der Bundeswehr
Universität München

Galoismodulstruktur von l-Einheitengruppen in l-ten Kreisteilungskörpern

Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)

vorgelegt von
Dipl.-Math. Mario Christian Romsy
am 12. Mai 2010

Tag der mündlichen Prüfung:	27. Juli 2010
Vorsitzender der Kommission:	Prof. Dr. Andreas Karcher
1. Berichterstatter:	Prof. Dr. Cornelius Greither
2. Berichterstatter:	Prof. Dr. Werner Bley
3. Berichterstatter:	Prof. Dr. Peter Hertling
4. Berichterstatter:	Prof. DDr. Stefan Schäffler

Universität der Bundeswehr München
Fakultät für Informatik

Inhaltsverzeichnis

Einleitung

Sei K/F eine endliche Galoiserweiterung mit $G = \mathrm{Gal}(K/F)$. Weiter bezeichnen wir die Ringe der ganzen Zahlen von K und F wie üblich mit $\mathcal{O}_K$ beziehungsweise mit $\mathcal{O}_F$. Offenbar kann man $\mathcal{O}_K$ als Modul über dem Gruppenring $\mathcal{O}_F[G]$ auffassen und es stellt sich die natürliche Frage nach der Struktur dieses Moduls. Wenn $\mathcal{O}_K$ frei über $\mathcal{O}_F[G]$ ist, hat $\mathcal{O}_K$ eine Normalbasis über $\mathcal{O}_F$. In diesem Fall spricht man auch von trivialer Galoismodulstruktur von K/F.

Für $F = \mathbb{Q}$ besagt der Satz von Hilbert-Speiser, dass $\mathcal{O}_K$ für jede endliche zahme abelsche Erweiterung $K/\mathbb{Q}$ frei über $\mathcal{O}_\mathbb{Q}[G] = \mathbb{Z}[G]$ ist. In Anlehnung an dieses Ergebnis nennt man einen Körper F Hilbert-Speiser, wenn jede endliche zahme abelsche Erweiterung E/F triviale Galoismodulstruktur hat. Allerdings haben Greither et al. in [GRRS99] gezeigt, dass nur der Körper der rationalen Zahlen $\mathbb{Q}$ diese Eigenschaft besitzt, die Situation für beliebige Körper L also komplizierter ist. Für eine eingehende Auseinandersetzung mit diesem Thema verweisen wir hier auf das Buch von Fröhlich [Fr83], in dem auch folgendes Ergebnis von Noether zu finden ist ([Fr83, Kapitel 1, §1]):

Sei K/F eine Galoiserweiterung nicht-archimedisch lokaler Körper mit Galoisgruppe G. Genau dann ist $\mathcal{O}_K$ frei über $\mathcal{O}_F[G]$, wenn K/F zahm verzweigt ist.

In dieser Arbeit werden wir uns jedoch nicht mit der additiven Galoismodulstruktur der Ringe ganzer Zahlen von Zahlkörpern beschäftigen, sondern mit der multiplikativen Galoismodulstruktur spezieller Einheitengruppen. Allerdings möchten wir an dieser Stelle anmerken, dass beide Fragestellungen durchaus Gemeinsamkeiten aufweisen. So führt Chinburg in [Chi83] eine einheitliche Notation ein, indem er Begriffe beider Fragestellungen, die für das jeweils zugehörige Problem ähnliche Rollen spielen, miteinander identifiziert. Dadurch gelingt es ihm, einige Betrachtungen für beide Aufgabenstellungen parallel durchzuführen.
Der nächste zur Untersuchung multiplikativer Galoismodulstruktur hinleitende Schritt ist die folgende Umformulierung eines Ergebnisses von Minkowski (siehe [Nar04, Theorem 3.26a]):

Sei $K/\mathbb{Q}$ eine Galoiserweiterung mit $G = \mathrm{Gal}(K/\mathbb{Q})$. Weiter bezeichnen wir mit $U(K)$ die Einheitengruppe des Rings der ganzen Zahlen $\mathcal{O}_K$ von K und mit $\mu(K)$ die Gruppe der Einheitswurzeln in K. Dann gibt es einen zyklischen $\mathbb{Z}[G]$-Untermodul C von $\overline{U}(K) := U(K)/\mu(K)$ mit $\left|\overline{U}(K)/C\right| < \infty$.

Dies führt uns zu folgender Definition: Ist $\overline{U}(K)$ ein zyklischer $\mathbb{Z}[G]$-Modul, so nennt man einen Erzeuger α von $\overline{U}(K)$ *Minkowski-Einheit*.

Wir beschränken unsere Betrachtungen auf Körpererweiterungen $K/\mathbb{Q}$ mit

$$K \subseteq \mathbb{Q}(\zeta_l)^+ = \mathbb{Q}(\zeta_l + \zeta_l^{-1}),$$

wobei $l > 2$ eine Primzahl und ζ_l eine primitive l-te Einheitswurzel ist. Diese Körpererweiterungen sind also insbesondere reell und zyklisch.

Für ein erstes Ergebnis zur Frage nach der Existenz von Minkowski-Einheiten in reellen Erweiterungen $K/\mathbb{Q}$ zitieren wir ein weiteres Mal Narkiewicz [Nar04, Theorem 3.28]:

Sei p eine ungerade Primzahl derart, dass die Klassenzahl $h_{\mathbb{Q}(\zeta_p)} = 1$ ist. Dann gibt es in jeder zyklischen Galoiserweiterung $K/\mathbb{Q}$ vom Grad p eine Minkowski-Einheit. Allerdings haben die primen Kreisteilungskörper $\mathbb{Q}(\zeta_p)$ nur für $p \leq 19$ Klassenzahl 1.

Weitere Arbeiten zu diesem Problem stammen beispielsweise von Marko ([Mar96], [Mar05]). Eines der Hauptergebnisse von [Mar05] besagt, dass in der reellen zyklischen Erweiterung $K/\mathbb{Q}$ mit $[K : \mathbb{Q}] \in \{6, 10, 14\}$ genau dann eine Minkowski-Einheit existiert, wenn die Normabbildung

$$U(K) \to U(F)$$

für jeden Unterkörper $F \subset K$ surjektiv ist.

Fröhlich zeigt in [Fr92] unter anderem, dass $\overline{U}(K)$ lokal frei, also projektiv, über $\mathbb{Z}[G]$ ist, wenn $[K : \mathbb{Q}]$ eine Primzahlpotenz ist, G zyklisch ist und nur eine Primzahl in K verzweigt, diese aber voll verzweigt ist.
In dieser Arbeit, die sich allgemein mit der Galoismodulstruktur von Einheitengruppen in reellen abelschen Zahlkörpern beschäftigt, beschreibt Fröhlich in der Einleitung den Stand der Forschung in diesem Gebiet wie folgt:

„Our topic is the Galois module structure of their groups of units. Practically nothing has been known about this [...]. Whether or when there is a Minkowski unit is an old question without an answer. Even in terms of examples the information has been minimal.“

Auch wenn [Fr92] bereits 1992 erschienen ist und seitdem, wie oben angeführt, einige Erfolge erzielt wurden, so ist diese Beschreibung unseres Wissens, in etwas abgeschwächter Form, auch heute noch gültig. Hier sollten wir sogleich klarstellen, dass auch diese Dissertation, selbst für unsere eingeschränkte Klasse von Körpererweiterungen, keine allgemeine Lösung liefert. Wir werden jedoch zumindest, wenn auch nur konditionell, die bemängelte Armut an Beispielen etwas bessern.
Diese Beispiele erhalten wir durch eine Verbindung der Einheitengruppe modulo $\mathbb{Z}$-Torsion, $\overline{U}(K)$, mit unserem eigentlichen Studienobjekt, den l-Einheiten modulo $\mathbb{Z}$-Torsion in diesen Körpern, die wir an dieser Stelle kurz einführen möchten:

Bekanntlich ist l in $\mathbb{Q}(\zeta_l)^+$ und damit auch in jedem Unterkörper $\mathbb{Q} \neq K \subseteq \mathbb{Q}(\zeta_l)^+$ voll verzweigt. Bezeichnen wir mit $\mathfrak{l}_K$ das einzige Primideal über (l) in K, so definiert man die l-Einheiten in K durch

$$U_l(K) := \{\alpha \in K \mid v_{\mathfrak{p}}(\alpha) = 0 \text{ für alle Primideale } \mathfrak{p} \neq \mathfrak{l}_K\},$$

wobei $v_{\mathfrak{p}}$ die übliche diskrete $\mathfrak{p}$-Bewertung ist. Die $\mathbb{Z}$-Torsionsuntergruppe von $U_l(K)$ besteht offensichtlich, wie bei $U(K)$ auch, nur aus $\{-1, 1\}$ und man definiert die l-Einheiten modulo Torsion

$$\overline{U}_l(K) := U_l(K)/\{-1, 1\}.$$

Nach dem Dirichletschen Einheitensatz gilt für $\overline{U}_l := \overline{U}_l(\mathbb{Q}(\zeta_l)^+)$ bekanntlich $\overline{U}_l \cong \mathbb{Z}^{\frac{l-1}{2}}$. In dieser Dissertation möchten wir untersuchen, ob $\overline{U}_l$ projektiv oder sogar frei über $\mathbb{Z}[G]$ ist. Insbesondere suchen wir nach Beispielen, in denen Projektivität, nicht aber Freiheit von $\overline{U}_l$ über $\mathbb{Z}[G]$ gegeben ist.

Natürlich kann man allgemeiner für eine Galoiserweiterung K/F und eine endliche Menge S von Primstellen in K die sogenannten S-Einheiten $U_S(K)$ definieren. Die Untersuchung der Galoismodulstruktur von S-Einheitengruppen ist Gegenstand einer Vielzahl von Arbeiten, etwa von Chinburg ([Chi83], [Chi84]), Fröhlich ([Fr89]) und Dubois ([Dub00]), um nur einige zu nennen. Weiss hat zu diesem Thema auch ein Buch [Wei96] verfasst. Die Ergebnisse der oben genannten Arbeiten sind allerdings recht allgemeiner Form und teilweise gebunden an schwer überprüfbare Voraussetzungen an die Primstellenmenge S. Für die Untersuchung der l-Einheiten, und damit für diese Dissertation, sind sie deshalb nur mittelbar relevant.

Wir möchten jetzt noch einen anderen Aspekt ansprechen, der für uns von großer Bedeutung ist. Wie beispielsweise in dem bereits zitierten Satz [Nar04, Theorem 3.28], werden wir feststellen, dass die Galoismodulstruktur der l-Einheiten modulo Torsion in sehr enger Verbindung mit der Klassenzahl $h_l^+ =$

$h_{\mathbb{Q}(\zeta_l)^+}$ steht. Um mit Hilfe unserer theoretischen, von den Klassenzahlen abhängigen, Ergebnisse auch nicht-triviale Beispiele zu erhalten, benötigen wir Primzahlen l derart, dass $h_l^+ \neq 1$ ist.
Doch damit treffen wir auf ein weiteres großes Problem der Zahlentheorie. Bis heute ist kein effizientes Verfahren zur Bestimmung von h_l^+ für beliebige Primzahlen l bekannt. Ein klassisches Resultat ist gegeben durch die sogenannte Minkowski-Schranke. Im Fall reeller algebraischer Zahlkörper $K/\mathbb{Q}$ gilt demnach, dass jedes gebrochene Ideal äquivalent zu einem Ideal $\mathfrak{a}$ mit

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \cdot \sqrt{D_K}$$

ist, wobei N die Idealnorm, $[K : \mathbb{Q}] = n$ und D_K die Diskriminante von K ist. Für $K = \mathbb{Q}(\zeta_l)^+$ ist $D_K = l^{(l-3)/2}$, sodass diese Ungleichung als

$$N(\mathfrak{a}) \leq \left(\frac{l-1}{2}\right)! \cdot l^{(l-3)/4} \cdot \left(\frac{l-1}{2}\right)^{-\frac{l-1}{2}}$$

geschrieben werden kann. Eine Überprüfung aller Ideale, die diese Normungleichung erfüllen, ist schon für mäßig große l praktisch nicht durchführbar; bereits für $l = 71$ ist die Schranke größer als 10^{17}, für $l = 163$ größer als 10^{54}. Unter Verwendung von Ergebnissen von Odlyzko ([Od75],[Od76],[Od77]) war Masley, siehe dazu [Mas78], in der Lage, unter anderem die Klassenzahlen von $\mathbb{Q}(\zeta_l)^+$ für alle Primzahlen $2 < l < 71$ zu bestimmen. Auf dieser Arbeit aufbauend und unter Voraussetzung der verallgemeinerten Riemannschen Vermutung konnte van der Linden in [vdL82] diese Liste von Klassenzahlen h_l^+ bis $l \leq 163$ erweitern. Allerdings sind auch diese Ergebnisse für unsere Zwecke nur von geringem Nutzen - unter allen Primzahlen $l \leq 163$ ist nur für $l = 163$ die Klassengruppe nicht trivial. Wir werden in Abschnitt 4.7 zeigen, dass die l-Einheiten modulo Torsion in diesem einen Fall trotzdem $\mathbb{Z}[G]$-frei sind.[1]

Die Basis für unsere Folgerungen aus theoretischen Erkenntnissen liefert eine Arbeit von Schoof [Sch03]. Ihr Ausgangspunkt ist eine Tatsache, die auch wir vielfach nutzen werden:
Die Klassengruppe Cl_l^+ von $\mathbb{Q}(\zeta_l)^+$ hat die gleiche Mächtigkeit wie $B_l := U(\mathbb{Q}(\zeta_l)^+)/\mathrm{Cyc}(\mathbb{Q}(\zeta_l)^+)$, wobei $\mathrm{Cyc}(\mathbb{Q}(\zeta_l)^+)$ die Kreiseinheiten von $\mathbb{Q}(\zeta_l)^+$ bezeichnet.
Eine weitere wichtige Zutat bildet die Erkenntnis, dass sowohl B_l als auch Cl_l^+ als endliche $\mathbb{Z}[G]$-Moduln Jordan-Hölder-Reihen besitzen und, dass für jede Schranke S die größten Untermoduln von B_l und Cl_l^+, für die alle Jordan-Hölder-Faktoren weniger als S Elemente haben, gleichmächtig sind. Zudem

[1] Unter der Voraussetzung, dass tatsächlich, wie vermutet, $h_{163}^+ = 4$ gilt.

führt Schoof ein Verfahren zur Berechnung der Jordan-Hölder-Faktoren von B_l mit bestimmter (kleiner) Ordnung ein. Damit erstellt er eine Liste von Teilern[2] $\tilde{h}_l^+$ der Klassenzahlen h_l^+, für die insbesondere entweder $h_l^+ = \tilde{h}_l^+$ oder $h_l^+ > 80000 \cdot \tilde{h}_l^+$ gilt. Die daraus resultierende Vermutung, dass in den meisten, oder gar allen Fällen tatsächlich die Gleichheit von h_l^+ und $\tilde{h}_l^+$ gilt, untermauert Schoof, indem er mit Hilfe von Cohen-Lenstra-Heuristiken erklärt, dass die von ihm erstellte Liste von Klassenzahlteilern mit einer Wahrscheinlichkeit von über 98% in der Tat eine Liste der Klassenzahlen ist. Insbesondere gilt demnach die angesprochene Gleichheit von Pseudoklassenzahl und Klassenzahl für jede einzelne Primzahl l mit noch höherer Wahrscheinlichkeit.
Wir werden diese vermutete Gleichheit in unseren Folgerungen stets voraussetzen, ohne es jedes Mal explizit zu erwähnen. Die numerischen Ergebnisse in dieser Arbeit sind somit nur unter der Annahme $\tilde{h}_l^+ = h_l^+$ gültig. In einigen Fällen, in denen eine etwas schwächere Annahme ausreichend ist, machen wir dies gesondert kenntlich.

Wir skizzieren jetzt noch den Aufbau dieser Arbeit. Der erste Teil von Kapitel 1 fasst Grundlagen der Homologischen Algebra zusammen; der zweite Abschnitt beschäftigt sich mit Pullback-Diagrammen und den zugehörigen Mayer-Vietoris-Sequenzen.
Kapitel 2 ist den Kreiszahlen und den Kreiseinheiten in $\mathbb{Q}(\zeta_l)^+$ gewidmet. Die Sätze 2.7 und 2.9, welche die Galoismodulstruktur der Kreiszahlen modulo $\mathbb{Z}$-Torsion, $\overline{\mathrm{Cn}}$, in Abhängigkeit von der Klassenzahl $h_{\mathbb{Q}(\zeta_l)^+}$ vollständig beschreiben, bilden hier das Hauptergebnis.
Die $\mathbb{Z}[G]$-Projektivität von $\overline{U}_l$ ist das Thema des dritten Kapitels. Dabei unterscheiden wir zwei Hauptfälle. Sind $\frac{l-1}{2}$ und h_l^+ koprim, so liefert Satz 3.3 eine eindeutige Aussage zur $\mathbb{Z}[G]$-Projektivität von $\overline{U}_l$. Der andere Fall, $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) \neq 1$, unterteilt sich in einige Unterfälle, wobei wir uns an der Liste von Schoof orientieren und letztlich für alle darin auftretenden l mit obiger Eigenschaft nachweisen können, dass $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv ist.
In Kapitel 4 untersuchen wir die $\mathbb{Z}[G]$-projektiven Moduln $\overline{U}_l$ auf $\mathbb{Z}[G]$-Freiheit. Da $\mathbb{Z}[G]$-Projektivität von $\overline{U}_l$ in den Beispielen aus Schoofs Liste nur für $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) = 1$ auftritt, beschränken wir unsere Betrachtungen auf diesen Fall. Zur Untersuchung von $\overline{U}_l$ definieren wir in Abschnitt 4.1 ein zugehöriges Ideal $X \subset \mathbb{Z}[G]$, das unter anderem genau dann frei beziehungsweise projektiv über $\mathbb{Z}[G]$ ist, wenn $\overline{U}_l$ diese Eigenschaft hat und das zudem die Gleichung $|\mathbb{Z}[G]/X| = |\overline{U}_l/\overline{\mathrm{Cn}}|$ erfüllt. Auf diese Weise können einige Betrachtungen vereinfacht werden. Des Weiteren verlagern wir einen Großteil der Überlegungen und Rechnungen in geeignete relativ kleine Unterkörper

[2] Im folgenden werden diese auch Pseudo-Klassenzahlen genannt.

K der reellen Kreisteilungskörper $\mathbb{Q}(\zeta_l)^+$ (Abschnitt 4.3). In Abschnitt 4.4 zeigen wir dann, dass es genau dann eine Minkowski-Einheit in $K \subseteq \mathbb{Q}(\zeta_l)^+$ gibt, wenn die l-Einheiten modulo Torsion $\overline{U}_l(K)$ triviale Galoismodulstruktur haben, also $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-frei sind.
Während Abschnitt 4.6 die ersten Beispiele für Projektivität und gleichzeitige Nichtfreiheit von $\overline{U}_l$ über $\mathbb{Z}[G]$ liefert, weisen wir in Abschnitt 4.7, ausgehend von Schoofs Liste, für 35 von 67 noch offenen Fällen die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ und damit auch die Existenz einer Minkowski-Einheit in $\mathbb{Q}(\zeta_l)^+$ nach.
Ein komplizierteres Verfahren, mit dem unter gewissen Umständen nachgewiesen werden kann, wenn $\overline{U}_l$ nicht $\mathbb{Z}[G]$-frei ist, beschreiben wir in Abschnitt 4.8. Die Anwendung dieses Verfahrens ist in 17 weiteren Fällen erfolgreich. Als kleinstes Beispiel für Projektivität und Nichtfreiheit von $\overline{U}_l$ über $\mathbb{Z}[G]$ finden wir auf diese Weise $l = 491$. In $\mathbb{Q}(\zeta_{491})^+$ gibt es demnach keine Minkowski-Einheit. Die bezüglich des Grads über $\mathbb{Q}$ kleinsten gefundenen Körper mit dieser Eigenschaft sind die Unterkörper von $\mathbb{Q}(\zeta_l)^+$ vom Grad 35 für $l \in \{491, 631, 5531\}$. Letztlich unbeantwortet bleibt die Frage nach der Galoismodulstruktur von $\overline{U}_l$ in 15 Fällen.
Für die Rechnungen in unseren Folgerungen verwenden wir das Computeralgebrasystem PARI/GP [PARI] und einen gängigen PC mit zwei Prozessorkernen (Taktfrequenz jeweils 2.26 GHz) und 4 GB Arbeitsspeicher. Die numerischen Ergebnisse zu Kapitel 3 und Kapitel 4 sind in Anhang A beziehungsweise Anhang C zu finden, die zugehörigen PARI/GP-Skripte in Anhang B beziehungsweise Anhang D.

Danksagung

Als erstes möchte ich meinem Betreuer, Prof. Dr. Cornelius Greither, meinen ganz herzlichen Dank aussprechen. Er hat mich mit bewundernswerter Geduld an dieses Forschungsgebiet herangeführt, mir in zahlreichen Gesprächen wertvolle Ratschläge gegeben und dadurch diese Arbeit überhaupt möglich gemacht.
Prof. Dr. Werner Bley danke ich vielmals für die Übernahme des Zweitgutachtens.
Für die angenehme Arbeitsatmosphäre, inklusive mancher auflockernder, nicht ganz so ernst gemeinten Diskussion, danke ich allen Mitarbeitern des Instituts für Theoretische Informatik und Mathematik. Meinem Kollegen Dr. Sebastian Petersen gilt mein zusätzlicher Dank für einige konstruktive Gespräche und das Teilen seiner Erfahrungen mit dem Promotionsprozess.
Weiter danke ich Prof. Cristian Popescu für eine hilfreiche Diskussion über Kohomologiegruppen, die wir zu Beginn meiner Promotionszeit führten.
Lieber Dank gilt auch meiner Familie und meiner Freundin Susanne für die stete Unterstützung, die mir gerade bei der Überwindung lokaler Minima sehr geholfen hat und für das Verständnis, das sie mir durchgehend entgegenbrachten. Zusätzlich danke ich meiner Schwester für das Korrekturlesen dieser Arbeit. Erfreulich zu bemerken ist insbesondere, dass auf diese Weise eine eher unangenehme Körperweiterung doch noch ihrer Bestimmung als Körpererweiterung nachgehen konnte.

Kapitel 1

Grundlagen

1.1 Homologische Algebra

Zur Untersuchung der l-Einheiten auf Projektivität benötigen wir einige grundlegende Aussagen aus dem Bereich der Gruppenkohomologie. Dazu führen wir einige wichtige Begriffe ein. Diesem Abschnitt liegen vor allem [Gr07], [Mil08], [BIV89] und [Rup95] zu Grunde.
Im weiteren Verlauf sei R ein kommutativer Ring mit Einselement.

Definition 1.1. Eine Folge von R-Moduln $(M_i)_{i\in\mathbb{Z}}$ zusammen mit Homomorphismen $(m_i)_{i\in\mathbb{Z}}$

$$\ldots \to M_{i+1} \overset{m_{i+1}}{\to} M_i \overset{m_i}{\to} M_{i-1} \to \ldots,$$

so dass $\mathrm{Im}(m_{i+1}) \subset \ker(m_i)$, d.h. $m_i \circ m_{i+1} = 0$, gilt, bezeichnet man als *Kettenkomplex* $M_\bullet$. *Analog dazu besteht ein Kokettenkomplex* $M^\bullet$ *aus* R*-Moduln* $(M^i)_{i\in\mathbb{Z}}$ *und Homomorphismen* $(m^i)_{i\in\mathbb{Z}}$

$$\ldots \to M^{i-1} \overset{m_i}{\to} M^i \overset{m_{i+1}}{\to} M^{i+1} \to \ldots,$$

so dass $\mathrm{Im}(m^i) \subset \ker(m^{i+1})$. *Die* i*-te Homologie eines Kettenkomplexes* $M_\bullet$ *ist dann definiert als*

$$H_i(M_\bullet) := \frac{\ker(m_i)}{\mathrm{Im}(m_{i+1})},$$

die i*-te Kohomologie eines Kokettenkomplexes* $M^\bullet$ *als*

$$H^i(M^\bullet) := \frac{\ker(m_{i+1})}{\mathrm{Im}(m_i)}.$$

Bemerkung. Oft werden auch nur einseitige (Ko-)Kettenkomplexe der Form

$$\ldots \to M_{i+1} \overset{m_{i+1}}{\to} M_i \to \ldots \to M_0 \to 0$$

bzw.

$$0 \to M^0 \to \ldots \to M_i \overset{m_{i+1}}{\to} M_{i+1} \to \ldots$$

betrachtet.

Definition 1.2. Sei M ein R-Modul. Eine exakte Sequenz

$$\ldots \to P_{i+1} \to P_i \to \ldots \to P_0 \to M \to 0$$

projektiver R-Moduln $(P_i)_{i\geq 0}$ heißt *projektive Auflösung von M. Analog bezeichnet man eine exakte Sequenz*

$$0 \to M \to I_0 \to I_1 \to \ldots$$

mit injektiven R-Moduln $(I_i)_{i\geq 0}$ als injektive Auflösung von M.

Satz 1.3. *Sei R ein kommutativer Ring und M ein R-Modul. Dann gibt es sowohl eine projektive als auch eine injektive Auflösung von M.*

Beweis. [BIV89, 3.14 a), 13.6] □

Betrachtet man eine projektive Auflösung eines Moduls M wie in obiger Definition und einen kovarianten additiven rechtsexakten Funktor F, so ist

$$\ldots \to F(P_{i+1}) \to F(P_i) \to \ldots \to F(P_0) \to 0$$

nicht notwendig exakt, aber zumindest ein Kettenkomplex $F(P_\bullet)$. Man definiert die *linksabgeleiteten Funktoren von F*, L_iF, durch

$$L_iF(M) := H_i(F(P_\bullet)).$$

Ähnliches gilt für eine injektive Auflösung von M und einen kovarianten additiven linksexakten Funktor F'. Die injektive Auflösung bleibt im Allgemeinen unter F' nicht exakt, aber

$$0 \to F'(I_0) \to F'(I_1) \to \ldots$$

bildet einen Kokettenkomplex $F'(I^\bullet)$ und man definiert die *rechtsabgeleiteten Funktoren*, R^iF', durch

$$R^iF'(M) := H^i(F'(I^\bullet)).$$

Proposition 1.4. *In obiger Situation sind die links- bzw. rechtsabgeleiteten Funktoren von der Wahl der projektiven bzw. injektiven Auflösung von M unabhängig.*

Beweis. [Gr07, Proposition 3.1 und Proposition 3.5]. □

Satz 1.5. *Sei F ein rechtsexakter, F' ein linksexakter kovarianter additiver Funktor auf der Kategorie der R-Moduln Mod_R. Für die links- bzw. rechtsabgeleiteten Funktoren L_iF bzw. R^iF' gelten die folgenden Aussagen:*

a) Für alle R-Moduln M gilt $L_0F(M) \cong F(M)$.

b) Ist P ein projektiver R-Modul, so gilt $L_iF(P) = 0$ für alle $i > 0$.

c) Sei $0 \to M_1 \to M_2 \to M_3 \to 0$ exakt. Dann gibt es eine lange exakte Sequenz

$$\begin{aligned} \ldots \to L_iF(M_1) &\to L_iF(M_2) \to L_iF(M_3) \\ &\to L_{i-1}F(M_1) \to \ldots \to L_0F(M_3) \to 0. \end{aligned}$$

d) Für alle R-Moduln M gilt $R_0F'(M) \cong F'(M)$.

e) Ist J ein injektiver R-Modul, so ist $R^iF'(J) = 0$ für alle $i > 0$.

f) Sei $0 \to M_1 \to M_2 \to M_3 \to 0$ exakt. Dann gibt es eine lange exakte Sequenz

$$0 \to R^0F'(M_1) \to R^0F'(M_2) \to R^0F'(M_3) \to R^1F'(M_3) \to \ldots .$$

Beweis. Für linksabgeleitete Funktoren siehe [Gr07, Theorem 3.2], für rechtsabgeleitete Funktoren [Gr07, Theorem 3.6] □

Auf ganz ähnliche Weise kann man auch abgeleitete Funktoren kontravarianter Funktoren definieren. Wir verzichten an dieser Stelle darauf.

Bemerkung. Bekanntlich sind für einen R-Modul N die kovarianten Funktoren $\mathrm{Hom}(N, \cdot)$ und $\cdot \otimes_R N$ links- bzw. rechtsexakt. Damit können Funktoren

$$\mathrm{Ext}^i_R(N, \cdot) := R^i\mathrm{Hom}(N, \cdot) \text{ und } \mathrm{Tor}^R_i(\cdot, N) := L_i \cdot \otimes_R N$$

und daraus wiederum Bifunktoren $\mathrm{Ext}^i_R(\cdot, \cdot)$ bzw. $\mathrm{Tor}^R_i(\cdot, \cdot)$ für $i \geq 0$ definiert werden. Wir fassen noch einige Eigenschaften von Ext^i_R zusammen (siehe beispielsweise [BIV89, §13]).

a) $\mathrm{Ext}^0_R(M, N) = \mathrm{Hom}_R(M, N)$ für alle R-Moduln M und N.

b) Für einen injektiven R-Modul I gilt $\mathrm{Ext}^i_R(M, I) = 0$ für alle R-Moduln M und alle $i \geq 1$.

c) Ist P ein projektiver R-Modul, so ist $\mathrm{Ext}^i_R(P, M) = 0$ für alle R-Moduln M und alle $i > 0$.

d) Sei $0 \to M_1 \to M_2 \to M_3 \to 0$ eine exakte Sequenz von R-Moduln und N ein weiterer R-Modul. Dann gibt es lange exakte Sequenzen

$$\begin{aligned} \mathrm{Ext}^0_R(M_3, N) &\to \ldots \to \mathrm{Ext}^i_R(M_3, N) \to \mathrm{Ext}^i_R(M_2, N) \\ &\to \mathrm{Ext}^i_R(M_1, N) \to \mathrm{Ext}^{i+1}_R(M_3, N) \to \ldots \end{aligned}$$

und

$$\begin{aligned} \mathrm{Ext}^0_R(N, M_1) &\to \ldots \to \mathrm{Ext}^i_R(N, M_1) \to \mathrm{Ext}^i_R(N, M_2) \\ &\to \mathrm{Ext}^i_R(N, M_3) \to \mathrm{Ext}^{i+1}_R(N, M_1) \to \ldots . \end{aligned}$$

Nun sei G eine Gruppe, Mod_G die Kategorie der G-Moduln, Ab die Kategorie der abelschen Gruppen und $Q_{M,G}$ die von $\{gm - m \mid m \in M, g \in G\}$ erzeugte Untergruppe eines G-Moduls M.

Definition 1.6. Mit Hilfe des linksexakten kovarianten additiven Funktors

$$\cdot^G : Mod_G \to Ab, M \mapsto M^G := \{m \in M \mid gm = m \text{ für alle } g \in G\}$$

definiert man für einen G-Modul M

$$R^i \cdot^G (M) =: H^i(G, M)$$

die *i-te Kohomologiegruppe von G mit Koeffizienten in M. Analog wird durch*

$$L_i \cdot_G (M) =: H_i(G, M)$$

die i-te Homologiegruppe von G mit Koeffizienten in M definiert, wobei $\cdot_G$ der rechtsexakte kovariante additive Funktor

$$\cdot_G : Mod_G \to Ab, M \mapsto M_G := M/Q_{M,G}$$

ist.

Man stellt fest, dass die (Ko-)Homologiegruppen

$$H^i(G, M) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M) \text{ und } H_i(G, M) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(G, M)$$

für $i \geq 0$ erfüllen. Mit Satz 1.5 erhält man für die 0-ten (Ko-)Homologiegruppen

$$H_0(G, M) = M/I_G M \quad \text{und } H^0(G, M) = M^G,$$

wobei $I_G \subset \mathbb{Z}[G]$ das Augmentationsideal, also der Kern der Augmentationsabbildung

$$\text{aug} : \mathbb{Z}[G] \to \mathbb{Z}, \sum_{\sigma \in G} a_\sigma \sigma \mapsto \sum_{\sigma \in G} a_\sigma$$

ist. Agiert G trivial auf M, so gilt zudem (siehe [Mil08, II, Example 1.18])

$$H^1(G, M) = \text{Hom}(G, M).$$

Satz 1.7. *Sei G eine endliche Gruppe. Dann gelten die folgenden Aussagen:*

a) Sei $0 \to M_1 \to M_2 \to M_3 \to 0$ eine exakte Sequenz von G-Moduln. Dann gibt es lange exakte Sequenzen

$$0 \to H^0(G, M_1) \to H^0(G, M_2) \to H^0(G, M_3) \to H^1(G, M_1) \to \dots$$

und

$$\dots \to H_1(G, M_3) \to H_0(G, M_1) \to H_0(G, M_2) \to H_0(G, M_3) \to 0.$$

b) Für alle G-Moduln M und $i \geq 1$ gilt $|G| \cdot H^i(G, M) = 0$.

c) Sei $M = \oplus_{j=1}^r M_{p_j}$ ein endlicher G-Modul, wobei die p_j paarweise verschiedene Primzahlen sind und $|M_{p_j}| = p_j^{e_j}$ mit $e_j \geq 1$. Dann gilt

$$H^i(G, M) \cong \oplus_{j=1}^r H^i(G, M_{p_j}) \text{ für alle } i \geq 1.$$

d) Sei M ein G-Modul, p prim und $r \geq 1$ derart, dass $p^r M = 0$ ist, so gilt $p^r \cdot H^i(G, M) = 0$ für alle $i \geq 1$.

e) Sei M ein endlicher G-Modul. Dann gilt $|M| \cdot H^i(G, M) = 0$ für alle $i \geq 1$.

f) Sei M ein endlicher G-Modul mit $\text{ggT}(|G|, |M|) = 1$.
Dann gilt $H^i(G, M) = 0$ für alle $i \geq 1$.

Beweis. a) Folgt direkt aus der Definition und Satz 1.5.

b) [Mil08, II, Corollary 1.31].

c) [Cob55, Lemma 2].

d) [Cob55, Theorem 4].

e) Folgt direkt aus c) und d).

f) Folgt aus b) und e).

□

Wir führen jetzt die *Tate-Kohomologie* ein. Für die Konstruktion der Tate-Kohomologie aus der oben definierten Homologie und Kohomologie verweisen wir auf [Mil08, II, Abschnitt 3].

Definition 1.8. Sei G eine endliche abelsche Gruppe und $N_G := \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ das *Normelement* und $I_G \subset \mathbb{Z}[G]$ das Augmentationsideal. Für einen G-Modul M und $i \in \mathbb{Z}$ definiert man die *i-te Tate-Kohomologiegruppe von G mit Koeffizienten in M* durch

$$\hat{H}^i(G, M) := \begin{cases} H^i(G, M) & \text{für } i \geq 1 \\ M^G / N_G(M) & \text{für } i = 0 \\ \ker(N_G)/I_G M & \text{für } i = -1 \\ H_{-i-1}(G, M) & \text{für } i \leq -2. \end{cases}$$

M wird *kohomologisch trivial* genannt, wenn $\hat{H}^i(H, M) = 0$ für alle $i \in \mathbb{Z}$ und alle Untergruppen $H \subseteq G$ gilt.

Satz 1.9. *Sei*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

eine exakte Sequenz von G-Moduln. Dann erhält man eine lange exakte Sequenz

$$\ldots \hat{H}^i(G, M_1) \to \hat{H}^i(G, M_2) \to \hat{H}^i(G, M_3) \to \hat{H}^{i+1}(G, M_1) \to \ldots$$

Beweis. [Mil08, II, Abschnitt 3] □

In dieser Arbeit werden wir hauptsächlich G-Moduln für endliche *zyklische* Gruppen G betrachten. Die Tate-Kohomologie hat in diesem Fall eine besonders angenehme Eigenschaft.

Proposition 1.10. *Sei G eine endliche zyklische Gruppe und M ein G-Modul. Dann gibt es für alle $i \in \mathbb{Z}$ einen Isomorphismus*

$$\hat{H}^i(G, M) \cong \hat{H}^{i+2}(G, M).$$

Beweis. [Mil08, II, Proposition 3.4]. □

Diese Proposition ermöglicht sofort die Übertragung der Ergebnisse aus Satz 1.7 auf die Tate-Kohomologie bezüglich endlicher zyklischer Gruppen.

Satz 1.11. *Sei G eine endliche zyklische Gruppe. Es gelten die folgenden Aussagen:*

a) Für alle G-Moduln M und $i \in \mathbb{Z}$ gilt $|G| \cdot \hat{H}^i(G, M) = 0$.

b) Sei $M = \oplus_{j=1}^{r} M_{p_j}$ ein endlicher G-Modul, wobei die p_j paarweise verschiedene Primzahlen sind und $|M_{p_j}| = p_j^{e_j}$ mit $e_j \geq 1$. Dann gilt

$$\hat{H}^i(G, M) \cong \oplus_{j=1}^{r} \hat{H}^i(G, M_{p_j}) \text{ für alle } i \in \mathbb{Z}.$$

c) Sei M ein G-Modul, p prim und $r \geq 1$ derart, dass die Ordnung aller $m \in M$ p^r teilt, so gilt $p^r \cdot \hat{H}^i(G, M) = 0$ für alle $i \in \mathbb{Z}$.

d) Sei M ein endlicher G-Modul. Dann gilt $|M| \cdot \hat{H}^i(G, M) = 0$ für alle $i \in \mathbb{Z}$.

e) Sei M ein endlicher G-Modul mit $\mathrm{ggT}(|G|, |M|) = 1$.
Dann gilt $\hat{H}^i(G, M) = 0$ für alle $i \in \mathbb{Z}$.

□

Die Aussagen von Satz 1.7 lassen sich, wie viele andere Eigenschaften der ursprünglichen (Ko-)Homologie auch, in allgemeiner Form auf die Tate-Kohomologie übertragen. Für diese Arbeit genügt uns jedoch die Betrachtung dieser speziellen Situation.
Zum Ende dieses Abschnitts soll noch ein Satz formuliert werden, der kohomologische Trivialität mit $\mathbb{Z}[G]$-Projektivität verbindet.

Satz 1.12. *Sei G eine endliche Gruppe und M ein $\mathbb{Z}[G]$-Modul. Ist M $\mathbb{Z}[G]$-projektiv, so ist M kohomologisch trivial. Ist M kohomologisch trivial und zudem $\mathbb{Z}$-frei, so ist M sogar $\mathbb{Z}[G]$-projektiv.*

Beweis. [Brw82, Seite 148 und Kapitel VI, (8.10) Theorem] □

1.2 Pullback und Mayer-Vietoris-Sequenz

In diesem Abschnitt führen wir Pullback-Diagramme und eine damit verbundene spezielle Form der Mayer-Vietoris Sequenz ein. Eine detaillierte Behandlung dieses Stoffes ist in den Büchern von Silvester [Sil81] und Milnor [Mln71], die auch die Grundlage für diesen Abschnitt bilden, zu finden. Wir beginnen mit einer

Proposition 1.13. *Sei R ein kommutativer Ring und M ein R-Modul. Dann sind die folgenden Aussagen äquivalent:*

a) M ist ein endlich erzeugter projektiver R-Modul von konstantem Rang 1.

b) Es gilt $M^{dual} \otimes_R M \cong R$, wobei $M^{dual} := \mathrm{Hom}_R(M, R)$.

c) Es gibt einen R-Modul N mit $N \otimes_R M \cong R$.

Beweis. [Sil81, Proposition 21] □

Definition 1.14. Einen R-Modul M, der die Eigenschaften aus Proposition 1.13 hat, nennt man *invertierbar*.

Für einen invertierbaren R-Modul M bezeichne $[M]$ die Isomorphie-Klasse von M. Sind M und N zwei invertierbare R-Moduln, so ist bekanntlich auch $M \otimes_R N$ invertierbar. Damit wird durch

$$[M] \cdot [N] := [M \otimes_R N]$$

eine Multiplikation definiert, mit der die Menge der Isomorphie-Klassen invertierbarer R-Moduln zu einer Gruppe wird. Diese Gruppe wird als *Picardgruppe von R*, kurz $\mathrm{Pic}(R)$, bezeichnet. Wir bemerken noch, dass $[R]$ das neutrale Element von $\mathrm{Pic}(R)$ ist und die Inversen durch $[M]^{-1} = [M^{dual}]$ gegeben sind.
Sei nun ein kommutatives Diagramm

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow{j_1} & S \end{array}$$

von Ringen R, R_1, R_2 und S und Ringhomomorphismen i_1, i_2, j_1 und j_2 gegeben. Dieses Diagramm wird als *Pullback-Diagramm* oder auch *kartesisches Quadrat* bezeichnet, wenn es für jedes Paar $(r_1, r_2) \in R_1 \times R_2$ mit $j_1(r_1) = j_2(r_2)$ genau ein $r \in R$ mit $i_1(r) = r_1$ und $i_2(r) = r_2$ gibt.
Eine einfache Art eines Pullback-Diagramms liefert folgendes bekanntes

Lemma 1.15. *Sei R ein kommutativer Ring und seien $I, J \subset R$ Ideale. Dann ist*

$$\begin{array}{ccc} R/(I \cap J) & \xrightarrow[i_2]{} & R/J \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ R/I & \xrightarrow{j_1} & R/(I+J), \end{array}$$

wobei alle Abbildungen die kanonischen (surjektiven) Ringhomomorphismen sind, ein Pullback-Diagramm. □

Beispiel 1. Sei q eine Primzahl, $R = \mathbb{Z}[x]$, $I = (x-1)$ und $J = (\phi_q(x))$ das vom q-ten Kreisteilungspolynom $\phi_q(x) = \sum_{i=0}^{q-1} x^i$ erzeugte Ideal. Es ist klar, dass $I \cap J = ((x-1) \cdot \phi_q(x)) = (x^q - 1)$ gilt. Des Weiteren gilt wegen

$$q = \phi_q(x) - (x-1) \cdot \sum_{i=0}^{q-2} (q-1-i)x^i$$

offensichtlich

$$(q, x-1) = (x-1, \phi_q(x)) = I + J.$$

Man erhält also nach Lemma 1.15 ein Pullback-Diagramm

$$\begin{array}{ccc} \mathbb{Z}[x]/(x^q-1) & \xrightarrow[i_2]{} & \mathbb{Z}[x]/(\phi_q(x)) \cong \mathbb{Z}[\zeta_q] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z} \cong \mathbb{Z}[x]/(x-1) & \xrightarrow{j_1} & \mathbb{Z}[x]/(q, x-1) \cong \mathbb{F}_q, \end{array}$$

wobei ζ_q eine primitive q-te Einheitswurzel ist. Wir möchten dieses Beispiel noch etwas erweitern. Für $2 \leq m \in \mathbb{Z}$ bezeichne $G_m = \langle \sigma_m \rangle$ eine zyklische Gruppe der Ordnung m. Sei $\delta \geq 2$ eine ganze Zahl, die zu q teilerfremd ist. Dann wird durch $\sigma_{q\delta} \mapsto \sigma_q \cdot \sigma_\delta$ ein Isomorphismus

$$\mathbb{Z}[G_{q\delta}] \cong \mathbb{Z}[G_q][G_\delta]$$

definiert, dessen Umkehrung durch $\sigma_q^i \cdot \sigma_\delta^j \mapsto \sigma_{q\delta}^{\varphi^{-1}(i,j)}$ gegeben ist. Dabei ist $\varphi : \mathbb{Z}/q\delta\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/\delta\mathbb{Z}$ der Isomorphismus aus dem Chinesischen

Restsatz. Zusammen mit Obigem erhalten wir das nachfolgende Pullback-Diagramm

$$\begin{array}{ccc} \mathbb{Z}[G_{q\delta}] \cong \mathbb{Z}[G_\delta][G_q] & \xrightarrow[i_2]{} & \mathbb{Z}[\zeta_q][G_\delta] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z}[G_\delta] & \xrightarrow{j_1} & \mathbb{F}_q[G_\delta]. \end{array}$$

Jetzt soll die Verbindung von Pullback-Diagrammen und projektiven Moduln erläutert werden. Sei dazu $f : A \to B$ ein Ringhomomorphismus und M ein A-Modul. Dann ist $B \otimes_A M$ ein A-Modul und mit Hilfe von

$$b_1(b_2 \otimes m) = b_1 b_2 \otimes m \text{ für } b_1, b_2 \in B \text{ und } m \in M$$

ein B-Modul. Wir schreiben statt $B \otimes_A M$ auch $f_\# M$. Die kanonische Abbildung

$$M \to f_\# M, m \mapsto 1 \otimes_A m$$

bezeichnen wir wieder mit f.
Im weiteren Verlauf sei j_2 stets surjektiv. Weiter seien ein Pullback-Diagramm wie oben und über R_1 beziehungsweise R_2 endlich erzeugte projektive Moduln P_1 und P_2 gegeben. Gibt es einen S-Isomorphismus

$$h : j_{1\#} P_1 \to j_{2\#} P_2,$$

so wird

$$M := (P_1, P_2, h) := \{(p_1, p_2) \mid h(j_1(p_1)) = j_2(p_2)\}$$

durch

$$r(p_1, p_2) := (i_1(r)p_1, i_2(r)p_2) \text{ für } r \in R$$

zu einem R-Modul. Diese Konstruktion hat bemerkenswerte Eigenschaften, von denen wir einige zusammenfassen zu einem

Satz 1.16. *Unter den obigen Voraussetzungen gelten die folgenden Aussagen:*

a) Der Modul $M = (P_1, P_2, h)$ ist ein endlich erzeugter projektiver R-Modul.

b) Jeder endlich erzeugte projektive R-Modul M ist isomorph zu einem durch obige Konstruktion entstandenen Modul (P_1, P_2, h).

c) Sei $M = (P_1, P_2, h)$. Dann gilt $P_1 \cong i_{1\#} M$ und $P_2 \cong i_{2\#} M$.

d) $M = (P_1, P_2, h)$ *ist genau dann ein invertierbarer* R*-Modul, wenn* P_1 *invertierbarer* R_1*-Modul und* P_2 *invertierbarer* R_2*-Modul ist.*

Beweis. a) [Sil81, Proposition 59]

b) [Sil81, Proposition 60]

c) [Sil81, Proposition 61]

d) [Sil81, Corollary 65]

□

Satz 1.17. *Sei*

$$\begin{array}{ccc} R & \xrightarrow[i_2]{} & R_2 \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow{j_1} & S \end{array}$$

ein Pullback-Diagramm. Mit folgenden Abbildungen

$f_1(r) = (i_1(r), i_2(r))$ *für* $r \in R^\star$,

$g_1(r_1, r_2) = j_1(r_1) \cdot (j_2(r_2))^{-1}$ *für* $r_1 \in R_1^\star, r_2 \in R_2^\star$,

$\rho(s) = (R_1, R_2, s)$ *für* $s \in S^\star$,

$f_0((P_1, P_2, h)) = ([P_1], [P_2])$ *für alle invertierbaren* R*-Moduln* (P_1, P_2, h),

$g_0(([P_1], [P_2])) = [j_{1\#}P_1][j_{2\#}P_2]^{-1}$ *für invertierbare Moduln* P_1 *über* R_1 *und* P_2 *über* R_2,

ist die Sequenz

$$R^\star \xrightarrow{f_1} R_1^\star \oplus R_2^\star \xrightarrow{g_1} S^\star \xrightarrow{\rho} \mathrm{Pic}(R) \xrightarrow{f_0} \mathrm{Pic}(R_1) \oplus \mathrm{Pic}(R_2) \xrightarrow{g_0} \mathrm{Pic}(S)$$

exakt. Diese Sequenz wird Mayer-Vietoris-Sequenz genannt.

Beweis. [Sil81, Propostion 66] □

Bemerkung. Insbesondere ist nach Satz 1.16 d) $\rho(s) = (R_1, R_2, s)$ für $s \in S^\star$ ein invertierbarer R-Modul.

In Kapitel 4 benötigen wir die Techniken dieses Abschnittes in einer sehr speziellen Form unter anderem für den Nachweis der Nichtfreiheit bestimmter Moduln. Dieser für uns relevante Spezialfall soll zum Abschluß dieses Kapitels diskutiert werden:

Beispiel 2. Gegeben sei ein Pullback-Diagramm

$$\begin{array}{ccc} R & \xrightarrow{i_2} & R_2 \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ R_1 & \xrightarrow{j_1} & S, \end{array}$$

wobei wir R durchgehend mit $\{(r_1, r_2) \in R_1 \times R_2 \mid j_1(r_1) = j_2(r_2)\}$ identifizieren. Seien $\eta_1 \in R_1$ und $\eta_2 \in R_2$ so, dass $j_1(\eta_1), j_2(\eta_2) \in S^\star$ gilt. Zusätzlich sei $X \subset R$ ein projektives Ideal mit $i_1(X) = (\eta_1)$ und $i_2(X) = (\eta_2)$ und

$$\tilde{X} = \{(r_1, r_2) \in (\eta_1) \times (\eta_2) \mid j_1(r_1) = j_2(r_2)\} \subset R.$$

Wir zeigen jetzt, dass

$$X \cong \tilde{X} \cong (R_1, R_2, j_1(\eta_1)/j_2(\eta_2))$$

gilt.

1.) Für die erste Isomorphie bemerken wir zuerst, dass offensichtlich

$$X \subset \tilde{X}$$

gilt. Sei nun $\mathfrak{p} \subset R$ prim und $(a, b) \in \tilde{X}$. Lokalisierungen nach $\mathfrak{p}$ machen wir durch einen entsprechenden Index deutlich. Somit ist $X_\mathfrak{p}$ frei über $R_\mathfrak{p}$, es gibt also $(\alpha, \beta) \in R_\mathfrak{p}$ mit $X_\mathfrak{p} = (\alpha, \beta)R_\mathfrak{p}$. Da $\eta_1 \in i_{1,\mathfrak{p}}(X_\mathfrak{p})$ und $\eta_2 \in i_{2,\mathfrak{p}}(X_\mathfrak{p})$ ist, gibt es $r_1 \in (R_1)_\mathfrak{p}$ und $r_2 \in (R_2)_\mathfrak{p}$ mit

$$\eta_1 = r_1\alpha \text{ und } \eta_2 = r_2\beta.$$

Auf Grund der Invertierbarkeit von $j_{1,\mathfrak{p}}(\eta_1) = j_{1,\mathfrak{p}}(r_1)j_{1,\mathfrak{p}}(\alpha)$ und $j_{1,\mathfrak{p}}(\eta_2) = j_{2,\mathfrak{p}}(r_2)j_{2,\mathfrak{p}}(\beta)$ in $S_\mathfrak{p}$ muss auch $j_{1,\mathfrak{p}}(\alpha) = j_{2,\mathfrak{p}}(\beta)$ invertierbar sein. Für $(a, b) \in \tilde{X}_\mathfrak{p}$ gibt es $s_1 \in (R_1)_\mathfrak{p}$ und $s_2 \in (R_2)_\mathfrak{p}$ derart, dass

$$a = s_1\eta_1 \text{ und } b = s_2\eta_2, \text{ also } a = s_1r_1\alpha \text{ und } b = s_2r_2\beta$$

gilt. Nach Voraussetzung ist also

$$j_{1,\mathfrak{p}}(s_1r_1)j_{1,\mathfrak{p}}(\alpha) = j_{1,\mathfrak{p}}(a) = j_{2,\mathfrak{p}}(b) = j_{2,\mathfrak{p}}(\beta)j_{2,\mathfrak{p}}(s_2r_2),$$

woraus $(s_1r_1, s_2r_2) \in R_\mathfrak{p}$ folgt. Somit ist

$$(a, b) = (s_1r_1, s_2r_2)(\alpha, \beta) \in R_\mathfrak{p}(\alpha, \beta) = X_\mathfrak{p}.$$

2.) Nach Voraussetzung wird durch Multiplikation mit $j_1(\eta_1)/j_2(\eta_2)$ ein Isomorphismus $S \to S$ definiert. Damit liefert die Hintereinanderschaltung der Isomorphismen

$$\begin{array}{ll} S \otimes_{j_1} R_1 \to S, & s \otimes_{j_1} r_1 \mapsto s j_1(r_1), \\ (\cdot j_1(\eta_1)/j_2(\eta_2)) : S \to S, & s \mapsto s j_1(\eta_1)/j_2(\eta_2) \text{ und} \\ S \to S \otimes_{j_2} R_2, & s \mapsto s \otimes_{j_1} 1 \end{array}$$

einen Isomorphismus

$$h : S \otimes_{j_1} R_1 \to S \otimes_{j_2} R_2.$$

Der projektive R-Modul $(R_1, R_2, h) = (R_1, R_2, j_1(\eta_1)/j_2(\eta_2))$ ist somit durch

$$\begin{aligned} (R_1, R_2, j_1(\eta_1)/j_2(\eta_2)) &= \{(r_1, r_2) \in R_1 \times R_2 \mid h(1 \otimes_{j_1} r_1) = 1 \otimes_{j_2} r_2\} \\ &= \{(r_1, r_2) \in R_1 \times R_2 \mid j_1(r_1)\frac{j_1(\eta_1)}{j_2(\eta_2)} = j_2(r_2)\} \\ &= \{(r_1, r_2) \in R_1 \times R_2 \mid j_1(r_1\eta_1) = j_2(r_2\eta_2)\} \end{aligned}$$

gegeben. Mit

$$\tilde{X} = \{(r_1\eta_1, r_2\eta_2) \in R_1 \times R_2 \mid (r_1, r_2) \in R, j_1(r_1\eta_1) = j_2(r_2\eta_2)\}$$

erhalten wir letztlich die gewünschte Isomorphie

$$\tilde{X} \to (R_1, R_2, j_1(\eta_1)/j_2(\eta_2)), \quad (r_1\eta_1, r_2\eta_2) \mapsto (r_1, r_2).$$

□

Kapitel 2

Kreiszahlen und Kreiseinheiten

In diesem Kapitel beschäftigen wir uns mit der Struktur der Kreiszahlen und der Kreiseinheiten. Dazu sei l eine ungerade Primzahl, $n \in \mathbb{N}$, ζ_{l^n} eine primitive l^n-te Einheitswurzel, $\mathbb{Q}(\zeta_{l^n})^+ = \mathbb{Q}(\zeta_{l^n} + \zeta_{l^n}^{-1})$ der maximal reelle Unterkörper von $\mathbb{Q}(\zeta_{l^n})$ und G die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_{l^n})^+/\mathbb{Q})$.
Wir beginnen mit der grundlegenden

Definition 2.1 (vgl. [Wa97, §8.1])**.** Die *Kreiszahlen* $V = V(l^n)$ *von* $\mathbb{Q}(\zeta_{l^n})$ sind definiert als die multiplikative Gruppe, die von

$$\{\pm\zeta_{l^n}, 1 - {\zeta_{l^n}}^a \mid 1 \leq a \leq l^n - 1\}$$

erzeugt wird. Weiter definieren wir die Kreiszahlen $\mathrm{Cn} = \mathrm{Cn}(l^n)$ von $\mathbb{Q}(\zeta_{l^n})^+$ durch

$$\mathrm{Cn} = V \cap \mathbb{R}$$

und die *Kreiseinheiten* $\mathrm{Cyc}(\mathbb{Q}(\zeta_{l^n})^+)$ *von* $\mathbb{Q}(\zeta_{l^n})^+$ als

$$\mathrm{Cyc} = \mathrm{Cyc}(l^n) = \mathrm{Cyc}(\mathbb{Q}(\zeta_{l^n})^+) = \mathrm{Cn} \cap U.$$

Dabei sei $U = U(l^n) = U(\mathbb{Q}(\zeta_{l^n})^+)$ die Einheitengruppe des Rings der ganzen Zahlen $\mathcal{O}_{\mathbb{Q}(\zeta_{l^n})^+}$ von $\mathbb{Q}(\zeta_{l^n})^+$.

In dieser Arbeit betrachten wir die oben genannten Objekte meist modulo $\mathbb{Z}$-Torsion. Dies machen wir, wie allgemein üblich, durch einen Querbalken kenntlich. Beispielsweise schreiben wir $\overline{U}$ für die Einheiten modulo $\mathbb{Z}$-Torsion.

Bemerkung. Die Kreiszahlen bzw. Kreiseinheiten können analog für $\mathbb{Q}(\zeta_n)$ mit beliebigem $n \not\equiv 2 \mod 4$ eingeführt werden (siehe [Wa97, §8.1]).

Einheiten und Kreiseinheiten von $\mathbb{Q}(\zeta_{l^n})^+$ stehen in engem Zusammenhang mit der Klassenzahl $h_{\mathbb{Q}(\zeta_{l^n})^+} = h_{l^n}^+$ von $\mathbb{Q}(\zeta_{l^n})^+$. Der folgende Satz enthält dieses wohlbekannte und für diese Arbeit grundlegende Resultat.

Satz 2.2 ([Wa97, Theorem 8.2])**.** *Sei l eine Primzahl, $n \geq 1$ und seien* $\mathrm{Cyc}(l^n)$ *die Kreiseinheiten von $\mathbb{Q}(\zeta_{l^n})^+$ und $h_{l^n}^+$ die Klassenzahl von $\mathbb{Q}(\zeta_{l^n})^+$. Dann gilt*

$$[U(l^n) : \mathrm{Cyc}(l^n)] = h_{l^n}^+.$$

□

Da die $\mathbb{Z}$-Torsionsuntergruppen von $U(l^n)$ und $\mathrm{Cyc}(l^n)$ gleich sind, sie bestehen nur aus $+1$ und -1, erhalten wir $U(l^n)/\mathrm{Cyc}(l^n) \cong \overline{U}(l^n)/\overline{\mathrm{Cyc}}(l^n)$ und insbesondere

$$[\overline{U}(l^n) : \overline{\mathrm{Cyc}}(l^n)] = h_{l^n}^+.$$

Lemma 2.3. *Sei H eine endliche abelsche Gruppe, $N_H = \sum_{\sigma \in H} \sigma \in \mathbb{Z}[H]$ das Normelement und I_H das Augmentationsideal. Dann gelten die folgenden Aussagen:*

a) Für alle $\sigma \in H$ gilt $\sigma N_H = N_H$.

b) $\langle N_H \rangle_{\mathbb{Z}[H]} = N_H \cdot \mathbb{Z}$.

c) $I_H = \oplus_{1 \neq \sigma \in H}(\sigma - 1)\mathbb{Z}$, wobei $1 \in H$ das neutrale Element ist. Insbesondere gilt $I_H = \langle \sigma_H - 1 \rangle_{\mathbb{Z}[H]}$, wenn $H = \langle \sigma_H \rangle$ zyklisch ist.

d) Für $\alpha \in \mathbb{Z}[H]$ gilt

$$\sigma\alpha = \alpha \text{ für alle } \sigma \in H \Leftrightarrow \alpha \in \mathbb{Z}[H] \cdot N_H.$$

Beweis. a) Für jedes $\sigma \in H$ ist $\tilde{\sigma} : H \to H, h \mapsto \sigma h$ bijektiv, woraus sofort die Behauptung folgt.

b) Folgt aus a).

c) Sei $\alpha = \sum_{\sigma \in H} a_\sigma \sigma \in I_H$. Somit gilt

$$a_1 = -\sum_{1 \neq \sigma \in H} a_\sigma,$$

also

$$\alpha = a_1 \cdot 1 + \sum_{1 \neq \sigma \in H} a_\sigma \sigma = -\sum_{1 \neq \sigma \in H} a_\sigma + \sum_{1 \neq \sigma \in H} a_\sigma \sigma = \sum_{1 \neq \sigma \in H} a_\sigma(\sigma - 1).$$

Andererseits gilt wegen $\mathrm{aug}(\sigma - 1) = 0$ offensichtlich

$$\oplus_{1 \neq \sigma \in H}(\sigma - 1)\mathbb{Z} \subset I_H.$$

Wir bemerken noch, dass $\sigma^n - 1 = (\sigma - 1)(1 + \ldots + \sigma^{n-1})$ für $n \geq 2$ gilt.

d) Nach a) ist „$\Leftarrow$“ klar. Sei nun $\alpha = \sum_{\sigma\in H} a_\sigma\sigma \in \mathbb{Z}[H]\setminus\{0\}$ mit $\sigma\alpha = \alpha$ für alle $\sigma \in H$ (für $\alpha = 0$ ist nichts zu zeigen). Sei $a_{\sigma_k} \neq 0$. Zu jedem $j \neq k$ gibt es ein k_j, so dass $\sigma_k \cdot \sigma_{k_j} = \sigma_j$ ist. Damit bekommen wir

$$\alpha = \sum_{\sigma\in H} a_\sigma\sigma = \sigma_{k_j}\alpha = \sum_{\sigma\in H} a_\sigma(\sigma_{k_j}\sigma).$$

Koeffizientenvergleich ergibt $a_{\sigma_j} = a_{\sigma_k}$, also $\alpha \in \mathbb{Z}\cdot N_H$.

□

Wir möchten nun die Kreiseinheiten mit dem Augmentationsideal in Verbindung bringen. Dazu benötigen wir noch eine

Proposition 2.4. *Sei l eine ungerade Primzahl, $n \in \mathbb{N}$, g eine Primitivwurzel modulo l^n und ζ eine primitive l^n-te Einheitswurzel. Dann gilt*

$$\langle\eta'\rangle_{\mathbb{Z}[G]} = \overline{\mathrm{Cyc}}, \text{ wobei } \eta' = \zeta^{\frac{1-g}{2}}\frac{1-\zeta^g}{1-\zeta}.$$

Beweis. [Wa97, Prop. 8.11] □

Obwohl einige Aussagen in der allgemeineren Form ebenso gültig wären, beschränken wir uns im weiteren Verlauf auf den Fall $n = 1$ und schreiben auch ζ statt ζ_l. Die Galoisgruppe

$$\begin{aligned} G &:= \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q}) \\ &= \left\{\sigma_a : \zeta+\zeta^{-1} \mapsto \zeta^a+\zeta^{-a} \mid 1 \le a \le \frac{l-1}{2}\right\} \cong (\mathbb{Z}/l\mathbb{Z})^\star/\{\pm 1\} \end{aligned}$$

ist zyklisch und wird von σ_g erzeugt, wobei g wie oben eine Primitivwurzel modulo l ist. Im weiteren Verlauf wählen wir eine beliebige feste Primitivwurzel modulo l aus und schreiben statt σ_g auch σ_G oder σ. Aus $l \equiv 1 \mod 2$ folgt, dass $\sigma_2 \in G$ und damit auch $\sigma_{1/2} \in G$ ist. Zusammen mit

$$\eta' = \zeta^{\frac{1-g}{2}}\frac{1-\zeta^g}{1-\zeta} = \zeta^{\frac{1}{2}}\cdot\zeta^{\frac{-g}{2}}\frac{\zeta^g-1}{\zeta-1} = \frac{\zeta^{\frac{-g}{2}}(\zeta^g-1)}{\zeta^{\frac{-1}{2}}(\zeta-1)} = \frac{\zeta^{\frac{g}{2}}-\zeta^{\frac{-g}{2}}}{\zeta^{\frac{1}{2}}-\zeta^{\frac{-1}{2}}}$$

ergibt sich also, dass für

$$\eta := \eta'^{\sigma_2} = \frac{\zeta^g-\zeta^{-g}}{\zeta-\zeta^{-1}}$$

ebenfalls $\langle\eta\rangle_{\mathbb{Z}[G]} = \overline{\mathrm{Cyc}}$ gilt.

Proposition 2.5. *Es gilt* $\overline{\mathrm{Cyc}} \cong \mathbb{Z}[G]/(N_G) \cong I_G$.

Beweis. Zur ersten Isomorphie betrachten wir

$$\tau : \mathbb{Z}[G] \to \overline{\mathrm{Cyc}}, \alpha \to \eta^\alpha.$$

Aus

$$\eta^{N_G} = \frac{(\zeta^g - \zeta^{-g})^{N_G}}{(\zeta - \zeta^{-1})^{N_G}} = \frac{(\zeta - \zeta^{-1})^{\sigma_g N_G}}{(\zeta - \zeta^{-1})^{N_G}} = \frac{(\zeta - \zeta^{-1})^{N_G}}{(\zeta - \zeta^{-1})^{N_G}} = 1$$

folgt sofort $\overline{\mathrm{Cyc}}^{N_G} = 1$ und damit die Existenz der induzierten Abbildung

$$\overline{\tau} : \mathbb{Z}[G]/(N_G) \to \overline{\mathrm{Cyc}}, \alpha \mapsto \eta^\alpha.$$

Weiter ist $\overline{\tau}$ aufgrund der Surjektivität von τ auch surjektiv. Nach dem Dirichletschen Einheitensatz und Satz 2.2 ist $\overline{\mathrm{Cyc}} \cong \mathbb{Z}^{\frac{l-3}{2}}$ als $\mathbb{Z}$-Modul. Jedoch gilt ebenfalls $\mathbb{Z}[G]/(N_G) \cong \mathbb{Z}[x]/(x^{\frac{l-3}{2}} + \ldots + 1) \cong \mathbb{Z}^{\frac{l-3}{2}}$ (Isomorphie von $\mathbb{Z}$-Moduln). Somit muss $\overline{\tau}$ sogar bijektiv sein.

Die zweite Isomorphie ergibt sich durch Anwendung von Lemma 2.3:

$$\mathbb{Z}[G]/(N_G) \cong \mathbb{Z}[x]/(x^{\frac{l-3}{2}} + \ldots + 1) \cong (x-1)\mathbb{Z}[x]/(x^{\frac{l-1}{2}} - 1) \cong I_G.$$

□

Als nächstes wenden wir uns den Kreiszahlen Cn zu. Sei

$$\lambda^+ := (1 - \zeta)(1 - \zeta^{-1}),$$

wobei ζ eine primitive l-te Einheitswurzel für eine Primzahl $l \neq 2$ ist. In $\mathbb{Q}(\zeta_l)^+$ ist l voll verzweigt und es gilt $(l) = (\lambda^+)^{\frac{l-1}{2}}$. Also ist λ^+ das (bis auf Assoziierte) einzige Primelement von $\mathcal{O}_{\mathbb{Q}(\zeta_l)^+}$ über l. Nach Definition von $\overline{\mathrm{Cn}}$ liegt λ^+ in $\overline{\mathrm{Cn}}$ und man könnte deshalb vermuten, dass dies „schon alles“ ist, also, dass $\overline{\mathrm{Cn}} = \langle \lambda^+ \rangle_{\mathbb{Z}[G]}$ ist. Dies ist allerdings nicht der Fall, wie folgende Proposition zeigt.

Proposition 2.6. *Mit obigen Bezeichnungen gilt*

1.) $\langle \lambda^+ \rangle_{\mathbb{Z}[G]} = (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}}^2$ *und*

2.) $\overline{\mathrm{Cn}} = (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}}$.

Insbesondere folgt, dass $\langle \lambda^+ \rangle_{\mathbb{Z}[G]}$ *und* $\overline{\mathrm{Cn}}$ *freie* $\mathbb{Z}$*-Moduln vom Rang* $\frac{l-1}{2}$ *sind und* $\langle \lambda^+ \rangle_{\mathbb{Z}[G]}$ *aus Ranggründen auch* $\mathbb{Z}[G]$*-frei ist.*

Beweis. 1.) Sei $\alpha \in \mathbb{Z}[G]$ und aug die Augmentationsabbildung. Dann gilt

$$(\lambda^+)^\alpha = (\lambda^+)^{\mathrm{aug}(\alpha)} \cdot (\lambda^+)^{\alpha - \mathrm{aug}(\alpha)},$$

wobei $\alpha - \mathrm{aug}(\alpha)$ offenbar in I_G liegt. Da $I_G = \langle \sigma_g - 1 \rangle_{\mathbb{Z}[G]}$ ist, reicht es somit zu zeigen, dass $\langle (\lambda^+)^{\sigma_g - 1} \rangle_{\mathbb{Z}[G]} = \overline{\mathrm{Cyc}}^2 = \langle \eta'^2 \rangle_{\mathbb{Z}[G]}$ ist:

$$(\lambda^+)^{\sigma_g - 1} = \frac{(1-\zeta^g)(1-\zeta^{-g})}{(1-\zeta)(1-\zeta^{-1})} = \frac{(\zeta^{\frac{g}{2}} - \zeta^{\frac{-g}{2}})^2}{(\zeta^{\frac{1}{2}} - \zeta^{\frac{-1}{2}})^2} = (\eta^{\sigma_{1/2}})^2 = \eta'^2.$$

2.) $\overline{\mathrm{Cn}} \supseteq (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}}$ folgt direkt aus $\lambda^+ \in \overline{\mathrm{Cn}}$ und $\overline{\mathrm{Cyc}} \subset \overline{\mathrm{Cn}}$. Sei nun $\theta \in \overline{\mathrm{Cn}}$. Dann ist $\theta \in \overline{U}_l$ und wegen $(l) = (\lambda^+)^{\frac{l-1}{2}}$ gilt $(\theta) = (\lambda^+)^z$ für ein $z \in \mathbb{Z}$, bzw.

$$\theta = u \cdot (\lambda^+)^z$$

für ein $u \in \overline{U}$ und ein $z \in \mathbb{Z}$. Mit θ und λ^+ muss also auch u in der Gruppe $\overline{\mathrm{Cn}}$ und damit in $\overline{\mathrm{Cyc}} = \overline{\mathrm{Cn}} \cap \overline{U}$ liegen.

□

Die Kreiszahlen werden also über $\mathbb{Z}[G]$ nicht von λ^+ erzeugt. Es stellt sich nun die Frage, ob $\overline{\mathrm{Cn}}$ zumindest in einigen Fällen trotzdem $\mathbb{Z}[G]$-frei ist. Wir suchen dazu nach einem $\alpha \in \mathbb{Q}[G]$, so dass $\langle (\lambda^+)^\alpha \rangle_{\mathbb{Z}[G]} = \overline{\mathrm{Cn}}$ ist. Einen Hinweis für die Suche liefert die Bedingung $\alpha^{-1} \in \mathbb{Z}[G]$, um sicherzustellen, dass λ^+ in $\langle (\lambda^+)^\alpha \rangle_{\mathbb{Z}[G]}$ liegt.

Satz 2.7. *Sei $l \equiv 3 \mod 4$ prim, σ ein Erzeuger von $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$, $\alpha = \frac{1+\sigma}{2} \in \mathbb{Q}[G]$ und $\gamma = (\lambda^+)^\alpha$. Dann gilt für die Kreiszahlen* Cn *von $\mathbb{Q}(\zeta_l)^+$*

$$\overline{\mathrm{Cn}} = \langle \gamma \rangle_{\mathbb{Z}[G]}.$$

Beweis. 1.) Nach dem Beweis von Prop. 2.6 ist $(\lambda^+)^{\sigma-1} \in \overline{\mathrm{Cyc}}^2$. Damit gilt

$$(\lambda^+)^\alpha = \lambda^+ \cdot (\lambda^+)^{\frac{\sigma-1}{2}} = \lambda^+ \cdot ((\lambda^+)^{\sigma-1})^{\frac{1}{2}} \in (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}},$$

also $\langle (\lambda^+)^\alpha \rangle_{\mathbb{Z}[G]} \subseteq (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}}$.

2.) Für die andere Inklusion benötigen wir zunächst:

i.) $\tilde{\alpha} := \sum_{i=0}^{l-1} (-1)^i \sigma^i \in \mathbb{Z}[G]$ erfüllt $\tilde{\alpha} \cdot \alpha = 1$, denn

$$\begin{aligned}
\left(\sum_{i=0}^{l-1} (-1)^i \sigma^i \right) \cdot \left(\frac{1+\sigma}{2} \right) &= \frac{1}{2} \left(\sum_{i=0}^{l-1} (-1)^i \sigma^i + \sum_{i=0}^{l-1} (-1)^i \sigma^{i+1} \right) \\
&= \frac{1}{2} \left(\sum_{i=0}^{l-1} (-1)^i \sigma^i + \sum_{i=1}^{l} (-1)^{i-1} \sigma^i \right) \\
&= 1.
\end{aligned}$$

ii.) $\tilde{\alpha}_N := -\sum_{i=1}^{(l-1)/2} \sigma^{2i-1} \in \mathbb{Z}[G]$ erfüllt $\tilde{\alpha}_N \cdot (2\alpha) \equiv 1 \mod N_G$, denn

$$\begin{aligned} -\left(\sum_{i=1}^{(l-1)/2} \sigma^{2i-1}\right) \cdot (1+\sigma) &= -\sum_{i=1}^{(l-1)/2} \sigma^{2i-1} - \sum_{i=1}^{(l-1)/2} \sigma^{2i} \\ &= -N_G + 1 \equiv 1 \mod N_G. \end{aligned}$$

Wegen i) ist also

$$\lambda^+ = \left((\lambda^+)^\alpha\right)^{\tilde{\alpha}} \in \left\langle (\lambda^+)^\alpha \right\rangle_{\mathbb{Z}[G]}.$$

Aufgrund ii) und Proposition 2.5 gilt

$$(\eta^{1+\sigma})^{\tilde{\alpha}_N} = \eta^{-N_G} \cdot \eta = \eta,$$

d.h.

$$(1+\sigma) : \overline{\mathrm{Cyc}} \to \overline{\mathrm{Cyc}}, \eta \mapsto \eta^{1+\sigma}$$

ist ein Isomorphismus. Wir erhalten

$$(\overline{\mathrm{Cyc}}^2)^\alpha = (\overline{\mathrm{Cyc}})^{1+\sigma} = \overline{\mathrm{Cyc}}$$

und damit $\overline{\mathrm{Cn}} = (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}} \subset \left\langle (\lambda^+)^\alpha \right\rangle_{\mathbb{Z}[G]}$.

□

Da wir eine Isomorphie $\overline{\mathrm{Cn}} \cong \mathbb{Z}^{\frac{l-1}{2}} \cong \mathbb{Z}[G]$ von $\mathbb{Z}$-Moduln haben, bilden die Kreiseinheiten modulo Torsion für $l \equiv 3 \mod 4$ also einen freien $\mathbb{Z}[G]$-Modul. Bevor wir den Strukturssatz für $\overline{\mathrm{Cn}}$ im zweiten Fall, $l \equiv 1 \mod 4$, formulieren, benötigen wir noch einen Hilfssatz.

Lemma 2.8. *Sei H eine endliche zyklische Gruppe, $I_H \subset \mathbb{Z}[H]$ das Augmentationsideal und $J \subseteq H$ eine Untergruppe. Dann gilt*

$$\hat{H}^0(J, I_H) \cong 0 \quad \text{und} \quad \hat{H}^1(J, I_H) = \mathbb{Z}/|J|\mathbb{Z}.$$

Beweis. Aus der Exaktheit von

$$0 \to I_H \to \mathbb{Z}[H] \to \mathbb{Z} \to 0$$

folgt mittels der $\mathbb{Z}[H]$-Projektivität von $\mathbb{Z}[H]$, dass

$$\hat{H}^i(J, \mathbb{Z}) \cong \hat{H}^{i+1}(J, I_H) \text{ für alle } i \in \mathbb{Z}.$$

Nun ist J als Untergruppe von H ebenfalls zyklisch und endlich. Zusammen mit Satz 1.10 und der Trivialität von $\mathbb{Z}$ als J-Modul ergibt sich somit

$$\hat{H}^0(J, I_H) \cong \hat{H}^{-1}(J, \mathbb{Z}) \cong \hat{H}^1(J, \mathbb{Z}) \cong \mathrm{Hom}(J, \mathbb{Z}) = 0.$$

Die Definition von $\hat{H}^1$ und abermals die Endlichkeit von J liefern letztlich

$$\hat{H}^1(J, I_H) \cong \hat{H}^0(J, \mathbb{Z}) \cong \mathbb{Z}^J / N_J\mathbb{Z} = \mathbb{Z}/|J|\mathbb{Z}.$$

□

Satz 2.9. *Sei $l \equiv 1 \mod 4$, $G_u \subset G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ eine Untergruppe ungerader Ordnung, $G_g \subseteq G$ eine Untergruppe gerader Ordnung. Dann gilt*

1.) $\hat{H}^i(G_g, \overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z}$ für alle $i \in \mathbb{Z}$ *und*

2.) $\hat{H}^i(G_u, \overline{\mathrm{Cn}}) = 0$ für alle $i \in \mathbb{Z}$.

Da $|G| = \frac{l-1}{2}$ wegen $l \equiv 1 \mod 4$ gerade ist, folgt aus 1.) insbesondere, dass

$$\hat{H}^i(G, \overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z} \text{ für alle } i \in \mathbb{Z}.$$

Beweis. Zunächst sei $J \subseteq G$ eine beliebige Untergruppe. Wir betrachten die exakte Sequenz

$$1 \to \left\langle \lambda^+ \right\rangle_{\mathbb{Z}[G]} = (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}}^2 \to \overline{\mathrm{Cn}} = (\lambda^+)^{\mathbb{Z}} \cdot \overline{\mathrm{Cyc}} \to I_G/2I_G \to 0,$$

wobei wir $\overline{\mathrm{Cyc}} \cong I_G$ verwenden, und erhalten, da $\langle \lambda^+ \rangle_{\mathbb{Z}[G]}$ $\mathbb{Z}[G]$-frei ist, die exakte Sequenz

$$\begin{aligned} \ldots \to 0 &= \hat{H}^i(J, \left\langle \lambda^+ \right\rangle_{\mathbb{Z}[G]}) \to \hat{H}^i(J, \overline{\mathrm{Cn}}) \\ &\to \hat{H}^i(J, I_G/2I_G) \to \hat{H}^{i+1}(J, \left\langle \lambda^+ \right\rangle_{\mathbb{Z}[G]}) = 0 \to \ldots, \end{aligned}$$

also

$$(\star) \qquad \hat{H}^i(J, \overline{\mathrm{Cn}}) \cong \hat{H}^i(J, I_G/2I_G) \text{ für alle } i \in \mathbb{Z}.$$

Da J zudem zyklisch ist, reicht es somit, die Behauptung für $\hat{H}^i(J, I_G/2I_G)$, $i \in \{0, 1\}$, zu zeigen.
Nun liefert

$$0 \to I_G \xrightarrow{\cdot 2} I_G \to I_G/2I_G \to 0$$

die exakte Sequenz

$$\begin{aligned} \ldots \to \hat{H}^0(J, I_G) &\to \hat{H}^0(J, I_G/2I_G) \to \hat{H}^1(J, I_G) \xrightarrow{\cdot 2} \hat{H}^1(J, I_G) \\ &\to \hat{H}^1(J, I_G/2I_G) \to \hat{H}^2(J, I_G) \to \ldots, \end{aligned}$$

die mit Hilfe von obigem Lemma zu

$$(\star\star) \qquad 0 \to \hat{H}^0(J, I_G/2I_G) \to \mathbb{Z}/|J|\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/|J|\mathbb{Z} \to \hat{H}^1(J, I_G/2I_G) \to 0$$

wird.

1.) Ist $J = G_g$, so gilt

$$\hat{H}^0(G_g, I_G/2I_G) \cong \ker(\cdot 2 : \mathbb{Z}/|G_g|\mathbb{Z} \to \mathbb{Z}/|G_g|\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

und

$$\hat{H}^1(G_g, I_G/2I_G) \cong (\mathbb{Z}/|G_g|\mathbb{Z})/\mathrm{Im}(\cdot 2 : \mathbb{Z}/|G_g|\mathbb{Z} \to \mathbb{Z}/|G_g|\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

2.) Hat $J = G_u$ ungerade Ordnung, so ist die Multiplikation mit 2 bijektiv und $(\star\star)$ ergibt

$$\hat{H}^0(G_u, I_G/2I_G) \cong \ker(\cdot 2 : \mathbb{Z}/|G_u|\mathbb{Z} \to \mathbb{Z}/|G_u|\mathbb{Z}) = 0$$

und

$$\hat{H}^1(G_u, I_G/2I_G) \cong (\mathbb{Z}/|G_u|\mathbb{Z})/\mathrm{Im}(\cdot 2 : \mathbb{Z}/|G_u|\mathbb{Z} \to \mathbb{Z}/|G_u|\mathbb{Z}) \cong 0.$$

□

Wir fassen zusammen: Während die Kreiszahlen modulo Torsion, $\overline{\mathrm{Cn}}(l)$, für $l \equiv 3 \mod 4$ $\mathbb{Z}[G]$-frei sind, so sind sie für $l \equiv 1 \mod 4$ nach Satz 1.12 und Satz 2.9 nicht einmal $\mathbb{Z}[G]$-projektiv. Im nächsten Kapitel benutzen wir diese Ergebnisse zur Untersuchung von $\overline{U}_l$, den l-Einheiten modulo Torsion.

Kapitel 3

Projektivität von $\overline{U}_l$ als $\mathbb{Z}[G]$-Modul

Auch in diesem Kapitel bezeichnet l durchgehend eine ungerade Primzahl, ζ_l eine primitive l-te Einheitswurzel und $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$. Weiter werden wir häufiger diskrete Bewertungen nutzen, für die wir die übliche Notation, v mit entsprechendem Index, verwenden. In Kapitel 2 haben wir bereits bemerkt, dass l in $\mathcal{O}_{\mathbb{Q}(\zeta_l)^+}$ voll verzweigt und

$$(l) = (\lambda^+)^{\frac{l-1}{2}}$$

gilt, wobei $\lambda^+ = (1-\zeta_l)(1-\zeta_l{}^{-1})$ das (bis auf Assoziierte) einzige Primelement von $\mathcal{O}_{\mathbb{Q}(\zeta_l)^+}$ über l ist.

Definition 3.1. Mit obiger Notation definieren wir die *l-Einheiten* in $\mathbb{Q}(\zeta_l)^+$ durch

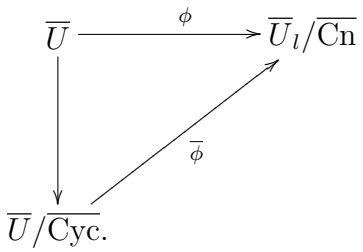
$$U_l := \{\alpha \in \mathbb{Q}(\zeta_l)^+ \mid v_{\mathfrak{p}}(\alpha) = 0 \text{ für alle Primideale } \mathfrak{p} \neq (\lambda^+)\}.$$

Wir bemerken, dass die Kreiszahlen Cn in U_l enthalten sind. Zudem sind die l-Einheiten modulo Torsion nach einer bekannten Verallgemeinerung des Dirichletschen Einheitensatzes $\mathbb{Z}$-frei vom Rang $|G| + 1 = \frac{l-1}{2}$. Sie bilden jedoch offenbar auch einen $\mathbb{Z}[G]$-Modul, so dass sich die natürliche Frage nach der Struktur von $\overline{U}_l$ als $\mathbb{Z}[G]$-Modul ergibt. Ziel dieser Arbeit ist es, möglichst viele Erkenntnisse zu diesem Problem zu gewinnen.
Wir beginnen mit einer kleinen Abwandlung von Satz 2.2, die nötig ist, um einige Ergebnisse aus dem vorherigen Kapitel zur Klassifizierung von $\overline{U}_l$ als $\mathbb{Z}[G]$-Modul verwenden zu können.

Lemma 3.2. *Seien l und ζ_l wie oben und bezeichne h_l^+ die Klassenzahl von $\mathbb{Q}(\zeta_l)^+$. Dann sind $\overline{U}_l/\overline{\mathrm{Cn}}$ und $\overline{U}/\overline{\mathrm{Cyc}}$ isomorphe G-Moduln. Insbesondere gilt*

$$[\overline{U}_l : \overline{\mathrm{Cn}}] = h_l^+.$$

Beweis. Betrachte das Diagramm



Ist $u \in \overline{U}$ mit $\phi(u) = 0$ gegeben, so ist $u \in \overline{\mathrm{Cn}}$ und damit $u \in \overline{U} \cap \overline{\mathrm{Cn}} = \overline{\mathrm{Cyc}}$, woraus sofort die Injektivität von $\overline{\phi}$ folgt. Für $u \in \overline{U}_l$ gilt jedoch $\phi(v) = \overline{u}$, wobei $v = u \cdot (\lambda^+)^{-v_{\lambda^+}(u)} \in \overline{U}$ und $\lambda^+ \in \overline{\mathrm{Cn}}$ ist, was die Surjektivität von $\overline{\phi}$ beweist. □

Nach Satz 1.12 gilt, da $\overline{U}_l$ $\mathbb{Z}$-frei ist, dass

$\overline{U}_l$ genau dann $\mathbb{Z}[G]$-projektiv ist, wenn $\overline{U}_l$ kohomologisch trivial ist.

Diese Äquivalenz werden wir im Folgenden oft gebrauchen.

3.1 1. Fall: $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) = 1$

Aus obigem Lemma wissen wir, dass $\overline{U}_l/\overline{\mathrm{Cn}}$ ein endlicher $\mathbb{Z}[G]$-Modul mit $|\overline{U}_l/\overline{\mathrm{Cn}}| = h_l^+$ ist. Damit kommen wir zu folgendem

Satz 3.3. *Sei $l > 2$ prim und $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) = 1$. Genau dann ist $\overline{U}_l$ $\mathbb{Z}[G]$-projektiv, wenn $l \equiv 3 \mod 4$ ist.*

Beweis. Die exakte Sequenz

$$1 \to \overline{\mathrm{Cn}} \to \overline{U}_l \to \overline{U}_l/\overline{\mathrm{Cn}} \to 1$$

ergibt

$$\ldots \to \hat{H}^{i-1}(G, \overline{U}_l/\overline{\mathrm{Cn}}) \to \hat{H}^i(G, \overline{\mathrm{Cn}}) \to \hat{H}^i(G, \overline{U}_l) \to \hat{H}^i(G, \overline{U}_l/\overline{\mathrm{Cn}}) \to \ldots .$$

Da $|G| = \frac{l-1}{2}$ und $|\overline{U}_l/\overline{\mathrm{Cn}}| = h_l^+$ teilerfremd sind, aber beide $\hat{H}^i(G, \overline{U}_l/\overline{\mathrm{Cn}})$ annullieren, gilt $\hat{H}^i(G, \overline{U}_l/\overline{\mathrm{Cn}}) = 0$ für alle $i \in \mathbb{Z}$. Es folgt mit Satz 2.7 und

Satz 2.9, dass

$$\hat{H}^i(G, \overline{U}_l) \cong \hat{H}^i(G, \overline{\mathrm{Cn}}) \cong \begin{cases} 0 & \text{für } l \equiv 3 \mod 4, \\ \mathbb{Z}/2\mathbb{Z} & \text{für } l \equiv 1 \mod 4. \end{cases}$$

Im ersten Fall gilt die Isomorphie natürlich auch für alle Untergruppen $H \subseteq G$, so dass die Behauptung folgt. □

Bemerkung. Man beachte den Spezialfall $h_l^+ = 1$. Für $l \equiv 1 \mod 4$ gilt wie gezeigt, dass $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv ist. Für $l \equiv 3 \mod 4$ folgt aus der $\mathbb{Z}[G]$-Freiheit von $\overline{\mathrm{Cn}}$ wegen $|\overline{U}_l/\overline{\mathrm{Cn}}| = h_l^+ = 1$, d.h. $\overline{U}_l = \overline{\mathrm{Cn}} \cong \mathbb{Z}[G]$, dass $\overline{U}_l$ sogar $\mathbb{Z}[G]$-frei ist (mit dem aus Satz 2.7 bekannten Erzeuger).

Folgerung 1. Unter der Annahme, dass die von Schoof in [Sch03] veröffentlichten vermuteten Klassenzahlen allesamt den wahren Klassenzahlen entsprechen, ergibt sich folgendes Bild:

a) Für 925 von den 1228 Primzahlen $2 \neq l < 10000$, also etwa 75%, hat $\mathbb{Q}(\zeta_l)^+$ die Klassenzahl 1. In 548 von diesen 925 Fällen sind die l-Einheiten modulo Torsion nach Satz 3.3 $\mathbb{Z}[G]$-frei; in den restlichen 377 Fällen ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv.

b) Von den 303 Primzahlen, für die die Klassenzahl ungleich eins ist, erfüllen 209 die Bedingung $\mathrm{ggT}\left(\frac{l-1}{2}, \tilde{h}_l^+\right) = 1$. Davon wiederum tritt 140 mal der Fall $l \equiv 1 \mod 4$, also Nicht-Projektivität von $\overline{U}_l$ über $\mathbb{Z}[G]$ auf. Die übrigen 69 Fälle mit $l \equiv 3 \mod 4$, in denen $\overline{U}_l$ also $\mathbb{Z}[G]$-projektiv ist, werden im nächsten Kapitel einer weiteren Untersuchung, nämlich auf $\mathbb{Z}[G]$-Freiheit, unterzogen.

3.2 2. Fall: $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) \neq 1$

Diesen Fall werden wir in einige Unterfälle zerlegen. Wir beginnen mit der Voraussetzung, dass $l \equiv 1 \mod 4$ ist und h_l^+ ungerade ist. Nehmen wir an, dass $\overline{U}_l$ $\mathbb{Z}[G]$-projektiv, also kohomologisch trivial ist. Dann liefert die exakte Sequenz

$$1 \to \overline{\mathrm{Cn}} \to \overline{U}_l \to \overline{U}_l/\overline{\mathrm{Cn}} \to 1$$

zusammen mit Satz 2.9

$$\hat{H}^i(G, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \hat{H}^{i+1}(G, \overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z} \text{ für alle } i \in \mathbb{Z}.$$

Nun wird aber $\mathbb{Z}/2\mathbb{Z}$ nicht von der ungeraden Zahl h_l^+ annulliert, was einen Widerspruch zu Satz 1.11 bedeutet. Wir formulieren dieses Ergebnis noch als

Satz 3.4. *Sei $l \equiv 1 \mod 4$ eine Primzahl derart, dass die Klassenzahl h_l^+ ungerade ist. Dann ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv*[1]. □

Folgerung 2. Die Liste von Schoof [Sch03] enthält 94 Primzahlen l, für die $\mathrm{ggT}\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$ gilt. Davon ist in 50 Fällen obiges Kriterium anwendbar.

Ausgehend von Schoofs Tabelle bleiben noch 44 Fälle zu untersuchen. Zumindest in einigen davon hilft die folgende Aussage weiter:

Proposition 3.5. *Sei $p \neq 2$ prim und $H = \langle \sigma_H \rangle$ eine endliche zyklische Gruppe der Ordnung p^i ($i \geq 1$). Weiter sei M ein endlicher H-Modul. Dann gelten die folgenden Aussagen:*

1.) *Wenn $v_p(|M|) = 1$ ist, so gilt $\hat{H}^0(H, M) \cong \mathbb{Z}/p\mathbb{Z}$.*

2.) *Sei $i \geq 2$ und $v_p(|M|) = 2$.*

   a) *Agiert H trivial auf M, so ist $\hat{H}^0(H, M) \cong \mathbb{Z}/p^2\mathbb{Z}$.*

   b) *Agiert H nicht-trivial auf M, so ist $\hat{H}^0(H, M) \cong \mathbb{Z}/p\mathbb{Z}$.*

Beweis. Zuerst bemerken wir, dass M als direkte Summe $M_p \oplus M_r$ geschrieben werden kann, wobei M_p die Sylow p-Untergruppe von M ist und $p \nmid |M_r|$. Auf Grund von Satz 1.11 gilt dann, da H eine p-Gruppe ist, dass

$$\hat{H}^i(H, M) \cong \hat{H}^i(H, M_p) \oplus \hat{H}^i(H, M_r) = \hat{H}^i(H, M_p) \text{ für alle } i \in \mathbb{Z}.$$

Im weiteren Verlauf setzen wir deshalb voraus, dass M eine p-Gruppe ist. Da M ein H-Modul ist, gibt es einen Homomorphismus von H nach $\mathrm{Aut}(M)$, den wir mit τ bezeichnen wollen.

1.) Aus $|M| = p$ folgt $M \cong \mathbb{Z}/p\mathbb{Z}$ und damit $\mathrm{Aut}(M) \cong (\mathbb{Z}/p\mathbb{Z})^\star$, also $|\mathrm{Aut}(M)| = p-1$. Die Ordnung von $\tau(\sigma_H)$ muss einerseits $|\mathrm{Aut}(M)| = p-1$ teilen, andererseits hat $\tau(\sigma_H)$ wegen $|H| = p^i$ Ordnung p^j, wobei $0 \leq j \leq i$ ist. Somit kann σ_H nur trivial auf M agieren, das heißt, dass M H-invariant ist. Mit $N_H M = |H| \cdot M = 0$ ergibt sich schließlich $\hat{H}^0(H, M) = M^H / N_H M = M \cong \mathbb{Z}/p\mathbb{Z}$.

2.) a) Wenn H trivial auf M agiert, folgt sofort

$$\hat{H}^0(H, M) = M^H / N_H M = M/|H|M = M \cong \mathbb{Z}/p^2\mathbb{Z}.$$

[1] Ist $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) = 1$, so ist die Aussage bereits Teil von Satz 3.3.

b1) Ist $M \cong \mathbb{Z}/p^2\mathbb{Z}$, so gilt $\mathrm{Aut}(M) \cong (\mathbb{Z}/p^2\mathbb{Z})^\star$, also $|\mathrm{Aut}(M)| = p(p-1)$. Somit hat $\tau(\sigma_H)$ die Ordnung p und man erhält

$$\sigma_H : M \to M, m \mapsto (1 + p \cdot n) \cdot m \text{ für ein } n \in \{1, \ldots, p-1\}.$$

Nun folgt aus

$$(1 + p \cdot n) \cdot m = m \quad \Leftrightarrow \quad p \cdot n \cdot m = 0 \quad \Leftrightarrow \quad m \in pM,$$

dass $M^H = pM$ ist. Da ${\sigma_H}^p$ trivial auf M agiert, gilt weiter

$$N_{\langle {\sigma_H}^p \rangle} M = pM.$$

Nun hat $\langle \sigma_H \rangle \,/\, \langle {\sigma_H}^p \rangle$, genau wie pM, die Ordnung p. Wir können also 1.) anwenden und erhalten

$$N_H M = N_{\langle \sigma_H \rangle / \langle {\sigma_H}^p \rangle} \cdot N_{\langle {\sigma_H}^p \rangle} M = N_{\langle \sigma_H \rangle / \langle {\sigma_H}^p \rangle}(pM) = p \cdot (pM) = 0,$$

woraus die Behauptung $\hat{H}^0(H, M) = M^H / N_H = pM \cong \mathbb{Z}/p\mathbb{Z}$ folgt.

b2) Für den anderen Fall, $M \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, gilt $\mathrm{Aut}(M) \cong \mathrm{Gl}(2, \mathbb{F}_p)$ und damit

$$|\mathrm{Aut}(M)| = (p^2 - 1)(p^2 - p).$$

Da $p \mid\mid |\mathrm{Aut}(M)|$ muss $M^{\langle {\sigma_H}^p \rangle} = M$ und $N_{\langle {\sigma_H}^p \rangle} M = pM = 0$ sein. Wegen

$$\begin{aligned} N_H M &= N_{\langle \sigma_H \rangle / \langle {\sigma_H}^p \rangle} N_{\langle {\sigma_H}^p \rangle} M = N_{\langle \sigma_H \rangle / \langle {\sigma_H}^p \rangle}(pM) \\ &= N_{\langle \sigma_H \rangle / \langle {\sigma_H}^p \rangle} 0 = 0 \end{aligned}$$

bleibt noch $M^H \cong \mathbb{Z}/p\mathbb{Z}$ zu zeigen. Sei dazu $A = \tau(\sigma_H) \in \mathrm{Gl}(2, \mathbb{F}_p)$ mit $A^p = E_2$, wobei $E_2 \in \mathrm{Gl}(2, \mathbb{F}_p)$ die Identität ist. Zudem sei χ_A das charakteristische Polynom von A. Für $x \in \mathbb{F}_p$ gilt nun

$$\begin{aligned} \chi_A(x) &= (\chi_A(x))^p = (\det(A - xE_2))^p = \det((A - xE_2)^p) \\ &= \det(A^p - x^p E_2^p) = \det(E_2 - xE_2) = (x-1)^2. \end{aligned}$$

Das bedeutet, dass A Eigenwert 1 (mit algebraischer Vielfachheit 2) hat. Für $A \neq E_2$ folgt, dass $\mathrm{Eig}(A, 1)$, der Eigenraum von A zum Eigenwert 1, Dimension 1 hat. Daraus ergibt sich schließlich

$$|M^{\langle \sigma_H \rangle}| = |\mathrm{Eig}(A, 1)| = p \text{ und } M^H / N_H M = M^H \cong \mathbb{Z}/p\mathbb{Z}.$$

□

Die Konstellation $l \equiv 3 \mod 4$ und ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$ tritt in Schoofs Tabelle genau zweimal auf. In beiden Fällen können wir jedoch mit dieser Proposition zeigen, dass $\overline{U}_l$ jeweils nicht $\mathbb{Z}[G]$-projektiv ist:

Folgerung 3. Nach Schoof [Sch03] hat $\mathbb{Q}(\zeta_l)^+$ für $l = 3571$, $\frac{l-1}{2} = 3 \cdot 5 \cdot 7 \cdot 17$, die vermutete Klassenzahl $\tilde{h}_l^+ = 7$. Sei $G_7 \subset G$ die Untergruppe der Ordnung 7. Nach Teil 1 der obigen Proposition erhalten wir

$$\hat{H}^0(G_7, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \mathbb{Z}/7\mathbb{Z}.$$

Wegen $l \equiv 3 \mod 4$ gilt nach Satz 2.7

$$\hat{H}^i(G_7, \overline{\mathrm{Cn}}) = 0 \text{ für alle } i \in \mathbb{Z} \text{ und damit } \hat{H}^0(G_7, \overline{U}_l) \cong \mathbb{Z}/7\mathbb{Z} \neq 0.$$

Somit ist $\overline{U}_l$ nicht kohomologisch trivial.

Folgerung 4. Für $l = 7351$, $\frac{l-1}{2} = 3 \cdot 5^2 \cdot 7^2$ ist $\tilde{h}_l^+ = 7^2$. Sei $G_{49} \subset G$ die Untergruppe der Ordnung 49. Nach Teil 2 von Proposition 3.5 gilt also

$$\hat{H}^0(G_{49}, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \mathbb{Z}/49\mathbb{Z} \text{ oder } \hat{H}^0(G_{49}, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \mathbb{Z}/7\mathbb{Z},$$

was mit Satz 2.7, analog zu Folgerung 3, zu

$$\hat{H}^0(G_{49}, \overline{U}_l) \cong \hat{H}^0(G_{49}, \overline{U}_l/\overline{\mathrm{Cn}}) \neq 0,$$

also der Nicht-Projektivität von $\overline{U}_l$ führt.

Die bis hierhin noch nicht auf Projektivität untersuchten Fälle zeichnen sich alle durch $l \equiv 1 \mod 4$, $\tilde{h}_l^+ \equiv 0 \mod 2$ und ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$ aus. Für zwei dieser l liefert uns jedoch wieder Proposition 3.5 in Verbindung mit Satz 2.9 eine Antwort:

Folgerung 5. Betrachten wir $l_1 = 1009$, $\frac{l_1-1}{2} = 2^3 \cdot 3^2 \cdot 7$ mit $\tilde{h}_l^+ = 2^2 \cdot 7$ und $l_2 = 9601$, $\frac{l_2-1}{2} = 2^6 \cdot 3 \cdot 5^2$ mit $\tilde{h}_l^+ = 2^4 \cdot 5$. Abkürzend verwenden wir $G_1 := \mathrm{Gal}(\mathbb{Q}(\zeta_{l_1})^+/\mathbb{Q})$ bzw. $G_2 := \mathrm{Gal}(\mathbb{Q}(\zeta_{l_2})^+/\mathbb{Q})$. Weiter seien $G_{1,7} \subset G_1$ die Sylow 7-Untergruppe von G_1 und $G_{2,5^2} \subset G_2$ die Sylow 5-Untergruppe von G_2. Nehmen wir jetzt an, dass $\overline{U}_{l_i}$ $\mathbb{Z}[G_i]$-projektiv ist $(i = 1, 2)$. Dann ergäbe sich einerseits mit Satz 2.9

$$\hat{H}^0(G_{1,7}, \overline{U}_{l_1}/\overline{\mathrm{Cn}}(l_1)) \cong \hat{H}^1(G_{1,7}, \overline{\mathrm{Cn}}(l_1)) = 0$$

beziehungsweise

$$\hat{H}^0(G_{2,5^2}, \overline{U}_{l_2}/\overline{\mathrm{Cn}}(l_2)) \cong \hat{H}^1(G_{2,5^2}, \overline{\mathrm{Cn}}(l_1)) = 0$$

und andererseits nach Teil 1 von Proposition 3.5

$$\hat{H}^0(G_{1,7}, \overline{U}_{l_1}/\overline{\mathrm{Cn}}(l_1)) \cong \mathbb{Z}/7\mathbb{Z} \text{ bzw. } \hat{H}^0(G_{2,5^2}, \overline{U}_{l_2}/\overline{\mathrm{Cn}}(l_2)) \cong \mathbb{Z}/5\mathbb{Z}.$$

Dieser Widerspruch zeigt, dass die l-Einheiten modulo Torsion auch in diesen beiden Fällen nicht $\mathbb{Z}[G]$-projektiv sind.

Auf die restlichen 40 Fälle mit $l \equiv 1 \mod 4$ und $\tilde{h}_l^+ \equiv 0 \mod 2$ ist obige Proposition nicht anwendbar. Mit einem anderen Ansatz sind jedoch in allen 42 Fällen, also auch in den in Folgerung 5 behandelten Fällen, die l-Einheiten modulo Torsion als nicht $\mathbb{Z}[G]$-projektiv zu entlarven.
Nach Satz 2.9 gilt hier

$$\hat{H}^i(G_g, \overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z}$$

für alle $i \in \mathbb{Z}$ und für alle Untergruppen $G_g \subseteq G$ gerader Ordnung.
Annahme: $\overline{U}_l$ ist $\mathbb{Z}[G]$-projektiv.
Somit müsste

$$\hat{H}^i(G_g, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z}$$

für alle $i \in \mathbb{Z}$ und für alle Untergruppen $G_g \subseteq G$ gerader Ordnung gelten. Sei im weiteren Verlauf G_2 die Sylow-2 Untergruppe von $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$.
Als Motivation für unser weiteres Vorgehen betrachten wir ein

Beispiel 3. Sei $h_l^+ = 4$ und $|G_2| = 2$, so folgt unter der Annahme $\overline{U}_l/\overline{\mathrm{Cn}} \cong \mathbb{Z}/4\mathbb{Z}$ durch eine einfache Rechnung $\hat{H}^0(G_2, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \mathbb{Z}/2\mathbb{Z}$. Eine ähnliche Rechnung zeigt $\hat{H}^0(G_2, \overline{U}_l/\overline{\mathrm{Cn}}) \ncong \mathbb{Z}/2\mathbb{Z}$ falls $\overline{U}_l/\overline{\mathrm{Cn}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Um die Behauptung in diesem Beispiel zu beweisen, würde also der Nachweis von $\overline{U}_l/\overline{\mathrm{Cn}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ausreichen. Allerdings werden wir einen anderen Weg wählen, der über die Klassengruppe $\mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)$ führt. Bekanntlich gilt zwar $|\mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)| = |\overline{U}(l)/\overline{\mathrm{Cyc}}(l)|$, aber nicht unbedingt $\mathrm{Cl}(\mathbb{Q}(\zeta_l)^+) \cong \overline{U}(l)/\overline{\mathrm{Cyc}}(l)$. Folgendes Resultat von Schoof ist für uns von großer Bedeutung.

Satz 3.6 ([Sch03, Proposition 5.1 b)])**.** *Für jede Untergruppe H von G gilt*

$$\hat{H}^i(H, U(l)/\mathrm{Cyc}(l)) \cong \hat{H}^i(H, \mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)) \text{ für alle } i \in \mathbb{Z}.$$

Da $U(l)/\mathrm{Cyc}(l) \cong \overline{U}(l)/\overline{\mathrm{Cyc}}(l)$ gilt und nach Lemma 3.2 auch die $\mathbb{Z}[G]$-Moduln $\overline{U}(l)/\overline{\mathrm{Cyc}}(l)$ und $\overline{U}_l/\overline{\mathrm{Cn}}$ isomorph sind, erhalten wir insbesondere

$$\hat{H}^i(H, \overline{U}_l/\overline{\mathrm{Cn}}) \cong \hat{H}^i(H, \mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)) \text{ für alle } i \in \mathbb{Z}.$$

Unsere Annahme führt also zu

$$\hat{H}^i(G_2, \mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)) \cong \mathbb{Z}/2\mathbb{Z} \text{ für alle } i \in \mathbb{Z}.$$

Der nächste Schritt führt uns von der Klassengruppe $\mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)$ zu Klassengruppen von Unterkörpern K von $\mathbb{Q}(\zeta_l)^+$. Für einen Teiler δ von $|G| = \frac{l-1}{2}$ bezeichne K_δ den Unterkörper von $\mathbb{Q}(\zeta_l)^+$ mit $[K_\delta : \mathbb{Q}] = \delta$. Weiter seien $\delta^\star$ beziehungsweise δ_p die kleinsten ganzen Zahlen, so dass $h_{K_{\delta^\star}} = h_l^+$ beziehungsweise $p^{v_p(h_l^+)} | h_{K_{\delta_p}}$ gilt.

Satz 3.7 ([Wa97, Theorem 10.1])**.** *Sei L/K eine Erweiterung von Zahlkörpern. Gibt es keine unverzweigte abelsche Erweiterung F/K mit $F \subsetneq L$, so ist die Normabbildung*

$$N_{L/K} : \mathrm{Cl}(L) \to \mathrm{Cl}(K)$$

surjektiv. Insbesondere gilt $h_K \mid h_L$.

Da für primes l und $K \subset L \subset \mathbb{Q}(\zeta_l)$ die Körpererweiterung L/K voll verzweigt ist, erhalten wir sofort das folgende

Korollar 3.8. *Seien $l \neq p$ Primzahlen und $K \subset L \subset \mathbb{Q}(\zeta_l)$. Ist $h_K = h_L$, so bildet die Norm einen G-Isomorphismus $\mathrm{Cl}(K) \cong \mathrm{Cl}(L)$. Ist $\mathrm{Cl}(K)$ eine p-Gruppe mit der gleichen Ordnung wie die Sylow-p Untergruppe $\mathrm{Cl}(L)_p$ von $\mathrm{Cl}(L)$, so sind $\mathrm{Cl}(K)$ und $\mathrm{Cl}(L)_p$ isomorphe G-Moduln.* □

Für einen endlichen G-Modul M mit $|M| = 2^e \cdot u$, wobei u ungerade ist, gibt es eine Zerlegung $M = M_u \oplus M_2$, wobei M_2 die Sylow-2 Untergruppe von M ist. Nach Satz 1.11 gilt damit für alle Untergruppen $H \subseteq G$

$$\hat{H}^i(H, M) \cong \hat{H}^i(H, M_u) \oplus \hat{H}^i(H, M_2) \text{ für alle } i \in \mathbb{Z}.$$

Insbesondere ergibt $H = G_2$ wegen $\mathrm{ggT}\,(|G_2|, |M_u|) = 1$

$$\hat{H}^i(G_2, M) \cong \hat{H}^i(G_2, M_u) \oplus \hat{H}^i(G_2, M_2) \cong \hat{H}^i(G_2, M_2) \text{ für alle } i \in \mathbb{Z}.$$

Insgesamt erhalten wir also

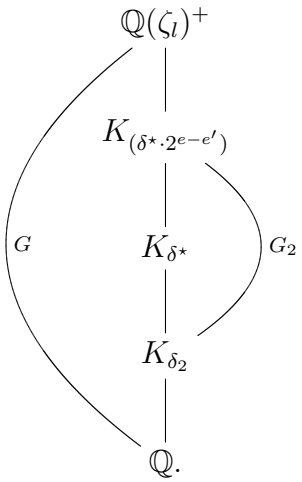
$$\begin{aligned} \hat{H}^i(G_2, \overline{U}_l/\overline{\mathrm{Cn}}) &\cong \hat{H}^i(G_2, \mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)) \cong \hat{H}^i(G_2, \mathrm{Cl}(\mathbb{Q}(\zeta_l)^+)_2) \\ &\cong \hat{H}^i(G_2, \mathrm{Cl}(K_{\delta^\star})_2) \cong \hat{H}^i(G_2, \mathrm{Cl}(K_{\delta_2})) \\ &\cong \hat{H}^i(G_2, \mathrm{Cl}(K_{\delta_2})_2) \text{ für alle } i \in \mathbb{Z}. \end{aligned}$$

Wir unterteilen den letzten Schritt in zwei Fälle

1.) δ_2 ist ungerade Wir definieren ganze Zahlen e und e' durch

$$e = v_2\left(\frac{l-1}{2}\right) \text{ und } e' = v_2(\delta^\star)$$

und erhalten folgende Situation:



Insbesondere ist $\mathrm{Cl}(K_{\delta_2})$ G_2-trivial, es gilt also

$$\mathrm{Cl}(K_{\delta_2})^{G_2} = \mathrm{Cl}(K_{\delta_2}).$$

Bevor wir nun einen weiteren Satz aus [Wa97] zitieren und verwenden können, müssen wir für eine endliche abelsche p-Gruppe A (p prim) zwei Größen definieren. Bekanntlich gilt

$$A \cong \oplus \mathbb{Z}/p^{a_i}\mathbb{Z}$$

mit bestimmten $a_i \in \mathbb{Z}$. Für $a \geq 1$ sei $n_a(A)$ die Anzahl der i mit $a_i = a$, $r_a(A)$ die Anzahl der i mit $a_i \geq a$.

Satz 3.9 ([Wa97, Theorem 10.8])**.** *Sei L/K eine zyklische Erweiterung vom Grad n, p prim mit $p \nmid n$ und f die Ordnung von $p \mod n$. Für alle Zwischenkörper $K \subseteq E \subsetneq L$ teile p die Klassenzahl h_E von E nicht. Dann gilt für die Sylow-p Untergruppe $\mathrm{Cl}(L)_p$ von $\mathrm{Cl}(L)$*

$$r_a(\mathrm{Cl}(L)_p) \equiv n_a(\mathrm{Cl}(L)_p) \equiv 0 \mod f$$

für alle a. Teilt p die Klassenzahl h_L von L, so ist der p-Rang r_1 von $\mathrm{Cl}(L)_p$ mindestens f.

Folgerung 6. In allen 31 Fällen, in denen δ_2 ungerade ist, ist $\delta_2 \in \{3, 5, 7\}$, also insbesondere eine ungerade Primzahl. Allgemein können wir hier feststellen, dass dann $K_{\delta_2}/\mathbb{Q}$ eine zyklische Erweiterung vom Grad δ_2 ist, so dass keine echten Zwischenkörper $\mathbb{Q} \subsetneq E \subsetneq K_{\delta_2}$ existieren. Also gilt

$$r_a(\mathrm{Cl}(K_{\delta_2})) \equiv n_a(\mathrm{Cl}(K_{\delta_2})) \equiv 0 \mod f,$$

wobei f die Ordnung von 2 modulo δ_2 ist. Dies liefert in 29 Fällen, allen bis auf $l = 1777$ und $l = 7841$, sofort

$$\mathrm{Cl}(K_{\delta_2})_2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{für } \delta_2 = 3, \\ (\mathbb{Z}/2\mathbb{Z})^4 & \text{für } \delta_2 = 5, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{für } \delta_2 = 7. \end{cases}$$

Zusammen mit $(\mathrm{Cl}(K_{\delta_2})_2)^{G_2} = \mathrm{Cl}(K_{\delta_2})_2$ folgt deshalb

$$N_{G_2}(\mathrm{Cl}(K_{\delta_2})_2) = |G_2|(\mathrm{Cl}(K_{\delta_2})_2) = 0.$$

Für $l = 1777$ bzw. $l = 7841$ ist $\delta_2 = 3$ bzw. $\delta_2 = 7$, $\tilde{h}_l^+ = 16$ bzw. $\tilde{h}_l^+ = 421 \cdot 64$ und $|G_2| = 2^3$ bzw. $|G_2| = 2^4$. Hier ist nach Satz 3.9 zwar keine eindeutige Aussage möglich[2], man erhält jedoch

$$\mathrm{Cl}(K_3) \cong (\mathbb{Z}/2\mathbb{Z})^4 \text{ oder } \mathrm{Cl}(K_3) \cong (\mathbb{Z}/4\mathbb{Z})^2,$$

beziehungsweise

$$\mathrm{Cl}(K_7) \cong (\mathbb{Z}/2\mathbb{Z})^6 \text{ oder } \mathrm{Cl}(K_7) \cong (\mathbb{Z}/4\mathbb{Z})^3.$$

Somit folgt auch in diesen Fällen zusammen mit der G_2-Invarianz von $\mathrm{Cl}(K_{\delta_2})$

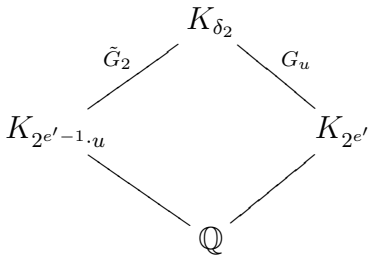
$$N_{G_2}(\mathrm{Cl}(K_{\delta_2})_2) = |G_2|(\mathrm{Cl}(K_{\delta_2})_2) = 0.$$

Insgesamt ergibt sich das bereits angekündigte Ergebnis,

$$\begin{aligned} \hat{H}^0(G_2, \overline{U}_l/\overline{\mathrm{Cn}}) &\cong \hat{H}^0(G_2, \mathrm{Cl}(K_{\delta_2})_2) = (\mathrm{Cl}(K_{\delta_2})_2)^{G_2}/N_{G_2}(\mathrm{Cl}(K_{\delta_2})_2) \\ &= (\mathrm{Cl}(K_{\delta_2})_2) \ncong \mathbb{Z}/2\mathbb{Z}, \end{aligned}$$

$\overline{U}_l$ ist nicht $\mathbb{Z}[G]$-projektiv.

2.) δ_2 ist gerade Wieder definieren wir ganze Zahlen e' und u durch $\delta_2 = 2^{e'} \cdot u$, wobei u ungerade ist. Weiter seien $G_u, \tilde{G}_2 \subset G$ Untergruppen der Ordnung u beziehungsweise 2, wodurch wir folgendes Bild erhalten:



[2]Mit PARI/GP kann man die Struktur der Klassengruppen problemlos als $(\mathbb{Z}/4\mathbb{Z})^2$ für $l = 1777$ und $(\mathbb{Z}/2\mathbb{Z})^6$ für $l = 7841$ identifizieren.

Nach Satz 3.7 ist $N_{G_u}(\mathrm{Cl}(K_{\delta_2})_2) = \mathrm{Cl}(K_{2^{e'}})_2$. Zudem bemerken wir, dass wegen nachfolgendem Satz 2 kein Teiler von $h_{K_{2^{e'}}}$ ist, also

$$(\star) \quad N_{G_u}(\mathrm{Cl}(K_{\delta_2})_2) = \mathrm{Cl}(K_{2^{e'}})_2 = 0$$

gilt.

Satz 3.10 ([Wa97, Theorem 10.4 b)])**.** *Sei $L/\mathbb{Q}$ eine Galoiserweiterung, p eine Primzahl und $\mathrm{Gal}(L/K)$ eine p-Gruppe. Weiter sei maximal eine endliche Primstelle verzweigt. Dann gilt $p \nmid h_L$.*

Wir möchten jetzt durch

$$\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2) \ncong \mathbb{Z}/2\mathbb{Z}$$

einen Widerspruch zur Annahme nachweisen.
Dazu stellen wir fest, dass $\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2)$ von $|\tilde{G}_2| = 2$ annulliert wird und offenbar ein G_u-Modul, somit auch $\mathbb{F}_2[G_u]$-Modul, ist. Zusammen mit $(\star)$ folgt, dass $\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2)$ ein $\mathbb{F}_2[G_u]/(N_{G_u})$-Modul ist.

Folgerung 7. Die noch zu bearbeitenden 11 Fälle sind durch

$$\delta_2 \in \{2 \cdot 3, 4 \cdot 3\},$$

d.h. $u = 3$, gekennzeichnet. Somit ist $\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2)$ ein $\mathbb{F}_2[G_3]/(N_{G_3})$-Modul. Jedoch ist $x^2 + x + 1$ irreduzibel über $\mathbb{F}_2$, also

$$\mathbb{F}_2[G_3]/(N_{G_3}) \cong \mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_4.$$

$\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2)$ ist demnach ein $\mathbb{F}_4$-Vektorraum, was

$$|\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2)| = 4^i$$

für ein $i \in \mathbb{N}_0$ bedeutet und

$$\hat{H}^0(\tilde{G}_2, \mathrm{Cl}(K_{\delta_2})_2) \ncong \mathbb{Z}/2\mathbb{Z}$$

nach sich zieht.

Bemerkung. Man kann mit jeder Untergruppe $H \subset G_2$ statt $\tilde{G}_2$ arbeiten. Ähnlich wie oben zeigt man, dass $\hat{H}^0(H, \mathrm{Cl}(K_{\delta_2})_2)$ ein $\mathbb{Z}/2^s\mathbb{Z}[G_u]/(N_{G_u})$-Modul ist, wobei $|H| = 2^s$ und $\delta_2 = 2^{e'} \cdot u$ mit ungeradem $u \in \mathbb{N}$ ist. Gilt nun $|\hat{H}^0(H, \mathrm{Cl}(K_{\delta_2})_2)| \neq 0$, so kann man zeigen, dass $|\hat{H}^0(H, \mathrm{Cl}(K_{\delta_2})_2)| \geq 4$ sein muss.

Dies schließt unsere Untersuchungen von $\overline{U}_l$ auf $\mathbb{Z}[G]$-Projektivität ab. Die Ergebnisse dieses Kapitels sind in den Tabellen in Anhang A zusammengefasst, die zugehörigen PARI/GP-Skripte sind in Anhang B zu finden.

Abbildung 3.1: Situation nach Kapitel 3

Kapitel 4

Untersuchung von $\overline{U}_l$ auf $\mathbb{Z}[G]$-Freiheit

In dem gesamten Kapitel sei $l \equiv 3 \mod 4$ eine Primzahl, ζ_l eine primitive l-te Einheitswurzel, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ und $\mathrm{ggT}\left(|G|, h_l^+\right) = 1$. G ist hier also zyklisch der Ordnung $n := \frac{l-1}{2}$ und wir bezeichnen einen Erzeuger mit σ_G oder kurz mit σ. Des Weiteren gilt mit diesen Voraussetzungen nach Satz 2.7, dass $\overline{\mathrm{Cn}} = \langle\gamma\rangle_{\mathbb{Z}[G]}$ $\mathbb{Z}[G]$-frei ist, wobei Cn wie zuvor die Kreiszahlen bezeichnet. Für die l-Einheiten U_l ist $\overline{U}_l$ $\mathbb{Z}$-frei und nach Satz 3.3 auch $\mathbb{Z}[G]$-projektiv.
Dieses Kapitel ist der Frage gewidmet, in welchen Fällen $\overline{U}_l$ frei beziehungsweise nicht frei über $\mathbb{Z}[G]$ ist. Bei der Untersuchung ist es in einigen Schritten hilfreich, statt mit $\overline{U}_l \supset \overline{\mathrm{Cn}} \cong \mathbb{Z}[G]$ mit Idealen $X \subset \mathbb{Z}[G]$ zu arbeiten, die in gewisser Weise die gleichen Eigenschaften wie $\overline{U}_l$ haben.

4.1 Das zu $\overline{U}_l$ gehörende Ideal X

Für einen $\mathbb{Z}$-Modul M sei

$$M^\perp := \mathrm{Hom}_\mathbb{Z}(M, \mathbb{Z})$$

der $\mathbb{Z}$-Dual von M. Auf natürliche Weise ist $M^\perp$ wieder ein $\mathbb{Z}$-Modul und es gilt $(M^\perp)^\perp \cong M$ für alle endlich erzeugten freien $\mathbb{Z}$-Moduln M.

Definition 4.1. Sei H eine endliche abelsche Gruppe und M ein $\mathbb{Z}[H]$-Modul. Wie man leicht nachrechnen kann, wird $M^\perp$ durch

$$\left(\sum_i \alpha_i h_i\right) f(m) := f\left(\left(\sum_i \alpha_i h_i^{-1}\right) m\right) = \sum_i \alpha_i f\left(h_i^{-1} m\right)$$

für $f \in M^\perp$, $m \in M$ und $\alpha_i \in \mathbb{Z}, h_i \in H$ für alle i, zu einem $\mathbb{Z}[H]$-Modul. Diesen nennen wir den *zu M kontragredienten Modul*.

Bemerkung. Für die Einführung kontragredienter Moduln ist die Voraussetzung der Kommutativität von H nicht notwendig. In unserem Fall wird auch durch

$$\left(\sum_i \alpha_i h_i\right) f(m) := \sum_i \alpha_i f\left(h_i m\right)$$

eine $\mathbb{Z}[H]$-Modulstruktur auf $M^\perp$ definiert.

Proposition 4.2. *Sei H eine endliche Gruppe. Dann gilt*

$$(\mathbb{Z}[H])^\perp \cong \mathbb{Z}[H]$$

als $\mathbb{Z}[H]$-Moduln.

Beweis. Für den allgemeinen Beweis verweisen wir auf [CR81, Corollary 10.29]. Wir zeigen die Aussage für die in dieser Arbeit auftretende Situation, in der $H = \langle \sigma_H \rangle$ zyklisch ist. Sei $|H| = t$, dann ist

$$({\sigma_H}^0, \sigma_H, \ldots, {\sigma_H}^{t-1})$$

eine $\mathbb{Z}$-Basis von $\mathbb{Z}[H]$ und

$$(({\sigma_H}^0)^\star, {\sigma_H}^\star, \ldots, ({\sigma_H}^{t-1})^\star)$$

mit $({\sigma_H}^i)^\star \cdot ({\sigma_H}^j) = \delta_{ij}$, wobei δ_{ij} das Kronecker-Delta ist, die zugehörige (Dual-)Basis von $(\mathbb{Z}[H])^\perp$. Es bleibt zu zeigen, dass der $\mathbb{Z}$-Isomorphismus

$$(\mathbb{Z}[H])^\perp \to \mathbb{Z}[H], ({\sigma_H}^i)^\star \mapsto {\sigma_H}^i$$

$\mathbb{Z}[H]$ linear ist. Dies folgt jedoch sofort aus der Beobachtung, dass

$${\sigma_H}^i \cdot ({\sigma_H}^j)^\star \cdot ({\sigma_H}^l) = ({\sigma_H}^j)^\star \cdot ({\sigma_H}^{l-i}) = \begin{cases} 1 \text{ für } j = l - i, \\ 0 \text{ für } j \neq l - i, \end{cases}$$

also ${\sigma_H}^i \cdot ({\sigma_H}^j)^\star = ({\sigma_H}^{i+j})^\star$ ist. □

Da $\mathrm{Hom}_\mathbb{Z}(-, \mathbb{Z})$ ein additiver Funktor ist, gilt

$$(M \oplus N)^\perp = M^\perp \oplus N^\perp$$

für zwei $\mathbb{Z}$-Moduln M und N. Zusammen mit Proposition 4.2 erhält man folgendes

Korollar 4.3. *Ein endlich erzeugter $\mathbb{Z}[H]$-Modul M ist genau dann $\mathbb{Z}[H]$-frei (projektiv), wenn $M^\perp$ $\mathbb{Z}[H]$-frei (projektiv) ist.* □

Wir benötigen jetzt noch einen weiteren Dualitätsbegriff.

Definition 4.4. Für einen $\mathbb{Z}$-Modul M definiert man den *Pontrjagin-Dualmodul*

$$M^\vee := \mathrm{Hom}_\mathbb{Z}(M, \mathbb{Q}/\mathbb{Z}).$$

Bemerkung. 1.) Der Begriff der Pontrjagin-Dualität wird üblicherweise in wesentlich allgemeinerer Form definiert. In dieser Arbeit ist jedoch nur der angeführte Fall von Interesse. Dies gilt auch für den Dualitätssatz von Pontrjagin, dessen Aussage

$$(H^\vee)^\vee \cong H$$

für endliche abelsche Gruppen H ist (siehe [Lam98, Example 19.29]).

2.) Für alle endlichen $\mathbb{Z}$-Moduln M gilt

$$|M| = |M^\vee|.$$

Denn: Für geeignete $n_1, \ldots, n_r$ ($r \in \mathbb{N}$) mit $|M| = \prod_{i=1}^r n_i$ gilt

$$M \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r.$$

Ein Homomorphismus von $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_r \to \mathbb{Q}/\mathbb{Z}$ ist durch die Wirkung auf den r Elementen $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ eindeutig bestimmt. Da es genau n_i verschiedene Homomorphismen von $\mathbb{Z}/n_i\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, nämlich $1 \mapsto \frac{t}{n_i}$ mit $t \in \{0, 1, \ldots, n_i - 1\}$, gibt, folgt die Behauptung.

Lemma 4.5. *Seien $M \subset N$ projektive $\mathbb{Z}$-Moduln mit $|N/M| < \infty$. Dann ist*

$$M^\perp/N^\perp \cong (N/M)^\vee.$$

Beweis. Die exakte Sequenz

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

ergibt

$$\begin{aligned} \mathrm{Ext}^0_\mathbb{Z}(N/M, \mathbb{Z}) \to \mathrm{Ext}^0_\mathbb{Z}(N/M, \mathbb{Q}) \to \mathrm{Ext}^0_\mathbb{Z}(N/M, \mathbb{Q}/\mathbb{Z}) \to \\ \to \mathrm{Ext}^1_\mathbb{Z}(N/M, \mathbb{Z}) \to \mathrm{Ext}^1_\mathbb{Z}(N/M, \mathbb{Q}) \to \ldots \end{aligned}$$

und somit

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}(N/M,\mathbb{Z}) = 0 \to \mathrm{Hom}_{\mathbb{Z}}(N/M,\mathbb{Q}) = 0 \to \mathrm{Hom}_{\mathbb{Z}}(N/M,\mathbb{Q}/\mathbb{Z})\\ \to \mathrm{Ext}^1_{\mathbb{Z}}(N/M,\mathbb{Z}) \to 0 = \mathrm{Ext}^1_{\mathbb{Z}}(N/M,\mathbb{Q}),\end{aligned}$$

wobei die ersten beiden Gleichheiten die Endlichkeit von N/M verwenden, die dritte Gleichheit, dass $\mathbb{Q}$ ein injektiver $\mathbb{Z}$-Modul ist. Als Ergebnis bleibt

$$(\star) \qquad \mathrm{Ext}^1_{\mathbb{Z}}(N/M,\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(N/M,\mathbb{Q}/\mathbb{Z}) = (N/M)^\vee .$$

Weiter haben wir die exakte Sequenz

$$0 \to M \to N \to N/M \to 0,$$

die auf ähnliche Weise zu

$$\begin{aligned}0 = \mathrm{Hom}_{\mathbb{Z}}(N/M,\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(N,\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}) \to\\ \to \mathrm{Ext}^1_{\mathbb{Z}}(N/M,\mathbb{Z}) \to 0 = \mathrm{Ext}^1_{\mathbb{Z}}(N,\mathbb{Z})\end{aligned}$$

und, in Verbindung mit $(\star)$, zu der exakten Sequenz

$$0 \to N^\perp \to M^\perp \to (N/M)^\vee \to 0$$

führt. □

Korollar 4.6. *Seien $M \subset N$ projektive $\mathbb{Z}$-Moduln mit $|N/M| < \infty$. Dann gilt*

$$|N/M| = \left|M^\perp/N^\perp\right| .$$

Beweis. Nach voriger Bemerkung und Lemma 4.5 gilt

$$|N/M| = |(N/M)^\vee| = \left|M^\perp/N^\perp\right| .$$

□

Wieder bezeichnen wir für einen H-Modul M und eine Untergruppe $J \subset H$ mit

$$M^J = \{m \in M \mid \sigma(m) = m \text{ für alle } \sigma \in J\}$$

die J-Invarianten von M.

Lemma 4.7. *Seien $M \subset N$ $\mathbb{Z}[H]$-Moduln, M $\mathbb{Z}[H]$-projektiv und $J \subset H$ eine Untergruppe. Dann gilt $(N/M)^J \cong N^J/M^J$.*

Beweis. Aus der exakten Sequenz

$$0 \to M \to N \to N/M \to 0$$

erhält man die Exaktheit von

$$0 \to M^J \to N^J \to (N/M)^J \to H^1(J, M) \to \ldots,$$

wobei aus der $\mathbb{Z}[H]$-Projektivität von M $H^1(J, M) = 0$ und damit die Behauptung folgt. □

Ein weiterer Hilfssatz stellt eine Verbindung von Invarianten eines Moduls mit den Invarianten des Pontrjagin-Duals her.

Lemma 4.8. *Sei $H = \langle \sigma_H \rangle$ eine endliche zyklische Gruppe und M ein endlicher $\mathbb{Z}[H]$-Modul. Dann gilt*

$$M^H = 0 \;\Leftrightarrow\; (M^\vee)^H = 0.$$

Beweis. $M^H = \{m \in M \mid \sigma_H(m) = m\} = 0$ ist äquivalent dazu, dass $(\sigma_H - 1)$ injektiv auf M ist. Da M endlich ist, ist dies wiederum äquivalent zur Surjektivität von $(\sigma_H - 1)$ auf M. Mit

$$M_H = M/\langle \{\sigma_H(m) - m \mid m \in M\} \rangle = M/(I_H M)$$

gilt nun folgende Kette von Äquivalenzen:

$$(\sigma_H - 1) \text{ ist surjektiv auf } M \;\Leftrightarrow\; M_H = 0 \;\Leftrightarrow\; (M_H)^\vee = 0 \;\Leftrightarrow\; (M^\vee)^H = 0.$$

Hierbei möchten wir kurz die letzte Äquivalenz erläutern:
Ist $f \in \mathrm{Hom}_\mathbb{Z}(M_H, \mathbb{Q}/\mathbb{Z})$, so gilt $f(m_1) = f(m_2)$ für alle $m_1, m_2 \in M$ mit $m_1 \equiv m_2 \mod I_H M$. Für ein beliebiges $m \in M$ ist also insbesondere $f((\sigma_H{}^{-1} - 1) \cdot m) = f(0) = 0$ und es folgt

$$0 = ((\sigma_H - 1) \cdot f)(m), \text{ also } (\sigma_H \cdot f)(m) = f(m),$$

also $\sigma_H f = f$. Gilt andererseits $\sigma_H f = f$ für $f \in \mathrm{Hom}_\mathbb{Z}(M, \mathbb{Q}/\mathbb{Z})$, so folgt $\alpha f = 0$ für alle $\alpha \in I_H = \langle \sigma_H - 1 \rangle$ und damit

$$f(m_1) = f(m_2) \text{ für alle } m_1, m_2 \in M \text{ mit } m_1 \equiv m_2 \mod I_H M.$$

□

In Satz 2.7 haben wir gesehen, dass die Kreiszahlen modulo Torsion $\mathbb{Z}[G]$-frei mit Erzeuger

$$\gamma = \left((1-\zeta_l)(1-\zeta_l^{-1})\right)^{\frac{1+\sigma}{2}}$$

sind. Wir bezeichnen den $\mathbb{Z}[G]$-Isomorphismus

$$\overline{\mathrm{Cn}} \to \mathbb{Z}[G], \gamma \mapsto 1$$

mit τ_1 und den daraus resultierenden (dualen) $\mathbb{Z}[G]$-Isomorphismus

$$(\overline{\mathrm{Cn}})^\perp \to (\mathbb{Z}[G])^\perp, \gamma^\star \mapsto (\sigma^0)^\star = 1^\star$$

mit $\tau_1^\perp$.
Betrachtet man jetzt die exakte Sequenz

$$0 \to \overline{\mathrm{Cn}} \to \overline{U}_l \to \overline{U}_l/\overline{\mathrm{Cn}} \to 0,$$

so erhält man die Exaktheit von

$$\begin{aligned} 0 = \mathrm{Hom}_\mathbb{Z}(\overline{U}_l/\overline{\mathrm{Cn}}, \mathbb{Z}) &\to (\overline{U}_l)^\perp = \mathrm{Hom}_\mathbb{Z}(\overline{U}_l, \mathbb{Z}) \\ &\to (\overline{\mathrm{Cn}})^\perp = \mathrm{Hom}_\mathbb{Z}(\overline{\mathrm{Cn}}, \mathbb{Z}) \to \dots, \end{aligned}$$

wobei die erste Gleichheit aus der Endlichkeit von $\overline{U}_l/\overline{\mathrm{Cn}}$ folgt. Die Einschränkung

$$\mathrm{Hom}_\mathbb{Z}(\overline{U}_l, \mathbb{Z}) \to \mathrm{Hom}_\mathbb{Z}(\overline{\mathrm{Cn}}, \mathbb{Z})$$

ist also injektiv, das heißt, wir können $(\overline{U}_l)^\perp$ als Untermodul von $(\overline{\mathrm{Cn}})^\perp$ auffassen. Damit kommen wir zu folgender

Definition 4.9. Das *zu $\overline{U}_l$ gehörende Ideal* $X \subset \mathbb{Z}[G]$ wird definiert durch

$$X := \tau_2(\tau_1^\perp((\overline{U}_l)^\perp)),$$

wobei $\tau_2 : (\mathbb{Z}[G])^\perp \to \mathbb{Z}[G]$ der $\mathbb{Z}[G]$-Isomorphismus aus Proposition 4.2 ist.

Bemerkung. 1.) Korollar 4.3 liefert, dass $\overline{U}_l$ genau dann $\mathbb{Z}[G]$-frei bzw. projektiv ist, wenn X diese Eigenschaft hat. In diesem Kapitel ist X also stets $\mathbb{Z}[G]$-projektiv.

2.) Der $\mathbb{Z}[G]$-Isomorphismus $(\tau_1^\perp)^{-1} \circ {\tau_2}^{-1} : \mathbb{Z}[G] \to \overline{\mathrm{Cn}}^\perp$ induziert einen $\mathbb{Z}[G]$-Isomorphismus $\mathbb{Z}[G]/X \to \overline{\mathrm{Cn}}^\perp/\overline{U}_l^\perp$ und es folgt zusammen mit Korollar 4.6

$$|\mathbb{Z}[G]/X| = |(\overline{\mathrm{Cn}})^\perp/(\overline{U}_l)^\perp| = |\overline{U}_l/\overline{\mathrm{Cn}}| = h_l^+.$$

4.2 Ein erster Ansatz

Im vorherigen Abschnitt haben wir gesehen, dass $\overline{U}_l$ genau dann $\mathbb{Z}[G]$-frei ist, wenn das zugehörige Ideal $X \subseteq \mathbb{Z}[G]$ frei ist. Dies ist gleichbedeutend damit, dass X ein von einem Nichtnullteiler erzeugtes zyklisches Ideal ist. Es stellt sich somit die natürliche Frage, ob es in $\mathbb{Z}[G]$ für jedes h_l^+ mit $\mathrm{ggT}\left(|G|, h_l^+\right) = 1$ überhaupt ein Ideal $I = (\eta)$ mit Norm h_l^+ gibt. Die folgende Proposition beantwortet diese Frage positiv.

Proposition 4.10. *Sei $H = \langle \sigma_H \rangle$ eine endliche Gruppe der Ordnung $m > 1$, $s \in \mathbb{N}$ mit $\mathrm{ggT}\,(m, s) = 1$ und $\eta := \sum_{i=0}^{s-1} {\sigma_H}^i \in \mathbb{Z}[H]$. Dann gilt*

$$|(\mathbb{Z}[H]/(\eta)| = \mathrm{Norm}_{\mathbb{Z}[H]}(\eta) = s.$$

Insbesondere ist η Nichtnullteiler in $\mathbb{Z}[G]$ und (η) frei über $\mathbb{Z}[G]$.

Beweis. Die erste Gleichheit ist wohlbekannt (siehe [SchSt80, Satz 50.4]). Bezüglich der $\mathbb{Z}$-Basis $(1, \sigma_H, \ldots, {\sigma_H}^{m-1})$ von $\mathbb{Z}[H]$ hat die Multiplikation mit $h = \sum_{i=0}^{m-1} h_i {\sigma_H}^i$,

$$h\cdot : \mathbb{Z}[H] \to \mathbb{Z}[H], \alpha \mapsto h \cdot \alpha,$$

die darstellende Matrix

$$\mathcal{M}(h\cdot) = \begin{pmatrix} h_0 & h_1 & \cdots & h_{m-2} & h_{m-1} \\ h_{m-1} & h_0 & \cdots & h_{m-3} & h_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ h_1 & h_2 & \cdots & h_{m-1} & h_0 \end{pmatrix}^T.$$

Für $h = \eta$ und $s < m$ ergibt sich

$$h_i = \begin{cases} 1 & \text{für } i \leq s-1 \\ 0 & \text{sonst.} \end{cases}$$

Bekanntlich gilt

$$\mathrm{Norm}_{\mathbb{Z}[H]}(\eta) = \det(\mathcal{M}(\eta\cdot)).$$

Sei ζ eine primitive m-te Einheitswurzel. Dann lässt sich, da $\mathcal{M}(\eta\cdot)^T$, genau wie $\mathcal{M}(\eta\cdot)$ auch, eine zirkulante Matrix ist, die Determinante mit Hilfe der Formel

$$\begin{aligned} \det(\mathcal{M}(\eta\cdot)) &= \det(\mathcal{M}(\eta\cdot)^T) = \prod_{i=0}^{m-1} \left(\sum_{j=0}^{m-1} \zeta^{ij} h_j \right) \\ &= \prod_{i=0}^{m-1} \left(\sum_{j=0}^{s-1} \zeta^{ij} h_j \right) = \prod_{i=0}^{m-1} \left(\sum_{j=0}^{s-1} \zeta^{ij} \right) \end{aligned}$$

bestimmen (siehe bespielsweise [GKPS]).
Wir bemerken an dieser Stelle, dass diese Formel ebenso für $s \geq m$ gültig ist, da die Einträge in $\mathcal{M}(\eta\cdot)$ durch Reduktion von η mittels ${\sigma_H}^m = 1$ gegeben sind und damit, wegen $\zeta^m = 1$, den Koeffizienten der Potenzen von ζ entsprechen.
Es bleibt also $\prod_{i=0}^{m-1} \left(\sum_{j=0}^{s-1} \zeta^{ij} \right) = s$ zu zeigen.

1.) Für $i = 0$ ist $\sum_{j=0}^{s-1} \zeta^{ij} = \sum_{j=0}^{s-1} 1 = s$.

2.) Für $i \neq 0$ gilt

$$\left(\sum_{j=0}^{s-1} \zeta^{ij} \right) (1 - \zeta^i) = \sum_{j=0}^{s-1} \zeta^{ij} - \sum_{j=0}^{s-1} \zeta^{i(j+1)} = 1 - \zeta^{is}.$$

Wegen $\mathrm{ggT}\,(m, s) = 1$ ist auch ζ^s eine primitive m-te Einheitswurzel und es gilt $\prod_{i=1}^{m-1}(1 - \zeta^{is}) = \prod_{i=1}^{m-1}(1 - \zeta^i) \neq 0$.

Unter Verwendung von 1.) und 2.) ergibt sich somit

$$\begin{aligned} \prod_{i=0}^{m-1} \left(\sum_{j=0}^{s-1} \zeta^{ij} \right) \cdot \prod_{i=1}^{m-1} (1 - \zeta^i) &= s \cdot \prod_{i=1}^{m-1} \left((1 - \zeta^i) \sum_{j=0}^{s-1} \zeta^{ij} \right) \\ &= s \cdot \prod_{i=1}^{m-1} (1 - \zeta^{is}) = s \cdot \prod_{i=1}^{m-1} (1 - \zeta^i), \end{aligned}$$

also die Behauptung. □

Zwangsläufig lautet die nächste Frage, in welchen der in diesem Kapitel zu betrachtenden 69 Fälle Proposition 4.10 tatsächlich einen Erzeuger von X und damit die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ liefert.
Hier sind $|G|$ und $s = \tilde{h}_l^+$ teilerfremd, sodass für $\eta = \sum_{i=0}^{s-1} \sigma^i$ die Gleichheit $\mathbb{Z}[G]/(\eta) = \tilde{h}_l^+$ gilt. Sei nun aug die Augmentationsabbildung. Für jedes Element $\alpha \in (\eta)$ teilt s somit $\mathrm{aug}(\alpha)$. Das Normelement $N_G = \sum_{i=0}^{n-1} \sigma^i$ erfüllt zudem $\mathrm{aug}(N_G) = |G|$, es kann auf Grund von $\mathrm{ggT}\,(s, |G|) = 1$ also nicht in (η) liegen. Nach Lemma 2.3 gilt jedoch $(\mathbb{Z}[G])^G = (N_G)$. Mit Hilfe von Lemma 4.7 und der $\mathbb{Z}[G]$-Freiheit von (η) erhält man also

$$(\mathbb{Z}[G]/(\eta))^G \cong \mathbb{Z}[G]^G/(\eta)^G$$

und damit letztlich

$$(\mathbb{Z}[G]/(\eta))^G \cong \mathbb{Z}[G]^G/(\eta)^G \neq 0.$$

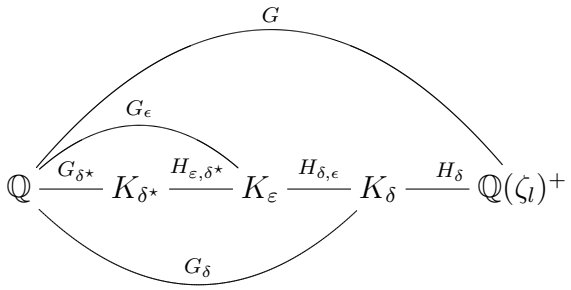
Im nächsten Abschnitt, genauer gesagt in Proposition 4.24, werden wir jedoch sehen, dass $(\mathbb{Z}[G]/X)^G = 0$ gilt. Die Frage nach der Anwendbarkeit von Propostion 4.10 ist somit schnell beantwortet - die Proposition ist auf unsere Fragestellung in keinem der 69 Fälle anwendbar.

Bemerkung. Für jedes Element $\alpha \in \mathbb{Z}[G]$ mit $\mathrm{aug}(\alpha) = 1$ gilt $\alpha \cdot N_G = N_G$ und damit in der Tat

$$(\mathbb{Z}[G]/(\alpha))^G \cong \mathbb{Z}[G]^G/(\alpha)^G = 0.$$

4.3 Arbeiten in Unterkörpern $K \subset \mathbb{Q}(\zeta_l)^+$ und den zugehörigen Gruppenringen

Die Gruppenringe, die in unseren Anwendungen auftreten, sind oft sehr groß - zu groß insbesondere für computergestützte Berechnungen. Aus diesem Grund werden wir in diesem Abschnitt zeigen, dass die für uns relevanten Informationen über $\overline{U}_l$ beziehungsweise X oft bereits durch die Untersuchung in geeigneten, hinreichend kleinen Unterkörpern K von $\mathbb{Q}(\zeta_l)^+$ zugänglich werden. In diesem Abschnitt und dem gesamtem Kapitel 4 verwenden wir folgende Notation (die bereits in Kapitel 3 eingeführt wurde).



Dabei sei $K_\delta \subset \mathbb{Q}(\zeta_l)^+$ der Unterkörper mit $[K_\delta : \mathbb{Q}] = \delta$ und $\delta^\star$ die kleinste natürliche Zahl mit $h_{K_{\delta^\star}} = h_l^+$. Einen fest gewählten Erzeuger der zyklischen Gruppe $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ der Ordnung $n := \frac{l-1}{2}$ bezeichnen wir weiterhin mit σ_G oder einfach σ. Dann ist $H_\delta = \langle \sigma^\delta \rangle$ zyklisch der Ordnung $\frac{n}{\delta}$ und $\overline{\sigma} \in G/H_\delta = G_\delta$ ist ein Erzeuger von G_δ, den wir mit σ_δ bezeichnen. Wir bemerken noch, dass daraus insbesondere $\alpha^{\sigma_\varepsilon} = \alpha^{\sigma_\delta}$ für alle $\alpha \in K_\varepsilon$ folgt.
Mit $\lambda_\delta = N_{\mathbb{Q}(\zeta_l)^+/K_\delta}(\lambda^+)$ bezeichnen wir das (bis auf Assoziierte) einzige Primelement aus $\mathcal{O}_{K_\delta}$ über l, wobei $\lambda^+ = \lambda_n = (1-\zeta_l)(1-\zeta_l^{-1})$ ist.

Die l-Einheiten $U_l^{(\delta)}$ in K_δ werden damit durch

$$U_l^{(\delta)} = \{\alpha \in K_\delta \mid v_\mathfrak{p}(\alpha) = 0 \text{ für alle Primideale } \mathfrak{p} \neq (\lambda_\delta)\}$$

definiert. Die Kreiszahlen $\mathrm{Cn}^{(\delta)}$ in K_δ sind durch

$$\mathrm{Cn}^{(\delta)} = \mathrm{Cn} \cap K_\delta$$

gegeben.
Dass sowohl l-Einheiten als auch Kreiszahlen Galoisabstieg zulassen, also

$$U_l^{(\varepsilon)} = \left(U_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} \text{ beziehungsweise } \mathrm{Cn}^{(\varepsilon)} = \left(\mathrm{Cn}^{(\delta)}\right)^{H_{\delta,\varepsilon}}$$

erfüllen, ist klar. Wir benötigen diese Eigenschaft jedoch für die l-Einheiten und Kreiszahlen modulo Torsion.

Lemma 4.11. *Unter den Voraussetzungen dieses Kapitels gilt*

$$\overline{U}_l^{(\varepsilon)} = \left(\overline{U}_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} \text{ und } \overline{\mathrm{Cn}}^{(\varepsilon)} = \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}}$$

Beweis. Hier besteht die Torsion jeweils nur aus $\{-1, 1\}$. Zudem ist $|H_{\delta,\varepsilon}|$ ungerade. Somit erhalten wir aus der exakten Sequenz

$$0 \to \{-1, 1\} \to U_l^{(\delta)} \to \overline{U}_l^{(\delta)} \to 0$$

die exakte Sequenz

$$0 \to \{-1, 1\}^{H_{\delta,\varepsilon}} \to \left(U_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} \to \left(\overline{U}_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} \to H^1(H_{\delta,\varepsilon}, \{-1, 1\}) = 0.$$

Dies entspricht

$$0 \to \{-1, 1\} \to U_l^{(\varepsilon)} \to \left(\overline{U}_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} \to 0$$

und liefert die Behauptung für die l-Einheiten. Der Beweis für die Kreiszahlen läuft analog. □

Lemma 4.12. *Sei H eine endliche Gruppe und M ein projektiver $\mathbb{Z}[H]$-Modul. Dann gilt $M^J = N_J M$ für alle Untergruppen $J \subset H$, wobei N_J das zu J gehörige Normelement ist.*

Beweis. Als projektiver $\mathbb{Z}[H]$-Modul ist M nach Satz 1.12 kohomologisch trivial, woraus sofort

$$M^J / N_J M = \hat{H}^0(J, M) = 0$$

folgt. □

Korollar 4.13. *Für $K_\varepsilon \subset K_\delta$ gelten die folgenden Aussagen:*

1.) $\mathbb{Z}[G_\delta]^{H_{\delta,\varepsilon}} \cong \mathbb{Z}[G_\varepsilon]$.

2.) Ist $\overline{U}_l^{(\delta)}$ $\mathbb{Z}[G_\delta]$*-frei, so ist auch* $\overline{U}_l^{(\varepsilon)}$ $\mathbb{Z}[G_\varepsilon]$*-frei.*

Beweis. 1.) Wir beweisen eine allgemeinere Aussage. Sei H eine endliche Gruppe und $J \subset H$ ein Normalteiler. Dann gilt nach Lemma 4.12

$$\mathbb{Z}[H]^J = N_J\mathbb{Z}[H].$$

Wir zeigen jetzt, dass durch $1 \mapsto N_J$ ein Isomorphismus $\mathbb{Z}[H/J] \to N_J\mathbb{Z}[H]$ definiert wird. Für $h \in H$ gilt genau dann $N_J h = N_J$, wenn $h \in J$ ist. Also gilt für $h_1, h_2 \in H$ genau dann $h_1 \equiv h_2 \mod J$, wenn $N_J h_1 = N_J h_2$. Hieraus folgt die Wohldefiniertheit und die Injektivität obiger Abbildung. Da die Surjektivität offensichtlich gilt, folgt die Behauptung.

2.) Sei $\overline{U}_l^{(\delta)}$ $\mathbb{Z}[G_\delta]$-frei. Aus Ranggründen gilt dann $\overline{U}_l^{(\delta)} \cong \mathbb{Z}[G_\delta]$ und somit unter Verwendung von 1.)

$$\overline{U}_l^{(\varepsilon)} = (\overline{U}_l^{(\delta)})^{H_{\delta,\varepsilon}} \cong \mathbb{Z}[G_\delta]^{H_{\delta,\varepsilon}} \cong \mathbb{Z}[G_\varepsilon].$$

□

Bemerkung. Als weitere Folge von Lemma 4.12 halten wir fest, dass

$$\overline{\mathrm{Cn}}^{(\varepsilon)} = \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}} = N_{H_{\delta,\varepsilon}}\overline{\mathrm{Cn}}^{(\delta)}$$

gilt und zusammen mit der $\mathbb{Z}[G]$-Freiheit von $\overline{\mathrm{Cn}} = \langle\gamma\rangle_{\mathbb{Z}[G]}$ aus Satz 2.7 insbesondere die $\mathbb{Z}[G_\delta]$-Freiheit von $\overline{\mathrm{Cn}}^{(\delta)} = \langle N_{H_\delta}\gamma\rangle$ folgt. Wir definieren

$$\gamma_\delta = N_{H_\delta}\gamma$$

und bemerken, dass

$$\gamma_\varepsilon = N_{H_\varepsilon}\gamma = N_{H_{\delta,\varepsilon}}\gamma_\delta$$

gilt. Wie am Ende des ersten Abschnitts dieses Kapitels wird also durch

$$\tau_{1,\delta}^{\perp} : \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^{\perp} \to (\mathbb{Z}[G_\delta])^{\perp}, (\gamma_\delta)^\star \mapsto (\sigma_\delta{}^0)^\star = 1_\delta^\star$$

ein $\mathbb{Z}[G_\delta]$-Isomorphismus definiert.

Von besonderer Bedeutung ist nun der folgende

Satz 4.14. *Seien $K_\delta \subset \mathbb{Q}(\zeta_l)^+$, $\overline{U}_l{}^{(\delta)}$ und $\overline{\mathrm{Cn}}^{(\delta)}$ wie oben. Dann gilt*

$$\left|\overline{U}_l{}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right| = h_{K_\delta}.$$

Beweis. Zuerst bemerken wir, dass nach Korollar 4.6

$$\left|\overline{U}_l{}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right| = \left|\mathbb{Z}[G_\delta]/X^{(\delta)}\right|$$

gilt. Bezeichne, wie zuvor, mit U die Einheiten des Rings der ganzen Zahlen und mit $\mathrm{Cyc} = \mathrm{Cn} \cap U$ die Kreiseinheiten von $\mathbb{Q}(\zeta_l)^+$. Für die Einheiten $U^{(\delta)} = U \cap K_\delta = U^{H_\delta}$ des Rings der ganzen Zahlen von K_δ und die entsprechenden Kreiseinheiten $\mathrm{Cyc}^{(\delta)}$ lässt sich analog zu Lemma 3.2

$$\overline{U}_l{}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)} \cong \overline{U}^{(\delta)}/\overline{\mathrm{Cyc}}^{(\delta)}$$

zeigen. Es bleibt somit noch zu zeigen, dass $\left|\overline{U}^{(\delta)}/\overline{\mathrm{Cyc}}^{(\delta)}\right| = h_{K_\delta}$ gilt. Dazu nutzen wir ein Ergebnis von Hasse, das jedoch eine andere Art von Kreiseinheiten benötigt. Wir verwenden an dieser Stelle die Notation aus [vdL82].

Definition 4.15. Sei $K \neq \mathbb{Q}$ ein reeller abelscher Zahlkörper mit Führer f. Weiter sei

$$\eta_a := \frac{\zeta_{2f} - {\zeta_{2f}}^{-1}}{{\zeta_{2f}}^{a} - {\zeta_{2f}}^{-a}},$$

wobei ζ_{2f} eine primitive $(2f)$-te Einheitswurzel ist. In der Tat ist η_a für von $2f$ teilerfremde a in $U(\mathbb{Q}(\zeta_f)^+)$ und man definiert die *Gruppe der Hasse-Kreiseinheiten von K* durch

$$\begin{aligned} C_H(K) &:= \langle \pm N_{\mathbb{Q}(\zeta_f)^+/F}(\eta_a) \mid \mathrm{ggT}\,(a, 2f) = 1, \mathbb{Q} \neq F \subset K \text{ Unterkörper} \rangle \\ &\subset U(K) = {\mathcal{O}_K}^\star. \end{aligned}$$

Für die Hasse-Kreiseinheiten gilt nun der fundamentale

Satz 4.16. *Sei $K/\mathbb{Q}$ eine reelle zyklische Erweiterung. Dann gilt*

$$[U(K) : C_H(K)] = h_K.$$

Beweis. [Ha52, II, Abschnitt 18, Satz 9] □

In dem Spezialfall $\mathbb{Q} \neq K \subset \mathbb{Q}(\zeta_l)^+$ mit $l \neq 2$ prim, ist l der Führer aller Unterkörper $\mathbb{Q} \neq F \subset K$, woraus sich mit

$$\langle \pm N_{\mathbb{Q}(\zeta_l)^+/F}(\eta_a) \mid \mathrm{ggT}\,(a, 2l) = 1\rangle \subset \langle \pm N_{\mathbb{Q}(\zeta_l)^+/K}(\eta_a) \mid \mathrm{ggT}\,(a, 2l) = 1\rangle$$

die einfache Gleichheit

$$C_H(K) = \langle \pm N_{\mathbb{Q}(\zeta_l)^+/K}(\eta_a) \mid \mathrm{ggT}\,(a, 2l) = 1\rangle$$

ergibt. In diesem Fall gilt folgendes

Lemma 4.17. *Sei $l \neq 2$ prim. Für $\mathbb{Q} \neq K \subset \mathbb{Q}(\zeta_l)^+$ gilt $C_H(K) = \mathrm{Cyc}(K)$.*

Beweis. Da die Torsionsuntergruppen in beiden Fällen aus $\{-1, 1\}$ bestehen, genügt die Betrachtung modulo Torsion. Sei ζ_{2l} eine primitive $(2l)$-te Einheitswurzel und $\zeta_l = {\zeta_{2l}}^2$.

1.) Sei zunächst $K = \mathbb{Q}(\zeta_l)^+$. Für $1 \leq a \leq \frac{l-1}{2}$ und $l \neq 2$ prim gilt $\mathrm{ggT}\,(l+2, 2l) = \mathrm{ggT}\,(2a+l, 2l) = 1$. Unter Verwendung von $\zeta_{2l}^l = -1$ folgt somit

$$\begin{aligned}
\frac{{\zeta_l}^a - {\zeta_l}^{-a}}{\zeta_l - {\zeta_l}^{-1}} &= \frac{{\zeta_{2l}}^{2a} - {\zeta_{2l}}^{-2a}}{{\zeta_{2l}}^2 - {\zeta_{2l}}^{-2}} = \frac{{\zeta_{2l}}^{2a+l} - {\zeta_{2l}}^{-2a-l}}{{\zeta_{2l}}^{l+2} - {\zeta_{2l}}^{-l-2}} \\
&= \left(\frac{{\zeta_{2l}}^{2a+l} - {\zeta_{2l}}^{-2a-l}}{\zeta_{2l} - {\zeta_{2l}}^{-1}}\right) / \left(\frac{{\zeta_{2l}}^{l+2} - {\zeta_{2l}}^{-l-2}}{\zeta_{2l} - {\zeta_{2l}}^{-1}}\right) \\
&= \frac{\eta_{l+2}}{\eta_{2a+l}} \in C_H(K).
\end{aligned}$$

Andererseits gilt für $\mathrm{ggT}\,(a, 2l) = 1$

$$\begin{aligned}
\eta_a &= \frac{\zeta_{2l} - {\zeta_{2l}}^{-1}}{{\zeta_{2l}}^a - {\zeta_{2l}}^{-a}} = {\zeta_{2l}}^{1-a}\frac{1 - {\zeta_{2l}}^{-2}}{1 - {\zeta_{2l}}^{-2a}} = {\zeta_l}^{\frac{1-a}{2}}\frac{1 - {\zeta_l}^{-1}}{1 - {\zeta_l}^{-a}} \\
&= {\zeta_l}^{\frac{l+1-(l+a)}{2}}\frac{1 - {\zeta_l}^{-l-1}}{1 - {\zeta_l}^{-l-a}} = \frac{{\zeta_l}^{\frac{l+1}{2}}(1 - {\zeta_l}^{-l-1})}{{\zeta_l}^{\frac{l+a}{2}}(1 - {\zeta_l}^{-l-a})} = \frac{{\zeta_l}^{\frac{l+1}{2}} - {\zeta_l}^{-\frac{l+1}{2}}}{{\zeta_l}^{\frac{l+a}{2}} - {\zeta_l}^{-\frac{l+a}{2}}} \\
&= \left(\frac{{\zeta_l}^{\frac{l+1}{2}} - {\zeta_l}^{-\frac{l+1}{2}}}{\zeta_l - {\zeta_l}^{-1}}\right) / \left(\frac{{\zeta_l}^{\frac{l+a}{2}} - {\zeta_l}^{-\frac{l+a}{2}}}{\zeta_l - {\zeta_l}^{-1}}\right) \in \mathrm{Cyc}(K).
\end{aligned}$$

Somit gilt die Behauptung für $K = \mathbb{Q}(\zeta_l)^+$.

2.) Mit Hilfe von 1.) bleibt für jede Untergruppe $H_\delta \subset G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ wegen

$$\overline{\mathrm{Cyc}}(K_\delta) = \overline{\mathrm{Cyc}}(\mathbb{Q}(\zeta_l)^+) \cap K_\delta = \overline{\mathrm{Cyc}}(\mathbb{Q}(\zeta_l)^+)^{H_\delta}$$

und

$$\overline{C}_H(K_\delta) = N_{H_\delta}(\overline{C}_H(\mathbb{Q}(\zeta_l)^+))$$

noch

$$N_{H_\delta}(\overline{\mathrm{Cyc}}(\mathbb{Q}(\zeta_l)^+)) = \overline{\mathrm{Cyc}}(\mathbb{Q}(\zeta_l)^+)^{H_\delta}$$

zu zeigen. Nach Proposition 2.5 gilt $\overline{\mathrm{Cyc}}(\mathbb{Q}(\zeta_l)^+) \cong I_G$. Die exakte Sequenz

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

liefert die exakte (Tate-)Kohomologiesequenz

$$\begin{aligned}\ldots \to \hat{H}^{-1}(H_\delta, \mathbb{Z}[G]) &\to \hat{H}^{-1}(H_\delta, \mathbb{Z}) \\ &\to \hat{H}^0(H_\delta, I_G) \to \hat{H}^0(H_\delta, \mathbb{Z}[G]) \to \ldots .\end{aligned}$$

Da $\mathbb{Z}[G]$ trivialerweise projektiv über sich selbst ist, folgt die Exaktheit von

$$0 \to \hat{H}^{-1}(H_\delta, \mathbb{Z}) \to \hat{H}^0(H_\delta, I_G) \to 0$$

und damit letztlich

$$\begin{aligned}{I_G}^{H_\delta}/N_{H_\delta} I_G = \hat{H}^0(H_\delta, I_G) &\cong \hat{H}^{-1}(H_\delta, \mathbb{Z}) \\ &\cong H^1(H_\delta, \mathbb{Z}) \cong \mathrm{Hom}(H_\delta, \mathbb{Z}) = 0.\end{aligned}$$

□

Dieses Lemma schließt, in Verbindung mit Satz 4.16, den Beweis von Satz 4.14 ab. □

Zusammen mit der $\mathbb{Z}[G_\delta]$-Freiheit von $\overline{\mathrm{Cn}}^{(\delta)}$ und Satz 4.14 ergibt sich, analog zu Satz 3.3, folgendes

Korollar 4.18. *Unter den Voraussetzungen dieses Kapitels ist $\overline{U}_l^{(\delta)}$ $\mathbb{Z}[G_\delta]$-projektiv.*

□

Um das zu $\overline{U}_l$ gehörende Ideal X zu definieren, mussten wir im ersten Abschnitt dieses Kapitels zeigen, dass die Einschränkung

$$\mathrm{Hom}_{\mathbb{Z}}(\overline{U}_l, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\overline{\mathrm{Cn}}, \mathbb{Z})$$

injektiv ist. Diese Herleitung lässt sich dank Satz 4.14 identisch auf die allgemeinere Situation übertragen, denn aus

$$\left|\overline{U}_l^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right| = h_{K_\delta} < \infty$$

folgt

$$\mathrm{Hom}_{\mathbb{Z}}(\overline{U}_l^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}, \mathbb{Z}) = 0.$$

Aus der exakten Sequenz

$$0 \to \overline{\mathrm{Cn}}^{(\delta)} \to \overline{U}_l^{(\delta)} \to \overline{U}_l^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)} \to 0$$

resultiert damit die Exaktheit von

$$0 = \mathrm{Hom}_{\mathbb{Z}}(\overline{U}_l^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}, \mathbb{Z}) \to \left(\overline{U}_l^{(\delta)}\right)^\perp \to \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^\perp \to \ldots .$$

Definition 4.19. Das zu $\overline{U}_l^{(\delta)}$ gehörende Ideal $X^{(\delta)} \subset \mathbb{Z}[G_\delta]$ ist definiert durch

$$X^{(\delta)} := \tau_{2,\delta}(\tau_{1,\delta}^{\perp}((\overline{U}_l^{(\delta)})^{\perp})).$$

Dabei ist $\tau_{2,\delta} : (\mathbb{Z}[G_\delta])^{\perp} \to \mathbb{Z}[G_\delta]$ der $\mathbb{Z}[G_\delta]$-Isomorphismus, der durch Proposition 4.2 gegeben ist und $\tau_{1,\delta}^{\perp} : \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^{\perp} \to (\mathbb{Z}[G_\delta])^{\perp}$ der $\mathbb{Z}[G_\delta]$-Isomorphismus aus der Bemerkung nach Korollar 4.13.

Bemerkung. 1.) Wieder folgt aus Korollar 4.3, dass $X^{(\delta)}$ genau dann $\mathbb{Z}[G_\delta]$-frei bzw. projektiv ist, wenn $\overline{U}_l^{(\delta)}$ dies erfüllt.

2.) Nach Korollar 4.18 sind alle $X^{(\delta)}$ in diesem Kapitel $\mathbb{Z}[G_\delta]$-projektiv.

3.) Nach Korollar 4.6 und Satz 4.14 gilt

$$\left|\mathbb{Z}[G_\delta]/X^{(\delta)}\right| = \left|\overline{U}_l^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right| = h_{K_\delta}.$$

4.) Ist $X^{(\delta)}$ für ein δ mit $K_\delta \subset \mathbb{Q}(\zeta_l)^+$ nicht $\mathbb{Z}[G_\delta]$-frei, so ist $\overline{U}_l$ nach Korollar 4.13 nicht $\mathbb{Z}[G]$-frei.

Als nächstes sollen auch die Begriffe der Augmentationsabbildung und des Augmentationsideals für diese allgemeinere Situation eingeführt werden.

Definition 4.20. Sei $K_\varepsilon \subset K_\delta \subset \mathbb{Q}(\zeta_l)^+$ und seien wie zuvor $G_\delta = \langle\sigma_\delta\rangle$ und $G_\varepsilon = \langle\sigma_\varepsilon\rangle$. Die *(relative) Augmentationsabbildung von* $\mathbb{Z}[G_\delta]$ *nach* $\mathbb{Z}[G_\varepsilon]$ wird durch

$$\mathrm{aug}_{\delta,\varepsilon} : \mathbb{Z}[G_\delta] \to \mathbb{Z}[G_\varepsilon], \quad \sigma_\delta \mapsto \sigma_\varepsilon$$

definiert. Durch $I_{\delta,\varepsilon} := \ker(\mathrm{aug}_{\delta,\varepsilon})$ ist das zugehörige (relative) Augmentationsideal gegeben. Ist $\varepsilon = 1$, so schreiben wir auch aug_δ statt $\mathrm{aug}_{\delta,1}$ und I_δ statt $I_{\delta,1}$. Für eine Untergruppe $J \subset G_\delta$ bezeichnen wir das Normelement $\sum_{g\in J} g \in \mathbb{Z}[G_\delta]$ mit N_J.

Für $G_\delta = G$ und $\varepsilon = 1$ entspricht $\mathrm{aug}_{\delta,\varepsilon}$ natürlich der bereits bekannten Augmentationsabbildung aug.
Die Augmentationsabbildung $\mathrm{aug}_{\delta,\varepsilon}$ ist offenbar ein surjektiver Ringhomomorphismus. Das Bild von $X^{(\delta)}$ ist also wieder ein Ideal in $\mathbb{Z}[G_\varepsilon]$. Dass es sich bei diesem Ideal gerade um $X^{(\varepsilon)}$ handelt, ist Aussage der

Proposition 4.21. *Sei* $K_\varepsilon \subset K_\delta \subset \mathbb{Q}(\zeta_l)^+$ *und* $\mathrm{aug}_{\delta,\varepsilon} : \mathbb{Z}[G_\delta] \to \mathbb{Z}[G_\varepsilon]$ *die Augementationsabbildung. Dann ist* $\mathrm{aug}_{\delta,\varepsilon}(X^{(\delta)}) = X^{(\varepsilon)}$.

Beweis. Betrachte dazu das folgende Diagramm

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbb{Z}}(\overline{U}_l^{(\delta)},\mathbb{Z}) & \xrightarrow[\pi_0]{} & \mathrm{Hom}_{\mathbb{Z}}(\overline{U}_l^{(\varepsilon)},\mathbb{Z}) \\
\big\downarrow{\scriptstyle \tau_{0,\delta}} & & \big\downarrow{\scriptstyle \tau_{0,\varepsilon}} \\
\mathrm{Hom}_{\mathbb{Z}}(\overline{\mathrm{Cn}}^{(\delta)},\mathbb{Z}) & \xrightarrow[\pi_1]{} & \mathrm{Hom}_{\mathbb{Z}}(\overline{\mathrm{Cn}}^{(\varepsilon)},\mathbb{Z}) \\
\big\downarrow{\scriptstyle \tau_{1,\delta}^{\perp}} & & \big\downarrow{\scriptstyle \tau_{1,\varepsilon}^{\perp}} \\
\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_\delta],\mathbb{Z}) & \xrightarrow[\pi_2]{} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_\varepsilon],\mathbb{Z}) \\
\big\downarrow{\scriptstyle \tau_{2,\delta}} & & \big\downarrow{\scriptstyle \tau_{2,\varepsilon}} \\
\mathbb{Z}[G_\delta] & \xrightarrow[\mathrm{aug}_{\delta,\varepsilon}]{} & \mathbb{Z}[G_\varepsilon],
\end{array}$$

wobei die Abbildungen π_0, π_1, $\tau_{0,\delta}$ und $\tau_{0,\varepsilon}$ die jeweiligen Einschränkungen sind. Damit ist das obere Rechteck sicherlich kommutativ. An dieser Stelle untersuchen wir, wie die Einschränkung π_1 auf den $(\gamma_\delta{}^{\sigma_\delta{}^i})^\star$, $0 \le i \le \delta-1$, wirkt. Sei dazu $\alpha \in \overline{\mathrm{Cn}}^{(\varepsilon)} \subset \overline{\mathrm{Cn}}^{(\delta)}$, das heißt, dass

$$\begin{aligned}
\alpha &= \prod_{i=0}^{\delta-1} \gamma_\delta{}^{N_{H_{\delta,\varepsilon}}\alpha_i\sigma_\delta{}^i} = \prod_{i=0}^{\delta-1} \gamma_\varepsilon{}^{\alpha_i\sigma_\delta{}^i} = \prod_{i=0}^{\delta-1} \gamma_\varepsilon{}^{\alpha_i\sigma_\varepsilon{}^i} \\
&= \prod_{i=0}^{\varepsilon-1} \gamma_\varepsilon{}^{(\alpha_i+\alpha_{i+\varepsilon}+\ldots+\alpha_{i+\delta-\varepsilon})\sigma_\varepsilon{}^i}
\end{aligned}$$

mit $\alpha_i \in \mathbb{Z}$ für alle i. Nun erhält man einerseits

$$\begin{aligned}
\left(\gamma_\delta{}^{\sigma_\delta{}^j}\right)^\star(\alpha) &= (\gamma_\delta{}^{\sigma_\delta{}^j})^\star \left(\prod_{i=0}^{\delta-1} \gamma_\delta{}^{N_{H_{\delta,\varepsilon}}\alpha_i\sigma_\delta{}^i}\right) \\
&= \prod_{i=0}^{\delta-1} \left(\gamma_\delta{}^{\sigma_\delta{}^j}\right)^\star \left(\gamma_\delta{}^{(1+\sigma_\delta{}^\varepsilon+\ldots+\sigma_\delta{}^{\delta-\varepsilon})\alpha_i\sigma_\delta{}^i}\right) \\
&= \alpha_j + \alpha_{j+\varepsilon} + \ldots + \alpha_{j+\delta-\varepsilon}
\end{aligned}$$

und andererseits

$$\begin{aligned}\left(\gamma_\varepsilon{}^{\sigma_\varepsilon{}^j}\right)^\star(\alpha) &= \left(\gamma_\varepsilon{}^{\sigma_\varepsilon{}^j}\right)^\star\left(\prod_{i=0}^{\varepsilon-1}\gamma_\varepsilon{}^{(\alpha_i+\alpha_{i+\varepsilon}+\ldots+\alpha_{i+\delta-\varepsilon})\sigma_\varepsilon{}^i}\right)\\ &= \prod_{i=0}^{\varepsilon-1}\left(\gamma_\varepsilon{}^{\sigma_\varepsilon{}^j}\right)^\star\left(\gamma_\varepsilon{}^{(\alpha_i+\alpha_{i+\varepsilon}+\ldots+\alpha_{i+\delta-\varepsilon})\sigma_\varepsilon{}^i}\right)\\ &= \alpha_j+\alpha_{j+\varepsilon}+\ldots+\alpha_{j+\delta-\varepsilon},\end{aligned}$$

wobei die Indizes modulo δ zu verstehen sind. Es folgt, dass für $0 \le i \le \delta-1$

$$\pi_1((\gamma_\delta{}^{\sigma_\delta{}^i})^\star) = (\gamma_\varepsilon{}^{\sigma_\varepsilon{}^i})^\star$$

gilt.
Wir wenden uns jetzt dem mittleren Rechteck zu. Der $\mathbb{Z}[G_\delta]$-Isomorphismus

$$\tau_{1,\delta}^\perp : \mathrm{Hom}_\mathbb{Z}(\overline{\mathrm{Cn}}^{(\delta)},\mathbb{Z}) \to \mathrm{Hom}_\mathbb{Z}(\mathbb{Z}[G_\delta],\mathbb{Z}), \quad \gamma_\delta^\star = (\gamma_\delta{}^{\sigma_\delta{}^0})^\star \mapsto (\sigma_\delta{}^0)^\star,$$

erfüllt insbesondere

$$\tau_{1,\delta}^\perp((\gamma_\delta{}^{\sigma_\delta{}^i})^\star) = (\sigma_\delta{}^i)^\star.$$

Analog wirkt der $\mathbb{Z}[G_\varepsilon]$-Isomorphismus

$$\tau_{1,\varepsilon}^\perp : \mathrm{Hom}_\mathbb{Z}(\overline{\mathrm{Cn}}^{(\varepsilon)},\mathbb{Z}) \to \mathrm{Hom}_\mathbb{Z}(\mathbb{Z}[G_\varepsilon],\mathbb{Z}), \quad \gamma_\varepsilon^\star = (\gamma_\varepsilon{}^{\sigma_\varepsilon{}^0})^\star \mapsto (\sigma_\varepsilon{}^0)^\star$$

auf der (kanonischen) $\mathbb{Z}$-Basis durch

$$\tau_{1,\varepsilon}^\perp((\gamma_\varepsilon{}^{\sigma_\varepsilon{}^i})^\star) = (\sigma_\varepsilon{}^i)^\star.$$

Zusammen mit der $\mathbb{Z}$-linearen Abbildung

$$\pi_2 : (\sigma_\delta{}^i)^\star \mapsto (\sigma_\varepsilon{}^i)^\star \text{ für } i \in \mathbb{Z}$$

und mit obiger Beschreibung von π_1 folgt die Kommutativität des mittleren Rechtecks.
Die Kommutativität des unteren Rechtecks folgt sofort aus

$$\begin{aligned}&\pi_2((\sigma_\delta{}^i)^\star) = (\sigma_\varepsilon{}^i)^\star, && \tau_{2,\varepsilon}((\sigma_\varepsilon{}^i)^\star) = \sigma_\varepsilon{}^i,\\ &\tau_{2,\delta}((\sigma_\delta{}^i)^\star) = \sigma_\delta{}^i \quad \text{und} && \mathrm{aug}_{\delta,\varepsilon}(\sigma_\delta{}^i) = \sigma_\varepsilon{}^i\end{aligned}$$

für alle $i \in \mathbb{Z}$.
Wegen

$$\tau_{2,\delta}(\tau_{1,\delta}^\perp(\tau_{0,\delta}(\mathrm{Hom}_\mathbb{Z}(\overline{U}_l^{(\delta)},\mathbb{Z})))) = X^{(\delta)}$$

und

$$\tau_{2,\varepsilon}(\tau_{1,\varepsilon}^\perp(\tau_{0,\varepsilon}(\mathrm{Hom}_\mathbb{Z}(\overline{U}_l^{(\varepsilon)},\mathbb{Z})))) = X^{(\varepsilon)}$$

bleibt die Surjektivität von π_0 nachzuweisen. Dazu führen wir sogenannte reine Untermoduln ein.

Definition 4.22. Sei W ein torsionsfreier $\mathbb{Z}$-Modul. Man nennt $V \subset W$ einen *reinen Untermodul von* W, wenn

$$x \in W, nx \in V \text{ für ein } n \in \mathbb{Z} \text{ stets } x \in V \text{ impliziert.}$$

Bemerkung. Für einen beliebigen kommutativen Ring R nennt man einen R-Untermodul V eines R-Moduls W *rein*, wenn für alle $x \in W$ und $r \in R$ mit $rx \in V$ folgt, dass es ein $y \in V$ mit $rx = ry$ gibt (siehe beispielsweise [CR06, §16 A]). Für unsere Zwecke genügt jedoch die obige spezielle Definition.

Nach Lemma 4.11 gilt für die l-Einheiten modulo Torsion

$$\left(\overline{U}_l^{(\delta)}\right)^{H_{\delta,\varepsilon}} = \overline{U}_l^{(\varepsilon)}.$$

Das wird nun verwendet, um zu zeigen, dass $\overline{U}_l^{(\varepsilon)} \subset \overline{U}_l^{(\delta)}$ rein ist. Sei also $x \in \overline{U}_l^{(\delta)}$ und $x^n \in \overline{U}_l^{(\varepsilon)}$ für ein $n \in \mathbb{Z}$. Es gilt

$$(x^{\sigma_{H_{\delta,\varepsilon}}})^n = x^{(n\sigma_{H_{\delta,\varepsilon}})} = (x^n)^{\sigma_{H_{\delta,\varepsilon}}} = x^n,$$

da x^n invariant unter $\sigma_{H_{\delta,\varepsilon}}$ ist. Somit ist $(x^{\sigma_{H_{\delta,\varepsilon}}}/x)^n = 1$, d.h. $x^{\sigma_{H_{\delta,\varepsilon}}}/x$ ist, als Torsionselement in $\overline{U}_l^{(\delta)}$, gleich 1. Deshalb muss x bereits in $\overline{U}_l^{(\varepsilon)}$ liegen.

Bemerkung.
1.) Sei W ein torsionsfreier $\mathbb{Z}$-Modul und V ein Untermodul von W. Dann ist V genau dann rein, wenn W/V torsionsfrei ist.

2.) Ist W ein torsionsfreier $\mathbb{Z}$-Modul, $V \subset W$ rein und W/V endlich erzeugt, so ist W/V $\mathbb{Z}$-frei.

Lemma 4.23. *Sei $V \subset W$ rein, W torsionsfrei und W/V endlich erzeugt. Dann ist die Einschränkung*

$$\mathrm{Hom}_{\mathbb{Z}}(W, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{Z})$$

surjektiv.

Beweis. Die exakte Sequenz

$$0 \to V \to W \to W/V \to 0$$

ergibt die exakte Sequenz

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(W/V, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(W, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(W/V, \mathbb{Z}),$$

wobei $\mathrm{Ext}^1_{\mathbb{Z}}(W/V, \mathbb{Z}) = 0$ aus der Freiheit von W/V folgt. Dies ergibt die Behauptung. □

Die Anwendung des Lemmas auf $\overline{U}_l^{(\varepsilon)} \subset \overline{U}_l^{(\delta)}$ beendet letztendlich den Beweis von Proposition 4.21. □

Bemerkung. Die Surjektivität von π_0 kann unter der zusätzlichen Voraussetzung $h_{K_\delta} = h_{K_\varepsilon}$ auch direkt aus der Kommutativität des Diagramms und der Surjektivität von $\mathrm{aug}_{\delta,\varepsilon}$ mittels

$$\left|(\overline{\mathrm{Cn}}^{(\delta)})^\perp/(\overline{U}_l^{(\delta)})^\perp\right| = \left|(\overline{\mathrm{Cn}}^{(\varepsilon)})^\perp/(\overline{U}_l^{(\varepsilon)})^\perp\right|$$

gefolgert werden.

Proposition 4.24. *Sei $K_\varepsilon \subset K_\delta \subset \mathbb{Q}(\zeta_l)^+$. Dann gilt*

$$\left(\overline{U}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}} \cong \left(\overline{U}^{(\delta)}\right)^{H_{\delta,\varepsilon}} / \left(\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}} = \overline{U}_l^{(\varepsilon)}/\overline{\mathrm{Cn}}^{(\varepsilon)}.$$

Insbesondere gilt also

$$\left(\overline{U}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}} = 0 \;\Leftrightarrow\; h_{K_\varepsilon} = 1$$

und damit

$$\left(\mathbb{Z}[G_\delta]/X^{(\delta)}\right)^{H_{\delta,\varepsilon}} = 0 \;\Leftrightarrow\; h_{K_\varepsilon} = 1.$$

Beweis. Die erste Aussage folgt mit der $\mathbb{Z}[G_\delta]$-Freiheit von $\overline{\mathrm{Cn}}^{(\delta)}$ aus Lemma 4.7 und aus Lemma 4.11. Diese Aussage und Satz 4.14 implizieren nun

$$\left(\overline{U}^{(\delta)}/\overline{\mathrm{Cn}}^{(\delta)}\right)^{H_{\delta,\varepsilon}} = 0 \;\Leftrightarrow\; h_{K_\varepsilon} = 1,$$

woraus sich mit Hilfe von Lemma 4.5 und Lemma 4.8 schließlich

$$\left(\mathbb{Z}[G_\delta]/X^{(\delta)}\right)^{H_{\delta,\varepsilon}} = 0 \;\Leftrightarrow\; h_{K_\varepsilon} = 1$$

ergibt. □

In Verbindung mit Satz 4.14 liefert dies eine weitere wichtige Aussage, die wir in einer Proposition zusammenfassen.

Proposition 4.25. *Sei q eine Primzahl, ζ_q eine primitive q-te Einheitswurzel und $\delta \geq 2$ eine zu q teilerfremde Zahl derart, dass $K_\delta \subset K_{q\delta} \subset \mathbb{Q}(\zeta_l)^+$ und $h_{K_\delta} = h_{K_{q\delta}}$ gilt.*

In dem Pullback-Diagramm (siehe Beispiel 1)

$$\begin{array}{ccc} \mathbb{Z}[G_{q\delta}] & \xrightarrow[i_2]{} & \mathbb{Z}[\zeta_q][G_\delta] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z}[G_\delta] & \xrightarrow{j_1} & \mathbb{F}_q[G_\delta] \end{array}$$

gilt $i_2(X^{(q\delta)}) = \mathbb{Z}[\zeta_q][G_\delta]$.

Beweis. Wir bemerken zunächst, dass $i_1 = \mathrm{aug}_{q\delta,\delta}$ und somit nach Proposition 4.21 $i_1(X^{(q\delta)}) = X^{(\delta)}$ gilt. Sei t eine Primzahl, die teilerfremd zu h_{K_δ} ist und bezeichne $i_{1,t}$ beziehungsweise $i_{2,t}$ die t-Lokalisierungen von i_1 und i_2. Die Lokalisierung $(X^{(q\delta)})_t$ ist dann bereits ganz $\mathbb{Z}_t[G_{q\delta}]$ und damit gilt

$$(i_2(X^{(q\delta)}))_t = i_{2,t}((X^{(p\delta)})_t) = \mathbb{Z}_t[\zeta_q][G_\delta].$$

Sei nun t eine Primzahl und ein Teiler von h_{K_δ}. Nach Voraussetzung ist $\mathrm{ggT}\,(t,q) = 1$ und damit

$$\begin{array}{ccc} \mathbb{Z}_t[G_{q\delta}] & \xrightarrow[i_2]{} & \mathbb{Z}_t[\zeta_q][G_\delta] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z}_t[G_\delta] & \xrightarrow{j_1} & (\mathbb{F}_q[G_\delta])_t = 0. \end{array}$$

Das heißt, dass

$$\mathbb{Z}_t[G_{q\delta}] \cong \mathbb{Z}_t[G_\delta] \times \mathbb{Z}_t[\zeta_q][G_\delta]$$

ist. Für $X^{(q\delta)}$ ergibt sich also

$$(X^{(q\delta)})_t \cong i_{1,t}((X^{(q\delta)})_t) \times i_{2,t}((X^{(q\delta)})_t) = (X^{(\delta)})_t \times (i_2(X^{(q\delta)}))_t,$$

was durch Betrachtung des Index von $(X^{(q\delta)})_t$ in $\mathbb{Z}_t[G_{q\delta}]$ zu

$$(i_2(X^{(q\delta)}))_t = \mathbb{Z}_t[\zeta_q][G_\delta]$$

und damit zur Behauptung führt. □

4.4 $\mathbb{Z}[G_\delta]$-Freiheit von $\overline{U}_l^{(\delta)}$ und die Existenz von Minkowski-Einheiten in K_δ

Wir beginnen diesen Abschnitt mit der grundlegenden

Definition 4.26. Sei $K/\mathbb{Q}$ eine endliche Galoiserweiterung mit Galoisgruppe G und sei $\overline{U}$ die Einheitengruppe von $\mathcal{O}_K$ modulo der Gruppe von Einheitswurzeln in K. Gibt es eine Einheit $\alpha \in \overline{U}$ derart, dass

$$\langle \alpha \rangle_{\mathbb{Z}[G]} = \overline{U}$$

ist, so nennt man α *Minkowski-Einheit* in K.

Bemerkung. Gelegentlich wird in der Literatur zwischen Minkowski-Einheiten und sogenannten starken Minkowski-Einheiten unterschieden. Wir verzichten hier auf Details, bemerken jedoch, dass in unserer Situation beide Begriffe ohnehin zusammenfallen ([Nar04, Proposition 3.27]).

Jetzt werden wir die Verbindung zwischen $\mathbb{Z}[G_\delta]$-Freiheit der l-Einheiten modulo Torsion $\overline{U}_l^{(\delta)}$ und der Existenz einer Minkowski-Einheit in K_δ herstellen. Dazu benötigen wir einen bekannten Hilfssatz.

Lemma 4.27. *Es gibt genau dann eine Minkowski-Einheit in K_δ, wenn $\overline{U}^{(\delta)}$ frei über $\mathbb{Z}[G]/(N_{G_\delta})$ ist.*

Beweis. Ist $\overline{U}^{(\delta)}$ frei über $\mathbb{Z}[G_\delta]/(N_{G_\delta})$, so ist aus $\mathbb{Z}$-Ranggründen die Existenz einer Minkowski-Einheit klar. Gilt andererseits $\overline{U}^{(\delta)} = \langle \alpha \rangle_{\mathbb{Z}[G_\delta]}$, so ist die Abbildung

$$\mathbb{Z}[G_\delta]/(N_{G_\delta}) \to \overline{U}^{(\delta)}, \quad 1 \mapsto \alpha$$

wegen $u^{N_{G_\delta}} = 1$ für alle $u \in \overline{U}^{(\delta)}$ sicher surjektiv. Die Injektivität folgt wieder aus der Tatsache, dass $\overline{U}^{(\delta)}$ und $\mathbb{Z}[G_\delta]/(N_{G_\delta})$ den gleichen $\mathbb{Z}$-Rang haben. □

Damit kommen wir bereits zum Hauptresultat dieses Abschnitts:

Satz 4.28. *Sei $l \equiv 3 \mod 4$ eine Primzahl mit $\mathrm{ggT}\left(\frac{l-1}{2}, h_l^+\right) = 1$ und δ ein Teiler von $\frac{l-1}{2}$. Dann gibt es genau dann eine Minkowski-Einheit in K_δ, wenn $\overline{U}_l^{(\delta)}$ frei über $\mathbb{Z}[G_\delta]$ ist.*

Beweis. Sei zunächst $\overline{U}_l^{(\delta)}$ $\mathbb{Z}[G_\delta]$-frei. Offensichtlich gilt

$$\overline{U}^{(\delta)} = \ker(N_{G_\delta} : \overline{U}_l^{(\delta)} \to \overline{U}_l^{(\delta)})$$

und damit wegen $\overline{U}_l^{(\delta)} \cong \mathbb{Z}[G_\delta]$

$$\overline{U}^{(\delta)} \cong \ker(N_{G_\delta} : \mathbb{Z}[G_\delta] \to \mathbb{Z}[G_\delta]) \cong I_\delta \cong \mathbb{Z}[G_\delta]/(N_{G_\delta}).$$

Dabei folgt die Isomorphie $\mathbb{Z}[G_\delta]/(N_{G_\delta}) \cong I_\delta$ exakt wie in Proposition 2.5. Wir setzen jetzt voraus, dass es eine Minkowski-Einheit in K_δ gibt. Nach obigem Lemma ist das gleichbedeutend mit der Aussage, dass $\overline{U}^{(\delta)}$ frei über $\mathbb{Z}[G_\delta]/(N_{G_\delta})$ ist. Analog zu Beispiel 1 sieht man, dass folgendes Diagramm ein Pullback-Diagramm ist:

$$\begin{array}{ccc} \mathbb{Z}[G_\delta] & \xrightarrow[i_2]{} & \mathbb{Z}[G_\delta]/(N_{G_\delta}) \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z} & \xrightarrow{j_1} & \mathbb{Z}/\delta\mathbb{Z}. \end{array}$$

Da $\overline{U}_l^{(\delta)}$ $\mathbb{Z}[G_\delta]$-projektiv ist, gilt $\overline{U}_l^{(\delta)} \cong (P_1, P_2, h)$ mit projektiven $\mathbb{Z}$- beziehungsweise $\mathbb{Z}[G_\delta]/(N_{G_\delta})$-Moduln P_1 und P_2. Weiter gilt nach Satz 1.16

$$P_2 \cong i_{2\#}\overline{U}_l^{(\delta)} = \overline{U}_l^{(\delta)} \otimes_{\mathbb{Z}[G_\delta]} \mathbb{Z}[G_\delta]/(N_{G_\delta}).$$

Wir zeigen jetzt, dass $\overline{U}^{(\delta)}$ und P_2 als $\mathbb{Z}[G_\delta]$-Moduln und damit auch als $\mathbb{Z}[G_\delta]/(N_{G_\delta})$-Moduln isomorph sind:

$$\begin{aligned} \overline{U}^{(\delta)} &= \ker(N_{G_\delta} : \overline{U}_l^{(\delta)} \to \overline{U}_l^{(\delta)}) \cong I_\delta \overline{U}_l^{(\delta)} \cong I_\delta \otimes_{\mathbb{Z}[G_\delta]} \overline{U}_l^{(\delta)} \\ &\cong \mathbb{Z}[G_\delta]/(N_{G_\delta}) \otimes_{\mathbb{Z}[G_\delta]} \overline{U}_l^{(\delta)} \cong P_2. \end{aligned}$$

Hier haben wir verwendet, dass für jeden projektiven Modul M über einem kommutativen Ring R und jedes Ideal $\mathfrak{a} \subset R$ ein R-Isomorphismus

$$\mathfrak{a} \otimes_R M \to \mathfrak{a}M$$

existiert.

Da $[\overline{U}^{(\delta)}] \in \mathrm{Pic}(\mathbb{Z}[G_\delta]/(N_{G_\delta}))$ trivial ist und $\mathrm{Pic}(\mathbb{Z}) = 0$ ist, gilt in der zu obigem Pullback-Diagramm gehörenden Mayer-Vietoris-Sequenz

$$\begin{aligned} \mathbb{Z}[G_\delta]^\star \xrightarrow{f_1} \mathbb{Z}^\star \oplus (\mathbb{Z}[G_\delta]/(N_{G_\delta}))^\star \xrightarrow{g_1} \mathbb{Z}/\delta\mathbb{Z}^\star \xrightarrow{\rho} \\ \mathrm{Pic}(\mathbb{Z}[G_\delta]) \xrightarrow{f_0} \mathrm{Pic}(\mathbb{Z}) \oplus \mathrm{Pic}(\mathbb{Z}[G_\delta]/(N_{G_\delta})) \xrightarrow{g_0} \mathrm{Pic}(\mathbb{Z}/\delta\mathbb{Z}), \end{aligned}$$

dass $[\overline{U}_l^{(\delta)}] \in \ker(f_0) = \mathrm{Im}(\rho)$ ist. Es genügt also zu zeigen, dass g_1 surjektiv ist und damit $\mathrm{Im}(\rho) = 0$ ist. Seien dazu $d, e \in (\mathbb{Z}/\delta\mathbb{Z})^\star$ so, dass $de = 1 + r \cdot \delta$ mit $r \in \mathbb{N}$ gilt. Definiere $\tau_d := \sum_{i=0}^{d-1} {\sigma_\delta}^i \in \mathbb{Z}[G_\delta]/(N_{G_\delta})$.
Offenbar gilt $j_2(\tau_d) = d$ und

$$\tau_d \cdot \sum_{i=0}^{e-1} {\sigma_\delta}^{id} = N_{G_\delta} + {\sigma_\delta}^{\delta} N_{G_\delta} + \ldots {\sigma_\delta}^{(r-1)\delta} N_{G_\delta} + {\sigma_\delta}^{r\delta} \equiv 1 \mod N_{G_\delta},$$

also $\tau_d \in (\mathbb{Z}[G_\delta]/(N_{G_\delta}))^\star$, woraus die Behauptung folgt. □

Bemerkung. Die im Beweis von Satz 4.28 genutzte Konstruktion der Einheit τ_d in $\mathbb{Z}[G_\delta]/(N_{G_\delta})$ ist in [Hoe92, (8)] zu finden.

4.5 Identifikation von $X^{(\delta)}$

Wir werden jetzt einige Ergebnisse von Abschnitt 4.3 einsetzen, um einen Ansatz zur Identifikation eines Erzeugendensystems von $X^{(\delta)}$ zu finden. In diesem Abschnitt werden wir häufig die Isomorphie

$$\mathbb{Z}[G_\delta] \cong \mathbb{Z}[x]/(x^\delta - 1), \quad \sigma_\delta \mapsto x,$$

verwenden.
Sei $h_{K_\delta} = p^e \cdot s$, wobei p eine Primzahl ist und $e, s \geq 1$ ganze Zahlen mit $\mathrm{ggT}\,(p, s) = 1$. Weiter sei $\delta_p \mid \delta$ die kleinste ganze Zahl, sodass $p^e \mid h_{K_{\delta_p}}$ ist. Zusätzlich setzen wir voraus, dass $p \nmid h_{K_\varepsilon}$ für alle von δ_p verschiedenen Teiler ε von δ_p. Es gilt

$$x^\delta - 1 = \prod_{\varepsilon \mid \delta} \phi_\varepsilon(x),$$

wobei $\phi_\varepsilon(x)$ das ε-te Kreisteilungspolynom ist. Wir definieren

$$r_1(x) := \prod_{\varepsilon \mid \delta_p, \varepsilon \neq \delta_p} \phi_\varepsilon(x)$$

und

$$r_2(x) := \prod_{\varepsilon \mid \delta, \varepsilon \nmid \delta_p} \phi_\varepsilon(x) = \frac{x^\delta - 1}{r_1(x)\phi_{\delta_p}(x)},$$

sodass $x^\delta - 1 = r_1(x)\phi_{\delta_p}(x)r_2(x)$ und $x^{\delta_p} - 1 = r_1(x)\phi_{\delta_p}(x)$ gilt.
Für die p-Lokalisierung haben wir somit, da $\mathrm{ggT}\,(p, \delta) = 1$ ist, Isomorphismen

$$\omega = (\omega_1, \omega_2, \omega_3) : \mathbb{Z}_p[G_\delta] \cong \mathbb{Z}_p[x]/(r_1(x)) \times \mathbb{Z}_p[x]/(\phi_{\delta_p}(x)) \times \mathbb{Z}_p[x]/(r_2(x))$$

und

$$\tilde{\omega} = (\tilde{\omega}_1, \omega_3) : \mathbb{Z}_p[G_\delta] \cong \mathbb{Z}_p[x]/(x^{\delta_p} - 1) \times \mathbb{Z}_p[x]/(r_2(x)).$$

Wir zeigen jetzt, dass

$$\omega_1((X^{(\delta)})_p) = \mathbb{Z}_p[x]/(r_1(x)) \text{ und } \omega_3((X^{(\delta)})_p) = \mathbb{Z}_p[x]/(r_2(x))$$

erfüllt ist.

1.) Angenommen, es gilt $\omega_1((X^{(\delta)})_p) \neq \mathbb{Z}_p[x]/(r_1(x))$. Dann gibt es ein $\varepsilon \mid \delta_p$, $\varepsilon \neq \delta_p$, sodass das Bild von $(X^{(\delta)})_p$ unter

$$\mathbb{Z}_p[G_\delta] \to \mathbb{Z}_p[x]/(x^\varepsilon - 1) \cong \mathbb{Z}_p[G_\varepsilon], \sigma_\delta \mapsto x \mapsto \sigma_\varepsilon$$

nicht ganz $\mathbb{Z}[G_\varepsilon]$ ist. Bezeichnet $\mathrm{aug}_{\delta,\varepsilon,p}$ die p-Lokalisierung von $\mathrm{aug}_{\delta,\varepsilon}$, so ist mit Proposition 4.21

$$\omega_1((X^{(\delta)})_p) = \mathrm{aug}_{\delta,\varepsilon,p}((X^{(\delta)})_p) = (X^{(\varepsilon)})_p$$

und wegen $\mathrm{ggT}\,(p, h_{K_\varepsilon}) = 1$ gilt nach Proposition 4.24

$$0 = \left(\overline{U}_l^{(\varepsilon)}/\overline{\mathrm{Cn}}^{(\varepsilon)}\right)_p = \left(\overline{U}_l^{(\varepsilon)}\right)_p / \left(\overline{\mathrm{Cn}}^{(\varepsilon)}\right)_p.$$

Lemma 4.5 und Lemma 4.8 führen damit zu

$$\mathbb{Z}_p[G_\varepsilon]/\omega_1((X^{(\delta)})_p) = \mathbb{Z}_p[G_\varepsilon]/(X^{(\varepsilon)})_p = 0,$$

also zu einem Widerspruch.

2.) Das Bild von $(X^{(\delta)})_p$ unter

$$\mathbb{Z}_p[G_\delta] \xrightarrow{\tilde{\omega}_1} \mathbb{Z}_p[x]/(x^{\delta_p} - 1) \cong \mathbb{Z}_p[G_{\delta_p}], \sigma_\delta \mapsto x \mapsto \sigma_{\delta_p}$$

ist

$$\mathrm{aug}_{\delta,\delta_p,p}((X^{(\delta)})_p) = (X^{(\delta_p)})_p,$$

wobei $\mathrm{aug}_{\delta,\delta_p,p}$ wie oben die p-Lokalisierung von $\mathrm{aug}_{\delta,\delta_p}$ bezeichnet. Wegen $\left|\mathbb{Z}_p[G_{\delta_p}]/(X^{(\delta_p)})_p\right| = p^e$ folgt aus

$$\begin{aligned} p^e &= \left|\mathbb{Z}_p[G_\delta]/(X^{(\delta)})_p\right| \\ &= \left|\mathbb{Z}_p[G_{\delta_p}]/(X^{(\delta_p)})_p\right| \cdot \left|\left(\mathbb{Z}_p[x]/(r_2(x))\right)/\omega_3\left((X^{(\delta)})_p\right)\right| \end{aligned}$$

schließlich $\omega_3\left((X^{(\delta)})_p\right) = \mathbb{Z}_p[x]/(r_2(x))$.

Wir beschreiben jetzt, welche Möglichkeiten für $(X^{(\delta)})_p$ in Frage kommen und wie man jeweils ein Erzeugendensystem von $(X^{(\delta)})_p$ erhält. Sei dazu

$$\phi_{\delta_p}(x) = \prod_{i=1}^{r} \varphi_i(x)$$

die Zerlegung von $\phi_{\delta_p}(x)$ in über $\mathbb{Z}_p$ irreduzible Faktoren. Dies liefert einen Isomorphismus

$$\chi_p : \mathbb{Z}_p[x]/(\phi_{\delta_p}(x)) \to \mathbb{Z}_p[x]/(\varphi_1(x)) \times \ldots \times \mathbb{Z}_p[x]/(\varphi_r(x)).$$

Nachdem die $\varphi_i(x)$ über $\mathbb{Z}_p$ irreduzibel sind, gibt es in $\mathbb{Z}_p[x]/(\varphi_i(x))$ nur die Ideale (p^j), für ganze Zahlen $j \geq 0$. Für das Bild von $(X^{(\delta)})_p$ unter χ_p gilt also

$$\chi_p(\omega_2((X^{(\delta)})_p)) = ((p^{a_1}), \ldots, (p^{a_r})),$$

wobei die a_i nichtnegative ganze Zahlen sind. Zudem erfüllen die a_i die Gleichung $e = \sum_{i=1}^{r} a_i \deg(\varphi_i)$, da der Index von $\omega_2((X^{(\delta)})_p)$ in $\mathbb{Z}_p[x]/(\phi_{\delta_p}(x))$ gerade p^e entspricht

Sei also

$$\chi_p(\omega_2((X^{(\delta)})_p)) = ((p^{a_1}), \ldots, (p^{a_r}))$$

mit $e = \sum_{i=1}^{r} a_i \deg(\varphi_i)$. Weiter sei $a = \max\{a_1, \ldots, a_r\}$. Wir setzen nun

$$\rho_0 = \prod_{j \text{ mit } a_j \neq 0} \varphi_j(\sigma_\delta).$$

Für alle $i \in \{1, \ldots, a\}$, für die es mindestens ein a_j mit $i = a_j$ gibt, definiert man

$$\rho_i = p^i \prod_{j \text{ mit } a_j > i} \varphi_j(\sigma_\delta).$$

Seien $\rho_0, \rho_{i_1}, \ldots, \rho_{i_v}, \rho_a$ die dadurch definierten Elemente. Man überprüft leicht, dass $(X^{(\delta)})_p$ von diesen erzeugt wird. Betrachten wir die Projektion

$$\pi_a : \mathbb{Z}_p \to \mathbb{Z}, \sum_{i=0}^{\infty} \alpha_i p^i \mapsto \sum_{i=0}^{a-1} \alpha_i p^i$$

so fällt auf, dass wegen $\rho_a = p^a$ auch $(\pi_a(\rho_0), \pi_a(\rho_{i_1}), \ldots \pi_a(\rho_{i_v}), p^a)$ ein Erzeugendensystem von $(X^{(\delta)})_p$ liefert. Damit ist auch klar, dass $(\tilde{X}^{(\delta)})_p = (X^{(\delta)})_p$ für

$$\tilde{X}^{(\delta)} = \langle \pi_a(\rho_0), \pi_a(\rho_{i_1}), \ldots \pi_a(\rho_{i_v}), p^a \rangle_{\mathbb{Z}[G_\delta]} \subset \mathbb{Z}[G_\delta]$$

erfüllt ist. Für den Fall, dass $s = 1$, also $h_{K_\delta} = p^e$ ist, liefert dies sogar $\tilde{X}^{(\delta)} = X^{(\delta)}$, da wegen $\rho_a = p^a \in \tilde{X}^{(\delta)}$ für alle Primzahlen $t \neq p$

$$(\tilde{X}^{(\delta)})_t = \mathbb{Z}_t[G_\delta] = (X^{(\delta)})_t$$

gilt.

4.6 Verbesserung des ersten Ansatzes

In Abschnitt 4.2 haben wir gesehen, dass für jedes h_l^+ mit $\mathrm{ggT}\left(h_l^+, |G|\right) = 1$ mindestens ein zyklisches Ideal $I \subset \mathbb{Z}[G]$ mit $|\mathbb{Z}[G]/I| = h_l^+$ existiert. Allerdings entspricht das von uns dort angegebene Ideal in keinem Fall dem zu $\overline{U}_l$ gehörenden Ideal $X \subset \mathbb{Z}[G]$. Mit dem zusätzlichen Wissen aus dem vorherigen Abschnitt gehen wir diesem Ansatz noch einmal nach. Die neue Idee basiert auf folgender

Bemerkung. Seien R und S kommutative Ringe mit Einselement, $f : R \to S$ ein surjektiver Ringhomomorphismus und $I \subset R$ ein Ideal. Da f surjektiv ist, ist $f(I) \subset S$ ein Ideal. Ist $I = (\eta)$ zyklisch, so ist das Ideal $f(I) = f((\eta)) \subset S$ ebenfalls zyklisch mit Erzeuger $f(\eta)$.

Wieder bezeichnen wir mit $\phi_i(x)$ das i-te Kreisteilungspolynom. Wir werden jetzt zeigen, dass es unter bestimmten Umständen einen surjektiven Ringhomomorphimus $\mathbb{Z}[G] \to \mathbb{Z}[x]/(\phi_{\delta_p}(x))$ gibt, der das zu $\overline{U}_l$ gehörende Ideal $X \subset \mathbb{Z}[G]$ auf ein nicht-zyklisches Ideal in $\mathbb{Z}[x]/(\phi_{\delta_p}(x))$ abbildet, woraus folgt, dass $\overline{U}_l$ in diesem Fall nicht $\mathbb{Z}[G]$-frei ist.
Seien $h_l^+ = p^e \cdot s$ und δ_p ähnlich wie in Abschnitt 4.5, genauer: sei p prim, $e, s \geq 1$ ganze Zahlen mit $h_{K_{\delta_p}} = p^e$, $p \nmid h_{K_\varepsilon}$ für alle von δ_p verschiedenen Teiler ε von δ_p und $\mathrm{ggT}\,(p, s) = 1$.
Behauptung: Das Bild von X unter der kanonischen Projektion

$$\pi : \mathbb{Z}[G] \cong \mathbb{Z}[x]/(x^n - 1) \to \mathbb{Z}[x]/(\phi_{\delta_p}(x))$$

hat Index p^e.
Mit der Notation aus Abschnitt 4.5, das heißt mit

$$r_1(x) = \prod_{\varepsilon | \delta_p, \varepsilon \neq \delta_p} \phi_\varepsilon(x),\ r_2(x) = \frac{x^n - 1}{r_1(x)\phi_{\delta_p}(x)},$$

gilt für den Isomorphismus

$$\omega = (\omega_1, \omega_2, \omega_3) : \mathbb{Z}_p[G] \cong \mathbb{Z}_p[x]/(r_1(x)) \times \mathbb{Z}_p[x]/(\phi_{\delta_p}(x)) \times \mathbb{Z}[x]/(r_2(x))$$

$\omega_1(X) = \mathbb{Z}_p[x]/(r_1(x))$ und $\omega_3(X) = \mathbb{Z}_p[x]/(r_2(x))$. Folglich ist

$$p^e = |\mathbb{Z}_p[G]/X_p| = \left|\left(\mathbb{Z}_p[x]/(\phi_{\delta_p}(x))\right)/\omega_2(X_p)\right|.$$

Des Weiteren gilt $\pi_p(X_p) = \omega_2(X_p)$ für die p-Lokalisierung π_p von π und $\pi_t(X_t) = \mathbb{Z}_t[x]/(\phi_{\delta_p}(x))$ für primes t mit $t \neq p$, woraus die Behauptung folgt.

Folgerung 8. Für $l = 4603$ ist $\tilde{h}_l^+ = 79$ und $\delta_{79} = 39$. Das Bild von X unter dem surjektiven Ringhomomorphismus

$$\pi : \mathbb{Z}[G] \cong \mathbb{Z}[x]/(x^{2301} - 1) \to \mathbb{Z}[x]/(\phi_{39}(x))$$

hat also Index 79. Da

$$\mathbb{Z}[x]/(\phi_{39}(x)) \cong \mathbb{Z}[\zeta_{39}] = \mathcal{O}_{\mathbb{Q}(\zeta_{39})},$$

können wir mit Hilfe von PARI/GP die Primidealzerlegung von $(79) \subset \mathcal{O}_{\mathbb{Q}(\zeta_{39})}$ berechnen. Da die Norm von $\pi(X) = 79$ ist, muss (79) in $\mathbb{Q}(\zeta_{39})$ vollständig zerfallen, und $\pi(X)$ muss einem der Primteiler von (79) in diesem Zahlring entsprechen. Mit dem Befehl *bnfisprincipal* sieht man nun, dass keines dieser Ideale ein Hauptideal ist. Somit kann $X \subset \mathbb{Z}[G]$ nicht zyklisch und $\overline{U}_{4603}$ nicht $\mathbb{Z}[G]$-frei sein. Ein weiterer Fall, $l = 7411$ mit $\tilde{h}_l^+ = 131$ und $\delta_{131} = 65$ führt auf dem gleichen Weg ebenfalls zur Nichtfreiheit von $\overline{U}_{7411}$ über $\mathbb{Z}[G]$.
Insbesondere folgt mit Satz 4.28, dass es für $l = 4603$ und $l = 7411$ keine Minkowski-Einheit in $\mathbb{Q}(\zeta_l)^+$ gibt.

Bemerkung. 1.) Alle anderen zur Untersuchung stehenden Fälle zeichnen sich dadurch aus, dass die Klassenzahlen von $\mathbb{Q}(\zeta_{\delta_p})$ jeweils 1 sind, also obiges Verfahren nicht anwendbar ist.

2.) Nach diesem Schema folgt in beiden Fällen, dass $\overline{U}_l^{(\delta_p)}$ nicht $\mathbb{Z}[G_{\delta_p}]$-frei ist. Sofern $h_{K_{\delta_p}}$ in beiden Fällen die vermuteten Eigenschaften hat und zudem ggT $\left(h_l^+, \frac{l-1}{2}\right) = 1$ gilt, so ist wegen Korollar 4.13 die Aussage, dass $\overline{U}_l$ zwar $\mathbb{Z}[G]$-projektiv, aber nicht $\mathbb{Z}[G]$-frei ist, korrekt - selbst, wenn $\tilde{h}_l^+$ nicht h_l^+ entspricht.

3.) Ein sehr ähnlicher Ansatz wird im Zusammenhang mit der Existenz von Minkowski-Einheiten am Ende von Abschnitt 3 einer Arbeit von Dubois [Dub00] erwähnt.

4.7 Explizite Bestimmung eines Erzeugers von X

Während wir in Abschnitt 4.6 zwei erste Beispiele gefunden haben, in denen $\overline{U}_l$ $\mathbb{Z}[G]$-projektiv aber nicht $\mathbb{Z}[G]$-frei ist, soll in diesem Abschnitt in anderen Fällen ein Erzeuger $\eta \in \mathbb{Z}[G]$ von X bestimmt und damit die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ nachgewiesen werden.

Satz 4.29. *Sei $l \equiv 3 \mod 4$ prim, $\delta^\star \geq 3$ prim und $h = h_l^+ = h_{K_{\delta^\star}} = \left(2^{\delta^\star - 1}\right)^s$ für eine ganze Zahl $s \geq 1$. Weiter sei das $\delta^\star$-te Kreisteilungspolynom $\phi_{\delta^\star}$ irreduzibel über $\mathbb{F}_2$. Dann sind die l-Einheiten modulo Torsion $\overline{U}_l$ $\mathbb{Z}[G]$-frei.*

Beweis. Da $\phi_{\delta^\star}$ über $\mathbb{F}_2$ irreduzibel ist, ist es dies nach dem Henselschen Lemma auch über $\mathbb{Z}_2$. Aus der Primalität von $\delta^\star$ folgt zudem, dass $\phi_{\delta^\star}$ vom Grad $\delta^\star - 1$ ist. Nach dem in Abschnitt 4.5 vorgestellten Verfahren folgt somit

$$X = (2^s, \phi_{\delta^\star}(\sigma)).$$

Wir benötigen jetzt einen Hilfssatz.

Lemma 4.30. *Seien $d \neq 1$ und m positive, ungerade Zahlen. Weiter sei $H = \langle \sigma_H \rangle$ eine zyklische Gruppe der Ordnung md und $\eta := \sum_{j=0}^{d-1} (-1)^j {\sigma_H}^j \in \mathbb{Z}[H]$. Dann gilt*

$$|\mathbb{Z}[H]/(\eta)| = \mathrm{Norm}_{\mathbb{Z}[H]}(\eta) = 2^{d-1}.$$

Beweis. Der Beweis ist ähnlich dem von Proposition 4.10. Die Multiplikation mit $h = \sum_{i=0}^{md-1} h_i {\sigma_H}^i$,

$$h\cdot : \mathbb{Z}[H] \to \mathbb{Z}[H], \alpha \mapsto h \cdot \alpha,$$

hat bezüglich der $\mathbb{Z}$-Basis $(1, \sigma_H, \ldots, {\sigma_H}^{md-1})$ von $\mathbb{Z}[H]$ die darstellende Matrix

$$\mathcal{M}(\eta\cdot) = \begin{pmatrix} h_0 & h_1 & \cdots & h_{md-2} & h_{md-1} \\ h_{md-1} & h_0 & \cdots & h_{md-3} & h_{md-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ h_2 & h_3 & \cdots & h_0 & h_1 \\ h_1 & h_2 & \cdots & h_{md-1} & h_0 \end{pmatrix}^T$$

wobei für $h = \eta$

$$h_i = \begin{cases} (-1)^i & \text{für } 0 \leq i \leq d-1, \\ 0 & \text{sonst,} \end{cases}$$

gilt. Wie im Beweis von Proposition 4.10 erhalten wir

$$\begin{aligned} \mathrm{Norm}_{\mathbb{Z}[H]}(\eta) &= \det(\mathcal{M}(\eta\cdot)) = \det(\mathcal{M}(\eta\cdot)^T) \\ &= \prod_{i=0}^{md-1} \left(\sum_{j=0}^{md-1} \zeta^{ij} h_j \right) = \prod_{i=0}^{md-1} \left(\sum_{j=0}^{d-1} \zeta^{ij} h_j \right) \\ &= \prod_{i=0}^{md-1} \left(\sum_{j=0}^{d-1} \zeta^{ij} (-1)^j \right). \end{aligned}$$

Hier sei ζ eine primitive md-te Einheitswurzel. Die Rechnung unterteilen wir in drei Schritte.

1.) Sei $k \geq 3$ ungerade und ζ eine primitive k-te Einheitswurzel. Dann ist auch ζ^2 eine primitive k-te Einheitswurzel und es gilt

$$\prod_{i=1}^{k-1}(1+\zeta^i) = \prod_{i=1}^{k-1}\frac{(1+\zeta^i)(1-\zeta^i)}{(1-\zeta^i)} = \frac{\prod_{i=1}^{k-1}(1-\zeta^{2i})}{\prod_{i=1}^{k-1}(1-\zeta^i)} = 1.$$

2.) Seien nun m und d wie in der Behauptung. Für $s \in \mathbb{N}$ sei ζ_s eine primitive s-te Einheitswurzel. Wir erhalten mit Hilfe von 1.)

$$\begin{aligned}
\prod_{i=1}^{m\cdot d-1}(1+{\zeta_{md}}^{id}) &= \prod_{i=1}^{md-1}(1+{\zeta_m}^i) \\
&= \left(\prod_{i=1}^{m-1}(1+{\zeta_m}^i)\right)\cdot\left(1+{\zeta_m}^i\right)\cdot \\
&\quad \cdot\left(\prod_{i=m+1}^{2m-1}(1+{\zeta_m}^i)\right)\cdot\ldots\cdot\left(\prod_{i=m(d-1)}^{md-1}(1+{\zeta_m}^i)\right) \\
&= 1\cdot 2\cdot 1\cdot\ldots\cdot 1 = 2^{d-1}
\end{aligned}$$

3.) Sei ζ eine primitive md-te Einheitswurzel. Betrachten wir zunächst $\varphi_i = \sum_{j=0}^{d-1}\zeta^{ij}(-1)^j$ für $i \in \{0,\ldots,md-1\}$. Multiplikation mit $(1+\zeta^i)$ bewirkt

$$\varphi_i\cdot(1+\zeta^i) = \sum_{j=0}^{d-1}(-1)^j\zeta^{ij} + \sum_{j=0}^{d-1}(-1)^j\zeta^{i(j+1)} = 1+\zeta^{di}.$$

und somit gilt nach 1.) und 2.) zusammen mit $\varphi_0 = 1$

$$\begin{aligned}
\mathrm{Norm}_{\mathbb{Z}[H]}(\eta) &= \det(\mathcal{M}(\eta\cdot)^T) = \prod_{i=0}^{md-1}\left(\sum_{j=0}^{d-1}\zeta^{ij}(-1)^j\right) \\
&= \prod_{i=0}^{md-1}\varphi_i = \prod_{i=1}^{md-1}\varphi_i\prod_{i=1}^{md-1}(1+\zeta^i) \\
&= \prod_{i=1}^{md-1}\varphi_i(1+\zeta^i) = \prod_{i=1}^{md-1}(1+\zeta^{di}) = 2^{d-1}.
\end{aligned}$$

□

Für $G = \langle\sigma\rangle$ sei $\eta = \sum_{j=0}^{\delta^\star-1}(-1)^j\sigma^j$ analog zu vorangegangenem Lemma und $\rho(\sigma) = \sum_{j=0}^{\frac{\delta^\star-3}{2}} \sigma^{2j+1}$. Da $\phi_{\delta^\star}(\sigma) = \sum_{j=0}^{\delta^\star-1}\sigma^j$ ist, erhalten wir

$$\eta = \sum_{j=0}^{\delta^\star-1}\sigma^j - 2\cdot\left(\sum_{j=0}^{\frac{\delta^\star-3}{2}}\sigma^{2j+1}\right) = \phi_{\delta^\star}(\sigma) - 2\rho(\sigma).$$

Daraus ergibt sich einerseits

$$\begin{aligned}\eta^s &= (\phi_{\delta^\star}(\sigma) - 2\rho(\sigma))^s = \sum_{j=0}^{s}\binom{s}{j}\phi_{\delta^\star}(\sigma)^j(-2\rho(\sigma))^{s-j}\\ &= 2^s\cdot(-\rho(\sigma))^s + \phi_{\delta^\star}(\sigma)\cdot\left(\sum_{j=1}^{s}\binom{s}{j}\phi_{\delta^\star}(\sigma)^{j-1}\cdot(-2\rho(\sigma))^{s-j}\right)\\ &\quad\in (2^s, \phi_{\delta^\star}(\sigma)),\end{aligned}$$

also $\eta^s \in (2^s, \phi_{\delta^\star}(\sigma)) = X$ und andererseits wegen

$$|\mathbb{Z}[G]/(\eta^s)| = \left(2^{\delta^\star-1}\right)^s = |\mathbb{Z}[G]/X|$$

sogar die Gleichheit

$$X = (\eta^s).$$

Aus Ranggründen ist somit X und nach Korollar 4.3 auch $\overline{U}_l$ frei über $\mathbb{Z}[G]$. □

Folgerung 9. In 31 Fällen ist $\delta^\star = 3$ und $\tilde{h}_l^+ = 4 = 2^{\delta^\star-1}$, woraus mit der Irreduzibilität von x^2+x+1 über $\mathbb{F}_2$

$$X = (2, \sigma^2+\sigma+1) = (\sigma^2-\sigma+1) \subset \mathbb{Z}[G]$$

und damit die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ folgt.

Ein weiterer Fall ist durch $\delta^\star = 5$ und $\tilde{h}_l^+ = 16 = 2^{\delta^\star-1}$ gekennzeichnet, was analog mit der Irreduzibilität von $x^4+x^3+x^2+x+1$ über $\mathbb{F}_2$ zu

$$X = (2, \sigma^4+\sigma^3+\sigma^2+\sigma+1) = (\sigma^4-\sigma^3+\sigma^2-\sigma+1) \subset \mathbb{Z}[G],$$

also zur $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ führt.

Von den verbliebenen 37 Fällen sind weitere drei derart, dass $\delta^\star$ prim ist und $\tilde{h}_l^+ = \left(2^{\delta^\star-1}\right)^2$ und $\phi_{\delta^\star}(x)$ irreduzibel über $\mathbb{F}_2$ ist. Deshalb liefert auch hier Satz 4.29 die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$. In allen hier behandelten Fällen folgt nach Satz 4.28 die Existenz einer Minkowski-Einheit in $\mathbb{Q}(\zeta_l)^+$ und allen Unterkörpern davon.

4.8 Ein weiteres Verfahren zum Nachweis der Nichtfreiheit von $\overline{U}_l$

Unter den Voraussetzungen dieses Kapitels ist $\overline{U}_l^{(\delta)}$ und damit auch $X^{(\delta)}$ für alle $\delta \mid \frac{l-1}{2}$ nach Korollar 4.18 $\mathbb{Z}[G_\delta]$-projektiv. Sei q eine Primzahl, ζ_q eine primitive q-te Einheitswurzel und $\delta \in \mathbb{Z}$ derart, dass $\mathrm{ggT}\,(q,\delta) = 1$ und $h_{K_\delta} = h_{K_{q\delta}}$ für $K_\delta \subset K_{q\delta} \subset \mathbb{Q}(\zeta_l)^+$ erfüllt ist. Nach Proposition 4.25 gilt dann in dem Pullback-Diagramm

$$\begin{array}{ccc} \mathbb{Z}[G_{q\delta}] & \xrightarrow[i_2]{} & \mathbb{Z}[\zeta_q][G_\delta] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z}[G_\delta] & \xrightarrow{j_1} & \mathbb{F}_q[G_\delta] \end{array}$$

$i_2(X^{(q\delta)}) = \mathbb{Z}[\zeta_q][G_\delta]$. Weiter ist nach Proposition 4.21 $i_1(X^{(q\delta)}) = X^{(\delta)} \subset \mathbb{Z}[G_\delta]$. Wir setzen voraus, dass $X^{(\delta)}$ ein von $\eta_\delta \in \mathbb{Z}[G_\delta]$ erzeugtes zyklisches Ideal ist, wobei $j_1(\eta_\delta) \in (\mathbb{F}_q[G_\delta])^\star$ ist. Mit Beispiel 2 erhalten wir

$$X^{(q\delta)} \cong (\mathbb{Z}[G_\delta], \mathbb{Z}[\zeta_q][G_\delta], j_1(\eta_\delta)).$$

Aus der exakten Sequenz

$$\begin{aligned} (\mathbb{Z}[G_{q\delta}])^\star \xrightarrow{f_1} \quad & (\mathbb{Z}[G_\delta])^\star \oplus (\mathbb{Z}[\zeta_q][G_\delta])^\star \xrightarrow{g_1} (\mathbb{F}_q[G_\delta])^\star \xrightarrow{\rho} \mathrm{Pic}(\mathbb{Z}[G_{q\delta}]) \\ & \xrightarrow{f_0} \mathrm{Pic}(\mathbb{Z}[G_\delta]) \oplus \mathrm{Pic}(\mathbb{Z}[\zeta_q][G_\delta]) \xrightarrow{g_0} \mathrm{Pic}(\mathbb{F}_q[G_\delta]), \end{aligned}$$

deren Existenz durch Satz 1.17 gegeben ist, ergibt sich, dass $X^{(q\delta)}$ genau dann $\mathbb{Z}[G_{q\delta}]$-frei ist, wenn

$$j_1(\eta_\delta) \in \mathrm{Im}(g_1) = j_1((\mathbb{Z}[G_\delta])^\star) \cdot j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star) = j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star)$$

ist, wobei die letzte Gleichheit aus $j_1((\mathbb{Z}[G_\delta])^\star) \subset j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star)$ folgt.

Wir stellen jetzt ein Verfahren vor, mit dem es gegebenenfalls nachweisbar ist, wenn $j_1(\eta_\delta) \notin j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star)$ gilt. Der folgende Satz bildet dafür die Grundlage.

Satz 4.31. *Sei $m \geq 3$ eine ganze Zahl, ζ_m eine primitive m-te Einheitswurzel und*

$$\iota_1 : \mathbb{Z}[\zeta_m] \to \mathbb{Z}[\zeta_m], \quad \zeta_m \mapsto {\zeta_m}^{-1}.$$

Weiter sei H eine abelsche Gruppe und

$$\iota_2 : H \to H, \quad h \mapsto h^{-1}.$$

Durch ι_1 und ι_2 wird auf $\mathbb{Z}[\zeta_m][H]$ eine Involution

$$\iota : \mathbb{Z}[\zeta_m][H] \to \mathbb{Z}[\zeta_m][H], \quad \sum_i r_i h_i \mapsto \sum_i \iota_1(r_i)\iota_2(h_i)$$

definiert. Bezeichnet

$$(\mathbb{Z}[\zeta_m][H])^{\star +} = \{\alpha \in (\mathbb{Z}[\zeta_m][H])^\star \mid \iota(\alpha) = \alpha\},$$

den Plusteil von $(\mathbb{Z}[\zeta_m][H])^\star$ bezüglich ι, so gilt für jedes $\alpha \in (\mathbb{Z}[\zeta_m][H])^\star$:

$$\alpha^2 = \alpha^+ \cdot {\zeta_m}^k \cdot h,$$

wobei $\alpha^+ \in (\mathbb{Z}[\zeta_m][H])^{\star +}$, $k \in \mathbb{Z}$ und $h \in H$ ist.

Beweis. Der Beweis basiert auf [Br83, 4.3].
Sei $\alpha \in (\mathbb{Z}[\zeta_m][H])^\star$ und $\frac{\alpha}{\iota(\alpha)} = \sum_i r_i h_i \in (\mathbb{Z}[\zeta_m][H])^\star$ mit $r_i \in \mathbb{Z}[\zeta_m]$ und $h_i \in H$ für alle i. Dann gilt

$$\alpha \cdot \iota(\alpha) = \iota(\alpha)\iota(\iota(\alpha)) \in (\mathbb{Z}[\zeta_m][H])^{\star +}$$

und

$$1 = \frac{\alpha}{\iota(\alpha)} \cdot \frac{\iota(\alpha)}{\alpha} = \frac{\alpha}{\iota(\alpha)} \cdot \iota\left(\frac{\alpha}{\iota(\alpha)}\right) = \sum_i r_i h_i \cdot \sum_i \iota_1(r_i) h_i^{-1}.$$

Somit erhält man

$$\sum_i r_i \iota_1(r_i) = 1.$$

Bezeichne $\overline{z}$ das komplex Konjugierte einer komplexen Zahl z. Als Element der abelschen Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ kommutiert die komplexe Konjugation mit den anderen Elementen von $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ und es gilt

$$\nu_a(\iota(r_i)) = \nu_a(\iota_1(r_i)) = \nu_a(\overline{r_i}) = \overline{\nu_a(r_i)}$$

für jede Einbettung $\nu_a : \mathbb{Z}[\zeta_m] \to \mathbb{C}, \zeta_m \mapsto \zeta_m^a$ ($a \in \{1, \ldots, m-1\}$). Dies führt zu

$$\begin{aligned} 1 &= \nu_a(1) = \nu_a\left(\sum_i r_i \iota_1(r_i)\right) = \sum_i \nu_a(r_i)\nu_a(\iota_1(r_i)) \\ &= \sum_i \nu_a(r_i)\overline{\nu_a(r_i)} = \sum_i |\nu_a(r_i)|^2 \end{aligned}$$

für alle a und damit zu $|\nu_a(r_i)| \leq 1$ für alle a und alle i. Wegen $r_i \in \mathbb{Z}[\zeta_m]$ gilt jedoch für festes i

$$N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(r_i) = \prod_{a=1}^{m-1} \nu_a(r_i) \in \mathbb{Z},$$

also $\prod_{a=1}^{m-1} |\nu_a(r_i)| \in \mathbb{Z}$. Somit kommen für $\prod_{a=1}^{m-1} |\nu_a(r_i)|$ nur die Werte 0 und 1 in Frage. Ist $\prod_{a=1}^{m-1} |\nu_a(r_i)| = 0$, so muss $r_i = 0$ sein. Andernfalls ist $\prod_{a=1}^{m-1} |\nu_a(r_i)| = 1$, also muss der Betrag aller Konjugierten von r_i gleich 1 und damit r_i eine m-te Einheitswurzel sein. Aus

$$1 = \sum_i r_i \iota_1(r_i) = \sum_i |r_i|^2$$

folgt jedoch, dass nur eines der r_i, nennen wir es r_{i_0}, von Null verschieden sein kann. Nach obigen Ausführungen gibt es somit ein $k \in \mathbb{Z}$, sodass $r_{i_0} = {\zeta_m}^k$ ist und

$$\frac{\alpha}{\iota(\alpha)} = r_{i_0} \cdot h_{i_0} = {\zeta_m}^k \cdot h_{i_0}$$

gilt. Durch Multiplikation mit $\alpha \cdot \iota(\alpha)$ liefert dies

$$\alpha^2 = \alpha\iota(\alpha) \cdot {\zeta_m}^k \cdot h_{i_0},$$

also die Behauptung. □

Sei q eine Primzahl und $\delta \geq 2$ eine zu q teilerfremde Zahl. Wir betrachten wieder das Pullback-Diagramm

$$\begin{array}{ccc} \mathbb{Z}[G_{q\delta}] & \xrightarrow[i_2]{} & \mathbb{Z}[\zeta_q][G_\delta] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbb{Z}[G_\delta] & \xrightarrow{j_1} & \mathbb{F}_q[G_\delta], \end{array}$$

wobei G_m für eine ganze Zahl m wieder eine zyklische Gruppe der Ordnung m mit Erzeuger σ_m bezeichnen soll.

Mit Hilfe der Involution

$$\bar{\iota} : \mathbb{F}_q[G_\delta] \to \mathbb{F}_q[G_\delta], \sum_i \alpha_i {\sigma_\delta}^i \mapsto \sum_i \alpha_i {\sigma_\delta}^{-i}$$

lässt sich der Plusteil

$$(\mathbb{F}_q[G_\delta])^+ = \{\alpha \in \mathbb{F}_q[G_\delta] \mid \bar{\iota}(\alpha) = \alpha\}$$

von $\mathbb{F}_q[G_\delta]$ und der Plusteil

$$(\mathbb{F}_q[G_\delta])^{\star+} = \{\alpha \in (\mathbb{F}_q[G_\delta])^\star \mid \overline{\iota}(\alpha) = \alpha\}$$

von $(\mathbb{F}_q[G_\delta])^\star$ definieren. Für die Involution $\iota : \mathbb{Z}[\zeta_q][G_\delta] \to \mathbb{Z}[\zeta_q][G_\delta]$ aus Satz 4.31 gilt offenbar

$$j_2 \circ \iota = \overline{\iota} \circ j_2.$$

Insbesondere ist damit $(\mathbb{F}_q[G_\delta])^{\star+}$ der Bildbereich der Restriktion von j_2 auf $(\mathbb{Z}[\zeta_q][G_\delta])^{\star+}$. Damit ergibt sich eine interessante Konsequenz aus Satz 4.31:

Korollar 4.32. *In obiger Situation gelten die folgenden beiden Aussagen.*

a) Sei $\alpha \in (\mathbb{Z}[\zeta_q][G_\delta])^\star$. Dann gibt es ein $k \in \mathbb{Z}$, sodass

$$\operatorname{ord}(j_2(\alpha)) \mid \left(2^k \cdot \delta \cdot \left|(\mathbb{F}_q[G_\delta])^{\star+}\right|\right)$$

gilt.

b) Sei $\overline{\alpha} \in (\mathbb{F}_q[G_\delta])^\star$ derart, dass $\operatorname{ord}(\overline{\alpha})$ einen ungeraden Faktor f hat, der kein Teiler von $\delta \cdot \left|(\mathbb{F}_q[G_\delta])^{\star+}\right|$ ist. Dann liegt $\overline{\alpha}$ nicht in $j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star)$.

Beweis. a) Sei $\alpha \in (\mathbb{Z}[\zeta_q][G_\delta])^\star$. Nach Satz 4.31 gibt es $k \in \mathbb{Z}$, $g \in G_\delta$ und $\alpha^+ \in (\mathbb{Z}[\zeta_q][G_\delta])^{\star+}$ mit $\alpha^2 = \zeta_m^k \cdot g \cdot \alpha^+$. Nun ist

$$(j_2(\alpha))^2 = j_2(\alpha^2) = j_2(\zeta_m^k) \cdot j_2(g) \cdot j_2(\alpha^+) = g \cdot j_2(\alpha^+).$$

Da die Ordnung von g die Gruppenordnung δ teilt und $j_2(\alpha^+)$ in $(\mathbb{F}_q[G_\delta])^{\star+}$ liegt, folgt die Behauptung.

b) Direkte Konsequenz aus a).

□

Die Idee ist nun, die Ordnung von $j_1(\eta_\delta) \in (\mathbb{F}_q[G_\delta])^\star$ zu bestimmen und dann zu prüfen, ob Korollar 4.32 anwendbar ist. Allerdings müssen wir dazu die Ordnung von $(\mathbb{F}_q[G_\delta])^{\star+}$ bestimmen. Diesem Problem soll im Folgenden nachgegangen werden.
Seien δ und q wie oben, also q prim und $\delta \geq 2$ teilerfremd zu q. Weiter bezeichnet $\phi_d(x)$, wie immer, das d-te Kreisteilungspolynom. Dann zerfällt $x^\delta - 1$ über $\mathbb{Q}$ und damit auch über $\mathbb{F}_q$ wie folgt

$$x^\delta - 1 = (x-1) \prod_{1 \neq d \mid \delta} \phi_d(x).$$

Allerdings müssen die Kreisteilungspolynome nicht irreduzibel über $\mathbb{F}_q$ sein. Sei

$$\phi_{d_i}(x) = \prod_{k=1}^{t_j} \varphi_{d_i,k}(x)$$

eine Zerlegung in über $\mathbb{F}_q$ irreduzible Faktoren und r die Anzahl der von 1 verschiedenen Teiler von δ. Dann gibt es einen Isomorphismus

$$\begin{aligned}\theta &= (\theta_{d_0,1}, \theta_{d_1,1}, \ldots, \theta_{d_r,t_r}) : \mathbb{F}_q[x]/(x^\delta - 1) \xrightarrow{\sim} \\ &\quad \mathbb{F}_q[x]/(\varphi_{d_0,1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_1,1}(x)) \times \ldots \times \mathbb{F}_q[x]/(\varphi_{d_r,t_r}(x)),\end{aligned}$$

wobei $\varphi_{d_0,1}(x) = x - 1$ ist und auf der rechten Seite ein Produkt von Körpern steht. Weiter gibt es

$$f_{d_0,1}(x), f_{d_1,1}(x), \ldots, f_{d_r,t_r}(x) \in \mathbb{F}_q[x]/(x^\delta - 1),$$

sodass

$$\theta_{d_j,l}(f_{d_i,k}(x)) = \begin{cases} 1 \text{ für } (d_j,l) = (d_i,k) \\ 0 \text{ für alle } (d_j,l) \neq (d_i,k). \end{cases}$$

Wir untersuchen nun, wie die Involution $\bar{\iota}$ die Polynome $\varphi_{d_i,k}(x)$ und damit auch die $f_{d_i,k}(x)$ verändert. Dazu sei ζ eine primitive δ-te Einheitswurzel in einem Erweiterungskörper von $\mathbb{F}_q$, beispielsweise $\overline{\mathbb{F}}_q$. Bekanntlich, siehe beispielsweise [Ju93, Theorem 1.2.3 und Theorem 1.5.4], sind die Polynome $\varphi_{d_i,1}(x), \ldots, \varphi_{d_i,t_i}(x)$ paarweise verschieden, haben für festes i den gleichen Grad g_i und es gibt ganze Zahlen $a_{ik} \in \{0, \ldots, \delta - 1\}$ mit

$$\varphi_{d_i,k}(x) = (x - \zeta^{a_{ik}}) \cdot (x - (\zeta^{a_{ik}})^q) \cdot \ldots \cdot (x - (\zeta^{a_{ik}})^{q^{g-1}}).$$

Das heißt, die auftretenden Exponenten sind gerade alle Elemente von

$$a_{ik}\langle q \rangle = \{a_{ik} \cdot q^l \mid l \in \mathbb{Z}\} \subset \mathbb{Z}/\delta\mathbb{Z},$$

sie liegen also in der Äquivalenzklasse von a_{ik} bezüglich der durch

$$a \sim_q b \Leftrightarrow \exists i \in \mathbb{Z} : a = q^i \cdot b$$

definierten Äquivalenzrelation $\sim_q$. Insbesondere ist der Grad von $\varphi_{d_i,k}(x)$ gleich der Mächtigkeit der entsprechenden Äquivalenzklasse $a_{ik}\langle q \rangle$.
Ist ζ^a, wobei $a \in \{0, \ldots, \delta - 1\}$, eine Nullstelle des Kreisteilungspolynoms $\phi_d(x)$, so gilt dies auch für das Konjugierte $\overline{\zeta^a} = \zeta^{-a}$. Es können nun zwei Fälle auftreten.

1.) Wenn mit $\zeta^{a_{ik}}$ auch $\overline{\zeta^{a_{ik}}}$ eine Nullstelle von $\varphi_{d_i,k}(x)$ ist, so ist für jede Nullstelle von $\varphi_{d_i,k}(x)$ auch das Konjugierte Nullstelle von $\varphi_{d_i,k}(x)$. Falls $\zeta^{a_{ik}} \neq 1$ ist, folgt dann insbesondere, dass $\varphi_{d_i,k}(x)$ geraden Grad hat. In diesem Fall ist somit jede Nullstelle von $\varphi_{d_i,k}(x)$ auch Nullstelle von dem Polynom

$$\begin{aligned}\overline{\iota}(\varphi_{d_i,k}(x)) &= \varphi_{d_i,k}(x^{\delta-1}) = \varphi_{d_i,k}(x^{-1}) \\ &= (x^{-1}-\zeta^{a_{ik}})\cdot(x^{-1}-(\zeta^{a_{ik}})^q)\cdot\ldots\cdot(x^{-1}-(\zeta^{a_{ik}})^{q^{g-1}}),\end{aligned}$$

das heißt $\varphi_{d_i,k}(x) \mid \overline{\iota}(\varphi_{d_i,k}(x))$. Das ist also genau dann der Fall, wenn mit a_{ik} auch das Inverse $-a_{ik} \in \mathbb{Z}/\delta\mathbb{Z}$ in $a_{ik}\langle q\rangle$ liegt.

2.) Sollte andererseits $\overline{\zeta^{a_{ik}}}$ keine Nullstelle von $\varphi_{d_i,k}(x)$ sein, so gibt es ein $l \neq k$ mit

$$\varphi_{d_i,l}(x) = (x-\overline{\zeta^{a_{ik}}})\cdot(x-(\overline{\zeta^{a_{ik}}})^q)\cdot\ldots\cdot(x-(\overline{\zeta^{a_{ik}}})^{q^{g-1}})$$

und es gilt

$$\varphi_{d_i,l}(x) \mid \overline{\iota}(\varphi_{d_i,k}(x)) \text{ und } \varphi_{d_i,k}(x) \mid \overline{\iota}(\varphi_{d_i,l}(x)).$$

In diesem Fall ist das Inverse $-a_{ik} \in \mathbb{Z}/\delta\mathbb{Z}$ von a_{ik} also nicht in $a_{ik}\langle q\rangle$, sondern in $a_{il}\langle q\rangle$.

Diese Ergebnisse lassen sich in beiden Fällen auf die Aktion von $\overline{\iota}$ auf $f_{d_i,k}(x)$ übertragen.

1.) Sind $\zeta^{a_{ik}}$ und $\overline{\zeta^{a_{ik}}}$ Nullstellen von $\varphi_{d_i,k}(x)$, so folgt

$$\theta_{d_j,l}(\overline{\iota}(f_{d_i,k}(x))) = \begin{cases}1 \text{ für } (d_j,l) = (d_i,k)\\ 0 \text{ für alle } (d_j,l) \neq (d_i,k).\end{cases}$$

also insbesondere $\overline{\iota}(f_{d_i,k}(x)) = f_{d_i,k}(x)$.

2.) Ist $k_1 \neq k_2$, $\zeta^{a_{ik_1}}$ Nullstelle von $\varphi_{d_i,k_1}(x)$ und $\overline{\zeta^{a_{ik_1}}}$ Nullstelle von $\varphi_{d_i,k_2}(x)$, so ergibt sich für $f_{d_i,k_1}(x)$, dass

$$\theta_{d_j,l}(\overline{\iota}(f_{d_i,k_1}(x))) = \begin{cases}1 \text{ für } (d_j,l) = (d_i,k_2)\\ 0 \text{ für alle } (d_j,l) \neq (d_i,k_2).\end{cases}$$

Insbesondere gilt damit $\overline{\iota}(f_{d_i,k_1}(x)) = f_{d_i,k_2}(x)$ und $\overline{\iota}(f_{d_i,k_2}(x)) = f_{d_i,k_1}(x)$.

Seien $\alpha = \sum \alpha_{d_j,l} f_{d_j,l}(x)$ und $\beta = \sum \beta_{d_j,l} f_{d_j,l}(x)$ aus $\mathbb{F}_q[x]/(x^\delta - 1)$. Im ersten Fall folgt somit aus

$$\theta_{d_i,k}(\alpha) = \theta_{d_i,k}(\alpha_{d_i,k} f_{d_i,k}(x)) = \theta_{d_i,k}(\beta_{d_i,k} f_{d_i,k}(x)) = \theta_{d_i,k}(\beta)$$

auch die Gleichheit

$$\theta_{d_i,k}(\bar{\iota}(\alpha)) = \theta_{d_i,k}(\bar{\iota}(\alpha_{d_i,k} f_{d_i,k}(x))) = \theta_{d_i,k}(\bar{\iota}(\beta_{d_i,k} f_{d_i,k}(x))) = \theta_{d_i,k}(\bar{\iota}(\beta)).$$

Mittels $\theta_{d_i,k}$ und $\bar{\iota}$ erhalten wir deshalb eine Involution

$$\bar{\iota}_{d_i,k} : \mathbb{F}_q[x]/(\varphi_{d_i,k}(x)) \to \mathbb{F}_q[x]/(\varphi_{d_i,k}(x)),$$

mit deren Hilfe $(\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^+$ beziehungsweise $(\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^{\star +}$ definiert werden kann.
Im zweiten Fall ergibt

$$(\theta_{d_i,k_1}(\alpha), \theta_{d_i,k_2}(\alpha)) = (\theta_{d_i,k_1}(\beta), \theta_{d_i,k_2}(\beta))$$

demnach

$$(\theta_{d_i,k_1}(\bar{\iota}(\alpha)), \theta_{d_i,k_2}(\bar{\iota}(\alpha))) = (\theta_{d_i,k_1}(\bar{\iota}(\beta)), \theta_{d_i,k_2}(\bar{\iota}(\beta))),$$

was ebenfalls zu einer Involution

$$\begin{aligned} \bar{\iota}_{d_i,k_1,k_2} \quad : \quad & \mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)) \\ & \to \mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)) \end{aligned}$$

und der Definition von $(\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^+$ führt.
Nun gilt für $\alpha \in \mathbb{F}_q[x]/(x^\delta - 1)$ genau dann $\bar{\iota}(\alpha) = \alpha$, also $\alpha \in (\mathbb{F}_q[G_\delta])^+$, wenn

$$\theta_{d_i,k}((\alpha)) = \bar{\iota}_{d_i,k}(\theta_{d_i,k}(\alpha))$$

beziehungsweise

$$(\theta_{d_i,k_1}(\alpha), \theta_{d_i,k_2}(\alpha)) = \bar{\iota}_{d_i,k_1,k_2}(\theta_{d_i,k_1}(\alpha), \theta_{d_i,k_2}(\alpha))$$

für alle $(d_i, k), (d_i, k_1)$ und (d_i, k_2) gilt. Die Ordnung des Plusteils von $(\mathbb{F}_q[G_\delta])^\star$ ist somit gleich dem Produkt der Ordnungen der auftretenden Plusteile

$(\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^{\star +}$ beziehungsweise $(\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^{\star +}$,

sodass wir lediglich Formeln für die Berechnung dieser kleineren Ordnungen benötigen:

1.) Seien $\zeta^{a_{ik}}$ und $\overline{\zeta^{a_{ik}}}$ Nullstellen von $\varphi_{d_i,k}(x)$, so ist

$$\bar{\iota}_{d_i,k} \in \mathrm{Gal}((\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))/\mathbb{F}_q) \text{ mit } (\bar{\iota}_{d_i,k})^2 = \mathrm{id}$$

und es gilt offensichtlich

$$\mathrm{Fix}(\bar{\iota}_{d_i,k}) = (\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^+.$$

Ist $a_{ik} = 0$, also $\zeta^{a_{ik}} = \overline{\zeta^{a_{ik}}}$, so ist $\varphi_{d_i,k}(x) = \varphi_{d_0,1}(x) = x - 1$ und folglich gilt bereits $\bar{\iota}_{d_0,1} = \mathrm{id}$. Andernfalls folgt

$$[\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)) : \mathrm{Fix}(\bar{\iota}_{d_i,k})] = |\{\mathrm{id}, \bar{\iota}_{d_i,k}\}| = 2.$$

Während im ersten Fall

$$\mathrm{Fix}(\bar{\iota}_{d_i,k}) \cong \mathbb{F}_q$$

gilt, folgt im zweiten Fall

$$\mathrm{Fix}(\bar{\iota}_{d_i,k}) \cong \mathbb{F}_{q^{g_i/2}}.$$

Eingeschränkt auf die Einheiten ergibt sich im ersten Fall

$$|(\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^{\star +}| = q - 1,$$

im zweiten Fall

$$|(\mathbb{F}_q[x]/(\varphi_{d_i,k}(x)))^{\star +}| = q^{g_i/2} - 1.$$

2.) Sei $\zeta^{a_{ik_1}}$ Nullstelle von $\varphi_{d_i,k_1}(x)$ und $\overline{\zeta^{a_{ik_1}}}$ Nullstelle von φ_{d_i,k_2} mit $k_1 \neq k_2$. Somit agiert $\bar{\iota}_{d_i,k_1,k_2}$ wie folgt auf $\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x))$:

$$\bar{\iota}_{d_i,k_1,k_2}(\sum_{j=0}^{g_i-1} \alpha_j x^j, \sum_{j=0}^{g_i-1} \beta_j x^j) = (\sum_{j=0}^{g_i-1} \beta_j x^{-j}, \sum_{j=0}^{g_i-1} \alpha_j x^{-j}).$$

Für jedes $\sum_{j=0}^{g_i-1} \alpha_j x^j$ gibt es offensichtlich genau ein $\sum_{j=0}^{g_i-1} \tilde{\alpha}_j x^j$ mit

$$\sum_{j=0}^{g_i-1} \alpha_j x^j \equiv \sum_{j=0}^{g_i-1} \tilde{\alpha}_j x^{-j} \mod \varphi_{d_i,k_1}(x).$$

Da $\bar{\iota}_{d_i,k_1,k_2}$ eine Involution ist, gilt zudem

$$\begin{aligned}
\bar{\iota}_{d_i,k_1,k_2}{}^2(\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j) &= \bar{\iota}_{d_i,k_1,k_2}(\sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^{-j}, \sum_{j=0}^{g_i-1}\alpha_j x^{-j}) \\
&= \bar{\iota}_{d_i,k_1,k_2}(\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\alpha_j x^{-j}) \\
&= (\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\alpha_j x^{-j}) \\
&= (\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j),
\end{aligned}$$

woraus insbesondere

$$\sum_{j=0}^{g_i-1}\alpha_j x^{-j} \equiv \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j \mod \varphi_{d_i,k_2}(x)$$

folgt. Somit gilt

$$\bar{\iota}_{d_i,k_1,k_2}(\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j) = (\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j),$$

also

$$(\sum_{j=0}^{g_i-1}\alpha_j x^j, \sum_{j=0}^{g_i-1}\tilde{\alpha}_j x^j) \in (\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^+.$$

Damit erhalten wir

$$|(\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^+| = q^{g_i}$$

und, da $(0,0)$ das einzige nicht-invertierbare Element aus $(\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^+$ ist,

$$|(\mathbb{F}_q[x]/(\varphi_{d_i,k_1}(x)) \times \mathbb{F}_q[x]/(\varphi_{d_i,k_2}(x)))^{\star +}| = q^{g_i} - 1.$$

Die obigen Ausführungen liefern ein einfaches Verfahren zur Bestimmung der Ordnung des Plusteils von $(\mathbb{F}_q[G_\delta])^\star$:

1.) Bestimme $\langle q\rangle \subset (\mathbb{Z}/\delta\mathbb{Z})^\star$.

2.) Setze $a_1 = 0$ und bestimme $\{a_2, \ldots, a_s\} \subset \{1, \ldots, \delta - 1\}$, sodass

$$\{0, \ldots, \delta - 1\} = \dot{\cup}_{i=1}^{s} a_i\langle q\rangle$$

ist.

3.) Setze $m_1 = q - 1$.

4) Teste für jedes Element a_i aus $\{a_2, \ldots, a_s\}$, ob das additive Inverse $-a_i \in \mathbb{Z}/\delta\mathbb{Z}$ auch in $a_i\langle q\rangle$ liegt. Ist dies der Fall, so berechnet man $m_i = q^{\frac{|a_i\langle q\rangle|}{2}} - 1$. Andernfalls setzt man $m_i = \sqrt{q^{|a_i\langle q\rangle|} - 1}$.

5.) Das Produkt $\prod_{i=1}^{s} m_i$ entspricht der Ordnung von $(\mathbb{F}_q[G_\delta])^{\star +}$.

Die folgenden zwei Beispiele veranschaulichen die Anwendung dieses Verfahrens.

Beispiel 4. a) Sei $\delta = 7$ und $q = 5$. Da 5 Primitivwurzel modulo 7 ist, folgt $\langle q\rangle = \{1, \ldots, 6\}$ und damit wiederum $\{0, 1, \ldots, 6\} = \{0\} \dot{\cup} \{1, \ldots, 6\}$, wobei $(\mathbb{Z}/7\mathbb{Z})^\star = a\langle 5\rangle$ für jedes $a \neq 0$ gilt[1]. Somit haben wir Involutionen

$$\bar{\iota}_{d_0,1} : \mathbb{F}_5[x]/(x-1) \to \mathbb{F}_5[x]/(x-1)$$

und

$$\bar{\iota}_{d_1,1} : \mathbb{F}_5[x]/(\phi_7(x)) \to \mathbb{F}_5[x]/(\phi_7(x)).$$

Das ergibt $m_0 = 5 - 1 = 4$ und $m_1 = 5^3 - 1$, also

$$|(\mathbb{F}_5[G_7])^{\star +}| = |\mathbb{F}_5^\star \times \mathbb{F}_{5^3}^\star| = 4 \cdot (5^3 - 1).$$

b) Sei $\delta = 7$ und $q = 11$. In $(\mathbb{Z}/7\mathbb{Z})^\star$ erhalten wir

$$\langle 11\rangle = \{1, 2, 4\}$$

und mit $a_2 = 1$ und $a_3 = 3$

$$\{0, 1, \ldots 7\} = \{0\} \dot{\cup} \{1, 2, 4\} \dot{\cup} \{3, 5, 6\}.$$

Hier ist $m_1 = 11 - 1 = 10$ und $m_2 = m_3 = \sqrt{q^3 - 1}$, woraus

$$|(\mathbb{F}_{11}[G_7])^{\star +}| = 10 \cdot (11^3 - 1)$$

folgt.

[1] Natürlich sieht man dies auch daran, dass $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ über $\mathbb{F}_5$ irreduzibel ist.

Damit haben wir alle Bausteine für das folgende Resultat beisammen.

Satz 4.33. *Sei l eine Primzahl derart, dass* $\mathrm{ggT}\left(h_l^+, \frac{l-1}{2}\right) = 1$ *gilt. In den folgenden Fällen sind die l-Einheiten modulo $\mathbb{Z}$-Torsion $\overline{U}_l$ projektiv, aber nicht frei über $\mathbb{Z}[G]$. Insbesondere gibt es damit nach Satz 4.28 in allen Zwischenkörpern $K_{q\delta} \subseteq K \subseteq \mathbb{Q}(\zeta_l)^+$ keine Minkowski-Einheit.*

a) $q\delta = 35 \mid \frac{l-1}{2}$, $\delta = 7$, $h_{K_7} = h_{K_{35}} = 8$,

b) $q\delta = 35 \mid \frac{l-1}{2}$, $\delta = 5$, $h_{K_5} = h_{K_{35}} = 11$,

c) $q\delta = 45 \mid \frac{l-1}{2}$, $\delta = 9$, $h_{K_9} = h_{K_{45}} = 19$,

d) $q\delta = 87 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{87}} = 7$,

e) $q\delta = 133 \mid \frac{l-1}{2}$, $\delta = 7$, $h_{K_7} = h_{K_{133}} = 8$,

f) $q\delta = 177 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{177}} = 13$,

g) $q\delta = 235 \mid \frac{l-1}{2}$, $\delta = 5$, $h_{K_5} = h_{K_{235}} = 11$,

h) $q\delta = 413 \mid \frac{l-1}{2}$, $\delta = 7$, $h_{K_7} = h_{K_{413}} = 8$,

i) $q\delta = 591 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{591}} = 19$,

j) $q\delta = 699 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{699}} = 7$,

k) $q\delta = 721 \mid \frac{l-1}{2}$, $\delta = 7$, $h_{K_7} = h_{K_{721}} = 8$,

l) $q\delta = 951 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{951}} = 73$,

m) $q\delta = 1329 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{1329}} = 19$,

n) $q\delta = 2391 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{2391}} = 7$,

o) $q\delta = 2913 \mid \frac{l-1}{2}$, $\delta = 3$, $h_{K_3} = h_{K_{2913}} = 13$.

Beweis. Wir fassen jetzt die allgemeine Beweismethode, die lediglich eine Aneinanderreihung und Anwendung der Ergebnisse dieses Abschnitts ist, zusammen. Die numerischen Daten, die in Verbindung mit diesen Ausführungen den Beweis vervollständigen, sind in Anhang C zu finden. Zur Veranschaulichung geben wir in den einzelnen Schritten die jeweils zugehörigen Daten für Fall a) an.

Mit Hilfe von Abschnitt 4.5 bestimmen wir zunächst das zu $\overline{U}_l^{(\delta)}$ gehörende Ideal $X^{(\delta)} \subset \mathbb{Z}[G_\delta]$.

Im Fall a) ergibt sich hier

$$X^{(7)} = (2, \sigma^3 + \sigma^2 + 1) \text{ oder } X^{(7)} = (2, \sigma^3 + \sigma + 1).$$

In den „kleinen“ Gruppenringen $\mathbb{Z}[G_\delta]$ lässt sich durch einen einfachen probabilistischen Algorithmus mit Hilfe eines Computers schnell ein Erzeuger η_δ von $X^{(\delta)}$ finden.
Für die beiden Möglichkeiten in Fall a) erhalten wir

$$X^{(7)} = (-\sigma^4 + \sigma^3 + \sigma) \text{ oder } X^{(7)} = (\sigma^6 + \sigma^5 - \sigma).$$

Wie zu Beginn dieses Abschnitts beschrieben, gilt damit

$$X^{(q\cdot\delta)} \cong (\mathbb{Z}[G_\delta], \mathbb{Z}[\zeta_q][G_\delta], j_1(\eta_\delta)),$$

wobei j_1 die Abbildung $\mathbb{Z}[G_\delta] \to \mathbb{F}_q[G_\delta]$ aus dem entsprechenden Pullback-Diagramm ist. Berechnet man jetzt die Ordnung von $j_1(\eta_\delta) \in (\mathbb{F}_q[G_\delta])^\star$ und mit dem vorgestellten Verfahren $\left|(\mathbb{F}_q[G_\delta])^{\star +}\right|$, so folgt mit Korollar 4.32, dass $j_1(\eta_\delta)$ nicht in $j_2((\mathbb{Z}[\zeta_q][G_\delta])^\star)$ liegt. Aus der zu dem Pullback-Diagramm gehörenden Mayer-Vietoris-Sequenz folgt also die Nichtfreiheit von $\overline{U}_l^{(\delta)}$, was, zusammen mit Korollar 4.13 die Behauptung liefert.
Dieser letzte Schritt liefert also für Fall a) die Ordnungen

$$\operatorname{ord}(j_1(-\sigma^4 + \sigma^3 + \sigma)) = 2^3 \cdot 3 \cdot 31 \text{ und } \operatorname{ord}(j_1(\sigma^6 + \sigma^5 - \sigma)) = 2^3 \cdot 3 \cdot 7 \cdot 31$$

in $\mathbb{F}_5[G_7]$ und wegen

$$3 \nmid (|G_7| \cdot |(\mathbb{F}_5[G_7])^{\star +}|) = 7 \cdot 2^4 \cdot 31$$

die Behauptung. □

Bemerkung. Natürlich lässt sich die hier vorgestellte Beweismethode auf eine Vielzahl weiterer Zahlenkombinationen anwenden. Die kritische Größe ist dabei δ; sollte dieses zu groß werden, wird man mit einfachen Mitteln keinen Erzeuger η_δ des zu $\overline{U}_l^{(\delta)}$ gehörenden Ideals $X^{(\delta)}$ mehr finden. Die hier getroffene Auswahl an Kombinationen ist leicht erklärt - es handelt sich dabei genau um die Kombinationen, die in den noch zu behandelnden Fällen der Liste von Schoof auftreten, in denen die vorgestellte Beweismethode Erfolg hat.

Der Beweis von Satz 4.33 liefert mehr, als die Aussage, dass $\overline{U}_l$ nicht $\mathbb{Z}[G]$-frei ist. In der Tat sind die Teiler von $j_1(\eta_\delta)$, die mittels Korollar 4.32 die Nichtfreiheit von $\overline{U}_l^{(q\delta)}$ über $\mathbb{Z}[G_{q\delta}]$ bezeugen, auch Teiler der Ordnung von $[\overline{U}_l^{(q\delta)}]$ in $\operatorname{Pic}(\mathbb{Z}[G_{q\delta}])$. Wir zeigen jetzt, dass die Ordnung von $[\overline{U}_l^{(q\delta)}]$ die Ordnung von $[\overline{U}_l] \in \operatorname{Pic}(\mathbb{Z}[G])$ teilt:

Lemma 4.34. *Sei $l > 2$ prim und seien ε_1 und ε_2 Teiler von $\frac{l-1}{2}$ derart, dass $\varepsilon_1 \mid \varepsilon_2$. Weiter seien G_{ε_1}, $H_{\varepsilon_2,\varepsilon_1}$ und $G_{\varepsilon_2} = G_{\varepsilon_1}/H_{\varepsilon_2,\varepsilon_1}$ wie zuvor. Dann definiert*

$$\mathrm{Pic}^{H_{\varepsilon_2,\varepsilon_1}} : \mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_2}]) \to \mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_1}]), \quad [M] \mapsto [M^{H_{\varepsilon_2,\varepsilon_1}}]$$

einen Homomorphismus mit $\mathrm{Pic}^{H_{\varepsilon_2,\varepsilon_1}}([\overline{U}_l^{(\varepsilon_2)}]) = [\overline{U}_l^{(\varepsilon_1)}]$.

Beweis. Nach Korollar 4.11 gilt $\left(\overline{U}_l^{(\varepsilon_2)}\right)^{H_{\varepsilon_2,\varepsilon_1}} = \overline{U}_l^{(\varepsilon_1)}$, woraus sofort

$$\mathrm{Pic}^{H_{\varepsilon_2,\varepsilon_1}}([\overline{U}_l^{(\varepsilon_2)}]) = [\overline{U}_l^{(\varepsilon_1)}]$$

folgt.
$\mathbb{Z}[G_{\varepsilon_2}]$ ist $\mathbb{Z}[G_{\varepsilon_2}]$-projektiv, sodass wir mit Lemma 4.12 und Korollar 4.13

$$N_{H_{\varepsilon_2,\varepsilon_1}}\mathbb{Z}[G_{\varepsilon_2}] = \mathbb{Z}[G_{\varepsilon_2}]^{H_{\varepsilon_2,\varepsilon_1}} = \mathbb{Z}[G_{\varepsilon_1}]$$

erhalten. Der Homomorphismus

$$\mathrm{aug}_{\varepsilon_2,\varepsilon_1} : \mathbb{Z}[G_{\varepsilon_2}] \to \mathbb{Z}[G_{\varepsilon_1}]$$

induziert bekanntlich einen Homomorphismus

$$\mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_2}]) \to \mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_1}]), \quad [M] \mapsto [M \otimes_{\mathbb{Z}[G_{\varepsilon_2}]} \mathbb{Z}[G_{\varepsilon_1}]].$$

$\mathbb{Z}[G_{\varepsilon_1}]$ ist via $\mathrm{aug}_{\varepsilon_2,\varepsilon_1}$ ein $\mathbb{Z}[G_{\varepsilon_2}]$-Modul. Man prüft schnell nach, dass die Abbildung

$$\mathbb{Z}[G_{\varepsilon_1}] \to (N_{H_{\varepsilon_2,\varepsilon_1}}) \subset \mathbb{Z}[G_{\varepsilon_2}], \quad 1 \mapsto N_{H_{\varepsilon_2,\varepsilon_1}}$$

ein $\mathbb{Z}[G_{\varepsilon_2}]$-Isomorphismus ist. Verwenden wir jetzt, wie schon in Abschnitt 4.4, dass für jeden projektiven Modul M über einem kommutativen Ring R und jedes Ideal $\mathfrak{a} \subset R$ die R-Moduln $\mathfrak{a}M$ und $\mathfrak{a} \otimes_R M$ isomorph sind, so erhalten wir die folgende Isomorphie

$$M \otimes_{\mathbb{Z}[G_{\varepsilon_2}]} \mathbb{Z}[G_{\varepsilon_1}] \cong M \otimes_{\mathbb{Z}[G_{\varepsilon_2}]} (N_{H_{\varepsilon_2,\varepsilon_1}}) \cong (N_{H_{\varepsilon_2,\varepsilon_1}})M \cong M^{H_{\varepsilon_2,\varepsilon_1}}$$

von $\mathbb{Z}[G_{\varepsilon_2}]$-Moduln. Damit sind $M \otimes_{\mathbb{Z}[G_{\varepsilon_2}]} \mathbb{Z}[G_{\varepsilon_1}]$ und $M^{H_{\varepsilon_2,\varepsilon_1}}$ auch über dem Faktorring $\mathbb{Z}[G_{\varepsilon_1}] = \mathbb{Z}[G_{\varepsilon_2}]/I_{\varepsilon_2,\varepsilon_1}$ isomorph.[2] $\mathrm{Pic}^{H_{\varepsilon_2,\varepsilon_1}}$ entspricht also gerade dem von $\mathrm{aug}_{\varepsilon_2,\varepsilon_1}$ induzierten Homomorphismus $\mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_2}]) \to \mathrm{Pic}(\mathbb{Z}[G_{\varepsilon_1}])$. □

Somit hat beispielsweise $[\overline{U}_l]$ für $l = 491$ mindestens die Ordnung 3, für $l = 5827$ mindestens die Ordnung 3^5.

[2] Wir wissen bereits, dass beide Moduln über $\mathbb{Z}[G_{\varepsilon_1}]$ sind; man sieht aber ebenso schnell, dass $I_{\varepsilon_2,\varepsilon_1}$ die beiden Moduln annulliert.

Wir führen jetzt noch einige Folgerungen an.

Folgerung 10. Für alle Primzahlen l in

$$\{491, 631, 827, 1063, 1567, 2351, 2659, 2927,\\ 3547, 4327, 4591, 4783, 5531, 5827, 6991, 9511\}$$

folgt mit Hilfe von Satz 4.33, dass die l-Einheiten modulo Torsion, $\overline{U}_l$, zwar $\mathbb{Z}[G]$-projektiv, aber nicht $\mathbb{Z}[G]$-frei sind. Die numerischen Daten für die Zuordnung zu den Fällen a)-o) sind in Anhang C zu finden. Wir bemerken an dieser Stelle, dass für die Gültigkeit dieser Aussage nicht notwendig ist, dass die von Schoof angegebenen Pseudo-Klassenzahlen tatsächlich den korrekten Klassenzahlen entsprechen; es wird nur benötigt, dass $h_{K_\delta} = h_{K_{q\delta}}$ gilt und die Klassenzahl h_l^+ teilerfremd zu $\frac{l-1}{2}$ ist. Ist letztere Bedingung nicht erfüllt, so ist nicht klar, ob die l-Einheiten modulo Torsion überhaupt $\mathbb{Z}[G]$-projektiv sind. Die Primzahl $l = 491$ liefert das kleinste Beispiel für $\mathbb{Q}(\zeta_l)^+$ ohne Minkowski-Einheit. Die vom Grad kleinsten Beispiele für Körper mit dieser Eigenschaft bilden die Unterkörper $K_{35} \subset \mathbb{Q}(\zeta_l)^+$ für $l \in \{491, 631, 5531\}$.

Folgerung 11. In dieser Folgerung sollen drei weitere Spezialfälle mit der in diesem Abschnitt vorgestellten Methode untersucht werden. Zur Abkürzung bezeichnen wir hier einen Erzeuger von G_3 mit σ statt mit σ_3.

a) Für $l = 8563$ gilt $\frac{l-1}{2} = 3 \cdot 1427$, $\delta^\star = 3$ und $h_{K_3} = \tilde{h}_l^+ = 49$. Hier bestimmt man schnell

$$|(\mathbb{F}_{1427}[G_3])^{\star +}| = 2033476 = 2^2 \cdot 23^2 \cdot 31^2.$$

Mit Abschnitt 4.5 ergeben sich drei verschiedene Möglichkeiten für $X^{(\delta^\star)}$, die wir im Folgenden mit den Mitteln aus diesem Abschnitt untersuchen.

i) $X^{(3)} = (49, \sigma + 31)$: Ein Erzeuger von $X^{(3)}$ ist hier durch $\eta_3 = -4\sigma^2 + \sigma + 4 \in \mathbb{Z}[G_3]$ gegeben. Da die Ordnung von $j_1(\eta_3)$ in $(\mathbb{F}_{1427}[G_3])^\star$ gleich $3 \cdot 7 \cdot 17 \cdot 23 \cdot 31$ ist, würden in diesem Fall die Faktoren 7 und 17 jeweils als Zeuge für die Nichtfreiheit von $\overline{U}_l$ über $\mathbb{Z}[G]$ fungieren.

ii) $X^{(3)} = (49, \sigma+19)$: Hier findet man einen Erzeuger, $\eta_3 = \sigma^2 - 4\sigma + 4$ von $X^{(3)}$, der die gleichen Eigenschaften wie η_3 in i) aufweist. Auch hier würde also folgen, dass $\overline{U}_l$ nicht $\mathbb{Z}[G]$-frei ist.

iii) $X^{(3)} = (7, \sigma^2 + 8\sigma + 15)$: Einen Erzeuger von $X^{(3)}$ bildet beispielsweise $\eta_3 = -2\sigma^2 + 5\sigma - 2$. Da $\mathrm{ord}(j_1(\eta_3)) = 3 \cdot 23 \cdot 31$ in $(\mathbb{F}_{1427}[G_3])^\star$ gilt, lässt sich Korollar 4.32 nicht anwenden; wir erhalten hier also keine Aussage über die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$.

Eine interessante offene Frage ist, ob mit den verfügbaren Informationen eine oder zwei der Möglichkeiten für $X^{(3)}$ ausgeschlossen werden können. An dieser Stelle bleibt die Frage nach der $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ also unbeantwortet.

b) Für die Primzahl $l = 9319$ gilt $\frac{l-1}{2} = 3 \cdot 1553$, $\delta^\star = 3$ und $\tilde{h}_l^+ = 4 \cdot 7$. Die vermutete Klassenzahl ist also keine Primzahlpotenz. Die zusätzliche Schwierigkeit, die es zu lösen gilt, ist hier die Identifizierung von $X^{(3)}$. Mit dem Verfahren aus Abschnitt 4.5 findet sich jedoch schnell

$$(X^{(3)})_2 = (2, \sigma^2 + \sigma + 1)$$

und

$$(X^{(3)})_7 = (7, \sigma + 3) \text{ oder } (X^{(3)})_7 = (7, \sigma + 5).$$

Da $(2, \sigma^2 + \sigma + 1) = (2, \sigma^2 + \sigma + 3)$ und sowohl $\sigma^2 + \sigma + 3$ in $\mathbb{Z}_7[G_3]$ als auch $\sigma + 3$ beziehungsweise $\sigma + 5$ in $\mathbb{Z}_2[G_3]$ invertierbar ist, erhalten wir

$$\begin{aligned} X^{(3)} &= (2, \sigma^2 + \sigma + 3) \cdot (7, \sigma + 3) = (14, (\sigma + 3)(\sigma^2 + \sigma + 3)) \\ &= (14, 4\sigma^2 + 6\sigma + 10) \end{aligned}$$

oder

$$\begin{aligned} X^{(3)} &= (2, \sigma^2 + \sigma + 3) \cdot (7, \sigma + 5) = (14, (\sigma + 5)(\sigma^2 + \sigma + 3)) \\ &= (14, 6\sigma^2 + 8\sigma + 16). \end{aligned}$$

In beiden Fällen lässt sich auch hier jeweils ein Erzeuger von $X^{(3)}$ bestimmen. Für

$$X^{(3)} = (14, 4\sigma^2 + 6\sigma + 10) = (\eta_1), \text{ wobei } \eta_1 = \sigma^2 - 3\sigma + 3 \text{ ist,}$$

und

$$X^{(3)} = (14, 6\sigma^2 + 8\sigma + 16) = (\eta_2), \text{ wobei } \eta_2 = \sigma^2 + 3\sigma - 3 \text{ ist,}$$

erhält man die Ordnung

$$\operatorname{ord}(j_1(\eta_1)) = \operatorname{ord}(j_1(\eta_2)) = 2411808 = 2^5 \cdot 3 \cdot 7 \cdot 37 \cdot 97$$

in $(\mathbb{F}_{1553}[G_3])^\star$. Da aber

$$|(\mathbb{F}_{1553}[G_3])^{\star +}| = 2408704 = 2^8 \cdot 97^2$$

ist, folgt mit Korollar 4.32 in beiden Fällen, dass $\overline{U}_l$ nicht $\mathbb{Z}[G]$-frei ist.

c) Auch für $l = 4219$ gilt $\delta^\star = 3$ und $h_{K_3} = \tilde{h}_l^+ = 4 \cdot 7$. Für $X^{(3)}$ ergeben sich also die gleichen Erzeuger wie in b). Da $\frac{l-1}{2} = 3 \cdot 19 \cdot 37$ ist, bestimmen wir die Ordnung von $j_1(\eta_1)$ und $j_1(\eta_2)$ in $(\mathbb{F}_{19}[G_3])^\star$ und in $(\mathbb{F}_{37}[G_3])^\star$. Das Ergebnis ist in allen Fällen $18 = 2 \cdot 3^2$, sodass wir hier wegen

$$|(\mathbb{F}_{19}[G_3])^{\star +}| = 2^2 \cdot 3^4 \text{ und } |(\mathbb{F}_{37}[G_3])^{\star +}| = 2^4 \cdot 3^4$$

keine Aussage über die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ erhalten.

Die letzte Folgerung aus Satz 4.33 ist unabhängig von Schoofs Liste.

Folgerung 12. Wir bestimmen mit Hilfe von PARI/GP zwei Listen,

a) Kand$(35, 7, 8)$ und

b) Kand$(35, 5, 11)$,

die alle Primzahlen $2 < l < 500000$ mit $l \equiv 3 \mod 4$ und

a) $35 \mid \frac{l-1}{2}$, $h_{K_7} = 8$ und $h_{K_5} = 1$ beziehungsweise

b) $35 \mid \frac{l-1}{2}$, $h_{K_5} = 11$ und $h_{K_7} = 1$

enthalten.
In diesen liegen alle Primzahlen in dem betrachteten Bereich, für die Satz 4.33 a) beziehungsweise b) möglicherweise anwendbar ist. Dazu zwei Bemerkungen:

1.) Wie in der Einleitung bereits erwähnt, ist die Berechnung von h_l^+ für $l > 67$ nach derzeitigem Kenntnisstand unmöglich. Das führt dazu, dass die Bedingung ggT $\left(h_l^+, \frac{l-1}{2}\right) = 1$ nicht geprüft werden kann. Folglich ist unklar, ob auch nur für eine Primzahl l aus diesen Listen die l-Einheiten modulo Torsion überhaupt nach Satz 3.3 $\mathbb{Z}[G]$-projektiv sind.

2.) Auch die Überprüfung von

a) $h_{K_{35}} = h_{K_7}$ beziehungsweise von

b) $h_{K_{35}} = h_{K_5}$

scheitert mit den zur Verfügung stehenden Mitteln an der Berechnung von $h_{K_{35}}$. Es ist klar, dass $h_{K_{35}} = h_{K_7}$ beziehungsweise $h_{K_{35}} = h_{K_5}$ die Gleichheiten $h_{K_5} = 1$ beziehungsweise $h_{K_7} = 1$ impliziert. Da die Umkehrung nicht gilt, ist die neu hinzugefügte und leicht prüfbare Bedingung $h_{K_5} = 1$ beziehungsweise $h_{K_7} = 1$ auch schwächer.

Diese beiden Einschränkungen sind auch in den Namen der Listen als „Kandidatenlisten“ eingegangen.

Abschließende Bemerkungen und Ausblick

Wir haben uns in dieser Arbeit mit der Galoismodulstruktur der l-Einheiten modulo Torsion, $\overline{U}_l$, in den (maximal) reellen Unterkörpern von l-ten Kreisteilungskörpern beschäftigt und zudem eine Verbindung zur Existenz von Minkowski-Einheiten hergestellt. Dabei haben wir unsere theoretischen Ergebnisse auf die ungeraden Primzahlen $2 < l < 10000$ übertragen, wobei wir angenommen haben, dass die von Schoof bestimmten Teiler der Klassenzahlen den Klassenzahlen selbst entsprechen[3]. Während wir uns in Kapitel 3 mit der $\mathbb{Z}[G]$-Projektivität von $\overline{U}_l$ befasst haben und in allen betrachteten Fällen zu einem Ergebnis gelangt sind, ist dies in Kapitel 4 bei der Untersuchung auf $\mathbb{Z}[G]$-Freiheit nicht vollständig gelungen. In Abschnitt 4.7 konnte für einige bestimmte Kombinationen von $\delta^\star$ und h_l^+ durch explizite Angabe eines Erzeugers des zu $\overline{U}_l$ gehörenden Ideals $X \subset \mathbb{Z}[G]$ die $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ nachgewiesen werden. Etwa die Hälfte der in diesem Kapitel zur Untersuchung stehenden Fälle aus Schoofs Liste wurden dadurch abgeschlossen. Aufbauend auf den Ergebnissen von Schoof konnte zudem bereits in Abschnitt 4.6 durch eine relativ einfache Überlegung die Frage nach der Existenz $\mathbb{Z}[G]$-projektiver und zugleich nicht $\mathbb{Z}[G]$-freier $\overline{U}_l$ positiv beantwortet werden. Das im Vergleich dazu deutlich kompliziertere Verfahren aus Abschnitt 4.8 lieferte weitere Beispiele, sowie eine von Schoofs Arbeit unabhängige Liste von Kandidaten, die diese Eigenschaft besitzen könnten. Ähnlich wie in den bereits beschriebenen Fällen $l = 4219$ und $l = 8563$, erbrachte die Untersuchung der Fälle $l \in \{191, 1459, 1831, 1987, 4339, 5051, 5119, 8287, 9127, 9551, 9907\}$ mit dieser Methode kein Ergebnis. An dieser Stelle sollte bemerkt werden, dass für $l = 1459$ wegen $\frac{l-1}{2} = 3^6$ ein Testen mit dem Verfahren aus 4.8 überhaupt nicht möglich ist. Die Ergebnislosigkeit der vorgestellten Methode in einigen Fällen ist natürlich nicht überraschend, kann aber allenfalls als Indiz auf mögliche $\mathbb{Z}[G]$-Freiheit von $\overline{U}_l$ gewertet werden. Ein Verfahren zum Nachweis von $\mathbb{Z}[G]$-Freiheit wäre hier eine wünschenswerte Ergänzung. Die letzten beiden Fälle aus Schoofs Liste, die bisher ungenannt blieben, sind $l = 1231$ und $l = 8431$. Bei diesen scheitert die Anwendung von 4.8 auf Grund eines anderen Problems. Für beide Primzahlen tritt die Nichttrivialität der Klassengruppe erst ab K_{15} auf, es gilt also $\delta^\star = 15$ und $h_{K_\delta} = 1$ für alle $\delta < \delta^\star$. Zur Bestimmung von $X^{(15)}$ ist nach Abschnitt 4.5 also $\mathbb{Z}[G_{15}]$ oder genauer $\mathbb{Z}[x]/(\phi_{15}(x))$ relevant. Man kann nachweisen, dass $\mathrm{Pic}(\mathbb{Z}[G_{15}]) \cong \mathbb{Z}/2\mathbb{Z}$ gilt und somit nicht klar ist, ob $X^{(15)}$ frei über $\mathbb{Z}[G_{15}]$ ist oder nicht. Diese Frage bleibt hier unbeantwortet, da einerseits die Versuche, mögliche Erzeuger von $X^{(15)}$ zu bestimmen, in beiden Fällen fehlschlugen und andererseits ein

[3] Wie bereits in der Einleitung erwähnt, gibt es heuristische Gründe, die diese Annahme sehr sinnvoll erscheinen lassen.

Nachweis von Nichtfreiheit ähnlich wie in Abschnitt 4.6 wegen $h_{\mathbb{Q}(\zeta_{15})} = 1$ nicht möglich ist.
Wir bemerken noch, dass sich die vorgestellten Verfahren problemlos auf die Untersuchung von l-Einheiten in l^s-ten Kreisteilungskörpern ($s \geq 1$) erweitern lassen. An dieser Stelle ist die Dissertation von Hakkarainen [Hak07] erwähnenswert, in der, ähnlich wie von Schoof, eine Liste von Klassenzahlteilern erstellt wurde. Dabei wurden alle reellen abelschen Zahlkörper $K/\mathbb{Q}$, deren Führer kleiner 2000 ist, untersucht. Für $\mathbb{Q}(\zeta_{l^s})^+$ mit primem l und $s \geq 2$ wurden jedoch keine von 1 verschiedenen Teiler von $h_{l^s}^+$ gefunden, sodass für explizite Rechnungen mit Hilfe der oben angesprochenen Erweiterungen eine Grundlage, nämlich (vermutete) Klassenzahlen, fehlen.

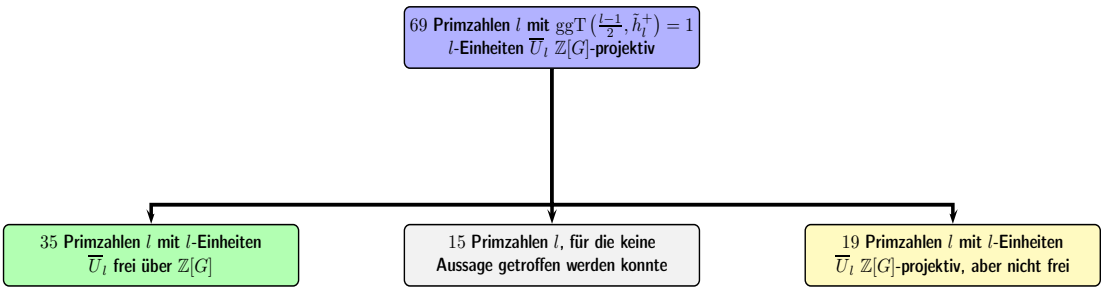


Abbildung 4.1: Situation nach Kapitel 4

Anhang A

Tabellen zur $\mathbb{Z}[G]$-Projektivität

Zu Folgerung 1: 140 Primzahlen $l < 10000$ mit $l \equiv 1 \mod 4$, $\tilde{h}_l^+ \neq 1$ und $\mathrm{ggT}\left(\frac{l-1}{2}, \tilde{h}_l^+\right) = 1$. Damit ist $\overline{U}_l$ für alle diese l nicht $\mathbb{Z}[G]$-projektiv[1].

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	l	$\frac{l-1}{2}$	$\tilde{h}_l^+$
257	$128 = 2^7$	3	1901	$950 = 2 \cdot 5^2 \cdot 19$	3
313	$156 = 2^2 \cdot 3 \cdot 13$	7	2029	$1014 = 2 \cdot 3 \cdot 13^2$	7
457	$228 = 2^2 \cdot 3 \cdot 19$	5	2113	$1056 = 2^5 \cdot 3 \cdot 11$	37
521	$260 = 2^2 \cdot 5 \cdot 13$	27	2153	$1076 = 2^2 \cdot 269$	5
577	$288 = 2^5 \cdot 3^2$	7	2213	$1106 = 2 \cdot 7 \cdot 79$	3
761	$380 = 2^2 \cdot 5 \cdot 19$	3	2381	$1190 = 2 \cdot 5 \cdot 7 \cdot 17$	11
821	$410 = 2 \cdot 5 \cdot 41$	11	2417	$1208 = 2^3 \cdot 151$	697
829	$414 = 2 \cdot 3^2 \cdot 23$	47	2473	$1236 = 2^2 \cdot 3 \cdot 103$	5
857	$428 = 2^2 \cdot 107$	5	2617	$1308 = 2^2 \cdot 3 \cdot 109$	13
877	$438 = 2 \cdot 3 \cdot 73$	49	2621	$1310 = 2 \cdot 5 \cdot 131$	11
953	$476 = 2^2 \cdot 7 \cdot 17$	71	2753	$1376 = 2^5 \cdot 43$	9
977	$488 = 2^3 \cdot 61$	5	2777	$1388 = 2^2 \cdot 347$	3
1069	$534 = 2 \cdot 3 \cdot 89$	7	3001	$1500 = 2^2 \cdot 3 \cdot 5^3$	121
1093	$546 = 2 \cdot 3 \cdot 7 \cdot 13$	5	3041	$1520 = 2^4 \cdot 5 \cdot 19$	13
1153	$576 = 2^6 \cdot 3^2$	19	3137	$1568 = 2^5 \cdot 7^2$	9
1229	$614 = 2 \cdot 307$	3	3217	$1608 = 2^3 \cdot 3 \cdot 67$	7
1297	$648 = 2^3 \cdot 3^4$	275	3221	$1610 = 2 \cdot 5 \cdot 7 \cdot 23$	3
1373	$686 = 2 \cdot 7^3$	3	3253	$1626 = 2 \cdot 3 \cdot 271$	5
1381	$690 = 2 \cdot 3 \cdot 5 \cdot 23$	7	3313	$1656 = 2^3 \cdot 3^2 \cdot 23$	133
1429	$714 = 2 \cdot 3 \cdot 7 \cdot 17$	5	3433	$1716 = 2^2 \cdot 3 \cdot 11 \cdot 13$	37
1601	$800 = 2^5 \cdot 5^2$	7	3469	$1734 = 2 \cdot 3 \cdot 17^2$	13
1697	$848 = 2^4 \cdot 53$	17	3529	$1764 = 2^2 \cdot 3^2 \cdot 7^2$	19
1861	$930 = 2 \cdot 3 \cdot 5 \cdot 31$	11	3581	$1790 = 2 \cdot 5 \cdot 179$	11
1873	$936 = 2^3 \cdot 3^2 \cdot 13$	25	3697	$1848 = 2^3 \cdot 3 \cdot 7 \cdot 11$	5
1889	$944 = 2^4 \cdot 59$	49	4001	$2000 = 2^4 \cdot 5^3$	3

[1] Auch für $l \equiv 1 \mod 4$ mit $\tilde{h}_l^+ = 1$ ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv. Diese weiteren 377 Fälle führen wir hier jedoch nicht an.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	l	$\frac{l-1}{2}$	$\tilde{h}_l^+$
4073	$2036 = 2^2 \cdot 509$	5	6737	$3368 = 2^3 \cdot 421$	9
4177	$2088 = 2^3 \cdot 3^2 \cdot 29$	19	6781	$3390 = 2 \cdot 3 \cdot 5 \cdot 113$	13
4201	$2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$	11	6949	$3474 = 2 \cdot 3^2 \cdot 193$	5
4241	$2120 = 2^3 \cdot 5 \cdot 53$	9	6961	$3480 = 2^3 \cdot 3 \cdot 5 \cdot 29$	17
4409	$2204 = 2^2 \cdot 19 \cdot 29$	9	7229	$3614 = 2 \cdot 13 \cdot 139$	5
4457	$2228 = 2^2 \cdot 557$	5	7369	$3684 = 2^2 \cdot 3 \cdot 307$	13
4481	$2240 = 2^6 \cdot 5 \cdot 7$	291	7417	$3708 = 2^2 \cdot 3^2 \cdot 103$	109
4493	$2246 = 2 \cdot 1123$	3	7481	$3740 = 2^2 \cdot 5 \cdot 11 \cdot 17$	3
4649	$2324 = 2^2 \cdot 7 \cdot 83$	3	7529	$3764 = 2^2 \cdot 941$	5
4657	$2328 = 2^3 \cdot 3 \cdot 97$	5	7561	$3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$	37
4793	$2396 = 2^2 \cdot 599$	5	7621	$3810 = 2 \cdot 3 \cdot 5 \cdot 127$	7
4817	$2408 = 2^3 \cdot 7 \cdot 43$	17	7673	$3836 = 2^2 \cdot 7 \cdot 137$	3
4861	$2430 = 2 \cdot 3^5 \cdot 5$	7	7817	$3908 = 2^2 \cdot 977$	5
4889	$2444 = 2^2 \cdot 13 \cdot 47$	5	7937	$3968 = 2^7 \cdot 31$	41
4937	$2468 = 2^2 \cdot 617$	5	8069	$4034 = 2 \cdot 2017$	3
4993	$2496 = 2^6 \cdot 3 \cdot 13$	5	8101	$4050 = 2 \cdot 3^4 \cdot 5^2$	13
5081	$2540 = 2^2 \cdot 5 \cdot 127$	3	8269	$4134 = 2 \cdot 3 \cdot 13 \cdot 53$	37
5101	$2550 = 2 \cdot 3 \cdot 5^2 \cdot 17$	11	8297	$4148 = 2^2 \cdot 17 \cdot 61$	45
5209	$2604 = 2^2 \cdot 3 \cdot 7 \cdot 31$	29	8317	$4158 = 2 \cdot 3^3 \cdot 7 \cdot 11$	113
5261	$2630 = 2 \cdot 5 \cdot 263$	3	8377	$4188 = 2^2 \cdot 3 \cdot 349$	5
5273	$2636 = 2^2 \cdot 659$	7	8389	$4194 = 2 \cdot 3^2 \cdot 233$	19
5297	$2648 = 2^3 \cdot 331$	3	8597	$4298 = 2 \cdot 7 \cdot 307$	3
5333	$2666 = 2 \cdot 31 \cdot 43$	3	8681	$4340 = 2^2 \cdot 5 \cdot 7 \cdot 31$	11
5413	$2706 = 2 \cdot 3 \cdot 11 \cdot 41$	23	8689	$4344 = 2^3 \cdot 3 \cdot 181$	5
5417	$2708 = 2^2 \cdot 677$	7	8837	$4418 = 2 \cdot 47^2$	3
5437	$2718 = 2 \cdot 3^2 \cdot 151$	31	8893	$4446 = 2 \cdot 3^2 \cdot 13 \cdot 19$	7
5441	$2720 = 2^5 \cdot 5 \cdot 17$	11	9001	$4500 = 2^2 \cdot 3^2 \cdot 5^3$	31
5477	$2738 = 2 \cdot 37^2$	3	9013	$4506 = 2 \cdot 3 \cdot 751$	7
5557	$2778 = 2 \cdot 3 \cdot 463$	1387	9029	$4514 = 2 \cdot 37 \cdot 61$	7
5581	$2790 = 2 \cdot 3^2 \cdot 5 \cdot 31$	73	9041	$4520 = 2^3 \cdot 5 \cdot 113$	17
5701	$2850 = 2 \cdot 3 \cdot 5^2 \cdot 19$	101	9049	$4524 = 2^2 \cdot 3 \cdot 13 \cdot 29$	7
5741	$2870 = 2 \cdot 5 \cdot 7 \cdot 41$	3	9241	$4620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	13
6053	$3026 = 2 \cdot 17 \cdot 89$	3	9277	$4638 = 2 \cdot 3 \cdot 773$	7
6073	$3036 = 2^2 \cdot 3 \cdot 11 \cdot 23$	13	9281	$4640 = 2^5 \cdot 5 \cdot 29$	3
6113	$3056 = 2^4 \cdot 191$	5	9293	$4646 = 2 \cdot 23 \cdot 101$	3
6229	$3114 = 2 \cdot 3^2 \cdot 173$	13	9377	$4688 = 2^4 \cdot 293$	5
6257	$3128 = 2^3 \cdot 17 \cdot 23$	29	9413	$4706 = 2 \cdot 13 \cdot 181$	81
6337	$3168 = 2^5 \cdot 3^2 \cdot 11$	97	9521	$4760 = 2^3 \cdot 5 \cdot 7 \cdot 17$	113
6361	$3180 = 2^2 \cdot 3 \cdot 5 \cdot 53$	61	9613	$4806 = 2 \cdot 3^3 \cdot 89$	7
6421	$3210 = 2 \cdot 3 \cdot 5 \cdot 107$	41	9689	$4844 = 2^2 \cdot 7 \cdot 173$	29
6449	$3224 = 2^3 \cdot 13 \cdot 31$	5	9749	$4874 = 2 \cdot 2437$	3
6529	$3264 = 2^6 \cdot 3 \cdot 17$	13	9817	$4908 = 2^2 \cdot 3 \cdot 409$	17
6577	$3288 = 2^3 \cdot 3 \cdot 137$	5321	9829	$4914 = 2 \cdot 3^3 \cdot 7 \cdot 13$	5
6581	$3290 = 2 \cdot 5 \cdot 7 \cdot 47$	11	9833	$4916 = 2^2 \cdot 1229$	3
6673	$3336 = 2^3 \cdot 3 \cdot 139$	17	9857	$4928 = 2^6 \cdot 7 \cdot 11$	73

Zu Folgerung 1: 69 Primzahlen $l < 10000$ mit $l \equiv 3 \mod 4$, $\tilde{h}_l^+ \neq 1$ und ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) = 1$. Damit ist $\overline{U}_l$ für alle diese Primzahlen $\mathbb{Z}[G]$-projektiv[2].

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	l	$\frac{l-1}{2}$	$\tilde{h}_l^+$
163	$81 = 3^4$	4	4783	$2391 = 3 \cdot 797$	7
191	$95 = 5 \cdot 19$	11	5051	$2525 = 5^2 \cdot 101$	1451
491	$245 = 5 \cdot 7^2$	8	5119	$2559 = 3 \cdot 853$	31
547	$273 = 3 \cdot 7 \cdot 13$	4	5479	$2739 = 3 \cdot 11 \cdot 83$	4
607	$303 = 3 \cdot 101$	4	5531	$2765 = 5 \cdot 7 \cdot 79$	8
631	$315 = 3^2 \cdot 5 \cdot 7$	11	5659	$2829 = 3 \cdot 23 \cdot 41$	4
827	$413 = 7 \cdot 59$	8	5779	$2889 = 3^3 \cdot 107$	4
1063	$531 = 3^2 \cdot 59$	13	5827	$2913 = 3 \cdot 971$	13
1231	$615 = 3 \cdot 5 \cdot 41$	211	6079	$3039 = 3 \cdot 1013$	4
1399	$699 = 3 \cdot 233$	4	6163	$3081 = 3 \cdot 13 \cdot 79$	4
1459	$729 = 3^6$	247	6247	$3123 = 3^2 \cdot 347$	16
1567	$783 = 3^3 \cdot 29$	7	6991	$3495 = 3 \cdot 5 \cdot 233$	7
1699	$849 = 3 \cdot 283$	4	7027	$3513 = 3 \cdot 1171$	4
1831	$915 = 3 \cdot 5 \cdot 61$	7	7411	$3705 = 3 \cdot 5 \cdot 13 \cdot 19$	131
1879	$939 = 3 \cdot 313$	4	7639	$3819 = 3 \cdot 19 \cdot 67$	4
1951	$975 = 3 \cdot 5^2 \cdot 13$	4	7687	$3843 = 3^2 \cdot 7 \cdot 61$	16
1987	$993 = 3 \cdot 331$	7	7867	$3933 = 3^2 \cdot 19 \cdot 23$	4
2131	$1065 = 3 \cdot 5 \cdot 71$	4	7879	$3939 = 3 \cdot 13 \cdot 101$	4
2311	$1155 = 3 \cdot 5 \cdot 7 \cdot 11$	4	8011	$4005 = 3^2 \cdot 5 \cdot 89$	4
2351	$1175 = 5^2 \cdot 47$	11	8191	$4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$	4
2659	$1329 = 3 \cdot 443$	19	8287	$4143 = 3 \cdot 1381$	7
2803	$1401 = 3 \cdot 467$	4	8431	$4215 = 3 \cdot 5 \cdot 281$	31
2927	$1463 = 7 \cdot 11 \cdot 19$	8	8563	$4281 = 3 \cdot 1427$	49
3271	$1635 = 3 \cdot 5 \cdot 109$	4	8647	$4323 = 3 \cdot 11 \cdot 131$	4
3547	$1773 = 3^2 \cdot 197$	16777	8731	$4365 = 3^2 \cdot 5 \cdot 97$	4
3727	$1863 = 3^4 \cdot 23$	4	8831	$4415 = 5 \cdot 883$	16
3931	$1965 = 3 \cdot 5 \cdot 131$	256	8887	$4443 = 3 \cdot 1481$	4
4099	$2049 = 3 \cdot 683$	4	9127	$4563 = 3^3 \cdot 13^2$	31
4219	$2109 = 3 \cdot 19 \cdot 37$	28	9283	$4641 = 3 \cdot 7 \cdot 13 \cdot 17$	4
4327	$2163 = 3 \cdot 7 \cdot 103$	8	9319	$4659 = 3 \cdot 1553$	28
4339	$2169 = 3^2 \cdot 241$	7	9391	$4695 = 3 \cdot 5 \cdot 313$	4
4567	$2283 = 3 \cdot 761$	4	9511	$4755 = 3 \cdot 5 \cdot 317$	73
4591	$2295 = 3^3 \cdot 5 \cdot 17$	19	9551	$4775 = 5^2 \cdot 191$	541
4603	$2301 = 3 \cdot 13 \cdot 59$	79	9907	$4953 = 3 \cdot 13 \cdot 127$	31
4639	$2319 = 3 \cdot 773$	4			

[2]Für $l \equiv 3 \mod 4$ mit $\tilde{h}_l^+ = 1$ ist $\overline{U}_l$ sogar frei über $\mathbb{Z}[G]$. Diese 548 Fälle führen wir hier jedoch nicht an.

Zu Folgerung 2: 50 Primzahlen $l < 10000$ mit $l \equiv 1 \mod 4$ ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$ und $\tilde{h}_l^+ \equiv 1 \mod 2$. Damit ist $\overline{U}_l$ für alle diese Primzahlen nicht $\mathbb{Z}[G]$-projektiv.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	l	$\frac{l-1}{2}$	$\tilde{h}_l^+$
229	$114 = 2 \cdot 3 \cdot 19$	3	5281	$2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$	9
401	$200 = 2^3 \cdot 5^2$	45	5501	$2750 = 2 \cdot 5^3 \cdot 11$	11
641	$320 = 2^6 \cdot 5$	495	5521	$2760 = 2^3 \cdot 3 \cdot 5 \cdot 23$	9
733	$366 = 2 \cdot 3 \cdot 61$	3	5641	$2820 = 2^2 \cdot 3 \cdot 5 \cdot 47$	9
1129	$564 = 2^2 \cdot 3 \cdot 47$	63	5821	$2910 = 2 \cdot 3 \cdot 5 \cdot 97$	3
1489	$744 = 2^3 \cdot 3 \cdot 31$	57	6133	$3066 = 2 \cdot 3 \cdot 7 \cdot 73$	3
2081	$1040 = 2^4 \cdot 5 \cdot 13$	25	6481	$3240 = 2^3 \cdot 3^4 \cdot 5$	5
2089	$1044 = 2^2 \cdot 3^2 \cdot 29$	27	6521	$3260 = 2^2 \cdot 5 \cdot 163$	5
2437	$1218 = 2 \cdot 3 \cdot 7 \cdot 29$	7	6997	$3498 = 2 \cdot 3 \cdot 11 \cdot 53$	21
2557	$1278 = 2 \cdot 3^2 \cdot 71$	147	7057	$3528 = 2^3 \cdot 3^2 \cdot 7^2$	147
2677	$1338 = 2 \cdot 3 \cdot 223$	3	7333	$3666 = 2 \cdot 3 \cdot 13 \cdot 47$	13
2713	$1356 = 2^2 \cdot 3 \cdot 113$	3	7537	$3768 = 2^3 \cdot 3 \cdot 157$	3
2857	$1428 = 2^2 \cdot 3 \cdot 7 \cdot 17$	3	7573	$3786 = 2 \cdot 3 \cdot 631$	9
2917	$1458 = 2 \cdot 3^6$	21	7753	$3876 = 2^2 \cdot 3 \cdot 17 \cdot 19$	1875
3121	$1560 = 2^3 \cdot 3 \cdot 5 \cdot 13$	305	7873	$3936 = 2^5 \cdot 3 \cdot 41$	27
3181	$1590 = 2 \cdot 3 \cdot 5 \cdot 53$	5	8017	$4008 = 2^3 \cdot 3 \cdot 167$	130473
3229	$1614 = 2 \cdot 3 \cdot 269$	9	8161	$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	5
3877	$1938 = 2 \cdot 3 \cdot 17 \cdot 19$	3	8501	$4250 = 2 \cdot 5^3 \cdot 17$	5
3889	$1944 = 2^3 \cdot 3^5$	3	8581	$4290 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	9
4049	$2024 = 2^3 \cdot 11 \cdot 23$	23	8713	$4356 = 2^2 \cdot 3^2 \cdot 11^2$	201
4229	$2114 = 2 \cdot 7 \cdot 151$	7	8761	$4380 = 2^2 \cdot 3 \cdot 5 \cdot 73$	81
4441	$2220 = 2^2 \cdot 3 \cdot 5 \cdot 37$	25	9133	$4566 = 2 \cdot 3 \cdot 761$	21
4597	$2298 = 2 \cdot 3 \cdot 383$	21	9161	$4580 = 2^2 \cdot 5 \cdot 229$	5
4729	$2364 = 2^2 \cdot 3 \cdot 197$	39	9181	$4590 = 2 \cdot 3^3 \cdot 5 \cdot 17$	25
4933	$2466 = 2 \cdot 3^2 \cdot 137$	9	9697	$4848 = 2^4 \cdot 3 \cdot 101$	63

Zu Folgerung 3 bzw. Folgerung 4: 2 Primzahlen $l < 10000$ mit $l \equiv 3 \mod 4$, $\tilde{h}_l^+ \neq 1$ und ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$. In beiden Fällen ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	l	$\frac{l-1}{2}$	$\tilde{h}_l^+$
3571	$1785 = 3 \cdot 5 \cdot 7 \cdot 17$	7	7351	$3675 = 3 \cdot 5^2 \cdot 7^2$	49

Zu Folgerung 6: 31 Primzahlen $l < 10000$ mit $l \equiv 1 \mod 4$ und $\mathrm{ggT}\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$, $\tilde{h}_l^+ \equiv 0 \mod 2$ und $\delta_2 \neq 2$ prim. $\overline{U}_l$ ist also für alle diese Primzahlen nicht $\mathbb{Z}[G]$-projektiv. In der Tabelle geben die Einträge für δ jeweils den Grad des Unterkörpers von $\mathbb{Q}(\zeta_l)^+$ an, bei dem der entsprechende Faktor von $\tilde{h}_l^+$ auftritt.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	δ	δ_2	$\mathrm{Cl}(K_{\delta_2})$
277	$138 = 2 \cdot 3 \cdot 23$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
397	$198 = 2 \cdot 3^2 \cdot 11$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
853	$426 = 2 \cdot 3 \cdot 71$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
941	$470 = 2 \cdot 5 \cdot 47$	16	5	5	$(\mathbb{Z}/2\mathbb{Z})^4$
1009[1]	$504 = 2^3 \cdot 3^2 \cdot 7$	$7 \cdot 4$	$2, 3$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
1777	$888 = 2^3 \cdot 3 \cdot 37$	16	3	3	$(\mathbb{Z}/2\mathbb{Z})^4$ oder[2] $(\mathbb{Z}/4\mathbb{Z})^2$
1789	$894 = 2 \cdot 3 \cdot 149$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
2161	$1080 = 2^3 \cdot 3^3 \cdot 5$	16	5	5	$(\mathbb{Z}/2\mathbb{Z})^4$
2689	$1344 = 2^6 \cdot 3 \cdot 7$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
2797	$1398 = 2 \cdot 3 \cdot 233$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
3037	$1518 = 2 \cdot 3 \cdot 11 \cdot 23$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
3301	$1650 = 2 \cdot 3 \cdot 5^2 \cdot 11$	$16 \cdot 151$	$5, 15$	5	$(\mathbb{Z}/2\mathbb{Z})^4$
3517	$1758 = 2 \cdot 3 \cdot 293$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
4789	$2394 = 2 \cdot 3^2 \cdot 7 \cdot 19$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
4801	$2400 = 2^5 \cdot 3 \cdot 5^2$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
5197	$2598 = 2 \cdot 3 \cdot 433$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
5953	$2976 = 2^5 \cdot 3 \cdot 31$	$4 \cdot 7$	$3, 3$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
6037	$3018 = 2 \cdot 3 \cdot 503$	$4 \cdot 7$	$3, 6$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
6301	$3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7$	8	7	7	$(\mathbb{Z}/2\mathbb{Z})^3$
6553	$3276 = 2^2 \cdot 3^2 \cdot 7 \cdot 13$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
6637	$3318 = 2 \cdot 3 \cdot 7 \cdot 79$	$3 \cdot 4 \cdot 3$	$2, 3, 6$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
6709	$3354 = 2 \cdot 3 \cdot 13 \cdot 43$	$4 \cdot 7$	$3, 3$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
6833	$3416 = 2^3 \cdot 7 \cdot 61$	8	7	7	$(\mathbb{Z}/2\mathbb{Z})^3$
7297	$3648 = 2^6 \cdot 3 \cdot 19$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
7589	$3794 = 2 \cdot 7 \cdot 271$	8	7	7	$(\mathbb{Z}/2\mathbb{Z})^3$
7841	$3920 = 2^4 \cdot 5 \cdot 7^2$	$421 \cdot 8 \cdot 8$	$5, 7, 7$	7	$(\mathbb{Z}/2\mathbb{Z})^6$ oder[3] $(\mathbb{Z}/4\mathbb{Z})^3$
8209	$4104 = 2^3 \cdot 3^3 \cdot 19$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
8629	$4314 = 2 \cdot 3 \cdot 719$	$4 \cdot 7$	$3, 3$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
9421	$4710 = 2 \cdot 3 \cdot 5 \cdot 157$	$4 \cdot 11 \cdot 7 \cdot 11$	$3, 5, 6, 10$	3	$(\mathbb{Z}/2\mathbb{Z})^2$
9649	$4824 = 2^3 \cdot 3^2 \cdot 67$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$
9721	$4860 = 2^2 \cdot 3^5 \cdot 5$	4	3	3	$(\mathbb{Z}/2\mathbb{Z})^2$

[1] siehe auch Folgerung 5.
[2] Satz 3.9 liefert diese Möglichkeiten; mit PARI/GP erhält man $\mathrm{Cl}(K_{\delta_2}) \cong (\mathbb{Z}/4\mathbb{Z})^2$.
[3] Satz 3.9 liefert diese Möglichkeiten; mit PARI/GP erhält man $\mathrm{Cl}(K_{\delta_2}) \cong (\mathbb{Z}/2\mathbb{Z})^6$.

Zu Folgerung 7: 11 Primzahlen $l < 10000$ mit $l \equiv 1 \mod 4$ und $\mathrm{ggT}\left(\frac{l-1}{2}, \tilde{h}_l^+\right) \neq 1$, $\tilde{h}_l^+ \equiv 0 \mod 2$ und $\delta_2 = 2^e \cdot p$ ($p \neq 2$ prim). Für alle diese Primzahlen ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv. Auch hier geben die Einträge für δ jeweils den Grad des Unterkörpers von $\mathbb{Q}(\zeta_l)^+$ an, bei dem der entsprechende Faktor von $\tilde{h}_l^+$ auftritt.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	δ	$\delta_2 = \delta^\star$
349	$174 = 2 \cdot 3 \cdot 29$	$4 \cdot 4$	$3, 6$	6
709	$354 = 2 \cdot 3 \cdot 59$	$4 \cdot 4$	$3, 6$	6
937	$468 = 2^2 \cdot 3^2 \cdot 13$	$4 \cdot 4$	$3, 6$	6
4261	$2130 = 2 \cdot 3 \cdot 5 \cdot 71$	$4 \cdot 4$	$3, 6$	6
4297	$2148 = 2^2 \cdot 3 \cdot 179$	$16 \cdot 16$	$3, 6$	6
4357	$2178 = 2 \cdot 3^2 \cdot 11^2$	$5 \cdot 4 \cdot 4$	$2, 3, 6$	6
4561	$2280 = 2^3 \cdot 3 \cdot 5 \cdot 19$	$4 \cdot 4$	$3, 6$	6
7489	$3744 = 2^5 \cdot 3^2 \cdot 13$	$7 \cdot 4 \cdot 16$	$3, 3, 6$	6
9109	$4554 = 2 \cdot 3^2 \cdot 11 \cdot 23$	$4 \cdot 4$	$3, 6$	6
9337	$4668 = 2^2 \cdot 3 \cdot 389$	$4 \cdot 4 \cdot 4$	$3, 6, 12$	12
9601[1]	$4800 = 2^6 \cdot 3 \cdot 5^2$	$4 \cdot 5 \cdot 4$	$3, 4, 6$	6

[1] siehe auch Folgerung 5.

Anhang B

PARI/GP-Skripte zur $\mathbb{Z}[G]$-Projektivität

Datenbestand

PrimeList enthält alle Primzahlen aus der Liste von Schoof, für die die vermutete Klassenzahl von $\mathbb{Q}(\zeta_l)^+$ nicht 1 ist.

```
PrimeList= [163,191,229,257,277,313,349,397,401,457,491,521,547,577,607,
631,641,709,733,761,821,827,829,853,857,877,937,941,953,977,1009,1063,
1069,1093,1129,1153,1229,1231,1297,1373,1381,1399,1429,1459,1489,1567,
1601,1697,1699,1777,1789,1831,1861,1873,1879,1889,1901,1951,1987,2029,
2081,2089,2113,2131,2153,2161,2213,2311,2351,2381,2417,2437,2473,2557,
2617,2621,2659,2677,2689,2713,2753,2777,2797,2803,2857,2917,2927,3001,
3037,3041,3121,3137,3181,3217,3221,3229,3253,3271,3301,3313,3433,3469,
3517,3529,3547,3571,3581,3697,3727,3877,3889,3931,4001,4049,4073,4099,
4177,4201,4219,4229,4241,4261,4297,4327,4339,4357,4409,4441,4457,4481,
4493,4561,4567,4591,4597,4603,4639,4649,4657,4729,4783,4789,4793,4801,
4817,4861,4889,4933,4937,4993,5051,5081,5101,5119,5197,5209,5261,5273,
5281,5297,5333,5413,5417,5437,5441,5477,5479,5501,5521,5531,5557,5581,
5641,5659,5701,5741,5779,5821,5827,5953,6037,6053,6073,6079,6113,6133,
6163,6229,6247,6257,6301,6337,6361,6421,6449,6481,6521,6529,6553,6577,
6581,6637,6673,6709,6737,6781,6833,6949,6961,6991,6997,7027,7057,7229,
7297,7333,7351,7369,7411,7417,7481,7489,7529,7537,7561,7573,7589,7621,
7639,7673,7687,7753,7817,7841,7867,7873,7879,7937,8011,8017,8069,8101,
8161,8191,8209,8269,8287,8297,8317,8377,8389,8431,8501,8563,8581,8597,
8629,8647,8681,8689,8713,8731,8761,8831,8837,8887,8893,9001,9013,9029,
9041,9049,9109,9127,9133,9161,9181,9241,9277,9281,9283,9293,9319,9337,
9377,9391,9413,9421,9511,9521,9551,9601,9613,9649,9689,9697,9721,9749,
9817,9829,9833,9857,9907];
```

Länge der Liste PrimeList:

```
maxlength = length(PrimeList);
```

ClassNumbers enthält die zu den in PrimeList gegebenen Primzahlen vermuteten Faktoren der Klassenzahlen.

```
ClassNumbers=
[4,11,3,3,4,7,[4,4],4,[5,9],5,8,27,4,7,4,11,[5,11,9],[4,4],3,3,11,8,47,
4,5,[7,7],[4,4],16,71,5,[7,4],13,7,5,[3^2,7],19,3,211,[11,25],3,7,4,5,
[13,19],[3,19],7,7,17,4,4^2,4,7,11,25,4,49,3,4,7,7,[5,5],[3,3,3],37,4,
5,16,3,4,11,11,[17,41],7,5,[3,7,7],13,11,19,3,4,3,9,3,4,4,3,[3,7],8,
[11,11],4,13,[5,61],3^2,5,7,3,[3,3],5,4,[16,151],[19,7],37,13,4,19,
[19,883],7,11,5,4,3,3,16^2,3,23,5,4,19,11,[4,7],7,9,[4,4],[4^2,4^2],8,
7,[5,4,4],3^2,[5,5],5,[3,97],3,[4,4],4,19,[3,7],79,4,3,5,[3,13],7,4,5,
4,17,7,5,[3,3],5,5,1451,3,11,31,4,29,3,7,[3,3],3,3,23,7,31,11,3,4,11,
3^2,8,[19,73],73,9,4,101,3,4,3,13,[4,7],[4,7],3,13,4,5,3,4,13,4^2,29,8,
97,61,41,5,5,5,13,4,[17,313],11,[3,4,3],17,[4,7],9,13,8,5,17,7,[3,7],4,
[3,7,7],5,4,13,[7,7],13,131,109,3,[7,4,4^2],5,3,37,3^2,8,7,4,3,4^2,
[3,25,5^2],5,[421,8,8],4,[3^2,3],4,41,4,[3,19,3,7,109],3,13,5,4,4,37,7,
[5,9],113,5,19,31,5,7^2,[3,3],3,[4,7],4,11,5,[3,67],4,[3^3,3],16,3,4,7
,31,7,7,17,7,[4,4],31,[3,7],5,[5,5],13,7,3,4,3,[4,7],[4,4,4],5,4,[3,27],
[4,11,7,11],73,113,541,[4,5,4],7,4,29,[7,9],4,3,17,5,3,73,31];
```

Degrees enthält die Grade, bei denen die Klassenzahlen in ClassNumbers auftreten.

```
Degrees= [3,5,2,2,3,3,[3,6],3,[2,8],4,7,26,3,2,3,5,[4,5,8],[3,6],2,2,
10,7,46,3,4,[3,6],[3,6],5,7,4,[2,3],3,6,2,[2,3],9,2,15,[2,8],2,6,3,2,
[3,9],[2,3],3,2,4,3,3,3,3,5,8,3,16,2,3,3,2,[2,10],[2,6,18],12,3,2,5,
2,3,5,10,[4,8],3,4,[2,3,6],4,10,3,2,3,2,8,2,3,3,2,[2,6],7,[5,7],3,4,
[2,20],2,2,3,2,[2,6],2,3,[5,15],[3,6],12,6,3,3,[3,9],3,5,4,3,2,2,5,2,
22,4,3,18,5,[3,3],2,4,[3,6],[3,6],7,3,[2,3,6],2,[2,4],4,[2,32],2,[3,6],
3,9,[2,6],39,3,2,4,[2,12],3,3,4,3,8,6,2,[2,6],4,4,5,2,10,3,3,14,2,2,
[2,6],2,2,11,2,6,10,2,3,5,2,7,[3,6],9,4,3,10,2,3,2,3,[3,3],[3,6],2,12,
3,2,2,3,6,3,4,7,48,20,10,4,2,4,12,3,[4,8],5,[2,3,6],8,[3,3],4,6,7,2,8,
3,[2,6],3,[2,2,14],2,3,6,[3,21],12,65,12,2,[3,3,6],4,2,6,2,7,3,3,2,3,
[2,3,4],2,[5,7,7],3,[2,6],3,4,3,[2,3,6,6,12],2,2,4,3,3,3,3,[4,4],14,4,
6,15,2,3,[2,6],2,[3,3],3,10,2,[2,33],3,[2,6],5,2,3,6,10,6,2,4,2,[3,6],
3,[2,6],4,[2,10],3,3,2,3,2,[3,3],[3,6,12],4,3,[2,26],[3,5,6,10],3,28,
5,[3,4,6],6,3,28,[3,4],3,2,4,2,2,8,3]
```

Die folgende Methode dient dazu, aus der Liste ClassNumbers eine vereinfachte Liste ClassNumbersSimple zu erzeugen, die die vermuteten Klassenzahlen enthält.

```
{simplifyList(liste)=
  local(i,j,ret);
  ret=listcreate(maxlength);
  for(i=1,length(liste),
    listput(ret,1);
    if(length(liste[i])>1,
      for(j=1,length(liste[i]),
        ret[i]=ret[i]*liste[i][j];
        ));
    if(length(liste[i])==1, ret[i]=liste[i]);
    );
  return (ret);
  }
```

Verwendung obiger Funktion zur Erstellung der bereits angesprochenen Liste ClassNumbersSimple.

```
ClassNumbersSimple = simplifyList(ClassNumbers);
```

Erstellung zweier Listen, GaloisGroupOrderSimple und GaloisGroupOrder, die die Ordnung $\frac{l-1}{2}$ der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ für $l \in$ PrimeList beziehungsweise deren Faktorisierung enthalten.

```
{GaloisGroupOrder = listcreate(303);
 GaloisGroupOrderSimple = listcreate(303);
 for(i=1,maxlength,
  listput(GaloisGroupOrderSimple, (PrimeList[i]-1)/2);
  listput(GaloisGroupOrder, factor(GaloisGroupOrderSimple[i]));
  );
 kill(i);
  }
```

Hilfsfunktionen

Eingabe der Funktion listList sind zwei Listen bigList und indList. Sie liefert die Teilliste von bigList, deren Elemente durch die Einträge in indList (Indizes) gegeben sind.

```
{listList(bigList,indList)=
  local(i,ret);
  ret=listcreate(length(indList));
  for(i=1,length(indList),
    listput(ret, bigList[indList[i]])
    );
  return (ret);
  }
```

Die Funktion isElement(element,inpList) gibt 1 aus, wenn element in der Liste inpList enthalten ist, sonst 0.

```
{isElement(element, inpList)=
  local(i,ret);
  ret=0;
  for(i=1, length(inpList),
    if(inpList[i]==element, ret=1);
    );
  return (ret);
  }
```

Die Funktion extendedLCM(inpList) liefert das kleinste gemeinsame Vielfache aller Zahlen in inpList.

```
{extendedLCM(inpList)=
  local(i,ret);
  if(length(inpList)==1,
    ret=inpList[1],
    ret=lcm(inpList[1],inpList[2]);
    for(i=3,length(inpList),
      ret=lcm(ret,inpList[i]);
      );
    );
  return (ret);
  }
```

Die Funktion filterCoprime(indList, inpList1, inpList2) liefert eine Liste aller Indizes i aus indList, so dass inpList1[i] und inpList2[i] koprim sind.

```
{filterCoprime(indList, inpList1, inpList2) =
  local(i,ret);
  ret = listcreate(length(indList));
  for(i=1,length(indList),
    if(gcd(inpList1[indList[i]],inpList2[indList[i]])==1,
      listput(ret,i);
      );
    );
  return (ret);
  }
```

Die Hilfsfunktion filterRmodS(R,S,indList, inpList) liefert eine Liste aller Indizes i aus indList, so dass inpList[i] $\equiv R \mod S$ ist.

```
{filterRmodS(R,S,indList,inpList)=
  local(i,ret);
  ret=listcreate(length(indList));
  for(i=1,length(indList),
    if((inpList[indList[i]]%S)==R,
      listput(ret,i);
      );
    );
  return (ret);
  }
```

Die Funktion subcyclo(n,d) liefert alle Unterkörper von $\mathbb{Q}(\zeta_n)$ bis zum Grad d; sie ist eine leicht abgewandelte Version der gleichnamigen Funktion aus dem User's Guide für PARI/GP [PARI], Seite 98 (die beim Autor eine Fehlermeldung lieferte, was die kleine Veränderung nötig machte). Die Ausgabe ist eine Liste der die Unterkörper über $\mathbb{Q}$ definierenden Polynome, direkt gefolgt vom jeweiligen Führer.

```
subcyclo(n, d = -1)=
  {
  local(Z,G,S);
  if (d < 0, d = n);
  Z = znstar(n);
  G = matdiagonal(Z[2]);
  S = [];
  forsubgroup(H = G, d,
    S = concat(S, galoissubcyclo(Z, mathnf(concat(G,H)),2));
    );
    S
  }
```

Untersuchung von $\overline{U}_l$ auf $\mathbb{Z}[G]$-Projektivität

Folgerung 1a

Berechnung zweier Listen ClassNumber1_3mod4 und ClassNumber1_1mod4 aller Primzahlen l mit $2 < l < 10000$, $\tilde{h}_l^+ = 1$ und $\frac{l-1}{2} \equiv 1$ bzw. $3 \mod 4$. Im ersten Fall ist $\overline{U}_l$ $\mathbb{Z}[G]$-frei, im zweiten Fall nicht projektiv über $\mathbb{Z}[G]$.

```
ClassNumber1_3mod4 = listcreate(1228);
ClassNumber1_1mod4 = listcreate(1228);
{folgerung1a()=
  local(i);
  for(i=2,1229,
    if(!(isElement(prime(i),PrimeList)),
      if(prime(i)%4==3,
        listput(ClassNumber1_3mod4, prime(i)),
        listput(ClassNumber1_1mod4, prime(i))
        );
      );
    );
  }
```

Zur Vorbereitung für weitere Berechnungen werden zwei Listen, ClassNumber_OrderG_Coprime und ClassNumber_OrderG_NotCoprime, mit den Indizes aller Elemente l aus PrimeList, für die $|\mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})| = |G| = \frac{l-1}{2}$ und $\tilde{h}_l^+$ teilerfremd bzw. nicht teilerfremd sind, erstellt.

```
ClassNumber_OrderG_Coprime =  listcreate(maxlength);
ClassNumber_OrderG_NotCoprime = listcreate(maxlength);

{CoprimeOrNot()=
  local(i);
  for(i=1,maxlength,
    if(gcd((PrimeList[i]-1)/2, ClassNumbersSimple[i])==1,
      listput(ClassNumber_OrderG_Coprime, i),
      listput(ClassNumber_OrderG_NotCoprime, i)
      );
    );
  }
```

Folgerung 1b

Berechnung zweier Listen ClassNumber_OrderG_Coprime_1mod4 und ClassNumber_OrderG_Coprime_3mod4 mit den Indizes aller Elemente l aus PrimeList, für die $|G|$ und $\tilde{h}_l^+$ teilerfremd sind und $l \equiv 1$ bzw. $3 \mod 4$ ist. Im ersten Fall ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv, im zweiten Fall schon.

```
ClassNumber_OrderG_Coprime_1mod4 =
  listcreate(length(ClassNumber_OrderG_Coprime));
ClassNumber_OrderG_Coprime_3mod4 =
  listcreate(length(ClassNumber_OrderG_Coprime));
{folgerung1b()=
  local(i);
  for(i=1,length(ClassNumber_OrderG_Coprime),
    if(PrimeList[ClassNumber_OrderG_Coprime[i]]%4==1,
      listput(ClassNumber_OrderG_Coprime_1mod4,ClassNumber_OrderG_Coprime[i]),
      listput(ClassNumber_OrderG_Coprime_3mod4,ClassNumber_OrderG_Coprime[i])
      );
    );
  }
```

Folgerung 2

Berechnung einer Liste ClassNumber_OrderG_NotCoprime_hOdd_1mod4, die die Indizes aller Elemente l aus PrimeList enthält, für die $|G|$ und $\tilde{h}_l^+$ nicht teilerfremd sind und $\tilde{h}_l^+$ ungerade sowie $l \equiv 1 \mod 4$ ist. $\overline{U}_l$ ist hier nicht $\mathbb{Z}[G]$-projektiv. Des Weiteren werden analog Listen für $l \equiv 3 \mod 4$, ClassNumber_OrderG_NotCoprime_3mod4, bzw. für $\tilde{h}_l^+ \equiv 0 \mod 2$, ClassNumber_OrderG_NotCoprime_hEven, berechnet. Sie werden etwas später benötigt.

```
ClassNumber_OrderG_NotCoprime_hOdd_1mod4 =
  listcreate(length(ClassNumber_OrderG_NotCoprime));
ClassNumber_OrderG_NotCoprime_3mod4 =
  listcreate(length(ClassNumber_OrderG_NotCoprime));
ClassNumber_OrderG_NotCoprime_hEven =
  listcreate(length(ClassNumber_OrderG_NotCoprime));
{folgerung2()=
  local(i);
  for(i=1, length(ClassNumber_OrderG_NotCoprime),
    if(PrimeList[ClassNumber_OrderG_NotCoprime[i]]%4==1,
      if((ClassNumbersSimple[ClassNumber_OrderG_NotCoprime[i]]%2)==1,
        listput(ClassNumber_OrderG_NotCoprime_hOdd_1mod4, ClassNumber_OrderG_NotCoprime[
            i]),
        listput(ClassNumber_OrderG_NotCoprime_hEven, ClassNumber_OrderG_NotCoprime[i])
        ),
      listput(ClassNumber_OrderG_NotCoprime_3mod4, ClassNumber_OrderG_NotCoprime[i])
      );

    );
  }
```

Folgerung 3 und **Folgerung 4** benötigen keine weiteren computergestützten Berechnungen.

Folgerung 5

ClassNumber_OrderG_NotCoprime_hEven wird durchsucht, für welche l es einen von 2 verschiedenen gemeinsamen Primteiler p von $|G| = \frac{l-1}{2}$ und $\tilde{h}_l^+$ gibt, so dass $\nu_p(\tilde{h}_l^+) \in \{1, 2\}$ und $\nu_p(|G|) \geq \nu_p(\tilde{h}_l^+)$ ist. In der Liste ClassNumber_OrderG_NotCoprime_hEven_aw5 werden die Indizes dieser Primzahlen in PrimeList gespeichert. In diesen Fällen ist $\overline{U}_l$ nicht $\mathbb{Z}[G]$-projektiv.

```
ClassNumber_OrderG_NotCoprime_hEven_aw5 =
  listcreate(length(ClassNumber_OrderG_NotCoprime_hEven));

{folgerung5()=
  local(i,j,OrderG,factorsH);
  for(i=1,length(ClassNumber_OrderG_NotCoprime_hEven),
    OrderG=GaloisGroupOrderSimple[ClassNumber_OrderG_NotCoprime_hEven[i]];
    factorsH=factor(ClassNumbersSimple[ClassNumber_OrderG_NotCoprime_hEven[i]]);
    for(j=1,length(factorsH~),
      if(!(factorsH[j,1]==2)&&(factorsH[j,2]<3),
        if(OrderG%(factorsH[j,1]^factorsH[j,2])==0,
          listput(ClassNumber_OrderG_NotCoprime_hEven_aw5,
              ClassNumber_OrderG_NotCoprime_hEven[i]);
          );
        );
      );
    );
  }
```

Die Funktion deg2() liefert die Liste ClassNumber_OrderG_NotCoprime_hEven_deg2 mit den δ_2-Werten für alle $\mathbb{Q}(\zeta_l)^+$, die durch ClassNumber_OrderG_NotCoprime_hEven gegeben sind.

```
ClassNumber_OrderG_NotCoprime_hEven_deg2 =
  listcreate(length(ClassNumber_OrderG_NotCoprime_hEven));
{deg2()=
  local(i,j,ClassNumber,Degree);
  for(i=1,length(ClassNumber_OrderG_NotCoprime_hEven),
    ClassNumber=ClassNumbers[ClassNumber_OrderG_NotCoprime_hEven[i]];
    Degree=listcreate(length(ClassNumber));
    if(length(ClassNumber)==1,
      listput(ClassNumber_OrderG_NotCoprime_hEven_deg2, Degrees[
          ClassNumber_OrderG_NotCoprime_hEven[i]]),
      for(j=1,length(ClassNumber),
        if(ClassNumber[j]%2==0,
          listput(Degree,Degrees[ClassNumber_OrderG_NotCoprime_hEven[i]][j]);
          );
        );
      listput(ClassNumber_OrderG_NotCoprime_hEven_deg2, extendedLCM(Degree));
      );
    );
  }
```

Folgerung 6 und Folgerung 7

Aus obiger Liste bestimmt folgerung6_7() zwei Listen, ClassNumber_OrderG_NotCoprime_hEven_deg2Even und ClassNumber_OrderG_NotCoprime_hEven_deg2Odd, mit den Indizes aus PrimeList, so dass der Grad δ_2 gerade bzw. ungerade ist. Nach Betrachtung dieser Listen sind keine weiteren computergestützten Rechnungen mehr nötig - $\overline{U}_l$ ist in allen Fällen nicht $\mathbb{Z}[G]$-projektiv.

```
ClassNumber_OrderG_NotCoprime_hEven_deg2Even =
  listcreate(length(ClassNumber_OrderG_NotCoprime_hEven_deg2));
ClassNumber_OrderG_NotCoprime_hEven_deg2Odd =
  listcreate(length(ClassNumber_OrderG_NotCoprime_hEven_deg2));
{folgerung6_7()=
  local(i);
  for(i=1,length(ClassNumber_OrderG_NotCoprime_hEven_deg2),
    if(ClassNumber_OrderG_NotCoprime_hEven_deg2[i]%2==0,
      listput(ClassNumber_OrderG_NotCoprime_hEven_deg2Even,
          ClassNumber_OrderG_NotCoprime_hEven[i]),
      listput(ClassNumber_OrderG_NotCoprime_hEven_deg2Odd,
          ClassNumber_OrderG_NotCoprime_hEven[i])
      );
    );
  }
```

Berechnung der die Unterkörper von $\mathbb{Q}(\zeta_l)$ bis zum Grad 3 bzw. 7 über $\mathbb{Q}$ definierenden Polynome für $l = 1777$ ($\delta_2 = 3$) bzw. $l = 7841$ ($\delta_2 = 7$).

```
subcyclo(1777,3)
subcyclo(7841,7)
```

Berechnung der Klassengruppen in beiden Fällen.

```
bnfclgp(x^3 + x^2 - 592*x + 724)
bnfclgp( x^7 + x^6 - 3360*x^5 + 54087*x^4 +
  1523280*x^3 - 24904626*x^2 - 194909041*x + 2439485891)
```

Anhang C

Tabellen zur $\mathbb{Z}[G]$-Freiheit

Untersucht werden 69 Primzahlen $2 < l < 10000$ mit $l \equiv 3 \mod 4$, $\tilde{h}_l^+ \neq 1$ und ggT $\left(\frac{l-1}{2}, \tilde{h}_l^+\right) = 1$. Nach Kapitel 2 gilt für die Kreiszahlen modulo Torsion $\overline{\mathrm{Cn}} \cong \mathbb{Z}[G]$, wobei $G = \langle\sigma\rangle$ wie zuvor die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_l)^+/\mathbb{Q})$ bezeichnet. Nach Kapitel 3 sind die l-Einheiten modulo Torsion $\overline{U}_l$ für alle diese Primzahlen $\mathbb{Z}[G]$-projektiv.

Zu Folgerung 9: 31 Primzahlen l mit $\tilde{h}_l^+ = 2^2$ und $\delta^\star = 3$. Da $\phi_3(x) = x^2 + x + 1$ irreduzibel über $\mathbb{F}_2$ ist, gilt $X = (2, \sigma^2 + \sigma + 1) = (\sigma^2 - \sigma + 1)$ für das zu $\overline{U}_l$ gehörende Ideal $X \subset \mathbb{Z}[G]$. Damit ist $\overline{U}_l$ in allen diesen Fällen $\mathbb{Z}[G]$-frei.

l	$\frac{l-1}{2}$	l	$\frac{l-1}{2}$
163	$81 = 3^4$	5659	$2829 = 3 \cdot 23 \cdot 41$
547	$273 = 3 \cdot 7 \cdot 13$	5779	$2889 = 3^3 \cdot 107$
607	$303 = 3 \cdot 101$	6079	$3039 = 3 \cdot 1013$
1399	$699 = 3 \cdot 233$	6163	$3081 = 3 \cdot 13 \cdot 79$
1699	$849 = 3 \cdot 283$	7027	$3513 = 3 \cdot 1171$
1879	$939 = 3 \cdot 313$	7639	$3819 = 3 \cdot 19 \cdot 67$
1951	$975 = 3 \cdot 5^2 \cdot 13$	7867	$3933 = 3^2 \cdot 19 \cdot 23$
2131	$1065 = 3 \cdot 5 \cdot 71$	7879	$3939 = 3 \cdot 13 \cdot 101$
2311	$1155 = 3 \cdot 5 \cdot 7 \cdot 11$	8011	$4005 = 3^2 \cdot 5 \cdot 89$
2803	$1401 = 3 \cdot 467$	8191	$4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$
3271	$1635 = 3 \cdot 5 \cdot 109$	8647	$4323 = 3 \cdot 11 \cdot 131$
3727	$1863 = 3^4 \cdot 23$	8731	$4365 = 3^2 \cdot 5 \cdot 97$
4099	$2049 = 3 \cdot 683$	8887	$4443 = 3 \cdot 1481$
4567	$2283 = 3 \cdot 761$	9283	$4641 = 3 \cdot 7 \cdot 13 \cdot 17$
4639	$2319 = 3 \cdot 773$	9391	$4695 = 3 \cdot 5 \cdot 313$
5479	$2739 = 3 \cdot 11 \cdot 83$		

Zu Folgerung 9: 1 Primzahl l mit $\tilde{h}_l^+ = 2^4$ und $\delta^\star = 5$. Da $\phi_5(x) = x^4+x^3+x^2+x+1$ irreduzibel über $\mathbb{F}_2$ ist, gilt $X = (\sigma^4-\sigma^3+\sigma^2-\sigma+1)$ für das zu $\overline{U}_l$ gehörende Ideal $X \subset \mathbb{Z}[G]$. Damit ist $\overline{U}_l$ in diesem Fall frei über $\mathbb{Z}[G]$.

l	$\frac{l-1}{2}$
8831	$4415 = 5 \cdot 883$

Zu Folgerung 9: 3 Primzahlen l mit $\tilde{h}_l^+ = 2^i$ ($i \in \{4,8\}$ und $\delta^\star \in \{3,5\}$. Da $\phi_3(x)$ und $\phi_5(x)$ irreduzibel über $\mathbb{F}_2$ sind, gilt $X = (\sigma^2-\sigma+1)$ beziehungsweise $X = (\sigma^4-\sigma^3+\sigma^2-\sigma+1)$ für das zu $\overline{U}_l$ gehörende Ideal $X \subset \mathbb{Z}[G]$. In diesen Fällen ist $\overline{U}_l$ also frei über $\mathbb{Z}[G]$.

l	$\frac{l-1}{2}$	$\tilde{h}_l^+$	$\delta^\star$	η
3931	$1965 = 3 \cdot 5 \cdot 131$	256	5	$(\sigma^4-\sigma^3+\sigma^2-\sigma+1)^2$
6247	$3123 = 3^2 \cdot 347$	16	3	$(\sigma^2-\sigma+1)^2$
7687	$3843 = 3^2 \cdot 7 \cdot 61$	16	3	$(\sigma^2-\sigma+1)^2$

Numerische Daten zum Beweis von Satz 4.33

a) $\delta \cdot q = 35$, $\delta = 7$, $q = 5$, $h_{K_7} = h_{K_{35}} = 8$

$X^{(7)} \subset \mathbb{Z}[G_7]$	η mit $X^{(7)} = (\eta)$	ord(η) in $\mathbb{F}_5[G_7]$	$\lvert(\mathbb{F}_5[G_7])^{\star+}\rvert$
$(2, \sigma^3+\sigma^2+1)$	$-\sigma^4+\sigma^3+\sigma$	$2^3 \cdot 3 \cdot 31$	$2^4 \cdot 31$
$(2, \sigma^3+\sigma+1)$	$\sigma^6+\sigma^5-\sigma$	$2^3 \cdot 3 \cdot 7 \cdot 31$	$2^4 \cdot 31$

b) $\delta \cdot q = 35$, $\delta = 5$, $q = 7$, $h_{K_5} = h_{K_{35}} = 11$

$X^{(5)} \subset \mathbb{Z}[G_5]$	η mit $X^{(5)} = (\eta)$	ord(η) in $\mathbb{F}_7[G_5]$	$\lvert(\mathbb{F}_7[G_5])^{\star+}\rvert$
$(11, \sigma+8)$	$-\sigma^3+2\sigma^2-\sigma+1$	$2^2 \cdot 3 \cdot 5^2$	$2^5 \cdot 3^2$
$(11, \sigma+7)$	$-2\sigma^4+4\sigma^3-4\sigma^2+3\sigma$	$2^3 \cdot 3 \cdot 5^2$	$2^5 \cdot 3^2$
$(11, \sigma+6)$	$2\sigma^4-\sigma^2-\sigma+1$	$2^2 \cdot 3 \cdot 5^2$	$2^5 \cdot 3^2$
$(11, \sigma+2)$	$2\sigma^4-2\sigma^3+2\sigma^2-1$	$2 \cdot 3 \cdot 5^2$	$2^5 \cdot 3^2$

c) $\delta \cdot q = 45$, $\delta = 9$, $q = 5$, $h_{K_9} = h_{K_{45}} = 19$

$X^{(9)} \subset \mathbb{Z}[G_9]$	η mit $X^{(9)} = (\eta)$	ord(η) in $\mathbb{F}_5[G_9]$	$\lvert(\mathbb{F}_5[G_9])^{\star+}\rvert$
$(19, \sigma+15)$	$-\sigma^6+\sigma^3+\sigma$	$2^2 \cdot 3 \cdot 7 \cdot 31$	$2^6 \cdot 31$
$(19, \sigma+14)$	$\sigma^8-\sigma^6+2\sigma^5-2\sigma^4+2\sigma^3-2\sigma^2+2\sigma-1$	$2^2 \cdot 3 \cdot 7 \cdot 31$	$2^6 \cdot 31$
$(19, \sigma+13)$	$\sigma^6-\sigma^4+\sigma^3+\sigma-1$	$2^2 \cdot 3^2 \cdot 7 \cdot 31$	$2^6 \cdot 31$
$(19, \sigma+10)$	$2\sigma^8-2\sigma^6-\sigma^5+2\sigma^4+2\sigma^3-\sigma^2-2\sigma+1$	$2^2 \cdot 3^2 \cdot 7 \cdot 31$	$2^6 \cdot 31$
$(19, \sigma+3)$	$-\sigma^6+\sigma^5+\sigma^3-\sigma^2+1$	$2^2 \cdot 3^2 \cdot 7 \cdot 31$	$2^6 \cdot 31$
$(19, \sigma+2)$	$\sigma^8+\sigma^7-\sigma^3-\sigma^2+1$	$2^2 \cdot 3^2 \cdot 7 \cdot 31$	$2^6 \cdot 31$

d) $\delta \cdot q = 87$, $\delta = 3$, $q = 29$, $h_{K_3} = h_{K_{87}} = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{29}[G_3]$	$\lvert(\mathbb{F}_{29}[G_3])^{\star +}\rvert$
$(7, \sigma + 5)$	$-\sigma^2 + 2\sigma$	$5 \cdot 7$	$2^4 \cdot 7^2$
$(7, \sigma + 3)$	$2\sigma - 1$	$3 \cdot 5 \cdot 7$	$2^4 \cdot 7^2$

e) $\delta \cdot q = 133$, $\delta = 7$, $q = 19$, $h_{K_7} = h_{K_{133}} = 8$

$X^{(7)} \subset \mathbb{Z}[G_7]$	η mit $X^{(7)} = (\eta)$	ord(η) in $\mathbb{F}_{19}[G_7]$	$\lvert(\mathbb{F}_{19}[G_7])^{\star +}\rvert$
$(2, \sigma^3 + \sigma^2 + 1)$	$-\sigma^6 + 2\sigma^4 + 2\sigma^3 + \sigma^2 - \sigma - 2$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 127$	$2^2 \cdot 3^5 \cdot 127$
$(2, \sigma^3 + \sigma + 1)$	$\sigma^6 + 2\sigma^5 - \sigma^4 - \sigma^3 + 2\sigma^2 - 2$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 127$	$2^2 \cdot 3^5 \cdot 127$

f) $\delta \cdot q = 177$, $\delta = 3$, $q = 59$, $h_{K_3} = h_{K_{177}} = 13$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{59}[G_3]$	$\lvert(\mathbb{F}_{59}[G_3])^{\star +}\rvert$
$(13, \sigma + 10)$	$-\sigma^2 + \sigma + 2$	$2^3 \cdot 3 \cdot 5 \cdot 29$	$2^2 \cdot 29^2$
$(13, \sigma + 4)$	$-\sigma^2 + 2\sigma + 1$	$2^3 \cdot 5 \cdot 29$	$2^2 \cdot 29^2$

g) $\delta \cdot q = 235$, $\delta = 5$, $q = 47$, $h_{K_5} = h_{K_{235}} = 11$

$X^{(5)} \subset \mathbb{Z}[G_5]$	η mit $X^{(5)} = (\eta)$	ord(η) in $\mathbb{F}_{47}[G_5]$	$\lvert(\mathbb{F}_{47}[G_5])^{\star +}\rvert$
$(11, \sigma + 8)$	$4\sigma^4 - 2\sigma^3 + 3\sigma - 4$	$2^6 \cdot 3 \cdot 13 \cdot 17 \cdot 23$	$2^6 \cdot 3 \cdot 23^2$
$(11, \sigma + 7)$	$-\sigma^3 + \sigma^2 + \sigma$	$2^6 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 23$	$2^6 \cdot 3 \cdot 23^2$
$(11, \sigma + 6)$	$2\sigma^4 - 2\sigma^3 + 2\sigma^2 - \sigma$	$2^6 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 23$	$2^6 \cdot 3 \cdot 23^2$
$(11, \sigma + 2)$	$4\sigma^4 - 4\sigma^2 - 2\sigma + 3$	$2^6 \cdot 3 \cdot 5 \cdot 13 \cdot 17 \cdot 23$	$2^6 \cdot 3 \cdot 23^2$

h) $\delta \cdot q = 413$, $\delta = 7$, $q = 59$, $h_{K_7} = h_{K_{413}} = 8$

$X^{(7)} \subset \mathbb{Z}[G_7]$	η mit $X^{(7)} = (\eta)$	ord(η) in $\mathbb{F}_{59}[G_7]$	$\lvert(\mathbb{F}_{59}[G_7])^{\star +}\rvert$
$(2, \sigma^3 + \sigma^2 + 1)$	$2\sigma^6 + -\sigma^4 + \sigma^3 + \sigma - 2$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 3541$	$2^2 \cdot 29^2 \cdot 3541$
$(2, \sigma^3 + \sigma + 1)$	$2\sigma^6 + \sigma^5 + \sigma^4 - 2\sigma^2 - 1$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 3541$	$2^2 \cdot 29^2 \cdot 3541$

i) $\delta \cdot q = 591$, $\delta = 3$, $q = 197$, $h_{K_3} = h_{K_{591}} = 19$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{197}[G_3]$	$\lvert(\mathbb{F}_{197}[G_3])^{\star +}\rvert$
$(19, \sigma + 12)$	$-\sigma^2 + 3$	$2^2 \cdot 7 \cdot 11$	$2^4 \cdot 7^4$
$(19, \sigma + 8)$	$-\sigma + 3$	$2^2 \cdot 7 \cdot 11$	$2^4 \cdot 7^4$

j) $\delta \cdot q = 699$, $\delta = 3$, $q = 233$, $h_{K_3} = h_{K_{699}} = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{233}[G_3]$	$\lvert(\mathbb{F}_{233}[G_3])^{\star +}\rvert$
$(7, \sigma + 5)$	$-\sigma^2 + 2\sigma$	$2^3 \cdot 3^2 \cdot 13 \cdot 29$	$2^6 \cdot 29^2$
$(7, \sigma + 3)$	$2\sigma^2 - \sigma$	$2^3 \cdot 3^2 \cdot 13 \cdot 29$	$2^6 \cdot 29^2$

k) $\delta \cdot q = 721$, $\delta = 7$, $q = 103$, $h_{K_7} = h_{K_{721}} = 8$

$X^{(7)} \subset \mathbb{Z}[G_7]$	η mit $X^{(7)} = (\eta)$	ord(η) in $\mathbb{F}_{103}[G_7]$	$\lvert(\mathbb{F}_{103}[G_7])^{\star +}\rvert$
$(2, \sigma^3 + \sigma^2 + 1)$	$\sigma^5 - 2\sigma^4 + 2\sigma^3 - \sigma + 1$	$2^3 \cdot 7 \cdot 13 \cdot 17 \cdot 3571$	$2^2 \cdot 3^3 \cdot 17^2 \cdot 3571$
$(2, \sigma^3 + \sigma + 1)$	$\sigma^6 + 2\sigma^3 + \sigma^2 - 2\sigma - 1$	$2^3 \cdot 7 \cdot 13 \cdot 17 \cdot 3571$	$2^2 \cdot 3^3 \cdot 17^2 \cdot 3571$

l) $\delta \cdot q = 951$, $\delta = 3$, $q = 317$, $h_{K_3} = h_{K_{951}} = 73$

$X^{(3)} \subset \mathbb{Z}[G_3])$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{317}[G_3]$	$\lvert(\mathbb{F}_{317}[G_3])^{\star+}\rvert$
$(73, \sigma + 65)$	$6\sigma^2 - 2\sigma - 3$	$2^2 \cdot 53 \cdot 79$	$2^4 \cdot 79^2$
$(73, \sigma + 9)$	$6\sigma^2 - 3\sigma - 2$	$2^2 \cdot 3 \cdot 53 \cdot 79$	$2^4 \cdot 79^2$

m) $\delta \cdot q = 1329$, $\delta = 3$, $q = 443$, $h_{K_3} = h_{K_{1329}} = 19$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{443}[G_3]$	$\lvert(\mathbb{F}_{443}[G_3])^{\star+}\rvert$
$(19, \sigma + 12)$	$3\sigma - 2$	$2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 37$	$2^2 \cdot 13^2 \cdot 17^2$
$(19, \sigma + 8)$	$-2\sigma + 3$	$2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 37$	$2^2 \cdot 13^2 \cdot 17^2$

n) $\delta \cdot q = 2391$, $\delta = 3$, $q = 797$, $h_{K_3} = h_{K_{2391}} = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{797}[G_3]$	$\lvert(\mathbb{F}_{797}[G_3])^{\star+}\rvert$
$(7, \sigma + 5)$	$-\sigma^2 + 2\sigma$	$2^3 \cdot 7 \cdot 19 \cdot 199$	$2^4 \cdot 199^2$
$(7, \sigma + 3)$	$2\sigma - 1$	$2^3 \cdot 3 \cdot 7 \cdot 19 \cdot 199$	$2^4 \cdot 199^2$

o) $\delta \cdot q = 2913$, $\delta = 3$, $q = 971$, $h_{K_3} = h_{K_{2913}} = 13$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{971}[G_3]$	$\lvert(\mathbb{F}_{971}[G_3])^{\star+}\rvert$
$(13, \sigma + 10)$	$-2\sigma^2 + \sigma + 2$	$3^5 \cdot 97$	$2^2 \cdot 5^2 \cdot 97^2$
$(13, \sigma + 4)$	$2\sigma^2 + \sigma - 2$	$3^5 \cdot 97$	$2^2 \cdot 5^2 \cdot 97^2$

Zu Folgerung 10: 16 Primzahlen $2 < l < 10000$, für die unter der Voraussetzung $h_l^+ = \tilde{h}_l^+$ mit Satz 4.33 folgt, dass die l-Einheiten modulo Torsion zwar $\mathbb{Z}[G]$-projektiv, aber nicht $\mathbb{Z}[G]$-frei sind.

l	$\frac{l-1}{2}$	$[K_\delta : \mathbb{Q}]$	h_{K_δ}	q	$h_{K_{q\delta}}$	nicht frei nach Satz 4.33
491	$5 \cdot 7^2$	7	8	5	8	a)
631	$3^2 \cdot 5 \cdot 7$	5	11	7	11	b)
827	$7 \cdot 59$	7	8	59	8	h)
1063	$3^2 \cdot 59$	3	13	59	13	f)
1567	$3^3 \cdot 29$	3	7	29	7	d)
2351	$5^2 \cdot 47$	5	11	47	11	g)
2659	$3 \cdot 443$	3	19	443	19	m)
2927	$7 \cdot 11 \cdot 19$	7	8	19	7	e)
3547	$3^2 \cdot 197$	3	19	197	19	i)
4327	$3 \cdot 7 \cdot 103$	7	8	103	8	k)
4591	$3^3 \cdot 5 \cdot 17$	9	19	5	19	c)
4783	$3 \cdot 797$	3	7	797	7	n)
5531	$5 \cdot 7 \cdot 79$	7	8	5	8	a)
5827	$3 \cdot 971$	3	13	971	13	o)
6991	$3 \cdot 5 \cdot 233$	3	7	233	7	j)
9511	$3 \cdot 5 \cdot 317$	3	73	317	73	l)

Zu Folgerung 11 sind alle relevanten Daten bereits angeführt worden.

Zu Folgerung 12: In Kand(h, p_1, p_2) sind alle Primzahlen $l < 500000$ mit $(p_1 \cdot p_2) \mid \frac{l-1}{2}$, $l \equiv 3 \mod 4$, $h_{K_{p_1}} = h$ und $h_{K_{p_2}} = 1$. Gilt $h_{K_{p_1 \cdot p_2}} = h$ und ggT $\left(h_l^+, \frac{l-1}{2}\right) = 1$, so sind die l-Einheiten modulo Torsion für $(h, p_1, p_2) = (11, 5, 7)$ und für $(h, p_1, p_2) = (8, 7, 5)$ nach nach Satz 4.33 b) beziehungsweise a) zwar $\mathbb{Z}[G]$-projektiv, aber nicht $\mathbb{Z}[G]$-frei.

$$\begin{aligned}
\text{Kand}(11,5,7) &= \{631, 19531, 28211, 37871, 51871, 90931, 104231, 117671,\\
&= 124951, 126631, 131251, 143711, 159811, 161071, 164431,\\
&= 184031, 187951, 204751, 269431, 301211, 302891, 316471,\\
&= 331871, 336491, 350771, 353011, 357211, 365471, 388711,\\
&= 404251, 438131, 441631, 456611, 460531, 481531, 490631\}
\end{aligned}$$

$$\begin{aligned}
\text{Kand}(8,7,5) &= \{491, 5531, 17431, 28771, 35491, 39971, 84211, 117811,\\
&= 128591, 145391, 173531, 216371, 224491, 225611, 241711,\\
&= 291271, 302191, 347411, 358331, 365611, 372611, 407471,\\
&= 416011, 432251, 449051\}
\end{aligned}$$

Daten zu Fällen, in denen das Verfahren aus Abschnitt 4.8 keine Aussage liefert:

a) $l = 191$, $\frac{l-1}{2} = 5 \cdot 19$, $\delta^\star = 5$, $h_{K_5} = \tilde{h}_l^+ = 11$

$X^{(5)} \subset \mathbb{Z}[G_5]$	η mit $X^{(5)} = (\eta)$	ord(η) in $\mathbb{F}_{19}[G_5]$
$(11, \sigma + 8)$	$-2\sigma^3 - \sigma^2 + 2\sigma + 2$	$2^3 \cdot 3^2 \cdot 5$
$(11, \sigma + 7)$	$2\sigma^3 + 2\sigma^2 - \sigma - 2$	$2^3 \cdot 3^2 \cdot 5$
$(11, \sigma + 6)$	$-\sigma^4 + \sigma^3 + 2\sigma^2 - 1$	$2^3 \cdot 3^2 \cdot 5$
$(11, \sigma + 2)$	$-2\sigma^4 + 2\sigma^3 - \sigma + 2$	$2^3 \cdot 3^2 \cdot 5$

$|(\mathbb{F}_{19}[G_5])^{\star +}| = 2^3 \cdot 3^6$

b) $l = 1831$, $\frac{l-1}{2} = 3 \cdot 5 \cdot 61$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_5[G_3]$	ord(η) in $\mathbb{F}_{61}[G_3]$
$(7, \sigma + 5)$	$2\sigma^2 - 1$	$2^3 \cdot 3$	$2^2 \cdot 3 \cdot 5$
$(7, \sigma + 3)$	$2\sigma - 1$	$2^3 \cdot 3$	$2^2 \cdot 3 \cdot 5$

$|(\mathbb{F}_5[G_3])^{\star +}| = 2^4$, $|(\mathbb{F}_{61}[G_3])^{\star +}| = 2^4 \cdot 3^2 \cdot 5^2$

c) $l = 1987$, $\frac{l-1}{2} = 3 \cdot 331$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{331}[G_3]$
$(7, \sigma + 5)$	$2\sigma^2 - 1$	$2 \cdot 5 \cdot 11$
$(7, \sigma + 3)$	$2\sigma - 1$	$2 \cdot 5 \cdot 11$

$|(\mathbb{F}_{331}[G_3])^{\star +}| = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11^2$

d) $l = 4339$, $\frac{l-1}{2} = 3^2 \cdot 241$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{241}[G_3]$
$(7, \sigma + 5)$	$2\sigma^2 - 1$	$2^4 \cdot 3 \cdot 5$
$(7, \sigma + 3)$	$2\sigma - 1$	$2^4 \cdot 3 \cdot 5$

$|(\mathbb{F}_{241}[G_3])^{\star +}| = 2^8 \cdot 3^2 \cdot 5^2$

e) $l = 5051$, $\frac{l-1}{2} = 5^2 \cdot 101$, $\delta^\star = 5$, $h_{K_5} = \tilde{h}_l^+ = 1451$

$X^{(5)} \subset \mathbb{Z}[G_5]$	η mit $X^{(5)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{101}[G_5]$
$(1451, \sigma + 906)$	$2\sigma^4 + 3\sigma^3 - \sigma^2 + \sigma - 4$	$2^2 \cdot 5^2$
$(1451, \sigma + 828)$	$-\sigma^4 + 3\sigma^3 + 2\sigma^2 - 4\sigma + 1$	$2^2 \cdot 5^2$
$(1451, \sigma + 739)$	$2\sigma^4 + \sigma^3 + 3\sigma^2 - 4\sigma - 1$	$2^2 \cdot 5^2$
$(1451, \sigma + 430)$	$-4\sigma^4 + 3\sigma^3 + \sigma^2 + 2\sigma - 1$	$2^2 \cdot 5^2$

$|(\mathbb{F}_{101}[G_5])^{\star +}| = 2^6 \cdot 5^6$

f) $l = 5119$, $\frac{l-1}{2} = 2 \cdot 3 \cdot 853$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 31$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{853}[G_3]$
$(31, \sigma + 26)$	$-\sigma^2 - 2\sigma + 4$	$2^2 \cdot 3 \cdot 71$
$(31, \sigma + 6)$	$-\sigma^2 + 4\sigma - 2$	$2^2 \cdot 3 \cdot 71$

$|(\mathbb{F}_{853}[G_3])^{\star +}| = 2^4 \cdot 3^2 \cdot 71^2$

g) $l = 8287$, $\frac{l-1}{2} = 3 \cdot 1381$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 7$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{1381}[G_3]$
$(7, \sigma + 5)$	$2\sigma^2 - 1$	$3 \cdot 5 \cdot 23$
$(7, \sigma + 3)$	$2\sigma - 1$	$3 \cdot 5 \cdot 23$

$|(\mathbb{F}_{1381}[G_3])^{\star +}| = 2^4 \cdot 3^2 \cdot 5^2 \cdot 23^2$

h) $l = 9127$, $\frac{l-1}{2} = 3^3 \cdot 13^2$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 31$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	$\mathrm{ord}(\eta)$ in $\mathbb{F}_{13}[G_3]$
$(31, \sigma + 26)$	$-\sigma^2 - 2\sigma + 4$	$2^2 \cdot 3$
$(31, \sigma + 6)$	$-\sigma^2 + 4\sigma - 2$	2^2

$|(\mathbb{F}_{13}[G_3])^{\star +}| = 2^4 \cdot 3^2$

i) $l = 9551$, $\frac{l-1}{2} = 5^2 \cdot 191$, $\delta^\star = 5$, $h_{K_5} = \tilde{h}_l^+ = 541$

$X^{(5)} \subset \mathbb{Z}[G_5]$	η mit $X^{(5)} = (\eta)$	ord(η) in $\mathbb{F}_{191}[G_5]$
$(541, \sigma + 493)$	$\sigma^3 - 3\sigma + 1$	$2 \cdot 5 \cdot 19$
$(541, \sigma + 417)$	$-3\sigma^3 + 4\sigma^2 - 4\sigma + 4$	$2 \cdot 5 \cdot 19$
$(541, \sigma + 401)$	$\sigma^2 + 3\sigma - 3$	$2 \cdot 5 \cdot 19$
$(541, \sigma + 313)$	$-3\sigma^2 + 3\sigma + 1$	$2 \cdot 5 \cdot 19$

$|(\mathbb{F}_{191}[G_5])^{\star +}| = 2^3 \cdot 5^3 \cdot 19^3$

j) $l = 9907$, $\frac{l-1}{2} = 3 \cdot 13 \cdot 127$, $\delta^\star = 3$, $h_{K_3} = \tilde{h}_l^+ = 31$

$X^{(3)} \subset \mathbb{Z}[G_3]$	η mit $X^{(3)} = (\eta)$	ord(η) in $\mathbb{F}_{13}[G_3]$	ord(η) in $\mathbb{F}_{127}[G_3]$
$(31, \sigma + 26)$	$-\sigma^2 - 2\sigma + 4$	$2^2 \cdot 3$	$3^2 \cdot 7$
$(31, \sigma + 6)$	$-\sigma^2 + 4\sigma - 2$	2^2	$3^2 \cdot 7$

$|(\mathbb{F}_{13}[G_3])^{\star +}| = 2^4 \cdot 3^2$, $|(\mathbb{F}_{127}[G_3])^{\star +}| = 2^2 \cdot 3^4 \cdot 7^2$

Anhang D

PARI/GP-Skripte zur $\mathbb{Z}[G]$-Freiheit

Wir verwenden den Datenbestand und einige Funktionen aus Anhang B. Insbesondere sind die zu betrachtenden Fälle durch die Liste ClassNumber_OrderG_Coprime_3mod4 gegeben. Abkürzend wird dieser Liste ein neuer Name, UlProjective, gegeben. Einige probabilistische Funktionen nutzen eine zusätzliche Eingabevariable namens *coeffBound*, die eine Schranke für die Größe der zufällig gewählten Werte angibt. In der Anwendung werden hierfür ganze Zahlen zwischen 2 und 20 gewählt.

```
UlProjective = ClassNumber_OrderG_Coprime_3mod4;
```

Zur Erinnerung: PrimeList enthält die zugehörigen Primzahlen l und Degrees die Grade der Unterkörper von $\mathbb{Q}(\zeta_l)^+$, bei denen die Klassenzahlen aus ClassNumbers auftreten. ClassNumbersSimple enthält jeweils die vermuteten Klassenzahlen.

Folgerung 8

Hier wird berechnet, wie das Ideal (79) in $\mathcal{O}_{\mathbb{Q}(\zeta_{39})}$ bzw. das Ideal (131) in $\mathcal{O}_{\mathbb{Q}(\zeta_{65})}$ zerfällt. Danach wird geprüft, ob die in der Zerlegung auftretenden Primideale Hauptideale sind. Dazu wird bnfisprincipal auf jeden Idealfaktor angewendet und der erste Teil des Ergebnisvektors ausgegeben. Ein Ideal ist genau dann ein Hauptideal, wenn dieser Teil dem Nullvektor entspricht. Bei den Berechnungen wird mehr Arbeitsspeicher und eine größere Präzision benötigt.

```
allocatemem(512000000);
\p100;

{folgerung8_1()=
  local(K39,facs79,i,tmp);
  K39 = bnfinit(polcyclo(39));
  facs79 = idealfactor(K39,79);
  for(i=1, length(facs79~),
    tmp = bnfisprincipal(K39,facs79[i,1]);
    print(tmp[1]);
    );
  }
```

```
{folgerung8_2()=
  local(K65,facs131,i,tmp);
  K65 = bnfinit(polcyclo(65));
  facs131 = idealfactor(K65,131);
  for(i=1, length(facs131~),
    tmp = bnfisprincipal(K65,facs131[i,1]);
          print(tmp[1]);
    );
  }
```

Folgerung 9

Die Funktion folgerung9 verwendet die Hilfsfunktion isFreeBy4_7, um zu testen, für welche Primzahlen l die Voraussetzungen von Satz 4.29 erfüllt sind. Die entsprechenden Indizes werden in die Liste UlFree geschrieben, die anderen in die Liste UlProjective_2.

```
UlFree = listcreate(length(UlProjective));
UlProjective_2 = listcreate(length(UlProjective));


{folgerung9() =
  local(i,degree);
  for(i=1,length(UlProjective),
    degree=Degrees[UlProjective[i]];
    if(!(length(degree)==1),
      listput(UlProjective_2,UlProjective[i])
      ,
      if(isFreeBy4_7(PrimeList[UlProjective[i]],degree,ClassNumbersSimple[UlProjective[i
          ]]),
        listput(UlFree,UlProjective[i]),
        listput(UlProjective_2,UlProjective[i])
        );
      );
    );
  }
```

Die Routine isFreeBy4_7 testet, ob die l-Einheiten modulo Torsion, $\overline{U}_l$, mit gegebenem $delta = \delta^\star$ und gegebener Klassenzahl $h = \tilde{h}_l^+$ nach Satz 4.29 $\mathbb{Z}[G]$-frei sind.

```
{isFreeBy4_7(l, delta, h)=
    local(factorsH, factorsPhi);
    if(l%4==3,
      factorsH=factor(h);
      if((delta>2) && isprime(delta) && (factorsH[1,2]%(delta-1)==0) && (length(factorsH
          ~)==1) && (factorsH[1,1]==2),
        factorsPhi = factor(Mod(1,2)*(x^delta-1)/(x-1));
        if(length(factorsPhi~)==1,
```

```
          return (1);
          );
          ,
          return (0);
        );
      ,
      return (0);
      );
  }
```

Die zur Index-Liste UlFree gehörende Liste von Primzahlen l, für die $\overline{U}_l$ nach Abschnitt 4.7 $\mathbb{Z}[G]$-frei ist, erhält man beispielsweise durch die Eingabe von listList(PrimeList,UlFree).

Betrachtung der restlichen Fälle, in denen $\tilde{h}_l^+$ eine Primzahlpotenz ist

Die Funktion apply4_8A gibt für Eingaben einer Primzahl p, einer dazu teilerfremden positiven, ganzen Zahl $delta = \delta$ und der (Klassen-)Zahl h aus, ob nach dem Verfahren von Abschnitt 4.8 die möglichen Ideale $X^{(p\delta)} \subset \mathbb{Z}[G_{p\delta}]$ mit $|\mathbb{Z}[G_{p\delta}]/X| = h$ und $|\mathbb{Z}[G_\delta]/X^{(\delta)}| = h$ frei sind über $\mathbb{Z}[G_{p\delta}]$ oder nicht. Das Durchlaufen mit den in Satz 4.33 angegebenen Werten liefert die in Anhang C angegebenen Ergebnisse und damit den numerischen Teil des Beweises von Satz 4.33.

```
{apply4_8A(h,delta,q,coeffBound) =
  local(i,j,k,factorsH,p,expo,factorsPol,poldeg,genListX,possibleX,genX,orderGenX,
        orderGenXfacs,orderPP,numNotFree);
  \\ Abbrechen, falls ggT(delta,p) nicht 1 ist.
  if(!(gcd(delta,q)==1), print("q und delta sind nicht teilerfremd."); return(0););
  \\ Abbrechen, falls q nicht prim ist.
  if(!isprime(q), print("q ist nicht prim."); return(0););
  \\ Faktorisierung der Klassenzahl und testen, ob diese eine Primzahlpotenz ist.
  factorsH=factor(h);
  if(!(length(factorsH~)==1),print("h ist keine Primzahlpotenz");return (0););
  p=factorsH[1,1];
  expo=factorsH[1,2];
  \\ Berechnen der Faktoren des delta-ten Kreisteilunspolynoms
  factorsPol=factorpadic(polcyclo(delta),p,1);
  poldeg = poldegree(factorsPol[1,1]);
  \\ Berechnen der in Frage kommenden Erzeugendensystemen von X.
  possibleX = getAllComb(length(factorsPol~),expo/poldeg);
  print("=================================");
  print("Test in Z[G_"delta"*"q"]");
  print("=================================");
  \\ Testen aller verschiedener X auf Nicht-Freiheit.
  numNotFree = 0;
  for(i=1, length(possibleX),
    \\ Erzeugerliste von X
    genListX=getGenList(p,delta,possibleX[i]);
    print("  ");
    print("Teste X = "genListX);
    \\ Suchen eines einzelnen Erzeugers von X.
    genX = lift(cyclicIdealSearch2(genListX,delta,h,coeffBound));
    print("Erzeuger gefunden: X = ("genX")");
    \\ Berechnung der Ordnung des Erzeugers von X in F_qG_delta
    orderGenX = orderPM(q,delta,genX);
    \\ Berechnung der Ordnung des Plusteils der Einheiten von F_qG_delta
    orderPP = orderPlusPart(q,delta);
    print("Ordnung von "genX" in F_"q"G_"delta" : "orderGenX " = "factor(orderGenX));
    print("Ordnund des Plusteils : "orderPP" = "factor(orderPP));
    orderGenXfacs=factor(orderGenX);
    for(k=1,length(orderGenXfacs~),
      \\ Wenn die Ordnung des Erzeugers von X in F_qG_delta einen Primfaktor ungleich 2
          hat, der,
```

```
      \\ falls er Teiler von delta ist, in ord(genX) haeufiger als in delta auftritt und
          zudem
      \\ kein Teiler des Plusteils der Einheiten von F_qG_delta ist, so kann X nicht
          frei sein.
       if(!(orderGenXfacs[k,1]==2)&&
        !(gcd(orderGenXfacs[k,1]^orderGenXfacs[k,2],delta)==orderGenXfacs[k,1]^
            orderGenXfacs[k,2])&&
        !(orderPP%orderGenXfacs[k,1]==0),

        print("X nicht Z[G_"delta"*"q"]-frei: Faktor "orderGenXfacs[k,1]);
        numNotFree=numNotFree+1;
        break;
        );
       );
    );
  if(numNotFree==length(possibleX),
    print(" ");
    print("X ist in allen moeglichen Faellen nicht Z[G_"delta"*"q"]-frei.");,
    print("Kein eindeutiges Ergebnis.");
    );
  }
```

Die folgende Funktion verwendet die vorherige Funktion apply4_8A. Hier sind die Voraussetzungen wie folgt: $h_l^+ = p^{expo}$ sei eine Primzahlpotenz und $h_{K_\delta} = h_l^+$. Weiter sei die Klassenzahl aller echten Unterkörper von K_δ eins.

```
{apply4_8B(l,h,delta,coeffBound)=
  local(i,factorsLm1,primefactorsLm1);
  \\ Testen, ob l prim ist.
  if(isprime(l)==0, print("l nicht prim"); return (0););
  \\ Testen, ob die l-Einheiten mod Torsion Z[G]-projektiv sind.
  if(!(l%4==3), print("Die l-Einheiten mod Torsion sind nicht Z[G]-projektiv"); return
      (0););
  \\ Durchlaufe apply4_8A f"ur  alle zu delta teilerfremden Primteiler q von (l-1)/2.
  \\ Erstelle Listen mit den Faktoren von (l-1)/2.
  factorsLm1 = factor((l-1)/2);
  primefactorsLm1 = listcreate(length(factorsLm1~));
  for(i=1,length(factorsLm1~),
    listput(primefactorsLm1,
      factorsLm1[i,1])
    );
  for(i=1,length(primefactorsLm1),
    if(gcd(primefactorsLm1[i],delta)==1,
      apply4_8A(h,delta,primefactorsLm1[i],coeffBound);
      );
    );
  }
```

Hilfsfunktionen für die beiden vorhergehenden Funktionen

Die Funktion getGenList erstellt aus einer Liste $[a_1, \ldots, a_s]$ von nichtnegativen ganzen Zahlen eine Liste von Erzeugern des Ideals X, dessen p-Lokalisierung $p^{a_1}\mathbb{Z}_p[x]/(\varphi_1(x)) \times \ldots \times p^{a_s}\mathbb{Z}_p[x]/(\varphi_s(x))$ ist und dessen Lokalisierungen bezüglich aller Primzahlen $t \neq p$ trivial ist. Die Polynome $\varphi_1(x), \ldots, \varphi_s(x)$ und die auftretende Potenz werden durch Faktorisierung des delta-ten Kreisteilungspolynoms über den p-adischen Zahlen berechnet.

```
{getGenList(p,delta,coeffList)=
  local(i,j,maxCoeff,polList,actGen,genList);
  maxCoeff=listMax(coeffList);
  genList=listcreate(maxCoeff+1);
  \\ p^maxCoeff wird als Erzeuger in das System aufgenommen.
  \\ Damit wird u.a. sichergestellt, dass das bezueglich jeder anderen
```

```
  \\ Primzahl lokalisierte Ideal trivial ist.
  listput(genList,p^maxCoeff);
  \\ polList enthaelt die Faktorisierung des delta-ten Kreisteilungspolynoms
  \\ bis zu einer Genauigkeit von maxCoeff.
  polList = factorpadic(polcyclo(delta),p,maxCoeff);
  \\ Treten alle moeglichen Faktoren mit dem gleichen Exponenten auf,
  \\ muss nur noch das Produkt dieser Faktoren hinzugefuegt werden.
  actGen=1;
  for(j=1,length(coeffList),
    if(!(coeffList[j]==0),
      actGen = actGen*lift(polList[j,1]);
      );
    );
  listput(genList,actGen);
  for(i=1,maxCoeff-1,
    actGen=p^i;
    if(isElement(i,coeffList),
      for(j=1,length(coeffList),
        if(!(coeffList[j]<=i),
          actGen = actGen*lift(polList[j,1]);
          );
        );
      listput(genList,actGen);
      );
    );
  return (genList);
  }
```

Die Funktion getAllComb liefert alle Listen der Länge vecLength mit nichtnegativen ganzzahligen Einträgen, deren Einträge aufsummiert vecSum ergeben.

```
{getAllComb(vecLength,vecSum) =
  local(i,singleComb,combinations);
  combinations=listcreate(vecLength^vecSum);
  for(i=0,(vecSum+1)^(vecLength+1)-1,
    singleComb = getMRepOf(vecSum+1,i,vecLength);
    if(listSum(singleComb)==vecSum,
      listput(combinations,singleComb);
      );
    );
  return (combinations);
  }
```

Die Hilfsfunktion getMRepOf liefert eine Liste mit den Koeffizienten von num zur Basis base, wobei die Liste genau maxlength Elemente hat. Der Wert von num darf also maximal $base^{(maxlength)} - 1$ sein.

```
{getMRepOf(base,num,maxlength)=
  local(i,repList);
  repList=listcreate(maxlength);
  for(i=1,maxlength,
    listput(repList,floor(num/(base^(maxlength-i))));
    num = num - repList[i]*base^(maxlength-i);
    );
  return (repList);
  }
```

Die Hilfsfunktion listSum liefert die Summe der Elemente einer Liste inpList.

```
{listSum(inpList) =
  local(i,ret);
  ret=0;
  for(i=1,length(inpList),
    ret=ret+inpList[i];
    );
  return (ret);
  }
```

Analog zu listSum liefert listMax den größten Eintrag einer Liste inpList nichtnegativer Zahlen.

```
{listMax(inpList)=
  local(i, retMax);
  retMax=0;
  for(i=1,length(inpList),
    retMax=max(retMax,inpList[i]);
    );
  return (retMax);
  }
```

Bestimmung eines Erzeugers des zu $\overline{U}_l^{(\delta)}$ gehörenden Ideals $X^{(\delta)}$

Sei G_m eine zyklische Gruppe der Ordnung m und $X \subseteq \mathbb{Z}[G_m]$ ein Ideal, das von den Elementen aus listOfGenerators erzeugt wird. Weiter sei $|\mathbb{Z}[G_m]/X| = indexX$. Die folgende Funktion versucht, einen Hauptidealerzeuger η von X zu finden, indem zufällige $\mathbb{Z}[G_m]$-Linearkombinationen der Elemente von listOfGenerators erzeugt werden und dann deren Norm auf Gleichheit mit $indexX$ getestet wird.

```
{cyclicIdealSearch(listOfGenerators,m,indexX,coeffBound) =
  local(i,j,listOfRandomElements, gen);
  while(!(norm(gen)==indexX),
    listOfRandomElements = listcreate(length(listOfGenerators));
    gen = Mod(0,x^m-1);
    for(i=1,length(listOfGenerators),
      listput(listOfRandomElements,0);
      );
    for(i=1,length(listOfRandomElements),
      for(j=0,m-1,
        listOfRandomElements[i] = listOfRandomElements[i] + x^j*(coeffBound - random(2*
            coeffBound));
        );
      );
    for(i=1,length(listOfRandomElements),
      gen = gen + Mod(listOfRandomElements[i]*listOfGenerators[i], x^m-1);
      );
    );
  return (gen);
  }
```

Alternativ kann auch die folgende Funktion verwendet werden. Dazu werden zufällig erzeugte Elemente $gen \in \mathbb{Z}[G_m]$ getestet, ob sie $norm(gen) = indexX$ erfüllen und, ob zudem das von gen erzeugte Ideal mit dem von listOfGenerators erzeugten Ideal übereinstimmt. Der Nachteil dieser Funktion ist der zusätzliche Test, ob $(gen) = (listOfGenerators)$ gilt; in der Praxis ist diese Methode trotzdem oft effizienter als die erste Variante und wird deshalb in apply4_8A verwendet.

```
{cyclicIdealSearch2(listOfGenerators,m,indexX,coeffBound) =
  local(gen);
  gen=1;
  while(!(isGeneratorOf(gen,listOfGenerators,m,indexX)),
    gen = getCyclicIdealGen(m,indexX,coeffBound);
    );
  return (gen);
  }
```

Die Hilfsfunktion isGeneratorOf liefert 1, wenn die Ideale (gen) und $X = (listOfGenerators)$ von $\mathbb{Z}[G_m]$ übereinstimmen. Dazu wird getestet, ob die Norm von gen gleich dem (vorgegebenen) Index von X in $\mathbb{Z}[G_m]$ ist und, ob alle Elemente von listOfGenerators in (gen) liegen.

```
{isGeneratorOf(gen,listOfGenerators,m,indexX)=
  local(a,i,j);
  if(norm(gen)==indexX,
    for(i=1,length(listOfGenerators),
      a=lift(listOfGenerators[i]/gen);
      for(j=0,length(a)-1,
        if(!(floor(polcoeff(a,j))==polcoeff(a,j)), return (0););
        );
      );
    return (1);
    ,
    return (0);
    );
  }
```

Die Hilfsunktion getCyclicIdealGen testet zufällig gewählte Elemente $gen \in \mathbb{Z}[G_m]$, ob sie ein Ideal mit gewünschtem Index $indexX$ erzeugen. Sobald ein derartiges Element gefunden ist, wird dieses ausgegeben.

```
{getCyclicIdealGen(m, indexX, coeffBound) =

  local(gen,i);
  gen = 0;
  while(!(norm(gen)==indexX),
    gen=0;
    for(i=0,m-1,
      gen = gen + x^i*(coeffBound - random(2*coeffBound));
      );
    gen = Mod(gen, x^m-1);
    );
  return (gen);
  }
```

Berechnung der Ordnung eines Elements aus $\mathbb{F}_p[x]/(x^m - 1)$

Eingabewerte der Funktion orderPM sind eine Primzahl p, eine ganze Zahl $m \geq 2$ und ein Element $elem \in \mathbb{Z}[x]$. Sei $elemF$ das aus $elem$ durch die kanonische Surjektion $\mathbb{Z}[x] \to \mathbb{F}_p[x]/(x^m - 1)$ erhaltene Element. Dieses wird auf Invertierbarkeit überprüft. Ist elemF invertierbar, so wird die Ordnung von $elemF$ ausgegeben, sonst 0.

```
{orderPM(p,m,elem)=
  local(i,orderUnitGroup, factorsOrderUnitGroup, elemF, exponent);
  orderUnitGroup = orderUnitsFPXM(p,m);
  factorsOrderUnitGroup = factor(orderUnitGroup);
  eins = Mod(Mod(1,p),Mod(1,p)*(x^m-1));
  elemF = Mod(Mod(1,p)*elem,Mod(1,p)*(x^m-1));
  \\ Teste, ob elemF invertierbar ist.
  if(!(elemF^orderUnitGroup==eins), return (0););
  \\ Ist elemF invertierbar, wird die Ordnung von elemF berechnet.
  exponent = orderUnitGroup;
  \\ Teste, wie oft jeder Faktor der Gruppenordnung die Ordnung von elemF teilt.
  for(i=1,length(factorsOrderUnitGroup~),
    for(j=1,factorsOrderUnitGroup[i,2],
```

```
      exponent=exponent/factorsOrderUnitGroup[i,1];
      if(!(elemF^exponent==eins), exponent=exponent*factorsOrderUnitGroup[i,1]; break);
      );
    );
  return(exponent);
  }
```

Berechnung der Ordnung des Plusteils $(\mathbb{F}_p[x]/(x^m-1))^{\star+}$

Die Funktion orderPlusPart bestimmt für die Eingabewerte p und m, wobei p eine Primzahl ist und $m \geq 2$ eine ganze Zahl, die Mächtigkeit von $(\mathbb{F}_p[x]/(x^m-1))^{\star+}$. Dazu werden die Äquivalenzklassen von $\mathbb{Z}/m\mathbb{Z}$ bezüglich der in Abschnitt 4.8 definierten Äquivalenzrelation $\sim_p$ berechnet. Dann wird geprüft, ob mit jedem (einem) a auch $-a$ in der selben Äquivalenzklasse liegt. Ist $H = \{a_1, \ldots, a_r\}$ diese Äquivalenzklasse und ζ eine primitive m-te Einheitswurzel in einer Erweiterung von $\mathbb{F}_p$, so agiert die Involution $\bar{\iota}$ in diesem Fall auf $\mathbb{F}_p[x]/(\phi_H(x))$, wobei $\phi_H(x) = (x-\zeta^{a_1})\cdot\ldots\cdot(x-\zeta^{a_r})$ ist. Andernfalls agiert $\bar{\iota}$ durch Vertauschen.

```
{orderPlusPart(p,m)=
  local(i,elementList,aeqKlassen,actNK,orderPP);
  \\ Erzeugen einer Liste der Elemente von Z/mZ ohne die 0.
  elementList=listcreate(m);
  for(i=1,m-1,
    listput(elementList, Mod(i,m));
    );
  \\ Berechnung der verschiedenen Aequivalenzklassen bzgl. \sim_p von Z/mZ bis auf [0]
  aeqKlassen = listcreate(m);
  while(!(length(elementList)==0),
    actNK=getNK(elementList[1],p,m);
    listput(aeqKlassen,actNK);
    elementList = deleteFromList(actNK,elementList);
    );
  \\ Ueberpruefung der Aequivalenzklassen und Berechnung der Ordnung des Plusteils
  orderPP = p-1;
  for(i=1,length(aeqKlassen),
    if(containsAddInv(aeqKlassen[i]),
      \\ Aequivalenzklasse enthaelt die additiv Inversen.
       orderPP = orderPP*(p^(length(aeqKlassen[i])/2)-1)
      ,
      \\ Aequivalenzklasse enthaelt die additiv Inversen nicht.
      orderPP = orderPP*((p^(length(aeqKlassen[i])))-1)^(1/2));
      );
    );
  return (round(orderPP));
  }
```

Die Hilfsfunktion orderUnitsFPXM berechnet die Mächtigkeit der Menge $(\mathbb{F}_p[x]/(x^m-1))^{\star}$.

```
{orderUnitsFPXM(p,m) =
  local(i, polFactors, ret);
  polFactors = factor(Mod(1,p)*(x^m-1));
  ret = 1;
  for(i=1,length(polFactors~),
    ret = ret*((p^(poldegree(polFactors[i,1])))-1)^polFactors[i,2]);
    );
  return (ret);
  }
```

Die Hilfsfunktion getNK gibt die Äquivalenzklasse $a\langle p\rangle$ für $a \in \mathbb{Z}/m\mathbb{Z}$ aus.

```
{getNK(a,p,m) =
  local(retList,tmp);
  retList=listcreate(znorder(Mod(p,m)));
  tmp = a*Mod(p,m);
  listput(retList,tmp);
  while(!(tmp==a),
    tmp = tmp*Mod(p,m);
    listput(retList,tmp);
    );
  return (retList);
  }
```

Die Hilfsfunktion deleteFromList(elementsToDelete, list) streicht aus der Liste list alle Elemente, die auch in der Liste elementsToDelete gespeichert sind und gibt die verkürzte Liste zurück. Es wird die in Anhang B verwendete Funktion isElement verwendet.

```
{deleteFromList(elementsToDelete, list) =
  local(i,retList);
  retList=listcreate(length(list));
  for(i=1,length(list),
    if(!(isElement(list[i],elementsToDelete)),
      listput(retList, list[i]);
      );
    );
  return (retList);
}
```

Die Funktion containsAddInv(list) überprüft nach Eingabe einer Liste list mit Elementen aus $\mathbb{Z}/m\mathbb{Z}$, ob neben list[1] auch -list[1] in der Liste enthalten ist.

```
{containsAddInv(list) =
  local(i);
  for(i=1,length(list),
    if((-list[i])==list[1],
      return (1);
      );
    );
  return (0);}
```

Berechnung aller Primzahlen $l < 500000$ mit $h_{K_7} = 8$ und $h_{K_5} = 1$ beziehungsweise $h_{K_5} = 11$ und $h_{K_7} = 1$

Die Funktion findCandidates(m1,m2,h,p1,p2) liefert eine Liste aller Primzahlen $m1 < l < m2$, sodass $l \equiv 3 \mod 4$, $(p1 \cdot p2) \mid \frac{l-1}{2}$, $h_{K_{p1}} = h$ und $h_{K_{p2}} = 1$. Dabei sind p1 und p2 Primzahlen und wie zuvor bezeichnet K_t den Unterkörper von $\mathbb{Q}(\zeta_l)$ mit $[K_t : \mathbb{Q}] = t$. Wir verwenden die Funktion subcyclo aus Anhang B. Für die Berechnungen wird mehr Arbeitsspeicher und eine größere Rechengenauigkeit benötigt.

```
allocatemem(512000000);
\p100

{findCandidates(m1,m2,h,p1,p2)=
  local(i,j,l,listOfPrimes, listOfPrimesHp1, subfieldList, clgp, candidateList);
  \\ Zu Beginn wird eine Liste aller Primzahlen l<m mit l== 3 mod 4 und (p1*p2)|((l-1)
      /2) erstellt,
  listOfPrimes = listcreate(ceil((1.0*m2-m1)/2));
  for(i=ceil((1.0*m1-1)/(2*p1*p2)),floor((1.0*m2-1)/(2*p1*p2)),
    l=i*2*p1*p2+1;
    if((l%4==3)&&(isprime(l)),
      listput(listOfPrimes,l);
      );
    );
  \\ Aus obiger Liste werden nun diejenigen Primzahlen l bestimmt, fuer
  \\ die h_{K_{p1}} = h ist.
  listOfPrimesHp1 = listcreate(length(listOfPrimes));
  for(i=1,length(listOfPrimes),
    subfieldList=subcyclo(listOfPrimes[i],p1);
    for(j=1,length(subfieldList),
      if(poldegree(subfieldList[j])==p1,
        clgp=bnfclgp(subfieldList[j]);
        print("F r l = "listOfPrimes[i]": Klassengruppe = "clgp);
        if(clgp[1]==h,
          listput(listOfPrimesHp1,listOfPrimes[i]);
          );
        );
      );
    );
  \\ Im letzten Schritt wird bei den verbleibenden Primzahlen getestet, ob die
      Klassenzahl von
  \\ h_{K_{p2}} = 1 ist. In diesem Fall wird die entsprechende Primzahl in die
      Kandidatenliste
  \\ eingetragen.
  candidateList = listcreate(length(listOfPrimesHp1));
  for(i=1,length(listOfPrimesHp1),
    subfieldList=subcyclo(listOfPrimesHp1[i],(p2));
    for(j=1,length(subfieldList),
      if(poldegree(subfieldList[j])==p2,
        clgp=bnfclgp(subfieldList[j]);
        print("F r l = "listOfPrimesHp1[i]": Klassengruppe = "clgp);
        if(clgp[1]==1,
          listput(candidateList,listOfPrimesHp1[i]);
          );
        );
      );
    );
  \\ Ausgabe der Kandidatenliste
  print(candidateList);
  }
```

Literaturverzeichnis

[AM69] M.Atiyah, I. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[BIV89] R. Brüske, F. Ischebeck, F. Vogel, *Kommutative Algebra*, BI Wissenschaftsverlag, 1989.

[Br83] J. Brinkhuis, *Normal integral bases and embedding problems*, Math. Annalen **264** (1983), 537-543.

[Br87] J. Brinkhuis, *Normal integral bases and complex conjugation*, J. reine angew. Math. **375/376** (1987), 157-166.

[Br92] J. Brinkhuis, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), 333-347.

[Brw82] K.S. Brown, *Cohomology of Groups*, GTM 87, Springer, 1982.

[Chi83] T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Inventiones math. **74** (1983), 321-349.

[Chi84] T. Chinburg, *Multiplicative Galois structure*, Lecture Notes in Mathematics **1068**, 23-32, Springer, 1984.

[Cob55] A.P. Cobbe, *On the cohomology groups of a finite group*, Quart. J. Math. Oxford (1955), 34-47.

[Coh96] H. Cohen, *A Course in Computational Algebraic Number Theory*, 3rd edition, GTM 138, Springer, 1996.

[CR81] C.W. Curtis, I. Reiner, *Methods of Representation Theory Vol.I*, John Wiley & Sons, 1981.

[CR06] C.W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, 1988.

[Dub00] I. Dubois, *S-unités et S-groupe de classes d'un corps de nombres cyclique de degré premier*, J. Number Theory **85** (2000), 35 - 58.

[Fr83] A. Fröhlich, *Galois module structure of algebraic integers*, Springer, 1983.

[Fr89] A. Fröhlich, *L-values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure)*, J. reine angew. Math. **397** (1989), 42-99.

[Fr92] A. Fröhlich, *Units in real Abelian fieldsr*, J. reine angew. Math. **429** (1992), 191-217.

[GKPS] D. Geller, I. Kra, S. Popescu, S. Simanca, *On circulant matrices*, Preprint, http://www.math.sunysb.edu/ sorin/eprints/circulant.pdf

[GRRS99] C. Greither, D.R. Reploge, K. Rubin, A. Srivastav, *Swan Modules and Hilbert-Speiser number fields*, J. Number Theory **79** (1999), 164-173.

[Gr07] P.A. Grillet, *Abstract Algebra*, 2. Auflage, Springer, 2007.

[Hoe92] K. Hoechsmann, *Constructing units in commutative group rings.* Manuscripta Math. **75** (1992), 5-23.

[Ha52] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*. Berlin 1952.

[Hak07] T. Hakkarainen, *On the computation of the class numbers of real abelian fields*. TUCS Dissertations No. **87**, 2007.

[Ju93] D. Jungnickel, *Finite Fields*, B.I. Wissenschaftsverlag, 1993.

[Lam98] T.Y. Lam, *Lectures on Modules and Rings*, GTM 189, Springer, 1998.

[Mar96] F. Marko, *On the existence of p-units and Minkowski units in totally real cyclic fields*, Abh. Math. Sem. Univ. Hamburg **66 (1)**, 1996.

[Mar05] F. Marko, *On the existence of Minkowski units in totally real cyclic fields*, Journal de Théorie des nombres Bordeaux **17** (2005), 195-206.

[Mas78] J.M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Mathematica **37**, No. 3, 1978, 297-319.

[Mil08] J.S. Milne, *Class Field Theory (v.4.00)*, www.jmilne.org/math/, 2008.

[Mil08b] J.S. Milne, *Algebraic Number Theory (v3.00)*, www.jmilne.org/math/, 2008.

[Mln71] J. Milnor, *Introduction to algebraic K-Theory*, Princeton University Press, 1971.

[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer, 3rd edition, 2004.

[Neu92] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.

[Od75] A. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Inventiones math. **29** (1975), 275-286.

[Od76] A. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. **29** (1976), 275-297.

[Od77] A. Odlyzko, *Lower bounds for discriminants of number fields II*, Tohoku Math. J. **29** (1977), 209-216.

[PARI] PARI/GP, version `2.3.4`, Bordeaux, 2008, http://pari.math.u-bordeaux.fr/.

[Rup95] W.M. Ruppert, *Kommutative Algebra II*, Vorlesungskript, http://www.mathematik.uni-erlangen.de/ ruppert/skripten.html, 1995.

[SchSt80] G. Scheja, U. Storch, *Lehrbuch der Algebra, Teil 1*, B.G. Teubner, 1980.

[Sch03] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), 913-937.

[Sil81] J.R. Silvester, *Introduction to Algebraic K-Theory*, Chapman and Hall, 1981.

[vdL82] F. J. van der Linden, *Class number computations of real abelian fields*, Math. Comp. **39** (1982), 693-707.

[Wa97] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, GTM 83, Springer, 1997.

[Wei96] A. Weiss, *Multiplicative Galois module structure*, Fields Institute monographs, American Mathematical Society, 1996.