Anzahl der verschiedenen Idealteiler von $\mathfrak{a}$. Wir erhalten folgende Abschätzung.

Lemma 2.20
Für alle $\epsilon > 0, m, b \in \mathbb{N}$ existieren Konstanten $c(\epsilon, m), c(\epsilon, m, b)$, so dass für alle Zahlkörper k vom Grad m gilt:

(1) $t_k(\mathfrak{a}) \leq c(\epsilon, m)\mathcal{N}(\mathfrak{a})^{\epsilon}$.

(2) $b^{\omega(\mathfrak{a})} \leq c(\epsilon, m, b)\mathcal{N}(\mathfrak{a})^{\epsilon}$.

Beweis
Der 1. Teil ist gerade die Aussage von [19, Lemma 2.2]. Sei nun $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ die Faktorisierung von $\mathfrak{a}$. Dann gilt: $t_k(\mathfrak{a}) = \prod_{\mathfrak{p}}(e_{\mathfrak{p}} + 1)$ und $b^{\omega(\mathfrak{a})} = \prod_{\mathfrak{p}} b$. Damit gilt $b^{\omega(\mathfrak{a})} < t_k(\mathfrak{a}^{b-1}) \leq c_1(\epsilon, m)\mathcal{N}(\mathfrak{a})^{(b-1)\epsilon}$ nach (1), woraus die gewünschte Abschätzung folgt. □

Falls im obigen Lemma für alle Primteiler $\mathfrak{p}$ bereits $e_{\mathfrak{p}} \geq b-1$ gilt, so erhalten wir direkt $b^{\omega(\mathfrak{a})} \leq t_k(\mathfrak{a})$.

Das folgende Lemma liefert eine obere Abschätzung für eine Summe, die später häufiger auftauchen wird. Für positive ganze Zahlen $r, e_1, \ldots, e_r$ summiere

$$\sum_{a_1^{e_1} \cdots a_r^{e_r} = n} 1$$

über alle Tupel $(a_1, \ldots, a_r) \in \mathbb{N}^r$ mit $a_1^{e_1} \cdots a_r^{e_r} = n$.

Lemma 2.21
Für $e_1, \ldots, e_r > 0$ mit $e := \min(e_i)$ und $m := |\{i \mid e_i = e\}|$ gilt:

$$\sum_{n \leq x} \sum_{a_1^{e_1} \cdots a_r^{e_r} = n} 1 = O(x^{1/e} \log(x)^{m-1}) \text{ für } x \to \infty.$$

Beweis
Der Fall $r = 1$ ist trivial. Für $m = r$ steht dies gerade in der Lösung zu [26, Exercise 2.5.1]. Wir beweisen nun die Aussage durch Induktion nach r, wobei wir $e_1 > e$ annehmen können. Es gilt:

$$\sum_{n \leq x} \sum_{a_1^{e_1} \cdots a_r^{e_r} = n} 1 = \sum_{a_1^{e_1} \leq x} \left(\sum_{n \leq \frac{x}{a_1^{e_1}}} \left(\sum_{a_2^{e_2} \cdots a_r^{e_r} = n} 1 \right) \right)$$

$$= \sum_{a_1^{e_1} \leq x} c(\frac{x}{a_1^{e_1}})^{1/e} \log(\frac{x}{a_1^{e_1}})^{m-1} + o(x^{1/e} \log(x)^{m-1}) \quad \text{(nach Ind.Vor.)}$$

$$\leq cx^{1/e} \log(x)^{m-1} \sum_{a_1^{e_1} \leq x} \frac{1}{a_1^{e_1/e}} + o(x^{1/e} \log(x)^{m-1}) \quad \text{(wegen } a_1^{e_1} \geq 1\text{)}$$

$$= \tilde{c}x^{1/e}\log(x)^{m-1} + o(x^{1/e}\log(x)^{m-1}),$$

da wegen $e_1 > e$ die Summe $\sum_{a_1^{e_1} \leq x} \frac{1}{a_1^{e_1/e}}$ für $x \to \infty$ konvergent ist. □

Falls unser Grundkörper k nicht $\mathbb{Q}$ ist, werden wir solche Summierungen auch für Ideale in $\mathcal{O}_k$ brauchen. Seien hierzu wieder $e_1, \ldots, e_r$ positive ganze Zahlen und $\mathfrak{a} \subseteq \mathcal{O}_k$ ein Ideal. Dann bezeichnet

$$\sum_{\mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r} = \mathfrak{a}} 1$$

die Summe über alle Tupel $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ von Idealen in $\mathcal{O}_k$ mit $\mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r} = \mathfrak{a}$. Wir erhalten das analoge Ergebnis zu Lemma 2.21.

Lemma 2.22
Für $e_1, \ldots, e_r > 0$ mit $e := \min(e_i)$ und $m := |\{i \mid e_i = e\}|$ gilt:

$$\sum_{\mathcal{N}(\mathfrak{a}) \leq x} \sum_{\mathfrak{a}_1^{e_1} \cdots \mathfrak{a}_r^{e_r} = \mathfrak{a}} 1 = O(x^{1/e}\log(x)^{m-1}) \text{ für } x \to \infty.$$

Beweis
Wir betrachten wieder zuerst den Fall $m = r$, welcher insbesondere $r = 1$ einschließt. In diesem Fall gilt:

$$\sum_{\mathcal{N}(\mathfrak{a}) \leq x} \sum_{(\mathfrak{a}_1 \cdots \mathfrak{a}_r)^e = \mathfrak{a}} 1 = \sum_{\mathcal{N}(\mathfrak{a}^e) \leq x} \sum_{\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}} 1 = \sum_{\mathcal{N}(\mathfrak{a}) \leq x^{1/e}} \sum_{\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}} 1,$$

weswegen wir o.B.d.A. $e = 1$ annehmen können. Wir bezeichnen mit $t_{k,r}(\mathfrak{a})$ die Anzahl der verschiedenen Faktorisierungen von $\mathfrak{a}$ in r Faktoren und erhalten $t_{k,r}(\mathfrak{a}) = \sum_{\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}} 1$. Analog zur Lösung von [26, Exercise 1.5.5] können wir zeigen, dass

$$\sum_{n=1}^{\infty} \sum_{\mathcal{N}(\mathfrak{a}) = n} \frac{t_{k,r}(\mathfrak{a})}{n^s} = \zeta_k^r(s)$$

gilt, wobei ζ_k die Dedekindsche–Zetafunktion des Zahlkörpers k bezeichnet. Da $\zeta_k^r(s)$ für $\Re(s) > 1$ absolut konvergiert, bei $s = 1$ einen Pol der Ordnung r besitzt und analytisch auf $\Re(s) = 1$ fortsetzbar ist, erhalten wir mit Satz 2.19

$$\sum_{\mathcal{N}(\mathfrak{a}) \leq x^{1/e}} \sum_{\mathfrak{a}_1 \cdots \mathfrak{a}_r = \mathfrak{a}} 1 \sim cx^{1/e}\log(x)^{r-1}$$

für $x \to \infty$ und eine geeignete Konstante $c > 0$.

Sei nun o.B.d.A. $e_1 > e$. Dann gilt:

$$\sum_{\mathcal{N}(\mathfrak{a})\leq x}\sum_{\mathfrak{a}_1^{e_1}\cdots\mathfrak{a}_r^{e_r}=\mathfrak{a}} 1 = \sum_{\mathcal{N}(\mathfrak{a}_1)^{e_1}\leq x}\left(\sum_{\mathcal{N}(\mathfrak{a})\leq x/\mathcal{N}(\mathfrak{a}_1)^{e_1}}\left(\sum_{\mathfrak{a}_2^{e_2}\cdots\mathfrak{a}_r^{e_r}=\mathfrak{a}} 1\right)\right).$$

Nach Induktion erhalten wir nun:

$$= \sum_{\mathcal{N}(\mathfrak{a}_1)^{e_1}\leq x} c\left(\frac{x}{\mathcal{N}(\mathfrak{a}_1)^{e_1}}\right)^{1/e}\log(x/\mathcal{N}(\mathfrak{a}_1)^{e_1})^{m-1} + o(x^{1/e}\log(x)^{m-1})$$

$$\leq cx^e\log(x)^{m-1}\sum_{\mathcal{N}(\mathfrak{a}_1)^{e_1}\leq x}\frac{1}{\mathcal{N}(\mathfrak{a}_1)^{e_1/e}} + o(x^{1/e}\log(x)^{m-1}).$$

Wegen $\mathcal{N}(\mathfrak{a}_1)^{e_1} \geq 1$ haben wir in der letzten Summe $\log(x/\mathcal{N}(\mathfrak{a}_1)^{e_1}) \leq \log(x)$ abgeschätzt. Nun konvergiert die Summe $\sum_{\mathcal{N}(\mathfrak{a}_1)^{e_1}\leq x}\frac{1}{\mathcal{N}(\mathfrak{a}_1)^{e_1/e}}$ für $x \to \infty$, weil $e_1 > e$, und wir erhalten das gewünschte Ergebnis. □

Wir brauchen noch eine weitere Variation dieser Summe:

Lemma 2.23
Für $e_1, \ldots, e_r, l_1, \ldots, l_r > 0$ mit $e := \min(e_i)$ und $m := \sum_{\{i:e_i=e\}} l_i$ gilt:

$$\sum_{\mathcal{N}(\mathfrak{a})\leq x}\sum_{\mathfrak{a}_1^{e_1}\cdots\mathfrak{a}_r^{e_r}=\mathfrak{a}} l_1^{\omega(\mathfrak{a}_1)}\cdots l_r^{\omega(\mathfrak{a}_r)} = O(x^{1/e}\log(x)^{m-1}) \text{ für } x \to \infty.$$

Beweis
Wie im Beweis zu Lemma 2.20 gilt:

$$l_i^{\omega(\mathfrak{a}_i)} \leq t_{k,l_i}(\mathfrak{a}_i) := \sum_{\mathfrak{a}_{i,1}\cdots\mathfrak{a}_{i,l_i}=\mathfrak{a}_i} 1.$$

Dabei gilt genau dann „=“, wenn $\mathfrak{a}_i$ quadratfrei ist. Wir erhalten also:

$$\sum_{\mathcal{N}(\mathfrak{a})\leq x}\sum_{\mathfrak{a}_1^{e_1}\cdots\mathfrak{a}_r^{e_r}=\mathfrak{a}} l_1^{\omega(\mathfrak{a}_1)}\cdots l_r^{\omega(\mathfrak{a}_r)} \leq \sum_{\mathcal{N}(\mathfrak{a})\leq x}\sum_{(\mathfrak{a}_{1,1}\cdots\mathfrak{a}_{1,l_1})^{e_1}\cdots(\mathfrak{a}_{r,1}\cdots\mathfrak{a}_{r,l_r})^{e_r}=\mathfrak{a}} 1.$$

Letztere Summe erfüllt nach Lemma 2.22 genau die gewünschte obere Abschätzung. □

2.9 Klassenkörpertheorie

Zur Beschreibung von abelschen Erweiterungen algebraischer Zahlkörper k wurde die sogenannte Klassenkörpertheorie entwickelt. Im Fall $k = \mathbb{Q}$ gilt der Satz von Kronecker–Weber, der besagt, dass jede abelsche Erweiterung $K/\mathbb{Q}$ in einem Kreisteilungskörper $\mathbb{Q}(\zeta_f)$ enthalten ist, wobei ζ_f eine primitive f–te Einheitswurzel ist. Das kleinste f mit $K \subseteq \mathbb{Q}(\zeta_f)$ heißt der Führer von $K/\mathbb{Q}$. Dieser erfüllt nach [28, Prop 8.1] folgende Eigenschaften.

Lemma 2.24
Es sei $K/\mathbb{Q}$ eine endliche abelsche Erweiterung mit Führer f. Dann gelten:

(1) $p \mid d_K$ genau dann, wenn $p \mid f$.

(2) p ist zahm verzweigt in $K/\mathbb{Q}$ genau dann, wenn $p \mid f$ und $p^2 \nmid f$.

Mit Hilfe dieses Lemmas können wir den Führer einer Erweiterung in vielen Fällen anhand der Verzweigung von $K/\mathbb{Q}$ bestimmen. Lediglich wenn wilde Verzweigung auftritt, kennen wir nicht die exakte Potenz von p, die in f aufgeht. Wir merken an, dass wilde Verzweigung nur für Primzahlen $p \leq [K : \mathbb{Q}]$ auftreten kann.

In der Klassenkörpertheorie werden diese Ergebnisse auf Grundkörper $k \neq \mathbb{Q}$ verallgemeinert. Die Rolle der Kreisteilungskörper wird von den sogenannten Strahlklassenkörpern eingenommen. Dies bedeutet, dass jede abelsche Erweiterung Teilkörper eines geeigneten Strahlklassenkörpers ist. Im Falle von $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ war die Galoisgruppe gerade $(\mathbb{Z}/f\mathbb{Z})^*$, also die multiplikative Gruppe von $\mathbb{Z}/f\mathbb{Z}$. Die Galoisgruppe des Strahlklassenkörpers ist die sogenannte Strahlklassengruppe, die wir im Folgenden einführen wollen.

Wir beschränken uns hier auf den idealtheoretischen Zugang. Für den idele–theoretischen Zugang und die Beweise der folgenden Aussagen verweisen wir auf [29, 22]. Wir fixieren im Folgenden einen Grundkörper k mit Maximalordnung $\mathcal{O}_k$. Wir bezeichnen mit $\mathfrak{m} := (\mathfrak{m}_0, \mathfrak{m}_\infty)$ den *(Erklärungs–)Modul*, wobei $\mathfrak{m}_0$ ein ganzes Ideal von $\mathcal{O}_k$ ist und $\mathfrak{m}_\infty$ eine formale Menge von reellen Stellen von k bezeichnet. Ein (gebrochenes) Ideal $\mathfrak{a}$ von $\mathcal{O}_k$ heißt koprim zu $\mathfrak{m}$, falls es koprim zu $\mathfrak{m}_0$ ist. Für eine algebraische Zahl $\alpha \in k$ definieren wir

$$\alpha \equiv 1 \bmod {}^*\mathfrak{m}, \text{ falls } \alpha \equiv 1 \bmod \mathfrak{m}_0 \text{ und } v(\alpha) > 0 \text{ für alle } v \in \mathfrak{m}_\infty.$$

Wir sagen, dass ein Modul $\mathfrak{m}$ einen Modul $\mathfrak{n}$ teilt, falls $\mathfrak{m}_0 \mid \mathfrak{n}_0$ und $\mathfrak{m}_\infty \subseteq \mathfrak{n}_\infty$ gelten. Die *Strahlklassengruppe* $\mathrm{Cl}_\mathfrak{m}$ ist die Faktorgruppe $I^\mathfrak{m}/H_\mathfrak{m}$, wobei $I^\mathfrak{m}$ die Gruppe der gebrochenen Ideale von $\mathcal{O}_k$ koprim zu $\mathfrak{m}_0$ und $H_\mathfrak{m}$ die Gruppe

der (gebrochenen) Hauptideale (α) von $\mathcal{O}_k$ bezeichnet, die einen Erzeuger $\alpha \equiv 1 \bmod {}^*\mathfrak{m}$ besitzen.

Sei nun $H_\mathfrak{m} \leq U \leq I^\mathfrak{m}$ eine beliebige Zwischengruppe. Der kleinste Modul $\mathfrak{n} \mid \mathfrak{m}$, so dass $I^\mathfrak{m}/U \to I^\mathfrak{n}/UH_\mathfrak{n}$ injektiv wird, heißt der *Führer* $\mathfrak{f}_U$ von U. Wir sagen, dass $H_\mathfrak{n} \leq U' \leq I^\mathfrak{n}$ *äquivalent* zu U ist, falls die Kerne der Homomorphismen $\mathrm{Cl}_{\mathfrak{m}\mathfrak{n}} \to I^\mathfrak{n}/U'$ und $\mathrm{Cl}_{\mathfrak{m}\mathfrak{n}} \to I^\mathfrak{m}/U$ übereinstimmen. In diesem Falle schreiben wir $U' \sim U$. Der Hauptsatz der Klassenkörpertheorie besagt nun (z.B. [29, Theorem 7.1]):

Satz 2.25
Es sei $\mathfrak{m}$ ein Modul.

(1) Für jedes $H_\mathfrak{m} \leq U \leq I^\mathfrak{m}$ existiert genau eine abelsche Erweiterung K/k mit $\mathrm{Gal}(K/k) \cong I^\mathfrak{m}/U$, wobei der Isomorphismus durch die sogenannte Artin–Abbildung

$$I^\mathfrak{m}/U \to \mathrm{Gal}(K/k), \mathfrak{a}U \mapsto (\mathfrak{a}, K/k)$$

gegeben ist, welche Primideale auf ihren Frobeniusautomorphismus abbildet.

(2) Für jede abelsche Erweiterung K/k existiert genau eine Klasse von Faktorgruppen $I^\mathfrak{m}/U$ mit $\mathrm{Gal}(K/k) \cong I^\mathfrak{m}/U$ via der Artin–Abbildung.

(3) Sei $\mathfrak{f}$ der Führer von $I^\mathfrak{m}/U$ und K/k die zugehörige abelsche Erweiterung. Dann ist ein Primideal $\mathfrak{p}$ von $\mathcal{O}_k$ genau dann in K verzweigt, wenn $\mathfrak{p} \mid \mathfrak{f}_0$ gilt. Es ist genau dann wild verzweigt, wenn $\mathfrak{p}^2 \mid \mathfrak{f}_0$ gilt.

Dieser Satz ist in kanonischer Weise die Verallgemeinerung des Satzes von Kronecker–Weber. Wir nennen den Körper, der zur Untergruppe $U = H_\mathfrak{m}$ gehört, den *Strahlklassenkörper* von $\mathfrak{m}$. Daher sind mit Hilfe des obigen Satzes alle abelschen Erweiterungen in einem geeigneten Strahlklassenkörper enthalten. Wenn wir den Fall $\mathfrak{m} = ((1), \emptyset)$ betrachten, so ist die zugehörige Strahlklassengruppe gerade die Idealklassengruppe des Zahlkörpers. Der zugehörige Strahlklassenkörper heißt *Hilbertscher Klassenkörper*. Er hat die Eigenschaft, dass er an allen endlichen und unendlichen Stellen unverzweigt ist. Sei nun $\mathfrak{m}_\infty$ die Menge aller reellen Stellen von k. Dann heißt der zu $\mathfrak{m} = ((1), \mathfrak{m}_\infty)$ gehörende Strahlklassenkörper der *große Hilbertsche Klassenkörper*. Dieser ist an allen endlichen Stellen unverzweigt. Die Ordnungen der beiden Strahlklassengruppen unterscheiden sich um eine 2–Potenz.

Für uns ist im Folgenden die Frage interessant, wieviele abelsche Erweiterungen eines Zahlkörpers k existieren, die (höchstens) in einer endlichen vorgegebenen Menge von Primidealen verzweigt sind. Aufgrund von Satz 2.25

(3) müssen wir bei dieser Fragestellung auch höhere Potenzen von Primidealen im Führer berücksichtigen. Zuerst beschreiben wir genauer die Struktur der Strahlklassengruppe. Für jeden Modul $\mathfrak{m}$ ist die folgende Sequenz von abelschen Gruppen mit offensichtlichen Abbildungen exakt, wobei Cl_k die Idealklassengruppe bezeichnet (z.B. in [22, S.125–126]):

$$1 \to H^{\mathfrak{m}}/H_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_k \to 1. \tag{2.2}$$

Hierbei bezeichnet $H^{\mathfrak{m}}$ die Gruppe der gebrochenen Hauptideale von $\mathcal{O}_k$, welche koprim zu $\mathfrak{m}_0$ sind. Wir wollen im Folgenden für ein $\ell \in \mathbb{P}$ den ℓ–Rang von $\mathrm{Cl}_{\mathfrak{m}}$ durch die Summe der ℓ–Ränge von Cl_k und $H^{\mathfrak{m}}/H_{\mathfrak{m}}$ nach oben abschätzen. Wir bezeichnen mit $k_{\mathfrak{m}}$ die Gruppe der Elemente von k, welche kongruent $1 \bmod {}^*\mathfrak{m}$ sind. Analog bezeichnen wir mit $k^{\mathfrak{m}}$ die Gruppe der Elemente von k, welche koprim zu $\mathfrak{m}$ sind. Nun gilt nach [22, Seite 125] die folgende Isomorphie von multiplikativen Gruppen:

$$H^{\mathfrak{m}}/H_{\mathfrak{m}} \cong k^{\mathfrak{m}}/\mathcal{O}_k^* k_{\mathfrak{m}}. \tag{2.3}$$

Letztere Gruppe ist eine Faktorgruppe der Gruppe $(\mathcal{O}_k/\mathfrak{m}_0)^* \times Z_2^{|\mathfrak{m}_\infty|}$, wobei zu jeder reellen Stelle in $\mathfrak{m}_\infty$ genau ein Z_2–Faktor korrespondiert. Wir können nun den folgenden Satz beweisen. Dabei bezeichnet im Folgenden $\mathrm{rk}_\ell(\mathrm{Cl}_K)$ den *ℓ–Rang* der Klassengruppe.

Satz 2.26
Es seien k ein algebraischer Zahlkörper mit r_1 reellen Einbettungen, ℓ eine Primzahl, S eine endliche Menge von Primidealen sowie

$$S_1 := \{\mathfrak{p} \in S \mid \mathfrak{p} \textit{ liegt nicht über } \ell\}.$$

Dann gibt es höchstens $\frac{\ell^s-1}{\ell-1}$ Z_ℓ–Erweiterungen von k, die höchstens in S verzweigt sind. Hierbei ist

$$s = \begin{cases} \mathrm{rk}_\ell(\mathrm{Cl}_k) + |S_1| + 2[k:\mathbb{Q}] & \ell > 2 \\ \mathrm{rk}_\ell(\mathrm{Cl}_k) + |S_1| + 2[k:\mathbb{Q}] + r_1 & \ell = 2 \end{cases}$$

Beweis
Die Idee des Beweises ist es, einen Modul $\mathfrak{m}$ so zu wählen, dass alle Z_ℓ–Erweiterungen Teilkörper des Strahlklassenkörpers von $\mathfrak{m}$ sind. Dabei ist klar, dass die unendlichen Stellen nur bei $\ell = 2$ eine Rolle spielen und jeweils höchstens einen Z_2–Faktor zur Strahlklassengruppe beitragen. Daher enthalte $\mathfrak{m}_\infty$ im Fall $\ell = 2$ alle r_1 reellen Stellen, ansonsten wählen wir diese Menge als leer. Wir definieren

$$\mathfrak{m}_0 := \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}},$$

wobei $e_\mathfrak{p} = 1$ für $\mathfrak{p} \in S_1$ gilt. Für $\mathfrak{p} \in S \setminus S_1$ tritt wilde Verzweigung auf und die folgenden Abschätzungen gelten für beliebige $e_\mathfrak{p} > 1$. Wir schätzen nun den ℓ–Rang von $(\mathcal{O}_k/\mathfrak{m}_0)^*$ ab. Mit Hilfe des chinesischen Restsatzes gilt:

$$(\mathcal{O}_k/\mathfrak{m}_0)^* \cong \prod_{\mathfrak{p}\in S}(\mathcal{O}_k/\mathfrak{p}^{e_\mathfrak{p}})^* \text{ für } \mathfrak{m}_0 = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{e_\mathfrak{p}}.$$

Für $e_\mathfrak{p} = 1$ ist $(\mathcal{O}_k/\mathfrak{p})^*$ gerade die multiplikative Gruppe eines endlichen Körpers, welche zyklisch ist. Dies erklärt den $|S_1|$–Teil in obiger Formel. Für größeres $e_\mathfrak{p}$ gilt $(\mathcal{O}_k/\mathfrak{p}^{e_\mathfrak{p}})^* \cong (\mathcal{O}_k/\mathfrak{p})^* \times (1+\mathfrak{p})/(1+\mathfrak{p}^{e_\mathfrak{p}})$. Dieser Fall kann nur auftreten, wenn $\mathfrak{p}$ über ℓ liegt. In diesem Fall ist die Ordnung der multiplikativen Gruppe des Restklassenkörpers koprim zu ℓ, während die zweite Gruppe eine ℓ–Gruppe ist. In [16] wird bewiesen, dass letztere Gruppe durch $[k_\mathfrak{p} : \mathbb{Q}_\ell] + 1$ Elemente erzeugt werden kann. Da

$$\sum_{\ell\in\mathfrak{p}}[k_\mathfrak{p} : \mathbb{Q}_\ell] = [k : \mathbb{Q}]$$

tritt der schlimmste Fall dann auf, wenn alle Primideale über ℓ in S enthalten sind und die zugehörigen Vervollständigungen den Grad 1 haben. In diesem Fall können wir den Beitrag dieser Primstellen in S durch $2[k : \mathbb{Q}]$ abschätzen. Der Beitrag der unverzweigten Erweiterungen zum ℓ–Rang wird durch den ℓ–Rang der Klassengruppe nach oben abgeschätzt. □

Korollar 2.27
Es seien k ein algebraischer Zahlkörper, $S \subseteq \mathbb{P}(k)$ eine endliche Teilmenge sowie $\ell \in \mathbb{P}$. Dann existiert eine Konstante $c(k,\ell)$, so dass die Anzahl der Z_ℓ–Erweiterungen von k, die höchstens in S verzweigt sind, nach oben beschränkt ist durch

$$\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_k)+3[k:\mathbb{Q}]}\ell^{|S|} = c(k,\ell)\ell^{|S|}.$$

Wir werden später (Lemma 4.15) dieses Ergebnis für genau in S verzweigte Z_ℓ–Erweiterungen verschärfen. Den ℓ–Rang der Klassengruppe können wir durch folgenden Satz abschätzen.

Satz 2.28
Für alle $\epsilon > 0$ und alle $n \in \mathbb{N}$ existieren Konstanten $c(n)$ und $c(n,\epsilon)$ derart, dass für alle Zahlkörper $k/\mathbb{Q}$ vom Grad n gilt:

$$|\,\mathrm{Cl}_k\,| \le c(n)d_k^{1/2}\log(d_k)^{n-1} \text{ sowie}$$
$$|\,\mathrm{Cl}_k\,| \le c(n,\epsilon)d_k^{1/2+\epsilon}.$$

Beweis
Die erste Aussage ist Theorem 4.4. in [28, Seite 153]. Die Zweite folgt dann unmittelbar. □

Kapitel 3

Zyklische Erweiterungen und Kranzprodukte

In diesem Kapitel wollen wir uns mit zyklischen Erweiterungen Z_ℓ beschäftigen, wobei ℓ eine Primzahl ist. Einerseits fassen wir Ergebnisse für die Zählfunktion $Z(k, Z_\ell; x)$ und ihrer zugeordneten Dirichletreihe $\Phi_{k,Z_\ell}(s)$ zusammen, wobei uns die Arbeiten von Cohen, Diaz y Diaz und Olivier [6, 7] als Vorlage dienen. Andererseits brauchen wir Verallgemeinerungen auf verwandte Zählfunktionen. Als Anwendung werden wir in Satz 3.29 für Gruppen der Bauart $G = Z_2 \wr H$ die Asymptotik der Funktion $Z(k, G; x)$ untersuchen und für viele H zeigen, dass

$$Z(k, G; x) \sim c(k, G) x^{a(G)}$$

gilt.

In der oben zitierten Arbeit [7, Theorem 1.1] wird folgendes Hauptergebnis bewiesen:

Satz 3.1 (Cohen, Diaz y Diaz, Olivier)
Es seien k ein Zahlkörper und ℓ eine Primzahl. Dann existiert eine explizit berechenbare Konstante $c(k, Z_\ell) > 0$ mit:

$$Z(k, Z_\ell; x) \sim c(k, Z_\ell) x^{a(G)} \log(x)^{b(k,G)}.$$

Hierbei sind $a(G)$ und $b(k, G)$ dieselben Konstanten wie in Vermutung 2.12.

Wir merken an, dass in dieser Arbeit auch bewiesen wird, dass die zugehörige Dirichletreihe $\Phi_{k,Z_\ell}(s)$ (siehe den folgenden Abschnitt) für $\Re(s) > a(G)$ absolut und lokal gleichmäßig konvergiert und bei $s = a(G)$ einen Pol der Ordnung $b(k, G) + 1$ hat. Weiterhin wird gezeigt, dass diese Funktion meromorph nach links fortsetzbar ist.

Wir werden in diesem Kapitel zwei verwandte Zählfunktionen für zyklische Gruppen vom Primzahlgrad untersuchen. Wir fixieren eine endliche Menge $S \subseteq \mathbb{P}(k)$ und definieren

$$Z(k, G, S; x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, d_{K/k} \text{ koprim zu } S, \mathcal{N}(d_{K/k}) \leq x\}|.$$

Wir erhalten dann in Satz 3.9 für ein $c(k, Z_\ell, S) > 0$:

$$c(k, Z_\ell, S) x^{a(Z_\ell)} \log(x)^{b(k,Z_\ell)} \leq Z(k, Z_\ell, S; x) \leq Z(k, Z_\ell; x) \text{ für } x >> 0.$$

Für $G = Z_2$ untersuchen wir auch die zugehörige Dirichletreihe und beweisen in Satz 3.12 das analoge Resultat zu Satz 3.1.

Wir betrachten dann eine weitere Zählfunktion, die diesmal alle Körpererweiterungen, aber mit abgeänderter Diskriminante zählt:

$$Z^S(k, G; x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, \mathcal{N}(d^S_{K/k}) \leq x\}|,$$

wobei $d^S_{K/k}$ den zu S koprimen Anteil von $d_{K/k}$ bezeichnet. Wir beweisen einige Abschätzungen für allgemeine Gruppen (Lemmata 3.14 und 3.15) und erhalten im Satz 3.23 eine Konstante $c(k, Z_\ell) > 0$ mit:

$$Z(k, Z_\ell; x) \leq Z^S(k, Z_\ell; x) \leq c(k, Z_\ell) \ell^{|S|} x^{a(Z_\ell)} \log(x)^{b(k,Z_\ell)}.$$

Für $G = Z_2$ zeigen wir wieder in Satz 3.16 ein analoges Resultat zu Satz 3.1.

Wir haben aus technischen Gründen auf die entsprechenden Aussagen für zyklische Gruppen ungerader Primzahlordnung verzichtet. Wir beweisen sie aber im Abschnitt 3.5 für den Fall $k = \mathbb{Q}$. Da einige technische Details für allgemeine Grundkörper k fehlen, treten hier einige Ideen noch deutlicher hervor.

Im Abschnitt 3.6 geben wir einen Satz an, der die Asymptotik der Zählfunktion von Z_ℓ bestimmt, wenn wir endlich viele lokale Vorgaben fordern.

3.1 Zeta–Funktionen und Heckesche L–Reihen

Wir werden einige Abschätzungen und Eigenschaften für Heckesche L–Reihen benötigen, die wir in diesem Abschnitt zusammenfassen.

Im Folgenden bezeichnet

$$\zeta_k(s) := \prod_{\mathfrak{p} \in \mathbb{P}(k)} (1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s})^{-1}, \quad \Re(s) > 1$$

die *Dedekindsche Zeta–Funktion* von k, welche für $\Re(s) > 1$ absolut und lokal gleichmäßig konvergiert. Weiterhin verwenden wir die Notation $\operatorname{res}_{s=1} \zeta_k(s)$ für das Residuum an der Stelle 1.

Für unsere Verallgemeinerungen von Satz 3.1 benötigen wir die folgenden Abschätzungen der Dedekindschen Zeta–Funktion ζ_k.

Lemma 3.2
Es sei k ein Zahlkörper vom Grad n mit Absolutdiskriminante d_k. Dann gelten:

(1) $|\zeta_k(s)| \leq \zeta_{\mathbb{Q}}(\Re(s))^n$ *für alle s mit* $\Re(s) > 1$.

(2) Für alle $0 < \epsilon \leq 1$ *gilt:*

$$\operatorname*{res}_{s=1} \zeta_k(s) \leq 2^{1+n}(d_k \pi^{-n/2})^{\epsilon} \epsilon^{1-n} \leq 2^{1+n} d_k^{\epsilon} \epsilon^{1-n}.$$

Beweis
Die erste Aussage ist Corollary 3 in [28, Seite 326]. Die zweite Aussage ist ebenfalls Corollary 3 auf Seite 332. □

Für ein Ideal $\mathfrak{c} \subseteq \mathcal{O}_k$ betrachten wir einen Charakter χ der Strahlklassengruppe $\mathrm{Cl}_{\mathfrak{c}}$, d.h. einen Homomorphismus von $\mathrm{Cl}_{\mathfrak{c}}$ nach $\mathbb{C}^*$. Dieser Charakter ist nur für Ideale koprim zu $\mathfrak{c}$ definiert. Sei $S := \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathfrak{p}|\mathfrak{c}\}$ die *Ausnahmemenge*. Für $\mathfrak{p} \in S$ definieren wir $\chi(\mathfrak{p}) = 0$ und setzen somit den Charakter χ multiplikativ auf alle Ideale fort. Wir definieren die *Heckesche L–Reihe*:

$$L_k(\chi, s) := \prod_{\mathfrak{p} \in \mathbb{P}(k)} (1 - \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^s})^{-1}.$$

Dieses Produkt konvergiert für $\Re(s) > 1$ absolut und lokal gleichmäßig. Für weitere Eigenschaften der Heckeschen L–Reihen verweisen wir z.B. auf [28, Seite 343ff].

Wir werden später obere Abschätzungen für $L_k(\chi, s)$ in Streifen der Form $a < \Re(s) \leq 1$ benötigen. Die folgende Aussage folgt direkt aus [17, Gleichung 5.20]. Der Beweis geht ähnlich wie der Beweis von Theorem 7.4 in [28, Seite 350], wobei noch das Konvexitätsprinzip [22, Seite 265] angewendet werden muss.

Satz 3.3
Es seien $\mathfrak{f}$ ein Ideal sowie χ ein Charakter der Strahlklassengruppe $\mathrm{Cl}_{\mathfrak{f}}$. Weiterhin seien $D := d_k \mathcal{N}(\mathfrak{f})$ sowie $\delta = 1$, falls χ der triviale Charakter ist. Ansonsten sei $\delta = 0$. Dann gilt für s mit $0 \leq \sigma := \Re(s) \leq 1$ sowie alle $\epsilon > 0$ die folgende Abschätzung:

$$|(s-1)^{\delta} L_k(s, \chi)| \leq c(\epsilon, n)(D|1+s|^n)^{(1-\sigma)/2+\epsilon}.$$

Wir erhalten das folgende Korollar.

Korollar 3.4
Mit den Notationen aus Satz 3.3 erhalten wir für alle $\epsilon > 0$:

$$|L_k(s,\chi) - \frac{R(\chi)}{s-1}| \leq c(\epsilon,n)(D|1+s|^n)^{(1-\sigma)/2+\epsilon},$$

wobei $R(\chi)$ das Residuum bei $s = 1$ von $L_k(s,\chi)$ bezeichnet. Hierbei ist $R(\chi) = 0$, wenn χ nicht der triviale Charakter ist.

Beweis
Falls χ nicht trivial ist, ist dies gerade die Aussage von Satz 3.3. Für den trivialen Charakter χ mit Ausnahmemenge S erhalten wir:

$$L_k(s,\chi) = \zeta_k(s)\prod_{\mathfrak{p}\in S}(1-\frac{1}{\mathcal{N}(\mathfrak{p})^s}).$$

Damit erhalten wir mit Lemma 3.2 für das Residuum bei $s = 1$:

$$|R(\chi)| \leq \tilde{c}(\epsilon,n)d_k^{\epsilon} \text{ für alle } \epsilon > 0.$$

Zusammen mit Satz 3.3 und der Dreiecksungleichung finden wir eine neue Konstante $c(\epsilon,n)$ mit

$$(s-1)L_k(s,\chi) - R(\chi) \leq c(\epsilon,n)(D|1+s|^n)^{(1-\sigma)/2+\epsilon}.$$

Da $L_k(s,\chi) - R(\chi)/(s-1)$ analytisch in $s = 1$ ist, erhalten wir die gewünschte Abschätzung für kleines $|s-1|$ mit Hilfe des Maximumsprinzips. □

3.2 Quadratische Erweiterungen

Die Anzahl der quadratischen Erweiterungen eines Zahlkörpers haben wir sehr gut unter Kontrolle. In diesem Abschnitt werden wir viele Aussagen aus [6] benutzen. Wir definieren die folgende Dirichletreihe:

$$\Phi_{k,Z_2}(s) = \sum_{[K:k]=2}\frac{1}{\mathcal{N}(d_{K/k})^s} = \sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

a_n ist somit die Anzahl der Körpererweiterungen mit Diskriminantennorm n und somit gilt $a_n \geq 0$. Der folgende Satz wird in [6] bewiesen:

Satz 3.5 (Cohen, Diaz y Diaz, Olivier)
Für einen Zahlkörper k mit $i(k)$ komplexen Einbettungen gilt für $\Re(s) > 1$:

$$\Phi_{k,Z_2}(s) = -1 + \frac{2^{-i(k)}}{\zeta_k(2s)} \sum_{\mathfrak{c}|2\mathcal{O}_k} \mathcal{N}(2\mathcal{O}_k/\mathfrak{c})^{1-2s} \sum_{\chi} L_k(s,\chi),$$

wobei χ die quadratischen Charaktere der Strahlklassengruppe $\mathrm{Cl}_{\mathfrak{c}^2}$ durchläuft und $L_k(s,\chi)$ die Heckesche L–Reihe von k für den Charakter χ ist.

Mit Hilfe von Satz 2.19 wird in [6] das folgende Korollar bewiesen.

Korollar 3.6 (Cohen, Diaz y Diaz, Olivier)

$$Z(k, Z_2; x) \sim 2^{-i(k)} \frac{\mathrm{res}_{s=1}\, \zeta_k(s)}{\zeta_k(2)} x,$$

wobei $2^{-i(k)} \frac{\mathrm{res}_{s=1}\, \zeta_k(s)}{\zeta_k(2)}$ gerade das Residuum in $s = 1$ von Φ_{k,Z_2} ist.

Mit Hilfe von Lemma 3.2 erhalten wir $\mathrm{res}_{s=1}\, \Phi_{k,Z_2}(s) = O_{\epsilon,n}(d_k^{\epsilon})$, wobei die Konstante nur von ϵ und n abhängig ist. Aufgrund der bekannten Eigenschaften der Dedekindschen Zeta–Funktion und der Heckeschen L–Reihen ist klar, dass Φ_{k,Z_2} eine meromorphe Fortsetzung auf $\Re(s) > 0$ besitzt. Wir werden im nächsten Kapitel Abschätzungen dieser Funktion für $\Re(s) \leq 1$ benötigen. Der folgende Satz wird implizit in [6] bewiesen:

Satz 3.7
Die Funktion $\Phi_{k,Z_2}(s)$ hat eine meromorphe Fortsetzung auf $\Re(s) > 1/2$. Sie besitzt in diesem Bereich nur einen einfachen Pol bei $s = 1$ mit Residuum $R(k) = \frac{2^{-i(k)}\, \mathrm{res}_{s=1}\, \zeta_k(s)}{\zeta_k(2)}$. Weiterhin ist die Funktion $g_k(s) := \Phi_{k,Z_2}(s) - \frac{R(k)}{s-1}$ für $\Re(s) > 1/2$ analytisch und es gilt in diesem Bereich für alle $\epsilon > 0$:

$$|g_k(s)| \leq c(\epsilon, [k:\mathbb{Q}])(d_k|1+s|^{[k:\mathbb{Q}]})^{(1-\sigma)/2+\epsilon} d_k^{1/2}.$$

Beweis
Das Residuum bei $s = 1$ erhalten wir aus Korollar 3.6. Mit Hilfe von Satz 3.5 erhalten wir eine Darstellung von Φ_{k,Z_2} als endliche Doppelsumme von Heckeschen L–Reihen, welche sogar für $\Re(s) > 0$ eine meromorphe Fortsetzung besitzen. Die im Nenner auftretende Funktion $\zeta_k(2s)$ ist für $\Re(s) > 1/2$ nullstellenfrei, da sie dort ein Eulerprodukt besitzt. Die Anzahl der Ideale, die $2\mathcal{O}_k$ teilen, sowie die Normen der auftretenden Ideale in der ersten Summe können mit Hilfe einer von $[k:\mathbb{Q}]$ abhängigen Konstante nach oben abgeschätzt werden. Die Anzahl der auftretenden quadratischen Charaktere ist

bis auf eine von $[k:\mathbb{Q}]$ abhängige Konstante gerade die Anzahl der Elemente der Ordnung 2 in der Klassengruppe von k, welche wir mit Satz 2.28 durch $O_{\epsilon,[k:\mathbb{Q}]}(d_k^{1/2+\epsilon})$ abschätzen. Die auftretenden L–Reihen schätzen wir mit Korollar 3.4 ab. Dabei können wir die auftretenden $\mathcal{N}(\mathfrak{f})$ durch eine von $[k:\mathbb{Q}]$ abhängige Konstante abschätzen, da $\mathfrak{f}$ nur von Primidealen über der 2 geteilt wird. Auf diese Weise erhalten wir das gewünschte Ergebnis. □

Die Abschätzung aus dem vorigen Satz wird nützlich sein, wenn wir mit Satz 2.19 Asymptotiken der zugehörigen Zählfunktionen ermitteln wollen. Für die Anwendung dieser Sätze ist nur die meromorphe Fortsetzung auf $\Re(s) = 1$ wichtig. Hier ergibt der obige Satz für alle $\epsilon > 0$:

$$|g_k(s)| \leq c(\epsilon, [k:\mathbb{Q}]) d_k^{1/2+\epsilon} |1+s|^{[k:\mathbb{Q}]\epsilon}.$$

Besonders ärgerlich ist hier der $d_k^{1/2+\epsilon}$–Anteil, durch den wir die Anzahl der Elemente der Ordnung 2 in der Klassengruppe abschätzen. Allgemein wird hier vermutet, dass diese Anzahl $O_{\epsilon,[k:\mathbb{Q}]}(d_k^{\epsilon})$ für alle $\epsilon > 0$ ist. Für $[k:\mathbb{Q}] = 2$ gilt dies aufgrund der Geschlechtertheorie und wird auch im Beweis [6, Section 4] der Asymptotik für D_4–Erweiterungen über $\mathbb{Q}$ benutzt.

3.3 Quadratische Erweiterungen mit Verzweigungsbedingungen

In diesem Abschnitt wollen wir uns zwei Varianten unserer Zählfunktion anschauen. Hierzu definieren wir für eine beliebige transitive Permutationsgruppe G und eine Menge von Primidealen $S \subseteq \mathbb{P}(k)$:

$$Z(k, G, S; x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, d_{K/k} \text{ koprim zu } S, \mathcal{N}(d_{K/k}) \leq x\}|.$$

Trivialerweise gilt $Z(k, G, S; x) \leq Z(k, G; x)$ für alle Mengen S. Die verallgemeinerte Vermutung besagt nun:

Vermutung 3.8
Für endliches $S \subseteq \mathbb{P}(k)$ gilt:

$$Z(k, G, S; x) \sim c(k, G, S) x^{a(G)} \log(x)^{b(k,G)},$$

wobei a und b dieselben Konstanten wie in Vermutung 2.12 sind.

Bevor wir zum quadratischen Fall kommen, wollen wir eine untere Abschätzung für zyklische Gruppen von Primzahlordnung angeben.

Satz 3.9
Es seien k ein Zahlkörper und $S \subseteq \mathbb{P}(k)$ eine endliche Teilmenge. Dann existiert eine Konstante $c(k, Z_\ell, S) > 0$ mit:

$$Z(k, Z_\ell, S; x) \geq c(k, Z_\ell, S) x^{a(Z_\ell)} \log(x)^{b(k, Z_\ell)} \text{ für } x >> 0.$$

Beweis
Der Beweis funktioniert wie der Beweis von [19, Theorem 2.6]. Der einzige Unterschied besteht darin, dass wir in der Induktion für $S = \emptyset$ obige Behauptung als wahr annehmen. Dies dürfen wir, da Vermutung 2.12 für abelsche Gruppen bewiesen ist [33]. □

Wir definieren die zugehörige Dirichletreihe zu $Z(k, Z_2, S; x)$ via

$$\Phi_{k,Z_2,S}(s) = \sum_K \frac{1}{\mathcal{N}(d_{K/k})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

wobei über alle quadratischen Körper K summiert wird, deren Diskriminante koprim zu S ist. Zur Untersuchung dieser Reihe steigen wir in den Beweis des Falls $S = \emptyset$ in [6, Seite 74/75] ein. Dort steht:

$$\Phi_{k,Z_2}(s) = -1 + \frac{2^{r_u(k)+1}}{4^{[k:\mathbb{Q}]s}} \sum_{\mathfrak{c}|(2)} \mathcal{N}(\mathfrak{c})^{2s-1} \prod_{\mathfrak{p}|\mathfrak{c}} (1 - \mathcal{N}(\mathfrak{p})^{-2s}) \sum_{\chi} \sum_{\mathfrak{a} \in A_\mathfrak{c}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s}, \quad (3.1)$$

wobei χ die quadratischen Charaktere der Strahlklassengruppe $\mathrm{Cl}_{\mathfrak{c}^2}$ durchläuft und $A_\mathfrak{c}$ die Menge der quadratfreien Ideale koprim zu $\mathfrak{c}$ ist. $r_u(k)$ ist hier der Einheitenrang von $\mathcal{O}_k$. Die hier gezählten Körpererweiterungen zu $(\mathfrak{a}, \mathfrak{c})$ haben gerade Diskriminante $4\mathfrak{a}/\mathfrak{c}^2$ [6, Prop. 3.4]. Daher müssen wir dafür sorgen, dass wir nur Ideale $\mathfrak{c} \mid (2)$ betrachten, so dass $(2)/\mathfrak{c}$ koprim zu S ist. Sei also $\mathfrak{d}$ gerade das maximale Ideal mit der Eigenschaft, dass $(2)/\mathfrak{d}$ koprim zu S ist. Dadurch, dass wir nicht mehr alle $\mathfrak{c} \mid (2)$ betrachten, ändert sich der Ausdruck (3.1) wie folgt:

$$\Phi_{k,Z_2,S}(s) = -1 + \frac{2^{r_u(k)+1}}{4^{[k:\mathbb{Q}]s}} \sum_{\mathfrak{d}|\mathfrak{c}|(2)} \mathcal{N}(\mathfrak{c})^{2s-1} \prod_{\mathfrak{p}|(\mathfrak{c}/\mathfrak{d})} (1 - \mathcal{N}(\mathfrak{p})^{-2s}) \sum_{\chi} \sum_{\mathfrak{a} \in A_{\mathfrak{c},S}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s},$$

wobei wir $A_{\mathfrak{c},S}$ als die Menge der quadratfreien Ideale koprim zu S und $\mathfrak{c}$ definieren.

Weiterhin wird in dieser Arbeit gezeigt:

$$\sum_{\mathfrak{a} \in A_\mathfrak{c}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \nmid \mathfrak{c}} (1 + \chi(\mathfrak{p}) \mathcal{N}(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p} \nmid \mathfrak{c}} \frac{1 - \mathcal{N}(\mathfrak{p})^{-2s}}{1 - \chi(\mathfrak{p}) \mathcal{N}(\mathfrak{p})^{-s}}$$

$$= \frac{L_k(s,\chi)}{\zeta_k(2s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-2s})}.$$

Nun sei $S = S_2 \dot\cup S_2'$, wobei S_2 gerade alle Primideale über der 2 aus S enthält. Wir beachten, dass $\mathfrak{c}$ stets durch alle Primideale aus S_2 teilbar ist, sowie $\chi(\mathfrak{p}) = 0$ für $\mathfrak{p} \mid \mathfrak{c}$ und erhalten aus der Definition von $A_{\mathfrak{c},S}$:

$$\sum_{\mathfrak{a}\in A_{\mathfrak{c},S}} \frac{\chi(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c},\mathfrak{p}\notin S_2'} (1+\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}\nmid\mathfrak{c},\mathfrak{p}\notin S_2'} \frac{1-\mathcal{N}(\mathfrak{p})^{-2s}}{1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}$$

$$= \frac{L_k(s,\chi)}{\zeta_k(2s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-2s})} \prod_{\mathfrak{p}\in S_2'} \frac{1-\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}{1-\mathcal{N}(\mathfrak{p})^{-2s}}$$

$$= \frac{L_k(s,\chi)}{\zeta_k(2s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-\mathcal{N}(\mathfrak{p})^{-2s})} \prod_{\mathfrak{p}\in S_2'} (1+\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})^{-1}$$

Wir setzen ein und beachten, dass $\mathfrak{d}$ stets koprim zu $\mathfrak{c}/\mathfrak{d}$ ist. Weiterhin nutzen wir aus, dass $\mathcal{N}(2\mathcal{O}_k) = 2^{[k:\mathbb{Q}]}$ sowie $r_u(k)+1+i(k) = [k:\mathbb{Q}]$ gilt, wobei $i(k)$ die Anzahl der komplexen Stellen von k bezeichnet. Wir erhalten:

$$\Phi_{k,Z_2,S}(s) = -1 + \frac{1}{2^{i(k)}\zeta_k(2s)} \sum_{\mathfrak{d}|\mathfrak{c}|(2)} \mathcal{N}(2/\mathfrak{c})^{1-2s} \prod_{\mathfrak{p}|\mathfrak{d}} (1-\mathcal{N}(\mathfrak{p})^{-2s})^{-1}$$

$$\sum_{\chi} L_k(s,\chi) \prod_{\mathfrak{p}\in S_2'} (1+\chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})^{-1}.$$

Aufgrund dieser Darstellung ist nun klar, dass $\Phi_{k,Z_2,S}$ eine auf $\Re(s) > 1/2$ meromorphe Funktion ist, die nur bei $s = 1$ einen Pol besitzt. Bevor wir das Residuum ausrechnen können, benötigen wir noch Eigenschaften der Eulerschen φ–Funktion für Ideale.

Definition 3.10
In Analogie zur herkömmlichen Eulerschen φ–Funktion für ganze Zahlen definieren wir $\varphi(\mathfrak{a}) := |(\mathcal{O}_k/\mathfrak{a})^*|$ für $\mathfrak{a} \trianglelefteq \mathcal{O}_k$.

Die folgenden Eigenschaften folgen aus elementaren Rechnungen.

Satz 3.11
Es gelten:

(1) $\varphi(\mathfrak{ab}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$ *für koprime Ideale* $\mathfrak{a},\mathfrak{b} \subseteq \mathcal{O}_k$,

(2) $\varphi(\mathfrak{p}^j) = \mathcal{N}(\mathfrak{p})^{j-1}(\mathcal{N}(\mathfrak{p})-1)$ *für alle Primideale* $\mathfrak{p}$ *und* $j \in \mathbb{N}$,

(3) $\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}(\mathfrak{p})) = \varphi(\mathfrak{c})/\mathcal{N}(\mathfrak{c})$ *für Ideale* $\mathfrak{c} \subseteq \mathcal{O}_k$,

(4) $\sum_{\mathfrak{c}|\mathfrak{a}} \varphi(\mathfrak{c}) = \mathcal{N}(\mathfrak{a})$ *für Ideale* $\mathfrak{a} \subseteq \mathcal{O}_k$.

Satz 3.12
Für endliches $S \subseteq \mathbb{P}(k)$ *ist die Dirichletreihe* $\Phi_{k,Z_2,S}$ *für* $\Re(s) > 1$ *absolut und lokal gleichmäßig konvergent. Sie besitzt bei* $s = 1$ *einen einfachen Pol mit Residuum*

$$\frac{\operatorname{res}_{s=1}\zeta_k(s)}{2^{i(k)}\zeta_k(2)} \prod_{\mathfrak{p}\in S}(1+1/\mathcal{N}(\mathfrak{p}))^{-1}.$$

Die Funktion ist auf den Bereich $\Re(s) > 1/2$ *meromorph fortsetzbar, wobei* $s = 1$ *der einzige Pol in diesem Bereich ist.*

Beweis
Die analytische Fortsetzung wurde bereits durch die Rechnungen vor diesem Satz bewiesen. Es verbleibt das Residuum auszurechnen. Die auftretenden Heckeschen L–Reihen sind meromorphe Funktionen für $\Re(s) > 1/2$, wobei höchstens bei $s = 1$ ein einfacher Pol auftreten kann. Dies kann nur passieren, wenn χ der triviale Charakter $\chi_{0,\mathfrak{c}}$ ist. In diesem Fall gilt für das Residuum:

$$\operatorname*{res}_{s=1} L_k(s,\chi_{0,\mathfrak{c}}) = \operatorname*{res}_{s=1}\zeta_k(s)\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}(\mathfrak{p})).$$

Wir definieren $\mathfrak{b} := \prod_{\mathfrak{p}\in S_2'}\mathfrak{p}$ sowie $A := \frac{\operatorname{res}_{s=1}\zeta_k(s)}{2^{i(k)}\zeta_k(2)}$ und schreiben kürzer:

$$D := \prod_{\mathfrak{p}|\mathfrak{d}}(1-\mathcal{N}(\mathfrak{p})^{-2})^{-1} \text{ und } B := \prod_{\mathfrak{p}\in S_2'}(1+1/\mathcal{N}(\mathfrak{p}))^{-1}.$$

Wir erhalten für das Residuum von $\Phi_{k,Z_2,S}$ an der Stelle $s = 1$:

$$ABD\sum_{\mathfrak{d}|\mathfrak{c}|(2)}\mathcal{N}(2/\mathfrak{c})^{-1}\prod_{\mathfrak{p}|\mathfrak{c}}(1-1/\mathcal{N}(\mathfrak{p}))$$

$$= ABD\sum_{\mathfrak{d}|\mathfrak{c}|(2)}\frac{\mathcal{N}(\mathfrak{c})}{\mathcal{N}(2\mathcal{O}_k)}\frac{\varphi(\mathfrak{c})}{\mathcal{N}(\mathfrak{c})} \text{ (mit Satz 3.11 (3))}$$

$$= ABD\sum_{\mathfrak{c}|((2)/\mathfrak{d})}\frac{\varphi(\mathfrak{c}\mathfrak{d})}{\mathcal{N}(2\mathcal{O}_k)} = ABD\frac{\varphi(\mathfrak{d})}{\mathcal{N}(2\mathcal{O}_k)}\sum_{\mathfrak{c}|((2)/\mathfrak{d})}\varphi(\mathfrak{c})$$

$$= ABD\frac{\varphi(\mathfrak{d})}{\mathcal{N}(2\mathcal{O}_k)}\mathcal{N}(2\mathcal{O}_k/\mathfrak{d}) = ABD\frac{\varphi(\mathfrak{d})}{\mathcal{N}(\mathfrak{d})} \text{ (mit Satz 3.11 (4))}$$

$$= AB \prod_{\mathfrak{p}|\mathfrak{d}} (1 - \mathcal{N}(\mathfrak{p})^{-2})^{-1} \prod_{\mathfrak{p}|\mathfrak{d}} (1 - 1/\mathcal{N}(\mathfrak{p})) = AB \prod_{\mathfrak{p}|\mathfrak{d}} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1}$$

$$= A \prod_{\mathfrak{p} \in S} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1}.$$

□

Interessanterweise zeigt sich beim Residuum, dass es nicht mehr nötig ist zwischen zahm und wild verzweigten Primidealen zu unterscheiden. Asymptotisch mittelt sich das heraus. Betrachten wir den interessanten Spezialfall $k = \mathbb{Q}$. Alle auftretenden Charaktere sind trivial, d.h. $L_{\mathbb{Q},\chi_{0,2}} = (1-1/2^s)\zeta(s)$ und $L_{\mathbb{Q},\chi_{0,1}} = \zeta(s)$.

Korollar 3.13

$$\Phi_{\mathbb{Q},Z_2,S}(s) = -1 + \frac{\zeta(s)}{\zeta(2s)} \prod_{\mathfrak{p} \in S} (1 + \mathcal{N}(\mathfrak{p})^{-s})^{-1} \textit{ falls } (2) \in S,$$

$$\Phi_{\mathbb{Q},Z_2,S}(s) = -1 + \frac{\zeta(s)}{\zeta(2s)} \prod_{\mathfrak{p} \in S_2'} (1 + \mathcal{N}(\mathfrak{p})^{-s})^{-1} (2^{1-2s} + (1 - 1/2^s)) \textit{ sonst.}$$

Für das Residuum ergibt sich:

$$\operatorname*{res}_{s=1} \Phi_{\mathbb{Q},Z_2,S}(s) = \frac{\operatorname{res}_{s=1} \zeta(s)}{\zeta(2)} \prod_{\mathfrak{p} \in S} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1}.$$

Beweis
Durch einfaches Einsetzen von $k = \mathbb{Q}$ in unsere Formel für $\Phi_{k,Z_2,S}(s)$. □

3.4 Die modifizierte Zählfunktion

Für eine ganze Zahl a und eine Menge S von Primzahlen bezeichnen wir mit a^S den zu S koprimen Anteil von a. Analog bezeichnen wir für eine Menge $S \subseteq \mathbb{P}(k)$ und ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_k$ mit $\mathfrak{a}^S$ den zu $\mathfrak{a}$ koprimen Anteil. Weiterhin definieren wir eine modifizierte Zählfunktion via:

$$Z^S(k, G; x) := |\{K/k \mid \mathrm{Gal}(K/k) = G, \mathcal{N}(d_{K/k}^S) \leq x\}|.$$

Der Unterschied zu $Z(k, G, S; x)$ ist, dass hier alle Körpererweiterungen gezählt werden, aber deren Diskriminanten modifiziert werden. Trivialerweise gilt für alle S:

$$Z(k, G; x) \leq Z^S(k, G; x).$$

Es gilt aber auch eine Art Umkehrung, welche eine leichte Verschärfung von Lemma 2.1 in [19] ist.

Lemma 3.14
Es seien G eine endliche Gruppe, k ein Zahlkörper vom Grad m und $S \subseteq \mathbb{P}(k)$ eine endliche Menge von Primidealen. Dann existiert eine Konstante $c(m,S,G) \geq 1$ mit folgender Eigenschaft:

$$Z^S(k,G;x/c(m,S,G)) \leq Z(k,G;x) \leq Z^S(k,G;x) \leq Z(k,G;c(m,S,G)x).$$

Beweis
Die Ungleichung $Z(k,G;x) \leq Z^S(k,G;x)$ gilt nach Definition. Sei nun K/k eine beliebige Erweiterung mit $\mathrm{Gal}(K/k) = G$. Für $\mathfrak{p} \in S$ sowie $p \in \mathfrak{p} \cap \mathbb{P}$ gibt es eine bekannte obere Schranke für den maximalen Exponenten e, so dass $p^e \mid \mathcal{N}(d_{K/k})$ gilt [31, Remark 1, Seite 16]. Diese Schranke ist nur abhängig von m, p und G. Wir definieren $c(m,S,G)$ als das Produkt über diese p–Potenzen für alle $\mathfrak{p} \in S$. Damit erhalten wir folgende Abschätzung für alle K/k mit $\mathrm{Gal}(K/k) = G$:

$$c(m,S,G)\mathcal{N}(d^S_{K/k}) \geq \mathcal{N}(d_{K/k}).$$

Hieraus folgt dann die erste und dritte Ungleichung. □

Falls wir entweder eine untere Abschätzung für $Z^S(k,G;x)$ oder eine obere Abschätzung für $Z(k,G;x)$ kennen, so erhalten wir noch stärker:

Lemma 3.15
Es seien G eine endliche Gruppe, k ein Zahlkörper vom Grad m und $S \subseteq \mathbb{P}(k)$ eine endliche Menge von Primidealen. Wir bezeichnen mit $a > 0$, $b \geq 0$ und $c(k,S) > 0$ weitere Konstanten.

(1) Aus $Z^S(k,G;x) \geq c(k,S)x^a \log(x)^b$ für $x >> 0$ folgt

$$Z(k,G;x) \geq \frac{c(k,S)}{\tilde{c}(m,S,G)^a} x^a \log(x)^b \text{ für } x >> 0.$$

(2) Aus $Z(k,G;x) \leq c(k,S)x^a \log(x)^b$ folgt

$$Z^S(k,G;x) \leq \tilde{c}(m,S,G)^a c(k,S) x^a \log(x)^b.$$

Beweis
Im ersten Fall erhalten wir mit Lemma 3.14

$$Z(k,G;x) \geq Z^S(k,G;x/c(m,S,G))$$

$$\geq c(k,S)c(m,S,G)^{-a}x^a \log(x/c(m,S,G))^b.$$

Wenn wir nun $\tilde{c}(m,S,G) > c(m,S,G)$ groß genug wählen, dann folgt die Behauptung für x groß genug.

Im zweiten Fall gilt nach Lemma 3.14

$$Z^S(k,G;x) \leq Z(k,G;c(m,S,G)x)$$

$$\leq c(k,S)c(m,S,G)^a x^a(\log(x)+\log(c(m,S,G)))^b,$$

welches sich asymptotisch wie gewünscht verhält. □

Im Folgenden sei Φ^S_{k,Z_ℓ} für $\ell \in \mathbb{P}$ die zu $Z^S(k,Z_\ell;x)$ assoziierte Dirichletreihe

$$\Phi^S_{k,Z_\ell}(s) = \sum_{[K:k]=2} \frac{1}{\mathcal{N}(d^S_{K/k})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Im Fall $\ell = 2$ geben wir analog zu Abschnitt 3.3 einen Beweis für die Asymptotik von $Z^S(k,Z_2;x)$ bzw. das analytische Verhalten der Funktion Φ^S_{k,Z_2} für beliebige Grundkörper k an. In diesem Abschnitt hatten wir den Beweis aus [6] so modifiziert, dass wir alle Erweiterungen weggelassen hatten, die in einem $\mathfrak{p} \in S$ verzweigt waren. Dabei hatten wir $S = S_2 \dot\cup S_2'$ geschrieben, wobei S_2 genau die Primideale über der 2 aus S enthält. Für ein Ideal $\mathfrak{c} \mid (2)$ definieren wir $B_{\mathfrak{c},S}$ als die Menge der quadratfreien Ideale koprim zu $\mathfrak{c}$, deren sämtliche Primteiler in S liegen. Im Abschnitt 3.3 hatten wir genau diese Ideale weggelassen, um die Funktion $\Phi_{k,Z_2,S}$ zu bestimmen. Wir merken an, dass hier eine quadratische Erweiterung, die zu $(\mathfrak{c},\mathfrak{ab})$ mit $\mathfrak{c} \mid (2), \mathfrak{a} \in A_{\mathfrak{c},S}$ und $\mathfrak{b} \in B_{\mathfrak{c},S}$ assoziiert ist, mit Diskriminante $4\mathfrak{a}/\mathfrak{c}^2$ berücksichtigt wird. Hierbei hatten wir das Ideal $\mathfrak{c}$ für die Sonderbehandlung der Primideale über der 2 benötigt. Auch hier müssen wir dafür sorgen, dass die entsprechenden Erweiterungen mit zu S koprimer Diskriminante gezählt werden. Dieses wird durch den Term $\mathcal{N}(\frac{\mathfrak{d}}{\mathrm{ggT}(\mathfrak{c},\mathfrak{d})})^{2s}$ erreicht, wobei $\mathfrak{d}$ der maximale Teiler von (2) ist, so dass $(2)/\mathfrak{d}$ koprim zu S ist. Weiterhin schreiben wir $\mathfrak{c} = \mathfrak{c}_1\mathfrak{c}_2$ mit $\mathfrak{c}_1 \mid (2)/\mathfrak{d}, \mathfrak{c}_2 \mid \mathfrak{d}$ und erhalten wegen $\mathfrak{c}_2 = \mathrm{ggT}(\mathfrak{c},\mathfrak{d})$:

$$\Phi^S_{k,Z_2}(s) = -1 + \frac{2^{r_u(k)+1}}{4^{[k:\mathbb{Q}]s}} \sum_{\mathfrak{c}_1 \mid (2)/\mathfrak{d}} \sum_{\mathfrak{c}_2 \mid \mathfrak{d}} \mathcal{N}(\frac{\mathfrak{d}}{\mathfrak{c}_2})^{2s} \mathcal{N}(\mathfrak{c}_1\mathfrak{c}_2)^{2s-1}$$

$$\prod_{\mathfrak{p}\mid\mathfrak{c}_1}(1-\mathcal{N}(\mathfrak{p})^{-2s}) \prod_{\mathfrak{p}\mid\mathfrak{c}_2}(1-1^{-2s}) \sum_{\chi} \sum_{\mathfrak{a}\in A_{\mathfrak{c}_1\mathfrak{c}_2,S}} \sum_{\mathfrak{b}\in B_{\mathfrak{c}_1\mathfrak{c}_2,S}} \frac{\chi(\mathfrak{ab})}{\mathcal{N}(\mathfrak{a})^s}.$$

$$= -1 + \frac{\mathcal{N}(\mathfrak{d}^{2s})\mathcal{N}(2)^{1-2s}}{2^{i(k)}} \sum_{\mathfrak{c}_1 \mid (2)/\mathfrak{d}} \mathcal{N}(\mathfrak{c}_1)^{2s-1} \prod_{\mathfrak{p}\mid\mathfrak{c}_1}(1-\mathcal{N}(\mathfrak{p})^{-2s})$$

$$\sum_{\chi} \sum_{\mathfrak{a} \in A_{\mathfrak{c}_1,S}} \sum_{\mathfrak{b} \in B_{\mathfrak{c}_1,S}} \frac{\chi(\mathfrak{ab})}{\mathcal{N}(\mathfrak{a})^s}.$$

Wie im Abschnitt 3.3 gilt: $N(2\mathcal{O}_k) = 2^{[k:\mathbb{Q}]}$ sowie $r_u(k) + 1 + i(k) = [k : \mathbb{Q}]$. Analog wie im Abschnitt 3.3 erhalten wir:

$$\sum_{\mathfrak{a} \in A_{\mathfrak{c}_1,S}} \sum_{\mathfrak{b} \in B_{\mathfrak{c}_1,S}} \frac{\chi(\mathfrak{ab})}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \nmid \mathfrak{c}_1, \mathfrak{p} \notin S} (1 + \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}) \prod_{\mathfrak{p} \nmid \mathfrak{c}_1, \mathfrak{p} \in S} (1 + \chi(\mathfrak{p}))$$

$$= \prod_{\mathfrak{p} \nmid \mathfrak{c}_1, \mathfrak{p} \notin S} \frac{1 - \mathcal{N}(\mathfrak{p})^{-2s}}{1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}} \prod_{\mathfrak{p} \in S} (1 + \chi(\mathfrak{p}))$$

$$= \frac{L_k(s,\chi)}{\zeta_k(2s) \prod_{\mathfrak{p}|\mathfrak{c}_1} (1 - \mathcal{N}(\mathfrak{p})^{-2s})} \prod_{\mathfrak{p} \in S} \frac{1 - \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s}}{1 - \mathcal{N}(\mathfrak{p})^{-2s}} \prod_{\mathfrak{p} \in S} (1 + \chi(\mathfrak{p}))$$

$$= \frac{L_k(s,\chi)}{\zeta_k(2s) \prod_{\mathfrak{p}|\mathfrak{c}_1} (1 - \mathcal{N}(\mathfrak{p})^{-2s})} \prod_{\mathfrak{p} \in S} \frac{(1 + \chi(\mathfrak{p}))}{(1 + \chi(\mathfrak{p})\mathcal{N}(\mathfrak{p})^{-s})^{-1}}.$$

Damit erhalten wir durch Einsetzen:

$$\Phi^S_{k,Z_2}(s) = -1 + \frac{\mathcal{N}(\mathfrak{d}^{2s})\mathcal{N}(2)^{1-2s}}{2^{i(k)}\zeta_k(2s)} \sum_{\mathfrak{c}_1 | (2)/\mathfrak{d}} \mathcal{N}(\mathfrak{c}_1)^{2s-1} \sum_{\chi} L_k(s,\chi) \prod_{\mathfrak{p} \in S} \frac{1 + \chi(\mathfrak{p})}{1 + \frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^s}}.$$

Wir erhalten das Analogon zu Satz 3.12. Dabei verweisen wir für die Interpretation des Ideals $\mathfrak{d}$ auf die Ausführungen nach Satz 3.25.

Satz 3.16
Für endliches $S \subseteq \mathbb{P}(k)$ ist die Dirichletreihe Φ^S_{k,Z_2} für $\Re(s) > 1$ absolut und lokal gleichmäßig konvergent. Sie besitzt bei $s = 1$ einen einfachen Pol mit Residuum

$$\frac{\operatorname{res}_{s=1} \zeta_k(s)}{2^{i(k)}\zeta_k(2)} \prod_{\mathfrak{p} \in S} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1} 2^{|S|} \mathcal{N}(\mathfrak{d}),$$

wobei $\mathfrak{d}$ der größte Teiler von $2\mathcal{O}_k$ ist, so dass $(2)/\mathfrak{d}$ koprim zu S ist. Die Funktion ist auf den Bereich $\Re(s) > 1/2$ meromorph fortsetzbar, wobei $s = 1$ der einzige Pol in diesem Bereich ist.

Beweis
Wir definieren

$$A := \frac{\operatorname{res}_{s=1} \zeta_k(s)}{2^{i(k)}\zeta_k(2)} \text{ sowie } B := \prod_{\mathfrak{p} \in S} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1} 2^{|S|}.$$

Mit dem analogen Schluss wie im Beweis zu Satz 3.12 für die trivialen Charaktere erhalten wir für das Residuum an der Stelle $s = 1$ folgenden Ausdruck, wobei wir $\chi(\mathfrak{p}) = 0$ für $\mathfrak{p} \mid \mathfrak{c}_1$ beachten:

$$AB\frac{\mathcal{N}(\mathfrak{d}^2)}{\mathcal{N}(2)} \sum_{\mathfrak{c}_1|(2)/\mathfrak{d}} \mathcal{N}(\mathfrak{c}_1) \prod_{\mathfrak{p}|\mathfrak{c}_1} (1 - 1/\mathcal{N}(\mathfrak{p}))$$

$$= AB\frac{\mathcal{N}(\mathfrak{d}^2)}{\mathcal{N}(2)} \sum_{\mathfrak{c}_1|(2)/\mathfrak{d}} \mathcal{N}(\mathfrak{c}_1)\frac{\phi(\mathfrak{c}_1)}{\mathcal{N}(\mathfrak{c}_1)} \text{ (mit Satz 3.11 (3))}$$

$$= AB\frac{\mathcal{N}(\mathfrak{d}^2)}{\mathcal{N}(2)}\mathcal{N}((2)/\mathfrak{d}) = AB\mathcal{N}(\mathfrak{d}).$$

In den letzten Umformungen haben wir zweimal Satz 3.11 ausgenutzt. □

Wir betrachten jetzt die Funktion

$$g_{k,S}(s) := \Phi^S_{k,Z_2}(s) - \frac{\mathrm{res}_{s=1}\, \Phi^S_{k,Z_2}(s)}{s-1},$$

welche nach obigem Satz analytisch für $\Re(s) > 1/2$ ist. Wir wollen nun das analoge Ergebnis zu Satz 3.7 angeben.

Satz 3.17
Die Funktion $g_{k,S}(s)$ ist für $\Re(s) > 1/2$ analytisch und es gilt für alle $\epsilon > 0$:

$$|g_{k,S}(s)| \leq c(\epsilon, [k:\mathbb{Q}])2^{|S|}(d_k|1+s|^{[k:\mathbb{Q}]})^{(1-\sigma)/2+\epsilon} d_k^{1/2}.$$

Beweis
Die Funktion Φ^S_{k,Z_2} unterscheidet sich von der Funktion Φ_{k,Z_2} einerseits durch das Weglassen von Summanden, andererseits werden Summanden mit

$$\mathcal{N}(\mathfrak{d}^{2s}) \text{ bzw. mit } \prod_{\mathfrak{p}\in S} \frac{1+\chi(\mathfrak{p})}{1+\frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^s}}$$

durchmultipliziert. Wegen $\chi(\mathfrak{p}) \neq 0$ für alle $\mathfrak{p} \in S$ sowie $\chi(\mathfrak{p}) = \pm 1$ erhalten wir für $\Re(s) > 0$:

$$\left|\prod_{\mathfrak{p}\in S} \frac{1+\chi(\mathfrak{p})}{1+\frac{\chi(\mathfrak{p})}{\mathcal{N}(\mathfrak{p})^s}}\right| \leq \prod_{\mathfrak{p}\in S} \frac{2}{1+\frac{1}{|\mathcal{N}(\mathfrak{p})^s|}} \leq 2^{|S|}.$$

Weiterhin ist $|\mathcal{N}(\delta^{2s})|$ für $1/2 < \Re(s) \leq 1$ durch eine von $[k:\mathbb{Q}]$ abhängige Konstante nach oben beschränkt, da $\mathfrak{d}$ nur von Idealen über der 2 geteilt wird. Damit folgt das gewünschte Ergebnis wie im Beweis von Satz 3.7. □

3.5 Z_ℓ–Erweiterungen mit Verzweigungsbedingungen

Für zyklische Gruppen Z_ℓ von ungerader Primzahlordnung könnten wir die analogen Aussagen wie in den Sätzen 3.16 und 3.17 beweisen. Hierzu müssten wir den Beweis in [7] analog zum Z_2–Fall variieren. Da dies ist aber sehr technisch und lang ist, geben wir hier einen Reduktionssatz an, der in vielen (wichtigen) Spezialfällen anwendbar ist, z.B. immer für den Fall $k = \mathbb{Q}$. Es sei also im Folgenden ℓ eine ungerade Primzahl. Mit Hilfe des Satzes von Kronecker–Weber sehen wir, dass eine Primzahl p in einer Z_ℓ–Erweiterung von $\mathbb{Q}$ genau dann verzweigt sein kann, wenn $p = \ell$ oder $p \equiv 1 \bmod \ell$ gilt. Weiterhin gibt es genau eine Z_ℓ–Erweiterung, die genau in einem solchen p verzweigt ist. Diese Erweiterung hat Diskriminante $p^{\ell-1}$, falls $p \neq \ell$. Ansonsten ist die Diskriminante $\ell^{2\ell-2}$.

Lemma 3.18
Es seien ℓ eine ungerade Primzahl und $K/\mathbb{Q}$ die Z_ℓ–Erweiterung, die nur in p verzweigt ist. Weiterhin sei $L \neq K$ eine Z_ℓ–Erweiterung, die in p verzweigt ist. Dann existiert in $KL/\mathbb{Q}$ genau ein Teilkörper $M =: \Psi(L)$ vom Grad ℓ, der in p unverzweigt ist. Je $\ell - 1$ Körper korrespondieren auf diese Weise zur selben in p unverzweigten Z_ℓ–Erweiterung. Es gilt: $d_M d_K = d_L$.

Beweis
Für $p \neq \ell$ ist dies Abhyankar's Lemma [28, Seite 236] bzw. Lemma 2.4. Für $p = \ell$ liegt es daran, dass es nach Kronecker–Weber keine in ℓ total verzweigte $Z_\ell \times Z_\ell$–Erweiterung von $\mathbb{Q}$ gibt. □

Wir merken an, dass die Aussage dieses Lemmas für zahm verzweigte Primideale auch für beliebige Grundkörper k gültig ist (unter der Annahme, dass ein K/k existiert, welches nur in $\mathfrak{p}$ verzweigt ist). Bei Primidealen, die über ℓ liegen, stimmt diese Aussage dann nicht mehr, wie das folgende Beispiel zeigt.

Beispiel 3.19
Es sei $k = \mathbb{Q}(\zeta_3)$, wobei ζ_3 eine dritte Einheitswurzel und $\mathfrak{p}$ das eindeutige Primideal ist, welches über (3) liegt. Dann sind $K_1 = k(\sqrt[3]{3})$ und $K_2 = k(\sqrt[3]{\zeta_3})$ nur in $\mathfrak{p}$ verzweigt und die Galoisgruppen sind jeweils Z_3. Da K_1K_2/k total verzweigt ist, ist $\mathfrak{p}$ in jedem Zwischenkörper vom Grad 3 verzweigt.

Satz 3.20
Es seien $S \subseteq \mathbb{P}(\mathbb{Q})$ eine endliche Teilmenge und $\ell > 2$ eine Primzahl. Dann gilt: $\Phi_{\mathbb{Q},Z_\ell,S}$ ist für $\Re(s) > 1/(\ell - 1)$ eine lokal gleichmäßig und absolut

konvergente Dirichletreihe mit einem einfachen Pol in $s = 1/(\ell - 1)$. *Die Funktion ist meromorph auf* $\Re(s) > 1/(2\ell - 2)$ *fortsetzbar und es gilt:*

$$Z(\mathbb{Q}, Z_\ell, S; x) \sim c(\ell, S) Z(\mathbb{Q}, Z_\ell; x),$$

wobei $0 < c(\ell, S) \leq 1$ *am Ende des Beweises angegeben wird.*

Beweis
Sei $(p) \in S$ ein Primideal mit der Eigenschaft, dass eine Körpererweiterung $K/\mathbb{Q}$ existiert mit $\mathrm{Gal}(K/\mathbb{Q}) = Z_\ell$, welche nur in p verzweigt ist. Wir definieren folgende Abbildung via Lemma 3.18:

$$\Psi : \{L/\mathbb{Q} \mid \mathrm{Gal}(L/\mathbb{Q}) = Z_\ell, p \mid d_L\} \setminus \{K\} \to \{L/\mathbb{Q} \mid \mathrm{Gal}(L/\mathbb{Q}) = Z_\ell, p \nmid d_L\}.$$

Diese Abbildung ist surjektiv und jedes Bild besitzt genau $\ell - 1$ Urbilder. Daher erhalten wir die folgende Beziehung für die Zählfunktionen:

$$Z(\mathbb{Q}, Z_\ell; x) = Z(\mathbb{Q}, Z_\ell, \{p\}; x) + (\ell - 1) Z(\mathbb{Q}, Z_\ell, \{p\}; x/d_K) + a(x),$$

wobei $a(x) = 1$ für $x \geq \mathcal{N}(d_K)$ ist. Ansonsten gilt $a(x) = 0$. Damit gilt für die zugehörigen Dirichletreihen:

$$\Phi_{\mathbb{Q}, Z_\ell}(s) = \Phi_{\mathbb{Q}, Z_\ell, \{p\}}(s) + \frac{\ell - 1}{d_K^s} \Phi_{\mathbb{Q}, Z_\ell, \{p\}}(s) + \frac{1}{d_K^s}.$$

O.B.d.A. können wir annehmen, dass in S nur Primideale enthalten sind, so dass eine nur in diesem Ideal verzweigte Z_ℓ–Erweiterung $K_i/\mathbb{Q}$ $(1 \leq i \leq |S|)$ existiert. Wir erhalten induktiv:

$$\Phi_{\mathbb{Q}, Z_\ell}(s) = \Phi_{\mathbb{Q}, Z_\ell, S}(s) \prod_{i=1}^{|S|} (1 + \frac{\ell - 1}{d_{K_i}^s}) + \frac{1}{\ell - 1} \left(\prod_{i=1}^{|S|} (1 + \frac{\ell - 1}{d_{K_i}^s}) - 1 \right).$$

Hierbei zählt

$$\frac{1}{\ell - 1} \left(\prod_{i=1}^{|S|} (1 + \frac{\ell - 1}{d_{K_i}^s}) - 1 \right)$$

gerade alle Z_ℓ–Erweiterungen, die als Teilkörper von $K_1 \cdots K_{|S|}/\mathbb{Q}$ auftreten. Wir merken an, dass es jeweils genau $(\ell - 1)^{j-1}$ Z_ℓ–Erweiterungen gibt, die in denselben j Primzahlen verzweigt sind. Damit gilt:

$$\Phi_{\mathbb{Q}, Z_\ell, S}(s) = \frac{\Phi_{\mathbb{Q}, Z_\ell}(s) - \frac{1}{\ell - 1} \left(\prod_{i=1}^{|S|} (1 + \frac{\ell - 1}{d_{K_i}^s}) - 1 \right)}{\prod_{i=1}^{|S|} (1 + \frac{\ell - 1}{d_{K_i}^s})}$$

$$= \left(\prod_{i=1}^{|S|}(1+\frac{\ell-1}{d_{K_i}^s})\right)^{-1} \Phi_{\mathbb{Q},Z_\ell}(s) - \frac{1}{\ell-1} + \left((\ell-1)\prod_{i=1}^{|S|}(1+\frac{\ell-1}{d_{K_i}^s})\right)^{-1}.$$

Alle beteiligten Funktionen auf der rechten Seite außer $\Phi_{\mathbb{Q},Z_\ell}$ sind für $\Re(s) > 0$ analytisch. Damit haben $\Phi_{\mathbb{Q},Z_\ell}$ und $\Phi_{\mathbb{Q},Z_\ell,S}$ dieselben Pole und sind im selben Bereich meromorphe Funktionen. Die entsprechende Aussage für $\Phi_{\mathbb{Q},Z_\ell}$ wird in [7, Prop. 4.6] bewiesen. Zur Bestimmung der asymptotischen Aussage müssen wir die Funktionen an der Stelle $s = 1/(\ell-1)$ auswerten. Wir erhalten also

$$c(\ell,S) = \prod_{(p)\in S\setminus\{(\ell)\}}(1+\frac{\ell-1}{p})^{-1} \prod_{(p)\in S\cap\{(\ell)\}}(1+\frac{\ell-1}{p^2})^{-1}.$$

□

Wir merken an, dass obiger Beweis im Prinzip auch für Z_2–Erweiterungen funktioniert. Hier gibt es aber drei nur in 2 verzweigte Erweiterungen: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\sqrt{-2})$. Hier müssten wir mit zwei dieser Erweiterungen im Beweis arbeiten. Für die ungeraden Primzahlen ändert sich nichts.

Für die modifizierte Zählfunktion erhalten wir den folgenden Satz, den wir analog zu Satz 3.20 beweisen können.

Satz 3.21
Es seien ℓ eine ungerade Primzahl und $S \subseteq \{p \in \mathbb{P}(\mathbb{Q}) \mid p \equiv 1 \bmod \ell$ oder $p = \ell\}$ eine endliche Teilmenge. Dann gilt: $\Phi^S_{\mathbb{Q},Z_\ell}$ ist für $\Re(s) > 1/(\ell-1)$ eine absolut konvergente Dirichletreihe mit einem einfachen Pol in $s = 1/(\ell-1)$. Die Funktion ist meromorph auf $\Re(s) > 1/(2\ell-2)$ fortsetzbar und es gilt:

$$Z^S(\mathbb{Q}, Z_\ell; x) \sim \ell^{|S|} c(\ell,S) Z(\mathbb{Q}, Z_\ell; x),$$

wobei $0 < c(\ell,S) \leq 1$ die in Satz 3.20 bestimmte Konstante ist.

Beweis
Wir zählen die Körpererweiterungen wie im Beweis von Satz 3.20. Der einzige Unterschied besteht darin, dass wir die Diskriminanten $d^s_{K_i}$ weglassen. Wir erhalten:

$$\Phi^S_{\mathbb{Q},Z_\ell}(s) = \Phi_{\mathbb{Q},Z_\ell,S}(s)\prod_{i=1}^{|S|}(1+\ell-1) + \frac{1}{\ell-1}\left(\prod_{i=1}^{|S|}(1+\ell-1)-1\right)$$

$$= \ell^{|S|}\Phi_{\mathbb{Q},Z_\ell,S}(s) + \frac{\ell^{|S|}-1}{\ell-1}.$$

□

Wir werden später noch eine obere Abschätzung für allgemeine Grundkörper k brauchen, die für alle $x > 0$ gilt. Für $k = \mathbb{Q}$ folgt diese Aussage wegen $c(\ell, S) \leq 1$ direkt aus Satz 3.21. Gleiches würde auch für beliebige Grundkörper gelten, wenn wir die Ergebnisse aus [7] entsprechend verallgemeinert hätten. Wir benötigen noch einige Hilfsaussagen.

Lemma 3.22
Es seien k ein Zahlkörper, $\ell \in \mathbb{P}$ und $T := \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathcal{N}(\mathfrak{p}) \equiv 1 \bmod \ell\}$. Weiterhin sei

$$\prod_{\mathfrak{p} \in T} \left(1 + \frac{\ell - 1}{\mathcal{N}(\mathfrak{p})^s}\right) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Dann gilt mit $e := \frac{\ell-1}{[k(\zeta_\ell):k]}$ für alle $x > 0$:

$$\sum_{n \leq x} a_n \leq c(k, \ell) x \log(x)^{e-1}.$$

Beweis
Wir erhalten folgende Identität für alle $\mathfrak{p} \in T$:

$$(1+(\ell-1)\mathcal{N}(\mathfrak{p})^{-s})(1-\mathcal{N}(\mathfrak{p})^{-s})^{\ell-1} = 1 - \binom{\ell}{2}\mathcal{N}(\mathfrak{p})^{-2s} + \cdots - (\ell-1)\mathcal{N}(\mathfrak{p})^{-\ell s}.$$

Nun ist

$$g(s) := \prod_{\mathfrak{p} \in T} \left(1 - \binom{\ell}{2}\mathcal{N}(\mathfrak{p})^{-2s} + \cdots - (\ell-1)\mathcal{N}(\mathfrak{p})^{-\ell s}\right)$$

für $s = 1$ ein konvergentes Produkt, welches wir durch eine von k abhängige Konstante nach oben abschätzen können. Es gilt also:

$$\prod_{\mathfrak{p} \in T} \left(1 + \frac{\ell - 1}{\mathcal{N}(\mathfrak{p})^s}\right) = g(s) \prod_{\mathfrak{p} \in T} (1 - \mathcal{N}(\mathfrak{p})^{-s})^{1-\ell}.$$

Sei nun $d := [k(\zeta_\ell) : k]$ ein Teiler von $\ell - 1$. Alle Primideale aus T sind in $k(\zeta_\ell)$ total zerlegt. Daher erhalten wir für ein $\mathfrak{p} \in T$ die Faktorisierung $\mathfrak{p}\mathcal{O}_{k(\zeta_\ell)} = \mathfrak{P}_1 \cdots \mathfrak{P}_d$. Wegen $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathfrak{P}_i)$ für $i = 1, \ldots, d$ und mit $e := (\ell - 1)/d$ erhalten wir für alle $\mathfrak{p} \in T$:

$$(1 - \mathcal{N}(\mathfrak{p})^{-s})^{1-\ell} = \prod_{\mathfrak{P} \mid \mathfrak{p}} (1 - \mathcal{N}(\mathfrak{P})^{-s})^{-e}.$$

Sei nun $\tilde{T} \subset \mathbb{P}(k(\zeta_\ell))$ die Menge der Primideale, die über Primidealen aus T liegen. Wir erhalten:

$$\prod_{\mathfrak{P}\in\tilde{T}} (1-\mathcal{N}(\mathfrak{P})^{-s})^{-e} = \zeta_{k(\zeta_\ell)}(s)^e \prod_{\mathfrak{P}\notin\tilde{T}} (1-\mathcal{N}(\mathfrak{P})^{-s})^{e}.$$

Alle Primideale, die nicht in $\tilde{T}$ liegen, liegen entweder über ℓ oder haben einen Trägheitsgrad, der mindestens 2 ist. Daher konvergiert dieses Eulerprodukt für $s = 1$ und nimmt einen Wert zwischen 0 und 1 an. Zu guter Letzt müssen wir noch die Asymptotik von $\zeta_{k(\zeta_\ell)}(s)^e$ betrachten. Mit Hilfe von Satz 2.19 erhalten wir, dass sich diese Funktion wie $dx \log(x)^{e-1}$ verhält. □

Im obigen Beweis haben wir an zwei Stellen bei der Abschätzung den Grundkörper k benötigt. Die obere Abschätzung des Eulerprodukts $g(s)$ für $s = 1$ können wir nur in Abhängigkeit von $[k : \mathbb{Q}]$ führen. Die zweite Abhängigkeit ist die Stelle, an der wir den Taubersatz auf $\zeta_{k(\zeta_\ell)}$ anwenden. Hier könnten wir mit größerem Aufwand für alle $\epsilon > 0$ zu einer gleichmäßigen oberen Abschätzung der folgenden Form kommen:

$$\sum_{n\le x} a_n \le c([k(\zeta_\ell) : \mathbb{Q}], \ell, \epsilon) d_k^\epsilon x \log(x)^{e-1}.$$

Diese Abschätzung ist für induktive Anwendungen sehr nützlich, wir werden sie aber in dieser Arbeit nicht verwenden. Im folgenden Satz hätte diese Verschärfung zur Folge, dass wir $c(k, \ell)$ durch $\tilde{c}([k(\zeta_\ell) : \mathbb{Q}], \ell, \epsilon) d_k^{1/2+\epsilon}$ ersetzen könnten, wobei wir die Klassengruppe mit Satz 2.28 abschätzen.

Satz 3.23
Es seien k ein Zahlkörper und $S \subseteq \mathbb{P}(k)$ eine endliche Menge. Dann existiert eine Konstante $c(k, \ell)$ (unabhängig von S) mit

$$Z^S(k, Z_\ell; x) \le c(k, \ell) \ell^{|S|} x^{1/(\ell-1)} \log(x)^{b(k,Z_\ell)} \text{ für alle } x > 0.$$

Beweis
Wegen $Z^S(k, G; x) \le Z^{S'}(k, G; x)$ für alle $x > 0$ und $S \subseteq S'$ können wir ohne Einschränkung annehmen, dass S alle Primstellen über ℓ enthält. Hierbei können wir die zusätzlichen ℓ–Faktoren in $c(k, \ell)$ aufnehmen.

Für ein quadratfreies Ideal $\mathfrak{a} \in \mathbb{P}(k)$ bezeichnen wir mit

$$n_\mathfrak{a} := |\{K/k \mid \mathrm{Gal}(K/k) = Z_\ell, d^S_{K/k} = \mathfrak{a}^{\ell-1}\}|.$$

Wir merken an, dass Diskriminanten $(\ell-1)$te Potenz modulo S sind, da alle Primideale über ℓ in S liegen. Die Anzahl der Erweiterungen, die höchstens

in Primteilern von $\mathfrak{a}$ oder Primidealen aus S verzweigt sind, können wir nach Korollar 2.27 mit $\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_k)+3[k:\mathbb{Q}]+|S|}\ell^{\omega(\mathfrak{a})}$ nach oben abschätzen. Hierbei zählen wir auch Körpererweiterungen, die nicht in allen Primteilern von $\mathfrak{a}$ verzweigt sind. Wenn wir dies berücksichtigen, so können wir diese Abschätzung zu

$$n_\mathfrak{a} \leq \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_k)+3[k:\mathbb{Q}]+|S|}(\ell-1)^{\omega(\mathfrak{a})}$$

verfeinern (vgl. Lemma 4.15). Wir definieren nun die folgende Dirichletreihe, wobei $T \subseteq \mathbb{P}(k)$ alle Primideale enthält, deren Norm kongruent $1 \bmod \ell$ ist:

$$f(s) = \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_k)+3[k:\mathbb{Q}]+|S|}\prod_{\mathfrak{p}\in T}(1+\frac{\ell-1}{\mathcal{N}(\mathfrak{p})^s}) = \sum_{n\in\mathbb{N}}\frac{b_n}{n^s}.$$

Wenn wir $a_n := \sum_{\mathcal{N}(\mathfrak{a})=n} n_\mathfrak{a}$ setzen, erhalten wir mit obigen Rechnungen, dass $a_n \leq b_n$ für alle $n \in \mathbb{N}$ gilt. Das Eulerprodukt schätzen wir nun mit Lemma 3.22 ab. Wenn wir noch die $(\ell-1)$te Wurzel ziehen, erhalten wir das gewünschte Ergebnis. □

3.6 Zyklische Körper mit lokalen Vorgaben

Für einige unserer Anwendungen wollen wir Körpererweiterungen zählen, die an endlich vielen Stellen gewisse lokale Vorgaben erfüllen. Als Spezialfall des Grunwald–Wang–Theorems [30, Corollary 9.2.3] erhalten wir für zyklische Gruppen $G = Z_\ell$ von Primzahlordnung, dass stets Erweiterungen existieren, die endlich vielen lokalen Vorgaben genügen. Mit letzterem ist folgendes gemeint: Seien k ein Zahlkörper und $S \subset \mathbb{P}(k)$ eine endliche Teilmenge. Für $\mathfrak{p} \in S$ seien $k_\mathfrak{p}$ die Vervollständigung und $K_\mathfrak{P}/k_\mathfrak{p}$ eine lokale Körpererweiterung mit Galoisgruppe $H \leq G = Z_\ell$. Für einen Zahlkörper M ist $M \otimes_k k_\mathfrak{p}$ ein Produkt von Körpern. Wir bezeichnen mit $M_{\tilde{\mathfrak{P}}}$ einen dieser Körper. Ein Zahlkörper M *genüge den endlich vielen Vorgaben* $\{K_\mathfrak{P}/k_\mathfrak{p} \mid \mathfrak{p} \in S\}$, wenn $\mathrm{Gal}(M/k) = G$ gilt und $M_{\tilde{\mathfrak{P}}} \cong K_\mathfrak{P}$ für alle Stellen $\mathfrak{p} \in S$ gilt. Weiterhin können wir für eine Menge S_∞ von unendlichen Stellen eine analoge Vorgabe fordern. In diesem Abschnitt wollen wir folgenden Satz angeben.

Satz 3.24
Es seien k ein Zahlkörper und $\mathcal{L}_{Z_\ell}$ eine Menge von lokalen Vorgaben an den endlich vielen Stellen aus $S \subset \mathbb{P}(k)$ sowie S_∞, wobei alle lokalen Galoisgruppen Untergruppen von Z_ℓ sind. Wir bezeichnen mit $\mathcal{K}_{\mathcal{L},\ell}$ die Menge der Z_ℓ–Erweiterungen von k, die die lokalen Vorgaben erfüllen. Dann hat die Funktion

$$\Phi_{\mathcal{L},\ell}(s) := \sum_{K\in\mathcal{K}_{\mathcal{L},\ell}}\frac{1}{\mathcal{N}(d_{K/k})^s}$$

folgende Eigenschaften:

(1) $\Phi_{\mathcal{L},\ell}$ *konvergiert absolut und lokal gleichmäßig für* $\Re(s) > 1/(\ell-1)$.

(2) $\Phi_{\mathcal{L},\ell}$ *besitzt bei* $s = 1/(\ell-1)$ *einen* m*–fachen Pol mit* $m = b(k, Z_\ell) + 1$.

(3) Es existiert eine meromorphe Fortsetzung nach links und die gehobene Funktion erfüllt eine analoge Abschätzung wie in Satz 3.17.

Wir werden diesen Satz in dieser Arbeit nicht beweisen. David Wright beweist in [33] diese Version mit *einer* lokalen Vorgabe für alle abelschen Gruppen unter der Voraussetzung, dass eine globale Erweiterung existiert, die die lokale Vorgabe erfüllt. Er beweist zwar nicht explizit die Abschätzungen für $\Re(s) \leq 1$, aber diese folgen aus der Darstellung von $\Phi_{\mathcal{L},\ell}$ als Summe von Heckeschen L–Reihen. Es sollte klar sein, dass dieser Satz auf endlich viele Vorgaben verallgemeinert werden kann. Die meisten Aussagen, die wir in diesem Kapitel über die Funktionen $\Phi_{k,Z_2,S}$ bzw. Φ^S_{k,Z_2} hergeleitet haben, sind einfache Anwendungen dieses Satzes. Fast alle Ergebnisse in dieser Arbeit basieren auf den Ergebnissen, die wir über diese Funktionen bewiesen haben.

Wir werden Satz 3.24 nur im Kapitel 7 benötigen. So werden die Sätze 7.2 und 7.6 auf diesem Satz basieren. Wir merken an, dass für $k = \mathbb{Q}$ nur eine lokale Vorgabe benötigt wird. Eine weitere Anwendung dieses Satzes wäre die Verallgemeinerung der Rechnungen, die wir für Gruppen $Z_2 \wr H$ machen werden (Satz 3.29), auf Gruppen der Form $Z_\ell \wr H$.

Für den Fall $G = Z_2$ werden ähnliche Ergebnisse mit lokalen Vorgaben in [9] beschrieben. Aus Theorem 4.2 ergibt sich folgender Satz.

Satz 3.25 (Datskovsky–Wright)
Es seien k *ein Zahlkörper und* $\mathcal{L}_{Z_2}$ *eine Menge von lokalen Vorgaben an den endlich vielen Stellen* $S \subseteq \mathbb{P}(k)$ *sowie den unendlichen reellen Stellen* S_∞. *Dann gilt mit*

$$\Phi_{\mathcal{L},2}(s) := \sum_{K \in \mathcal{K}_{\mathcal{L},2}} \frac{1}{\mathcal{N}(d_{K/k})^s} = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} :$$

(1) $\Phi_{\mathcal{L},2}$ *konvergiert absolut und lokal gleichmäßig für* $\Re(s) > 1$.

(2)

$$\lim_{x \to \infty} \frac{\sum_{n \leq x} a_n}{x} = c(S, S_\infty) \operatorname*{res}_{s=1} \Phi_{k,Z_2}(s)$$

mit

$$c(S, S_\infty) = \frac{1}{2^{|S|+|S_\infty|}} \prod_{\mathfrak{p} \in S} (\mathcal{N}(d_{K_\mathfrak{P}/k_\mathfrak{p}})^{-1})(1 + \mathcal{N}(\mathfrak{p})^{-1})^{-1}.$$

Wir merken an, dass dieser Satz konsistent mit den Aussagen von Satz 3.12 ist. Hier wurde der zusätzliche Faktor $\prod_{\mathfrak{p}\in S}(1+\mathcal{N}(\mathfrak{p})^{-1})^{-1}$ bestimmt. Wenn wir berücksichtigen, dass alle lokalen Vorgaben unverzweigte Erweiterungen sind und wir für jedes Primideal $\mathfrak{p} \in S$ zwei Möglichkeiten haben (träge oder zerlegt), kommen wir durch das Aufsummieren der $2^{|S|}$ Möglichkeiten zum selben Ergebnis.

Etwas komplizierter können wir sehen, dass dieses Ergebnis mit Satz 3.16 übereinstimmt. Hier ist die Situation deswegen etwas komplizierter, weil wir die Diskriminanten verändern. Für eine Stelle in S müssen wir über alle möglichen lokalen Erweiterungen summieren, wobei wir den Ausdruck $\mathcal{N}(d_{K_\mathfrak{P}/k_\mathfrak{p}})^{-1}$ durch 1 ersetzen. Falls $\mathfrak{p}$ nicht über der 2 liegt, so haben wir 4 lokale Erweiterungen, nämlich die triviale (zerlegt), die träge und zwei verzweigte. Der Beitrag des lokalen Faktors $\mathfrak{p}$ ist dann:

$$\frac{1}{2}(1+1+1+1)(1+\mathcal{N}(\mathfrak{p})^{-1})^{-1} = 2(1+\mathcal{N}(\mathfrak{p})^{-1})^{-1}.$$

Hier ist die wilde Verzweigung deutlich komplizierter. Sei $\mathfrak{p}$ ein Primideal über der 2 und $k_\mathfrak{p}$ habe Grad d über $\mathbb{Q}_2$. Dann gibt es 2^{r+2} lokale Vorgaben. Mit der gleichen Rechnung wie bei den zahm verzweigten Primidealen erhalten wir als Faktor:

$$2 \cdot 2^r(1+\mathcal{N}(\mathfrak{p})^{-1})^{-1}.$$

Der 2^r–Beitrag muss also von $\mathcal{N}(\mathfrak{d})$ geleistet werden. Wenn wir annehmen, dass $S = \{\mathfrak{p}\}$ gilt, dann ist $\mathfrak{d} = \mathfrak{p}^e$ mit $\mathfrak{p}^e \mid\mid 2\mathcal{O}_k$. Damit gilt $\mathcal{N}(\mathfrak{p}^e) = 2^r$, wobei $r = [k_\mathfrak{p} : \mathbb{Q}_2]$.

3.7 Kranzprodukte der Form $Z_2 \wr H$

In diesem Abschnitt werden wir einige Ergebnisse über Kranzprodukte herleiten, welche mit ähnlichen Methoden wie in [6] erzielt werden. Dort wurde gezeigt, dass für die Diedergruppe $D_4 \leq S_4$ gilt:

$$Z(k, D_4; x) \sim c(k, D_4)x.$$

Insbesondere wurde dort auch die Konstante $c(k, D_4)$ explizit bestimmt. Bekanntermaßen ist $D_4 \cong Z_2 \wr Z_2$ und somit ein Kranzprodukt der Form $Z_2 \wr H$, welche wir in diesem Abschnitt untersuchen. Die grobe Idee, um solche Kranzprodukte in den Griff zu bekommen, ist die folgende. Wir summieren alle Körper mit Galoisgruppe H, wobei wir davon ausgehen, dass wir dies bereits genügend gut können. Für jeden dieser (unendlich vielen) Summanden

summieren wir wiederum alle relativ–quadratischen Erweiterungen. Hierzu hatten wir im Abschnitt 3.2 bereits geeignete Abschätzungen hergeleitet.

Wir merken an, dass erste obere Abschätzungen der Form

$$Z(k, H_1 \wr H_2; x) \leq c(k, H_1, H_2, \epsilon) x^{a(H_1 \wr H_2)+\epsilon}$$

unter geeigneten Voraussetzungen bereits in [23] gezeigt werden.

Es sei also H eine transitive Permutationsgruppe und K/k eine Körpererweiterung mit $\mathrm{Gal}(K/k) = H$. Sei weiterhin L/K eine Körpererweiterung vom Grad 2. Für die Erweiterung L/k erhalten wir nach Lemma 2.1: $d_{L/k} = d_{K/k}^2 \mathcal{N}_{K/k}(d_{L/K})$. Wir wollen nun alle Erweiterungen aufsummieren, die aufgrund eines solchen Körperturms entstehen. Mit anderen Worten wollen wir die Asymptotik der Funktion $\tilde{Z}(k, Z_2 \wr H; x) =$

$$|\{L/k \mid \exists K : \mathrm{Gal}(L/K) = Z_2, \mathrm{Gal}(K/k) = H, \mathcal{N}(d_{L/k}) \leq x\}|$$

untersuchen. Hierzu sei $\mathcal{K}_H := \{K/k \mid \mathrm{Gal}(K/k) = H\}$. Damit definieren wir:

$$\Phi(s) = \sum_{K \in \mathcal{K}_H} \frac{\Phi_{K,Z_2}(s)}{\mathcal{N}(d_{K/k})^{2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{3.2}$$

Aufgrund von [23] wissen wir, dass diese Dirichletreihe für $\Re(s) > 1$ konvergent ist. Der Koeffizient a_n zählt wieder die Anzahl der Körpererweiterungen L/k mit Absolutdiskriminante n. Die Galoisgruppe jeder solchen Körpererweiterung ist eine Untergruppe des Kranzprodukts $Z_2 \wr H$, welche noch Zusatzeigenschaften besitzt. Wir erhalten den folgenden Satz.

Satz 3.26
Wir nehmen an, dass es wenigstens eine Erweiterung mit Galoisgruppe H des Zahlkörpers k gibt und für alle $\epsilon > 0$ die folgende Abschätzung gilt:

$$Z(k, H; x) = O_{k,H,\epsilon}(x^{1+\epsilon}).$$

Dann besitzt die in (3.2) definierte Funktion $\Phi(s)$ eine meromorphe Fortsetzung auf $\Re(s) > 7/8$, wobei es in diesem Bereich genau einen einfachen Pol bei $s = 1$ gibt.

Beweis
Die Aussage ist wegen Satz 3.7 trivial, wenn es nur endlich viele Erweiterungen mit Galoisgruppe H von k gibt. Wegen $d_K = d_k^2 \mathcal{N}(d_{K/k})$ unterscheiden sich d_K und $\mathcal{N}(d_{K/k})$ nur durch eine von k abhängige Konstante. Aufgrund der Voraussetzung konvergiert die Dirichletreihe

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{K/k})^s} \tag{3.3}$$

absolut und lokal gleichmäßig für $\Re(s) > 1$. Wir betrachten die Funktion

$$g(s) := \sum_{K \in \mathcal{K}_H} \frac{\Phi_{K,Z_2}(s) - R(K)/(s-1)}{\mathcal{N}(d_{K/k})^{2s}},$$

wobei $R(K)$ das Residuum von Φ_{K,Z_2} bei $s = 1$ ist. Aus Satz 3.7 folgt, dass $g_K(s) := \Phi_{K,Z_2}(s) - R(K)/(s-1)$ eine auf $\Re(s) > 7/8$ analytische Funktion ist und für alle $\epsilon > 0$ die Abschätzung $|g_K(s)| = O_{\epsilon,[k:\mathbb{Q}]}(|d_K(s+1)^{[K:\mathbb{Q}]}|^{1/2+1/16+\epsilon})$ gilt. Wegen

$$2\frac{7}{8} - \frac{9}{16} = \frac{19}{16} > 1 \text{ und } (3.3)$$

konvergiert auch die Reihe

$$\sum_{K \in \mathcal{K}_H} \frac{g_K(s)}{\mathcal{N}(d_{K/k})^{2s}}$$

für $\Re(s) > 7/8$ absolut und lokal gleichmäßig. Damit ist $g(s)$ für $\Re(s) > 7/8$ eine analytische Funktion. Da wegen Lemma 3.2 auch $R(K) = O_{\epsilon,[k:\mathbb{Q}]}(d_K^{\epsilon})$ für alle $\epsilon > 0$ gilt, konvergiert wegen $d_K = d_k^{[K:k]}\mathcal{N}(d_{K/k})$ auch die Reihe

$$\frac{1}{s-1} \sum_{K \in \mathcal{K}_H} \frac{R(K)}{\mathcal{N}(d_{K/k})^{2s}}$$

absolut und lokal gleichmäßig für alle Gebiete, die in $\{s \in \mathbb{C} \mid \Re(s) > 7/8 \text{ und } s \neq 1\}$ enthalten sind. Wegen der absoluten Konvergenz aller beteiligten Reihen erhalten wir die gewünschte Aussage für

$$\Phi(s) = g(s) + \sum_{K \in \mathcal{K}_H} \frac{R(K)/(s-1)}{\mathcal{N}(d_{K/k})^{2s}}.$$

□

Wir erhalten als eine direkte Anwendung von Satz 2.19:

Korollar 3.27
Unter den Voraussetzungen aus Satz 3.26 gilt:

$$\tilde{Z}(k, Z_2 \wr H; x) \sim \operatorname*{res}_{s=1}(\Phi(s))x.$$

Aus dem Beweis des obigen Satzes ist sofort ersichtlich, dass die Voraussetzungen an die oberen Schranken für $Z(k, H; x)$ abgeschwächt werden können.

Somit kann es möglich sein, dass wir das asymptotische Verhalten der Funktion $\tilde{Z}(k, Z_2 \wr H; x)$ bestimmen können, ohne das exakte Verhalten der Funktion $Z(k, H; x)$ zu kennen. Als nächstes wollen wir zeigen, dass

$$\tilde{Z}(k, Z_2 \wr H; x) \sim Z(k, Z_2 \wr H; x)$$

gilt, d.h. die Körpererweiterungen, die nicht zum Kranzprodukt führen, tragen nichts zum Hauptterm der Asymptotik bei.

Lemma 3.28
Es seien $L/K/k$ Erweiterungen von Zahlkörpern mit $\mathrm{Gal}(K/k) = H$ und $[L : K] = 2$. Falls $p \mid\mid \mathcal{N}(d_{L/K})$ für eine in $K/\mathbb{Q}$ unverzweigte Primzahl p gilt, so folgt $\mathrm{Gal}(L/k) = Z_2 \wr H$.

Beweis
Da $p \mid\mid \mathcal{N}(d_{L/k})$ gilt, enthält $\mathrm{Gal}(L/k)$ eine Transposition. Wir wählen nun im Beweis von Lemma 2.14 das minimale Blocksystem, welches zum Teilkörper K korrespondiert. Nach dem Beweis permutiert die Transposition zwei Zahlen, die im selben Block liegen und die gewünschte Aussage folgt wie in diesem Beweis. □

Wir merken an, dass wir die analoge Aussage auch formulieren könnten, wenn wir die Primzahl p durch ein Primideal $\mathfrak{p} \in \mathbb{P}(k)$ ersetzen. Dies bedeutet aber keine wesentliche Verbesserung für die nachfolgenden Abschätzungen.

Wir wollen nun alle Körpererweiterungen aufsummieren, deren Galoisgruppe echte Untergruppe des Kranzprodukts $Z_2 \wr H$ ist. Wenn wir zeigen können, dass die Anzahl dieser Körper schwächer als linear wächst, haben wir unser Ziel erreicht. Daher definieren wir:

$$Y(k, Z_2 \wr H; x) :=$$

$$|\{L/K/k \mid \mathrm{Gal}(L/k) \neq Z_2 \wr H, \mathrm{Gal}(K/k) = H, [L : K] = 2, \mathcal{N}(d_{L/k}) \leq x\}|.$$

Wir schätzen diese Anzahl dadurch nach oben ab, dass wir alle Körpererweiterungen zählen, die nicht die Voraussetzungen von Lemma 3.28 erfüllen. Für einen solchen Körperturm $k \subset K \subset L$ gilt:

$$\mathcal{N}(d_{L/k}) = \mathcal{N}(d_{K/k}^2)\mathcal{N}(d_{L/K}) \geq \mathcal{N}(d_{K/k}^2)\mathcal{N}(d_{L/K})^{S_K},$$

wobei $S_K := \{p \in \mathbb{P} \mid p | \mathcal{N}(d_{K/k})\}$. Wir definieren

$$\hat{Z}^{S_K}(K, Z_2; x) := |\{L/K \mid \mathrm{Gal}(L/K) = Z_2, \mathcal{N}(d_{L/K})^{S_K} \leq x,$$

$$p \mid (\mathcal{N}(d_{L/K}))^{S_k} \Rightarrow p^2 \mid (\mathcal{N}(d_{L/K}))^{S_k} \forall p \in \mathbb{P}\}|$$

und erhalten

$$Y(k, Z_2 \wr H; x) \leq \sum_{K \in \mathcal{K}_H(x^{1/2})} \hat{Z}^{S_K}(K, Z_2; x/\mathcal{N}(d_{K/k}^2)),$$

wobei $\mathcal{K}_H(x)$ gerade die Körper aus $\mathcal{K}_H$ enthält, deren Diskriminante durch x beschränkt ist.

Wir benötigen also eine Abschätzung für $\hat{Z}^{S_K}(K, Z_2; x)$. Wir bezeichnen mit a_n die Anzahl der Körper aus dieser Menge mit $\mathcal{N}(d_{L/K})^{S_K} = n$. Da wir alle Primteiler aus S_K ignorieren und die übrigen Primteiler der Diskriminante $\mathcal{N}(d_{L/K})^{S_K}$ wenigstens quadratisch auftauchen, sind alle $a_n = 0$, für die eine Primzahl p mit $p||n$ existiert.

Wir wählen $S \subseteq \mathbb{P}(K)$ als die Menge, welche alle Primideale über Primteilern von n sowie Elementen aus S_K enthält. Wir schätzen nun a_n mit Hilfe von Satz 2.26 nach oben ab, indem wir alle Z_2–Erweiterungen zählen, die höchstens in S verzweigt sind. Wir erhalten also für $m := [K : \mathbb{Q}]$ die Abschätzung $|S| \leq (\omega(n) + |S_K|)m$, da über jeder Primzahl höchstens m Primideale liegen können. Wegen $r_1 \leq m$ erhalten wir aus Satz 2.26:

$$a_n \leq 2^{\mathrm{rk}_2(\mathrm{Cl}_K)} 2^{m(\omega(n)+|S_K|)} 2^{3m} \leq c(m, \epsilon) d_K^{1/2+\epsilon} 2^{m\omega(n)},$$

wobei wir die Klassengruppe mit Satz 2.28 sowie $2^{m|S_K|} = 2^{m\omega(d_K)} \leq \tilde{c}(m, \epsilon) d_K^{\epsilon}$ mit Lemma 2.20 abgeschätzt haben. Somit gilt:

$$\sum_{n \leq x} a_n \leq c(m, \epsilon) d_K^{1/2+\epsilon} \sum_{n \leq x^{1/2}} 2^{m\omega(n)}.$$

Mit Hilfe von Lemma 2.20 können wir $\sum_{n \leq x} (2^m)^{\omega(n)} = O(x^{1+\epsilon})$ abschätzen und erhalten mit neuer Konstante $c(m, \epsilon)$:

$$\hat{Z}^{S_K}(K, Z_2; x) \leq c(m, \epsilon) d_K^{1/2+\epsilon} x^{1/2+\epsilon}.$$

Wenn wir dies in obige Ungleichung für $Y(k, Z_2 \wr H; x)$ einsetzen, erhalten wir mit $d_K = d_k^2 \mathcal{N}(d_{K/k})$:

$$Y(k, Z_2 \wr H; x) \leq \sum_{K \in \mathcal{K}_H(x^{1/2})} c(m, \epsilon) (d_k^2 \mathcal{N}(d_K))^{1/2+\epsilon} \left(\frac{x}{\mathcal{N}(d_{K/k}^2)} \right)^{1/2+\epsilon}$$

$$\leq c(m, \epsilon) d_k^{1+2\epsilon} x^{1/2+\epsilon} \sum_{K \in \mathcal{K}_H(x^{1/2})} \frac{\mathcal{N}(d_{K/k})^{1/2+\epsilon}}{\mathcal{N}(d_{K/k})^{1+2\epsilon}}$$

Wegen $\mathcal{N}(d_{K/k}) \leq x^{1/2}$ erhalten wir:

$$Y(k, Z_2 \wr H; x) \leq c(m, \epsilon) d_k^{1+2\epsilon} x^{1/2+\epsilon} x^{1/4+\epsilon} \sum_{K \in \mathcal{K}_H(x^{1/2})} \frac{1}{\mathcal{N}(d_{K/k})^{1+2\epsilon}}.$$

Die letzte Summe ist nach der Voraussetzung aus Satz 3.26 konvergent, womit wir für alle $\epsilon > 0$ die folgende Abschätzung bewiesen haben:

$$Y(k, Z_2 \wr H; x) \leq c(k, H, m, \epsilon) x^{3/4+2\epsilon}.$$

Wegen $Z(k, Z_2 \wr H; x) + Y(k, Z_2 \wr H; x) = \tilde{Z}(k, Z_2 \wr H; x)$ sowie Satz 3.26 haben wir den folgenden Satz bewiesen:

Satz 3.29
Unter den Voraussetzungen von Satz 3.26 lässt sich die zu $Z_2 \wr H$ gehörige Dirichletreihe auf $\Re(s) > 7/8$ meromorph fortsetzen, wobei $s = 1$ der einzige Pol in diesem Bereich ist. Das Residuum r dieses Pols stimmt mit dem Residuum der Funktion $\Phi(s)$ überein. Es gilt:

$$Z(k, Z_2 \wr H; x) \sim rx.$$

Aufgrund der vorherigen Berechnungen können wir einen Ausdruck für das Residuum angeben:

Korollar 3.30
Es gilt:

$$\operatorname*{res}_{s=1}(\Phi(s)) = \sum_{K \in \mathcal{K}_H} \frac{\operatorname{res}_{s=1} \zeta_K(s)}{2^{i(K)} d_K^2 \zeta_K(2)},$$

wobei diese Summe konvergent ist.

Diese Ergebnisse sind in Übereinstimmung mit unserer Hauptvermutung.

Korollar 3.31
Die Vermutung 2.12 ist richtig für alle Gruppen der Form $Z_2 \wr H$ und alle Zahlkörper k, für die H die Voraussetzung des Satzes 3.26 erfüllt.

Wir merken an, dass diese Voraussetzung stets für abelsche Gruppen H erfüllt ist. Die Voraussetzung ist sogar nach [13] für alle regulären Gruppen H erfüllt, falls wir annehmen, dass wenigstens eine Erweiterung mit Galoisgruppe H existiert. Wir erhalten damit folgendes Korollar:

Korollar 3.32
Für gerades n existiert stets eine transitive Gruppe $G \leq S_n$ mit

$$Z(k, G; x) \sim c(k, G)x = c(k, G)x^{a(G)}.$$

Kapitel 4

Lösen von zentralen Einbettungsproblemen

In diesem Kapitel werden wir sogenannte Einbettungsprobleme studieren. Die geschickte Lösung solcher Einbettungsprobleme ist ein wichtiges Hilfsmittel für die Bestimmung unserer Asymptotiken. Wir beweisen folgenden gruppentheoretischen Reduktionssatz, der Probleme für auflösbare Gruppen auf die Betrachtung von semidirekten Produkten reduziert. Sei hierzu

$$1 \to A \to G \to H \to 1$$

eine exakte Sequenz von Gruppen, wobei A abelsch sein soll. Dann zeigen wir in Satz 4.7, dass $G \times_H G \cong G \times_H (A \rtimes H)$ gilt. Nehmen wir nun an, dass K/k eine Körpererweiterung mit Galoisgruppe H ist und L_1/K und L_2/K zwei Lösungen des zugehörigen Einbettungsproblems sind, für welche zusätzlich $L_1 \cap L_2 = K$ gilt. Dann bedeutet obige Isomorphie, dass die Körpererweiterung L_1L_2/K einen Zwischenkörper L_3 besitzt mit $\mathrm{Gal}(L_3/k) = A \rtimes H$. Umgekehrt führt die Kenntnis von Körpern L_1, L_3 mit $\mathrm{Gal}(L_1/k) = G$ und $\mathrm{Gal}(L_3/k) = A \rtimes H$ zu einem Zwischenkörper $K \leq L_2 \leq L_1L_3$ mit $\mathrm{Gal}(L_2) = G$ und $L_1 \neq L_2$. Auf diese Weise können wir alle Lösungskörper unseres gegebenen Einbettungsproblems auf das Finden einer Lösung und das Finden aller Lösungen des zugehörigen zerfallenden Einbettungsproblems reduzieren. Besonders einfach stellt sich die Situation dar, wenn wir zusätzlich annehmen, dass $A = Z_\ell$ die zyklische Gruppe mit ℓ Elementen ist und diese im Zentrum von G liegt. Dann ist obiges semidirektes Produkt sogar direkt und wir müssen lediglich Z_ℓ–Erweiterungen des Grundkörpers parametrisieren.

Für gute Abschätzungen unserer Zählfunktionen ist es wichtig eine erste Lösung mit möglichst wenig Verzweigung zu finden. Im Abschnitt 4.4 geben wir hierzu mehrere Resultate an. Später werden wir die Aussage von Satz 4.14

verwenden. Weiterhin verbessern wir in Lemma 4.15 die obere Abschätzung für die Anzahl der Z_ℓ–Erweiterungen von k, die genau in den Primidealen aus einer endlichen Menge $S \subseteq \mathbb{P}(k)$ verzweigt sind.

Im darauf folgenden Abschnitt beweisen wir in den Sätzen 4.17 und 4.18 obere Abschätzungen für direkte Produkte der Form $Z_\ell \times H$ sowie für Gruppen G, die zentrale Z_ℓ–Erweiterungen sind. Dieses Ergebnis kann auch auf nicht auflösbare Gruppen angewendet werden, wenn genügend über die Zählfunktion der Faktorgruppe G/Z_ℓ bekannt ist.

Wie bereits in der Einleitung angekündigt beweisen wir in Satz 4.25 den Hauptsatz für nilpotente Gruppen G, der uns zusammen mit Satz 4.30 folgendes liefert:

$$c_1(k,G)x^{a(G)} \leq Z(k,G;x) \leq c_2(k,G)x^{a(G)}\log(x)^{d(G)},$$

wobei $c_1(k,G)$ und $c_2(k,G)$ positive Konstanten sind und $d(G) \geq b(k,G)$ gilt.

4.1 Einbettungsprobleme

Definition 4.1
Es sei K/k eine Galoiserweiterung von Körpern mit Galoisgruppe H und

$$1 \longrightarrow U \longrightarrow G \xrightarrow{\kappa} H \longrightarrow 1$$

eine exakte Sequenz von endlichen Gruppen. Wir bezeichnen mit $\bar{k} \geq K$ einen algebraischen Abschluss von k und mit $\varphi : \mathrm{Gal}(\bar{k}/k) \to H \cong \mathrm{Gal}(K/k)$ einen Epimorphismus mit Kern $\mathrm{Gal}(\bar{k}/K)$. Ein Homomorphismus $\tilde{\varphi} : \mathrm{Gal}(\bar{k}/k) \to G$ heißt schwache Lösung zum Einbettungsproblem, falls $\kappa \circ \tilde{\varphi} = \varphi$ gilt. Falls $\tilde{\varphi}$ noch zusätzlich surjektiv ist, so heißt $\tilde{\varphi}$ Lösung des Einbettungsproblems. Der Fixkörper L von $\ker(\tilde{\varphi})$ heißt Lösungskörper. Das Einbettungsproblem heißt zentral, falls $U \leq \mathrm{Z}(G)$ gilt. Es heißt zerfallend, wenn obige Sequenz zerfallend ist, d.h. ein semidirektes Produkt G definiert.

Eine Gruppenerweiterung wie in Definition 4.1 heißt zerfallend, wenn es einen Schnitt gibt, ansonsten heißt sie nicht zerfallend. Wir merken an, dass die Galoisgruppe eines Lösungskörpers einer schwachen Lösung im Allgemeinen nur eine Untergruppe von G ist. Der Begriff einer schwachen Lösung ist z.B. wichtig für das Lokal–Global–Prinzip, mit dem die Existenz einer schwachen Lösung gezeigt werden kann.

Unter geeigneten Voraussetzungen ist eine schwache Lösung stets eine Lösung. Für eine endliche Gruppe G sei $\mathrm{Frat}(G)$ der Durchschnitt aller maximalen Untergruppen von G, welchen wir *Frattinigruppe* nennen.

Lemma 4.2

(1) Es sei $\tilde{\varphi}$ eine schwache Lösung eines Einbettungsproblems mit Kern $U \leq \mathrm{Frat}(G)$. Dann ist $\tilde{\varphi}$ auch eine Lösung des Einbettungsproblems.

(2) Ein Einbettungsproblem mit zyklischem Kern U von Primzahlordnung ist entweder zerfallend oder $U \leq \mathrm{Frat}(G)$.

Beweis

Der erste Teil ist die Aussage von [25, Proposition IV.5.1]. Wir nehmen nun an, dass $U \not\leq \mathrm{Frat}(G)$ gilt. Dann existiert eine maximale Untergruppe M von G mit $U \not\leq M$. Da M maximal ist, gilt $G = \langle M, U\rangle$. Wegen $U \not\leq M$ folgt nun $M \cap U = \{1\}$ und damit ist das Einbettungsproblem zerfallend. □

Es sei nun L ein Lösungskörper zu einer Lösung unseres Einbettungsproblems aus obiger Definition. Dann gilt natürlich $\mathrm{Gal}(L/k) = G$ und $K \subseteq L$. Ein Körper L mit diesen beiden Eigenschaften ist aber nicht notwendigerweise eine Lösung des Einbettungsproblems. Ein einfaches Beispiel erhalten wir mit $G = D_4$ und $H = Z_2 \times Z_2$. Es gibt 3 nicht äquivalente Gruppenerweiterungen von H mit zentralem Z_2–Kern, die zu $G = D_4$ führen. Körpertheoretisch sind diese verschiedenen Erweiterungen dadurch ausgezeichnet, dass es zu einer Lösung L genau eine quadratische Erweiterung M von k gibt mit $\mathrm{Gal}(L/M) = Z_4$. Alle Lösungen mit demselben M gehören zum gleichen Einbettungsproblem. Wenn wir alle Körper $L \supseteq K$ mit $\mathrm{Gal}(L/k) = G$ bestimmen wollen, so geht dies stets durch Lösen von endlich vielen Einbettungsproblemen, deren Anzahl nicht von K oder k abhängt.

Lemma 4.3

Es sei K/k eine normale Erweiterung von Zahlkörpern mit $\mathrm{Gal}(K/k) = H$ und G eine Gruppenerweiterung von H wie in Definition 4.1. Dann erhalten wir alle L/K mit $\mathrm{Gal}(L/k) = G$ als Lösungskörper von endlich vielen Einbettungsproblemen, deren Anzahl nur von G und H abhängt.

Beweis

Es seien die Notationen wie in Definition 4.1. Die Anzahl der verschiedenen Einbettungsprobleme, die zur selben Gruppe G führen, sind durch die Anzahl der Epimorphismen von G auf H nach oben beschränkt. Verschiedene Epimorphismen $\kappa : G \to H$ mit dem selben Kern unterscheiden sich nur um Automorphismen von H. Weiterhin hat G nur endlich viele Normalteiler, deren Quotienten isomorph zu H sind. Da beide Anzahlen endlich sind, folgt die Behauptung. □

Später wollen wir auch $Z(k, G; x)$ für nicht reguläre Permutationsgruppen G untersuchen. Wie dieses Lemma basieren viele unserer Zählmethoden auf

normalen Erweiterungen. Wir werden den Fall, dass $G \leq S_n$ keine reguläre Permutationsgruppe ist, d.h. eine Körpererweiterung K/k mit $\mathrm{Gal}(K/k) = G$ nicht normal ist, auf den normalen Fall zurückführen. Die Anzahl der entsprechenden Körpererweiterungen unterscheidet sich nur um eine Konstante.

Lemma 4.4
Es seien $G \leq S_n$ eine Permutationsgruppe und K/k eine Körpererweiterung mit $\mathrm{Gal}(K/k) = G$. Wir bezeichnen mit N/k die normale Hülle von K/k. Dann ist die Anzahl $c(G)$ der Teilkörper $k \leq L \leq N$ mit $\mathrm{Gal}(L/k) = G$ unabhängig von k und K.

Beweis
Hauptsatz der Galoistheorie □

Wir merken an, dass wir die analoge Aussage beweisen können, wenn wir isomorphe aber nicht identische Körpererweiterungen als gleich betrachten wollen. In diesem Falle dürfen wir für die Konstante nur jeweils einen Vertreter einer Konjugationsklasse von Untergruppen berücksichtigen.

4.2 Reduktion auf zerfallende Einbettungsprobleme

In diesem Abschnitt werden wir den Zusammenhang zwischen zerfallenden und nicht zerfallenden Einbettungsproblemen mit abelschem Kern untersuchen. Wir verwenden weiterhin die exakte Sequenz aus Definition 4.1. Bevor wir den nächsten Satz beweisen können, müssen wir noch das subdirekte Produkt (Faserprodukt) einführen. Körpertheoretisch ist dieses Produkt bei Komposita von großer Bedeutung. Nehmen wir an, dass wir zwei galoissche Körpererweiterung L_1, L_2 über k mit Galoisgruppen G_1 und G_2 haben. Der Schnitt $K := L_1 \cap L_2$ ist galoissch mit Galoisgruppe H, welche ein Quotient von G_1 und G_2 ist. Daher ist die Galoisgruppe von L_1L_2/k gerade das subdirekte Produkt, welches wir in der folgenden Definition erklären.

Definition 4.5
Es seien G_1, G_2, H endliche Gruppen und $\kappa_i : G_i \to H$ $(i = 1, 2)$ Epimorphismen. Dann definieren wir das subdirekte Produkt

$$G_1 \times_H G_2 := \{(g_1, g_2) \mid g_i \in G_i \ (i = 1, 2), \kappa_1(g_1) = \kappa_2(g_2)\}$$

mit komponentenweiser Operation.

Elementarerweise definiert dies eine Gruppe der Ordnung $|G_1||G_2|/|H|$. Wir kehren nun zurück zu unserem Einbettungsproblem aus Definition 4.1. Wenn wir zwei Lösungen L_1, L_2 mit $L_1 \cap L_2 = K$ unseres Einbettungsproblems kennen, dann gilt $\mathrm{Gal}(L_1L_2/k) = G \times_H G$. Der folgende Satz klärt die Struktur dieser Gruppe. Später werden wir für abelsche Normalteiler U weitere Eigenschaften dieser Gruppe herleiten.

Satz 4.6
Es sei G eine Gruppenerweiterung wie in Definition 4.1. Wir definieren

$$\Psi : G \to \mathrm{Aut}(U), g \mapsto (u \mapsto u^{(g^{-1})} = gug^{-1}).$$

Dann gilt:

$$G \times_H G \cong U \rtimes G,$$

wobei das semidirekte Produkt via Ψ definiert wird.

Beweis
Wir definieren $\Phi : U \rtimes G \to G \times_H G, (u, g) \mapsto (g, ug)$. Wegen $\kappa(u) = 1$ für $u \in U$ gilt $(g, ug) \in G \times_H G$. Weiterhin ist Φ ein Homomorphismus, da

$$\Phi(u_1, g_1)\Phi(u_2, g_2) = (g_1, u_1g_1)(g_2, u_2g_2) = (g_1g_2, u_1g_1u_2g_2)$$

und $\Phi((u_1, g_1)(u_2, g_2))$

$$= \Phi((u_1u_2^{(g_1^{-1})}, g_1g_2)) = (g_1g_2, u_1u_2^{(g_1^{-1})}g_1g_2) = (g_1g_2, u_1g_1u_2g_2).$$

Die Injektivität von Φ ist klar und da die beteiligten Gruppen von gleicher (endlicher) Ordnung sind, folgt auch die Surjektivität. □

Im Folgenden wollen wir uns auf Einbettungsprobleme mit abelschem Kern A konzentrieren:

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\kappa} H \longrightarrow 1 \tag{4.1}$$

Ausgehend von dieser Sequenz können wir A als H–Modul auffassen. Dies geschieht via $\Psi : H \to \mathrm{Aut}(A) : h \mapsto (a \mapsto a^{\kappa^{-1}(h)})$. Hierbei kann ein beliebiges Urbild von h genommen werden, da A abelsch ist. Wir merken an, dass für nicht abelsche Normalteiler diese Konstruktion nicht wohldefiniert ist. Zu gegebenen A, H und $\Psi : H \to \mathrm{Aut}(A)$ konstruieren wir wie oben ein semidirektes Produkt.

Der folgende Satz ist das Hauptziel dieses Abschnitts. Er stellt einen Zusammenhang zwischen zerfallenden und nicht zerfallenden Einbettungsproblemen mit abelschem Kern her.

Satz 4.7
Es sei G eine Gruppenerweiterung wie in (4.1). *Wir definieren* $\Psi : H \to \mathrm{Aut}(A), h \mapsto (a \mapsto a^{(\kappa^{-1}(h))^{-1}})$. *Dann gilt:*

$$G \times_H G \cong G \times_H (A \rtimes H),$$

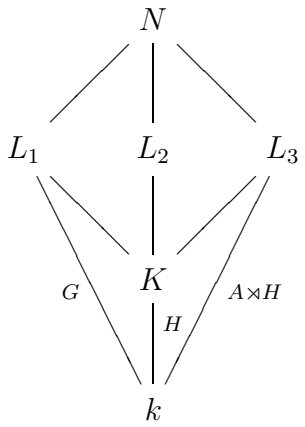
wobei das semidirekte Produkt via Ψ definiert wird. Insbesondere ist $A \rtimes H$ die Faktorgruppe von $G \times_H G$ nach dem Normalteiler $\{(a, a) \mid a \in A\}$.

Beweis
Der Homomorphismus Ψ lässt sich kanonischerweise auf ganz G definieren. Damit erhalten wir mit Satz 4.6, dass $G \times_H G \cong A \rtimes G$ gilt. Weiterhin ist $\Phi : A \rtimes G \to A \rtimes H, (a, g) \mapsto (a, \kappa(g))$ ein Homomorphismus, da der zu einem Element $h \in H$ gehörende Automorphismus aus $\mathrm{Aut}(A)$ unabhängig vom Urbild unter κ ist. Φ ist klarerweise surjektiv mit Kern $\{(1, a) \mid a \in A\}$. Dieser Kern wird mittels des Isomorphismus aus Satz 4.6 auf $\{(a, a) \mid a \in A\} \trianglelefteq G \times_H G$ abgebildet. Als nächstes ist dann klar, dass

$$A \rtimes G \to G \times_H (A \rtimes H), (a, g) \mapsto (g, (a, \kappa(g)))$$

ein Isomorphismus ist. □

Die Anwendung dieses Satzes korrespondiert zu folgendem Körperdiagramm:



In diesem Diagramm gehen wir davon aus, dass $\mathrm{Gal}(L_1/k) = \mathrm{Gal}(L_2/k) = G$ gilt. Weiterhin nehmen wir an, dass $L_1 \cap L_2 = K$ gilt. Dann existiert ein Körper $K \subseteq L_3 \subseteq N$ mit $\mathrm{Gal}(L_3/k) = A \rtimes H$. Ähnliches gilt, wenn wir Körper L_1, L_3 mit den obigen Galoisgruppen kennen. Dann garantiert uns dieser Satz die Existenz eines Körpers L_2 mit Galoisgruppe G. Je nach Einbettungsproblem kann es aber weitere Körper $K \subset L \subset N$ mit Galoisgruppe G geben. Deren Anzahl ist aber eine gruppentheoretische Invariante, welche im konkreten Fall einfach bestimmt werden kann (vgl. Satz 4.9).

4.3 Zentrale Einbettungsprobleme

In diesem Abschnitt werden wir zentrale Einbettungsprobleme mit Kern Z_ℓ studieren, wobei ℓ eine Primzahl ist. Dies wird es uns erlauben Methoden für nilpotente Gruppen zu entwickeln. Da hier die zugehörigen semidirekten Produkte direkt sind, spielen die Klassengruppen der beteiligten Zahlkörper nur eine untergeordnete Rolle.

Unser Einbettungsproblem zu $\mathrm{Gal}(K/k) = H$ hat daher die folgende Form:

$$1 \longrightarrow Z_\ell \longrightarrow G \xrightarrow{\kappa} H \longrightarrow 1 \tag{4.2}$$

Der einfachste Fall liegt vor, wenn eine primitive ℓ–te Einheitswurzel ζ_ℓ bereits in k enthalten ist. In diesem Fall ist das zu (4.2) assoziierte Einbettungsproblem ein sogenanntes *Brauer–Einbettungsproblem* [25, Kapitel IV.7]. Da die ℓ–ten Einheitswurzeln in k liegen, haben Lösungskörper L/K die Form $L = K(\sqrt[\ell]{\alpha})$ für geeignete $\alpha \in K$ (Kummertheorie). Es gibt aber noch weitere schöne Eigenschaften von Brauer–Einbettungsproblemen, z.B. ist das Lokal–Global–Prinzip gültig. All dies und der Beweis des folgenden Lemmas findet sich in obiger Referenz.

Lemma 4.8
Es sei $L = K(\sqrt[\ell]{\alpha})$ ein Lösungskörper für ein Brauer–Einbettungsproblem. Dann erhalten wir alle Lösungskörper als $K(\sqrt[\ell]{a\alpha})$, wobei a über die Elemente des Grundkörpers k ungleich 0 läuft.

Dieses Lemma war der Ausgangspunkt für die Bestimmung der Asymptotik von nilpotenten Erweiterungen in [19]. Mittels Kummertheorie wurde dort eine ähnliche Korrespondenz auch für Grundkörper k bewiesen, die keine ℓ–ten Einheitswurzeln enthalten. Hier werden wir diese Korrespondenz durch den gruppentheoretischen Ansatz aus dem letzten Abschnitt beweisen. Dabei werden wir für unseren Spezialfall die Aussage aus Satz 4.7 verschärfen.

Satz 4.9
Es sei G eine zentrale Erweiterung wie in (4.2) und $\tilde{G} = Z_\ell \times G \cong G \times_H G$. Dann gelten für $A := \{(a,b) \in Z_\ell \times G \mid \kappa(b) = 1\} \cong Z_\ell \times Z_\ell$:

(1) $A \leq \mathrm{Z}(\tilde{G}) = Z_\ell \times \mathrm{Z}(G)$.

(2) A besitzt $\ell + 1$ Untergruppen $U_1, \ldots, U_{\ell+1}$ der Ordnung ℓ. Alle diese Untergruppen sind Normalteiler von $\tilde{G}$.

(3) Alle Quotienten $\tilde{G}/U_i$ $(1 \leq i \leq \ell + 1)$ bis auf einen sind isomorph zu G. Der verbleibende Quotient ist isomorph zu $Z_\ell \times H$.

Beweis
Die Isomorphie $Z_\ell \times G \cong G \times_H G$ ist Satz 4.6. Die ersten beiden Aussagen sind elementar. Es sei a ein Erzeuger des Kerns von κ. Wir merken an, dass wir den ersten Faktor des direkten Produkts auch als die Untergruppe interpretieren, die im Kern von κ liegt. Dann können die Untergruppen $U_i \trianglelefteq Z_\ell \times G$ wie folgt beschrieben werden:

$$U_i := \langle (a, a^i) \rangle \ (1 \leq i \leq \ell) \text{ sowie } U_{\ell+1} := \langle (1, a) \rangle.$$

Klarerweise gilt $\tilde{G}/U_{\ell+1} \cong Z_\ell \times H$. Wir definieren die folgenden Bilder unter dem Isomorphismus Φ aus dem Beweis von Satz 4.6:

$$\tilde{U}_i = \Phi(U_i) = \langle (a^i, a^{i+1}) \rangle \text{ für } 1 \leq i \leq \ell.$$

Mit dem Isomorphiesatz gilt $(Z_\ell \times G)/U_i \cong (G \times_H G)/\tilde{U}_i$. Sei nun $(g, \tilde{g}) \in G \times_H G$ gegeben. Da $\kappa(g) = \kappa(\tilde{g})$ gilt, folgt $\tilde{g} = ga^j$ für ein geeignetes $j \in \{0, \ldots, \ell - 1\}$. Wir wählen nun $l \equiv -j \bmod \ell$. Damit gilt:

$$(g, ga^j)(a^i, a^{i+1})^l = (ga^{il}, ga^{j+(i+1)l}) = (ga^{il}, ga^{-l+(i+1)l}) = (ga^{il}, ga^{il}).$$

Damit gibt es in der Faktorgruppe $(G \times_H G)/\tilde{U}_i$ für jedes Element Vertreter, deren Komponenten übereinstimmen, was bedeutet, dass diese Faktorgruppe isomorph zu G ist. □

Dieser Satz zeigt, dass wir alle Lösungen unseres Einbettungsproblems (4.2) beschreiben können, sobald wir eine Lösung kennen. Seien hierzu L/K ein Lösungskörper und M/k eine Z_ℓ–Erweiterung mit $[ML : L] = \ell$. In diesem Fall erhalten wir mittels Satz 4.9 $\ell - 1$ neue Lösungen zu unserem Einbettungsproblem. Zwei zyklische Z_ℓ–Erweiterungen M_1, M_2 von k parametrisieren genau dann dieselben neuen Lösungen, falls $LM_1 = LM_2$ gilt. Diese Bedingung definiert auf der Menge der Z_ℓ–Erweiterungen von k eine Äquivalenzrelation. Aus technischen Gründen ist die triviale Erweiterung in der folgenden Definition enthalten:

$$\mathcal{M}_K := \{M/k \mid \mathrm{Gal}(M/k) \leq Z_\ell\}/\sim,$$

wobei $M_1 \sim M_2$ genau dann, wenn $LM_1 = LM_2$ gilt. Klarerweise ist $\sim$ nur von der maximalen elementarabelschen ℓ–Teilerweiterung von L/k abhängig. Falls $M_1 \subseteq L$ gilt, so liegt M_1 in der trivialen Klasse. Dann sind M_1, M_2, die nicht in der trivialen Klasse liegen, genau dann äquivalent, wenn $M_1 M_2 \cap L \neq k$ gilt. Da L/k aber nur endlich viele Z_ℓ–Erweiterungen enthält, erhalten wir folgenden Satz:

Satz 4.10
Es seien K/k eine galoissche Erweiterung von Zahlkörpern mit $\mathrm{Gal}(K/k) = H$ und L/K ein Lösungskörper des Einbettungsproblem (4.2). Wir definieren

$$\psi : \{\tilde{L}/K \mid \tilde{L} \text{ Lösungskörper}\} \to \mathcal{M}_K, \tilde{L} \mapsto M,$$

wobei M/k eine zyklische Erweiterung mit $LM = L\tilde{L}$ ist. Dann gelten:

(1) ψ ist eine Abbildung.

(2) Die triviale Klasse $\{M \subseteq L\}$ besitzt genau ein Urbild. Alle anderen Klassen besitzen genau $\ell - 1$ Urbilder.

(3) Es sei r der ℓ–Rang des maximalen abelschen Quotienten von G. Dann enthält die triviale Klasse genau $\frac{\ell^r-1}{\ell-1}+1$ Elemente. Alle anderen Klassen besitzen genau ℓ^r Elemente.

Beweis
ψ ist eine Abbildung, da mit Satz 4.9 und der vorangegangenen Diskussion jeder Lösung $\tilde{L}$ genau eine Klasse aus $\mathcal{M}_K$ zugeordnet wird. Weiterhin wird nur die ausgezeichnete Lösung L der trivialen Klasse zugeordnet. Wegen Satz 4.9 sehen wir, dass jeweils $\ell - 1$ andere Lösungen $\tilde{L}$ derselben Klasse zugeordnet werden. K/k besitzt nach Voraussetzung genau $\frac{\ell^r-1}{\ell-1}$ Zwischenkörper mit Galoisgruppe Z_ℓ über k. Zusammen mit der trivialen Erweiterung bilden diese die triviale Klasse. Für eine nicht triviale Klasse mit Vertreter M erhalten wir, dass LM $\frac{\ell^{r+1}-1}{\ell-1}$ Zwischenkörper mit Galoisgruppe Z_ℓ über k besitzt, von denen bereits $\frac{\ell^r-1}{\ell-1}$ in L liegen. Wir erhalten also

$$\frac{\ell^{r+1}-1}{\ell-1} - \frac{\ell^r-1}{\ell-1} = \frac{\ell^{r+1}-\ell^r}{\ell-1} = \ell^r$$

Körper in der Äquivalenzklasse von M. □

Mit Satz 4.10 haben wir alle Lösungen eines zentralen Einbettungsproblems mit zyklischem Kern durch zyklische Erweiterungen von k parametrisiert. Im Folgenden werden wir noch zwei Probleme lösen:

(1) Wie wählen wir zweckmäßigerweise die ausgezeichnete Lösung L?

(2) Wie berechnen wir die Diskriminante $d_{\tilde{L}/k}$ aus L und M?

4.4 Lösungen mit minimaler Verzweigung

Es wird sich als günstig erweisen, die ausgezeichnete Lösung L so zu wählen, dass L/K an möglichst wenigen Stellen verzweigt ist. Leider können wir neue Verzweigung im Allgemeinen nicht vermeiden, welches wir z.B. bei $k = \mathbb{Q}$ und $H = 1$ sehen. Immerhin können wir die neue Verzweigung erheblich beschränken. Aus technischen Gründen müssen wir unterscheiden, ob die primitive ℓ–te Einheitswurzel ζ_ℓ in k liegt.

Lemma 4.11
Es sei K/k eine Erweiterung algebraischer Zahlkörper mit $\mathrm{Gal}(K/k) = H$ und $\zeta_\ell \in k$. Weiterhin seien $S \subseteq \mathbb{P}(k)$ eine endliche Menge von Primidealen und $S' \subseteq \mathbb{P}(k)$ die Menge der verzweigten Primideale von K/k. Wir nehmen an, dass das zentrale Einbettungsproblem (4.2) lösbar ist. Dann existiert eine Lösung L/K, so dass L/k höchstens in $S' \cup \{\mathfrak{q}\} \cup \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathfrak{p}|\ell\}$ verzweigt ist, wobei $\mathfrak{q} \in \mathbb{P}(k) \setminus S$ gilt.

Beweis
Nach Kummertheorie gibt es eine Lösung $L = K(\sqrt[\ell]{\alpha})$ mit einem $\alpha \in K$. Da das Einbettungsproblem zentral ist, gilt für jedes $\sigma \in \mathrm{Gal}(K/k)$, dass L/K^σ abelsch ist. Damit gilt nach einem Lemma von Shafarevich [19, Lemma 2.8], dass $\alpha^\sigma \equiv \alpha \bmod (K^\times)^\ell$. Sei nun $(\alpha) = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ die Faktorisierung des Hauptideals (α). O.E. können wir annehmen, dass $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ unverzweigt in K/k sind. Wir definieren $\tilde{e}_i$ via $\tilde{e}_i \equiv e_i \bmod \ell$ $(1 \leq i \leq s)$. Wegen $\alpha^\sigma \equiv \alpha \bmod (K^\times)^\ell$ ist $\prod_{i=1}^s \mathfrak{p}_i^{\tilde{e}_i}$ $\mathrm{Gal}(K/k)$–invariant. Da diese $\mathfrak{p}_i$ zudem unverzweigt in K/k sind, gilt $\prod_{i=1}^s \mathfrak{p}_i^{\tilde{e}_i} = \mathfrak{b}\mathcal{O}_K$ für ein Ideal $\mathfrak{b} \subseteq \mathcal{O}_k$. In jeder Idealklasse existieren unendlich viele Primideale. Daher können wir ein $\mathfrak{q} \in \mathbb{P}(k) \setminus S$ wählen mit $\mathfrak{b}\mathfrak{q} = (b)$ für ein geeignetes $b \in \mathcal{O}_k$. Nach Lemma 4.8 ist $K(\sqrt[\ell]{b\alpha})$ eine andere Lösung zu unserem Einbettungsproblem. Wegen $(b\alpha) = (\mathfrak{q}\mathcal{O}_K)\mathfrak{a}^\ell \prod_{i=s+1}^r \mathfrak{p}_i^{e_i}$ für ein geeignetes Ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ erfüllt dieser Körper nach Kummertheorie die gewünschten Verzweigungseigenschaften. □

Mittels eines Theorems von Kochendörffer können wir nun auch den Fall $\zeta_\ell \notin k$ aufklären.

Satz 4.12
Es sei K/k eine Erweiterung algebraischer Zahlkörper mit $\mathrm{Gal}(K/k) = H$. Weiterhin seien $S \subseteq \mathbb{P}(k)$ eine endliche Teilmenge von Primidealen und $S' \subseteq \mathbb{P}(k)$ die Menge der verzweigten Primideale von K/k. Wir nehmen an, dass das zentrale Einbettungsproblem (4.2) lösbar ist. Dann existiert eine Lösung L/K, so dass L/k höchstens in $S' \cup \{\mathfrak{q}\} \cup \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathfrak{p}|\ell\}$ verzweigt ist, wobei $\mathfrak{q} \in \mathbb{P}(k) \setminus S$ gilt.

Beweis
Der Fall $\zeta_\ell \in k$ wurde bereits in Lemma 4.11 bewiesen. Daher nehmen wir im Folgenden an, dass $\zeta_\ell \notin k$ gilt. Falls unser Einbettungsproblem zerfallend ist, so gilt $G \cong Z_\ell \times H$. Es gibt stets eine Z_ℓ–Erweiterung von k, die in höchstens einem Primideal $\mathfrak{q} \notin S$ verzweigt ist. Daher nehmen wir zusätzlich an, dass unser Einbettungsproblem nicht zerfallend und damit ein Frattini–Einbettungsproblem (Lemma 4.2) ist.

Es sei $\tilde{L}$ eine beliebige Lösung des zentralen Einbettungsproblems (4.2). Dann ist auch das folgende Einbettungsproblem für $K(\zeta_\ell)/k(\zeta_\ell)$ lösbar:

$$1 \to Z_\ell \to \mathrm{Gal}(\tilde{L}(\zeta_\ell)/k(\zeta_\ell)) \to \mathrm{Gal}(K(\zeta_\ell)/k(\zeta_\ell)) \to 1.$$

Nach Lemma 4.11 können wir eine Lösung $\hat{L}$ mit den gewünschten Verzweigungseigenschaften finden. Nach dem Theorem von Kochendörffer [25, Thm.IV.8.2] kann ein (schwacher) Lösungskörper des ursprünglichen Einbettungsproblems in der normalen Hülle von $\hat{L}/k$ gefunden werden. Da dieses Einbettungsproblem ein Frattini–Einbettungsproblem ist, ist ein solcher Körper sogar schon ein Lösungskörper (Lemma 4.2) mit den gewünschten Verzweigungseigenschaften. □

Im zerfallenden Fall können wir stets eine Z_ℓ–Erweiterung von k finden, die höchstens in Primidealen über ℓ verzweigt ist. Daher kommen wir in diesem Fall ohne das Ideal $\mathfrak{q}$ aus. Wir merken an, dass die Norm des Ideals $\mathfrak{q}$ nur in Abhängigkeit vom Grundkörper k und der Menge S nach oben beschränkt werden kann. Zum Beispiel können wir für jede Idealklasse in $\mathcal{O}_{k(\zeta_\ell)}$ ein Primideal $\mathfrak{P}$ wählen, so dass $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_k$ nicht in S liegt. Wir können dann $\mathfrak{q}$ aus dieser konstruierten Menge wählen. Im Folgenden wird es für uns wichtig sein, die Existenz von Z_ℓ–Erweiterungen mit bestimmten Eigenschaften zu garantieren.

Satz 4.13
Es seien k ein Zahlkörper, ℓ eine Primzahl sowie $T \subseteq \mathbb{P}(k)$ so gewählt, dass die Primideale von $\mathcal{O}_{k(\zeta_\ell)}$, die über denen von T liegen, die Klassengruppe von $k(\zeta_\ell)$ erzeugen. Zusätzlich enthalte T alle Primideale, die über ℓ liegen. Dann gilt für ein beliebiges $\mathfrak{q} \in \mathbb{P}(k)$:

Wenn es eine Z_ℓ–Erweiterung von k gibt, die in $\mathfrak{q}$ verzweigt ist, dann gibt es auch eine Z_ℓ–Erweiterung von k, die in $\mathfrak{q}$ verzweigt und außerhalb von $T \cup \{\mathfrak{q}\}$ unverzweigt ist.

Beweis
Es sei K/k eine Z_ℓ–Erweiterung, die in $\mathfrak{q}$ verzweigt ist. Da in T alle Primideale über ℓ liegen und auch die Klassengruppe von $k(\zeta_\ell)$ erzeugt wird, zeigt der

Beweis von Satz 4.12, angewendet auf die triviale Gruppe H, die Existenz unserer gewünschten Erweiterung. □

Aufgrund von Klassenkörpertheorie ist klar, dass stets eine in $\mathfrak{q}$ verzweigte Z_ℓ–Erweiterung existiert, falls $\mathfrak{q}$ über ℓ liegt oder $\ell \mid (\mathcal{N}(\mathfrak{q}) - 1)$ gilt.

Wir können jetzt Satz 4.12 noch verschärfen.

Satz 4.14
Es sei K/k eine Erweiterung algebraischer Zahlkörper mit $\mathrm{Gal}(K/k) = H$. Weiterhin sei T wie in Satz 4.13 gewählt. Wir nehmen an, dass das zentrale Einbettungsproblem (4.2) lösbar ist. S' bezeichne die Menge der Primideale von $\mathcal{O}_K$, welche in jeder Lösung L/K verzweigt sind. Dann existiert eine Lösung L/K, die höchstens in

$$S' \cup \{\mathfrak{p} \mid \mathfrak{p} \text{ liegt über einem Primideal aus } T\}$$

verzweigt ist.

Beweis
Gegeben sei eine Lösung L_1 wie in Satz 4.12. Diese Lösung erfüllt schon alle gewünschten Eigenschaften für die nicht in K/k verzweigten Primideale. Sei nun $\mathfrak{p}$ ein solches verzweigtes Primideal, welches in einer Lösung L_2 unverzweigt ist. Die Erweiterung L_1L_2/K hat Galoisgruppe $Z_\ell \times Z_\ell$ und somit ist $\mathfrak{p}$ nach Lemma 2.4 in allen echten Zwischenkörpern von L_1L_2/K außer L_2 verzweigt. Insbesondere ist $\mathfrak{p}$ nach Lemma 2.4 in der Z_ℓ–Erweiterung verzweigt, welche nach Satz 4.9 Galoisgruppe $Z_\ell \times H$ hat. Daher existiert eine Z_ℓ–Erweiterung von k, welche in $\mathfrak{p}$ verzweigt ist. Nach Satz 4.13 gibt es nun eine Z_ℓ–Erweiterung M/k, welche in $\mathfrak{p}$ verzweigt und außerhalb von T unverzweigt ist. Wir betrachten nun die Körpererweiterung L_1M/K. In dieser Z_ℓ–Erweiterung gibt es genau einen echten Zwischenkörper $K < L < L_1M$, welcher in $\mathfrak{p}$ unverzweigt ist. Nach Satz 4.9 gilt $\mathrm{Gal}(L/K) = G$. Die Verzweigung von L_1 und L unterscheidet sich höchstens in $T \cup \{\mathfrak{p}\}$. Induktiv erhalten wir die gewünschte Lösung. □

Mit Hilfe von Satz 4.13 können wir nun auch das Ergebnis von Korollar 2.27 verschärfen.

Lemma 4.15
Es seien k ein algebraischer Zahlkörper, $S \subseteq \mathbb{P}(k)$ eine endliche Teilmenge sowie $\ell \in \mathbb{P}$. Dann existiert eine Konstante $c(k, \ell)$, so dass die Anzahl der Z_ℓ–Erweiterungen von k, die genau in S verzweigt sind, nach oben beschränkt ist durch

$$\ell^{c(k,\ell)}(\ell - 1)^{|S|}.$$

Beweis
Wir wählen die Menge T wie in Satz 4.13 und setzen $\tilde{S} := S \setminus T$. Wir wählen gemäß Satz 4.13 für jedes $\mathfrak{p} \in \tilde{S}$ eine Z_ℓ–Erweiterung, die in $\mathfrak{p}$ verzweigt und außerhalb von $T \cup \{\mathfrak{p}\}$ unverzweigt ist. Wir bezeichnen die Menge dieser Körpererweiterungen mit $M_{\tilde{S}}$. Weiterhin bezeichnen wir mit M_T eine Menge minimaler Anzahl, so dass das Kompositum dieser Körper die maximale elementarabelsche ℓ–Erweiterung N_T erzeugt, die höchstens in T verzweigt ist. Wir definieren N als das Kompositum all der Körper in $M_{\tilde{S}} \cup M_T$. Wir behaupten, dass N die maximale elementarabelsche ℓ–Erweiterung von k ist, die höchstens in $S \cup T = \tilde{S} \cup T$ verzweigt ist. Sei hierzu K/k eine beliebige Z_ℓ–Erweiterung, die höchstens in $S \cup T$ verzweigt ist. Falls kein $\mathfrak{p} \in \tilde{S}$ verzweigt ist, so ist K ein Teilkörper von N_T. Seien also $\mathfrak{p} \in \tilde{S}$ ein verzweigtes Primideal von K/k und $M \in M_S$ die Erweiterung, die in $\mathfrak{p}$ verzweigt ist. Dann liegt nach Lemma 2.4 im Kompositum KM eine Z_ℓ–Erweiterung von k, welche in $\mathfrak{p}$ unverzweigt ist. Induktiv erhalten wir so eine Erweiterung, welche für alle $\mathfrak{p} \in \tilde{S}$ unverzweigt ist. Damit haben wir $K \subseteq N$ gezeigt. Somit ist N tatsächlich die maximale elementarabelsche ℓ–Erweiterung von k, die höchstens in $S \cup T = \tilde{S} \cup T$ verzweigt ist.

Sei nun $N_{\tilde{S}}$ das Kompositum aller Z_ℓ–Erweiterungen aus $M_{\tilde{S}}$. Das Kompositum zweier Erweiterungen aus $M_{\tilde{S}}$ enthält wieder nach Lemma 2.4 genau $\ell - 1$ Erweiterungen, die in zwei Primidealen aus $\tilde{S}$ verzweigt sind. Induktiv erhalten wir so, dass $N_{\tilde{S}}$ genau $(\ell-1)^{|\tilde{S}-1|}$ Erweiterungen enthält, die in allen $\mathfrak{p} \in \tilde{S}$ verzweigt sind. Da alle Erweiterungen aus M_T in $\tilde{S}$ unverzweigt sind, enthält jedes Kompositum einer Z_ℓ–Erweiterung aus M_T sowie einer bisher konstruierten in $\tilde{S}$ verzweigten Erweiterung genau ℓ Teilkörper, die in ganz $\tilde{S}$ verzweigt sind. Daher erhalten wir als obere Abschätzung für diese Anzahl:

$$\ell^{|T|}(\ell-1)^{|\tilde{S}-1|} \leq \ell^{c(k,\ell)}(\ell-1)^{|S|}.$$

Hierbei ist klar, dass sich $|T|$ durch eine nur von k und ℓ abhängige Konstante nach oben abschätzen lässt. Weiterhin ist jede genau in S verzweigte Z_ℓ–Erweiterung in obiger Betrachtung mitgezählt worden. □

4.5 Direkte Produkte

Wir sind nun in der Lage, ein erstes induktives Ergebnis für eine obere Schranke für unsere gesuchte Asymptotik von $Z(k, G; x)$ anzugeben. Hierzu vergleichen wir die Lösungen unseres Einbettungsproblems (4.2) mit denen des zugehörigen zerfallenden Einbettungsproblems

$$1 \to Z_\ell \to Z_\ell \times H \to H \to 1.$$

Satz 4.16
Es seien Gruppen G, H wie in (4.2) sowie ein Zahlkörper k gegeben. Wir wählen eine endliche Menge $T \subseteq \mathbb{P}(k)$ wie in Satz 4.13. Dann existiert eine Konstante $c(k, G) > 0$ mit:

$$Z^T(k, G; x) \leq c(k, G, T) Z^T(k, H \times Z_\ell; x).$$

Beweis
Für eine gegebene Körpererweiterung K/k mit Galoisgruppe H wählen wir eine minimale Lösung L wie in Satz 4.14. Zu jedem weiteren Lösungskörper L_M ist nach Satz 4.10 eine zyklische Erweiterung M/k assoziiert, wobei $\ell - 1$ Körper zu demselben M gehören. Für unsere Abschätzung ist es nun wichtig den zu T koprimen Teil der Diskriminanten von L_M/K und KM/K zu vergleichen. Wegen der Minimalität der Lösung L stimmen diese Diskriminanten an allen Primidealen überein, die nicht in L/K verzweigt sind und koprim zu T sind. Ein Primideal $\mathfrak{p} \notin T$, welches in L/K verzweigt ist, ist in allen Lösungen verzweigt. Daher ist dieses Primideal wegen Lemma 2.4 in KM/K unverzweigt. Wir erhalten somit die Abschätzung: $\mathcal{N}(d^T_{L_M/K}) \geq \mathcal{N}(d^T_{KM/K})$ und damit $\mathcal{N}(d^T_{L_M/k}) \geq \mathcal{N}(d^T_{KM/k})$. Die Anzahl der verschiedenen Einbettungsprobleme $1 \to Z_\ell \to G \to H \to 1$ mit festem G und H ist eine Konstante, die nur von G und H abhängt (siehe Lemma 4.3). Da wir nur eine obere Abschätzung beweisen wollen, können wir ignorieren, dass nicht jedes Einbettungsproblem lösbar ist. Insgesamt finden wir so eine Konstante $c(k, G, T)$ mit

$$Z^T(k, G; x) \leq c(k, G, T) Z^T(k, H \times Z_\ell; x),$$

da wir je maximal $\ell - 1$ Körpern mit Gruppe G einen Körper mit Gruppe $H \times Z_\ell$ zuordnen können, der kleinere Diskriminante hat. □

Falls wir eine untere Schranke für $Z^T(k, H \times Z_\ell; x)$ kennen, so können wir mit Hilfe von Lemma 3.15 (1) auch die entsprechende Aussage für die normalen Zählfunktionen beweisen.

Als nächsten Schritt beweisen wir eine induktive obere Schranke für direkte Produkte $H \times Z_\ell$. Mit Hilfe des obigen Satzes erhalten wir so auch eine obere Schranke für beliebige zentrale Einbettungsprobleme mit Z_ℓ–Kern. Wir bezeichnen im Folgenden mit $\mathcal{K}(x)$ die Menge der Körpererweiterungen K/k mit $\mathrm{Gal}(K/k) = H$ und $\mathcal{N}(d_{K/k}) \leq x$.

Satz 4.17
Es seien $G = H \times Z_\ell$, k ein Zahlkörper sowie $n = |G|$. Zusätzlich gelte für alle $\epsilon > 0$:

$$Z(k, H; x) \leq c(k, H, \epsilon) x^{a(H)+\epsilon}.$$

Dann gilt:

(1) Falls $\frac{a(H)}{\ell} < \frac{\ell}{(\ell-1)n}$, *so gilt* $a(G) = \frac{\ell}{(\ell-1)n}$ *und*

$$Z(k,G;x) \leq c(k,G)x^{a(G)}\log(x)^{b(k,Z_\ell)}.$$

(2) Falls $\frac{a(H)}{\ell} \geq \frac{\ell}{(\ell-1)n}$, *so gilt* $a(G) = a(H)/\ell$ *und für alle* $\epsilon > 0$

$$Z(k,G;x) \leq c(k,G,\epsilon)x^{a(G)+\epsilon}.$$

Beweis
Nach [23, Lemma 4.1] gilt $a(G) = \max(\frac{a(H)}{\ell}, \frac{a(Z_\ell)}{n/\ell}) = \max(\frac{a(H)}{\ell}, \frac{\ell}{n(\ell-1)})$. Es seien K/k und M/k Erweiterungen mit Galoisgruppe H bzw. Z_ℓ, die zueinander disjunkt sind. (Falls es diese Erweiterungen mit $K \cap M = k$ nicht gibt, so gibt es keine Erweiterung mit Galoisgruppe G und die Aussage des Satzes ist trivial.) Dann gilt $\mathrm{Gal}(KM/k) = G$, $n = [K:k]\ell$ sowie

$$\mathcal{N}(d_{KM/k}) = \mathcal{N}(d_{K/k}^{\ell}\mathcal{N}_{K/k}(d_{KM/K})).$$

Wir bezeichnen mit $S_K \subseteq \mathbb{P}(k)$ die in K/k verzweigten Primideale. Dann gilt: $\mathcal{N}(d_{KM/K}) \geq \mathcal{N}(d_{KM/K}^{S_K}) = \mathcal{N}((d_{M/k}^{[K:k]})^{S_K})$. Daher erhalten wir mit $r_K := |S_K|$ folgende Abschätzung:

$$Z(k,G;x) \leq \sum_{K\in\mathcal{K}(x^{1/\ell})} Z^{S_K}(k,Z_\ell;\frac{x}{d_K^\ell})^{1/[K:k]}$$

$$\leq \sum_{K\in\mathcal{K}(x^{1/\ell})} \ell^{r_K} c(k,Z_\ell)(\frac{x}{d_K^\ell})^{\ell/(n(\ell-1))}\log((x/d_K^\ell)^{\ell/n})^{b(k,Z_\ell)} \text{ (Satz 3.23)}$$

$$\leq c(k,Z_\ell)x^{\ell/(n(\ell-1))}\log(x)^{b(k,Z_\ell)} \sum_{K\in\mathcal{K}(x^{1/\ell})} \frac{\ell^{r_K}}{d_K^{\ell^2/(n(\ell-1))}}$$

$$\leq c(k,Z_\ell)x^{\ell/(n(\ell-1))}\log(x)^{b(k,Z_\ell)} \sum_{K\in\mathcal{K}(x^{1/\ell})} \frac{c([K:\mathbb{Q}],\delta)d_K^\delta}{d_K^{\ell^2/(n(\ell-1))}} \text{ für alle } \delta > 0.$$

In der letzten Zeile haben wir ℓ^{r_K} durch $c([K:\mathbb{Q}],\delta)d_K^\delta$ gemäß Lemma 2.20 (2) nach oben abgeschätzt.
Wir bezeichnen mit $a(d)$ die Anzahl der Körper K mit $\mathrm{Gal}(K/k) = H$ und $\mathcal{N}(d_{K/k}) = d$. Für die Summe erhalten wir so ($[K:\mathbb{Q}] = \ell[k:\mathbb{Q}]$):

$$c([k:\mathbb{Q}],\ell,\delta)\sum_{d=1}^{x^{1/\ell}} \frac{a(d)}{d^{\ell^2/(n(\ell-1))-\delta}}. \tag{4.3}$$

Nach Voraussetzung gilt für die Summe:

$$\sum_{d=1}^{x} a(d) \leq c(k,H,\epsilon)x^{a(H)+\epsilon}.$$

Falls $\frac{a(H)}{\ell} < \frac{\ell}{(\ell-1)n}$ so konvergiert die Summe (4.3) für $x \to \infty$ nach Lemma 2.18.

Ansonsten können wir obige Abschätzung weiterführen und erhalten wegen $x \geq d^{\ell}$:

$$Z(k,G;x) \leq c(k,Z_\ell)x^{\ell/(n(\ell-1))}\log(x)^{b(k,Z_\ell)}c([k:\mathbb{Q}],\ell,\delta)x^{a(H)/\ell-\ell/(n(\ell-1))+\epsilon}$$

$$\sum_{d=1}^{x^{1/\ell}} \frac{a_d d^{\delta}}{d^{\ell^2/(n(\ell-1))}x^{a(H)/\ell-\ell/(n(\ell-1))+\epsilon}}$$

$$\leq c(k,G,\delta)x^{a(H)/\ell+2\epsilon}\sum_{d=1}^{x^{1/\ell}} \frac{a_d d^{\delta}}{d^{\ell^2/(n(\ell-1))}d^{a(H)-\ell^2/(n(\ell-1))+\ell\epsilon}}$$

$$= c(k,G,\delta)x^{a(G)+2\epsilon}\sum_{d=1}^{x^{1/\ell}} \frac{a_d}{d^{a(H)-\delta+\ell\epsilon}}.$$

Letztere Summe konvergiert wieder nach Lemma 2.18, wenn wir $\delta < \ell\epsilon$ wählen. □

Wir können mit diesem Ansatz kein besseres Ergebnis erwarten, da wir ℓ^{r_K} durch d_K^{δ} abschätzen müssen. Die Teilerfunktion verhält sich zwar im Mittel besser, aber ohne Zusatzinformation können wir nicht wissen, welche Diskriminanten von Körpern mit Galoisgruppe H angenommen werden. Wir werden im nächsten Abschnitt dieses Problem für nilpotente Erweiterungen G durch einen anderen Ansatz umgehen.

Satz 4.18
Es sei $G \leq S_n$ transitiv eine zentrale Erweiterung von H wie in (4.2). Zusätzlich gelte für alle $\epsilon > 0$:

$$Z(k,H;x) \leq c(k,H,\epsilon)x^{a(H)+\epsilon}.$$

Dann gilt:

(1) Falls $\frac{a(H)}{\ell} < \frac{\ell}{(\ell-1)n}$, so gilt:

$$Z(k,G;x) \leq c(k,G)x^{a(G)}\log(x)^{b(k,Z_\ell)}.$$

(2) Falls $\frac{a(H)}{\ell} \geq \frac{\ell}{(\ell-1)n}$, *so gilt für alle* $\epsilon > 0$*:*

$$Z(k, G; x) \leq c(k, G, \epsilon) x^{a(G)+\epsilon}.$$

Beweis
Wir erhalten nach Satz 4.16

$$Z(k, G; x) \leq Z^T(k, G; x) \leq Z^T(k, Z_\ell \times H; x).$$

Nun folgt die Aussage aus Satz 4.17 und Lemma 3.15 (2). □

4.6 Nilpotente Gruppen

In diesem Abschnitt wollen wir obere Abschätzungen für die Asymptotik von $Z(k, G; x)$ im Falle von nilpotenten Gruppen G herleiten. Für diese Gruppen können wir ziemlich viel beweisen, da die Klassengruppen von Zwischenkörpern keine Rolle spielen werden. Nilpotente Gruppen besitzen sogenannte Zentralreihen, d.h. jede nicht triviale nilpotente Gruppe G besitzt ein nicht triviales Zentrum $\mathrm{Z}(G)$. Falls $G/\mathrm{Z}(G)$ nicht trivial ist, besitzt es auch ein nicht triviales Zentrum, so dass rekursiv die sogenannte Zentralreihe entsteht. Wir können diese Zentralreihe weiter verfeinern, indem wir in jedem Schritt nur eine zentrale zyklische Gruppe von Primzahlordnung rausfaktorisieren.

Zu einer gegebenen nilpotenten Gruppe G können wir also Gruppen $G_r := G, G_{r-1}, \ldots, G_0 = 1$ und Epimorphismen $\phi_i : G_i \to G_{i-1}$ wählen, deren Kern Primzahlordnung p_i hat und im Zentrum von G_i liegt. Wir haben also:

$$1 \longrightarrow Z_{p_i} \longrightarrow G_i \xrightarrow{\phi_i} G_{i-1} \longrightarrow 1 \text{ zentral.}$$

Nehmen wir an, dass N/k eine galoissche Erweiterung mit Galoisgruppe G ist. Korrespondierend zur obigen Reihe können wir einen Körperturm $k = N_0 \subseteq N_1 \subseteq \ldots \subseteq N_r = N$ finden mit $\mathrm{Gal}(N_i/k) = G_i$ sowie $\mathrm{Gal}(N_i/N_{i-1}) = Z_{p_i}$.

Im Folgenden zeigen wir, wie wir die Diskriminanten der zugehörigen Körper möglichst genau bestimmen können. Bisher haben wir in diesem Kapitel G immer als abstrakte Gruppe aufgefasst, d.h. wir haben alle Schlüsse für die zugehörigen normalen Erweiterungen N/k gezeigt. Alle diese Überlegungen bleiben auch für nicht reguläre Permutationsgruppen G gültig, da wir mit Lemma 4.4 eine Zuordnung der nicht normalen Erweiterungen K/k zu ihren normalen Hüllen bekommen. Lediglich die Diskriminanten der Körpererweiterungen K/k und N/k werden unterschiedlich berechnet.

Lemma 4.19
Es sei $\mathfrak{p} \in \mathbb{P}(k)$ ein Primideal, welches in N/k zahm verzweigt ist. Wir bezeichnen mit σ einen Trägheitsgruppenerzeuger eines Ideals $\mathfrak{P} \subseteq \mathcal{O}_N$, welches über $\mathfrak{p}$ liegt. Da alle diese Primideale konjugiert sind, ist die Konjugationsklasse von σ unabhängig von dieser Wahl. Nun gilt:

$$v_{\mathfrak{p}}(d_{N/k}) = \mathrm{ind}(\sigma) = |G| - |G|/\operatorname{ord}(\sigma).$$

Nun sei $G \leq S_n$ als Permutationsgruppe gegeben und wir bezeichnen mit $K \leq N$ einen Teilkörper mit $\mathrm{Gal}(K/k) = G$. Dann gilt:

$$v_{\mathfrak{p}}(d_{K/k}) = \mathrm{ind}(\sigma),$$

wobei diesmal der Index von $\sigma \in G \leq S_n$ berechnet wird.

Im Allgemeinen werden wir einen Trägheitsgruppenerzeuger nicht bestimmen können. Um obere Schranken für unsere Zählfunktion zu bekommen, werden wir den Index eines Trägheitsgruppenerzeugers nach unten abschätzen. Hierzu werden wir ausnutzen, in welchem Schritt $\mathfrak{p}$ zum ersten Mal im Körperturm $N_r/N_{r-1}/\ldots/N_0$ verzweigt ist.
Wir bezeichnen mit $1 \leq i \leq r$ die Zahl mit $\mathfrak{p} \mid d_{N_i/k}$ aber $\mathfrak{p} \nmid d_{N_{i-1}/k}$. In diesem Fall wissen wir, dass ein Trägheitsgruppenerzeuger von $\mathfrak{p}$ in G_i gerade ein zentrales Element der Ordnung p_i in G_i ist, also im Kern von ϕ_i liegt. Wir definieren ψ_i und A_i für $1 \leq i \leq r$ wie folgt:

$$\psi_i : G \to G_i,\ x \mapsto \phi_{i+1} \circ \ldots \circ \phi_r(x), \quad A_i := \psi_i^{-1}(\ker(\phi_i) \setminus \{1\}).$$

Damit wissen wir, dass unser Trägheitsgruppenerzeuger σ in der Menge A_i liegt. Für unsere untere Abschätzung des Index definieren wir:

$$a_i := \min_{g \in A_i}(\mathrm{ind}(g))$$

und erhalten somit $v_{\mathfrak{p}}(d_{K/k}) \geq a_i$. Für $1 \leq i \leq r$ definieren wir $\mathfrak{a}_i \subseteq \mathcal{O}_k$ als das Produkt der Primideale in $\mathcal{O}_k$, welche in N_i zum ersten Mal verzweigen. Auf diese Weise haben wir N/k bzw. K/k ein Tupel von koprimen und quadratfreien Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ zugeordnet und den folgenden Satz bewiesen. Dabei merken wir an, dass bei wild verzweigten Primidealen die linke Seite größer wird.

Satz 4.20
Es sei K/k eine Erweiterung mit Galoisgruppe $G \leq S_n$ und a_i, $\mathfrak{a}_i$ seien für $1 \leq i \leq r$ wie im vorigen Abschnitt definiert. Dann gilt:

$$\mathcal{N}(d_{K/k}) \geq \mathcal{N}(\mathfrak{a}_1)^{a_1} \cdots \mathcal{N}(\mathfrak{a}_r)^{a_r}.$$

Da $\ker(\phi_i) \cong Z_{p_i}$ erhalten wir folgende wichtige Eigenschaft der Mengen A_i.

Bemerkung 4.21
Für die oben definierten Mengen $A_1, \ldots, A_r$ gelten:

(1) $G \setminus \{1\} = A_1 \dot\cup \ldots \dot\cup A_r$.

(2) $|A_i| = |p_i - 1||\ker(\psi_i)| = (p_i - 1)p_{i+1} \cdots p_r$ *für* $1 \leq i \leq r$.

Bevor wir weitermachen, geben wir zwei kurze Beispiele an.

Beispiel 4.22
Sei $G = Q_8 \leq S_8$ die Quaternionengruppe. Diese besitzt ein Element der Ordnung 2 und sechs Elemente der Ordnung 4. In obiger Notation erhalten wir:

$$G_3 = Q_8, G_2 \cong Z_2 \times Z_2, G_1 \cong Z_2, G_0 = 1.$$

Da alle Elemente aus G_1 bzw. G_2 unter ψ_i $(i = 1, 2)$ zu Elementen der Ordnung 4 liften, bestehen die Mengen A_1 und A_2 nur aus Elementen der Ordnung 4, die in Q_8 alle den Index 6 haben. Daher erhalten wir $a_1 = a_2 = 6$ (Zykeltyp 4^2). Die Menge A_3 besteht nur aus dem zentralen Element der Ordnung 2 und daher erhalten wir $a_3 = 4$ (Zykeltyp 2^4). Für ein Tupel von quadratfreien Idealen $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ erhalten wir so die Abschätzung

$$\mathcal{N}(d_{K/k}) \geq \mathcal{N}(\mathfrak{a}_1)^6 \mathcal{N}(\mathfrak{a}_2)^6 \mathcal{N}(\mathfrak{a}_3)^4.$$

Beispiel 4.23
Sei nun $G = D_4(8) \leq S_8$ die Diedergruppe der Ordnung 8, welche 2 Elemente der Ordnung 4 und 5 Elemente der Ordnung 2 besitzt. Wir erhalten analog:

$$G_3 = D_4, G_2 \cong Z_2 \times Z_2, G_1 \cong Z_2, G_0 = 1.$$

Da $\mathrm{Z}(D_4) = Z_2$ ist ϕ_3 durch diese Angaben wohl definiert. Wir haben allerdings drei mögliche Wahlen für ϕ_2, da $Z_2 \times Z_2$ drei verschiedene Faktorgruppen isomorph zu Z_2 hat. Für die Menge A_1 müssen wir die Urbildmenge unter ψ_1 eines Elements der Ordnung 2 in G bestimmen. Da diese Menge 4 Elemente enthält, müssen auch Elemente der Ordnung 2 dabei sein, woraus $a_1 = 4$ folgt. Nun ist der nicht triviale Anteil des Kerns von ϕ_2 ein Element der Ordnung 2. Die Urbilder hängen jetzt stark von der Wahl von ϕ_2 ab. In einem Fall erhalten wir zwei Urbilder der Ordnung 4 unter ψ_2. In den beiden anderen Fällen erhalten wir Elemente der Ordnung 2. Je nach Wahl erhalten wir also $a_2 = 6$ oder $a_2 = 4$. Die geschicktere Wahl ist natürlich diejenige, die zu $a_2 = 6$ führt (siehe Anmerkungen nach Beispiel 4.27).

Es stellt sich nun die Frage, ob und wie viele Körper K/k zu einem gegebenen Tupel $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ wie oben assoziiert sind.

Wir bezeichnen mit I_k die Halbgruppe der Ideale von $\mathcal{O}_k$ und definieren folgende Abbildung:

$$\Phi : \{K/k \mid \mathrm{Gal}(K/k) = G\} \to I_k^r, K \mapsto (\mathfrak{a}_1, \ldots, \mathfrak{a}_r). \tag{4.4}$$

Wir erinnern daran, dass $\omega(\mathfrak{a})$ die Anzahl der Primteiler von $\mathfrak{a}$ bezeichnet.

Satz 4.24
Für $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) \in I^r$ definieren wir

$$b_i := \omega(\prod_{j=1}^{i-1} \mathfrak{a}_j) + c(k),$$

wobei wir die Konstante $c(k)$ nur in Abhängigkeit von k und den p_i wählen können. Dann besitzt $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ höchstens

$$p_1^{b_1} \cdots p_r^{b_r} (p_1 - 1)^{\omega(\mathfrak{a}_1)} \cdots (p_r - 1)^{\omega(\mathfrak{a}_r)}$$

Urbilder unter der obigen Abbildung Φ.

Beweis
Wir werden im Folgenden beweisen, dass $(p_i)^{b_i}(p_i - 1)^{\omega(\mathfrak{a}_i)}$ für $1 \leq i \leq r$ eine obere Schranke für die Anzahl der Urbilder der zu G_i gehörenden Funktion ist. Die Behauptung des Satzes folgt dann durch Aufmultiplizieren dieser Zahlen.

In Satz 4.10 haben wir bewiesen, dass wir Lösungen zu zentralen Einbettungsproblemen mit Z_ℓ–Kern durch zyklische Erweiterungen des Grundkörpers parametrisieren können. Wir müssen uns im i–ten Schritt überlegen, wie viele Z_ℓ–Erweiterungen M/k (mit $\ell = p_i$) maximal zur Verzweigung in $\mathfrak{a}_i$ führen können. Da bereits verzweigte Primideale weiterverzweigen dürfen, müssen wir auch Verzweigung in $\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}$ berücksichtigen. Dies bedeutet, dass wir die Anzahl der Z_ℓ–Erweiterungen von k nach oben abschätzen wollen, welche höchstens in den Primidealen verzweigt sind, welche $\mathfrak{a}_1 \cdots \mathfrak{a}_i$ teilen. Da es nur endlich viele Primideale in $\mathcal{O}_k$ gibt, welche über ℓ liegen, können wir mit Korollar 2.27 die Anzahl der Z_ℓ–Erweiterungen, die höchstens in Primteilern von $\mathfrak{a}_1 \cdots \mathfrak{a}_i$ verzweigt sind, durch $\ell^{c(k,\ell)} \ell^{\omega(\mathfrak{a}_1 \cdots \mathfrak{a}_i)}$ abschätzen. Da die Primideale, die $\mathfrak{a}_i$ teilen zusätzlich alle verzweigen müssen, können wir für diesen Teil die bessere Abschätzung aus Lemma 4.15 verwenden und erhalten als obere Schranke:

$$\ell^{c(k,\ell)} \ell^{\omega(\mathfrak{a}_1 \cdots \mathfrak{a}_{i-1})} (\ell - 1)^{\omega(\mathfrak{a}_i)}.$$

Wir definieren $c(k)$ als das Maximum aller auftretenden $c(k, p_i)$ (Wir hatten $\ell = p_i$ gesetzt.). Die Behauptung folgt nun unmittelbar. □

Nun können wir den Hauptsatz dieses Abschnitts beweisen. Die Konstante $a(G)$ im folgenden Satz ist wie in Definition 2.9 definiert und ist damit wie vermutet. Entscheidend ist der Zusammenhang

$$a(G)^{-1} = \mathrm{ind}(G) = \min_{1 \le i \le r} \{a_i\}.$$

Die Konstante d kann größer als erwartet sein (siehe Lemma 4.26).

Satz 4.25
Es sei G eine transitive nilpotente Untergruppe der S_n. Dann existieren Konstanten $c(k, G), d(G)$ mit

$$Z(k, G; x) \le c(k, G) x^{a(G)} \log(x)^{d(G)}.$$

Beweis
Wir definieren $p_1, \ldots, p_r$ sowie $b_1, \ldots, b_r$ wie in Satz 4.24. Dann erhalten wir mit Hilfe der Sätze 4.24 und 4.20, wobei die folgende Summe wie im Abschnitt 2.8 definiert ist:

$$Z(k, G; x) \le \sum_{\mathcal{N}(\mathfrak{a}) \le x} \sum_{\mathfrak{a}_1^{a_1} \cdots \mathfrak{a}_r^{a_r} = \mathfrak{a}} p_1^{b_1} \cdots p_r^{b_r} (p_1 - 1)^{\omega(\mathfrak{a}_1)} \cdots (p_r - 1)^{\omega(\mathfrak{a}_r)}$$

$$= (p_1 \cdots p_r)^{c(k)} \sum_{\mathcal{N}(\mathfrak{a}) \le x} \sum_{\mathfrak{a}_1^{a_1} \cdots \mathfrak{a}_r^{a_r} = \mathfrak{a}} p_2^{\omega(\mathfrak{a}_1)} \cdots p_r^{\omega(\mathfrak{a}_1 \cdots \mathfrak{a}_{r-1})} (p_1 - 1)^{\omega(\mathfrak{a}_1)} \cdots (p_r - 1)^{\omega(\mathfrak{a}_r)}$$

$$= (p_1 \cdots p_r)^{c(k)} \sum_{\mathcal{N}(\mathfrak{a}) \le x} \sum_{\mathfrak{a}_1^{a_1} \cdots \mathfrak{a}_r^{a_r} = \mathfrak{a}} l_1^{\omega(\mathfrak{a}_1)} \cdots l_r^{\omega(\mathfrak{a}_r)},$$

wobei $l_r = (p_r - 1), l_{r-1} = p_r(p_{r-1} - 1), \ldots, l_1 = p_r \cdots p_2(p_1 - 1)$. Wir erhalten nun die gewünschte obere Abschätzung mit Lemma 2.23. □

Wir schätzen die Konstante $d(G)$ wie folgt ab.

Lemma 4.26
In der Situation von Satz 4.25 gilt für alle Zahlkörper k:

$$b(k, G) \le |\{\sigma \in G \mid \mathrm{ind}(\sigma) = \mathrm{ind}(G)\}| - 1 \le d(G) \le |G| - 2.$$

Beweis
Die erste Ungleichung folgt direkt aus der Definition von $b(k, G)$. Nach Bemerkung 4.21 und dem Beweisende von Satz 4.25 erhalten wir:

$$G \setminus \{1\} = A_1 \dot\cup \ldots \dot\cup A_r \text{ und } l_i = |A_i| = (p_i - 1) p_{i+1} \cdots p_r \ (1 \le i \le r).$$

Nun liefert Lemma 2.23 gerade

$$d(G)+1=\sum_{\{i:a_i=\mathrm{ind}(G)\}} l_i=\sum_{\{i:a_i=\mathrm{ind}(G)\}} |A_i|$$

Da 1 in keinem A_i enthalten ist, erhalten wir die obere Abschätzung $d(G)\leq |G|-2$. Da jedes Element $\sigma\in G$ mit $\mathrm{ind}(\sigma)=\mathrm{ind}(G)$ in einem der mitgezählten A_i liegen muss, folgt die untere Abschätzung. □

Es gibt aber Situationen, wo die beiden Konstanten $b(k,G)$ und $d(G)$ übereinstimmen. Wir setzen Beispiel 4.22 fort.

Beispiel 4.27
Sei $G=Q_8\leq S_8$ die Quaternionengruppe. Diese besitzt nur ein Element der Ordnung 2. Damit erhalten wir $a(G)=1/4$ und $b(k,G)=0$. Wenn wir uns der Einfachheit halber noch auf $k=\mathbb{Q}$ beschränken, so erhalten wir (alle Ideale in $\mathbb{Z}$ sind Hauptideale, daher summieren wir über deren positive Erzeuger):

$$Z(\mathbb{Q},Q_8;x)\leq 2^3\sum_{a^6b^6c^4\leq x} 4^{\omega(a)}2^{\omega(b)}.$$

Dabei entsteht die 2^3 durch dreimalige Vorzeichenwahl (Berücksichtigung der unendlichen Stelle). Diese Summe können wir mit Lemma 2.23 durch $c(\mathbb{Q},Q_8)x^{1/4}$ nach oben abschätzen. In Beispiel 4.31 zeigen wir für eine Konstante $\tilde{c}(\mathbb{Q},Q_8)>0$ und $x>>0$: $Z(\mathbb{Q},Q_8;x)>\tilde{c}(\mathbb{Q},Q_8)x^{1/4}$.

Wir merken an, dass die selbe Argumentation für $k\neq\mathbb{Q}$ funktioniert. Im Falle $G=D_4\leq S_8$ erhalten wir $d(D_4)=4>2=b(k,D_4)$, wenn wir in Beispiel 4.23 die geschicktere Wahl getroffen haben. Bei der ungeschickten Wahl erhalten wir $d(G)=6$.

4.7 Untere Schranken

In diesem Abschnitt werden wir einige Methoden für untere Schranken unserer Zählfunktion herleiten. Ein wesentliches Problem bei unteren Schranken ist, dass wir hier nicht mehr die Einbettungshindernisse ignorieren dürfen. Glücklicherweise zeigt sich in unseren Beispielen, dass die Einbettungshindernisse nur den Exponenten beim log–Faktor beeinflussen.

Im Folgenden sei $G\leq S_n$ eine Permutationsgruppe und

$$1\to A\to G\to H\to 1 \tag{4.5}$$

eine exakte Sequenz von Gruppen. In diesem Abschnitt wird K/k stets eine Körpererweiterung mit Galoisgruppe H sein. Weiterhin sei $\mathrm{Gal}(L/k) = G \leq S_n$. Die normale Hülle von L/k bezeichnen wir mit N.

Eine erste untere Abschätzung für $Z(k, G; x)$ erhalten wir, wenn wir eine normale Körpererweiterung N/k mit Galoisgruppe G betrachten. In diesem Fall ist $K = N^A$ der Fixkörper unter A. Aufgrund dieser Konstruktion ist das zu K/k und (4.5) gehörige Einbettungsproblem lösbar. Wir wollen im Folgenden alle Lösungen dieses fest vorgegebenen Einbettungsproblems zählen, was natürlich eine untere Abschätzung für unser Problem gibt.

Als erstes betrachten wir zentrale Einbettungsprobleme mit Kern $A = Z_\ell$.

Satz 4.28
Es sei $G \leq S_n$ eine zentrale Erweiterung mit $A = Z_\ell$ wie in (4.5). *Falls eine Körpererweiterung L/k existiert mit* $\mathrm{Gal}(L/k) = G$, *so gilt:*

$$Z(k, G; x) \geq c(k, G) x^{\ell/(n(\ell-1))} \log(x)^{b(k, Z_\ell)} \text{ für } x \text{ groß genug.}$$

Beweis
Es sei N die normale Hülle von L/k und K der Fixkörper unter Z_ℓ. Wegen der bereits bekannten Lösung ist das zu (4.5) gehörige Einbettungsproblem lösbar. Nach Satz 4.9 haben wir eine Korrespondenz zwischen allen Lösungen und Z_ℓ–Erweiterungen M/k. Die Anzahl der Körper M, die dieselbe Erweiterung parametrisieren, ist durch eine von G abhängige Konstante nach oben beschränkt. Wir betrachten im Folgenden nur diejenigen M, deren Diskriminante koprim zu d_N ist. Wie bezeichnen mit L_M bzw. N_M eine durch M parametrisierte Lösung. Wegen der Koprimheit erhalten wir

$$\mathcal{N}(d_{N_M/k}) = \mathcal{N}(d_{N/k} d_{M/k}^{|G|/\ell}) \text{ bzw. } \mathcal{N}(d_{L_M/k}) = \mathcal{N}(d_{L/k} d_{M/k}^{n/\ell}).$$

Bei letzterer Gleichung haben wir ausgenutzt, dass zentrale Elemente $\neq 1$ in transitiven Gruppen keine Fixpunkte haben. Insbesondere haben alle Zykel dieselbe Länge. Es sei S die Menge der Primideale, welche $d_{N/k}$ teilen. Damit folgt für x groß genug:

$$\begin{aligned} Z(k, G; x) &\geq \tilde{c}(k, G) Z(k, Z_\ell, S; x^{\ell/n}/d_L) \\ &\geq c(k, G, S, Z_\ell) x^{\ell/(n(\ell-1))} \log(x^{\ell/n}/d_L)^{b(k, Z_\ell)}. \end{aligned}$$

Dabei folgt die letzte Ungleichung aus Satz 3.9. Da S und Z_ℓ in Abhängigkeit von G und L gewählt werden, folgt die Behauptung für $x >> 0$. □

Da ein zentrales Element der Ordnung ℓ in $G \leq S_n$ stets aus n/ℓ ℓ–Zykeln besteht, ist dessen Index gerade $n(\ell-1)/\ell$. Jetzt stellt sich die Frage, für

welche Gruppen $a(G) = \ell/(n(\ell-1))$ gilt, d.h., dass dieses Element gerade den Minimalindex hat. Wir sehen z.B. bei $G = D_4 \leq S_4$, dass der Minimalindex 1 ist, aber unser zentrales Element Index 2 hat.

Beispiel 4.29
Es sei $G = \mathrm{SL}_2(3) \leq S_8$. Es gilt $\mathrm{Z}(G) = Z_2$ und $a(G) = 1/4$. Hier erhalten wir durch Anwendung von Satz 4.28: $Z(k, \mathrm{SL}_2(3); x) \geq cx^{a(G)}$ für x groß genug und ein geeignetes $c > 0$.

Eine ganze Klasse von Gruppen stellen die ℓ–Gruppen G in regulärer Darstellung dar. Da der minimale Index einer Gruppe immer in einem Element von Primzahlordnung angenommen wird und alle nicht–trivialen Elemente fixpunktfrei operieren, gilt hier $a(G) = \ell/(|G|(\ell-1))$. Dieses Argument können wir auf eine beliebige nilpotente Gruppe in regulärer Darstellung erweitern, indem wir das Einbettungsproblem bezüglich einer zyklischen Gruppe kleinster Ordnung betrachten. Wir haben den folgenden Satz bewiesen (siehe auch [19, Theorem 6.3]):

Satz 4.30 (Klüners–Malle)
Es sei G eine nilpotente Gruppe in regulärer Darstellung. Dann existiert eine Konstante $c(k, G) > 0$, so dass für x groß genug gilt:

$$Z(k, G; x) \geq c(k, G)x^{a(G)}.$$

Beispiel 4.31
Es sei $G = Q_8 \leq S_8$ die Quaternionengruppe. Aus Beispiel 4.27 wissen wir $a(Q_8) = 1/4$ und $b(k, Q_8) = 0$. Mit obigem Satz erhalten wir:

$$Z(k, Q_8; x) \geq cx^{a(Q_8)} \text{ für } x >> 0.$$

Für ℓ–Gruppen in beliebiger Darstellung kann es nichtzentrale Elemente geben, die nicht fixpunktfrei operieren. Z.B. gilt für $G = D_4 \leq S_4$: $a(G) = 1$. Unser Satz liefert aber für diese Gruppe nur $Z(k, D_4; x) > cx^{1/2}$. Wir wissen aber nach [6] bzw. Satz 3.29, dass $Z(k, D_4; x) \sim c(k, D_4)x$ gilt.

Als weitere Anwendung betrachten wir direkte Produkte.

Beispiel 4.32
Es sei $G = Z_\ell \times H \leq S_n$ eine transitive Gruppe in natürlicher Darstellung und wir nehmen an, dass eine Körpererweiterung K/k mit $\mathrm{Gal}(K/k) = H$ existiert. Dann liefert uns Satz 4.28 eine untere Abschätzung der Form:

$$Z(k, G; x) \geq c_1(k, G)x^{\ell/(n(\ell-1))} \log(x)^{b(k, Z_\ell)} \text{ für } x >> 0.$$

Falls wir zusätzlich im 1. Fall von Satz 4.17 sind, so gilt für $x >> 0$:

$$c_1(k, G)x^{a(G)} \log(x)^{b(k,G)} \leq Z(k, G; x) \leq c_2 x^{a(G)} \log(x)^{b(k,G)}.$$

Kapitel 5

Ein Gegenbeispiel zur Asymptotik–Vermutung

Wir werden in diesem Kapitel zeigen, dass sich die Funktion $Z(\mathbb{Q}, Z_3 \wr Z_2; x)$ nicht so verhält, wie wir es nach Vermutung 2.12 erwarten. Wir betrachten im Folgenden die Gruppe $G = Z_3 \wr Z_2 \leq S_6$ und erhalten $a(G) = 1/2$ und $b(\mathbb{Q}, G) = 0$. Letzteres gilt deswegen, da es nur eine $\mathbb{Q}$–Konjugationsklasse vom Zykeltyp $1^3 3$ gibt, obwohl es zwei $\mathbb{Q}(\sqrt{-3})$–Konjugationsklassen dieses Zykeltyps gibt. Mit Vermutung 2.12 würden wir erhalten:

$$Z(\mathbb{Q}, G; x) \sim c(\mathbb{Q}, G) x^{1/2}.$$

Wie in Abschnitt 3.7 betrachten wir die verwandte Funktion

$$\tilde{Z}(\mathbb{Q}, Z_3 \wr Z_2; x) := |\{L/\mathbb{Q} \mid \exists K : \mathrm{Gal}(L/K) = Z_3, \mathrm{Gal}(K/\mathbb{Q}) = Z_2, d_L \leq x\}|.$$

Die auftretenden Galoisgruppen $\mathrm{Gal}(L/\mathbb{Q})$ sind gerade S_3, Z_6 und G, alle aufgefasst als transitive Untergruppe der S_6. Auch für diese Funktion würde nach Vermutung 2.12

$$\tilde{Z}(\mathbb{Q}, G; x) \sim \tilde{c}(\mathbb{Q}, G) x^{1/2}$$

folgen. Wenn wir im Folgenden nur die Körpererweiterungen betrachten, welche $K = \mathbb{Q}(\sqrt{-3})$ enthalten, so erhalten wir die folgende untere Abschätzung:

$$\tilde{Z}(\mathbb{Q}, Z_3 \wr Z_2; x) \geq Z(K, Z_3; x/d_K^3) \geq c(K, Z_3) x^{1/2} \log(x) \text{ für } x >> 0.$$

Hierbei haben wir die letzte Abschätzung nach Satz 3.1 erhalten. Hiermit ergibt sich bereits ein Widerspruch zur Vermutung 2.12. Wir zeigen nun, dass

sich der Widerspruch schon für G ergibt. Da Vermutung 2.12 für abelsche Gruppen bewiesen ist, erhalten wir:

$$Z(\mathbb{Q}, Z_6; x) \leq c(\mathbb{Q}, Z_6)x^{1/3}.$$

Für die symmetrische Gruppe $S_3(6) \leq S_6$ in regulärer Darstellung werden wir in Lemma 6.9 zeigen, dass wegen der Gültigkeit der Vermutung 6.6 für $\ell = 3$ gilt:

$$Z(\mathbb{Q}, S_3(6); x) \leq c(\mathbb{Q}, S_3(6))x^{1/3}.$$

Für unsere Zwecke wird aber eine einfacher zu erhaltende Abschätzung reichen, die wir im Folgenden zeigen. Sei $N/\mathbb{Q}$ ein normaler Körper mit Galoisgruppe S_3 und K ein Teilkörper vom Grad 3. Wegen $d_N \geq d_K^2$ und der bekannten linearen Asymptotik für S_3 [10] erhalten wir die triviale Abschätzung:

$$Z(\mathbb{Q}, S_3(6); x) \leq \tilde{c}(\mathbb{Q}, S_3(6))x^{1/2},$$

die ausreichend ist, um zu folgern:

Korollar 5.1
Für $G = Z_3 \wr Z_2$ gilt:

$$Z(\mathbb{Q}, G; x) \geq c(\mathbb{Q}, Z_3)x^{1/2}\log(x) = c(\mathbb{Q}, Z_3)x^{a(G)}\log(x)^{b(\mathbb{Q},G)+1} \text{ für } x >> 0.$$

Das Problem bei diesem Beispiel liegt darin, dass der kritische quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{-3})$ als Zwischenkörper angenommen wird. K ist der einzige quadratische Körper, für den $b(K, Z_3) = 1$ gilt. Für alle anderen Körper ist diese Konstante gerade 0. Wir werden im Folgenden die Gruppe $G = Z_3 \wr Z_2$ weiter untersuchen.

Dabei werden wir folgenden Satz benötigen [15, Corollary 4.3]:

Satz 5.2 (Helfgott und Venkatesh)
Es seien K ein quadratischer Zahlkörper und $\lambda > 0,44178$. Dann gilt für alle $\epsilon > 0$:

$$3^{\mathrm{rk}_3(\mathrm{Cl}_K)} \leq c(\epsilon)d_K^{\lambda+\epsilon}.$$

Dieser Satz ist eine Verschärfung von Satz 2.28, da wir im Allgemeinen $\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_K)}$ nur durch $|\mathrm{Cl}_K|$ also durch $d_k^{1/2+\epsilon}$ nach oben abschätzen können.

Lemma 5.3
Es seien K ein quadratischer Zahlkörper und $S \subseteq \mathbb{P}(K)$ eine endliche Teilmenge. Dann existieren höchstens $c(K)2^{|S|}$ Z_3–Erweiterungen von K, welche genau in S verzweigt sind. Hierbei ist $c(K) \leq c(\epsilon)d_K^{\lambda+\epsilon}$ mit λ wie in Satz 5.2 für alle $\epsilon > 0$.

Beweis
Dies folgt direkt aus Lemma 4.15, wobei wir die verbesserte Abschätzung aus Satz 5.2 benutzen. □

Mit Hilfe dieses Lemmas erhalten wir folgendes Korollar.

Korollar 5.4
Für einen quadratischen Zahlkörper K gilt:

$$Z(K, Z_3; x) \leq c(K, Z_3) x^{1/2} \log(x) \text{ mit } c(K, Z_3) \leq c(\epsilon) d_K^{\lambda+\epsilon} \text{ für alle } \epsilon > 0.$$

Beweis
Wir ordnen jeder Z_3–Erweiterung L/K die Menge S seiner verzweigten Primideale zu. Sei a_n die Anzahl dieser Erweiterungen mit $\mathcal{N}(d_{L/K}) = n$. Wir betrachten nun mit $c(K)$ aus obigem Lemma die Dirichletreihe

$$\Phi(s) = c(K) \prod_{\mathfrak{p} \in \mathbb{P}(K)} (1 + 2/\mathcal{N}(\mathfrak{p})^{2s}) = \sum_{n \in \mathbb{N}} \frac{b_n}{n^s}.$$

Da für jedes in L verzweigte Primideal $\mathfrak{p}^2 \mid d_{L/K}$ gilt, erhalten wir nach obiger Rechnung: $a_n \leq b_n$ sowie $b_n \geq 0$ für alle $n \in \mathbb{N}$. Da es sich bei $\Phi(s)$ im wesentlichen (vgl. Lemma 2.20) um die erzeugende Funktion der Teilerfunktion t_K handelt, erhalten wir mit Lemma 2.22, dass

$$\sum_{n=1}^{x} a_n \leq \sum_{n=1}^{x} b_n \leq c(K, \epsilon) x^{1/2} \log(x)$$

für alle $\epsilon > 0$ gilt. □

Wie wir bereits wissen, ist diese Abschätzung für $K = \mathbb{Q}(\sqrt{-3})$ scharf in dem Sinne, dass der Log–Faktor tatsächlich in der Asymptotik auftritt. Für alle anderen K würden wir erwarten, dass kein Log–Faktor auftritt. Dies können wir dadurch beweisen, dass wir in dem Eulerprodukt nur Primideale berücksichtigen, deren Norm kongruent 1 modulo 3 sind. Andere Primideale können in Z_3–Erweiterungen nicht verzweigt sein. Für $K \neq \mathbb{Q}(\sqrt{-3})$ stellt sich heraus, dass diese Primideale gerade Dichte $1/2$ haben. Wenn wir dies in unserer Abschätzung berücksichtigen, so erhalten wir die entsprechende Abschätzung ohne Log–Faktor. Da wir dies aber im Folgenden nicht benötigen, verzichten wir hier auf die Details. Wir können nun den folgenden Satz beweisen:

Satz 5.5
Für $G = Z_3 \wr Z_2$ existieren Konstanten $c_1(\mathbb{Q}, G), c_2(\mathbb{Q}, G) > 0$ mit

$$c_1(\mathbb{Q}, G) x^{1/2} \log(x) \leq Z(\mathbb{Q}, G; x) \leq c_2(\mathbb{Q}, G) x^{1/2} \log(x) \text{ für } x >> 0.$$

Beweis
Die untere Abschätzung ist gerade Korollar 5.1. Für die obere Abschätzung gilt für einen Körperturm $L/K/\mathbb{Q}$ mit $\mathrm{Gal}(L/K) = Z_3$ sowie $[K:\mathbb{Q}] = 2$:

$$d_L = d_K^3 \mathcal{N}(d_{L/K}).$$

Mit $\mathcal{K}(x) := \{K/\mathbb{Q} \mid [K:\mathbb{Q}] = 2, d_K^3 \leq x\}$ erhalten wir:

$$Z(\mathbb{Q}, G; x) \leq \sum_{K \in \mathcal{K}(x)} Z(K, Z_3; x/d_K^3)$$

$$\leq \sum_{K \in \mathcal{K}(x)} c(K, Z_3)(x/d_K^3)^{1/2} \log(x/d_K^3) \quad \text{(Korollar 5.4)}$$

$$\leq \sum_{K \in \mathcal{K}(x)} c(\epsilon) \frac{d_K^{\lambda+\epsilon}}{d_K^{3/2}} x^{1/2} \log(x) = c(\epsilon) x^{1/2} \log(x) \sum_{K \in \mathcal{K}(x)} \frac{1}{d_K^{3/2-\lambda-\epsilon}}.$$

Da $3/2 - \lambda - \epsilon > 1$ für ϵ klein genug, konvergiert letztere Summe. Insgesamt erhalten wir die gewünschte obere Abschätzung. □

Wir merken an, dass es notwendig war, $3^{\mathrm{rk}_3(\mathrm{Cl}_K)}$ durch $O(d_K^{1/2-\epsilon})$ abzuschätzen. Ansonsten hätten wir die letzte Abschätzung im Beweis so nicht führen können.

Eine andere interessante Anmerkung ergibt sich, wenn wir die Funktion $Z(\mathbb{Q}, G, S; x)$ für $S = \{(3)\}$ betrachten. Damit schließen wir $K = \mathbb{Q}(\sqrt{-3})$ als Zwischenkörper aus. Wenn wir die Rechnung in Korollar 5.4 für $K \neq \mathbb{Q}(\sqrt{-3})$ ohne den Log–Faktor in der oberen Abschätzung gezeigt hätten, so würde jetzt für $x >> 0$ folgen:

$$c_1(\mathbb{Q}, G, S) x^{1/2} \leq Z(\mathbb{Q}, G, S; x) \leq c_2(\mathbb{Q}, G, S) x^{1/2},$$

wobei $c_1(\mathbb{Q}, G, S), c_2(\mathbb{Q}, G, S) > 0$ geeignete Konstanten sind. Damit verhalten sich die Asymptotiken von $Z(\mathbb{Q}, G; x)$ und $Z(\mathbb{Q}, G, S; x)$ unterschiedlich. Für die Zählfunktion $Z^S(\mathbb{Q}, G; x)$ erhalten wir allerdings mit Lemma 3.15 für $x >> 0$:

$$\tilde{c}_1(\mathbb{Q}, G, S) x^{1/2} \log(x) \leq Z^S(\mathbb{Q}, G; x) \leq \tilde{c}_2(\mathbb{Q}, G, S) x^{1/2} \log(x).$$

Nun stellt sich die Frage, ob wir eine neue Vermutung für den Exponenten des Log–Faktors in Vermutung 2.12 formulieren können. Naheliegend wäre es zu vermuten, den maximalen abelschen Quotienten von G zu berücksichtigen. Im Falle $G = Z_3 \wr Z_2$ wäre dies gerade die zyklische Gruppe Z_6. Für die Elemente der Ordnung 3 vom Index 2 spielt der Körper $K = \mathbb{Q}(\sqrt{-3})$ eine entscheidende Rolle. Wenn dieser Körper als Zwischenkörper auftauchen

kann, so hat dies in diesem Beispiel die gleiche Auswirkung, als wenn wir diesen Körper als Grundkörper wählen. Heuristisch ist klar, dass

$$c_1(K,G)x^{1/2}\log(x) \leq Z(K,G;x) \leq c_2(K,G)x^{1/2}\log(x) \text{ für } x >> 0$$

gilt. Dabei können wir den analogen Beweis wie im Fall über $\mathbb{Q}$ führen. Bei der oberen Schranke fehlt uns allerdings das Analogon zu Satz 5.2.

Leider ist das Betrachten des maximalen abelschen Quotienten von G nicht ausreichend, wie wir an der Gruppe $G = Z_2 \times (Z_3 \wr Z_3) \leq S_{18}$ sehen. Wegen $a(Z_2) = 1$ und $a(Z_3 \wr Z_3) = 1/2$ erhalten wir $a(G) = 1/4$. Weiterhin gilt $b(\mathbb{Q},G) = 0$ und $b(\mathbb{Q}(\sqrt{-3}),G) = 1$, da diesmal Elemente vom Zykeltyp $3^2 1^{12}$ den Minimalindex annehmen. Heuristisch vermuten wir nun folgende Ergebnisse:

$$Z(\mathbb{Q}, Z_3 \wr Z_3; x) \leq c(\mathbb{Q}, Z_3 \wr Z_3)x^{1/2} \text{ sowie } Z(\mathbb{Q},G;x) \leq c(\mathbb{Q},G)x^{1/4}.$$

Die erste Abschätzung könnten wir zeigen, wenn wir eine Konstantenabschätzung wie in Korollar 5.4 ohne die Log–Faktoren gezeigt hätten (vgl. Anmerkungen vor Satz 3.23. Hierbei reicht es sogar aus, die Klassenzahl von kubischen Körpern K mit $d_K^{1/2+\epsilon}$ abzuschätzen). Für die zweite Abschätzung können wir momentan keinen Beweis angeben. Wir sind im zweiten Fall von Satz 4.17. Auch wenn wir in der Voraussetzung das ϵ „einsparen“, können wir mit dieser Beweismethode das gewünschte Ergebnis nicht erzielen. Da die kritischen Stellen der beteiligten Funktionen an verschiedenen Punkten liegen, zeigt die heuristische Erfahrung, dass das vermutete Ergebnis stimmen sollte.

Kapitel 6

Diedergruppen und die Cohen–Lenstra–Heuristik

In diesem Kapitel werden wir untere Schranken für die Zählfunktion von Diedergruppen D_ℓ bestimmen. Diedergruppen D_ℓ mit $\ell > 2$ prim sind die einfachsten (auflösbaren) Gruppen, welche kein Zentrum besitzen. Daher sind mehrere Methoden aus Kapitel 4 nicht anwendbar. Wir werden feststellen, dass wir gute obere Schranken nur dann bekommen können, wenn wir genauere Informationen über die Verteilung von Klassengruppen quadratischer Zahlkörper kennen. Diese Verteilung wird in der sogenannten Cohen–Lenstra–Heuristik [8] vermutet. Wir werden in Satz 6.9 unter der Annahme einer schwachen Form der Cohen–Lenstra–Heuristik eine gute obere Schranke für Diedergruppen D_ℓ über $\mathbb{Q}$ beweisen. Umgekehrt werden wir zeigen, dass die Cohen–Lenstra–Heuristik falsch ist, falls unsere gewünschte obere Schranke für Diedergruppen nicht gilt (siehe Abschnitt nach Vermutung 6.6). Für $\ell = 3$ wird in [10] genau die Form der Cohen–Lenstra–Heuristik bewiesen, welche wir für unsere Abschätzungen brauchen. Dies führte auch zum Beweis der Asymptotik für S_3–Erweiterungen. In [9] werden diese Ergebnisse auf beliebige Grundkörper k verallgemeinert.

Eine gute untere Abschätzung für die Zählfunktion von Diedergruppen D_ℓ beweisen wir in Satz 6.4.

6.1 Untere Schranken für Diedergruppen

In diesem Abschnitt wollen wir untere Schranken für Diedergruppen $G = D_\ell < S_\ell$ der Ordnung 2ℓ beweisen, wobei $\ell > 2$ eine Primzahl ist. Eine solche

Diedergruppe ist ein semidirektes Produkt:

$$1 \to Z_\ell \to D_\ell \to Z_2 \to 1.$$

Der Index von G wird in Elementen der Ordnung 2 angenommen, welche genau einen Fixpunkt besitzen, d.h. $\mathrm{ind}(G) = \ell - 1 - (\ell-1)/2 = (\ell-1)/2$. Wenn wir die Methode aus Abschnitt 4.7 anwenden, d.h. einen Körper M/k mit Galoisgruppe Z_2 fixieren, erhalten wir nur $Z(k, D_\ell; x) > cx^{1/(\ell-1)}$ für x groß genug. Im Gegensatz zu diesen Fall ist hier die Faktorgruppe Z_2 für das asymptotische Wachstum „verantwortlich“. Daher muss eine erfolgreiche Methode verschiedene Körper M/k mit Galoisgruppe Z_2 berücksichtigen. Im Folgenden bezeichnet $D_\ell(2\ell) \leq S_{2\ell}$ die Diedergruppe D_ℓ in ihrer regulären Darstellung.

Lemma 6.1
Es seien $\ell > 2$ prim und $N/M/k$ Erweiterungen von Zahlkörpern mit $\mathrm{Gal}(M/k) = Z_2$ sowie $\mathrm{Gal}(N/M) = Z_\ell$. Dann gilt genau eine der folgenden Aussagen:

(1) $\mathrm{Gal}(N/k) = Z_2 \times Z_\ell$. *In diesem Fall existiert ein Zwischenkörper $k \subseteq M \subseteq N$ mit $\mathrm{Gal}(M/k) = Z_\ell$.*

(2) $\mathrm{Gal}(N/k) = D_\ell(2\ell) \leq S_{2\ell}$.

(3) $\mathrm{Gal}(N/k) = Z_\ell \wr Z_2 \cong Z_\ell^2 \rtimes Z_2$. *In diesem Fall besitzt die normale Hülle von N/k einen Zwischenkörper L mit $\mathrm{Gal}(L/k) = D_\ell$.*

Beweis
Nach dem Lemma von Krasner und Kaloujnine [20] ist $\mathrm{Gal}(N/k) \leq Z_\ell \wr Z_2 \leq S_{2\ell}$ transitiv. Die einzigen in Frage kommenden Untergruppen sind $Z_\ell \wr Z_2, D_\ell$ und $Z_\ell \times Z_2$. Da Z_ℓ und D_ℓ noch zusätzlich Quotienten von $Z_\ell \wr Z_2$ sind, folgen die weiteren Aussagen. □

Es sei nun eine Erweiterung M/k mit $\mathrm{Gal}(M/k) = Z_2$ gegeben. Dann finden wir nach obigem Lemma eine D_ℓ–Erweiterung $N/M/k$, falls $\mathrm{Gal}(N/M) = Z_\ell$ gilt und wir vermeiden das direkte Produkt zu bekommen.

Lemma 6.2
Es seien $\ell > 2$, $\mathrm{Gal}(M/k) = Z_2$ und $\mathrm{Gal}(N/M) = Z_\ell$. Weiterhin existiere ein $\mathfrak{p} \in \mathbb{P}(k)$ mit folgenden Eigenschaften:

(1) $\mathcal{N}(\mathfrak{p}) \equiv 1 \bmod \ell$,

(2) $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1\mathfrak{P}_2$ *für Primideale $\mathfrak{P}_1, \mathfrak{P}_2$ von $\mathcal{O}_M$,*

(3) $\mathfrak{P}_1$ *ist verzweigt und* $\mathfrak{P}_2$ *ist unverzweigt in* N/M.

Dann gilt $\mathrm{Gal}(N/k) \cong Z_\ell \wr Z_2$. *Daher existiert ein* L/k *vom Grad* ℓ *mit* $\mathrm{Gal}(L/k) = D_\ell$ *dessen normale Hülle* M *enthält, und der in der normalen Hülle von* N/k *enthalten ist.*

Beweis
Wir müssen nach Lemma 6.1 nur zeigen, dass N/k nicht normal ist. Dies ist aber der Fall, da über $\mathfrak{p}$ sowohl verzweigte als auch unverzweigte Primideale liegen. □

Im nächsten Schritt müssen wir zeigen, dass unter geeigneten Voraussetzungen Körpererweiterungen existieren, die diese Voraussetzungen erfüllen.

Satz 6.3
Es seien k *ein Zahlkörper,* $\ell \in \mathbb{P}$ *und* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \mathbb{P}(k)$ *Primideale mit* $\mathcal{N}(\mathfrak{p}_i) \equiv 1 \bmod \ell$. *Weiterhin sei* $s > r + \mathrm{rk}_\ell + 1$, *wobei* r *den Einheitenrang von* $\mathcal{O}_k$ *und* rk_ℓ *den* ℓ*–Rang der Klassengruppe von* k *bezeichnen. Dann existiert eine* Z_ℓ*–Erweiterung von* k, *welche außerhalb von* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *unverzweigt und in wenigstens einem dieser Primideale verzweigt ist.*

Beweis
Wir definieren das Ideal $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ und betrachten die Strahlklassengruppe A von $\mathfrak{a}$. Nach [22, S. 126-127] gilt:

$$A/\mathrm{Cl}(k) \cong (\mathcal{O}_k/\mathfrak{a})^\times/(U_k \cap k_\mathfrak{a}),$$

wobei U_k die Einheitengruppe von $\mathcal{O}_k$ und $k_\mathfrak{a}$ die Elemente von $k^\times$ kongruent $1 \bmod \mathfrak{a}$ bezeichnet. Da der ℓ–Rang von U_k/U_k^ℓ höchstens $r+1$ (Torsionseinheiten!) ist, ist $Z_\ell^{\mathrm{rk}_\ell+1}$ eine Faktorgruppe von $A/\mathrm{Cl}(k)$. Damit existiert eine in wenigstens einem dieser Primideale verzweigte Z_ℓ–Erweiterung von k mit den gewünschten Eigenschaften. □

Nun können wir eine untere Schranke für Dieder–Erweiterungen beweisen.

Satz 6.4
Es seien D_ℓ *und* $D_\ell(2\ell)$ *die Diedergruppe mit* 2ℓ *Elementen auf* ℓ *bzw.* 2ℓ *Punkten und* k *ein Zahlkörper. Dann existieren Konstanten* $c(k, D_\ell) > 0$ *sowie* $c(k, D_\ell(2\ell)) > 0$, *so dass für* $x >> 0$ *folgendes gilt:*

$$Z(k, D_\ell; x) > c(k, D_\ell) x^{a(D_\ell)} \text{ und } Z(k, D_\ell(2\ell); x) > c(k, D_\ell(2\ell)) x^{a(D_\ell(2\ell))}.$$

Beweis
Es sei r der größtmögliche Einheitenrang einer quadratischen Erweiterung

M/k und $s > r + \mathrm{rk}_\ell(\mathrm{Cl}_k) + 1$. Nun sei $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \subseteq \mathbb{P}(k)$ eine Menge mit der Eigenschaft, dass die Norm aller Primideale kongruent 1 modulo ℓ ist (existiert nach Dirichlet). Wir betrachten nun einen beliebigen quadratischen Zahlkörper M/k, der in allen Primidealen von S total zerlegt ist. Falls $\mathrm{rk}_\ell(\mathrm{Cl}_M) > \mathrm{rk}_\ell(\mathrm{Cl}_k)$ gilt, so hat dies sofort zur Folge, dass eine nicht triviale Idealklasse existiert, welche nicht invariant unter $\mathrm{Gal}(M/k)$ ist. Nach Satz 6.5 erhalten wir also eine unverzweigte Erweiterung N/M mit $\mathrm{Gal}(N/k) = D_\ell(2\ell)$. Ansonsten gilt nach Satz 6.3, dass eine Erweiterung $N/M/k$ mit Galoisgruppe $D_\ell(2\ell)$ existiert, so dass N/M höchstens in Primidealen verzweigt ist, die über denen aus S liegen. In beiden Fällen ergibt sich $\mathcal{N}(d^S_{N/k}) = \mathcal{N}(d^S_{M/k})^\ell$. Wir erinnern noch einmal an die Definition im Abschnitt 3.4, dass das S im Exponenten heißt, dass der koprime Anteil genommen wird. Da Involutionen in der natürlichen Darstellung von D_ℓ genau einen Fixpunkt haben, gilt für den Teilkörper $L \leq N$ mit $\mathrm{Gal}(L/k) = D_\ell$:

$$\mathcal{N}(d^S_{L/k}) = \mathcal{N}(d^S_{M/k})^{(\ell-1)/2}.$$

Wir bezeichnen nun mit $Y^S(k, Z_2; x)$ die Anzahl der Z_2–Erweiterungen von k, die in den Primidealen aus S total zerlegt sind. Für jeden dieser Körper erhalten wir nach obiger Überlegung eine Dieder–Erweiterung mit beschränkter Diskriminante. Wir erhalten also:

$$Z^S(k, D_\ell; x) \geq \tilde{c}(k, D_\ell, S) Y^S(k, Z_2; x^{2/(\ell-1)}) \geq \tilde{c}(k, G) x^{2/(\ell-1)}.$$

Letztere Abschätzung gilt nach Satz 3.25. Die Abhängigkeit der Konstante von S ist nicht nötig, da S in Abhängigkeit von k gewählt wurde. Die Behauptung $Z(k, D_\ell; x) > \tilde{c}(k, G) x^{2/(\ell-1)}$ folgt nun mit Lemma 3.15 (1). Für $D_\ell(2\ell)$ erhalten wir den Beweis analog. □

6.2 Obere Schranken für Diedergruppen der Ordnung 2ℓ

Wir nehmen dieselbe Notation wie in Beispiel 2.6: Sei also im Folgenden N/k eine normale Erweiterung mit Galoisgruppe $D_\ell(2\ell)$. Dann bezeichnen wir mit K bzw. M Zwischenkörper vom Grad ℓ bzw. 2 über k. Wir erhalten aus obigem Beispiel die Diskriminantenrelation

$$\mathcal{N}(d_{K/k}) = \mathcal{N}(d_{M/k})^d \mathcal{N}(d_{N/M})^{1/2} \text{ für } d = \frac{\ell - 1}{2}.$$

Dabei treten in $\mathcal{N}(d_{N/M})$ alle Primteiler quadratisch auf, so dass das Wurzelziehen wohldefiniert ist. Für den folgenden wohlbekannten Satz habe ich leider kein gutes Zitat gefunden.

Satz 6.5
Es seien $\ell > 2$ eine Primzahl und M/k eine Erweiterung von Zahlkörpern mit $\mathrm{Gal}(M/k) = \langle\sigma\rangle \cong Z_2$. Wir bezeichnen mit $A_\ell := \mathrm{Cl}_M \,/\, \mathrm{Cl}_M^\ell$ den $\mathbb{F}_\ell[Z_2]$–Modul, wobei σ in natürlicher Weise auf den Idealen operiert. Dann gelten:

(1) Mit $A_\ell^+ := \{a \in A_\ell \mid \sigma(a) = a\}$ und $A_\ell^- := \{a \in A_\ell \mid \sigma(a) = a^{-1}\}$ erhalten wir:
$$A_\ell = A_\ell^+ \oplus A_\ell^- .$$

(2) Die unverzweigten Körper N/M mit $\mathrm{Gal}(N/k) = D_\ell(2\ell)$ stehen in Bijektion zu den Untermoduln vom Index ℓ in A_ℓ^-.

(3) Im Fall $k = \mathbb{Q}$ ist A_ℓ^+ trivial, d.h. $A_\ell = A_\ell^-$.

Beweis
Das Element σ der Ordnung 2 kann nur Eigenwerte ± 1 haben. Die Aufteilung als direkte Summe folgt dann, weil $\mathrm{ggT}(\ell, 2) = 1$. Mit [18, Section 6] folgt, dass wir die Diedergruppe als Galoisgruppe von N/M erhalten, wenn der entsprechende Unterraum zum Eigenwert -1 korrespondiert. Damit haben wir (1) und (2) gezeigt. Falls es in (3) ein nichttriviales Ideal in A_ℓ^+ geben würde, so hätte die zugeordnete unverzweigte Erweiterung N/M die Eigenschaft, dass $\mathrm{Gal}(N/\mathbb{Q}) = Z_2 \times Z_\ell$ gilt. Alle nichttrivialen Trägheitsgruppenerzeuger haben Ordnung 2, was zur Folge hat, dass es eine unverzweigte Z_ℓ–Erweiterung von $\mathbb{Q}$ geben müsste, was zu einem Widerspruch führt. □

Im Folgenden wollen wir $k = \mathbb{Q}$ annehmen. Sei also $M/\mathbb{Q}$ eine quadratische Erweiterung, wobei wir zusätzlich annehmen wollen, dass ℓ die Klassenzahl h_M von M teilt. Nach [32, 34] existieren unendlich viele solche Erweiterungen. Nach Klassenkörpertheorie existiert also eine unverzweigte Z_ℓ–Erweiterung N/M. Nach Satz 6.5 korrespondieren diese unverzweigten Z_ℓ–Erweiterungen zu den Untergruppen vom Index ℓ in Cl_M. Wir erhalten also $(\ell^{\mathrm{rk}_\ell} - 1)/(\ell - 1)$ verschiedene solche Erweiterungen, wobei wir mit $\mathrm{rk}_\ell(\mathrm{Cl}_M)$ den ℓ–Rang der Klassengruppe bezeichnen.

Die folgende Formulierung ist ein Spezialfall der Cohen–Lenstra–Vermutung, siehe [8, Seite 57], welcher für $\ell = 3$ bewiesen ist [10].

Vermutung 6.6
(Cohen–Lenstra) Sei ℓ eine ungerade Primzahl. Dann ist der Durchschnitt von $\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_M)} - 1$ über alle imaginärquadratischen Körper m gleich 1, d.h.

$$\frac{\sum_{d_M \le x} \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_M)} - 1}{\sum_{d_M \le x} 1} \longrightarrow 1 \text{ für } x \longrightarrow \infty,$$

wobei wir über alle imaginärquadratischen Körper M mit $d_M \leq x$ summieren. Analog ist derselbe Durchschnitt über alle reellquadratischen Körper gerade ℓ^{-1}.

Da $Z(\mathbb{Q}, Z_2; x)$ linear wächst, erhalten wir direkt aus dieser Vermutung:

$$\sum_{d_M \leq x} \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_M)} - 1 \sim c(\mathbb{Q}, \ell, Z_2)x \text{ für } x \to \infty.$$

Die Klassengruppe eines Körpers M vom ℓ–Rang r hat genau $(\ell^r - 1)/(\ell - 1)$ zyklische Untergruppen der Ordnung ℓ. Damit erhalten wir nach unserer Vorüberlegung genauso viele Diedererweiterungen $N/\mathbb{Q}$, die unverzweigt über M sind. Wir erhalten also folgende untere Abschätzung:

$$Z(\mathbb{Q}, D_\ell; x) \geq \sum_{d_M \leq x^{1/d}} \frac{\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_M)} - 1}{\ell - 1} \sim \frac{c(\ell)}{\ell - 1} x^{1/d},$$

wobei die letzte Asymptotik aus obiger Vermutung folgt. Sollte

$$\sum_{d_M \leq x} \ell^{\mathrm{rk}_\ell(\mathrm{Cl}_M)} - 1$$

größer als $O(x)$ sein, so würde dies direkt zu einem Widerspruch zur Asymptotik–Vermutung für Diedergruppen D_ℓ führen, da $a(D_\ell) = 1/d$ gilt.

Wir wollen nun obere Abschätzungen für diese Diedergruppen beweisen. Seien hierzu N/k eine normale $D_\ell(2\ell)$–Erweiterung und M bzw. K die Zwischenkörper vom Grad 2 bzw. ℓ über k.

Wie bei den nilpotenten Gruppen (siehe Satz 4.20) können wir N/k ein Paar $(\mathfrak{a}_1, \mathfrak{a}_2)$ zuordnen, wobei die quadratfreien Ideale $\mathfrak{a}_i \subset \mathcal{O}_k$ dadurch definiert sind, dass $\mathfrak{a}_1$ gerade die Primteiler von $d_{M/k}$ enthält und $\mathfrak{a}_2$ die Primideale enthält, welche in N/k verzweigt, aber in M/k unverzweigt sind. Damit erhalten wir folgende Aussage:

Lemma 6.7

(1) $\mathcal{N}(d_{N/k}) \geq \mathcal{N}(\mathfrak{a}_1)^\ell \mathcal{N}(\mathfrak{a}_2)^{2\ell-2}$.

(2) $\mathcal{N}(d_{K/k}) \geq \mathcal{N}(\mathfrak{a}_1)^d \mathcal{N}(\mathfrak{a}_2)^{\ell-1}$.

Wir merken an, dass im obigen Lemma genau dann Ungleichheit entsteht, wenn wilde Verzweigung auftritt. Durch diese Prozedur ordnen wir jeder Diedererweiterung ein Paar $(\mathfrak{a}_1, \mathfrak{a}_2)$ von quadratfreien und koprimen Idealen zu. Wir müssen nun abschätzen, wieviele Körper demselben Tupel zugeordnet

werden (vgl. Satz 4.24). Dabei korrespondiert das Ideal $\mathfrak{a}_1$ zu den quadratischen Erweiterungen und das Ideal $\mathfrak{a}_2$ zu den relativ–zyklischen Erweiterungen. Leider ist die Anzahl der relativ–zyklischen Erweiterungen sehr stark von der Klassengruppe des quadratischen Körpers M abhängig.

Lemma 6.8
Es existiert eine Konstante $c(K) > 0$ mit: Es seien M/k eine quadratische Erweiterung mit $\mathrm{rk}_\ell(\mathrm{Cl}_M) = r$ und $\mathfrak{a}$ ein Ideal von $\mathcal{O}_k$. Dann existieren höchstens

$$\frac{\ell^{r+\omega(\mathfrak{a})+c(k)} - 1}{\ell - 1}$$

Z_ℓ–Erweiterungen N/M mit $\mathrm{Gal}(N/k) = D_\ell(2\ell)$, welche nur in Primidealen verzweigt sind, welche über Primteilern von $\mathfrak{a}$ liegen. Zusätzlich ist jedes solche N im Strahlklassenkörper von $\mathfrak{a}\mathfrak{b}\mathcal{O}_M$ enthalten, wobei $\mathfrak{b} \subseteq \mathcal{O}_k$ ein Ideal ist, welches nur von Primidealen über ℓ geteilt wird.

Beweis
Es ist klar, dass jedes solche N im behaupteten Strahlklassenkörper enthalten ist. Wir benutzen die Aussagen aus [18, Sections 5 and 6] und erhalten, dass $\tilde{\mathfrak{a}} := \mathfrak{a}\mathcal{O}_M$ invariant unter σ ist, wobei $\mathrm{Gal}(M/k) = \langle\sigma\rangle$ gilt. Wir betrachten die Strahlklassengruppe $\mathrm{Cl}_{\tilde{\mathfrak{a}}}$ modulo ℓ–ten Potenzen als Z_2–Modul A. In [18, Sections 5 and 6] wird gezeigt, dass D_ℓ–Erweiterungen zu eindimensionalen (invarianten) Unterräumen von A mit Eigenwert -1 korrespondieren. Es sei $\mathfrak{p} \in \mathbb{P}(k)$ ein Primideal, welches nicht über ℓ liegt. Wir unterscheiden zwei Fälle und zeigen jeweils, dass der Beitrag zum Rang höchstens 1 ist. Falls $\mathfrak{p}$ zerlegt in M ist, so hat der Restklassenring $(\mathcal{O}_M/(\mathfrak{p}\mathcal{O}_M))^*$ ℓ–Rang 0 oder 2, wobei letzteres eintritt, wenn $\ell \mid (\mathcal{N}(\mathfrak{p}) - 1)$ gilt. In jedem Fall vertauscht σ die beiden Primideale in $\mathcal{O}_M$, welche über $\mathfrak{p}$ liegen. Daher besitzt unser zweidimensionaler Modul einen Eigenraum der Dimension 1 zum Eigenwert 1. Damit erhöht $\mathfrak{p}$ die Dimension des Eigenraums zum Eigenwert -1 um maximal 1. Im Fall, dass $\mathfrak{p}$ träge ist, ist der ℓ–Rang von $(\mathcal{O}_M/(\mathfrak{p}\mathcal{O}_M))^*$ höchstens 1. Analog zum Beweis von Satz 2.26 sammeln wir den Beitrag der Primideale von $\mathcal{O}_k$, die über ℓ liegen, in der Konstante $c(k)$. □

Wir beweisen nun für $k = \mathbb{Q}$ eine obere Abschätzung.

Satz 6.9
Unter der Annahme von Vermutung 6.6 gelten für alle ungeraden $\ell \in \mathbb{P}$:

$$Z(\mathbb{Q}, D_\ell; x) \leq c(\mathbb{Q}, \ell)x^{1/d} = c(\mathbb{Q}, \ell)x^{a(D_\ell)} \text{ mit } d = \frac{\ell - 1}{2},$$

$$Z(\mathbb{Q}, D_\ell(2\ell); x) \leq \tilde{c}(\mathbb{Q}, \ell)x^{1/\ell} = \tilde{c}(\mathbb{Q}, \ell)x^{a(D_\ell(2\ell))}.$$

Beweis
Wir betrachten reell- und imaginärquadratische Körper getrennt und parametrisieren diese durch quadratfreie $a \in \mathbb{Z}$. Mit $T = \{2, \ell\}$ sowie $\mathrm{rk}(a) := \mathrm{rk}_\ell(\mathrm{Cl}_{\mathbb{Q}(\sqrt{a})})$ erhalten wir im reellen Fall:

$$Z(\mathbb{Q}, D_\ell; x) \leq Z^T(\mathbb{Q}, D_\ell; x) \leq \sum_{a^d b^{\ell-1} \leq x} \frac{\ell^{\mathrm{rk}(a)+\omega(b)+c(\mathbb{Q})} - 1}{\ell - 1} \text{ (Lemma 6.8)}$$

$$\leq c(\mathbb{Q}) \sum_{a^d b^{\ell-1} \leq x} \ell^{\mathrm{rk}(a)} \ell^{\omega(b)} = c(\mathbb{Q}) \sum_{b^{\ell-1} \leq x} \ell^{\omega(b)} \sum_{a \leq \frac{x^{1/d}}{b^{(\ell-1)/d}}} \ell^{\mathrm{rk}(a)}$$

$$\leq \sum_{b^{\ell-1} \leq x} \frac{\ell^{\omega(b)} \hat{c}(\mathbb{Q}, \ell) x^{1/d}}{b^{(\ell-1)/d}}$$

$$= \hat{c}(\mathbb{Q}, \ell) x^{1/d} \sum_{b^{\ell-1} \leq x} \frac{\ell^{\omega(b)}}{b^{(\ell-1)/d}} \leq c(\mathbb{Q}, \ell) x^{1/d},$$

da die letzte Summe wegen $\ell - 1 > d = (\ell - 1)/2$ und Vermutung 6.6 konvergiert. Der zweite Teil des Satzes folgt analog, wobei d durch ℓ und $\ell - 1$ durch $2(\ell - 1)$ ersetzt wird. □

Die Vermutung 6.6 ist für $\ell = 3$ bewiesen [10]. Daher liefert Satz 6.9 für $\ell = 3$:

Bemerkung 6.10
Es gelten:

$$Z(\mathbb{Q}, S_3; x) \leq c(\mathbb{Q}, S_3)x \text{ und } Z(\mathbb{Q}, S_3(6); x) \leq c(\mathbb{Q}, S_3(6))x^{1/3}.$$

Diese Methoden funktionieren auch für beliebige Grundkörper k. Hier muss die Voraussetzung der Vermutung 6.6 entsprechend angepasst werden. In dem Beweis ist jetzt nicht mehr der ℓ–Rang von $\mathrm{Cl}_{k(\sqrt{a})}$ interessant. Wir müssen nach Satz 6.5 nun die Elemente in $\mathrm{Cl}_{k(\sqrt{a})}$ zählen, deren zugehörige Idealklassen nicht invariant unter der Galoisgruppe von $k(\sqrt{a})/k$ sind. Für $\ell = 3$ wird genau dies in [9] betrachtet. Daher erhalten wir:

Lemma 6.11
Für alle Zahlkörper k gilt:

$$Z(k, S_3; x) \leq c(k, S_3)x \text{ und } Z(k, S_3(6); x) \leq c(k, S_3(6))x^{1/3}.$$

Wir merken an, dass $Z(k, S_3; x) \sim c(K, S_3)x$ bereits in [9] bewiesen wird.
Im Folgenden beweisen wir eine obere Schranke für die Asymptotik von Diedergruppen, welche unabhängig von Vermutungen ist. Hierzu schätzen wir mit Satz 2.28 $\ell^{\mathrm{rk}(a)} \leq |\operatorname{Cl}_{\mathbb{Q}(\sqrt{a})}| = O(a^{1/2+\epsilon})$ ab und erhalten:

Satz 6.12
Für ungerade Primzahlen ℓ und alle $\epsilon > 0$ gilt:

$$Z(\mathbb{Q}, D_\ell; x) \leq c(\ell, \epsilon)x^{3a(D_\ell)/2+\epsilon} \text{ bzw. } Z(\mathbb{Q}, D_\ell(2\ell); x) \leq \tilde{c}(\ell, \epsilon)x^{3a(D_\ell(2\ell))/2+\epsilon}.$$

Beweis
Analog zum Beweis von Satz 6.9 erhalten wir:

$$Z(\mathbb{Q}, D_\ell; x) \leq Z^T(\mathbb{Q}, D_\ell; x) \leq c(\mathbb{Q}) \sum_{b^{\ell-1} \leq x} \ell^{\omega(b)} \sum_{a \leq \frac{x^{1/d}}{b^{(\ell-1)/d}}} \ell^{\mathrm{rk}(a)}$$

$$\leq c(\mathbb{Q}, \epsilon) \sum_{b^{\ell-1} \leq x} \ell^{\omega(b)} \sum_{a \leq \frac{x^{1/d}}{b^{(\ell-1)/d}}} a^{1/2+\epsilon}$$

Wegen

$$\sum_{a \leq \frac{x^{1/d}}{b^{(\ell-1)/d}}} a^{1/2+\epsilon} \leq \int_0^{x^{1/d} b^{(\ell-1)/d}} a^{1/2+\epsilon}\, da = \frac{1}{3/2+\epsilon} \frac{x^{(3/2+\epsilon)/d}}{b^{3(\ell-1)/(2d)+\epsilon(\ell-1)/d}}$$

erhalten wir wegen $2d = \ell - 1$ und $b^{\epsilon(\ell-1)/d} \geq 1$:

$$Z(\mathbb{Q}, D_\ell; x) \leq \frac{c(\mathbb{Q}, \epsilon)}{3/2+\epsilon} \sum_{b^{\ell-1} \leq x} \ell^{\omega(b)} \frac{x^{(3/2+\epsilon)/d}}{b^{3(\ell-1)/(2d)}} = \tilde{c}(\mathbb{Q}, \epsilon)x^{(3/2+\epsilon)/d} \sum_{b^{\ell-1} \leq x} \frac{\ell^{\omega(b)}}{b^3}.$$

Da die letzte Summe konvergiert und $a(D_\ell) = 1/d$ gilt, folgt die Behauptung.
Der zweite Fall geht analog. □

Kapitel 7

Verallgemeinerte Quaternionengruppen

In diesem Kapitel werden wir für sogenannte verallgemeinerte Quaternionengruppen G die präzise Form der Vermutung 2.12 beweisen, d.h. wir zeigen

$$Z(k, G; X) \sim c(k, G) x^{a(G)} \log(x)^{b(k,G)}.$$

Bisher waren solche Ergebnisse nur für abelsche Gruppen und Gruppen von kleinem Grad bekannt (S_3, D_4). Neben den Kranzprodukten (Satz 3.29) liefert dies eine zweite unendliche Serie von Gruppen, für die wir die präzise Form der Vermutung 2.12 beweisen können. Am Ende dieses Kapitels beweisen wir obere Schranken für dizyklische Gruppen. Auch für diese unendliche Serie würden wir die exakte Asymptotik bekommen, wenn wir für quadratische Zahlkörper und $2 \neq \ell \in \mathbb{P}$

$$\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_{\mathbb{Q}(\sqrt{a})})} = O_\epsilon(a^{1/2-\epsilon})$$

abschätzen könnten.

7.1 Die Quaternionengruppe Q_8

Für die Quaternionengruppe $Q_8 \leq S_8$ hatten wir in den Beispielen 4.27 und 4.31 gesehen, dass Konstanten $c(k, Q_8), d(k, Q_8) > 0$ existieren mit:

$$Z(k, Q_8; x) \leq c(k, Q_8) x^{1/4} \text{ sowie } Z(k, Q_8; x) \geq d(k, Q_8) x^{1/4} \text{ für } x >> 0.$$

Wir wollen untersuchen, ob wir obige „$\sim$“–Abschätzung erhalten können. Wie im Kapitel 3 ist es nützlich die zugehörige Dirichlet–Reihe zu betrachten, d.h.

wir summieren über alle Körpererweiterungen mit Galoisgruppe Q_8:

$$\Phi_{k,Q_8}(s) = \sum_{\mathrm{Gal}(L/k)=Q_8} \frac{1}{\mathcal{N}(d_{L/k})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Sei L/k eine Erweiterung mit Galoisgruppe Q_8. Da Q_8 genau eine Untergruppe der Ordnung 2 besitzt, gibt es genau einen Teilkörper K vom Grad 4. Es gilt: $\mathrm{Gal}(K/k) = Z_2 \times Z_2 =: H$. Wir betrachten also das zentrale Einbettungsproblem zu

$$1 \to Z_2 \to Q_8 \to Z_2 \times Z_2 \to 1.$$

Bei der oberen Abschätzung in Kapitel 4 hatten wir angenommen, dass jedes solche Einbettungsproblem lösbar ist, was natürlich nicht stimmt. Wir bezeichnen mit

$$\mathcal{K}_H := \{K/k \mid \mathrm{Gal}(K/k) = H, \text{ einbettbar in eine } Q_8\text{–Erweiterung}\}.$$

Zu jeder Q_8–Erweiterung L/k korrespondiert auf diese Weise genau ein Körper K aus der Menge $\mathcal{K}_H$ mit $K \leq L$. Wenn wir die endliche Menge $T \subseteq \mathbb{P}(k)$ wie in Satz 4.14 wählen, d.h. T enthalte alle Primideale über der 2 sowie genügend Primideale, um die Klassengruppe zu erzeugen, so erhalten wir mit $S_K := T \cup \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathfrak{p} \mid d_{K/k}\}$:

$$d_{L/k}^T = (d_{K/k}^T)^3 (d_{M/k}^{S_K})^4.$$

Dabei ist M die quadratische Erweiterung, die mittels Satz 4.10 der Körpererweiterung L/k zugeordnet ist. Da T alle Primideale über der 2 enthält, müssen wir keine wilde Verzweigung berücksichtigen. Wir haben in den Beispielen 4.22 und 4.27 ermittelt, dass $v_{\mathfrak{p}}(d_{L/k}) = 6$ für alle in K/k zahm verzweigten Primideale $\mathfrak{p}$ gilt. Wegen $v_{\mathfrak{p}}(d_{K/k}) = 2$ stimmt der Exponent 3. Analog erhalten wir den Exponenten 4.

Wie im Abschnitt 3.4 bezeichnen wir mit $\Phi_{k,Q_8}^T(s)$ die modifizierte Zählfunktion zu $Z^T(k, Q_8; x)$ und erhalten:

$$\Phi_{k,Q_8}^T(s) = \frac{1}{4} \sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{K/k}^T)^{3s}} \sum_{[M:k] \leq 2} \frac{1}{\mathcal{N}(d_{M/k}^{S_K})^{4s}}$$

$$= \frac{1}{4} \sum_{K \in \mathcal{K}_H} \frac{\Phi_{k,Z_2}^{S_K}(4s)}{\mathcal{N}(d_{K/k}^T)^{3s}}. \tag{7.1}$$

Der Vorfaktor $1/4$ kommt aus dem 3. Teil von Satz 4.10. Den 2. Teil dieses Satzes brauchen wir wegen $\ell = 2$ nicht zu berücksichtigen. Durch das Mitbetrachten der trivialen Erweiterung $M = k$ brauchen wir die triviale Klasse nicht gesondert zu behandeln, da auch diese Klasse 4 Elemente enthält. Da die Vermutung 2.12 für abelsche Gruppen bewiesen ist, erhalten wir $Z(k, Z_2 \times Z_2; x) \sim c(k, Z_2 \times Z_2) x^{1/2} \log(x)^2$ und damit konvergiert

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{K/k}^T)^{3s}}$$

für $\Re(s) > 1/6$. Weiterhin sagt Satz 3.16, dass $\Phi_{k,Z_2}^{S_K}(4s)$ für $\Re(s) > 1/4$ konvergiert und bei $s = 1/4$ einen einfachen Pol hat. Zusätzlich gibt es eine analytische Fortsetzung dieser Funktion nach links. Wäre diese Funktion nicht von S_K abhängig, so könnten wir sofort schließen, dass $Z^T(k, Q_8; x) \sim c(k, T, Q_8) x^{1/4}$ gilt.

Wir verwenden einen ähnlichen Ansatz wie im Abschnitt 3.7. Wir definieren:

$$g^T(s) := \frac{1}{4} \sum_{K \in \mathcal{K}_H} \frac{g_{k,S_K}(4s)}{\mathcal{N}(d_{K/k}^T)^{3s}},$$

wobei

$$g_{k,S_K}(s) := \Phi_{k,Z_2}^{S_K}(s) - \frac{\operatorname{res}_{s=1} \Phi_{k,Z_2}^{S_K}(s)}{s-1}$$

die Funktion aus Satz 3.17 ist, welche für $\Re(s) > 1/2$ analytisch ist und dabei für alle $\epsilon > 0$ folgende Abschätzung erfüllt ($\Re(s) = \sigma$, $n = [k : \mathbb{Q}]$):

$$\begin{aligned} |g_{k,S_K}(s)| &\le c(\epsilon, n) 2^{|S_K|} (d_k |1+s|^n)^{(1-\sigma)/2+\epsilon} d_k^{1/2} \\ &\le c(\epsilon, n, d_k) 2^{|S_K|} |1+s|^{n(1-\sigma)/2+\epsilon}. \end{aligned}$$

Hieraus folgt, dass die Reihe $g^T(s)$ für $\Re(s) > 1/6$ konvergiert. Wir erinnern daran (siehe Satz 3.16), dass $\mathfrak{d}$ der größte Teiler von $2\mathcal{O}_k$ ist, so dass $(2)/\mathfrak{d}$ koprim zu S_K ist. Mit

$$R(K) := \operatorname*{res}_{s=1} \Phi_{k,Z_2}^{S_K}(s) = \frac{\operatorname{res}_{s=1} \zeta_k(s)}{2^{i(k)} \zeta_k(2)} \prod_{\mathfrak{p} \in S_K} (1 + 1/\mathcal{N}(\mathfrak{p}))^{-1} 2^{|S_K|} \mathcal{N}(\mathfrak{d})$$

konvergiert auch die Reihe (vgl. Satz 3.16):

$$\frac{1}{4} \sum_{K \in \mathcal{K}_H} \frac{R(K)/(4s-1)}{\mathcal{N}(d_{K/k}^T)^{3s}}$$

$$= \frac{1}{4}\frac{\operatorname{res}_{s=1}\zeta_k(s)}{2^{i(k)}\zeta_k(2)} \sum_{K\in\mathcal{K}_H} \frac{\prod_{\mathfrak{p}\in S_K}(1+1/\mathcal{N}(\mathfrak{p}))^{-1}2^{|S_K|}\mathcal{N}(\mathfrak{d})/(4s-1)}{\mathcal{N}(d_{K/k}^T)^{3s}}$$

absolut und lokal gleichmäßig für alle Gebiete, die in $\{s \in \mathbb{C} \mid \Re(s) > 1/6, s \neq 1/4\}$ enthalten sind. Wir merken an, dass $\prod_{\mathfrak{p}\in S_K}(1+1/\mathcal{N}(\mathfrak{p}))^{-1}\mathcal{N}(\mathfrak{d}) \leq \mathcal{N}(\mathfrak{d})$ durch eine von n abhängige Konstante nach oben abgeschätzt werden kann. Somit erhalten wir aus der Darstellung

$$\Phi_{k,Q_8}^T(s) = g^T(s) + \frac{1}{4}\sum_{K\in\mathcal{K}_H} \frac{R(K)/(4s-1)}{\mathcal{N}(d_{K/k}^T)^{3s}},$$

dass $\Phi_{k,Q_8}^T(s)$ bei $s = 1/4$ einen einfachen Pol hat und meromorph auf $\Re(s) > 1/6$ fortsetzbar ist, wobei $s = 1/4$ der einzige Pol in diesem Bereich bleibt. Wir erhalten als direkte Anwendung des Tauber–Satzes 2.19:

Korollar 7.1
Für ein $c(k, Q_8, T) > 0$ gilt:

$$Z^T(k, Q_8; x) \sim c(k, Q_8, T)x^{1/4}.$$

Im Folgenden wollen wir die Funktion $Z(k, Q_8; x)$ untersuchen. Der einzige Grund für die Einführung von T war die einfach zu beweisende Relation:

$$d_{L/k}^T = (d_{K/k}^T)^3(d_{M/k}^{S_K})^4.$$

Für die Vereinfachung sind zwei Dinge verantwortlich:

(1) Die Verzweigung an wild verzweigten Stellen ist schwieriger zu bestimmen.

(2) Die minimale Lösung, die wir mit Satz 4.14 wählen, kann in einem bisher unverzweigten Primideal verzweigt sein.

Nehmen wir an, dass $\mathfrak{q}$ ein Primideal ist, welches in unserer minimalen Lösung neu verzweigt und in einer Z_2–Erweiterung M/k verzweigt ist. Unter der Annahme, dass $\mathfrak{q}$ nicht über 2 liegt, führt dies dazu (siehe Satz 4.10), dass unser neuer Körper nicht in $\mathfrak{q}$ verzweigt ist.

Als erstes werden wir die Primideale aus T entfernen, die nicht über 2 liegen. Seien hierzu

$$\tilde{T} := \{\mathfrak{p} \in T \mid 2 \in \mathfrak{p}\} \subseteq T \text{ sowie } U := (T \setminus \tilde{T}) \cup \{\mathcal{O}_k\}.$$

Wir wählen zu jedem Körper $K \in \mathcal{K}_H$ eine minimale Lösung gemäß Satz 4.14. Es gibt nun höchstens ein in unserer minimalen Lösung verzweigtes

Primideal $\mathfrak{q}$ mit $\mathfrak{q} \notin \tilde{T}$ sowie $\mathfrak{q} \nmid d_{K/k}$. Dieses Primideal muss dann in U liegen, welches wir K zuordnen. Falls kein weiteres Primideal benötigt wird, so ordnen wir K das Ideal $\mathcal{O}_k$ zu. Wir bezeichnen mit $K_{H,\mathfrak{q}}$ die Menge der Körper aus $\mathcal{K}_H$, denen wir auf diese Weise $\mathfrak{q}$ zuordnen. Weiterhin sei nun $S_K := \{\mathfrak{p} \mid d_{K/k}\} \cup \tilde{T}$. Wir teilen die Summe (7.1) auf und erhalten:

$$\Phi^{\tilde{T}}_{k,Q_8}(s) = \frac{1}{4} \sum_{\mathfrak{q} \in U} \sum_{K \in K_{H,\mathfrak{q}}} \frac{\mathcal{N}(\mathfrak{q})^{-4s} \Phi^{S_K}_{k,Z_2,\{\mathfrak{q}\}}(4s) + \mathcal{N}(\mathfrak{q})^{4s} \tilde{\Phi}^{S_K}_{k,Z_2,\{\mathfrak{q}\}}(4s)}{\mathcal{N}(d^T_{K/k})^{3s}},$$

wobei $\Phi^{S_K}_{k,Z_2,\{\mathfrak{q}\}}$ die Dirichletreihe zu den Z_2–Erweiterungen von k ist, welche in $\mathfrak{q}$ unverzweigt sind und wo wir die Verzweigung in S_K ignorieren. $\tilde{\Phi}^{S_K}_{k,Z_2,\{\mathfrak{q}\}}$ zählt dieselben Erweiterungen mit dem einzigen Unterschied, dass sie nun in $\mathfrak{q}$ verzweigt sind. Aufgrund der Aufteilung ist es uns möglich die Korrekturfaktoren (hier $\mathcal{N}(\mathfrak{q}^{\pm 4s})$) explizit anzugeben. Gleiches können wir für die wilde Verzweigung tun.

Da in T nur endliche viele Stellen enthalten sind und für jede Stelle nur endliche viele lokale Erweiterungen existieren, gibt es nur endlich viele Möglichkeiten für alle diese Stellen lokale Vorgaben zu machen. Sei also $L_{\mathcal{L}}$ die Menge aller lokalen Vorgaben für Z_2 an den Stellen aus T. Damit gilt:

$$\{K/k \mid \mathrm{Gal}(K/k) = Z_2\} = \dot{\bigcup_{\mathcal{L} \in L_{\mathcal{L}}}} \mathcal{K}_{\mathcal{L}},$$

wobei $\mathcal{K}_{\mathcal{L}}$ die Menge der Z_2–Erweiterungen ist, die die lokalen Vorgaben erfüllen. Durch diese Aufteilung ist nun für jede Vorgabe ermittelbar, was die tatsächliche Verzweigung an den Stellen aus T ist. Dies berücksichtigen wir durch entsprechende Vorfaktoren $c(K, T, \mathcal{L})$ und erhalten:

$$\Phi_{k,Q_8}(s) = \frac{1}{4} \sum_{K \in \mathcal{K}_H} \sum_{\mathcal{L} \in L_{\mathcal{L}}} c(K, T, \mathcal{L})^s \frac{\Phi^{S_K}_{\mathcal{L}}(4s)}{\mathcal{N}(d_{K/k})^{3s}}, \tag{7.2}$$

wobei $\Phi^{S_K}_{\mathcal{L}}$ die zur lokalen Vorgabe $\mathcal{L}$ gehörige Dirichlet–Reihe ist, bei der wir zusätzlich die Primstellen aus S_K ignorieren.

Satz 7.2
Für alle Zahlkörper k konvergiert die Dirichlet–Reihe $\Phi_{k,Q_8}(s)$ für $\Re(s) > 1/4$ absolut und lokal gleichmäßig. Sie hat einen einfachen Pol bei $s = 1/4$ und ist meromorph auf $\Re(s) > 1/6$ (ohne weiteren Pol) fortsetzbar. Weiterhin gilt:

$$Z(k, Q_8; x) \sim c(k, Q_8) x^{1/4}.$$

Beweis
Wir haben in Gleichung (7.2) bereits eine Darstellung von Φ_{k,Q_8} als Summe über die einbettbaren $Z_2 \times Z_2$–Körper berechnet. Mit Satz 3.24 und den gleichen Argumenten, die wir am Anfang dieses Abschnitts für Φ^T_{k,Q_8} benutzt haben, können wir zeigen, dass

$$\sum_{K \in \mathcal{K}_H} \frac{\Phi_{\mathcal{L}}^{S_K}(4s)}{\mathcal{N}(d_{K/k})^{3s}}$$

genau die gewünschten Meromorphie–Eigenschaften besitzt. Da die Menge $L_{\mathcal{L}}$ endlich ist, folgt die meromorphe Fortsetzbarkeit. Die Asymptotik folgt wie gewöhnlich durch Anwendung unseres Tauber–Satzes 2.19. □

Im Fall $k = \mathbb{Q}$ können wir $T = \{(2)\}$ wählen. Für eine lokale Vorgabe ist Satz 3.24 in [33] bewiesen. Zusätzlich haben wir für $k = \mathbb{Q}$ einen unabhängigen Beweis, der die lokalen Erweiterungen über $\mathbb{Q}_2$ studiert. Wir haben hier auf die Angabe dieses Beweises verzichtet, da er anscheinend nicht auf andere Situationen verallgemeinerbar ist.

7.2 Verallgemeinerte Quaternionengruppen

Die Beweismethode aus dem letzten Abschnitt lässt sich genauso auf eine unendliche Klasse von Gruppen, die sogenannten verallgemeinerten Quaternionengruppen, anwenden. Wir definieren zunächst eine noch allgemeinere Klasse von Gruppen.

Definition 7.3
Es sei $A = \langle a \rangle$ die zyklische Gruppe der Ordnung $2m$ für ein $m > 1$. Dann ist

$$\mathrm{Dic}(A) := \langle a, x \mid a^{2m} = 1, x^2 = a^m, x^{-1}ax = a^{-1} \rangle$$

die dizyklische Gruppe der Ordnung $4m$. Im Spezialfall $m = 2^l$ nennen wir $\mathrm{Dic}(A)$ die (verallgemeinerte) Quaternionengruppe Q_{4m} der Ordnung $4m$.

Klarerweise ist Q_8 die uns bereits bekannte Quaternionengruppe. Die Aussagen des folgenden Lemmas folgen direkt aus der Definition.

Lemma 7.4
Es sei $\mathrm{Dic}(A)$ die dizyklische Gruppe der Ordnung $4m$. Dann gelten:

(1) $A \trianglelefteq \mathrm{Dic}(A)$.

(2) x *hat Ordnung* 4 *in* $\mathrm{Dic}(A)$.

(3) Das Zentrum $\mathrm{Z}(\mathrm{Dic}(A))$ *von* $\mathrm{Dic}(A)$ *ist* $\langle x^2 \rangle$.

(4) Jedes Element von $\mathrm{Dic}(A)$ *hat eine Darstellung* $a^k x^j$ *mit* $j = 0$ *oder* 1 *sowie* $1 \leq k \leq 2m$.

(5) x^2 *ist das einzige Element der Ordnung 2 in* $\mathrm{Dic}(A)$.

Im Folgenden nehmen wir an, dass $G = Q_{4m}$ mit einer 2–Potenz m ist. Diese Gruppe besitzt als transitive Gruppe nur die reguläre Darstellung. Wir erhalten, dass $H := G/\mathrm{Z}(G)$ isomorph zur Diedergruppe D_m ist. Weiterhin wird $\mathrm{ind}(G) = 4m - 2m = 2m$ von der einzigen Involution angenommen. Wir müssen nun wieder das Verzweigungsverhalten einer Q_{4m}–Erweiterung studieren. Sei hierzu L/k eine Erweiterung mit Galoisgruppe Q_{4m} und K der Fixkörper unter dem zentralen Element der Ordnung 2. Wir erhalten:

$$d_{L/k} = d_{K/k}^2 \mathcal{N}_{K/k}(d_{L/K}).$$

Wie im vorigen Abschnitt bezeichnen wir mit $\mathcal{K}_H$ die Menge der H–Erweiterungen, die in Q_{4m} einbettbar sind. Wir fixieren die übliche endliche Ausnahmemenge T und wählen zu jedem $K \in \mathcal{K}_H$ eine minimale Lösung L_K.
Sei nun $\sigma \in H$ ein Element der Ordnung o und $\tau \in G$ eines der Urbilder. Wir merken an, dass unabhängig von der Wahl des Urbilds dieses immer Ordnung $2o$ hat. Nun gilt:

$$\mathrm{ind}(\sigma) = 2m - 2m/o = 2m(1 - 1/o) \text{ und}$$

$$\mathrm{ind}(\tau) = 4m - 4m/(2o) = 2m + 2m(1 - 1/o).$$

Wir erhalten also für $S_K := \{\mathfrak{p} \in \mathbb{P}(k) \mid \mathfrak{p} | d_{K/k}\} \cup T$:

$$d_{L_K/k}^T = d_{K/k}^T \prod_{\mathfrak{p} \in S_K \setminus T} \mathfrak{p}^{2m}.$$

Da alle bereits in K verzweigten Elemente mindestens Ordnung 2 (in K) haben, haben ihre Urbilder in G damit mindestens Index $4m - 4m/4 = 3m$.

Lemma 7.5
Die Reihe

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{L_K/k})^s}$$

konvergiert für $\Re(s) > 1/(3m)$ *absolut und lokal gleichmäßig.*

Beweis
Wir imitieren den Beweis von Satz 4.25, wobei wir die Exponenten a_i nach der Vorüberlegung durch $3m$ nach unten abschätzen. Sei also $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) \in \mathcal{O}_k^r$ ein Tupel, welches einen Körper K parametrisiert. Dann gilt:

$$d_{L_K/k} \geq \mathcal{N}(\mathfrak{a}_1)^{3m} \cdots \mathcal{N}(\mathfrak{a}_r)^{3m}.$$

Da jedem Körper K genau ein Körper L_K zugeordnet ist, erhalten wir mit dem analogen Beweis wie in Satz 4.25, dass die Dirichletreihe für $\Re(s) > 1/(3m)$ absolut und lokal gleichmäßig konvergiert. □

Sei nun L eine Lösung, die nach Satz 4.10 durch die zyklische Z_2–Erweiterung M parametrisiert wird. Dann gilt:

$$d_{L/k}^T = d_{L_K/k}^T (d_{M/k}^{S_K})^{2m}.$$

Analog zum vorherigen Q_8–Fall erhalten wir:

$$\Phi_{k,Q_{4m}}^T(s) = 1/4 \sum_{K \in \mathcal{K}_H} \frac{\Phi_{k,Z_2}^{S_K}(2ms)}{\mathcal{N}(d_{L_K/k}^T)^s}.$$

Wieder analog zum Q_8–Fall können wir dann das Verhalten der Funktion $\Phi_{k,Q_{4m}}^T$ und damit die Asymptotik von $Z^T(k, Q_{4m}; x)$ bestimmen.

Anschließend entfernen wir wieder T durch die Zerlegung von $\Phi_{k,Z_2}^{S_K}$ in die endlich vielen lokalen Fälle und erhalten:

$$\Phi_{k,Q_{4m}}(s) = 1/4 \sum_{K \in \mathcal{K}_H} \sum_{\mathcal{L} \in L_{\mathcal{L}}} c(K, T, \mathcal{L})^s \frac{\Phi_{\mathcal{L}}^{S_K}(2ms)}{\mathcal{N}(d_{L_K/k})^s}.$$

Da nach Satz 3.24

$$\sum_{K \in \mathcal{K}_H} c(K, T, \mathcal{L})^s \frac{\Phi_{\mathcal{L}}^{S_K}(2ms)}{\mathcal{N}(d_{L_K/k})^s}$$

für $\Re(s) > 1/(2m)$ absolut und lokal gleichmäßig konvergiert, bei $s = 1/(2m)$ einen einfachen Pol besitzt und ansonsten meromorph nach links fortsetzbar ist, wobei die fortgesetzte Funktion analog nach oben abgeschätzt werden kann, haben wir folgenden Satz bewiesen.

Satz 7.6
Es seien $m = 2^l$ und Q_{4m} die verallgemeinerte Quaternionengruppe der Ordnung $4m$. Dann konvergiert für alle Zahlkörper k die Dirichlet–Reihe $\Phi_{k,Q_{4m}}(s)$ für $\Re(s) > 1/(2m)$ absolut und lokal gleichmäßig. Sie hat einen einfachen Pol bei $s = 1/4$ und ist meromorph auf $\Re(s) > 1/(3m)$ fortsetzbar. Weiterhin gilt:

$$Z(k, Q_{4m}; x) \sim c(k, Q_{4m}) x^{1/(2m)} = c(k, Q_{4m}) x^{a(Q_{4m})}.$$

7.3 Dizyklische Gruppen

Im vorherigen Abschnitt haben wir die verallgemeinerten Quaternionengruppen als Spezialfall der dizyklischen Gruppen kennengelernt. Alle dizyklischen Gruppen G haben die für uns schöne Eigenschaft, dass nur ein Element der Ordnung 2 existiert, welches dann den Minimalindex bestimmt und dafür sorgt, dass $b(k,G) = 0$ ist. Betrachten wir den Fall $m = 3$, d.h. die Gruppe $G = \mathrm{Dic}(Z_6)$, welche Ordnung 12 hat. Dies ist die Gruppe $12T_5$ in der Liste der transitiven Gruppen, d.h. die transitive Untergruppe der S_{12}, die wir durch Eingabe von *TransitiveGroup(12,5);* in Gap oder Magma bekommen. Wir erhalten folgende exakte und zentrale Sequenz.

$$1 \to Z_2 \to G \to H := D_3 \to 1.$$

Die Diedergruppe D_3 ist natürlich die symmetrische Gruppe S_3. Sei also wieder $\mathcal{K}_H$ die Menge der $S_3(6)$–Körper über k, die sich in G einbetten lassen. Weiterhin sei L_K wieder eine minimale Lösung. Wir erhalten:

$$\Phi_{k,\mathrm{Dic}(Z_6)}(s) = 1/2 \sum_{K \in \mathcal{K}_H} \sum_{\mathcal{L} \in L_{\mathcal{L}}} c(K,T,\mathcal{L})^s \frac{\Phi_{\mathcal{L}}^{S_K}(6s)}{\mathcal{N}(d_{L_K/k})^s}.$$

Wir können das Verhalten dieser Funktion bestimmen, wenn wir genügend über die Funktion

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{L_K/k})^s} \text{ bzw. } \sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d^T_{L_K/k})^s}$$

wissen. Dabei haben wir folgendes Problem. Aus Bemerkung 6.10 wissen wir, dass

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d_{K/k})^s} = O(x^{1/3})$$

ist. Da $d_{L_K/k} = d^2_{K/k} \mathcal{N}_{K/k}(d_{L_K/K})$ gilt, können wir obige Summe durch $O(x^{1/6})$ abschätzen, was uns aber nicht genügt. Wir imitieren lieber den Beweis von Satz 6.9. Dabei werden S_3–Erweiterungen durch Paare $(\mathfrak{a}, \mathfrak{b})$ parametrisiert. Hierbei beachten wir, dass Elemente der Ordnung 2 in S_3 zu Elementen der Ordnung 4 mit Zykeltyp 4^3 in G werden. Elemente der Ordnung 3 behalten ihre Ordnung (Zykeltyp 3^4) oder liften zu Elementen der Ordnung 6. Wir erhalten für $k = \mathbb{Q}$ die Ungleichung $d_{L_K} \geq a^9 b^8$, wobei nun $a, b > 0$ die Erzeuger der Hauptideale sind. Wir erhalten:

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d^T_{L_K/k})^s} \leq \sum_{a^9 b^8 \leq x} \frac{3^{\mathrm{rk}(a)+\omega(b)+c(\mathbb{Q})} - 1}{2}$$

$$\leq c(\mathbb{Q}) \sum_{a^9 \leq x} 3^{\mathrm{rk}(a)} \sum_{b \leq x^{1/8}/a^{9/8}} 3^{\omega(b)} \leq c(\mathbb{Q}) x^{1/8} \log(x)^2 \sum_{a^9 \leq x} \frac{3^{\mathrm{rk}(a)}}{a^{9/8}}.$$

Die letzte Summe ist für $x \to \infty$ konvergent, womit gezeigt ist, dass

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d^T_{L_K/k})^s}$$

für $\Re(s) > 1/8$ konvergiert. Damit folgt dann analog wie im vorigen Abschnitt:

Satz 7.7
Für $G = 12T_5$ ist $\Phi_{\mathbb{Q},G}(s)$ für $\Re(s) > 1/6$ konvergent, hat bei $s = 1/6$ einen einfachen Pol und besitzt eine meromorphe Fortsetzung nach links. Wir erhalten:

$$Z(\mathbb{Q}, G; x) \sim c(\mathbb{Q}, G) x^{1/6} = c(\mathbb{Q}, G) x^{a(G)}.$$

Wir merken an, dass wir wegen [9] und Lemma 6.11 obigen Satz auch für beliebige Grundkörper k beweisen können. Wenn wir wie in Satz 6.12 die Klassenzahl von $\mathbb{Q}(\sqrt{a})$ mit $O(a^{1/2+\epsilon})$ abschätzen, erhalten wir für $G = \mathrm{Dic}(Z_{2\ell})$:

$$\sum_{K \in \mathcal{K}_H} \frac{1}{\mathcal{N}(d^T_{L_K/k})^s} \leq c(\mathbb{Q}) \sum_{b^{4\ell-4} \leq x} \ell^{\omega(b)} \sum_{a \leq \frac{x^{1/(3\ell)}}{b^{(4\ell-4)/3\ell}}} \ell^{\mathrm{rk}(a)}$$

$$\leq c(\mathbb{Q}, \epsilon) \sum_{b^{4\ell-4} \leq x} \ell^{\omega(b)} \sum_{a \leq \frac{x^{1/(3\ell)}}{b^{(4\ell-4)/3\ell}}} a^{1/2+\epsilon}$$

$$\leq c(\mathbb{Q}, \epsilon) \sum_{b^{4\ell-4} \leq x} \ell^{\omega(b)} \frac{x^{(3/2+\epsilon)/(3\ell)}}{b^{3(4\ell-4)/(6\ell)}} = x^{1/(2\ell)+\tilde{\epsilon}} \sum_{b^{4\ell-4} \leq x} \frac{\ell^{\omega(b)}}{b^{2-2/\ell}}.$$

Da $\ell > 2$ konvergiert die letzte Summe und wir erhalten den folgenden Satz.

Satz 7.8
Es sei $G = \mathrm{Dic}(Z_{2\ell})$ für ein $\ell \in \mathbb{P}$ und daher $a(G) = 1/(2\ell)$. Dann existieren für alle $\epsilon > 0$ Konstanten $c_1(\mathbb{Q}, G), c_2(\mathbb{Q}, G, \epsilon) > 0$ mit:

$$c_1(\mathbb{Q}, G) x^{a(G)} \leq Z(\mathbb{Q}, G; x) \leq c_2(\mathbb{Q}, G, \epsilon) x^{a(G)+\epsilon} \text{ für } x >> 0.$$

Beweis
Die untere Schranke folgt mit Satz 4.28, die obere Schranke folgt aus den vorherigen Rechnungen. □

Falls wir $\ell^{\mathrm{rk}(a)}$ durch $O(x^{1/2-\epsilon})$ abschätzen könnten, würden wir wie im Fall $\ell = 3$ die volle Vermutung beweisen können. Auch dieser Satz lässt sich auf beliebige Grundkörper k verallgemeinern.

Literaturverzeichnis

[1] A. M. Baily. On the density of discriminants of quartic fields, *J. Reine Angew. Math.* **315** (1980), 190–210.

[2] K. Belabas. Paramétrisation de structures algébriques et densité de discriminants [d'après bhargava]. *Seminaire Bourbaki* **56eme annee** (2004).

[3] M. Bhargava. Gauss composition and generalizations. In *Algorithmic number theory (Sydney, 2002)*, Band 2369 aus *Lecture Notes in Comput. Sci.*, Seiten 1–8. Springer, Berlin, 2002.

[4] R. Brauer. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, *Math. Nachr.* **4** (1950), 158–174.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[6] H. Cohen, F. Diaz y Diaz, und M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$, *Compositio Math.* **133** (2002), 65–93.

[7] H. Cohen, F. Diaz y Diaz, und M. Olivier. On the density of discriminants of cyclic extensions of prime degree, *J. Reine Angew. Math.* **550** (2002), 169–209.

[8] H. Cohen und H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983*, Band 1068 aus *Lecture Notes in Math.*, Seiten 33–62. Springer, Berlin, 1984.

[9] B. Datskovsky und D. Wright. Density of discriminants of cubic extensions, *J. reine angew. Math.* **386** (1988), 116–138.

[10] H. Davenport und H. Heilbronn. On the density of discriminants of cubic fields. II, *Proc. Roy. Soc. London Ser. A* **322** (1971), 405–420.

[11] H. Delange. Generalisation du theoreme de Ikehara, *Ann. Sci. École Norm. Sup.(3)* **71** (1954), 213–242.

[12] J. Dixon und B. Mortimer. *Permutation groups.* Springer, Berlin-Heidelberg-New York, 1996.

[13] J. Ellenberg und A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. arXiv math.NT/0309153, 2003.

[14] J. Ellenberg und A. Venkatesh. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric Methods in Algebra and Number Theory*, Band 235 aus *Progress in Mathematics*, Seiten 151–168. Birkhäuser, 2005.

[15] H. Helfgott und A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. arXiv:math.NT/0405180, 2004.

[16] F. Hess, S. Pauli, und M. E. Pohst. Computing the multiplicative group of residue class rings, *Math. Comput.* **72** (2003), 1531–1548.

[17] H. Iwaniec und E. Kowalski. *Analytic Number Theory*, Band 53 aus *Colloquium Publications.* American Mathematical Society, 2004.

[18] J. Klüners und C. Fieker. Minimal discriminants for small fields with Frobenius groups as Galois groups, *J. Numb. Theory* **99** (2003), 318–337.

[19] J. Klüners und G. Malle. Counting nilpotent Galois extensions, *J. Reine Angew. Math.* **572** (2004), 1–26.

[20] M. Krasner und L. Kaloujnine. Produit complet des groupes de permutation et problème d'extension de groupes II, *Acta Sci. Math. (Szeged)* **14** (1951), 39–66.

[21] S. Kuroda. Über die Klassenzahlen algebraischer Zahlkörper, *Nagoya Math. J.* **1** (1950), 1–10.

[22] S. Lang. *Algebraic Number Theory.* Springer, Berlin-Heidelberg-New York, 1986.

[23] G. Malle. On the distribution of Galois groups, *J. Numb. Theory* **92** (2002), 315–322.

[24] G. Malle. On the distribution of Galois groups II, *Exp. Math.* **13** (2004), 129–135.

[25] G. Malle und B. H. Matzat. *Inverse Galois Theory.* Springer Verlag, Heidelberg, 1999.

[26] R. Murty. *Problems in Analytic Number Theory.* Springer, 2001.

[27] W. Narkiewicz. *Number Theory.* World Scientific, 1983.

[28] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer, 1989.

[29] J. Neukirch. *Algebraische Zahlentheorie.* Springer, Berlin-Heidelberg-New York, 1992.

[30] J. Neukirch, A. Schmidt, und K. Wingberg. *Cohomology of Number Fields.* Springer, Berlin-Heidelberg-New York, 2000.

[31] J.-P. Serre. *Local Fields.* Springer, New York, 1995.

[32] K. Soundararajan. Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc. (2)* **61** (2000), 681–690.

[33] D. Wright. Distribution of discriminants of abelian extensions, *Proc. London Math. Soc.* **58** (1989), 17–50.

[34] G. Yu. A note on the divisibility of class numbers of real quadratic fields, *J. Numb. Theory* **97** (2002), 35–44.

Symbolverzeichnis

S_n	symmetrische Gruppe auf n Punkten	Seite 7
$S_3(6)$	S_3 auf 6 Punkten	Seite 7
$\mathrm{Gal}(K/k)$	Galoisgruppe von K/k	Seite 7
$d_{K/k}$	Relativdiskriminante	Seite 7
$\mathcal{O}_k$	Maximalordnung von k	Seite 7
$\mathbb{P}(k)$	Menge der Primideale von $\mathcal{O}_k$	Seite 8
$[K:k]$	Körpergrad	Seite 8
$\mathcal{N}_{K/k}(\mathfrak{a})$	Norm eines Ideals	Seite 8
$\mathcal{N}$	Absolutnorm eines Ideals	Seite 8
d_k	Absolutdiskriminante von k	Seite 8
N^H	Fixkörper von N unter H	Seite 8
s_{G/H_i}	Permutationscharakter zur Untergruppe H_i	Seite 8
ℓ	eine Primzahl	Seite 9
Z_ℓ	zyklische Gruppe mit ℓ Elementen	Seite 9
$v_\mathfrak{p}(\mathfrak{a})$	$\mathfrak{p}$–Bewertung von $\mathfrak{a}$	Seite 9
$p^k \mid\mid b$	p^k teilt genau b	Seite 9
$U \trianglelefteq G$	U Normalteiler von G	Seite 10
$H \leq G$	H Untergruppe von G	Seite 10
$G := U \rtimes H$	semidirektes Produkt von U mit H	Seite 10
$\mathrm{Aut}(U)$	Automorphismengruppe von U	Seite 11
$H_1 \wr H_2$	Kranzprodukt von H_1 mit H_2	Seite 11
$Z(k, G; x)$	Anzahl Körper mit Galoisgruppe G und Diskriminante kleiner gleich x	Seite 12
$f \sim g$	$\lim_{x\to\infty} f(x)/g(x) = 1$	Seite 12
$f = O(g)$	$\limsup_{x\to\infty} f(x)/g(x) < \infty$	Seite 12
$f = o(g)$	$\limsup_{x\to\infty} f(x)/g(x) = 0$	Seite 12
$x >> 0$	für x groß genug	Seite 12
$\mathrm{ind}(\sigma)$	Index einer Permutation	Seite 12
$\mathrm{ind}(G)$	Minimalindex einer Gruppe	Seite 12
$a(G)$	$\mathrm{ind}(G)^{-1}$	Seite 12
$\bar{k}$	algebraischer Abschluss von k	Seite 13

G_k	absolute Galoisgruppe von k	Seite 13
$\Re(s)$	Realteil von s	Seite 16
$\Im(s)$	Imaginärteil von s	Seite 16
$\Gamma(s)$	Gamma–Funktion	Seite 17
$\omega(\mathfrak{a})$	Anzahl der verschiedenen Primteiler von $\mathfrak{a}$	Seite 17
$t_k(\mathfrak{a})$	Anzahl der verschiedenen Idealteiler von $\mathfrak{a}$	Seite 17
$\mathfrak{m}$	$= (\mathfrak{m}_0, \mathfrak{m}_\infty)$ Erklärungs–Modul	Seite 21
$\mathrm{Cl}_\mathfrak{m}$	Strahlklassengruppe von $\mathfrak{m}$	Seite 21
$I^\mathfrak{m}$	gebrochene Ideale koprim zu $\mathfrak{m}_0$	Seite 21
$H_\mathfrak{m}$	gebrochene Hauptideale (α) mit $\alpha \equiv 1 \bmod {}^*\mathfrak{m}$.	Seite 21
Cl_k	Klassengruppe von k.	Seite 23
$H^\mathfrak{m}$	gebrochene Hauptideale koprim zu $\mathfrak{m}_0$	Seite 23
rk_ℓ	ℓ–Rang der Klassengruppe von k	Seite 23
$\zeta_k(s)$	Dedekindsche Zeta–Funktion	Seite 27
$\mathrm{res}_{s=1}\,\zeta_k(s)$	Residuum an der Stelle 1	Seite 27
$Z(k, G, S; x)$	Anzahl Körper koprim zu S mit Galoisgruppe G und Diskriminante kleiner gleich x	Seite 30
$\Phi_{k,G,S}(s)$	Dirichletreihe zu $Z(k, G, S; x)$	Seite 31
φ	Eulersche φ–Funktion	Seite 32
a^S	zu S koprimer Anteil von a	Seite 34
$Z^S(k, G; x)$	Zählfunktion koprim zu S	Seite 34
$\Phi^S_{k,G}(s)$	Dirichletreihe zu $Z^S(k, G; x)$	Seite 36
S_∞	Teilmenge von unendlichen Stellen	Seite 44
$\mathrm{Frat}(G)$	Frattinigruppe	Seite 55
$G_1 \times_H G_2$	subdirektes Produkt	Seite 56
$\mathcal{M}_K$	Menge von Z_ℓ–Erweiterungen	Seite 60
$\mathcal{K}(x)$	Menge von Körpererweiterungen mit Diskriminante kleiner gleich x	Seite 66
D_ℓ	Diedergruppe mit 2ℓ Elementen.	Seite 83
$D_\ell(2\ell)$	Diedergruppe D_ℓ in regulärer Darstellung	Seite 84
$\mathrm{Dic}(A)$	dizyklische Gruppe	Seite 98

Index