Nadja Zimmermann

Die Normeinsgruppen biquadratischer Zahlkörpererweiterungen

2006

Die Normeinsgruppen biquadratischer Zahlkörpererweiterungen

Inaugural-Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften im Fachbereich
Mathematik und Informatik
der Mathematisch-Naturwissenschaftlichen Fakultät
der Westfälischen Wilhelms-Universität Münster

vorgelegt von

Nadja Zimmermann
aus Bonn
- 2006 -

unter der Betreuung von
Prof. Dr. Falko Lorenz

am
mathematischen Institut
der Westfälischen Wilhelms-Universität Münster
Einsteinstraße 62, D-48149 Münster

Dekan:	Prof. Dr. Klaus Hinrichs
Erster Gutachter:	Prof. Dr. Falko Lorenz
Zweiter Gutachter:	Prof. Dr. Franz Lemmermeyer
Tag der mündlichen Prüfung:	04.07.2006
Tag der Promotion:	04.07.2006

Inhaltsverzeichnis Seite

Einleitung

Für eine galoissche Erweiterung K/k endlichen Grades gilt $H^{-1}(G, K^\times) = 1$, wenn die Galoisgruppe G der Erweiterung zyklisch ist. Dies besagt Satz 90 von Hilbert, der sich in Hilberts Zahlbericht von 1897 ([H]) befindet und in der Zahlentheorie eine bedeutsame Rolle spielt. Wie in einer Arbeit von F. Lorenz ([L]) thematisiert, bleibt diese Aussage für allgemeineres G nicht länger richtig. Ziel der vorliegenden Arbeit ist es nun, die Gruppe $H^{-1}(G, K^\times)$ insbesondere im Falle biquadratischer Erweiterungen algebraischer Zahlkörper genauer zu untersuchen. Einerseits werden wir mit elemenaren Methoden zeigen, dass $H^{-1}(G, K^\times)$ für gewisse biquadratische Erweiterungen von $\mathbb{Q}$ nicht-trivial ist (durch explizite Angabe von Cozyklen, die keine Coränder sind), andererseits werden wir $H^{-1}(G, K^\times)$ mit Hilfe der kohomologischen Fassung der Klassenkörpertheorie nach Tate für biquadratische Zahlkörpererweiterungen genau bestimmen.

Im Folgenden bezeichne K/k stets eine galoissche Körpererweiterung endlichen Grades, mit Galoisgruppe G. Für die Operation von G auf der multiplikativen Gruppe $K^\times$ des Körpers K (oder allgemeiner auf einem G-Modul A) sei in Exponentenschreibweise

$$a^\sigma := \sigma(a)$$

für $a \in K^\times$ und $\sigma \in G$. Die zugehörige Operation des ganzzahligen Gruppenringes $\mathbb{Z}G$ werde entsprechend notiert. Insbesondere ist also

$$a^{1-\sigma} = a/a^\sigma.$$

Die Erweiterung K/k heißt *zyklisch*, wenn ihre Galoisgruppe $G = G(K/k)$ zyklisch ist; bezeichnet dann σ einen Erzeuger von G, so präsentiert sich die Normabbildung $N = N_{K/k} : K^\times \to K^\times$ wie folgt:

$$N(z) = z^{1+\sigma+\sigma^2+\cdots+\sigma^{n-1}}$$

für $z \in K^\times$; dabei bezeichnet n die Ordnung von G (allgemeiner wird über alle Elemente einer endlichen Gruppe G summiert).

"Satz 90 von Hilbert". *Sei K/k zyklisch und σ ein Erzeuger von G. Für $z \in K^\times$ gelte $N_{K/k}(z) = 1$. Dann ist z darstellbar in der Form*

$$z = a^{1-\sigma}$$

mit einem $a \in K^\times$.

Dieser Satz lässt sich kürzer auch folgendermaßen formulieren.

"Satz 90 von Hilbert". *Für zyklisches K/k ist $H^{-1}(G, K^\times) = 1$.*

Dabei bezeichnet $H^{-1}(G, K^\times)$ die Tate-Kohomologie der endlichen Gruppe G mit Koeffizienten in der mulitiplikativen Gruppe $K^\times$ des Körpers K, mit der natürlichen Operation der Galoisgruppe G auf $K^\times$ (vgl. [AW], [B], [Ws] für Definition und Eigenschaften der Tate-Kohomologie). Für einen beliebigen G-Modul A bezeichne A^{1-G} die von den Elementen der Form $a^{1-\sigma}$ mit $\sigma \in G$ erzeugte Untergruppe von A. Wegen $N(a^\sigma) = N(a)$ gilt dann

$$A^{1-G} \subset \mathrm{Kern}(N)$$

und weiter

$$H^{-1}(G, A) = \mathrm{Kern}(N)/A^{1-G}$$

("Cozyklen modulo Coränder").

Eine Einführung in den Satz 90 von Hilbert, andere Formulierungen sowie Verallgemeinerungen finden sich in einem Artikel von F. Lorenz ([L]), der Grundlage und Ausgangspunkt der vorliegenden Arbeit ist. Insbesondere wird in diesem Artikel die Frage thematisiert, ob und inwieweit der Satz 90 von Hilbert für nicht-zyklische Gruppen richtig bleibt. Angeregt durch diese Fragestellung ist das zentrale Thema der vorliegenden Arbeit die Untersuchung der Gruppe $H^{-1}(G, K^\times)$ für biquadratische Erweiterungen von Zahlkörpern (d. h. mit Galoisgruppe $G \simeq (\mathbb{Z}/2)^2$). Im lokalen Fall, also für Erweiterungen lokaler Körper, wird in [L] zumindest im nicht-dyadischen Fall (wenn die Charakteristik der Resklassenkörper von 2 verschieden ist) mit elementaren Methoden der algebraischen Zahlentheorie nachgewiesen, dass $H^{-1}(G, K^\times)$ für biquadratische Erweiterungen lokaler Körper nicht-trivial ist. Im globalen Fall, und genauer gesagt im Fall algebraischer Zahlkörper, wird dies dann unter Heranziehung der kohomologischen Fassung der Klassenkörpertheorie nach Tate gezeigt ([L, S. 356]). Eine der Zielsetzungen der vorliegenden Arbeit war es, im Falle von Erweiterungen algebraischer Zahlkörper, also im globalen Fall, einen elementaren Beweis zu geben, dass $H^{-1}(G, K^\times)$ nicht-trivial ausfallen kann für nicht-zyklische Galoisgruppen G. Dies geschieht in Kapitel 1, wo für biquadratische Erweiterungen $K/\mathbb{Q}$ explizit Cozklen angegeben werden, die keine Coränder sind und daher nicht-triviale Elemente von $H^{-1}(G, K^\times)$ repräsentieren; in einigen Fällen gelingt es, die Gruppen $H^{-1}(G, K^\times)$ vollständig zu bestimmen (vgl. Kapitel 2).

Während im lokalen Fall $H^{-1}(G, K^\times)$ nur von der Gruppe G abhängt, wird in [L] gezeigt, dass dies im globalen Fall nicht länger richtig bleibt; dazu werden für Beispiele biquadratischer Erweiterungen algebraischer Zahlkörper mit Hilfe der kohomologischen Fassung der Klassenkörpertheorie nach Tate einige der Gruppen $H^{-1}(G, K^\times)$ bestimmt. In Kapitel 3 der vorliegenden Arbeit wird eine Charakterisierung der Gruppen $H^{-1}(G, K^\times)$ im Falle biquadratischer Erweiterungen algebraischer Zahlkörper gegeben; nach einigen Vorbereitungen wird dies in Kapitel 4 dann angewandt zur expliziten Bestimmung von $H^{-1}(G, K^\times)$ für biquadratische Erweiterungen $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ mit quadratfreien $a, b \in \mathbb{Z}$.

In Kapitel 3 wird folgendes Theorem bewiesen.

3.1 Theorem. *Sei K/k eine biquadratische Erweiterung algebraischer Zahlkörper, mit Galoisgruppe $G \simeq (\mathbb{Z}/2)^2$. Dann ist $H^{-1}(G, K^\times)$ bis auf Isomorphie vollständig bestimmt durch die Anzahl n der Stellen $\mathfrak{p}$ von k mit lokaler Galoisgruppe $G_\mathfrak{p} = G$. Genauer gilt für alle $n \geq 0$*

$$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{n-1},$$

wobei $(\mathbb{Z}/2)^{-1} = 0$ zu lesen ist im Falle $n = 0$. Jede Zahl $n \geq 0$ lässt sich für eine biquadratische Erweiterung $K/\mathbb{Q}$ realisieren.

Der Beweis von Theorem 3.1 erfolgt unter Heranziehung der kohomologischen Fassung der Klassenkörpertheorie nach Tate (in Kapitel 1 werden wir hingegen mit elementaren Methoden zeigen, dass $H^{-1}(G, K^\times)$ nicht-trivial ist für biquadratische Erweiterungen $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ in den Fällen mit $n \geq 2$ für a, b prim oder gleich -1).

Die eigentliche Schwierigkeit im Beweis von Theorem 3.1 stellt der Fall $n = 0$ dar. Ausgangspunkt der Betrachtungen ist die exakte Sequenz von G-Moduln

$$1 \to K^\times \to I_K \to C_K \to 1$$

mit der Idelgruppe I_K des Körpers K und der Idelklassengruppe C_K von K. Zu dieser kurzen exakten Sequanz von Koeffizientenmoduln gehört die lange exakte

Kohomologiesequenz

$$\to H^{i-1}(G, I_K) \to H^{i-1}(G, C_K) \to H^i(G, K^\times) \to H^i(G, I_K) \to H^i(G, C_K) \to$$

der Tate-Kohomologiegruppen der endlichen Gruppe G. Wie man mit Hilfe der kohomologischen Fassung der Klassenkörpertheorie nach Tate zeigen kann, zerfällt diese für $n > 0$ in die kurzen exakten Sequenzen

$$1 \to H^i(G, K^\times) \to H^i(G, I_K) \to H^i(G, C_K) \to 1.$$

Für $n = 0$ hat man hingegen die kurze exakte Sequenz

$$H^{-2}(G, I_K) \xrightarrow{g} H^{-2}(G, C_K) \to H^{-1}(G, K^\times) \to 1,$$

so dass es also den Cokern der Abbildung g zu bestimmen gilt. Durch Heranziehung der kohomologischen Fassung der Klassenkörpertheorie nach Tate ergibt sich, dass sich das Problem auf eine rein gruppenkohomologische Fragestellung zurückführen lässt. Es seien G_1, G_2, G_3 die drei Untergruppen der Ordnung 2 von $G \simeq (\mathbb{Z}/2)^2$. Dann geht es genauer gesagt darum, ob der Cokern der Abbildung

$$\bigoplus_{i=1}^{3} H_3(G_i) \to H_3(G),$$

die durch die Vorgabe

$$(z_i)_i \mapsto \sum_i \mathrm{cor}_G^{G_i}(z_i)$$

definiert ist, isomorph zu $(\mathbb{Z}/2)^2$ oder zu $(\mathbb{Z}/2)^3$ ist (einer dieser beiden Fälle tritt mit Sicherheit ein). Im ersten Fall wäre für $n = 0$ die Gruppe $H^{-1}(G, K^\times)$ stets isomorph zu $\mathbb{Z}/2$, im zweiten Fall hingegen stets trivial. Es genügte also, die Gruppe $H^{-1}(G, K^\times)$ für eine einzige Erweiterung, für die der Fall $n = 0$ vorliegt, zu kennen, um die Frage allgemein zu beantworten. Daher bieten sich verschiedene Möglichkeiten, das Problem anzugehen: einmal auf zahlentheortischem Wege durch Betrachtung einer speziellen Erweiterung, die den Fall $n = 0$ realisiert, und ansonsten auf gruppenkohomologischem Wege, indem man die Corestriktionsabbildungen zu verstehen sucht. Tatsächlich werden wir sogar drei Beweise liefern, nämlich neben dem zahlentheoretischen noch zwei gruppentheoretische. In einem Beweis werden wir mit allgemeinen kohomologischen Mitteln arbeiten, währen wir in einem weiteren die Corestriktionsabbildungen ganz explizit berechnen werden.

Wir wollen noch bemerken, dass für einen biquadratischen Erweiterungskörper $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ von $\mathbb{Q}$, mit quadratfreien $a, b \in \mathbb{Z}$, die Anzahl n der Stellen $\mathfrak{p}$ mit $G_\mathfrak{p} = G$ leicht berechnet werden kann (vgl. Kapitel 4). Insbesondere kann $G_p = G$ nur für Primteiler p von a oder b gelten sowie für $p = 2$.

4.2 Satz. *Es sei $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ eine biquadratische Erweiterung, mit quadratfreien $a, b \in \mathbb{Z}$. Für eine Primzahl p gilt $G_p = G$ genau in den Fällen*

i) $p \neq 2,\ \ p \mid a,\ \ p \nmid b,\ \ \left(\frac{b}{p}\right) = -1$

ii) $p \neq 2,\ \ p \nmid a,\ \ p \mid b,\ \ \left(\frac{a}{p}\right) = -1$

iii) $p \neq 2,\ \ p \mid a,\ \ p \mid b,\ \ \left(\frac{ab/p^2}{p}\right) = -1$

iv) $p = 2,\ \ a, b, (ab)_0 \not\equiv 1\ (8)$.

Dabei bezeichnet $\left(\frac{d}{p}\right)$ das Legendresymbol und d_0 den quadratfreien Kern von d.

Berechnung der Legendresymbole ergibt

Bemerkung. Der Fall $n = 0$ liegt vor z. B. für (a, b) = (-1,17), (2,17), (13,17), (2,-7), (5,-11), (-3,13) und (5,29).

Es besteht die folgende Charakterisierung des Falles $n = 0$.

Bemerkung. Der Fall $n = 0$ liegt genau dann vor, wenn für die Erweiterung K/k *nicht* der Hassesche Normensatz gilt, oder mit anderen Worten, wenn der Scholzsche Zahlknoten $\partial_{K/k}$ nicht-trivial ist.

In Kapitel 4 wird $H^{-1}(G, K^\times)$ für verschiedene Möglichkeiten von a, b berechnet, z. B. gilt

4.10 Satz. *Es sei $\mathbb{Q}(\sqrt{-1}, \sqrt{p_1 \dots p_m})/\mathbb{Q}$ eine biquadratische Erweiterung, mit paarweise verschiedenen Primzahlen $p_1, \dots, p_m$ und Galoisgruppe G. Es sei m_1 die Anzahl der p_i mit $p_i \equiv 3, 7$ (8). Dann liegt der Fall $n = 0$ vor für $m_1 = 0$, $p_1 \dots p_m \equiv \pm 1$ (8). Andernfalls gilt*

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1 - 1}$ falls $m_1 > 0$, $p_1 \dots p_m \equiv \pm 1$ (8);

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1}$ falls $p_1 \dots p_m \not\equiv \pm 1$ (8).

Im Fall $n = 0$ gilt $H^{-1}(G, K^\times) = 1$.

Für grundlegende Begriffe aus der Algebra und algebraischen Zahlentheorie verweisen wir auf die Lehrbücher [A1],[A2] und [AZ] von F. Lorenz.

1. Nicht-triviale Cozyklen in $H^{-1}(G, K^\times)$ für biquadratische Ereiterungen von $\mathbb{Q}$

Sei K/k eine endliche galoissche Erweiterung mit Gruppe G. Dann setzt man

$$C^{-1}(G, K^\times) = \{x \in K^\times : N_{K/k}x = 1\},$$
$$B^{-1}(G, K^\times) = \left\langle \frac{\sigma x}{x} : \sigma \in G, x \in K^\times \right\rangle.$$

Die Elemente von $C^{-1}(G, K^\times)$ werden (-1)-*Cozykel* genannt, die Elemente von $B^{-1}(G, K^\times)$ hingegen (-1)-*Coränder*. Die Faktorgruppe

$$H^{-1}(G, K^\times) = C^{-1}(G, K^\times)/B^{-1}(G, K^\times)$$

wird (-1)-te Kohomologiegruppe der Erweiterung K/k genannt. Weiter heißt es, für die Erweiterung K/k gelte Hilberts Satz 90, wenn die (-1)-te Kohomologiegruppe $H^{-1}(G, K^\times)$ trivial ist. Mehr darüber ist in dem Lehrbuch [A1] und in dem Artikel [L] zu erfahren.

Wir sprechen von einem nicht-trivialen (-1)-Cozykel, wenn derselbe kein (-1)-Corand ist. In diesem Kapitel werden wir für biquadratische Erweiterungen von $\mathbb{Q}$ und von $\mathbb{Q}_p$ nicht-triviale (-1)-Cozyklen explizit angeben. Dabei wird sich herausstellen, dass es unendlich viele biquadratische Erweiterungen von $\mathbb{Q}$ und von $\mathbb{Q}_p$ gibt, für die $H^{-1}(G, K^\times)$ nicht-trivial ausfällt.

1.i Quadratische Formen und Hilbertsymbole

Sei $k = \mathbb{Q}$ oder $k = \mathbb{Q}_p$ mit einer Primzahl p. Im Folgenden wird sich die Frage stellen, wann die quadratische Form

$$X_1^2 - aX_2^2 - bX_3^2$$

für $a, b \in k$ isotrop ist. Im Falle $k = \mathbb{Q}$ gibt hier ein Satz von LEGENDRE Aufschluss, den wir ohne Beweis zitieren werden, vgl. [A2, S. 275ff]. Was hingegen die p-adischen Körper betrifft, so hängt die Fragestellung eng mit dem Begriff des Hilbertsymbols zusammen. Die für uns wichtigen Sätze zur Berechnung von Hilbertsymbolen werden wir angeben, vgl. [AZ, S. 244]. Als erstes formulieren wir den grundlegenden

1.1 Satz. *Sei k ein Körper mit char $k \neq 2$. Dann sind für $a, b \in k$ die folgenden Aussagen äquivalent:*

i) b ist bei der Erweiterung $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ eine Norm;

ii) a ist bei der Erweiterung $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$ eine Norm;

iii) die quadratische Form $X_1^2 - aX_2^2 - bX_3^2$ ist über k isotrop;

iv) die quadratische Form $X_1^2 - aX_2^2 - bX_3^2 + abX_4^2$ ist über k isotrop.

Wenn k ein lokaler Körper und $\mathfrak{p}$ das Bewertungsideal von k ist, so lautet eine weitere äquivalente Aussage:

v) für das Hilbertsymbol $\left(\frac{a,b}{\mathfrak{p}}\right)$ gilt $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$.

Beweis: Wenn a in k ein Quadrat ist, so gilt jede der Aussagen i)-iv). Im folgenden sei a kein Quadrat in k. Aus Symmetriegründen kann Aussage ii) außer acht gelassen werden.

i) $\Rightarrow$ iii) Wenn b bei der Erweiterung $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ eine Norm ist, so gilt

$$b = x^2 - ay^2$$

für gewisse $x, y \in k$ und damit ist für $z = 1$ die Gleichung

$$x^2 - ay^2 - bz^2 = 0$$

erfüllt.

iii) $\Rightarrow$ iv) Diese Implikation ist klar.

iv) $\Leftrightarrow$ i) Es gebe $x, y, z, t \in k$ mit

$$x^2 - ay^2 - bz^2 + abt^2 = 0,$$

die nicht alle gleich 0 sind. Dann gilt

$$x^2 - ay^2 = b(z^2 - at^2)$$

und es ist $z^2 - at^2 \neq 0$, denn weil a in k kein Quadrat ist, ergäbe sich andernfalls $x = y = z = t = 0$. Die Gleichung kann also durch $z^2 - at^2$ geteilt werden und man erhält

$$b = \frac{x^2 - ay^2}{z^2 - at^2} = N_{k(\sqrt{a})/k}\left(\frac{x + y\sqrt{a}}{z + t\sqrt{a}}\right),$$

womit wir eine Darstellung von b als Norm bei der Erweiterung $k(\sqrt{a})/k$ haben.

Was die Äquivalenz i) $\Leftrightarrow$ v) im Falle eines lokalen Körpers betrifft, so verweisen wir auf [AZ, S. 240]. □

Ob die ersten vier äquivalenten Bedingungen von Satz 1.1 eintreten, lässt sich im Falle $k = \mathbb{Q}$ stets beantworten.

1.2 Theorem (Legendre 1798). *Es seien $r, s, t \in \mathbb{Z}$ paarweise teilerfremde und quadratfreie ganze Zahlen, die nicht alle dasselbe Vorzeichen haben. Genau dann ist die Gleichung*

$$rX_1^2 + sX_2^2 + tX_3^2 = 0$$

über $\mathbb{Z}$ nicht-trivial lösbar, wenn jede der Kongruenzen

$$X^2 \equiv -st(r), \quad Y^2 \equiv -rt(s), \quad Z^2 \equiv -rs(t)$$

in $\mathbb{Z}$ eine Lösung besitzt.

Beweis: Zum Beweis verweisen wir auf [A2, S. 275ff]. □

1.3 Korollar. *Sei p eine Primzahl. Dann gelten folgende Äquivalenzen:*

$$\begin{aligned}
&p \text{ Norm bei } \mathbb{Q}(i)/\mathbb{Q} \iff -1 \text{ Norm bei } \mathbb{Q}(\sqrt{p})/\mathbb{Q} \\
(1)\qquad &\iff X_1^2 + X_2^2 - pX_3^2 = 0 \text{ über } \mathbb{Z} \text{ nicht-trivial lösbar} \\
&\iff p = 2 \text{ oder } p \equiv 1(4).
\end{aligned}$$

$$\begin{aligned}
&p \text{ Norm bei } \mathbb{Q}(\sqrt{2})/\mathbb{Q} \iff 2 \text{ Norm bei } \mathbb{Q}(\sqrt{p})/\mathbb{Q} \\
&\iff -p \text{ Norm bei } \mathbb{Q}(\sqrt{2})/\mathbb{Q} \iff 2 \text{ Norm bei } \mathbb{Q}(\sqrt{-p})/\mathbb{Q} \\
(2)\qquad &\iff X_1^2 - 2X_2^2 - pX_3^2 = 0 \text{ über } \mathbb{Z} \text{ nicht-trivial lösbar} \\
&\iff X_1^2 - 2X_2^2 + pX_3^2 = 0 \text{ über } \mathbb{Z} \text{ nicht-trivial lösbar} \\
&\iff p = 2 \text{ oder } p \equiv 1(8) \text{ oder } p \equiv 7(8).
\end{aligned}$$

$$\begin{aligned}
&p \text{ Norm bei } \mathbb{Q}(\sqrt{-2})/\mathbb{Q} \iff -2 \text{ Norm bei } \mathbb{Q}(\sqrt{p})/\mathbb{Q} \\
(3)\qquad &\iff X_1^2 + 2X_2^2 - pX_3^2 = 0 \text{ über } \mathbb{Z} \text{ nicht-trivial lösbar} \\
&\iff p = 2 \text{ oder } p \equiv 1(8) \text{ oder } p \equiv 3(8).
\end{aligned}$$

1.4 Korollar. *Seien p und q voneinander verschiedene ungerade Primzahlen. Dann bestehen die folgenden Äquivalenzen:*

$$\begin{aligned} &q \text{ Norm bei } \mathbb{Q}(\sqrt{p})/\mathbb{Q} \iff p \text{ Norm bei } \mathbb{Q}(\sqrt{q})/\mathbb{Q} \\ &\iff X_1^2 - pX_2^2 - qX_3^2 = 0 \text{ über } \mathbb{Q} \text{ nicht-trivial lösbar} \\ &\iff \left(\tfrac{q}{p}\right) = \left(\tfrac{p}{q}\right) = 1. \end{aligned} \tag{4}$$

$$\begin{aligned} &-q \text{ Norm bei } \mathbb{Q}(\sqrt{p})/\mathbb{Q} \iff p \text{ Norm bei } \mathbb{Q}(\sqrt{-q})/\mathbb{Q} \\ &\iff X_1^2 - pX_2^2 + qX_3^2 = 0 \text{ über } \mathbb{Q} \text{ nicht-trivial lösbar} \\ &\iff \left(\tfrac{-q}{p}\right) = \left(\tfrac{p}{q}\right) = 1. \end{aligned} \tag{5}$$

Auch für $k = \mathbb{Q}_p$ mit einer Primzahl p lässt sich die Frage beatworten, ob die fünf äquaivalenten Bedingungen von Satz 1.1 eintreten. Sei p eine beliebige Primzahl. Wenn $\mathbb{Z}_p$ den Bewertungsring von $\mathbb{Q}_p$ bezeichnet, so ist $p\,\mathbb{Z}_p$ das Bewertungsideal von $\mathbb{Q}_p$. Das Hilbertsymbol zu $\mathbb{Q}_p$ schreibt sich deshalb $(\frac{\cdot,\cdot}{p})$. Ist p ungerade, so handelt es sich um ein zahmes Hilbertsymbol und es gilt

1.5 Satz. *Es sei p eine ungerade Primzahl. Für alle $a, b \in \mathbb{Z}_p^\times$ gelten dann die Gleichungen*

$$\left(\frac{a,b}{p}\right) = 1, \qquad \left(\frac{p,a}{p}\right) = \left(\frac{a}{p}\right)$$

und weiter ist

$$\left(\frac{p,p}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

All dies lässt sich durch die Gleichung

$$\left(\frac{p^\alpha a, p^\beta b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta}\left(\frac{a}{p}\right)^\beta \left(\frac{b}{p}\right)^\alpha$$

für $a, b \in \mathbb{Z}_p^\times$ und $\alpha, \beta \in \mathbb{Z}$ zusammenfassen.

Beweis: Wir verweisen auf [AZ, S. 244]. □

Für $p = 2$ ist $(\frac{\cdot,\cdot}{p})$ hingegen ein wildes Hilbertsymbol. Es ist ebenfalls der Berechnung zugänglich.

1.6 Satz. *Für alle $a, b \in \mathbb{Z}_2^\times$ gelten die Gleichungen*

$$\left(\frac{a,b}{2}\right) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}}, \qquad \left(\frac{2,a}{2}\right) = (-1)^{\frac{a^2-1}{8}}$$

und desweiteren ist

$$\left(\frac{2,2}{2}\right) = 1.$$

All diese Formeln lassen sich durch die Gleichung

$$\left(\frac{2^\alpha a, 2^\beta b}{2}\right) = (-1)^{\frac{a^2-1}{8}\beta + \frac{b^2-1}{8}\alpha + \frac{a-1}{2}\frac{b-1}{2}}$$

für $a, b \in \mathbb{Z}_2^\times$ und $\alpha, \beta \in \mathbb{Z}$ zusammenfassen.

Beweis: Siehe [AZ, S. 244]. □

1.ii Allgemeines über biquadratische Erweiterungen

In diesem Abschnitt werden wir ein Kriterium dafür angeben, wann bei einer biquadratischen Erweiterung ein (-1)-Cozykel ein (-1)-Corand ist. Den Einstieg ermöglicht der folgende

1.7 Satz. *Seien K/k eine endliche galoissche Erweiterung mit der Gruppe G und F ein Zwischenkörper von K/k. Für die Erweiterung K/F gelte Hilberts Satz 90. Sei α ein Element von $K^\times$ mit der Norm 1 über k und $N_{K/F}(\alpha) = \gamma$. Genau dann liegt α in der trivialen Klasse $B^{-1}(G, K^\times)$ von $H^{-1}(G, K^\times)$, wenn es ein $\beta \in B^{-1}(G, K^\times)$ mit $N_{K/F}(\beta) = \gamma$ gibt.*

Beweis: Im Falle $\alpha \in B^{-1}(G, K^\times)$ ist $\gamma = N_{K/F}\,\alpha$ die Norm eines Elementes von $B^{-1}(G, K^\times)$ über F. Gibt es umgekehrt ein $\beta \in B^{-1}(G, K^\times)$ mit $N_{K/F}\,\beta = \gamma$, so folgt $N_{K/F}(\alpha\,\beta^{-1}) = 1$ und $\alpha\,\beta^{-1}$ ist ein (-1)-Corand $\delta \in B^{-1}(G(K/F), K^\times)$, denn für die Erweiterung K/F gilt Hilberts Satz 90. Da $B^{-1}(G(K/F), K^\times)$ eine Untergruppe von $B^{-1}(G, K^\times)$ ist, liegt auch $\alpha = \beta\,\delta$ in $B^{-1}(G, K^\times)$. □

Für uns relevant ist der Fall einer biquadratischen Erweiterung K/k mit Gruppe $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ und quadratischem Zwischenkörper $k(\sqrt{a})$. Nach Satz 1.7 bestimmt jedes $\alpha \in K$, das über k die Norm 1 hat, genau dann ein nicht-triviales Element der Gruppe $H^{-1}(G, K^\times)$, wenn es *keinen* (-1)-Corand $\beta \in B^{-1}(G, K^\times)$ gibt, der über $k(\sqrt{a})$ dieselbe Norm wie α hat. Damit stellt sich die Frage, wann ein Element von $k(\sqrt{a})$ die Norm eines (-1)-Corandes ist. Die Antwort liefert

1.8 Satz. *Es seien k ein Körper mit char $k \neq 2$ und K/k eine biquadratische Erweiterung mit Gruppe G, und zwar sei $K = k(\sqrt{a}, \sqrt{b})$. Jedes $\gamma \neq 1$ aus $k(\sqrt{a})$, das über k die Norm 1 hat, besitzt für ein bestimmtes $c \in k$ die Darstellung*

$$\gamma = \frac{c + \sqrt{a}}{c - \sqrt{a}}.$$

Genau dann gibt es einen Corand $\beta \in B^{-1}(G, K^\times)$ mit Norm γ über $k(\sqrt{a})$, wenn die Gleichung

$$X_1^2 + (a - c^2)X_2^2 - bX_3^2 = 0 \tag{6}$$

über k eine nicht-triviale Lösung besitzt.

Beweis: Sei $k(\sqrt{a})$ Fixkörper des Automorphismus $\tau \in G$ und $k(\sqrt{b})$ Fixkörper des Automorphismus $\sigma \in G$. Jeder Corand $\delta \in B^{-1}(G, K^\times)$ ist von der Gestalt

$$\delta = \alpha^{1-\sigma}\beta^{1-\tau}$$

mit $\alpha, \beta \in K^\times$ und hat über $k(\sqrt{a})$ die Norm

$$\begin{aligned} N_\tau\,\delta = N_\tau\big(\alpha^{1-\sigma}\big) &= \alpha^{1-\sigma}\big(\alpha^{1-\sigma}\big)^\tau = \alpha^{1-\sigma}\alpha^{\tau-\sigma\tau} \\ &= \alpha^{1-\sigma}\alpha^{\tau-\tau\sigma} = \big(\alpha\alpha^\tau\big)^{1-\sigma}. \end{aligned}$$

Es gilt $\alpha = x_1 + x_2\sqrt{b}$ für eindeutig bestimmte $x_1, x_2 \in k(\sqrt{a})$; einsetzen ergibt

$$N_\tau\,\delta = \big(x_1^2 - bx_2^2\big)^{1-\sigma} = \big(x_1^2 - bx_2^2\big)\big((x_1^\sigma)^2 - b(x_2^\sigma)^2\big)^{-1}.$$

Für $i = 1, 2$ sei $x_i = s_i + t_i\sqrt{a}$ mit $s_i, t_i \in k$. Damit erhält man

$$\begin{aligned} N_\tau\, \delta &= \frac{(s_1 + t_1\sqrt{a})^2 - b(s_2 + t_2\sqrt{a})^2}{(s_1 - t_1\sqrt{a})^2 - b(s_2 - t_2\sqrt{a})^2} \\ &= \frac{s_1^2 + at_1^2 - bs_2^2 - abt_2^2 + 2(s_1t_1 - bs_2t_2)\sqrt{a}}{s_1^2 + at_1^2 - bs_2^2 - abt_2^2 - 2(s_1t_1 - bs_2t_2)\sqrt{a}}. \end{aligned}$$

Es sei nun ein von 1 verschiedenes $\gamma \in k(\sqrt{a})$ mit der Norm 1 über k gegeben. Nach Hilberts Satz 90 besteht für gewisse $r, s \in k$ die Darstellung

$$\gamma = \frac{r + s\sqrt{a}}{r - s\sqrt{a}} = \frac{r/s + \sqrt{a}}{r/s - \sqrt{a}},$$

wobei s wegen $\gamma \neq 1$ von 0 verschieden ist. Wir setzen $c = r/s$. Genau dann ist die Norm von δ über $k(\sqrt{a})$ gleich γ, wenn

$$\frac{s_1^2 + at_1^2 - bs_2^2 - abt_2^2 + 2(s_1t_1 - bs_2t_2)\sqrt{a}}{s_1^2 + at_1^2 - bs_2^2 - abt_2^2 - 2(s_1t_1 - bs_2t_2)\sqrt{a}} = \frac{c + \sqrt{a}}{c - \sqrt{a}}$$

gilt, was zu

$$\begin{aligned} &\big(s_1^2 + at_1^2 - bs_2^2 - abt_2^2 + 2(s_1t_1 - bs_2t_2)\sqrt{a}\big)\,\big(c - \sqrt{a}\big) \\ =&\big(s_1^2 + at_1^2 - bs_2^2 - abt_2^2 - 2(s_1t_1 - bs_2t_2)\sqrt{a}\big)\,\big(c + \sqrt{a}\big). \end{aligned}$$

umgeformt werden kann. Ausmultiplizieren ergibt, dass dies zu

$$\begin{aligned} &c(s_1^2 + at_1^2 - bs_2^2 - abt_2^2) - 2a(s_1t_1 - bs_2t_2) \\ &-\big((s_1^2 + at_1^2 - bs_2^2 - abt_2^2) - 2c(s_1t_1 - bs_2t_2)\big)\sqrt{a} \\ &= c(s_1^2 + at_1^2 - bs_2^2 - abt_2^2) - 2a(s_1t_1 - bs_2t_2) \\ &+\big((s_1^2 + at_1^2 - bs_2^2 - abt_2^2) - 2c(s_1t_1 - bs_2t_2)\big)\sqrt{a} \end{aligned}$$

äquivalent ist. Aufgrund der Eindeutigkeit der Darstellung der Elemente von $k(\sqrt{a})$ bzgl. der Basis $(1, \sqrt{a})$ ist letzteres genau dann der Fall, wenn

$$\begin{aligned} &s_1^2 + at_1^2 - bs_2^2 - abt_2^2 - 2c(s_1t_1 - bs_2t_2) \\ &= -\big((s_1^2 + at_1^2 - bs_2^2 - abt_2^2) - 2c(s_1t_1 - bs_2t_2)\big) \end{aligned}$$

gilt. Weil die Charakteristik von k nicht 2 ist, bedeutet dies

$$s_1^2 + at_1^2 - bs_2^2 - abt_2^2 - 2c(s_1t_1 - bs_2t_2) = 0.$$

Nochmaliges Umformen liefert die Gleichung

$$(s_1 - ct_1)^2 + (a - c^2)t_1^2 - b(s_2 - ct_2)^2 - b(a - c^2)t_2^2 = 0. \tag{7}$$

Zusammengefasst ist γ genau dann gleich der Norm eines Corandes δ über $k(\sqrt{a})$, wenn Gleichung (7) über k eine nicht-triviale Lösung s_1, t_1, s_2, t_2 besitzt. Weil die lineare Transformation

$$\begin{aligned} x &= s_1 - ct_1 \qquad & y &= t_1 \\ z &= s_2 - ct_2 \qquad & t &= t_2 \end{aligned}$$

einen Isomorphismus des des k-Vektoraumes k^4 darstellt, ist eine weitere äquivalente Aussage, dass die Gleichung

$$x^2 + (a - c^2)y^2 - bz^2 - b(a - c^2)t^2 = 0$$

über k eine nicht-triviale Lösung x, y, z, t besitzt. Das aber trifft nach Satz 1.1 genau dann zu, wenn

$$x^2 + (a - c^2)y^2 - bz^2 = 0$$

über k nicht-trivial lösbar ist. □

1.9 Korollar. *Es seien k ein Körper mit char $k \neq 2$ und K/k eine biquadratische Erweiterung mit Gruppe G, und zwar sei $K = k(\sqrt{a}, \sqrt{b})$. Genau dann ist -1 die Norm eines Corandes $\beta \in B^{-1}(G, K^\times)$ über $k(\sqrt{a})$, wenn die Gleichung*

$$X_1^2 + aX_2^2 - bX_3^2 = 0 \tag{8}$$

über k eine nicht-triviale Lösung besitzt. Einen Corand $\beta \in B^{-1}(G, K^\times)$ mit der Norm -1 über $k(\sqrt{ab})$ gibt es genau dann, wenn die Gleichung

$$X_1^2 - aX_2^2 - bX_3^2 = 0 \tag{9}$$

über k nicht-trivial lösbar ist.

Beweis: Es handelt sich um Satz 1.8 im Fall $c = 0$. Die erste Aussage folgt aus Satz 1.8, indem dieser auf das Zahlpaar (a, b) angewandt wird. Zum Beweis der zweiten Aussage wird Satz 1.8 auf (ab, a) angewandt. Demnach ist -1 genau dann die Norm eines Corandes über $k(\sqrt{ab})$, wenn die Gleichung

$$X_1^2 + abX_2^2 - aX_3^2 = 0$$

über k eine nicht-triviale Lösung besitzt. Äquivalent dazu ist, dass es über k eine nicht-triviale Lösung der Gleichung

$$aX_1^2 + b(aX_2)^2 - (aX_3)^2 = 0$$

gibt, und letzteres ist genau dann der Fall, wenn

$$aX_1^2 + bX_2^2 - X_3^2 = 0$$

über k nicht-trivial lösbar ist. Damit folgt die Behauptung. □

1.iii Biquadratische Erweiterungen von $\mathbb{Q}$ und $\mathbb{Q}_p$

In diesem Abschnitt werden wir für biquadratische Erweiterungen von $\mathbb{Q}$ und von p-adischen Körpern $\mathbb{Q}_p$ explizit (-1)-Cozyklen angeben, die keine (-1)-Coränder sind. Wir werden unendliche Serien von Erweiterungen vorstellen, für die $H^{-1}(G, K^\times)$ nicht-trivial ausfällt. Zudem werden wir feststellen, dass man in gewissen Fällen (-1)-Cozykel angeben kann, die nicht-trivial sind und in verschiedenen Klassen von $H^{-1}(G, K^\times)$ liegen. Auf diese Weise werden wir eine unendliche Reihe von Körpern angeben können, für die $H^{-1}(G, K^\times)$ nicht einmal zyklisch ist.

1.10.1 Satz. *Ist p eine Primzahl und $p \equiv 3(8)$, so gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{p}, i)/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{p}, i)$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Es gilt $p = a^2 + 2b^2$ für gewisse $a, b \in \mathbb{Z}$, und für derartige a und b ist

$$\frac{a + \sqrt{p}}{b(1 + i)} \tag{10}$$

ein Element von K der Norm -1 über $\mathbb{Q}(\sqrt{p}\, i)$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt.

1.10.2 Zusatz. *Seien p wie in Satz 1.10.1 und $a, b \in \mathbb{Z}$, so dass $p = a^2 + 2b^2$. Dann sind unter den lokalen Erweiterungen genau*

$$\mathbb{Q}_2(\sqrt{p}, i)/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{p}, i)/\mathbb{Q}_p$$

ebenfalls biquadratisch und das Element (10) *von $\mathbb{Q}(\sqrt{p}, i)$ hat auch dort die Norm 1. Wie bei der globalen Erweiterung gehört es nicht zu den (-1)-Corändern.*

Beweis von Satz 1.10.1: Zuerst zeigen wir, dass ein Element von K mit der Norm -1 über $\mathbb{Q}$ nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt. Wir wenden den zweiten Teil von Korollar 1.9 auf die Erweiterung $K/\mathbb{Q}$ an, wobei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ mit $a = -1$ und $b = p$ gilt. Genau dann gibt es einen Corand $\beta \in B^{-1}(G, K^\times)$ mit Norm -1 über $\mathbb{Q}(\sqrt{p}\,i)$, wenn die Gleichung

$$X_1^2 - (-1)X_2^2 - pX_3^2 = 0$$

über $\mathbb{Q}$ eine nicht-triviale Lösung besitzt. Aufgrund der Voraussetzung $p \equiv 3(8)$ ist dies nicht der Fall, vgl. Korollar 1.3. Wenn wir zeigen können, daß es ein $\alpha \in K$ mit Norm -1 über $\mathbb{Q}(\sqrt{p}\,i)$ gibt, ist die Behauptung bewiesen.

Wir wollen jetzt nachweisen, dass -2 bei der Erweiterung $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ eine Norm ist. Die Diskriminante von $\mathbb{Q}(\sqrt{-2})$ ist -8, vgl. [AZ, S. 49/50]. Sie ist nicht durch p teilbar und p damit in $\mathbb{Q}(\sqrt{-2})$ nicht verzweigt. Der Zerlegungstyp von p in $\mathbb{Q}(\sqrt{-2})$ ist am Wert des Legendresymbols $(\frac{-8}{p})$ zu erkennen; wegen

$$\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)\cdot(-1) = 1$$

ist p in $\mathbb{Q}(\sqrt{-2})$ voll zerlegt, d. h. das Ideal (p) des Ganzheitsringes von $\mathbb{Q}(\sqrt{-2})$ ist das Produkt zweier verschiedener zueinander konjugierter Primideale ([AZ, S. 113] sowie [AZ, S. 103]). Nach [AZ, S.49/50] ist $\mathbb{Z}[\sqrt{-2}]$ der Ganzheitsring von $\mathbb{Q}(\sqrt{-2})$, denn die Diskriminante -8 von $\mathbb{Q}(\sqrt{-2})$ ist nicht zu 1 modulo 4 kongruent. Weil $\mathbb{Q}(\sqrt{-2})$ die Klassenzahl 1 hat (vgl. [AZ, S. 114]), ist der Ganzheitsring $\mathbb{Z}[\sqrt{-2}]$ ein Hauptidealring[1] (vgl. [AZ, S. 45]) und als solcher faktoriell. Es gibt daher ein Primelement π von $\mathbb{Z}[\sqrt{-2}]$, so dass

$$(p) = (\pi)(\overline{\pi}),$$

was gleichbedeutend ist mit

$$p = \pi\overline{\pi}.$$

Durch Anwendung der Normabbildung $N = N_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}$ erhält man

$$p^2 = N\pi N\overline{\pi},$$

und weil die Normen bei imaginärquadratischen Zahlkörpern nur nicht-negative Werte annehmen, folgt schließlich

$$N\pi = N\overline{\pi} = p.$$

Damit ist gezeigt, dass es ein $z = a + b\sqrt{-2}$ aus $\mathbb{Z}[\sqrt{-2}]$ mit

$$p = Nz = a^2 + 2b^2$$

gibt. Insbesondere ist p Norm bei der Erweiterung $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, was im übrigen auch aus Korollar 1.3 folgt, da nach Voraussetzung $p \equiv 3(8)$ gilt. Nach Satz 1.1 ist

[1] Der Ring $\mathbb{Z}[\sqrt{-2}]$ ist sogar euklidisch.

dann auch -2 Norm bei der Erweiterung $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, so dass es ein $\alpha \in \mathbb{Q}(\sqrt{p})$ mit $N_{K/\mathbb{Q}(\sqrt{p}\,i)}(\alpha) = -2$ gibt. Ein α dieser Art kann anhand der Darstellung von p als Norm bei $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ sofort angegeben werden, nämlich

$$\alpha = \frac{a + \sqrt{p}}{b}.$$

Andererseits gilt $N_{K/\mathbb{Q}(\sqrt{p}\,i)}(1+i) = 2$, so dass zusammen

$$N_{K/\mathbb{Q}(\sqrt{p}\,i)}\left(\frac{a+\sqrt{p}}{b(1+i)}\right) = -1$$

folgt. Nach dem oben Gesagten ist $(a + \sqrt{p})/(b(1+i))$ ein Element von $K^\times$ der Norm 1 über $\mathbb{Q}$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt. □

Beweis des Zusatzes 1.10.2: Wie aus Satz 4.2 (siehe Einleitung) unmittelbar folgt, sind unter den lokalen Erweiterungen nur $\mathbb{Q}_2(\sqrt{p}, i)/\mathbb{Q}_2$ und $\mathbb{Q}_p(\sqrt{p}, i)/\mathbb{Q}_p$ biquadratisch. Durch Berechnung zweier Hilbertsymbole kann weiter sofort verifiziert werden, dass die Gleichung

$$X_1^2 + X_2^2 - pX_3^2 = 0$$

unter der Voraussetzung $p \equiv 3(8)$ auch über $\mathbb{Q}_2$ und $\mathbb{Q}_p$ keine nicht-triviale Lösung besitzt. Dabei ist das Hilbertsymbol über $\mathbb{Q}_2$ ein wildes, das über $\mathbb{Q}_p$ hingegen zahm. Beide sind jedoch der Berechnung zugänglich (Satz 1.5, Satz 1.6), und zwar gilt

$$\left(\frac{-1, p}{2}\right) = (-1)^{\frac{-1-1}{2}\frac{p-1}{2}} = -1,$$
$$\left(\frac{-1, p}{p}\right) = \left(\frac{-1}{p}\right) = -1.$$

Also ist der im Satz angegebene (-1)-Cozykel mit der Norm -1 über $\mathbb{Q}(\sqrt{p}\,i)$ nach Korollar 1.9 auch bei den lokalen Erweiterungen $\mathbb{Q}_2(\sqrt{p}, i)/\mathbb{Q}_2$ und $\mathbb{Q}_p(\sqrt{p}, i)/\mathbb{Q}_p$ kein (-1)-Corand. □

1.10.3 Beispiele.[2]

Erweiterung	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$	$\frac{1+\sqrt{3}}{1+i}$
$\mathbb{Q}(\sqrt{11}, i)/\mathbb{Q}$	$\frac{3+\sqrt{11}}{1+i}$
$\mathbb{Q}(\sqrt{19}, i)/\mathbb{Q}$	$\frac{1+\sqrt{19}}{3(1+i)}$ oder $\frac{13+3\sqrt{19}}{1+i}$
$\mathbb{Q}(\sqrt{43}, i)/\mathbb{Q}$	$\frac{5+\sqrt{43}}{3(1+i)}$ oder $\frac{59+9\sqrt{43}}{1+i}$
$\mathbb{Q}(\sqrt{59}, i)/\mathbb{Q}$	$\frac{3+\sqrt{59}}{5(1+i)}$ oder $\frac{23+3\sqrt{59}}{1+i}$
$\mathbb{Q}(\sqrt{67}, i)/\mathbb{Q}$	$\frac{7+\sqrt{67}}{3(1+i)}$ oder $\frac{221+27\sqrt{67}}{1+i}$
$\mathbb{Q}(\sqrt{83}, i)/\mathbb{Q}$	$\frac{9+\sqrt{83}}{1+i}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.11.1 Satz. *Es sei p eine Primzahl, und zwar sei $p \equiv 3(8)$ oder $p \equiv 5(8)$. Dann gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{2}, \sqrt{p})/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Das Element

$$1 + \sqrt{2}$$

von K hat über $\mathbb{Q}(\sqrt{p})$ die Norm -1 und liegt nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder.

1.11.2 Satz. *Ist p eine Primzahl und $p \equiv 5(8)$, so gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$, und für derartige a und b ist*

$$\frac{a + \sqrt{p}}{b} \tag{11}$$

ein Element von $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$, das über $\mathbb{Q}(\sqrt{2})$ die Norm -1 hat und nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt ($G = G(K/\mathbb{Q})$), da es sich von $1 + \sqrt{2}$ nur um einen Corand unterscheidet.

1.11.3 Zusatz. *Für p wie in Satz 1.11.1 sind unter den lokalen Erweiterungen genau*

$$\mathbb{Q}_2(\sqrt{2}, \sqrt{p})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{2}, \sqrt{p})/\mathbb{Q}_p$$

ebenfalls biquadratisch und das Element $1 + \sqrt{2}$ von $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ ist auch dort ein Element der Norm 1, das nicht zu den (-1)-Coründern gehört. Für $p \equiv 5(8)$ gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$, und dann ist das Element (11) von $\mathbb{Q}(\sqrt{2}, \sqrt{p})$ auch bei den beiden lokalen Erweiterungen ein Element der Norm 1, das in derselben Klasse wie $1 + \sqrt{2}$ liegt und deshalb kein Corand ist.

Beweis von Satz 1.11.1: Offenbar ist -1 die Norm von $1 + \sqrt{2}$ bezüglich der Erweiterung $K/\mathbb{Q}(\sqrt{p})$. Mit Korollar 1.9 wollen wir uns davon überzeugen, dass ein Element von K der Norm -1 über $\mathbb{Q}(\sqrt{p})$ kein Corand ist. Dazu haben wir die quadratische Form

$$X_1^2 + pX_2^2 - 2X_3^2$$

zu betrachten. Sie ist nach Korollar 1.3 nicht isotrop, weshalb Elemente von K mit Norm -1 bei $K/\mathbb{Q}(\sqrt{p})$ wie behauptet keine Coränder sind. □

Beweis von Satz 1.11.2: Aufgrund der Kongruenz $p \equiv 1(4)$ gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$, vgl. [N,S. 1]. Das Element (11) von K hat wie $1 + \sqrt{2}$ die Norm -1 über $\mathbb{Q}(\sqrt{2p})$. Nach Satz 90 von Hilbert unterscheiden sie sich deshalb nur um einen Corand voneinander, doch $1+\sqrt{2}$ liegt nach Satz 1.11.1 in einer nicht-trivialen Klasse von $H^{-1}(G, K^\times)$. □

Beweis von Zusatz 1.11.3: Wie sich aus Satz 4.2 (siehe Einleitung) ergibt, sind unter den lokalen Erweiterungen nur $\mathbb{Q}_2(\sqrt{2}, \sqrt{p})/\mathbb{Q}_2$ und $\mathbb{Q}_p(\sqrt{2}, \sqrt{p})/\mathbb{Q}_p$ biquadratisch. Bezüglich $\mathbb{Q}_2(\sqrt{2}, \sqrt{p})/\mathbb{Q}_2(\sqrt{2p})$ und $\mathbb{Q}_p(\sqrt{2}, \sqrt{p})/\mathbb{Q}_p(\sqrt{2p})$ haben $1 + \sqrt{2}$ und das Element (11) von K die Norm -1. Ob es sich um Coränder handelt, ist nach Korollar 1.9 an der quadratischen Form

$$X_1^2 - 2X_2^2 - pX_3^2$$

zu erkennen. Sie ist über $\mathbb{Q}_2$ und $\mathbb{Q}_p$ nicht isotrop, wie man durch Berchnung zweier Hilbertsymbole erkennt (vgl. Satz 1.5, Satz 1.6). Genauer gesagt gilt

$$\left(\frac{2,p}{2}\right) = (-1)^{\frac{p^2-1}{8}} = -1,$$
$$\left(\frac{2,p}{p}\right) = \left(\frac{2}{p}\right) = -1.$$

Also haben wir mit Elementen der Norm 1 zu tun, die keine Coränder sind. □

1.11.4 Beispiele.[2]

Erweiterung	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$	$1+\sqrt{2}$ oder $\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right)^3$
$\mathbb{Q}(\sqrt{2},\sqrt{11})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{13})/\mathbb{Q}$	$1+\sqrt{2}$ oder $\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13} = \left(\frac{3+\sqrt{13}}{2}\right)^3$
$\mathbb{Q}(\sqrt{2},\sqrt{19})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{29})/\mathbb{Q}$	$1+\sqrt{2}$ oder $\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29} = \left(\frac{5+\sqrt{29}}{2}\right)^3$
$\mathbb{Q}(\sqrt{2},\sqrt{37})/\mathbb{Q}$	$1+\sqrt{2}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{2},\sqrt{43})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{53})/\mathbb{Q}$	$1+\sqrt{2}$ oder $\frac{7+\sqrt{53}}{2}$ oder $182+25\sqrt{53} = \left(\frac{7+\sqrt{53}}{2}\right)^3$
$\mathbb{Q}(\sqrt{2},\sqrt{59})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{61})/\mathbb{Q}$	$1+\sqrt{2}$ oder $\frac{6+\sqrt{61}}{5}$
$\mathbb{Q}(\sqrt{2},\sqrt{67})/\mathbb{Q}$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2},\sqrt{83})/\mathbb{Q}$	$1+\sqrt{2}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.12.1 Satz. *Sei p eine Primzahl und $p \equiv 5(12)$, d. h. p sei modulo 24 zu einer der Zahlen 5, 17 kongruent. Dann gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{3}, \sqrt{p})/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{p})$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Es gilt $p = a^2 + b^2$ für gewisse $a, b \in \mathbb{Z}$, und für derartige a und b ist

$$\frac{a + \sqrt{p}}{b} \tag{12}$$

ein Element von $K = \mathbb{Q}(\sqrt{3}, \sqrt{p})$ der Norm -1 über $\mathbb{Q}(\sqrt{3})$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt.

1.12.2 Zusatz. *Seien p wie in Satz 1.12.1 und $a, b \in \mathbb{Z}$, so dass $p = a^2 + b^2$. Dann sind unter den lokalen Erweiterungen*

$$\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

ebenfalls biquadratisch und das Element (12) von $\mathbb{Q}(\sqrt{3}, \sqrt{p})$ hat auch dort die Norm 1, gehört jedoch nicht zu den (-1)-Coändern. Die lokale Erweiterung

$$\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2$$

ist für $p \equiv 5(24)$ biquadratisch, für $p \equiv 17(24)$ hingegen nur quadratisch. Dies sind sämtliche biquadratischen lokalen Erweiterungen. Gilt $p \equiv 5(24)$, so ist das Element (12) von $\mathbb{Q}(\sqrt{3}, \sqrt{p})$ bei $\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2$ ein Corand.

Beweis von Satz 1.12.1: Wegen $p \equiv 1(4)$ gibt es $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$, vgl. [N, S. 1]. Das Element (12) von K hat die Norm -1 über $\mathbb{Q}(\sqrt{3})$. Wir zeigen jetzt, dass ein Element von K der Norm -1 über $\mathbb{Q}(\sqrt{3})$ kein Corand ist. Nach Korollar 1.9 sind Elemente von K mit Norm -1 bei $K/\mathbb{Q}(\sqrt{3})$ genau dann Coränder, wenn die quadratische Form

$$X_1^2 + 3X_3^2 - pX_3^2$$

isotrop ist. Das ist wegen $(\frac{p}{3}) = -1$ nicht der Fall, denn die Kongruenz $X^2 \equiv p(3)$ ist damit in $\mathbb{Z}$ nicht lösbar, vgl. Theorem 1.2. Also ist das Element (11) von K wie behauptet kein Corand. □

Beweis von Zusatz 1.12.2: Man erhält durch Anwendung von Satz 4.2 (siehe Einleitung), dass die lokalen Erweiterungen $\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3$ und $\mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$ biquadratisch sind. Wenn die quadratische Form

$$X_1^2 - 3X_2^2 - pX_3^2$$

nicht isotrop ist, sind Elemente mit der Norm -1 bei $\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3(\sqrt{3p})$ oder $\mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p(\sqrt{3p})$ nach Korollar 1.9 keine Coränder. Sie ist nicht isotrop, denn es gilt

$$\left(\frac{3, p}{3}\right) = \left(\frac{p}{3}\right) = -1,$$
$$\left(\frac{3, p}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) - 1.$$

Daher ist das Element (12) von K in $\mathbb{Q}_3(\sqrt{3}, \sqrt{p})$ und $\mathbb{Q}_p(\sqrt{3}, \sqrt{p})$ kein Corand. Dass $\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2$ für $p \equiv 5(24)$ biquadratisch, für $p \equiv 17(24)$ hingegen quadratisch

ist, erkennt man wiederum mit Satz 4.2. Im Falle $p \equiv 5(24)$ ist die quadratische Form

$$X_1^2 + 3X_2^2 - pX_3^2$$

über $\mathbb{Q}_2$ isotrop, denn nach Satz 1.6 gilt

$$\left(\frac{-3, p}{2}\right) = (-1)^{\frac{-3-1}{2}\frac{p-1}{2}} = 1.$$

Das Element (12) von K wird deshalb in $\mathbb{Q}_2(\sqrt{3}, \sqrt{p})$ zum Corand. □

1.12.3 Beispiele.[2]

Erweiterung	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$
$\mathbb{Q}(\sqrt{3}, \sqrt{17})/\mathbb{Q}$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{3}, \sqrt{29})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$
$\mathbb{Q}(\sqrt{3}, \sqrt{41})/\mathbb{Q}$	$\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$
$\mathbb{Q}(\sqrt{3}, \sqrt{53})/\mathbb{Q}$	$\frac{7+\sqrt{53}}{2}$ oder $182+25\sqrt{53}$
$\mathbb{Q}(\sqrt{3}, \sqrt{89})/\mathbb{Q}$	$\frac{8+\sqrt{89}}{5}$ oder $500+53\sqrt{89}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.13.1 Satz. *Sei p eine Primzahl, die einer der Konruenzen $p \equiv 5, 7, 11(12)$ und darüber hinaus noch $p \equiv \pm 1(8)$ genügt, d. h. p sei modulo 24 zu einer der Zahlen 7, 17, 23 kongruent. Dann gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{3}, \sqrt{p})/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{p})$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Es gilt $p = a^2 - 2b^2$ für gewisse $a, b \in \mathbb{Z}$, und für derartige a und b ist

$$\frac{a + \sqrt{p}}{b(1 + \sqrt{3})} \tag{13}$$

ein Element von $K = \mathbb{Q}(\sqrt{3}, \sqrt{p})$ der Norm -1 über $\mathbb{Q}(\sqrt{3p})$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt. Für $p \equiv 17(24)$ unterscheidet es sich von einem Element der Norm 1 wie in Satz 1.12.1 nur um einen Corand.

1.13.2 Zusatz. *Seien p wie in Satz 1.13.1 und $a, b \in \mathbb{Z}$, so dass $p = a^2 - 2b^2$. Für $p \equiv 7(24)$ sind unter den lokalen Erweiterungen nur*

$$\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

ebenfalls biquadratisch, für $p \equiv 17(24)$ sind es nur

$$\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

und für $p \equiv 23(24)$ sind es die Erweiterungen

$$\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2, \quad \mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3.$$

In jedem der genannten Fälle ist das Element (13) *von $\mathbb{Q}(\sqrt{3}, \sqrt{p})$ auch dort ein Element der Norm 1, das nicht zu den (-1)-Corändern gehört.*

Beweis von Satz 1.13.1: Diesen Satz beweist man mit Hilfe von Korollar 1.9. Zur Begründung der letzten Behauptung beachte man, dass beide Elemente über $\mathbb{Q}(\sqrt{3p})$ die Norm -1 haben. □

Beweis von Zusatz 1.13.2: Der Beweis erfolgt unter Heranziehung von Satz 4.2, Korollar 1.9 und der Sätze 1.5, 1.6. □

1.13.3 Beispiele.[2]

Erweiterung	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{3},\sqrt{7})/\mathbb{Q}$	$\frac{3+\sqrt{7}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{17})/\mathbb{Q}$	$\frac{5+\sqrt{17}}{2(1+\sqrt{3})}$
$\mathbb{Q}(\sqrt{3},\sqrt{23})/\mathbb{Q}$	$\frac{5+\sqrt{23}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{31})/\mathbb{Q}$	$\frac{7+\sqrt{31}}{3(1+\sqrt{3})}$ oder $\frac{39+7\sqrt{31}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{41})/\mathbb{Q}$	$\frac{7+\sqrt{41}}{2(1+\sqrt{3})}$
$\mathbb{Q}(\sqrt{3},\sqrt{47})/\mathbb{Q}$	$\frac{7+\sqrt{47}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{71})/\mathbb{Q}$	$\frac{11+\sqrt{71}}{5(1+\sqrt{3})}$ oder $\frac{59+7\sqrt{71}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{79})/\mathbb{Q}$	$\frac{9+\sqrt{79}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{89})/\mathbb{Q}$	$\frac{11+\sqrt{89}}{4(1+\sqrt{3})}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.14.1 Satz. *Es sei p eine Primzahl, die den Kongruenzen $p \equiv 5(12)$ und $p \equiv \pm 3(8)$ genügt, d. h. es gelte $p \equiv 5(24)$. Bei der Erweiterung*

$$\mathbb{Q}(\sqrt{3}, \sqrt{p})/\mathbb{Q}$$

mit der Galoisgruppe $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ erweist sich die (-1)-te Kohomologiegruppe $H^{-1}(G, \mathbb{Q}(\sqrt{3}, \sqrt{p})^\times)$ dann als nicht-zyklisch. *Genauer gibt es $a, b, c, d, e \in \mathbb{Z}$, so dass die Gleichungen*

$$\begin{aligned} a^2 + \ \ b^2 - p \ \ &= 0 \\ 2c^2 + 3d^2 - pe^2 &= 0 \end{aligned} \tag{14}$$

erfüllt sind, und für derartige a, b, c, d, e sind

$$\frac{a + \sqrt{p}}{b}, \quad \frac{3d + d\sqrt{3} + e\sqrt{p} + e\sqrt{3p}}{2c} \tag{15}$$

Elemente von $K = \mathbb{Q}(\sqrt{3}, \sqrt{p})$ mit der Norm -1 über $\mathbb{Q}(\sqrt{3})$ bzw. über $\mathbb{Q}(\sqrt{p})$, die nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegen und sich auch nicht um einen Corand unterscheiden.

1.14.2 Zusatz. *Seien p wie in Satz 1.14.1 und $a, b, c, d, e \in \mathbb{Z}$, die* (14) *genügen. Nach dem Zusatz 1.12.2 zu Satz 1.12.1 sind unter den lokalen Erweiterungen genau*

$$\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2, \quad \mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

ebenfalls biquadratisch und das erste der Elemente (15) *von $\mathbb{Q}(\sqrt{3}, \sqrt{p})$ ist bei*

$$\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

auch weiterhin ein Element der Norm 1, das nicht zu den (-1)-Coräandern gehört, während es bei $\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2$ ein Corand wird. Das zweite der Elemente (15) *wird bei $\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3$ ein Corand, bei*

$$\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{3}, \sqrt{p})/\mathbb{Q}_p$$

hingegen nicht. In $\mathbb{Q}_p(\sqrt{3}, \sqrt{p})$ erzeugen die Elemente (15) *von $\mathbb{Q}(\sqrt{3}, \sqrt{p})$ dieselbe nicht-triviale Klasse.*

Beweis von Satz 1.14.1: Die Lösbarkeit der ersten der Gleichungen (14) ergibt sich aus dem Zerlegungsverhalten von p in $\mathbb{Q}(i)$, vgl. [N, S. 1]. Zur Lösbarkeit der zweiten der Gleichungen (14) ist Theorem 1.2 von LEGENDRE heranzuziehen. Für das zweite der Elemente (15) gilt

$$N_{K/\mathbb{Q}(\sqrt{p})}\left(\frac{3d + d\sqrt{3} + e\sqrt{p} + e\sqrt{3p}}{2c}\right) = \frac{(3d + e\sqrt{p})^2 - 3(d + e\sqrt{p})^2}{4c^2}$$

$$= \frac{9d^2 + pe^2 - 3d^2 - 3pe^2 + 2(3de - 3de)\sqrt{p}}{4c^2} = \frac{6d^2 - 2pe^2}{4c^2} = \frac{-4c^2}{4c^2} = -1.$$

Die Behauptung ergibt sich mit Korollar 1.9. Um zu zeigen, dass die angegebenen (-1)-Cozyklen sich nicht um einen (-1)-Corand unterscheiden, betrachte man die Situation bei einer der lokalen Erweiterungen $\mathbb{Q}_2(\sqrt{3}, \sqrt{p})/\mathbb{Q}_2$ und $\mathbb{Q}_3(\sqrt{3}, \sqrt{p})/\mathbb{Q}_3$. Dort wird eines der Elemente α, β zum Corand, das andere hingegen nicht. Da sich α und β bei der lokalen Erweiterung nicht um einen Corand unterscheiden, ist dies um so weniger bei der globalen Erweiterung der Fall. □

Beweis von Zusatz 1.14.2: Der Beweis des Zusatzes erfolgt unter Heranziehung von Satz 4.2, Korollar 1.9 und der Sätze 1.5, 1.6. □

1.14.3 Beispiele.[3]

Erweiterung	1. Element der Norm 1, das kein Corand ist	2. Element der Norm 1, das kein Corand ist (es liegt in einer anderen Klasse)
$\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$	$\frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}$
$\mathbb{Q}(\sqrt{3},\sqrt{29})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$	$\frac{9+3\sqrt{3}+\sqrt{29}+\sqrt{87}}{2}$ oder $\frac{9+\sqrt{3}+\sqrt{29}+3\sqrt{87}}{26}$
$\mathbb{Q}(\sqrt{3},\sqrt{53})/\mathbb{Q}$	$\frac{7+\sqrt{53}}{2}$ oder $182+25\sqrt{53}$	$\frac{3+\sqrt{3}+\sqrt{53}+\sqrt{159}}{10}$

[3]Wenn innerhalb einer Spalte mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese nur um Coränder.

1.15.1 Satz. *Sind p und q ungerade Primzahlen mit $p \equiv 1(4)$ und $(\frac{q}{p}) = -1$, so gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Es gibt $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$, und für derartige a und b ist

$$\frac{a + \sqrt{p}}{b} \tag{16}$$

ein Element von $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ mit der Norm -1 über $\mathbb{Q}(\sqrt{q})$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt.

1.15.2 Zusatz. *Seien p und q wie in Satz 1.15.1 und $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$. Unter den lokalen Erweiterungen sind dann*

$$\mathbb{Q}_p(\sqrt{p}, \sqrt{q})/\mathbb{Q}_p, \quad \mathbb{Q}_q(\sqrt{p}, \sqrt{q})/\mathbb{Q}_q$$

ebenfalls biquadratisch und das Element (16) *von $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ hat auch dort die Norm 1. Wie bei der globalen Erweiterung gehört es nicht zu den (-1)-Coräandern.*

1.15.3 Bemerkung. Unter den Voraussetzungen von Zusatz 1.15.2 ist in gewissen Fällen auch die lokale Erweiterung $\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2$ biquadratisch.

Beweis von Satz 1.15.1: Man diesen Satz beweist mit Hilfe von Korollar 1.9. □

Beweis von Zusatz 1.15.2: Der Beweis erfolgt unter Heranziehung von Satz 4.2, Korollar 1.9 und der Sätze 1.5, 1.6. □

1.15.3 Beispiele.[2]

Erweiterungen	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{5},\sqrt{7})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{13})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{17})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{23})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{37})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{43})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5},\sqrt{47})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$
$\mathbb{Q}(\sqrt{13},\sqrt{5})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{7})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{11})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{19})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{31})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{37})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{41})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{13},\sqrt{47})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$
$\mathbb{Q}(\sqrt{17},\sqrt{5})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{7})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{11})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{23})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{29})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{31})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{37})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{17},\sqrt{41})/\mathbb{Q}$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{29},\sqrt{11})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{17})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{19})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{31})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{37})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{41})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{43})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{29},\sqrt{47})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$
$\mathbb{Q}(\sqrt{37},\sqrt{5})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{13})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{17})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{19})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{23})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{29})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{31})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{37},\sqrt{43})/\mathbb{Q}$	$\frac{1+\sqrt{17}}{6}$ oder $6+\sqrt{37}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.15.3 Beispiele (Fortsetzung).

Erweiterungen	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{41},\sqrt{7})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{11})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{13})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{17})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{19})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{29})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{41},\sqrt{47})/\mathbb{Q}$	$\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$

1.16.1 Satz. *Es seien p und q Primzahlen, und zwar sei $p \equiv 3(8)$ und $q \equiv 7(8)$. Dann gilt Hilberts Satz 90* nicht *für die Erweiterung*

$$\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}.$$

Sei $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ und bezeichne G die Galoisgruppe von $K/\mathbb{Q}$. Es gibt Elemente $a, b, c, d \in \mathbb{Z}$, so dass die Gleichungen

$$\begin{aligned} p &= a^2 + 2b^2 \\ q &= c^2 - 2d^2 \end{aligned} \tag{17}$$

erfüllt sind, und für derartige a, b, c, d ist

$$\frac{\frac{a+\sqrt{p}}{b}}{\frac{c+\sqrt{q}}{d}} = \frac{d(a+\sqrt{p})}{b(c+\sqrt{q})} \tag{18}$$

ein Element von $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ mit der Norm -1 über $\mathbb{Q}(\sqrt{pq})$, das nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegt.

1.16.2 Zusatz. *Seien p und q wie in Satz 1.16.1 und $a, b, c, d \in \mathbb{Z}$, für die* (17) *erfüllt ist. Wenn $(\frac{q}{p}) = -1$ gilt, so sind unter den lokalen Erweiterungen genau*

$$\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{p}, \sqrt{q})/\mathbb{Q}_p$$

ebenfalls biquadratisch, und gilt $(\frac{q}{p}) = 1$, so sind es die Erweiterungen

$$\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2, \quad \mathbb{Q}_q(\sqrt{p}, \sqrt{q})/\mathbb{Q}_q.$$

In beiden Fällen bleibt das Element (18) *von $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ auch dort ein Element der Norm 1, das nicht zu den (-1)-Coründern gehört.*

Beweis von Satz 1.16.1: Ber Beweis erfolgt mit Hilfe von Korollar 1.9. □

Beweis von Zusatz 1.16.2: Diesen Zusatz beweist man unter Heranziehung von Satz 4.2, Korollar 1.9 und der Sätze 1.5, 1.6. □

1.16.3 Beispiele.[2]

Erweiterung	Element der Norm 1, das kein Corand ist
$\mathbb{Q}(\sqrt{7},\sqrt{11})/\mathbb{Q}$	$\frac{3+\sqrt{7}}{3+\sqrt{11}}$
$\mathbb{Q}(\sqrt{7},\sqrt{19})/\mathbb{Q}$	$\frac{3(3+\sqrt{7})}{1+\sqrt{19}}$ oder $\frac{3+\sqrt{7}}{13+3\sqrt{19}}$
$\mathbb{Q}(\sqrt{7},\sqrt{43})/\mathbb{Q}$	$\frac{3(3+\sqrt{7})}{5+\sqrt{43}}$ oder $\frac{3+\sqrt{7}}{59+9\sqrt{43}}$
$\mathbb{Q}(\sqrt{23},\sqrt{11})/\mathbb{Q}$	$\frac{5+\sqrt{23}}{3+\sqrt{11}}$
$\mathbb{Q}(\sqrt{23},\sqrt{19})/\mathbb{Q}$	$\frac{3(5+\sqrt{23})}{1+\sqrt{19}}$ oder $\frac{5+\sqrt{23}}{13+3\sqrt{19}}$
$\mathbb{Q}(\sqrt{23},\sqrt{43})/\mathbb{Q}$	$\frac{3(5+\sqrt{23})}{5+\sqrt{43}}$ oder $\frac{5+\sqrt{23}}{59+9\sqrt{43}}$
$\mathbb{Q}(\sqrt{31},\sqrt{11})/\mathbb{Q}$	$\frac{7+\sqrt{31}}{3(3+\sqrt{11})}$ oder $\frac{39+7\sqrt{31}}{3+\sqrt{11}}$
$\mathbb{Q}(\sqrt{31},\sqrt{19})/\mathbb{Q}$	$\frac{7+\sqrt{31}}{1+\sqrt{19}}$, $\frac{7+\sqrt{31}}{3(13+3\sqrt{19})}$, $\frac{3(39+7\sqrt{31})}{1+\sqrt{19}}$ oder $\frac{39+7\sqrt{31}}{13+3\sqrt{19}}$
$\mathbb{Q}(\sqrt{31},\sqrt{43})/\mathbb{Q}$	$\frac{7+\sqrt{31}}{5+\sqrt{43}}$, $\frac{7+\sqrt{31}}{3(59+9\sqrt{43})}$, $\frac{3(39+7\sqrt{31})}{5+\sqrt{43}}$ oder $\frac{39+7\sqrt{31}}{59+9\sqrt{43}}$
$\mathbb{Q}(\sqrt{47},\sqrt{11})/\mathbb{Q}$	$\frac{7+\sqrt{47}}{3+\sqrt{11}}$
$\mathbb{Q}(\sqrt{47},\sqrt{19})/\mathbb{Q}$	$\frac{3(7+\sqrt{47})}{1+\sqrt{19}}$ oder $\frac{7+\sqrt{47}}{13+3\sqrt{19}}$
$\mathbb{Q}(\sqrt{47},\sqrt{43})/\mathbb{Q}$	$\frac{3(7+\sqrt{47})}{5+\sqrt{43}}$ oder $\frac{7+\sqrt{47}}{59+9\sqrt{43}}$

[2]Wenn mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese wenn nicht anders gesagt nur um Coränder.

1.17.1 Satz. *Es seien p und q Primzahlen, die den Kongruenzen $p \equiv 5(8)$, $q \equiv 3(4)$ genügen und für die $(\frac{q}{p}) = -1$ gilt. Bei der Erweiterung*

$$\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$$

mit der Galoisgruppe $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ erweist sich die (-1)-te Kohomologiegruppe dann als nicht-*zyklisch. Genauer gibt es Elemente α und β von $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, so dass die Gleichungen*

$$\begin{aligned} N_{K/\mathbb{Q}(\sqrt{q})}\, \alpha &= -1 \\ N_{K/\mathbb{Q}(\sqrt{p})}\, \beta &= -1 \end{aligned} \tag{19}$$

gelten, doch wenn $\alpha, \beta \in K$ von dieser Art sind, so handelt es sich um Elemente der Norm 1 über $\mathbb{Q}$, die nicht in der Gruppe $B^{-1}(G, K^\times)$ der (-1)-Coränder liegen und die zudem unterschiedliche nicht-triviale Klassen von $H^{-1}(G, K^\times)$ erzeugen.

1.17.2 Zusatz. *Seien p und q wie in Satz 1.17.1 und $\alpha, \beta \in K$ mit* (19)*. Nach dem Zusatz 1.15.2 zu Satz 1.15.1 sind dann unter den lokalen Erweiterungen genau*

$$\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{p}, \sqrt{q})/\mathbb{Q}_p, \quad \mathbb{Q}_q(\sqrt{p}, \sqrt{q})/\mathbb{Q}_q$$

ebenfalls biquadratisch und das Element α von $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ ist bei

$$\mathbb{Q}_p(\sqrt{p}, \sqrt{q})/\mathbb{Q}_p, \quad \mathbb{Q}_q(\sqrt{p}, \sqrt{q})/\mathbb{Q}_q$$

auch weiterhin ein Element der Norm 1, das nicht zu den (-1)-Coräandern gehört, während es bei $\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2$ ein Corand wird. Das Element β von $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ wird bei $\mathbb{Q}_q(\sqrt{p}, \sqrt{q})/\mathbb{Q}_q$ ein Corand, bei

$$\mathbb{Q}_2(\sqrt{p}, \sqrt{q})/\mathbb{Q}_2, \quad \mathbb{Q}_p(\sqrt{p}, \sqrt{q})/\mathbb{Q}_p$$

hingegen nicht. In $\mathbb{Q}_p(\sqrt{p}, \sqrt{q})$ liegen α und β in derselben nicht-trivialen Klasse.

Beweis von Satz 1.17.1: Aufgrund der Voraussetzung $p \equiv 1(4)$ gibt es $d, e \in \mathbb{Z}$, so dass $p = d^2 + e^2$ (vgl. [N, S. 1]). Damit ist

$$\alpha = \frac{d + \sqrt{p}}{e}$$

ein Element von K mit der Norm -1 über $\mathbb{Q}(\sqrt{q})$. Auf der anderen Seite gibt es $a, b, c \in \mathbb{Z}$, für die

$$2qa^2 - b^2 - pc^2 = 0$$

zutrifft. Dies zeigt man mit Theorem 1.2 von Legendre, denn es gilt

$$\left(\frac{2q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{q}{p}\right) = (-1) \cdot (-1) = 1,$$

$$\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = (-1) \cdot (-1) = 1.$$

Liegen a, b, c dieser Art vor, so ist

$$\beta = \frac{qa^2 + bc\sqrt{p} + ab\sqrt{q} + ac\sqrt{pq}}{qa^2 - b^2}$$

ein Element von K mit der Norm -1 über $\mathbb{Q}(\sqrt{p})$, denn man verifiziert

$$N_{K/\mathbb{Q}(\sqrt{p})}\left(\frac{qa^2+bc\sqrt{p}+ab\sqrt{q}+ac\sqrt{pq}}{qa^2-b^2}\right)=\frac{(qa^2+bc\sqrt{p})^2-q(ab+ac\sqrt{p})^2}{(qa^2-b^2)^2}$$
$$=\frac{q^2a^4+pb^2c^2-qa^2b^2-pqa^2c^2+2(qa^2bc-qa^2bc)\sqrt{p}}{(qa^2-b^2)^2}$$
$$=\frac{q^2a^4+b^2(2qa^2-b^2)-qa^2b^2-qa^2(2qa^2-b^2)}{(qa^2-b^2)^2}$$
$$=\frac{q^2a^4+2qa^2b^2-b^4-qa^2b^2-2q^2a^4+qa^2b^2}{(qa^2-b^2)^2}=\frac{-q^2a^4+2qa^2b^2-b^4}{(qa^2-b^2)^2}=-1.$$

Mit Hilfe von Korollar 1.9 zeigt man, dass α und β keine Coränder sind: Aufgrund der Voraussetzung $(\frac{p}{q})=-1$ ist die quadratische Form

$$X_1^2+qX_1^2-pX_3^2$$

nicht isotrop, und es folgt, dass α kein Corand ist. Wegen $(\frac{q}{p})=-1$ ist

$$X_1^2+pX_1^2-qX_3^2$$

nicht isotrop und β kein Corand. Es bleibt zu zeigen, dass α/β oder $\alpha\beta$ kein Corand ist. Die Norm von α über $\mathbb{Q}(\sqrt{p})$ hat die Gestalt

$$\frac{m+n\sqrt{p}}{m-n\sqrt{p}}$$

mit $m,n\in\mathbb{Z}$. Hierbei ist $n\neq 0$, weil α kein Corand ist; weiter kann man o. E. davon ausgehen, dass m und n teilerfremd seien. Die quadratische Form

$$X_1^2+\left(p-\left(\frac{m}{n}\right)^2\right)X_2^2-qX_3^2$$

ist nach Satz 1.8 nicht isotrop, oder äquivalent dazu ist

$$X_1^2-(m^2-pn^2)X_2^2-qX_3^2 \tag{20}$$

nicht isotrop. Die Norm von α/β (und $\alpha\beta$) über $\mathbb{Q}(\sqrt{p})$ ist

$$-\frac{m+n\sqrt{p}}{m-n\sqrt{p}}=\frac{pn+m\sqrt{p}}{pn-m\sqrt{p}},$$

so dass α/β nach Satz 1.8 genau dann Corand ist, wenn die quadratische Form

$$X_1^2+\left(p-\left(\frac{pn}{m}\right)^2\right)X_2^2-qX_3^2$$

isotrop ist. Das ist genau dann der Fall, wenn

$$X_1^2+p(m^2-pn^2)X_2^2-qX_3^2 \tag{21}$$

isotrop ist. Weil die quadratische Form (20) nicht isotrop ist und weiter $(\frac{-p}{q})=1$ gilt, kann man sich nun mit Theorem 1.2 von Legendre überlegen, dass auch die quadratische Form (21) nicht isotrop ist. Dabei wird benötigt, dass m^2-pn^2 nicht durch q teilbar ist. Angenommen, das Gegenteil sei der Fall. Weil m und n prim zueinander sind, sind sie dann auch jeweils prim zu q. Dann wäre aber p ein quadratsicher Rest modulo q im Widerspruch zur Voraussetzung $(\frac{p}{q})=-1$. Demnach sind $\alpha\beta$ und α/β wie behauptet keine Coränder. □

Beweis von Zusatz 1.17.2: Der Beweis erfolgt durch Anwendung von Satz 4.2, Korollar 1.9 und der Sätze 1.5, 1.6. Wir wollen nur kurz eine Begründung dafür geben, warum α und β in $\mathbb{Q}_p(\sqrt{p},\sqrt{q})$ zur selben nicht-trivialen Klasse gehören. Da α bei der Erweiterung $\mathbb{Q}_p(\sqrt{p},\sqrt{q})/\mathbb{Q}_p$ kein Corand ist, folgt mit Satz 1.8 dass die quadratische Form (20) über $\mathbb{Q}_p$ nicht isotrop ist. Nach Satz 1.1 gilt also

$$\Big(\frac{m^2-pn^2,q}{p}\Big)=-1.$$

Andererseits ist α/β nach Satz 1.8 genau dann ein Corand bei $\mathbb{Q}_p(\sqrt{p},\sqrt{q})/\mathbb{Q}_p$, wenn die quadratische Form (20) über $\mathbb{Q}_p$ isotrop ist. Dies ist der Fall, denn es gilt

$$\Big(\frac{-p(m^2-pn^2),q}{p}\Big)=\Big(\frac{-p,q}{p}\Big)\Big(\frac{m^2-pn^2,q}{p}\Big)=\Big(\frac{-p,q}{p}\Big)\cdot(-1)$$
$$=\Big(\frac{p,q}{p}\Big)\cdot(-1)=\Big(\frac{q}{p}\Big)\cdot(-1)=(-1)\cdot(-1)=1.$$

Anders als im globalen Fall liegen die (-1)-Cozyklen α und β hier also in derselben nicht-trivialen Klasse. □

1.17.3 Beispiele.[3]

Erweiterung	1. Element der Norm 1, das kein Corand ist	2. Element der Norm 1, das kein Corand ist (es liegt in einer anderen Klasse)
$\mathbb{Q}(\sqrt{5},\sqrt{7})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$, $2+\sqrt{5}$	$\frac{7+3\sqrt{5}+3\sqrt{7}+\sqrt{35}}{2}$
$\mathbb{Q}(\sqrt{5},\sqrt{23})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$, $2+\sqrt{5}$	$\frac{23+5\sqrt{5}+5\sqrt{23}+\sqrt{115}}{6}$, $\frac{23+3\sqrt{5}+\sqrt{23}+3\sqrt{115}}{22}$
$\mathbb{Q}(\sqrt{5},\sqrt{43})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$, $2+\sqrt{5}$	$\frac{43+9\sqrt{5}+9\sqrt{43}+\sqrt{215}}{38}$
$\mathbb{Q}(\sqrt{5},\sqrt{47})/\mathbb{Q}$	$\frac{1+\sqrt{5}}{2}$, $2+\sqrt{5}$	$\frac{47+21\sqrt{5}+7\sqrt{47}+3\sqrt{235}}{2}$
$\mathbb{Q}(\sqrt{13},\sqrt{7})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$, $18+5\sqrt{13}$	$\frac{7+\sqrt{7}+\sqrt{13}+\sqrt{91}}{6}$
$\mathbb{Q}(\sqrt{13},\sqrt{11})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$, $18+5\sqrt{13}$	$\frac{11+3\sqrt{11}+3\sqrt{13}+\sqrt{143}}{2}$
$\mathbb{Q}(\sqrt{13},\sqrt{19})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$, $18+5\sqrt{13}$	$\frac{19+5\sqrt{13}+5\sqrt{19}+\sqrt{247}}{6}$
$\mathbb{Q}(\sqrt{13},\sqrt{31})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$, $18+5\sqrt{13}$	$\frac{31+7\sqrt{13}+7\sqrt{31}+\sqrt{403}}{18}$
$\mathbb{Q}(\sqrt{13},\sqrt{47})/\mathbb{Q}$	$\frac{3+\sqrt{13}}{2}$, $18+5\sqrt{13}$	$\frac{47+9\sqrt{13}+9\sqrt{47}+\sqrt{611}}{34}$
$\mathbb{Q}(\sqrt{29},\sqrt{11})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$, $70+13\sqrt{29}$	$\frac{11+3\sqrt{11}+3\sqrt{29}+\sqrt{319}}{6}$
$\mathbb{Q}(\sqrt{29},\sqrt{19})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$, $70+13\sqrt{29}$	$\frac{19+3\sqrt{19}+3\sqrt{29}+\sqrt{551}}{10}$
$\mathbb{Q}(\sqrt{29},\sqrt{31})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$, $70+13\sqrt{29}$	$\frac{31+7\sqrt{29}+7\sqrt{31}+\sqrt{899}}{6}$
$\mathbb{Q}(\sqrt{29},\sqrt{43})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$, $70+13\sqrt{29}$	$\frac{43+13\sqrt{29}+13\sqrt{43}+\sqrt{1247}}{42}$
$\mathbb{Q}(\sqrt{29},\sqrt{47})/\mathbb{Q}$	$\frac{5+\sqrt{29}}{2}$, $70+13\sqrt{29}$	$\frac{47+7\sqrt{29}+7\sqrt{47}+\sqrt{1363}}{6}$

[3]Wenn innerhalb einer Spalte mehrere (-1)-Cozyklen angegeben sind, so unterscheiden sich diese nur um Coränder.

1.17.3 Beispiele (Fortsetzung).

Erweiterung	1. Element der Norm 1, das kein Corand ist	2. Element der Norm 1, das kein Corand ist (es liegt in einer anderen Klasse)
$\mathbb{Q}(\sqrt{37},\sqrt{19})/\mathbb{Q}$	$\frac{1+\sqrt{37}}{6}$, $6+\sqrt{37}$	$\frac{19+\sqrt{19}+\sqrt{37}+\sqrt{703}}{18}$
$\mathbb{Q}(\sqrt{37},\sqrt{23})/\mathbb{Q}$	$\frac{1+\sqrt{37}}{6}$, $6+\sqrt{37}$	$\frac{23+3\sqrt{23}+3\sqrt{37}+\sqrt{851}}{14}$
$\mathbb{Q}(\sqrt{37},\sqrt{31})/\mathbb{Q}$	$\frac{1+\sqrt{37}}{6}$, $6+\sqrt{37}$	$\frac{31+5\sqrt{31}+5\sqrt{37}+\sqrt{1147}}{6}$
$\mathbb{Q}(\sqrt{37},\sqrt{43})/\mathbb{Q}$	$\frac{1+\sqrt{37}}{6}$, $6+\sqrt{37}$	$\frac{43+7\sqrt{37}+7\sqrt{43}+\sqrt{1591}}{6}$

2. Berechnung von $H^{-1}(G, K^\times)$ in einigen expliziten Fällen

Sei K/k eine endliche galoissche Erweiterung mit Gruppe G. Im vorangegangenen Kapitel haben wir festgestellt, dass die Gruppe $H^{-1}(G, K^\times)$ für $k = \mathbb{Q}$ oder $k = \mathbb{Q}_p$ mit einer Primzahl p in vielen Fällen nicht-trivial ausfällt, wenn $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ gilt. Desweiteren konnten wir zeigen, dass unter gewissen Voraussetzungen die Gruppe $H^{-1}(G, K^\times)$ bei biquadratischen Erweiterungen über $\mathbb{Q}$ nicht einmal zyklisch ist. In diesem Kapitel werden wir die Gruppe $H^{-1}(G, K^\times)$ in einigen Fällen explizit berechnen. Auf jeden Fall ist $H^{-1}(G, K^\times)$ für Erweiterungen globaler Körper stets endlich. Beim Beweis spielt eine Rolle, dass die erste Homologiegruppe $H_1(G, \mathfrak{C}_K)$ der Divisorenklassengruppe $\mathfrak{C}_K$ endlich ist. Wenn K ein algebraischer Zahlkörper der Klassenzahl 1 ist, so ist $\mathfrak{C}_K = 1$ und damit auch $H_1(G, \mathfrak{C}_K)$ trivial. Unter dieser Voraussetzung aber wird jede Klasse von $H^{-1}(G, K^\times)$ durch ein Element der Einheitengruppe E_K repräsentiert. Diese Tatsache wird in gewissen Fällen die vollständige Bestimmung der Gruppe $H^{-1}(G, K^\times)$ ermöglichen.

2.i Zur Endlichkeit von $H^{-1}(G, K^\times)$ im Falle globaler Körper

Bei dem Beweis, dass $H^{-1}(G, K^\times)$ für galoissche Erweiterungen globaler Körper endlich ist, werden wir von der Fundamentalsequenz der algebraischen Zahlentheorie

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow \mathfrak{I}_K \longrightarrow \mathfrak{C}_K \longrightarrow 1$$

ausgehen (vgl. [AZ, S. 13]). Wir werden die Endlichkeit von $H^{-1}(G, K^\times)$ auf die Endlichkeit der Gruppen $H^{-1}(G, E_K)$, $H^{-2}(G, \mathfrak{C}_K)$ und $H^{-1}(G, \mathfrak{I}_K)$ zurückführen. Zur späteren expliziten Berechnung von $H^{-1}(G, K^\times)$ benötigen wir jedoch eine stärkere Aussage, die wir bereits an dieser Stelle formulieren wollen.

2.1 Satz. *Für jede galoissche Erweiterung K/k globaler Zahlkörper mit der Gruppe $G = G(K/k)$ ist die (-1)-te Kohomologiegruppe*

$$H^{-1}(G, \mathfrak{I}_K)$$

der Divisorengruppe $\mathfrak{I}_K$ von K trivial.

Dieser Satz wird gewöhnlich unter Heranziehung des Lemmas von Shapiro bewiesen. Hierauf wollen wir an dieser Stelle verzichten, um stattdessen einen anderen Beweis für algebraische Zahlkörper anzugeben. Es ist der Zahkörperfall, der uns im weiteren Verlauf des Kapitels noch interessieren wird.

Beweis von Satz 2.1: Es sei $\mathfrak{a} \in I_K$ ein Divisor mit der G-Norm 1 und für diesen gelte $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r \, (\mathfrak{q}_1 \dots \mathfrak{q}_s)^{-1}$ mit Primidealen $\mathfrak{p}_i$ und $\mathfrak{q}_j$ von K. Dann folgt

$$1 = \prod_{\sigma \in G} \left(\frac{\mathfrak{p}_1 \dots \mathfrak{p}_r}{\mathfrak{q}_1 \dots \mathfrak{q}_s} \right)^\sigma = \prod_{\sigma \in G} \frac{\mathfrak{p}_1^\sigma \dots \mathfrak{p}_r^\sigma}{\mathfrak{q}_1^\sigma \dots \mathfrak{q}_s^\sigma}$$

und Multiplikation mit den Nennern $\mathfrak{q}_1^\sigma \dots \mathfrak{q}_s^\sigma$ für $\sigma \in G$ ergibt

$$\prod_{\sigma \in G} \mathfrak{p}_1^\sigma \cdots \prod_{\sigma \in G} \mathfrak{p}_r^\sigma = \prod_{\sigma \in G} \mathfrak{q}_1^\sigma \cdots \prod_{\sigma \in G} \mathfrak{q}_s^\sigma. \tag{1}$$

Aufgrund der eindeutigen Primidealzerlegung von Idealen des Ganzheitsringes $\mathcal{O}_K$ (vgl. [AZ, S. 41/42]) gilt $r = s$; nach eventueller Umnummerierung der $\mathfrak{q}_i$ kann o. E. von $\mathfrak{p}_1 = \mathfrak{q}_1^{\sigma_1}$ für ein $\sigma_1 \in G$ ausgegangen werden. Bildung der G-Norm liefert

$$\prod_{\sigma \in G} \mathfrak{p}_1^\sigma = \prod_{\sigma \in G} \mathfrak{q}_1^\sigma,$$

so dass sich diese beiden Faktoren in Gleichung (1) gegenseitig aufheben. Induktiv folgt $\mathfrak{p}_i = \mathfrak{q}_i^{\sigma_i}$ für gewisse $\sigma_i \in G$ $(i = 2, \ldots, n)$ bei geeigneter Nummerierung der $\mathfrak{q}_i$. Also gilt

$$\mathfrak{a} = \frac{\mathfrak{p}_1 \ldots \mathfrak{p}_r}{\mathfrak{q}_1 \ldots \mathfrak{q}_s} = \frac{\mathfrak{q}_1^{\sigma_1} \ldots \mathfrak{q}_r^{\sigma_r}}{\mathfrak{q}_1 \ldots \mathfrak{q}_r}$$

und $H^{-1}(G, \mathfrak{I}_K)$ ist wie behauptet trivial. □

Wir kommen jetzt zu einer Hilfsbehauptung, die wir bei dem Beweis verwenden werden, dass die Gruppe $H^{-1}(G, E_K)$ endlich ist.

2.2 Lemma. *Jede Untergruppe B einer endlich erzeugten abelschen Gruppe A ist endlich erzeugt. Für die Minimalzahlen $r(A)$ bzw. $r(B)$ von Erzeugendensystemen von A bzw. B gilt $r(B) \leq r(A)$.*

Beweis: Sei $r = r(A)$. Dann gibt es einen Epimorphismus

$$p : F \longrightarrow A,$$

wobei F ein freier $\mathbb{Z}$-Modul in r Erzeugenden ist. Sei F' das Urbild von B unter p. Nun ist F' als Untergruppe von F ebenfalls endlich erzeugt mit

$$r(F') \leq r(F) \leq r,$$

denn jede Untergruppe von $\mathbb{Z}^r$ ist isomorph zu $\mathbb{Z}^d$ mit einem $d \leq r$, vgl. [A1, S. 198].[1] Als homomorphes Bild von F' ist also auch B endlich erzeugt, und es gilt

$$r(B) \leq r(F').$$

Zusammen mit der ersten Ungleichung folgt

$$r(B) \leq r = r(A),$$

was zu zeigen war. □

Um die Endlichkeit von $H^{-2}(G, \mathfrak{C}_K)$ zu zeigen, werden wir die folgende Aussage benötigen.

2.3 Lemma. *Sei G eine endliche Gruppe. Für einen endlich erzeugten G-Modul M sind die Homologiegruppen $H_p(G, M)$ für alle $p \geq 0$ endlich.*

Beweis: Ist E ein Erzeugendensystem von M über $\mathbb{Z}G$, so stellt

$$\{gm | g \in G, m \in E\}$$

ein Erzeugendensystem von M über $\mathbb{Z}$ dar. Also ist M eine endlich erzeugte abelsche Gruppe. Die Gruppen $H_p(G, M)$ erhält man wie folgt. Eine projektive Auflösung von $\mathbb{Z}$ über $\mathbb{Z}G$ ist eine exakte G-Sequenz

$$\ldots \longrightarrow F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

wobei alle F_i projektive $\mathbb{Z}G$-Moduln sind. Der G-Komplex

$$F : \quad \cdots \to F_2 \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0$$

[1] Genauer ist in der zweiten Ungleichung $r(F) = r$, aber darauf kommt es hier nicht an.

ergibt mit M über $\mathbb{Z}G$ tensoriert den Komplex

$$F \otimes_G M: \ \cdots \to F_2 \otimes_G M \longrightarrow F_1 \otimes_G M \longrightarrow F_0 \otimes_G M$$

von abelschen Gruppen. Für alle $p \geq 0$ ist

$$H_p(G, M) = H_p(F \otimes_G M),$$

vgl. [B, S. 56]. Eine mögliche Wahl von F ist die Standardauflösung von $\mathbb{Z}$ über $\mathbb{Z}G$ (s. [B, S. 18]), bei der F_p die von den $(g_0, \ldots, g_p) \in G^{p+1}$ erzeugte freie abelsche Gruppe mit der Operation $g(g_0, \ldots, g_p) = (gg_0, \ldots, gg_p)$ ist. Die Randabbildung $\partial_p : F_p \to F_{p-1}$ hat die Gestalt $\partial_p = \sum_{i=0}^{p} (-1)^i \partial_i$ mit

$$\partial_i(g_0, \ldots, g_p) = (g_0, \ldots, \hat{g}_i, \ldots, g_p);$$

hierbei bedeutet $\hat{g}_i$, dass die Komponente g_i ausgelassen wird. Die Augmentation $\varepsilon : F_0 \to \mathbb{Z}$ ist durch $\varepsilon(1) = 1$ gegeben. Jedes Element von $F_p \otimes_G M$ ist Summe von Produkten vom Typ

$$(g_0, g_1, \ldots, g_p) \otimes m = (1, g_0^{-1} g_1, \ldots, g_0^{-1} g_p) \otimes (g_0 m)$$

mit $(g_0, g_1, \ldots, g_p) \in G^{p+1}$ und $m \in M$. Es gibt endlich viele $m_1, \ldots, m_r \in M$, die M über $\mathbb{Z}$ erzeugen. Damit wird $F_p \otimes_G M$ als abelsche Gruppe von den

$$(1, g_0^{-1} g_1, \ldots, g_0^{-1} g_n) \otimes m_i$$

erzeugt und das sind $n^p \cdot r$ Elemente, wenn n die Ordnung von G bezeichnet. Als Untergruppe von $F_p \otimes_G M$ ist nach Lemma 2.2 dann auch $C_p(F \otimes M)$ endlich erzeugt. Es folgt die Endlichkeit von

$$H_p(G, M) = C_p(F \otimes M)/B_p(F \otimes M),$$

denn $H_p(G, M)$ ist eine Gruppe vom Exponenten n, s. [Ws, S. 89]. □

Wie bereits angedeutet kommen wir nun zu

2.4 Lemma. *Für jede galoissche Erweiterung K/k globaler Körper mit der Gruppe $G = G(K/k)$ ist die (-1)-te Kohomologiegruppe $H^{-1}(G, E_K)$ der Einheitengruppe E_K* endlich.

Beweis: Zuerst der Zahlkörperfall. Es bezeichne r die Anzahl der reellen und s die Anzahl der komplexen Stellen von K. Nach dem *Dirichletschen Einheitensatz* (vgl. [AZ, S. 63/64]) gilt

$$E_K \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$$

mit der Gruppe $\mu(K)$ der Einheitswurzeln in K. Da $H^{-1}(G, E_K)$ den Exponenten $n = K : k = r + 2s$ hat (vgl. [AW, S. 105], [AZ, S. 73/74]), liefert Anwendung von Lemma 2.2 für die Ordnung von $H^{-1}(G, E_K)$ die Abschätzung

$$\left|H^{-1}(G, E_K)\right| \leq n \cdot n^{r+s-1} = n^{r+s}.$$

Im Funktionenkörperfall bezeichne κ den Konstantenkörper von K. Es gilt

$$E_K = \kappa^{\times}$$

und κ ist endlich, so dass auch $H^{-1}(G, E_K)$ endlich ist. □

Im folgenden benötigen wir die Endlichkeit von $H^{-2}(G, \mathfrak{C}_K)$. Allgemeiner zeigen wir

2.5 Lemma. *Für jede galoissche Erweiterung K/k globaler Körper mit der Gruppe $G = G(K/k)$ sind die Homologiegruppen $H_p(G, \mathfrak{C}_K)$ der Divisorenklassengruppe $\mathfrak{C}_K$ für alle $p \geq 0$ endlich.*

Beweis: Im Zahlkörperfall ist $\mathfrak{C}_K$ die Klassengruppe von K; diese ist endlich (vgl. [AZ, S. 12/13]) und mit Lemma 2.3 folgt, dass auch die Gruppen $H_p(G, \mathfrak{C}_K)$ endlich sind.

Im Funktionenkörperfall ist $\mathfrak{C}_K$ unendlich, die Gruppe $\mathfrak{H}_K$ der Hauptdivisoren ist in der Gruppe $\mathfrak{I}_K^0$ der Divisoren vom Grad 0 enthalten und die Klassengruppe

$$\mathfrak{C}_K^0 = \mathfrak{I}_K^0/\mathfrak{H}_K$$

ist endlich (vgl. [AZ, S. 13/14], [AZ, S. 16]). Wegen der Inklusion $\mathfrak{H}_K \subset \mathfrak{I}_K^0$ wird durch die surjektive Gradabbildung $\mathfrak{I}_K \to \mathbb{Z}$ (vgl. [AZ, S. 166]) ein surjektiver Homomorphismus $\mathfrak{C}_K \to \mathbb{Z}$ bestimmt. Die kurze exakte G-Sequenz

$$0 \longrightarrow \mathfrak{C}_K^0 \longrightarrow \mathfrak{C}_K \longrightarrow \mathbb{Z} \longrightarrow 0$$

vermittelt die exakte Sequenz der Homologiegruppen

$$H_p(G, \mathfrak{C}_K^0) \longrightarrow H_p(G, \mathfrak{C}_K) \longrightarrow H_p(G, \mathbb{Z}),$$

vgl. [B, S. 71]. An dieser ist zu erkennen, dass

$$|H_p(G, \mathfrak{C}_K)| \leq \left|H_p(G, \mathfrak{C}_K^0)\right| \cdot |H_p(G, \mathbb{Z})|$$

gilt. Weil hierbei $\mathfrak{C}_K^0$ endlich und $\mathbb{Z}$ endlich erzeugt ist, folgt mit Lemma 2.3, dass die Homologiegruppen $H_p(G, \mathfrak{C}_K^0)$ und $H_p(G, \mathbb{Z})$ endlich sind. Also ist auch $H_p(G, \mathfrak{C}_K)$ endlich. □

Nach den vorbereitenden Aussagen über die Endlichkeit von $H^{-1}(G, E_K)$ sowie der Homologie von $\mathfrak{C}_K$ können wir den folgenden Satz formulieren.

2.6 Satz. *Für jede galoissche Erweiterung K/k globaler Körper mit der Gruppe $G = G(K/k)$ ist die (-1)-te Kohomologiegruppe $H^{-1}(G, K^\times)$ endlich.*

Beweis: Die kurze exakte G-Sequenz

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow K^\times/E_K \longrightarrow 1$$

vermittelt die exakte Sequenz der Kohomologiegruppen

$$H^{-1}(G, E_K) \longrightarrow H^{-1}(G, K^\times) \longrightarrow H^{-1}(G, K^\times/E_K), \tag{2}$$

vgl. [AW, S. 102] oder [B, S. 136]. Dabei ist $H^{-1}(G, E_K)$ nach Lemma 2.4 endlich; weiter erweist sich auch $H^{-1}(G, K^\times/E_K)$ als endlich. Dazu betrachte man die kurze exakte G-Sequenz

$$1 \longrightarrow K^\times/E_K \longrightarrow \mathfrak{I}_K \longrightarrow \mathfrak{C}_K \longrightarrow 1,$$

vgl. [AZ, S. 13]. Ein Stück der zugehörigen langen exakten Kohomologiesequenz (vgl. [AW, S. 102] oder [B, S. 136]) ist die Sequenz

$$H^{-2}(G, \mathfrak{C}_K) \longrightarrow H^{-1}(G, K^\times/E_K) \longrightarrow H^{-1}(G, \mathfrak{I}_K).$$

Gemäß Lemma 2.5 ist die Gruppe $H^{-2}(G, \mathfrak{C}_K) = H_1(G, \mathfrak{C}_K)$ endlich und nach Satz 2.1 gilt $H^{-1}(G, \mathfrak{I}_K) = 1$; es folgt

$$|H^{-1}(G, K^\times/E_K)| \leq |H^{-2}(G, \mathfrak{C}_K)|.$$

Aufgrund der exakten Sequenz (2) erhält man die Ungeleichung

$$\left|H^{-1}(G, K^\times)\right| \leq \left|H^{-1}(G, E_K)\right| \cdot \left|H^{-1}(G, K^\times/E_K)\right|,$$

woraus sich die Abschätzung

$$\left|H^{-1}(G, K^\times)\right| \leq \left|H^{-1}(G, E_K)\right| \cdot \left|H^{-2}(G, \mathfrak{C}_K)\right|$$

ergibt. Insbesondere ist $H^{-1}(G, K^\times)$ endlich. □

Für die spätere explizite Berechnung von $H^{-1}(G, K^\times)$ benötigen wir den folgenden Satz.

2.7 Satz. *Sei K/k eine galoissche Erweiterung algebraischer Zahlkörper mit der Gruppe $G = G(K/k)$. Der durch die Inklusion $E_K \subset K^\times$ der Einheitengruppe E_K vermittelte Homomorphismus*

$$H^{-1}(G, E_K) \longrightarrow H^{-1}(G, K^\times)$$

ist surjektiv, *wenn K die Klassenzahl 1 hat.*

Beweis: Zu K gehört die kanonische exakte G-Sequenz

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow \mathfrak{I}_K \longrightarrow \mathfrak{C}_K \longrightarrow 1$$

(vgl. [AZ, S. 13]); weil $\mathfrak{C}_K = 1$ ist, erhält man die kurze exakte G-Sequenz

$$1 \longrightarrow E_K \longrightarrow K^\times \longrightarrow \mathfrak{I}_K \longrightarrow 1.$$

Es folgt die Exaktheit der Sequenz der Kohomologiegruppen

$$H^{-1}(G, E_K) \longrightarrow H^{-1}(G, K^\times) \longrightarrow H^{-1}(G, \mathfrak{I}_K)$$

(vgl. [AW, S. 102] oder [B, S. 136]), und nach Satz 2.1 gilt $H^{-1}(G, \mathfrak{I}_K) = 1$. □

Eine äquivalente Formulierung dieses Satzes lautet, dass jeder (-1)-Cozykel sich nur um einen (-1)-Corand von einer Einheit von K unterscheidet, wenn K die Klassenzahl 1 hat.

2.ii Minkowski-Schranken biquadratischer Erweiterungskörper von $\mathbb{Q}$

Für einen algebraischen Zahlkörper K bezeichne d_K die Diskriminante von K. Es sei s die Anzahl der komplexen Stellen von K und $n = K : k$. Dann ist

$$m_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_k|^{\frac{1}{2}}$$

die Minkowski-Schranke von K, vgl. [AZ, S. 87]. Dabei ist die Diskriminante d_K per Definition die Diskriminante einer Ganzheitsbasis von K, vgl. [AZ, S. 49]. Wir wollen in diesem Abschnitt die Minkowski-Schranken biquadratischer Erweiterungskörper von $\mathbb{Q}$ berechnen, indem wir Ganzheitsbasen angeben und deren Diskriminanten ermitteln.

2.8 Satz. *Es seien a und b quadratfreie und teilerfremde ganze Zahlen, wobei $a \equiv 1(4)$, $a \neq 1$ und $b \not\equiv 1(4)$. Dann ist die Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ biquadratisch und*

$$1, \quad \frac{1+\sqrt{a}}{2}, \quad \sqrt{b}, \quad \frac{1+\sqrt{a}}{2}\sqrt{b}$$

ist eine Ganzheitsbasis des algebraischen Zahlkörpers $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, wobei $\sqrt{a}$ und $\sqrt{b}$ Wurzeln von a bzw. b bezeichnen. Weiter ist

$$d_K = (4 \cdot a \cdot b)^2$$

die Diskriminante von K.

Beweis: Die angegeben Basiselemente sind ganz, vgl. [AZ, S. 49/50]. Sei nun

$$\alpha = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{ab}$$

mit rationalen Zahlen x, y, z, t ein beliebiges ganzes Element von K, wobei $\sqrt{ab}$ eine Wurzel von ab bezeichne. Die Spur von α über jedem der Zwischenkörper von $K/\mathbb{Q}$ ist ebenfalls ganz, weil die Konjugierten von α sowie Summen von ganzen Elementen ganz sind, vgl. [AZ, S.17/18]. Also liegen die Spuren

$$S_{K/\mathbb{Q}(\sqrt{a})}\alpha = 2x + 2y\sqrt{a}$$
$$S_{K/\mathbb{Q}(\sqrt{ab})}\alpha = 2x + 2t\sqrt{ab}$$

von α über $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{ab})$ im Ganzheitsring des jeweils betrachteten Zwischenkörpers, was umgeformt die Inklusionen

$$2x - 2y + 4y\frac{1+\sqrt{a}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{a}}{2}$$
$$2x + 2t\sqrt{ab} \in \mathbb{Z} + \mathbb{Z}\sqrt{ab}$$

liefert, vgl. [AZ, S.49/50]. Aus ihnen folgt

$$2x - 2y \in \mathbb{Z}, \quad 2x \in \mathbb{Z}, \quad 2t \in \mathbb{Z}$$

und weiter

$$2y = 2x - (2x - 2y) \in \mathbb{Z}.$$

Es sei jetzt

$$\alpha = x' + y'\frac{1+\sqrt{a}}{2} + z'\sqrt{b} + t'\frac{1+\sqrt{a}}{2}\sqrt{b}$$

mit $x', y', z', t' \in \mathbb{Q}$ die Darstellung von α bzgl. der obigen Basis, die als Ganzheitsbasis von K zu erweisen ist. Zu zeigen ist, dass die Koeffizienten x', y', z', t' bereits in $\mathbb{Z}$ liegen. Wir formen die Gleichung zu

$$\alpha = \left(x' + \frac{y'}{2}\right) + \frac{y'}{2}\sqrt{a} + \left(z' + \frac{t'}{2}\right)\sqrt{b} + \frac{t'}{2}\sqrt{a}\sqrt{b}$$

um. Auf die oben beschriebene Art erhält man dann

$$2 \cdot \frac{y'}{2} \in \mathbb{Z}, \quad 2 \cdot \frac{t'}{2} \in \mathbb{Z}$$

und aus $y', t' \in \mathbb{Z}$ folgt, dass

$$y'\frac{1+\sqrt{a}}{2} + t'\frac{1+\sqrt{a}}{2}\sqrt{b}$$

ein ganzes Element von K ist. Damit ist auch

$$x' + z'\sqrt{b} = \alpha - \left(y' \frac{1+\sqrt{a}}{2} + t' \frac{1+\sqrt{a}}{2}\sqrt{b} \right)$$

ganz, was genau dann der Fall ist, wenn x' und z' in $\mathbb{Z}$ liegen. Also liegt jeder der Koeffizienten x', y', z', t' in $\mathbb{Z}$. Der Ganzheitsring $\mathcal{O}_K$ von $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ ist also in

$$\mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{a}}{2} + \mathbb{Z}\sqrt{b} + \mathbb{Z}\,\frac{1+\sqrt{a}}{2}\,\sqrt{b}$$

enthalten. Die umgekehrte Inklusion ist klar, da die vier Basiselemente wie gesagt ganz sind.

Die Diskriminante von K kann für jede Ganzheitsbasis $\beta_1, \beta_2, \beta_3, \beta_4$ von K mittels der Formel

$$d_K = \det \left(S_{K/\mathbb{Q}}(\beta_i \beta_j) \right)_{i,j=1,\ldots,4}$$

berechnet werden, vgl. [AZ, S. 47ff]. Einsetzen der obigen Basis liefert

$$d_K = \begin{vmatrix} S\,1 & S\left(\frac{1+\sqrt{a}}{2}\right) & S\left(\sqrt{b}\right) & S\left(\frac{1+\sqrt{a}}{2}\sqrt{b}\right) \\ S\left(\frac{1+\sqrt{a}}{2}\right) & S\left(\left(\frac{1+\sqrt{a}}{2}\right)^2\right) & S\left(\frac{1+\sqrt{a}}{2}\sqrt{b}\right) & S\left(\left(\frac{1+\sqrt{a}}{2}\right)^2\sqrt{b}\right) \\ S\left(\sqrt{b}\right) & S\left(\frac{1+\sqrt{a}}{2}\sqrt{b}\right) & S\,b & S\left(\frac{1+\sqrt{a}}{2}\,b\right) \\ S\left(\frac{1+\sqrt{a}}{2}\sqrt{b}\right) & S\left(\left(\frac{1+\sqrt{a}}{2}\right)^2\sqrt{b}\right) & S\left(\frac{1+\sqrt{a}}{2}\,b\right) & S\left(\left(\frac{1+\sqrt{a}}{2}\right)^2 b\right) \end{vmatrix}$$

$$= \begin{vmatrix} S\,1 & S\left(\frac{1+\sqrt{a}}{2}\right) & S\left(\sqrt{b}\right) & S\left(\frac{\sqrt{b}+\sqrt{a}\sqrt{b}}{2}\right) \\ S\left(\frac{1+\sqrt{a}}{2}\right) & S\left(\frac{1+a+2\sqrt{a}}{4}\right) & S\left(\frac{\sqrt{b}+\sqrt{a}\sqrt{b}}{2}\right) & S\left(\frac{(1+a)\sqrt{b}+2\sqrt{a}\sqrt{b}}{4}\right) \\ S\left(\sqrt{b}\right) & S\left(\frac{\sqrt{b}+\sqrt{a}\sqrt{b}}{2}\right) & S\,b & S\left(\frac{b+b\sqrt{a}}{2}\right) \\ S\left(\frac{\sqrt{b}+\sqrt{a}\sqrt{b}}{2}\right) & S\left(\frac{(1+a)\sqrt{b}+2\sqrt{a}\sqrt{b}}{4}\right) & S\left(\frac{b+b\sqrt{a}}{2}\right) & S\left(\frac{(1+a)b+2b\sqrt{a}}{4}\right) \end{vmatrix}$$

$$= \begin{vmatrix} 4 & 2 & 0 & 0 \\ 2 & 1+a & 0 & 0 \\ 0 & 0 & 4b & 2b \\ 0 & 0 & 2b & (1+a)b \end{vmatrix} = \begin{vmatrix} 4 & 2 \\ 2 & 1+a \end{vmatrix} \cdot \begin{vmatrix} 4b & 2b \\ 2b & (1+a)b \end{vmatrix}$$

$$= \big(4(1+a) - 4\big) \cdot \big(4b^2(1+a) - 4b^2\big)$$
$$= \big(4(1+a) - 4\big)^2 \cdot b^2 \ = (4 \cdot a \cdot b)^2,$$

womit die Behauptung bewiesen ist. □

2.9 Satz. *Es seien a und b quadratfreie, teilerfremde und von 1 verschiedene ganze Zahlen, wobei $a \equiv 1(4)$ und $b \equiv 1(4)$. Dann ist die Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ biquadratisch und*

$$1, \quad \frac{1+\sqrt{a}}{2}, \quad \frac{1+\sqrt{b}}{2}, \quad \frac{1+\sqrt{a}}{2}\,\frac{1+\sqrt{b}}{2}$$

ist eine Ganzheitsbasis des algebraischen Zahlkörpers $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, wobei $\sqrt{a}$ und $\sqrt{b}$ Wurzeln von a bzw. b bezeichnen. Weiter ist

$$d_K = (a \cdot b)^2$$

die Diskriminante von K.

Beweis: Die angegeben Basiselemente sind ganz, vgl. [AZ, S. 49/50]. Sei nun

$$\alpha = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{ab}$$

mit rationalen Zahlen x, y, z, t ein beliebiges ganzes Element von K, wobei $\sqrt{ab}$ eine Wurzel von ab bezeichne. Die Spuren von α über den Zwischenkörpern $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{ab})$ von $K/\mathbb{Q}$ sind

$$S_{K/\mathbb{Q}(\sqrt{a})}\alpha = 2x + 2y\sqrt{a}$$
$$S_{K/\mathbb{Q}(\sqrt{ab})}\alpha = 2x + 2t\sqrt{ab}$$

und liegen im Ganzheitsring des jeweils betrachteten Zwischenkörpers, da die Konjugierten von α sowie Summen von ganzen Elementen ganz sind, vgl. [AZ, S.17/18]. Diese Ganzheitsringe sind bekannt, vgl. [AZ, S.49/50], so dass man umgeformt die Inklusionen

$$2x - 2y + 4y\,\frac{1+\sqrt{a}}{2} \;\in\; \mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{a}}{2}$$
$$2x - 2t + 4t\,\frac{1+\sqrt{ab}}{2} \;\in\; \mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{ab}}{2}$$

erhält. Aus ihnen folgt

$$2x - 2y \in \mathbb{Z}, \quad 2x - 2t \in \mathbb{Z}, \quad 4t \in \mathbb{Z}$$

und weiter

$$2y - 2t = (2x - 2t) - (2x - 2y) \in \mathbb{Z}.$$

Es sei jetzt

$$\alpha = x' + y'\,\frac{1+\sqrt{a}}{2} + z'\,\frac{1+\sqrt{b}}{2} + t'\,\frac{1+\sqrt{a}}{2}\,\frac{1+\sqrt{b}}{2}$$

mit $x', y', z', t' \in \mathbb{Q}$ die Darstellung von α bzgl. der obigen Basis, die als Ganzheitsbasis von K zu erweisen ist. Zu zeigen ist, dass die Koeffizienten x', y', z', t' bereits in $\mathbb{Z}$ liegen. Wir formen die Gleichung zu

$$\alpha = \left(x' + \frac{y'}{2} + \frac{z'}{2} + \frac{t'}{4}\right) + \left(\frac{y'}{2} + \frac{t'}{4}\right)\sqrt{a} + \left(\frac{z'}{2} + \frac{t'}{4}\right)\sqrt{b} + \frac{t'}{4}\sqrt{a}\sqrt{b}$$

um. Auf die oben beschriebene Art erhält man dann

$$2 \cdot \left(\frac{y'}{2} + \frac{t'}{4}\right) - 2 \cdot \frac{t'}{4} \in \mathbb{Z}, \quad 4 \cdot \frac{t'}{4} \in \mathbb{Z}$$

und aus $y', t' \in \mathbb{Z}$ folgt, dass

$$y' \frac{1+\sqrt{a}}{2} + t' \frac{1+\sqrt{a}}{2} \frac{1+\sqrt{b}}{2}$$

ein ganzes Element von K ist. Damit ist auch

$$x' + z' \frac{1+\sqrt{b}}{2} = \alpha - \left(y' \frac{1+\sqrt{a}}{2} + t' \frac{1+\sqrt{a}}{2} \frac{1+\sqrt{b}}{2} \right)$$

ganz, was genau dann der Fall ist, wenn x' und z' in $\mathbb{Z}$ liegen. Also liegt jeder der Koeffizienten x', y', z', t' in $\mathbb{Z}$. Der Ganzheitsring $\mathcal{O}_K$ von $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ ist also in

$$\mathbb{Z} + \mathbb{Z} \frac{1+\sqrt{a}}{2} + \mathbb{Z} \frac{1+\sqrt{b}}{2} + \mathbb{Z} \frac{1+\sqrt{a}}{2} \frac{1+\sqrt{b}}{2}$$

enthalten. Die umgekehrte Inklusion ist klar, da die vier Basiselemente wie gesagt ganz sind.

Die Diskriminante von K kann für jede Ganzheitsbasis $\beta_1, \beta_2, \beta_3, \beta_4$ von K mittels der Formel

$$d_K = \det \left(S_{K/\mathbb{Q}}(\beta_i \beta_j) \right)_{i,j=1,\ldots,4}$$

berechnet werden, vgl. [AZ, S. 47ff]. Einsetzen der obigen Basis liefert

$$d_K = \begin{vmatrix} S\,1 & S\,\frac{1+\sqrt{a}}{2} & S\,\frac{1+\sqrt{b}}{2} & S\,\frac{1+\sqrt{a}}{2}\frac{1+\sqrt{b}}{2} \\ S\,\frac{1+\sqrt{a}}{2} & S\left(\frac{1+\sqrt{a}}{2}\right)^2 & S\,\frac{1+\sqrt{a}}{2}\frac{1+\sqrt{b}}{2} & S\left(\frac{1+\sqrt{a}}{2}\right)^2\frac{1+\sqrt{b}}{2} \\ S\,\frac{1+\sqrt{b}}{2} & S\,\frac{1+\sqrt{a}}{2}\frac{1+\sqrt{b}}{2} & S\left(\frac{1+\sqrt{b}}{2}\right)^2 & S\,\frac{1+\sqrt{a}}{2}\left(\frac{1+\sqrt{b}}{2}\right)^2 \\ S\,\frac{1+\sqrt{a}}{2}\frac{1+\sqrt{b}}{2} & S\left(\frac{1+\sqrt{a}}{2}\right)^2\frac{1+\sqrt{b}}{2} & S\,\frac{1+\sqrt{a}}{2}\left(\frac{1+\sqrt{b}}{2}\right)^2 & S\left(\frac{1+\sqrt{a}}{2}\right)^2\left(\frac{1+\sqrt{b}}{2}\right)^2 \end{vmatrix}$$

$$= \begin{vmatrix} S\,1 & S\,\frac{1+\sqrt{a}}{2} & S\,\frac{1+\sqrt{b}}{2} & S\,\frac{1+\sqrt{a}+\sqrt{b}+\sqrt{ab}}{4} \\ S\,\frac{1+\sqrt{a}}{2} & S\,\frac{1+a+2\sqrt{a}}{4} & S\,\frac{1+\sqrt{a}+\sqrt{b}+\sqrt{ab}}{4} & S\,\frac{(1+a+2\sqrt{a})(1+\sqrt{b})}{8} \\ S\,\frac{1+\sqrt{b}}{2} & S\,\frac{1+\sqrt{a}+\sqrt{b}+\sqrt{ab}}{4} & S\,\frac{1+b+2\sqrt{b}}{4} & S\,\frac{(1+\sqrt{a})(1+b+2\sqrt{b})}{8} \\ S\frac{1+\sqrt{a}+\sqrt{b}+\sqrt{ab}}{4} & S\frac{(1+a+2\sqrt{a})(1+\sqrt{b})}{8} & S\frac{(1+\sqrt{a})(1+b+2\sqrt{b})}{8} & S\frac{(1+\sqrt{a}+\sqrt{b}+\sqrt{ab})^2}{16} \end{vmatrix}$$

$$= \begin{vmatrix} 4 & 2 & 2 & 1 \\ 2 & 1+a & 1 & \frac{1+a}{2} \\ 2 & 1 & 1+b & \frac{1+b}{2} \\ 1 & \frac{1+a}{2} & \frac{1+b}{2} & \frac{(1+a)(1+b)}{4} \end{vmatrix}$$

$$= 4 \cdot \begin{vmatrix} 1+a & 1 & \frac{1+a}{2} \\ 1 & 1+b & \frac{1+b}{2} \\ \frac{1+a}{2} & \frac{1+b}{2} & \frac{(1+a)(1+b)}{4} \end{vmatrix} - 2 \cdot \begin{vmatrix} 2 & 1 & \frac{1+a}{2} \\ 2 & 1+b & \frac{1+b}{2} \\ 1 & \frac{1+b}{2} & \frac{(1+a)(1+b)}{4} \end{vmatrix}$$

$$+ 2 \cdot \begin{vmatrix} 2 & 1+a & \frac{1+a}{2} \\ 2 & 1 & \frac{1+b}{2} \\ 1 & \frac{1+a}{2} & \frac{(1+a)(1+b)}{4} \end{vmatrix} - \begin{vmatrix} 2 & 1+a & 1 \\ 2 & 1 & 1+b \\ 1 & \frac{1+a}{2} & \frac{1+b}{2} \end{vmatrix}$$

$$= 4\,\frac{ab + a^2b + ab^2 + a^2b^2}{4} - 2\,\frac{ab + ab^2}{2} + 2\,\frac{-ab - a^2b}{2} - (-ab)$$
$$= (a \cdot b)^2,$$

womit die Behauptung bewiesen ist. □

2.10 Satz. *Es seien a und b quadratfreie und teilerfremde ganze Zahlen, wobei $a \equiv 3(4)$ sowie $b \equiv 3(4)$. Dann ist die Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ biquadratisch und*

$$1, \quad \sqrt{a}\,, \quad \frac{1+\sqrt{ab}}{2}\,, \quad \frac{\sqrt{a}+\sqrt{b}}{2}$$

ist eine Ganzheitsbasis des algebraischen Zahlkörpers $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, wobei $\sqrt{a}$, $\sqrt{b}$ und $\sqrt{ab}$ Wurzeln von a, b bzw. ab bezeichnen. Weiter ist

$$d_K = (4 \cdot a \cdot b)^2$$

die Diskriminante von K.

Beweis: Zunächst einmal sind die angegebenen Basiselemente von K ganz, was für die ersten drei unmittelbar aus [AZ, S.49/50] folgt. Das letzte Basiselement ist ganz, weil sein Quadrat

$$\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right)^2 = \frac{a+b+2\sqrt{ab}}{4} = \frac{a+b-2}{4} + \frac{1+\sqrt{ab}}{2}$$

wegen $a + b - 2 \equiv 0(4)$ ein ganzes Element von $\mathbb{Q}(\sqrt{ab})$ ist, vgl. [AZ, S. 49/50] und [AZ, S. 18]. Sei nun $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ und

$$\alpha = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{ab}$$

mit rationalen Zahlen x, y, z, t ein ganzes Element von K, wobei $\sqrt{ab}$ eine Wurzel von ab bezeichne. Die Spuren von α über den Zwischenkörpern $\mathbb{Q}(\sqrt{b})$ und $\mathbb{Q}(\sqrt{ab})$ von $K/\mathbb{Q}$ sind

$$S_{K/\mathbb{Q}(\sqrt{b})}\alpha = 2x + 2z\sqrt{b}$$
$$S_{K/\mathbb{Q}(\sqrt{ab})}\alpha = 2x + 2t\sqrt{ab}$$

und liegen im Ganzheitsring des jeweils betrachteten Zwischenkörpers, da die Konjugierten von α sowie Summen von ganzen Elementen ganz sind, vgl. [AZ, S.17/18]. Diese Ganzheitsringe sind bekannt, vgl. [AZ, S.49/50], so dass man die Inklusionen

$$\begin{aligned} 2x + 2z\sqrt{b} &\in \mathbb{Z} + \mathbb{Z}\sqrt{b} \\ 2x - 2t + 4t\,\frac{1+\sqrt{ab}}{2} &\in \mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{ab}}{2} \end{aligned}$$

erhält. Aus ihnen folgt

$$2x \in \mathbb{Z}, \quad 2z \in \mathbb{Z}, \quad 2x - 2t \in \mathbb{Z}$$

und weiter

$$2t = 2x - (2x - 2t) \in \mathbb{Z}.$$

Es sei jetzt

$$\alpha = x' + y'\sqrt{a} + z'\,\frac{1+\sqrt{ab}}{2} + t'\,\frac{\sqrt{a}+\sqrt{b}}{2}$$

mit $x', y', z', t' \in \mathbb{Q}$ die Darstellung von α bzgl. der obigen Basis, die als Ganzheitsbasis von K zu erweisen ist. Zu zeigen ist, dass die Koeffizienten x', y', z', t' bereits in $\mathbb{Z}$ liegen. Wir formen die Gleichung zu

$$\alpha = \left(x' + \frac{z'}{2}\right) + \left(y' + \frac{t'}{2}\right)\sqrt{a} + \frac{t'}{2}\sqrt{b} + \frac{z'}{2}\sqrt{a}\sqrt{b}$$

um. Auf die oben beschriebene Art erhält man dann

$$2 \cdot \frac{t'}{2} \in \mathbb{Z}, \quad 2 \cdot \frac{z'}{2} \in \mathbb{Z}$$

und aus $z', t' \in \mathbb{Z}$ folgt, dass

$$z'\,\frac{1+\sqrt{ab}}{2} + t'\,\frac{\sqrt{a}+\sqrt{b}}{2}$$

ein ganzes Element von K ist. Damit ist auch

$$x' + y'\,\sqrt{a} = \alpha - \left(z'\,\frac{1+\sqrt{ab}}{2} + t'\,\frac{\sqrt{a}+\sqrt{b}}{2}\right)$$

ganz, was genau dann der Fall ist, wenn x' und y' in $\mathbb{Z}$ liegen. Also liegt jeder der Koeffizienten x', y', z', t' in $\mathbb{Z}$. Der Ganzheitsring $\mathcal{O}_K$ von $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ ist demnach in

$$\mathbb{Z} + \mathbb{Z}\sqrt{a} + \mathbb{Z}\,\frac{1+\sqrt{ab}}{2} + \mathbb{Z}\,\frac{\sqrt{a}+\sqrt{b}}{2}$$

enthalten. Die umgekehrte Inklusion ist klar, weil wie gesagt die vier Basiselemente ganz sind.

Die Diskriminante von K kann für jede Ganzheitsbasis $\beta_1, \beta_2, \beta_3, \beta_4$ von K mittels der Formel

$$d_K = \det\left(S_{K/\mathbb{Q}}(\beta_i\beta_j)\right)_{i,j=1,\ldots,4}$$

berechnet werden, vgl. [AZ, S. 47ff].

Einsetzen der obigen Basis liefert

$$d_K = \begin{vmatrix} S\,1 & S\left(\sqrt{a}\right) & S\left(\frac{1+\sqrt{ab}}{2}\right) & S\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right) \\ S\left(\sqrt{a}\right) & S\left(\sqrt{a}\cdot\sqrt{a}\right) & S\left(\sqrt{a}\,\frac{1+\sqrt{ab}}{2}\right) & S\left(\sqrt{a}\,\frac{\sqrt{a}+\sqrt{b}}{2}\right) \\ S\left(\frac{1+\sqrt{ab}}{2}\right) & S\left(\sqrt{a}\,\frac{1+\sqrt{ab}}{2}\right) & S\left(\left(\frac{1+\sqrt{ab}}{2}\right)^2\right) & S\left(\frac{1+\sqrt{ab}}{2}\,\frac{\sqrt{a}+\sqrt{b}}{2}\right) \\ S\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right) & S\left(\sqrt{a}\,\frac{\sqrt{a}+\sqrt{b}}{2}\right) & S\left(\frac{1+\sqrt{ab}}{2}\,\frac{\sqrt{a}+\sqrt{b}}{2}\right) & S\left(\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right)^2\right) \end{vmatrix}$$

$$= \begin{vmatrix} S\,1 & S\left(\sqrt{a}\right) & S\left(\frac{1+\sqrt{ab}}{2}\right) & S\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right) \\ S\left(\sqrt{a}\right) & S\,a & S\left(\frac{\sqrt{a}+a\sqrt{b}}{2}\right) & S\left(\frac{a+\sqrt{ab}}{2}\right) \\ S\left(\frac{1+\sqrt{ab}}{2}\right) & S\left(\frac{\sqrt{a}+a\sqrt{b}}{2}\right) & S\left(\frac{1+ab+2\sqrt{ab}}{4}\right) & S\left(\frac{(1+b)\sqrt{a}+(1+a)\sqrt{b}}{4}\right) \\ S\left(\frac{\sqrt{a}+\sqrt{b}}{2}\right) & S\left(\frac{a+\sqrt{ab}}{2}\right) & S\left(\frac{(1+b)\sqrt{a}+(1+a)\sqrt{b}}{4}\right) & S\left(\frac{a+b+2\sqrt{ab}}{4}\right) \end{vmatrix}$$

$$= \begin{vmatrix} 4 & 0 & 2 & 0 \\ 0 & 4a & 0 & 2a \\ 2 & 0 & 1+ab & 0 \\ 0 & 2a & 0 & a+b \end{vmatrix} = 4\cdot\begin{vmatrix} 4a & 0 & 2a \\ 0 & 1+ab & 0 \\ 2a & 0 & a+b \end{vmatrix} + 2\cdot\begin{vmatrix} 0 & 4a & 2a \\ 2 & 0 & 0 \\ 0 & 2a & a+b \end{vmatrix}$$

$$= 4\big(4a(1+ab)(a+b) - 2a(1+ab)2a\big) + 2\big(2a\cdot 2\cdot 2a - (a+b)\cdot 2\cdot 4a\big)$$
$$= 4\cdot 4a(1+ab)b + 2(-b\cdot 2\cdot 4a) \;= (4\cdot a\cdot b)^2,$$

womit die Behauptung bewiesen ist. □

2.11 Satz. *Es seien a und b quadratfreie und teilerfremde ganze Zahlen, wobei $a \equiv 2(4)$ und $b \equiv 3(4)$. Dann ist die Erweiterung $\mathbb{Q}(\sqrt{a},\sqrt{b})/\mathbb{Q}$ biquadratisch und*

$$1, \quad \sqrt{a}, \quad \sqrt{b}, \quad \frac{\sqrt{a}+\sqrt{ab}}{2}$$

ist eine Ganzheitsbasis des algebraischen Zahlkörpers $K = \mathbb{Q}(\sqrt{a},\sqrt{b})$, wobei $\sqrt{a}$, $\sqrt{b}$ und $\sqrt{ab}$ Wurzeln von a, b bzw. ab bezeichnen. Weiter ist

$$d_K = (8\cdot a\cdot b)^2$$

die Diskriminante von K.

Beweis: Als erstes sei angemerkt, dass die angegebenen Basiselemente von K ganz sind. Für die ersten drei folgt das unmittelbar aus [AZ, S.49/50], während das letzte Basiselement ganz ist, weil sein Quadrat

$$\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right)^2 = \frac{a+ab+2a\sqrt{b}}{4} = \frac{ab-a}{4} + a\frac{1+\sqrt{b}}{2}$$

wegen $ab - a \equiv 0(4)$ ein ganzes Element von $\mathbb{Q}(\sqrt{b})$ ist, vgl. [AZ, S. 49/50] und [AZ, S. 18]. Sei nun $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ und

$$\alpha = x + y\sqrt{a} + z\sqrt{b} + t\sqrt{ab}$$

mit rationalen Zahlen x, y, z, t ein ganzes Element von K, wobei $\sqrt{ab}$ eine Wurzel von ab bezeichne. Die Spur von α über dem Zwischenkörper $\mathbb{Q}(\sqrt{ab})$ von $K/\mathbb{Q}$ ist

$$S_{K/\mathbb{Q}(\sqrt{ab})}\alpha = 2x + 2t\sqrt{ab}$$

und liegt im Ganzheitsring von $\mathbb{Q}(\sqrt{ab})$, da die Konjugierten von α sowie Summen von ganzen Elementen ganz sind, vgl. [AZ, S.17/18]. Dieser Ganzheitsring ist bekannt, vgl. [AZ, S.49/50], so dass man die Inklusion

$$2x + 2t\sqrt{ab} \ \in \ \mathbb{Z} + \mathbb{Z}\sqrt{ab}$$

erhält. Aus ihr folgt

$$2t \in \mathbb{Z}.$$

Daher sei als nächstes

$$\beta = x + y\sqrt{a} + z\sqrt{b}$$

mit rationalen Zahlen x, y, z ein ganzes Element von K. Die Normen von β über den verschiedenen Zwischenkörpern von K sind ganz, weil alle Konjugierten von β sowie Produkte von ganzen Elementen ganz sind, vgl. [AZ, S.17/18]. Die Normen

$$N_{K/\mathbb{Q}(\sqrt{a})}\beta = x^2 + ay^2 - bz^2 + 2xy\sqrt{a}$$
$$N_{K/\mathbb{Q}(\sqrt{b})}\beta = x^2 + bz^2 - ay^2 + 2xz\sqrt{b}$$

von β über $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$ liegen also im jeweiligen Ganzheitsring, woraus sich die Inklusionen

$$x^2 + ay^2 - bz^2 + 2xy\sqrt{a} \ \in \ \mathbb{Z} + \mathbb{Z}\sqrt{a}$$
$$x^2 + bz^2 - ay^2 + 2xz\sqrt{b} \ \in \ \mathbb{Z} + \mathbb{Z}\sqrt{b}$$

ergeben, vgl. [AZ, S.49/50]. Betrachtet man nur die Komponenten zum Basiselement 1, so erhält man

$$x^2 + ay^2 - bz^2 \in \mathbb{Z}$$
$$x^2 + bz^2 - ay^2 \in \mathbb{Z}$$

und durch Addition folgt

$$2x^2 \in \mathbb{Z},$$

doch damit ist bereits

$$x \in \mathbb{Z}.$$

Es sei jetzt

$$\alpha = x' + y'\sqrt{a} + z'\sqrt{b} + t'\,\frac{\sqrt{a} + \sqrt{ab}}{2}$$

mit $x', y', z', t' \in \mathbb{Q}$ die Darstellung von α bzgl. der obigen Basis, die als Ganzheitsbasis von K zu erweisen ist. Zu zeigen ist, dass die Koeffizienten x', y', z', t' bereits in $\mathbb{Z}$ liegen. Wir formen die Gleichung zu

$$\alpha = x' + \left(y' + \frac{t'}{2}\right)\sqrt{a} + z'\sqrt{b} + \frac{t'}{2}\sqrt{a}\sqrt{b}$$

um. Auf die oben beschriebene Art erhält man dann

$$2 \cdot \frac{t'}{2} \in \mathbb{Z}$$

und aus $t' \in \mathbb{Z}$ folgt, dass

$$t' \, \frac{\sqrt{a} + \sqrt{ab}}{2}$$

ein ganzes Element von K ist. Damit ist auch

$$x' + y'\sqrt{a} + z'\sqrt{b} = \alpha - t' \, \frac{\sqrt{a} + \sqrt{ab}}{2}$$

ganz, woraus wie oben gezeigt $x' \in \mathbb{Z}$ folgt. Weiter ist dann

$$y'\sqrt{a} + z'\sqrt{b}$$

ganz und mithin auch

$$\sqrt{a} \cdot \left(y'\sqrt{a} + z'\sqrt{b} \right) = ay' + z'\sqrt{a}\sqrt{b}.$$

Weil $(1, \sqrt{a}\sqrt{b})$ eine Ganheitsbasis von $\mathbb{Q}(\sqrt{ab})$ ist, ergibt sich $z' \in \mathbb{Z}$. Auf analoge Weise liefert Multiplikation mit $\sqrt{b}$, dass $y' \in \mathbb{Z}$. Also liegt jeder der Koeffizienten x', y', z', t' in $\mathbb{Z}$. Der Ganzheitsring $\mathcal{O}_K$ von $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ ist demnach in

$$\mathbb{Z} + \mathbb{Z}\sqrt{a} + \mathbb{Z}\sqrt{b} + \mathbb{Z} \, \frac{\sqrt{a} + \sqrt{ab}}{2}$$

enthalten. Die umgekehrte Inklusion ist klar, weil wie gesagt die vier Basiselemente ganz sind.

Die Diskriminante von K kann für jede Ganzheitsbasis $\beta_1, \beta_2, \beta_3, \beta_4$ von K mittels der Formel

$$d_K = \det \left(S_{K/\mathbb{Q}}(\beta_i \beta_j) \right)_{i,j=1,\ldots,4}$$

berechnet werden, vgl. [AZ, S. 47ff]. Einsetzen der obigen Basis liefert

$$d_K = \begin{vmatrix} S\,1 & S\left(\sqrt{a}\right) & S\left(\sqrt{b}\right) & S\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right) \\ S\left(\sqrt{a}\right) & S\left(\sqrt{a}\cdot\sqrt{a}\right) & S\left(\sqrt{a}\cdot\sqrt{b}\right) & S\left(\sqrt{a}\,\frac{\sqrt{a}+\sqrt{ab}}{2}\right) \\ S\left(\sqrt{b}\right) & S\left(\sqrt{a}\cdot\sqrt{b}\right) & S\left(\sqrt{b}\cdot\sqrt{b}\right) & S\left(\sqrt{b}\,\frac{\sqrt{a}+\sqrt{ab}}{2}\right) \\ S\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right) & S\left(\sqrt{a}\,\frac{\sqrt{a}+\sqrt{ab}}{2}\right) & S\left(\sqrt{b}\,\frac{\sqrt{a}+\sqrt{ab}}{2}\right) & S\left(\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right)^2\right) \end{vmatrix}$$

$$= \begin{vmatrix} S\,1 & S\left(\sqrt{a}\right) & S\left(\sqrt{b}\right) & S\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right) \\ S\left(\sqrt{a}\right) & S\,a & S\left(\sqrt{a}\cdot\sqrt{b}\right) & S\left(\frac{a+a\sqrt{b}}{2}\right) \\ S\left(\sqrt{b}\right) & S\left(\sqrt{a}\cdot\sqrt{b}\right) & S\,b & S\left(\frac{b\sqrt{a}+\sqrt{ab}}{2}\right) \\ S\left(\frac{\sqrt{a}+\sqrt{ab}}{2}\right) & S\left(\frac{a+a\sqrt{b}}{2}\right) & S\left(\frac{b\sqrt{a}+\sqrt{ab}}{2}\right) & S\left(\frac{a+ab+2a\sqrt{b}}{4}\right) \end{vmatrix}$$

$$= \begin{vmatrix} 4 & 0 & 0 & 0 \\ 0 & 4a & 0 & 2a \\ 0 & 0 & 4b & 0 \\ 0 & 2a & 0 & a+ab \end{vmatrix} = 4 \cdot \begin{vmatrix} 4a & 0 & 2a \\ 0 & 4b & 0 \\ 2a & 0 & a+ab \end{vmatrix}$$

$$= 4\big(4a \cdot 4b \cdot (a+ab) - 2a \cdot 4b \cdot 2a\big)$$
$$= 4\big(4 \cdot 4 \cdot ab(a+ab) - 4 \cdot 4 \cdot aba\big) \; = (8 \cdot a \cdot b)^2,$$

womit die Behauptung bewiesen ist. □

2.12 Bemerkung. Die Sätze 2.8 und 2.9 folgen unmittelbar aus Satz 88 in Hilberts Zahlbericht ([H]). Bevor wir diesen formulieren, soll kurz etwas zum Begriff der linearen Disjunktheit gesagt werden. Seien K_1/k, K_2/k endliche Erweiterungen und $K = K_1K_2$ das Kompositum von K_1 und K_2. Dann sind die folgenden Aussagen äquivalent:

1. K_1/k und K_2/k sind linear disjunkt.

2. $K_1 : k = K : K_2$

3. Ist $\{a_i\}$ eine Basis von K_1 über k und $\{b_j\}$ eine Basis von K_2 über k, so ist die Menge $\{a_ib_j\}$ eine Basis von K über k.

4. Das Kompositum K kann mit $K_1 \otimes_k K_2$ kanonisch identifiziert werden.

Falls K_1/k galoissch ist oder die Grade von K_1/k und K_2/k teilerfremd sind, so lautet eine weitere äquivalente Bedingung:

5. $K_1 \cap K_2 = k$

"Satz 88 von Hilbert". *Seien K_1, K_2 zwei Zahlkörper der Grade n_1 und n_2 mit den zueinander primen Diskriminanten d_1, d_2. Dann sind K_1 und K_2 linear disjunkt, für den Ganzheitsring $\mathcal{O}_K$ des Kompositums $K = K_1K_2$ gilt*

$$\mathcal{O}_K = \mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$$

und für die Diskriminante d von K gilt

$$d = d_1^{n_2} d_2^{n_1}.$$

Mit den Resultaten 2.8-2.11 können wir nun die Minkowski-Schranken der dort vorkommenden Körper berechnen. Desweiteren benötigen wir

2.13 Lemma. *Sei $K/\mathbb{Q}$ eine endliche galoissche Erweiterung. Besitzt $K/\mathbb{Q}$ eine reelle Stelle, so ist $K/\mathbb{Q}$ total reell. Besitzt $K/\mathbb{Q}$ eine komplexe Stelle, so ist K total imaginär.*

Beweis: Da $K/\mathbb{Q}$ normal ist, wird K unter jeder Einbettung in $\mathbb{C}$ auf sich selbst abgebildet. Im Falle $K \subset \mathbb{R}$ ist jede dieser Einbettungen reell, sonst ist jede dieser Einbettungen komplex. □

2.14 Satz. *Es sei $a \geq 2$ eine quadratfreie ganze Zahl. Dann ist für $K = \mathbb{Q}(\sqrt{a}, i)$ die Erweiterung $K/\mathbb{Q}$ biquadratisch. Für die Minkowski-Schranke m_K von K gilt*

$$m_K = \frac{2 \cdot 3 \cdot d}{\pi^2} \quad \textit{mit} \quad d = \begin{cases} 2a & \textit{für gerades } a \\ a & \textit{sonst.} \end{cases}$$

Beweis: Allgemein ist die Minkowski-Schranke eines algebraischen Zahlkörpers K durch

$$m_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |d_k|^{\frac{1}{2}} \tag{3}$$

gegeben, wobei s die Anzahl der komplexen Stellen von K, n den Grad $K : k$ und d_K die Diskriminante von K bezeichnet, vgl. [AZ, S. 87]. Zwischen s und n besteht der Zusammenhang

$$n = r + 2s$$

mit r als der Anzahl der reellen Stellen von K, vgl. [AZ, S. 74] oder [N, S. 32]. Da $K = \mathbb{Q}(\sqrt{a}, i)$ den imaginärquadratischen Körper $\mathbb{Q}(i)$ enthält, ist nach Lemma 2.13 hier $r = 0$ und $s = 2$. Auch die Diskriminante d_K von $K = \mathbb{Q}(\sqrt{a}, i)$ kann sofort angegeben werden. Im Falle $a \equiv 2(4)$ ist Satz 2.11 anwendbar und es folgt

$$d_K = (8a)^2.$$

Für ungerades a ist hingegen $a \equiv 1(4)$ oder $-a \equiv 1(4)$. Anwendung von Satz 2.8 liefert

$$d_K = (4a)^2.$$

Damit liegt alles bereit und wir erhalten

$$\begin{aligned} m_K &= \left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4} |d_k|^{\frac{1}{2}} = \frac{4^2}{\pi^2} \frac{4 \cdot 3 \cdot 2}{4^4} 4 \cdot d \\ &= \frac{3 \cdot 2 \cdot d}{\pi^2} \qquad \text{mit} \quad d = \begin{cases} 2a & \text{falls } a \equiv 2(4) \\ a & \text{sonst} \end{cases} \end{aligned}$$

als Formel für die Minkowski-Schranke. □

2.15 Satz. *Es seien $a, b \geq 2$ quadratfreie, teilerfremde ganze Zahlen. Dann ist für $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ die Erweiterung $K/\mathbb{Q}$ biquadratisch. Es bezeichne m_K die Minkowski-Schranke von K.*

i) Ist $a \equiv 1(4)$ und $b \equiv 1(4)$, so gilt

$$m_K = \frac{3}{32} ab.$$

ii) Ist $a \equiv 1(4)$ oder $ab \equiv 1(4)$, aber $b \not\equiv 1(4)$, so gilt

$$m_K = \frac{3}{8} ab.$$

iii) Ist $a \equiv 2(4)$ und $b \equiv 3(4)$, so gilt

$$m_K = \frac{3}{4} ab.$$

Beweis: Für die Minkowski-Schranke von K gilt Formel (3) aus dem Beweis von Satz 2.14. Nach Lemma 2.13 ist hierbei $r = 4$ und $s = 0$, denn K ist rein reell. Die Diskriminante d_K liefert einer der Sätze 2.8-2.11; es gilt

$$|d_K|^{\frac{1}{2}} = \begin{cases} ab & \text{falls } a, b \equiv 1(4) \\ 4\,ab & \text{falls } a \equiv 1(4) \text{ oder } ab \equiv 1(4), b \not\equiv 1(4) \\ 8\,ab & \text{falls } a \equiv 2(3), b \equiv 3(4). \end{cases}$$

Durch Einsetzen in der Formel (3) erhalten wir

$$\begin{aligned} m_K &= \Big(\frac{4}{\pi}\Big)^0 \frac{4!}{4^4}\,|d_K|^{\frac{1}{2}} = \frac{4 \cdot 3 \cdot 2}{4^4}\,|d_K|^{\frac{1}{2}} = \frac{3}{32}\,|d_K|^{\frac{1}{2}} \\ &= \begin{cases} \frac{3}{32}\,ab & \text{falls } a, b \equiv 1(4) \\ \frac{3}{8}\,ab & \text{falls } a \equiv 1(4) \text{ oder } ab \equiv 1(4), b \not\equiv 1(4) \\ \frac{3}{4}\,ab & \text{falls } a \equiv 2(3), b \equiv 3(4) \end{cases} \end{aligned}$$

als Wert der Minkowski-Schranke. □

2.iii Biquadratische Erweiterungskörper von $\mathbb{Q}$ der Klassenzahl 1

In diesem Abschnitt werden wir für einige biquadratische Erweiterungen $K/\mathbb{Q}$ die Gruppe $H^{-1}(G, K^\times)$ explizit berechnen. Dabei werden wir verwenden, dass der Körper K die Klassenzahl 1 hat. Unter dieser Voraussetzung ist nach Satz 2.7 der natürliche Homomorphismus

$$H^{-1}(G, E_K) \longrightarrow H^{-1}(G, K^\times)$$

surjektiv, oder anders gesagt wird jede Klasse aus $H^{-1}(G, K^\times)$ durch eine Einheit von K repräsentiert. Es genügt daher, die von den Einheiten der Norm 1 erzeugten Klassen von $H^{-1}(G, K^\times)$ zu untersuchen. Bevor wir damit beginnen, muss der Nachweis erbracht werden, dass die betrachteten Körper tatsächlich die Klassenzahl 1 haben. Zur Vorbereitung beginnen wir mit

2.16 Lemma. *Seien K ein algebraischer Zahlkörper und $\mathfrak{p}$ eine Stelle von K. Genau dann ist das Primideal $\mathfrak{p}$ ein Hauptideal, wenn es im Ganzheitsring $\mathcal{O}_K$ ein Element α mit derselben Absolutnorm wie $\mathfrak{p}$ gibt, d. h. ein α mit*

$$\big|N_{K/\mathbb{Q}}\,\alpha\big| = \mathcal{N}\mathfrak{p}.$$

Beweis: Für jedes $\alpha \in K$ ist der Betrag von $N_{K/\mathbb{Q}}\,\alpha$ gleich der Absolutnorm des von α erzeugten Ideals, kurz

$$\big|N_{K/\mathbb{Q}}\,\alpha\big| = \mathcal{N}(\alpha),$$

vgl. [AZ, S. 52]. Demnach gibt es genau dann ein $\alpha \in \mathcal{O}_K$ mit Absolutnorm $\mathcal{N}\mathfrak{p}$, wenn es ein Hauptideal $(\alpha) \subset \mathcal{O}_K$ mit

$$\mathcal{N}(\alpha) = \mathcal{N}\mathfrak{p} \tag{4}$$

gibt. Wenn $\mathfrak{p}$ selbst ein Hauptideal ist, so wird (4) von $(\alpha) = \mathfrak{p}$ erfüllt. Es werde nun umgekehrt vorausgesetzt, das Hauptideal $(\alpha) \subset \mathcal{O}_K$ genüge (4). Sei

$$(\alpha) = \mathfrak{p}_1 \ldots \mathfrak{p}_r\,\mathfrak{q}_1 \ldots \mathfrak{q}_s$$

die Zerlegung des Ideals (α) als Produkt von Primidealen, wobei $\mathfrak{p}$ und alle $\mathfrak{p}_i$ über derselben Primzahl p liegen, während die $\mathfrak{q}_i$ Teiler von Primzahlen $q_i \neq p$ sind. Die Normen aller über p liegenden Stellen $\mathfrak{p}'$ sind gleich derselben Potenz von p, denn $\mathcal{N}\mathfrak{p}'$ ist die Elementezahl des Restklassenkörpers $\mathcal{O}_K/\mathfrak{p}'$ (vgl. [AZ, S. 4]), doch alle $\mathfrak{p}'$ haben denselben Restklassengrad über p (vgl. [AZ, S. 103/104] oder [N, S. 58]). Damit folgt

$$\mathcal{N}\,\alpha = \left(\mathcal{N}\mathfrak{p}\right)^r \mathcal{N}\mathfrak{q}_1 \ldots \mathcal{N}\mathfrak{q}_s,$$

wobei jedes $\mathcal{N}\mathfrak{q}_i$ Potenz einer von p verschiedenen Primzahl ist. Es folgt, daß $r = 1$ und $s = 0$ sein muß, weil (α) und alle über p liegenden Stellen dieselbe Norm haben. Da alle über p liegenden Stellen konjugiert sind (vgl. [AZ, S. 103]), ist $\mathfrak{p}_1$ ein zu $\mathfrak{p}$ konjugiertes Hauptideal und $\mathfrak{p}$ demzufolge selbst ein Hauptideal. □

Wir haben jetzt ein Kriterium, um zu bestimmen, wann ein Primideal von K ein Hauptideal ist. Mit diesem gelangt man zu dem folgenden Resultat.

2.17 Satz. *Die algebraischen Zahlkörper*

$$\mathbb{Q}(\sqrt{2}, i), \quad \mathbb{Q}(\sqrt{3}, i), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{17}),$$
$$\mathbb{Q}(\sqrt{3}, \sqrt{5}), \quad \mathbb{Q}(\sqrt{3}, \sqrt{7}), \quad \mathbb{Q}(\sqrt{13}, \sqrt{17})$$

haben die Klassenzahl 1.

Beweis: Zu zeigen ist, dass in jedem der genannten Körper K alle gebrochenen Ideale Hauptideale sind. Dabei genügt es die ganzen Ideale zu betrachten, deren Absolutnorm die $Minkowski - Schranke\ m_K$ nicht überschreitet, denn in jeder Idealklasse von K liegt ein Ideal dieser Art, vgl. [AZ, S. 86/87]. Unter allen ganzen Idealen $\mathfrak{a}$ von K mit Absolutnorm $\mathcal{N}\mathfrak{a} \leq m_K$ braucht man desweiteren nur die Primideale zu betrachten, wie jetzt gezeigt werden soll. Es sei $\mathfrak{a}$ ein ganzes Ideal von K und

$$\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

die Zerlegung von $\mathfrak{a}$ als Produkt von Primidealen, vgl. [AZ, S. 41]. Dann gilt für die Absolutnorm $\mathcal{N}\mathfrak{a}$ von $\mathfrak{a}$ die Gleichung

$$\mathcal{N}\mathfrak{a} = \mathcal{N}\mathfrak{p}_1 \ldots \mathcal{N}\mathfrak{p}_r,$$

vgl. [AZ, S. 15] oder [N, S. 36/37]. Hieran ist insbesondere zu erkennen, dass die Absolutnormen der $\mathfrak{p}_i$ die Absolutnorm von $\mathfrak{a}$ teilen. Wenn $\mathcal{N}\mathfrak{a}$ nicht größer als die Minkowski-Schranke ist, so gilt dasselbe also auch für die Absolutnormen der $\mathfrak{p}_i$. Sind nun alle $\mathfrak{p}_i$ Hauptideale, so ist $\mathfrak{a}$ als Produkt von Hauptidealen ebenfalls ein Hauptideal.

Nach Lemma 2.16 ist schließlich bekannt, daß ein Primideal $\mathfrak{p}$ von K genau dann ein Hauptideal ist, wenn es ein Element α von $\mathcal{O}_K$ gibt, das dieselbe Absolutnorm wie das Ideal $\mathfrak{p}$ hat, wobei mit "Absolutnorm" der Betrag der Norm von α gemeint ist.

Nachdem wir beschrieben haben, wie vorzugehen ist, wollen wir jetzt die Körper K im einzelnen betrachten. Zunächst einmal liegen die Minkowski-Schranken nach den Sätzen 2.14, 2.15 in den folgenden Intervallen.

Körper	Minkowski-Schranke	Intervall
$\mathbb{Q}(\sqrt{2},i)$	$\frac{2\cdot 3\cdot 4}{\pi^2}=\frac{24}{\pi^2}$	[2,3[
$\mathbb{Q}(\sqrt{3},i)$	$\frac{2\cdot 3\cdot 3}{\pi^2}=\frac{18}{\pi^2}$	[1,2[
$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\frac{3\cdot 3}{2}=\frac{9}{2}$	[4,5[
$\mathbb{Q}(\sqrt{2},\sqrt{17})$	$\frac{3\cdot 17}{4}=\frac{51}{4}$	[12,13[
$\mathbb{Q}(\sqrt{3},\sqrt{5})$	$\frac{3\cdot 3\cdot 5}{8}=\frac{45}{8}$	[5,6[
$\mathbb{Q}(\sqrt{3},\sqrt{7})$	$\frac{3\cdot 3\cdot 7}{8}=\frac{63}{8}$	[7,8[
$\mathbb{Q}(\sqrt{13},\sqrt{17})$	$\frac{3\cdot 13\cdot 17}{32}=\frac{663}{32}$	[20,21[

Im folgenden werden wir für jeden der Körper K alle Primzahlen p betrachten, die unterhalb der Minkowski-Schranke liegen. Für die Primideale $\mathfrak{p}$ von K, die über p liegen, gilt dann möglicherweise $\mathcal{N}\mathfrak{p} \leq m_K$. Anhand des Zerlegungsverhaltens von p in K (vgl. [AZ, S. 113] oder Abschnitt 4.2) ist zu erkennen, welchen Wert $\mathcal{N}\mathfrak{p}$ annimmt (es ist derselbe für alle $\mathfrak{p}|p$). Nachdem dieser bestimmt ist, wird ein ganzes Element von K angegeben, das dieselbe Absolutnorm hat, womit der Beweis erbracht ist, daß es sich um ein Hauptideal handelt.

1. Es sei $K=\mathbb{Q}(\sqrt{2},i)$. Dann ist $m_K \in [2,3[$ und es gilt

$$(2)=\mathfrak{p}^4 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}=2$$
$$1+\zeta_8 \in \mathcal{O}_K,$$
$$N_{K/\mathbb{Q}(\sqrt{2})}(1-\zeta_8)=(1-\zeta_8)(1-\overline{\zeta_8})=1+\zeta_8\overline{\zeta_8}-(\zeta_8+\overline{\zeta_8})=2-2\,\mathrm{Re}\,\zeta_8=2-\sqrt{2}$$

2. Es sei $K=\mathbb{Q}(\sqrt{3},i)$. Dann ist $m_K \in [1,2[$.

3. Es sei $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Dann ist $m_K \in [4,5[$ und es gilt

$$(2)=\mathfrak{p}^4 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}=2$$
$$\frac{2+\sqrt{2}+\sqrt{2}\sqrt{3}}{2}=1+\frac{\sqrt{2}+\sqrt{2}\sqrt{3}}{2}\in\mathcal{O}_K,$$
$$N_{K/\mathbb{Q}(\sqrt{2})}\left(\frac{2+\sqrt{2}+\sqrt{2}\sqrt{3}}{2}\right)=\frac{(2+\sqrt{2})^2-2\cdot 3}{4}=\frac{4+2-6+4\sqrt{2}}{4}=\sqrt{2}$$
$$(3)=\mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}=3^2$$

4. Es sei $K=\mathbb{Q}(\sqrt{2},\sqrt{17})$. Dann ist $m_K \in [12,13[$ und es gilt

$$(2)=\mathfrak{p}_1^2\mathfrak{p}_2^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1=\mathcal{N}\mathfrak{p}_2=2$$

$$\frac{1+2\sqrt{2}+\sqrt{17}}{2} = \sqrt{2} + \frac{1+\sqrt{17}}{2} \in \mathcal{O}_K,$$
$$N_{K/\mathbb{Q}(\sqrt{2})}\left(\frac{1+2\sqrt{2}+\sqrt{17}}{2}\right) = \frac{(1+2\sqrt{2})^2 - 17}{4} = \frac{1+8-17+4\sqrt{2}}{4}$$
$$= -2 + \sqrt{2}$$

$$(3) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 3^2$$
$$\frac{2+3\sqrt{2}+\sqrt{2}\sqrt{17}}{2} = 1 + \sqrt{2} + \frac{\sqrt{2}+\sqrt{2}\sqrt{17}}{2} \in \mathcal{O}_K,$$
$$N_{K/\mathbb{Q}(\sqrt{2})}\left(\frac{2+3\sqrt{2}+\sqrt{2}\sqrt{17}}{2}\right) = \frac{(2+3\sqrt{2})^2 - 2\cdot 17}{4} = \frac{4+18-34+12\sqrt{2}}{4}$$
$$= -3 + 3\sqrt{2}$$

$$(5) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 5^2$$

$$(7) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 7^2$$

$$(11) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 11^2$$

5. Es sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Dann ist $m_K \in [5, 6[$ und es gilt

$$(2) = \mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p} = 2^2$$
$$1 + \sqrt{3} \in \mathcal{O}_K, \quad N_{K/\mathbb{Q}(\sqrt{5})}(1+\sqrt{3}) = -2$$

$$(3) = \mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p} = 3^2$$

$$(5) = \mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p} = 5^2$$

6. Es sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Dann ist $m_K \in [7, 8[$ und es gilt

$$(2) = \mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p} = 2^2$$
$$1 + \sqrt{3} \in \mathcal{O}_K, \quad N_{K/\mathbb{Q}(\sqrt{7})}(1+\sqrt{3}) = -2$$

$$(3) = \mathfrak{p}_1^2\mathfrak{p}_2^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 3$$
$$1 + \sqrt{3} + \sqrt{7} \in \mathcal{O}_K, \quad N_{K/\mathbb{Q}(\sqrt{3})}(1+\sqrt{3}+\sqrt{7}) = (1+\sqrt{3})^2 - 7$$
$$= 1 + 3 - 7 + 2\sqrt{3} = -3 + 2\sqrt{3}$$

$$(5) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 5^2$$

$$(7) = \mathfrak{p}^2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p} = 7^2$$

7. Es sei $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Dann ist $m_K \in [20, 21[$ und es gilt

$$(2) = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathcal{O}_K, \quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 2^2$$
$$\frac{3+\sqrt{17}}{2} = 1 + \frac{1+\sqrt{17}}{2} \in \mathcal{O}_K,$$
$$N_{K/\mathbb{Q}(\sqrt{2})}\left(\frac{3+\sqrt{17}}{2}\right) = \frac{9-17}{4} = -2$$

$(3) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 3^2$
$4 + \sqrt{13} \in \mathcal{O}_K$, $\quad N_{K/\mathbb{Q}(\sqrt{17})}(4 + \sqrt{13}) = 3$

$(5) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 5^2$

$(7) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 7^2$

$(11) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 11^2$

$(13) = \mathfrak{p}_1^2\mathfrak{p}_2^2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 13$
$\dfrac{2 + \sqrt{13} + \sqrt{17}}{2} = \dfrac{1 + \sqrt{13}}{2} + \dfrac{1 + \sqrt{17}}{2} \in \mathcal{O}_K,$
$N_{K/\mathbb{Q}(\sqrt{13})}\left(\dfrac{2 + \sqrt{13} + \sqrt{17}}{2}\right) = \dfrac{(2 + \sqrt{13})^2 - 17}{4} = \dfrac{4 + 13 - 17 + 4\sqrt{13}}{4}$
$= \sqrt{13}$

$(17) = \mathfrak{p}_1^2\mathfrak{p}_2^2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 17$
$1 + 2\sqrt{13} + 2\sqrt{17} \in \mathcal{O}_K,$
$N_{K/\mathbb{Q}(\sqrt{17})}(1 + 2\sqrt{13} + 2\sqrt{17}) = (1 + 2\sqrt{17})^2 - 4 \cdot 13 = 1 + 4 \cdot 17 - 4 \cdot 13 + 4\sqrt{17}$
$= 17 + 4\sqrt{17}$

$(19) = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, $\quad \mathcal{N}\mathfrak{p}_1 = \mathcal{N}\mathfrak{p}_2 = 19^2$

Damit ist der Beweis erbracht, dass jeder der genannten Körper die Klassenzahl 1 hat. □

Der nun kommende Satz soll auf sehr direkte Weise bewiesen werden.

2.18 Satz. *Für die im folgenden auftretenden Körper K bezeichne $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ die Galoisgruppe der biquadratischen Erweiterung K/k. Dann gilt*

$$H^{-1}(G,\, \mathbb{Q}(\sqrt{2}, i)^\times) = 1,$$
$$H^{-1}(G,\, \mathbb{Q}(\sqrt{2}, \sqrt{17})^\times) = 1,$$
$$H^{-1}(G,\, \mathbb{Q}(\sqrt{13}, \sqrt{17})^\times) = 1;$$

andererseits sind die Gruppen in den folgenden Fällen nicht-trivial, und genauer gilt:

$$H^{-1}(G,\, \mathbb{Q}(\sqrt{3}, i)^\times) \simeq \mathbb{Z}/2,$$
$$H^{-1}(G,\, \mathbb{Q}(\sqrt{2}, \sqrt{3})^\times) \simeq \mathbb{Z}/2,$$
$$H^{-1}(G,\, \mathbb{Q}(\sqrt{3}, \sqrt{5})^\times) \simeq (\mathbb{Z}/2)^2,$$
$$H^{-1}(G,\, \mathbb{Q}(\sqrt{3}, \sqrt{7})^\times) \simeq \mathbb{Z}/2.$$

Beweis: Sei zuerst $K = \mathbb{Q}(\sqrt{2}, i)$ oder $K = \mathbb{Q}(\sqrt{3}, i)$. Weil K die Klassenzahl 1 hat, wird nach Satz 2.7 jede Klasse von $H^{-1}(G, K^\times)$ durch eine Einheit von K repräsentiert. Da die G-Konjugierten einer Einheit von K ebenfalls Einheiten von K sind, ist die Norm einer Einheit von K über $\mathbb{Q}(i)$ als Produkt von Einheiten von

K eine Einheit von $\mathbb{Q}(i)$. Der Ganzheitsring von $\mathbb{Q}(i)$ ist $\mathbb{Z}[i]$ (vgl. [AZ, S. 49/50]) und seine Einheitengruppe ist $\{\pm 1, \pm i\}$ (vgl. [N, S. 3]). Dabei ist -1 Norm eines Corandes über $\mathbb{Q}(i)$, denn es gilt

$$-1 = i^2 = N_{K/\mathbb{Q}(i)}\, i = N_{K/\mathbb{Q}(i)} \left(\frac{1+i}{1-i} \right).$$

Es bleibt zu klären, was mit Einheiten von K ist, die über $\mathbb{Q}(i)$ die Norm i oder $-i$ haben. Beginnen wir mit $K = \mathbb{Q}(\sqrt{2}, i)$. Ob i bei $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(i)$ die Norm eines Corandes ist, erkennt man nach Satz 1.8 an der quadratischen Form

$$X_1^2 + (-1 - 1^2)X_2^2 - 2X_3^2.$$

Wie man sofort bemerkt, ist diese isotrop und i demzufolge Norm eines Corandes über $\mathbb{Q}(i)$. Weil auch -1 Norm eines Corandes über $\mathbb{Q}(i)$ ist, sind in $K = \mathbb{Q}(\sqrt{2}, i)$ also alle Einheiten Coränder und mit Satz 2.7 folgt, dass $H^{-1}(G, K^\times)$ in diesem Fall trivial ist. Kommen wir nun zu $K = \mathbb{Q}(\sqrt{3}, i)$. Um zu erkennen, ob i bei $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}(i)$ die Norm eines Corandes ist, haben wir wiederum nach Satz 1.8 die quadratische Form

$$X_1^2 + (-1 - 1^2)X_2^2 - 3X_3^2$$

zu betrachten. Sie ist nicht isotrop, weil die Kongruenz $X^2 \equiv 2(3)$ wegen $(\frac{2}{3}) = -1$ in $\mathbb{Z}$ nicht lösbar ist, vgl. Korollar 1.3. Es folgt, dass i nicht Norm eines Corandes über $\mathbb{Q}(i)$ ist. Wenn man ein Element von K angeben kann, das über $\mathbb{Q}(i)$ die Norm i hat, so ist dieses kein Corand und gehört damit einer nicht-trivialen Klasse von $H^{-1}(G, K^\times)$ an. Tatsächlich gilt

$$N_{K/\mathbb{Q}(i)} \left(\frac{1 + 2i + \sqrt{3}i}{2} \right) = \frac{(1+2i)^2 - 3 \cdot (-1)}{4} = \frac{1 - 4 + 3 + 4i}{4} = i,$$

womit nachgewiesen ist, dass die Norm i bei $K/\mathbb{Q}(i)$ wirklich auftritt. Die von $(1+2i+\sqrt{3}i)/2$ erzeugte Klasse aus $H^{-1}(G, K^\times)$ ist die einzige nicht-triviale Klasse, denn ansonsten kommt nur die Norm $-i$ über $\mathbb{Q}(i)$ für Einheiten aus nicht-trivialen Klassen von $H^{-1}(G, K^\times)$ in Frage, doch

$$\frac{1 + 2i + \sqrt{3}i}{2} \cdot \frac{1+i}{1-i}$$

ist ein Element von K mit der Norm $-i$ über $\mathbb{Q}(i)$ und unterscheidet sich von $(1 + 2i + \sqrt{3}i)/2$ nur um einen Corand. Ein weiterer Erzeuger der nicht-trivialen Klasse von $H^{-1}(G, K^\times)$ ist

$$\frac{1 + \sqrt{3}}{1 + i},$$

vgl. Satz 1.10.1.

Als nächstes betrachten wir $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $K = \mathbb{Q}(\sqrt{2}, \sqrt{17})$. Auch hier gilt nach Satz 2.7: Weil K die Klassenzahl 1 hat, wird jede Klasse von $H^{-1}(G, K^\times)$ durch eine Einheit von K repräsentiert. Die Norm einer Einheit von K über $\mathbb{Q}(\sqrt{2})$ ist eine Einheit von $\mathbb{Q}(\sqrt{2})$. Die Einheitengruppe von $\mathbb{Q}(\sqrt{2})$ ist

$$E_{\mathbb{Q}(\sqrt{2})} = \{\pm 1\} \times < 1 + \sqrt{2} >$$

(vgl. [AZ, S. 63/64]), denn die Grundeinheit von $\mathbb{Q}(\sqrt{2})$ ist $1+\sqrt{2}$ (vgl. [N, S. 45/46]). Die Grundeinheit selbst kommt als Norm über $\mathbb{Q}(\sqrt{2})$ von Elementen der Norm 1 über $\mathbb{Q}$ nicht in Frage, weil sie über $\mathbb{Q}$ die Norm -1 hat. Die Gruppe der Einheiten mit Norm 1 über $\mathbb{Q}$ ist die Untergruppe $\{\pm 1\} \times < (1 + \sqrt{2})^2 >$ von $E_{\mathbb{Q}(\sqrt{2})}$. Im

Folgenden gilt es zu bestimmen, ob es in K Coränder mit den Normen -1 oder $\pm(1+\sqrt{2})^2$ über $\mathbb{Q}(\sqrt{2})$ gibt. Fangen wir mit $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ an. Korollar 1.9 liefert, dass -1 genau dann bei $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})$ die Norm eines Corandes ist, wenn die quadratische Form

$$X_1^2 + 2X_2^2 - 3X_3^2$$

isotrop ist. Dies trifft zu, denn die Kongruenz $X^2 \equiv -2(3)$ ist in $\mathbb{Z}$ lösbar, vgl. auch Korollar 1.3. Nach Satz 1.8 ist andererseits das Element

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

von $E_{\mathbb{Q}(\sqrt{2})}$ genau dann bei $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})$ die Norm eines Corandes, wenn die quadratische Form

$$X_1^2 + (2-2^2)X_2^2 - 3X_3^2$$

eine nicht-triviale Nullstelle besitzt. Das ist nicht der Fall, denn die Kongruenz $X^2 \equiv 2(3)$ ist in $\mathbb{Z}$ nicht lösbar, s. o. oder vgl. Korollar 1.3. Demzufolge gibt es keinen Corand mit der Norm $(1+\sqrt{2})^2$ über $\mathbb{Q}(\sqrt{2})$. Jedes Element von K mit der Norm $(1+\sqrt{2})^2$ über $\mathbb{Q}(\sqrt{2})$ ist demnach kein Corand und liegt somit in einer nicht-trivialen Klasse von $H^{-1}(G,K^\times)$. Offenbar ist $1+\sqrt{2}$ ein solches. Die von ihm erzeugte Klasse ist das einzige nicht-triviale Element von $H^{-1}(G,K^\times)$, wie wir uns jetzt kurz überlegen wollen. Da die Gruppe $H^{-1}(G,K^\times)$ den Index 2 hat, sind $(1+\sqrt{2})^4$ und überhaupt alle geraden Potenzen von $(1+\sqrt{2})^2$ Normen von Coränder. Ebenso ist nach dem oben Gezeigten -1 Norm eines Corandes. Daher unterscheidet sich jedes Element der Gruppe $\{\pm 1\}\times < (1+\sqrt{2})^2 >$ um die Norm eines Corandes von 1 oder von $(1+\sqrt{2})^2$ und es folgt dass 1 und $1+\sqrt{2}$ die beiden einzigen Klassen von $H^{-1}(G,K^\times)$ ausmachen. Um zu $K = \mathbb{Q}(\sqrt{2},\sqrt{17})$ zu kommen, nach Korollar 1.9 ist -1 genau dann bei $\mathbb{Q}(\sqrt{2},\sqrt{17})/\mathbb{Q}(\sqrt{2})$ die Norm eines Corandes, wenn die quadratische Form

$$X_1^2 + 2X_2^2 - 17X_3^2$$

isotrop ist. Da wegen $(\frac{-2}{17}) = 1$ die Kongruenz $X^2 \equiv 2(17)$ in $\mathbb{Z}$ lösbar ist, gibt es eine nicht-triviale Nullstelle, vgl. Korollar 1.3. Ob $(1+\sqrt{2})^2$ bei $\mathbb{Q}(\sqrt{2},\sqrt{17})/\mathbb{Q}(\sqrt{2})$ die Norm eines Corandes ist, kann man nach Satz 1.8 an der quadratischen Form

$$X_1^2 + (2-2^2)X_2^2 - 17X_3^2$$

erkennen. Auch sie ist isotrop, denn wegen $(\frac{2}{17}) = 1$ ist die Kongruenz $X^2 \equiv 2(17)$ in $\mathbb{Z}$ lösbar, vgl. auch Korollar 1.3. Damit ist gezeigt, dass im Falle $K = \mathbb{Q}(\sqrt{2},\sqrt{17})$ alle Elemente von K mit der Norm 1 über $\mathbb{Q}$ bereits Coränder sind. Dieses Ergebnis wird in einem späteren Kapitel von Bedeutung sein.

Wir wenden uns nun $K = \mathbb{Q}(\sqrt{3},\sqrt{5})$ und $K = \mathbb{Q}(\sqrt{3},\sqrt{7})$ zu. Weil auch hier K die Klassenzahl 1 hat, wird nach Satz 2.7 jede Klasse von $H^{-1}(G,K^\times)$ durch eine Einheit von K repräsentiert. Die Norm einer Einheit von K über $\mathbb{Q}(\sqrt{3})$ ist eine Einheit von $\mathbb{Q}(\sqrt{3})$, liegt also in der Einheitengruppe

$$E_{\mathbb{Q}(\sqrt{3})} = \{\pm 1\}\times < 2+\sqrt{3} >$$

von $\mathbb{Q}(\sqrt{3})$, vgl. [AZ, S. 63/64]. Dabei ist $2+\sqrt{3}$ die Grundeinheit von $\mathbb{Q}(\sqrt{3})$, vgl. [N, S. 45/46]. Es stellt sich die Frage, ob es in K Coränder mit den Normen -1 oder $\pm(2+\sqrt{3})$ über $\mathbb{Q}(\sqrt{3})$ gibt. Betrachten wir als erstes $K = \mathbb{Q}(\sqrt{3},\sqrt{5})$. Um zu bestimmen, ob -1 bei $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{3})$ die Norm eines Corandes ist, ziehen wir gemäß Korollar 1.9 die quadratische Form

$$X_1^2 + 3X_2^2 - 5X_3^2$$

heran. Sie ist nicht isotrop, denn wegen $(\frac{5}{3}) = -1$ ist die Kongruenz $X^2 \equiv 5(3)$ in $\mathbb{Z}$ nicht lösbar, vgl. Theorem 1.2. Ob die Grundeinheit

$$2 + \sqrt{3} = \frac{3 + \sqrt{3}}{3 - \sqrt{3}}$$

von $\mathbb{Q}(\sqrt{3})$ bei $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3})$ die Norm eines Corandes ist, ist nach Satz 1.8 an der quadratischen Form

$$X_1^2 + (3 - 3^2)X_2^2 - 5X_3^2$$

zu erkennen. Sie ist ebenfalls nicht isotrop, weil wie gesagt die Kongruenz $X^2 \equiv 5(3)$ wegen $(\frac{5}{3}) = -1$ in $\mathbb{Z}$ nicht lösbar ist, vgl. Theorem 1.2. Nach Satz 1.8 ist schließlich das Element

$$-(2 + \sqrt{3}) = \frac{1 + \sqrt{3}}{1 - \sqrt{3}}$$

von $E_{\mathbb{Q}(\sqrt{3})}$ genau dann bei $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{3})$ die Norm eines Corandes, wenn die quadratische Form

$$X_1^2 + (3 - 1^2)X_2^2 - 5X_3^2$$

isotrop ist. Auch dieser Fall tritt nicht ein (vgl. Korollar 1.3), denn wegen $(\frac{-2}{5}) = -1$ ist die Kongruenz $X^2 \equiv -2(5)$ in $\mathbb{Z}$ nicht lösbar. Im Ergebnis ist also weder -1 noch $2 + \sqrt{3}$ noch $-(2 + \sqrt{3})$ die Norm eines Corandes über $\mathbb{Q}(\sqrt{3})$. Wir können jedoch sofort Elemente von K angeben, die über $\mathbb{Q}(\sqrt{3})$ gerade diese Normen haben. Es gilt

$$N_{K/\mathbb{Q}(\sqrt{3})}(2 + \sqrt{5}) = -1$$

sowie

$$N_{K/\mathbb{Q}(\sqrt{3})}\left(\frac{1 + 2\sqrt{3} + \sqrt{5}}{2}\right) = \frac{(1 + 2\sqrt{3})^2 - 5}{4} = \frac{1 + 12 - 5 + 4\sqrt{3}}{4} = 2 + \sqrt{3}$$

und weiter hat man

$$\begin{aligned} N_{K/\mathbb{Q}(\sqrt{3})}\left(\frac{3 + \sqrt{3} + \sqrt{5} + \sqrt{15}}{2}\right) &= \frac{(3 + \sqrt{3})^2 - 5(1 + \sqrt{3})^2}{4} \\ &= \frac{9 + 3 - 5 - 15 + (6 - 10)\sqrt{3}}{4} = -(2 + \sqrt{3}). \end{aligned}$$

Es handelt sich um Elemente von K der Norm 1 über $\mathbb{Q}$, die Vertreter nicht-trivialer Klassen von $H^{-1}(G, K^\times)$ sind. Genauer gesagt liegen

$$2 + \sqrt{5}, \quad \frac{1 + 2\sqrt{3} + \sqrt{5}}{2}, \quad \frac{3 + \sqrt{3} + \sqrt{5} + \sqrt{15}}{2}$$

nach Satz 1.7 in paarweise verschiedenen nicht-trivialen Klassen von $H^{-1}(G, K^\times)$, denn auch ihre Quotienten haben über $\mathbb{Q}(\sqrt{3})$ die Normen -1 und $\pm(2 + \sqrt{3})$, und diese Einheiten von $\mathbb{Q}(\sqrt{3})$ sind nicht Normen von Corändern. Weitere nicht-triviale Klassen aus $H^{-1}(G, K^\times)$ gibt es nicht, wie wir kurz zeigen wollen. Da $H^{-1}(G, K^\times)$ den Index 2 hat, sind alle geraden Potenzen von $2 + \sqrt{3}$ Normen von Corändern. Jedes Element der Einheitengruppe von $\mathbb{Q}(\sqrt{3})$ unterscheidet sich also um die Norm eines Corandes von -1 oder $\pm(2 + \sqrt{3})$, so dass sich jedes Element von K mit Norm 1 über $\mathbb{Q}$ um einen Corand von 1 oder einem der oben genannten Elemente von K unterscheidet. Für $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ erhalten wir demnach $H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^2$. Kommen wir nun zu $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Um die Frage zu beantworten, ob -1 bei

$\mathbb{Q}(\sqrt{3},\sqrt{7})/\mathbb{Q}(\sqrt{3})$ die Norm eines Corandes ist, betrachten wir gemäß Korollar 1.9 die quadratische Form

$$X_1^2 + 3X_2^2 - 7X_3^2.$$

Sie ist nach Theorem 1.2 isotrop, denn es gilt $(\frac{-3}{7}) = (\frac{7}{3}) = 1$ und somit sind die Kongruenzen $X^2 \equiv -3(7)$ und $X^2 \equiv 7(3)$ in $\mathbb{Z}$ lösbar. Also ist -1 die Norm eines Corandes über $\mathbb{Q}(\sqrt{3})$. Um zu erkennen, ob $2+\sqrt{3}$ bei $\mathbb{Q}(\sqrt{3},\sqrt{7})/\mathbb{Q}(\sqrt{3})$ die Norm eines Corandes ist, ziehen wir die quadratische Form

$$X_1^2 + (3-3^2)X_2^2 - 7X_3^2$$

heran. Diese ist nach Theorem 1.2 nicht isotrop, weil $(\frac{6}{7}) = -1$ gilt und daher die Kongruenz $X^2 \equiv 6(7)$ in $\mathbb{Z}$ nicht lösbar ist. Wenn man ein Element von K angeben kann, das über $\mathbb{Q}(\sqrt{3})$ die Norm $2+\sqrt{3}$ hat, so liegt dieses in einer nicht-trivialen Klasse von $H^{-1}(G, K^\times)$. Tatsächlich gilt

$$N_{K/\mathbb{Q}(\sqrt{3})}\left(\frac{3+3\sqrt{3}+\sqrt{7}+\sqrt{21}}{2}\right) = \frac{(3+3\sqrt{3})^2 - 7(1+\sqrt{3})^2}{4}$$
$$= \frac{9+27-7-21+(18-14)\sqrt{3}}{4} = 2+\sqrt{3},$$

womit ein Element aus einer nicht-trivialen Klasse von $H^{-1}(G, K^\times)$ gefunden ist. Genauer wird von

$$\frac{3+3\sqrt{3}+\sqrt{7}+\sqrt{21}}{2}$$

die einzige nicht-triviale Klasse von $H^{-1}(G, K^\times)$ erzeugt, denn $H^{-1}(G, K^\times)$ hat den Index 2, so dass alle geraden Potenzen von $2+\sqrt{3}$ Normen von Corändern sind. Jedes Element der Einheitengruppe von $\mathbb{Q}(\sqrt{3})$ unterscheidet sich demzufolge um die Norm eines Corandes von 1 oder von $2+\sqrt{3}$. Ein weiterer Verteter der nicht-trivialen Klasse von $H^{-1}(G, K^\times)$ ist

$$\frac{1+\sqrt{3}}{3+\sqrt{7}},$$

vgl. Satz 1.16.1.

Als letztes bleibt $K = \mathbb{Q}(\sqrt{13},\sqrt{17})$ zu betrachten. Auch in diesem Fall hat K die Klassenzahl 1, so dass nach Satz 2.7 jede Klasse von $H^{-1}(G, K^\times)$ durch eine Einheit von K repräsentiert wird. Die Norm einer Einheit von K über $\mathbb{Q}(\sqrt{13})$ ist eine Einheit von $\mathbb{Q}(\sqrt{13})$. Die Einheitengruppe von $\mathbb{Q}(\sqrt{13})$ ist

$$E_{\mathbb{Q}(\sqrt{13})} = \{\pm 1\} \times \left\langle \frac{3+\sqrt{13}}{2} \right\rangle$$

(vgl. [AZ, S. 63/64]), denn die Grundeinheit von $\mathbb{Q}(\sqrt{13})$ ist $(3+\sqrt{13})/2$ (vgl. [N, S. 45/46]). Die Grundeinheit $(3+\sqrt{13})/2$ hat über $\mathbb{Q}$ die Norm -1 und kann daher nicht Norm von Elementen von K der Norm 1 über $\mathbb{Q}$ sein. Die Gruppe der Einheiten von $\mathbb{Q}(\sqrt{13})$ mit Norm 1 über $\mathbb{Q}$ ist

$$\{\pm 1\} \times \left\langle \left(\frac{3+\sqrt{13}}{2}\right)^2 \right\rangle.$$

Es gilt zu klären, was mit Elementen von K der Norm -1 oder $\pm((3+\sqrt{13})/2)^2$ über $\mathbb{Q}(\sqrt{13})$ ist. Zunächst wollen wir prüfen, ob -1 bei $\mathbb{Q}(\sqrt{13},\sqrt{17})/\mathbb{Q}(\sqrt{13})$ die Norm eines Corandes ist. Nach Korollar 1.9 ist dies genau dann der Fall, wenn die quadratische Form

$$X_1^2 + 13X_2^2 - 17X_3^2$$

isotrop ist. Das ist sie (vgl. Theorem 1.2), denn wegen $(\frac{-13}{17}) = (\frac{17}{13}) = 1$ sind die Kongruenzen $X^2 \equiv -13(17)$ und $X^2 \equiv 17(13)$ über $\mathbb{Z}$ lösbar. Ob

$$\left(\frac{3+\sqrt{13}}{2}\right)^2 = \frac{13+3\sqrt{13}}{13-3\sqrt{13}}$$

bei $\mathbb{Q}(\sqrt{13},\sqrt{17})/\mathbb{Q}(\sqrt{13})$ die Norm eines Corandes ist, ist nach Satz 1.8 an der quadratischen Form

$$X_1^2 + (13 - \big(\frac{13}{3}\big)^2)X_2^2 - 17X_3^2$$

zu erkennen. Genauso kann man auch die quadratische Form

$$X_1^2 + (13 \cdot 3^2 - 13^2)X_2^2 - 17X_3^2$$

und in einem zweiten Schritt

$$X_1^2 - 13X_2^2 - 17X_3^2$$

betrachten. Diese Formen sind ebenfalls isotrop, denn wegen $(\frac{13}{17}) = (\frac{17}{13}) = 1$ sind die Kongruenzen $X^2 \equiv 13(17)$ und $X^2 \equiv 17(13)$ über $\mathbb{Z}$ lösbar, vgl. Theorem 1.2. Es folgt, dass die Gruppe $H^{-1}(G, K^\times)$ für $K = \mathbb{Q}(\sqrt{13},\sqrt{17})$ trivial ist. Dieses Resultat wird wie das im Fall $K = \mathbb{Q}(\sqrt{2},\sqrt{17})$ an späterer Stelle von Bedeutung sein. □

Im Beweis von Satz 2.18 haben wir explizit Coränder angegeben, welche die nichttrivialen Klassen von $H^{-1}(G, K^\times)$ erzeugen. Das halten wir in einer Tabelle fest:

Körper	$H^{-1}(G, K^\times)$	erzeugende Elemente von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{2}, i)$	0	
$\mathbb{Q}(\sqrt{3}, i)$	$\mathbb{Z}/2$	$\frac{1+\sqrt{3}}{1+i}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{17})$	0	
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	$(\mathbb{Z}/2)^2$	$2+\sqrt{5}$, $\frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}$
$\mathbb{Q}(\sqrt{3}, \sqrt{7})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{7}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{13}, \sqrt{17})$	0	

Durch die Betrachtung weiterer Körper der Klassenzahl 1 erhält man noch eine Reihe von Beispielen, in denen die Berechnung von $H^{-1}(G, K^\times)$ auf eine relativ elementare Art möglich ist. Die Ergebnisse sind auf den folgenden Seiten in Tabellen wiedergegeben.

Körper	$H^{-1}(G, K^\times)$	erzeugendes Element von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{2}, i)$	0	
$\mathbb{Q}(\sqrt{3}, i)$	$\mathbb{Z}/2$	$\frac{1+\sqrt{3}}{1+i}$
$\mathbb{Q}(\sqrt{5}, i)$	0	
$\mathbb{Q}(\sqrt{7}, i)$	0	
$\mathbb{Q}(\sqrt{11}, i)$	$\mathbb{Z}/2$	$\frac{3+\sqrt{11}}{1+i}$
$\mathbb{Q}(\sqrt{13}, i)$	0	
$\mathbb{Q}(\sqrt{19}, i)$	$\mathbb{Z}/2$	$\frac{1+\sqrt{19}}{3(1+i)}$ oder $\frac{13+3\sqrt{19}}{1+i}$
$\mathbb{Q}(\sqrt{37}, i)$	0	
$\mathbb{Q}(\sqrt{43}, i)$	$\mathbb{Z}/2$	$\frac{5+\sqrt{43}}{3(1+i)}$ oder $\frac{59+9\sqrt{43}}{1+i}$
$\mathbb{Q}(\sqrt{67}, i)$	$\mathbb{Z}/2$	$\frac{7+\sqrt{67}}{3(1+i)}$ oder $\frac{221+27\sqrt{67}}{1+i}$

Körper	$H^{-1}(G, K^\times)$	erzeugendes Element von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $2+\sqrt{5}$
$\mathbb{Q}(\sqrt{2}, \sqrt{7})$	0	
$\mathbb{Q}(\sqrt{2}, \sqrt{11})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{13})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$
$\mathbb{Q}(\sqrt{2}, \sqrt{17})$	0	
$\mathbb{Q}(\sqrt{2}, \sqrt{19})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{23})$	0	
$\mathbb{Q}(\sqrt{2}, \sqrt{29})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$
$\mathbb{Q}(\sqrt{2}, \sqrt{31})$	0	
$\mathbb{Q}(\sqrt{2}, \sqrt{37})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{2}, \sqrt{43})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{47})$	0	
$\mathbb{Q}(\sqrt{2}, \sqrt{53})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $\frac{7+\sqrt{53}}{2}$ oder $182+25\sqrt{53}$
$\mathbb{Q}(\sqrt{2}, \sqrt{59})$	$\mathbb{Z}/2$	$1+\sqrt{2}$
$\mathbb{Q}(\sqrt{2}, \sqrt{61})$	$\mathbb{Z}/2$	$1+\sqrt{2}$ oder $\frac{6+\sqrt{61}}{5}$
$\mathbb{Q}(\sqrt{2}, \sqrt{67})$	$\mathbb{Z}/2$	$1+\sqrt{2}$

Körper	$H^{-1}(G,K^\times)$	erzeugende Elemente von $H^{-1}(G,K^\times)$
$\mathbb{Q}(\sqrt{3},\sqrt{5})$	$(\mathbb{Z}/2)^2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$, $\frac{3+\sqrt{3}+\sqrt{5}+\sqrt{15}}{2}$
$\mathbb{Q}(\sqrt{3},\sqrt{7})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{7}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{11})$	0	
$\mathbb{Q}(\sqrt{3},\sqrt{13})$	0	
$\mathbb{Q}(\sqrt{3},\sqrt{17})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$ oder $\frac{5+\sqrt{17}}{2(1+\sqrt{3})}$
$\mathbb{Q}(\sqrt{3},\sqrt{19})$	0	
$\mathbb{Q}(\sqrt{3},\sqrt{23})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{23}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{29})$	$(\mathbb{Z}/2)^2$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$, $\frac{9+3\sqrt{3}+\sqrt{29}+\sqrt{87}}{2}$
$\mathbb{Q}(\sqrt{3},\sqrt{31})$	$\mathbb{Z}/2$	$\frac{7+\sqrt{31}}{3(1+\sqrt{3})}$ oder $\frac{39+7\sqrt{31}}{1+\sqrt{3}}$
$\mathbb{Q}(\sqrt{3},\sqrt{37})$	0	
$\mathbb{Q}(\sqrt{3},\sqrt{41})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$ oder $\frac{7+\sqrt{41}}{2(1+\sqrt{3})}$
$\mathbb{Q}(\sqrt{3},\sqrt{43})$	0	
$\mathbb{Q}(\sqrt{3},\sqrt{47})$	$\mathbb{Z}/2$	$\frac{7+\sqrt{47}}{1+\sqrt{3}}$

Körper	$H^{-1}(G, K^\times)$	erzeugende Elemente von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{5}, \sqrt{7})$	$(\mathbb{Z}/2)^2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$, $\frac{7+3\sqrt{5}+3\sqrt{7}+\sqrt{35}}{2}$
$\mathbb{Q}(\sqrt{5}, \sqrt{11})$	0	
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$ oder $\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$ oder $\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{5}, \sqrt{19})$	0	
$\mathbb{Q}(\sqrt{5}, \sqrt{23})$	$(\mathbb{Z}/2)^2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$, $\frac{23+5\sqrt{5}+5\sqrt{23}+\sqrt{115}}{6}$
$\mathbb{Q}(\sqrt{5}, \sqrt{31})$	0	
$\mathbb{Q}(\sqrt{5}, \sqrt{37})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$ oder $\frac{1+\sqrt{37}}{6}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{5}, \sqrt{41})$	0	
$\mathbb{Q}(\sqrt{5}, \sqrt{43})$	$(\mathbb{Z}/2)^2$	$\frac{1+\sqrt{5}}{2}$ oder $2+\sqrt{5}$, $\frac{43+15\sqrt{5}+5\sqrt{43}+3\sqrt{215}}{6}$

Körper	$H^{-1}(G, K^\times)$	erzeugende Elemente von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{7}, \sqrt{11})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{7}}{3+\sqrt{11}}$
$\mathbb{Q}(\sqrt{7}, \sqrt{13})$	$(\mathbb{Z}/2)^2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$, $\frac{7+\sqrt{7}+\sqrt{13}+\sqrt{91}}{6}$
$\mathbb{Q}(\sqrt{7}, \sqrt{17})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{7}, \sqrt{19})$	$\mathbb{Z}/2$	$\frac{3(3+\sqrt{7})}{1+\sqrt{19}}$ oder $\frac{3+\sqrt{7}}{13+3\sqrt{19}}$
$\mathbb{Q}(\sqrt{7}, \sqrt{23})$	0	
$\mathbb{Q}(\sqrt{7}, \sqrt{29})$	0	
$\mathbb{Q}(\sqrt{7}, \sqrt{31})$	0	
$\mathbb{Q}(\sqrt{7}, \sqrt{37})$	0	
$\mathbb{Q}(\sqrt{7}, \sqrt{41})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$
$\mathbb{Q}(\sqrt{7}, \sqrt{43})$	$\mathbb{Z}/2$	$\frac{3(3+\sqrt{7})}{5+\sqrt{43}}$ oder $\frac{3+\sqrt{7}}{59+9\sqrt{43}}$
$\mathbb{Q}(\sqrt{7}, \sqrt{47})$	0	

Körper	$H^{-1}(G, K^\times)$	erzeugende Elemente von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{11}, \sqrt{13})$	$(\mathbb{Z}/2)^2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$, $\frac{11+3\sqrt{11}+3\sqrt{13}+\sqrt{143}}{2}$
$\mathbb{Q}(\sqrt{11}, \sqrt{17})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{11}, \sqrt{19})$	0	
$\mathbb{Q}(\sqrt{11}, \sqrt{23})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{11}}{5+\sqrt{23}}$
$\mathbb{Q}(\sqrt{11}, \sqrt{29})$	$(\mathbb{Z}/2)^2$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$, $\frac{11+3\sqrt{11}+3\sqrt{29}+\sqrt{319}}{6}$
$\mathbb{Q}(\sqrt{11}, \sqrt{31})$	$\mathbb{Z}/2$	$\frac{3(3+\sqrt{11})}{7+\sqrt{31}}$ oder $\frac{3+\sqrt{11}}{39+7\sqrt{31}}$
$\mathbb{Q}(\sqrt{11}, \sqrt{37})$	0	
$\mathbb{Q}(\sqrt{11}, \sqrt{41})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$
$\mathbb{Q}(\sqrt{11}, \sqrt{47})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{11}}{7+\sqrt{47}}$

Körper	$H^{-1}(G, K^\times)$	erzeugende Elemente von $H^{-1}(G, K^\times)$
$\mathbb{Q}(\sqrt{13}, \sqrt{17})$	0	
$\mathbb{Q}(\sqrt{13}, \sqrt{19})$	$(\mathbb{Z}/2)^2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$, $\frac{19+5\sqrt{13}+5\sqrt{19}+\sqrt{247}}{6}$
$\mathbb{Q}(\sqrt{13}, \sqrt{23})$	0	
$\mathbb{Q}(\sqrt{13}, \sqrt{29})$	0	
$\mathbb{Q}(\sqrt{13}, \sqrt{31})$	$(\mathbb{Z}/2)^2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$, $\frac{31+7\sqrt{13}+7\sqrt{31}+\sqrt{403}}{18}$
$\mathbb{Q}(\sqrt{13}, \sqrt{37})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$ oder $\frac{1+\sqrt{37}}{6}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{13}, \sqrt{41})$	$\mathbb{Z}/2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$ oder $\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$
$\mathbb{Q}(\sqrt{13}, \sqrt{47})$	$(\mathbb{Z}/2)^2$	$\frac{3+\sqrt{13}}{2}$ oder $18+5\sqrt{13}$, $\frac{47+9\sqrt{13}+9\sqrt{47}+\sqrt{611}}{34}$

Körper	$H^{-1}(G,K^\times)$	erzeugende Elemente von $H^{-1}(G,K^\times)$
$\mathbb{Q}(\sqrt{17},\sqrt{23})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{17},\sqrt{29})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$ oder $\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$
$\mathbb{Q}(\sqrt{17},\sqrt{31})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$
$\mathbb{Q}(\sqrt{17},\sqrt{37})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{17}}{4}$ oder $4+\sqrt{17}$ oder $\frac{1+\sqrt{37}}{6}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{19},\sqrt{23})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{19}}{3(5+\sqrt{23})}$ oder $\frac{13+3\sqrt{19}}{5+\sqrt{23}}$
$\mathbb{Q}(\sqrt{19},\sqrt{29})$	$(\mathbb{Z}/2)^2$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$, $\frac{19+3\sqrt{19}+3\sqrt{29}+\sqrt{551}}{10}$
$\mathbb{Q}(\sqrt{19},\sqrt{37})$	$(\mathbb{Z}/2)^2$	$\frac{1+\sqrt{37}}{6}$ oder $6+\sqrt{37}$, $\frac{19+\sqrt{19}+\sqrt{37}+\sqrt{703}}{18}$
$\mathbb{Q}(\sqrt{19},\sqrt{47})$	$\mathbb{Z}/2$	$\frac{1+\sqrt{19}}{3(7+\sqrt{47})}$ oder $\frac{13+3\sqrt{19}}{7+\sqrt{47}}$
$\mathbb{Q}(\sqrt{29},\sqrt{37})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$ oder $\frac{1+\sqrt{37}}{6}$ oder $6+\sqrt{37}$
$\mathbb{Q}(\sqrt{29},\sqrt{41})$	$\mathbb{Z}/2$	$\frac{5+\sqrt{29}}{2}$ oder $70+13\sqrt{29}$ oder $\frac{5+\sqrt{41}}{4}$ oder $32+5\sqrt{41}$
$\mathbb{Q}(\sqrt{37},\sqrt{41})$	0	

3. Zur Bestimmung von $H^{-1}(G, K^\times)$ für galoissche Erweiterungen algebraischer Zahlkörper

In diesem Kapitel soll gezeigt werden, wie die Gruppe $H^{-1}(G, K^\times)$ im Falle einer biquadratischen Erweiterung K/k algebraischer Zahlkörper mit der Galoisgruppe $G \simeq (\mathbb{Z}/2)^2$ unter Anwendung der kohomologischen Fassung der Klassenkörpertheorie nach Tate bestimmt werden kann. Wir formulieren sogleich das zentrale

3.1 Theorem. *Sei K/k eine biquadratische Erweiterung algebraischer Zahlkörper, mit Galoisgruppe $G \simeq (\mathbb{Z}/2)^2$. Dann ist $H^{-1}(G, K^\times)$ bis auf Isomorphie vollständig bestimmt durch die Anzahl n der Stellen $\mathfrak{p}$ von k mit lokaler Galoisgruppe $G_\mathfrak{p} = G$. Genauer gilt für alle $n \geq 0$*

$$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{n-1},$$

wobei $(\mathbb{Z}/2)^{-1} = 0$ im Falle $n = 0$ zu lesen ist. Jede Zahl $n \geq 0$ lässt sich für eine biquadratische Erweiterung $K/\mathbb{Q}$ realisieren.

Der Beweis von Theorem 3.1 wird sich über das gesamte Kapitel und einen Teil des folgenden Kapitels erstrecken. In diesem Kapitel werden wir die Gleichung $H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{n-1}$ beweisen, wobei der Fall $n = 0$ die eigentliche Schwierigkeit darstellen wird. Wie in der Einleitung bereits näher ausgeführt werden wir das Problem auf zwei verschiedene Weisen angehen: einmal soweit wie möglich mit klassisch-zahlentheoretischen Mitteln, wobei wir auf Resultate von Kapitel 2 zurückgreifen, zum anderen auf rein kohomologischem Wege. In Kapitel 4 schließlich werden wir zeigen, dass sich jedes $n \geq 0$ für eine biquadratische Erweiterung $K/\mathbb{Q}$ realisieren lässt und dass jede der zweielementigen Untergruppen von G als lokale Galoisgruppe auftritt (dies werden wir im Fall $n = 0$ benötigen).

3.i Zur kohomologischen Fassung der Klassenkörpertheorie nach Tate

Es sei K/k eine galoissche Erweiterung algebraischer Zahlkörper mit Galoisgruppe G. Anders als bei der Betrachtung lokaler Körper wird in dieser Situation nicht direkt mit der multiplikativen Gruppe $K^\times$ von K gearbeitet, sondern es wird mit der *Idelgruppe* I_K von K ein weiterer G-Modul in das Geschehen einbezogen. Bezeichnet $\mathcal{P}(K)$ die Menge aller Stellen (Äquivalenzklassen von Absolutbeträgen) von K, so gilt nach Definition

$$I_K = \{(\alpha_\mathfrak{p})_\mathfrak{p} \in \prod_{\mathfrak{p} \in \mathcal{P}(K)} K_\mathfrak{p}^\times : \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{ für fast alle Stellen } \mathfrak{p}\},$$

wobei $K_\mathfrak{p}$ die Komplettierung von K bzgl. $\mathfrak{p}$ und $U_\mathfrak{p}$ die Elemente vom Betrag 1 bezeichnet. Da jedes $a \in K^\times$ eine Einheit für fast alle Stellen $\mathfrak{p}$ von K ist, besteht eine natürliche Inklusion $K^\times \to I_K$, $a \to (\alpha_\mathfrak{p})_\mathfrak{p}$, mit $\alpha_\mathfrak{p} = a$ für alle $\mathfrak{p}$, und man erhält eine kurze exakte Sequenz von G-Moduln

$$1 \to K^\times \to I_K \to C_K \to 1$$

Die Faktorgruppe $C_K = I_K/K^\times$ ist die *Idelklassengruppe* von K, vgl. [AZ, S. 58]. Zu dieser kurzen exakten Sequenz von Koeffizientenmoduln gehört die lange exakte Kohomologiesequenz der Tate-Kohomologiegruppen der endlichen Gruppe G

$$\to H^{i-1}(G, I_K) \to H^{i-1}(G, C_K) \to H^i(G, K^\times) \to H^i(G, I_K) \to H^i(G, C_K) \to$$

(siehe etwa [CF, S. 102]). An dieser Stelle kommt nun die kohomologische Fassung der Klassenkörpertheorie nach Tate hinzu, nach der für alle $i \in \mathbb{Z}$ kanonische Isomorphismen

$$H^i(G, C_K) \simeq H^{i-2}(G, \mathbb{Z})$$

bestehen, siehe [CF, S. 197]. Außerdem gilt für alle $i \in \mathbb{Z}$

$$H^i(G, I_K) \simeq \bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H^i(G_\mathfrak{p}, K_\mathfrak{p}^\times) \simeq \bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H^{i-2}(G_\mathfrak{p}, \mathbb{Z}),$$

auch dies kanonisch ([CF, S. 177]). Die Summe erstreckt sich jeweils über alle $\mathfrak{p} \in \mathcal{P}(k)$, und mit $G_\mathfrak{p}$ wird für jede Stelle $\mathfrak{p}$ des Grundkörpers k die Zerlegungsgruppe von $\mathfrak{P}$ in Bezug auf die Erweiterung K/k bezeichnet, wobei $\mathfrak{P}$ eine der über $\mathfrak{p}$ liegenden Stellen von K ist; dann ist $G_\mathfrak{p}$ eine Untergruppe von G, die mit der lokalen Galoisgruppe $G(K_\mathfrak{P}/k_\mathfrak{p})$ identifiziert werden kann ([AZ, S. 105]; vgl. auch Kapitel 4). Genauer gesagt unterscheiden sich die Gruppen $G_\mathfrak{P}$ für die $\mathfrak{p}$ teilenden Stellen $\mathfrak{P}$ von K voneinander um kanonische Isomorphismen; im Falle einer abelschen Erweiterung K/k sind sie alle gleich, vgl. Abschnitt 4.i. Im zweiten Schritt wurde verwendet, dass wiederum nach Tate im Falle einer galoisschen Erweiterung lokaler Körper L/E stets $H^i(G(L/E), L^\times) \simeq H^{i-2}(G(L/E), \mathbb{Z})$ gilt.

Unter Verwendung dieser Isomorphismen präsentieren sich die Abbildungen

$$g : H^i(G, I_K) \to H^i(G, C_K)$$

in der langen exakten Kohomologiesequenz nun als Abbildungen

$$g : \bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H^{i-2}(G_\mathfrak{p}, \mathbb{Z}) \to H^{i-2}(G, \mathbb{Z})$$

und nach [CF, S. 198] gilt

$$g((z_\mathfrak{p})_\mathfrak{p}) = \sum_{\mathfrak{p} \in \mathcal{P}(k)} cor_G^{G_\mathfrak{p}}(z_\mathfrak{p}),$$

mit den Corestriktionsabbildungen

$$cor_G^{G_\mathfrak{p}} : H^{i-2}(G_\mathfrak{p}, \mathbb{Z}) \to H^{i-2}(G, \mathbb{Z}).$$

Wir sind interessiert an der Gruppe $H^{-1}(G, K^\times)$. Nach dem Vorangegangenen gibt es eine exakte Sequenz

$$\bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H^{-4}(G_\mathfrak{p}, \mathbb{Z}) \to H^{-4}(G, \mathbb{Z}) \to H^{-1}(G, K^\times) \to$$

$$\bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H^{-3}(G_\mathfrak{p}, \mathbb{Z}) \to H^{-3}(G, \mathbb{Z})$$

Nun stimmen die Tate-Kohomologiegruppen $H^{-q}(G, M)$ einer endlichen Gruppe G in Dimensionen $-q < -1$ mit den (gewöhnlichen) Homologiegruppen $H_{q-1}(G, M)$ von G überein, und die Corestriktionsabbildung

$$cor_G^U : H^{-q}(U, M) \to H^{-q}(G, M)$$

für eine Untergruppe $i : U \hookrightarrow G$ von G ist gleich der induzierten (funktoriellen) Abbildung

$$i_* : H_{q-1}(U, M) \to H_{q-1}(G, M)$$

([CF, S. 104], [B, S. 80, 130]). Es ergibt sich daher die folgende exakte Sequenz (die Homologiegruppen haben Koeffizienten in $\mathbb{Z}$, mit trivialer Gruppenoperation)

$$\bigoplus_{\mathfrak{p}\in\mathcal{P}(k)} H_3(G_\mathfrak{p}) \to H_3(G) \to H^{-1}(G, K^\times) \to \bigoplus_{\mathfrak{p}\in\mathcal{P}(k)} H_2(G_\mathfrak{p}) \to H_2(G),$$

und die äußersten linken und rechten Abbildungen sind die Summe der von den Inklusionen $i : G_\mathfrak{p} \hookrightarrow G$ induzierten Abbildungen.

Bemerkung. Nach dem Vorangegangenen gilt für eine galoissche Erweiterung L/E lokaler Körper $H^{-1}(G(L/E), L^\times) \simeq H^{-3}(G(L/E), \mathbb{Z}) \simeq H_2(G(L/E), \mathbb{Z})$, insbesondere hängt der Isomorphietyp der Gruppe $H^{-1}(G(L/E), L^\times)$ nur von der Gruppe $G(E/L)$ ab und nicht von der Körpererweiterung (die Gruppe $H_2(G, \mathbb{Z})$ wird auch als Schur-Multiplikator der Gruppe G bezeichnet). Wie sich zeigen wird, bleibt dies nicht mehr richtig für galoissche Erweiterungen algebraischer Zahlkörper (globaler Körper).

3.ii Biquadratische Erweiterungen

Die Ergebnisse von Abschnitt 3.i sollen nun auf biquadratische Erweiterungen K/k algebraischer Zahlkörper, mit Galoisgruppe $G = (\mathbb{Z}/2)^2$, angewandt werden, mit dem Ziel der Bestimmung der Gruppe $H^{-1}(G, K^\times)$. Wir beginnen mit einigen Kommentaren zur Berechnung der Homologiegruppen in der exakten Sequenz am Ende von Abschnitt 3.i.

Nach der Künneth-Formel für die Homologie von Gruppen gibt es eine spaltende exakte Sequenz ([B, S. 120],[HS, S .223])

$$0 \to \bigoplus_{i+j=n} H_i(\mathbb{Z}/2) \otimes H_j(\mathbb{Z}/2) \to H_n((\mathbb{Z}/2)^2) \to$$
$$\bigoplus_{i+j=n-1} \mathrm{Tor}(H_i(\mathbb{Z}/2), H_j(\mathbb{Z}/2)) \to 0,$$

insbesondere ist $H_n((\mathbb{Z}/2)^2)$ isomorph zur direkten Summe der beiden äußeren Gruppen. Zur Berechnung dieser Gruppen machen wir die folgenden Bemerkungen.

Für eine zyklische Gruppe $\mathbb{Z}/n$ der Ordnung n ist $H_0(\mathbb{Z}/n) \simeq \mathbb{Z}$, $H_i(\mathbb{Z}/n) \simeq \mathbb{Z}/n$ für ungerades i und $H_i(\mathbb{Z}/n) = 0$ in allen anderen Fällen (vgl. [B, S. 35]).

Der Torsionsfunktor $\mathrm{Tor} = \mathrm{Tor}_1^{\mathbb{Z}}$ hat folgende Eigenschaften (vgl. [SZ, S. 260]).

1. Ist A eine freie abelsche Gruppe und B eine beliebige abelsche Gruppe, so gilt $\mathrm{Tor}(A, B) = 0$.
2. Sei G eine beliebige abelsche Gruppe. Für alle $n \in \mathbb{N}$ ist $\mathrm{Tor}(\mathbb{Z}/n, G) = \{g \in G \mid ng = 0\}$.
3. Aus 2. folgt, dass $\mathrm{Tor}(\mathbb{Z}/n, A) = 0$ für jedes $n \in \mathbb{N}$ und jede torsionsfreie abelsche Gruppe A.
4. Aus 2. folgt, dass $\mathrm{Tor}(\mathbb{Z}/m, \mathbb{Z}/n) \simeq \mathbb{Z}/d$, für $m, n \in \mathbb{N}$ mit dem größten gemeinsamen Teiler d.

Andererseits gilt für das Tensorprodukt abelscher Gruppen

1. Für jede abelsche Gruppe A ist $A \otimes \mathbb{Z} \simeq \mathbb{Z} \otimes A \simeq A$.
2. Für $m, n \in \mathbb{N}$ mit größtem gemeinsamen Teiler d ist $\mathbb{Z}/m \otimes \mathbb{Z}/n \simeq \mathbb{Z}/d$.

Unter Verwendung dieser Eigenschaften ergibt sich nun aus der Künneth Formel

$H_3((\mathbb{Z}/2)^2)$
$\simeq H_0(\mathbb{Z}/2) \otimes H_3(\mathbb{Z}/2) \ \oplus \ H_3(\mathbb{Z}/2) \otimes H_0(\mathbb{Z}/2) \ \oplus \ \mathrm{Tor}(H_1(\mathbb{Z}/2), H_1(\mathbb{Z}/2))$
$\simeq \mathbb{Z} \otimes \mathbb{Z}/2 \ \oplus \ \mathbb{Z}/2 \otimes \mathbb{Z} \ \oplus \ \mathrm{Tor}(\mathbb{Z}/2, \mathbb{Z}/2);$
$\simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 = (\mathbb{Z}/2)^3;$

$H_2((\mathbb{Z}/2)^2) \simeq H_1(\mathbb{Z}/2) \otimes H_1(\mathbb{Z}/2) \simeq \mathbb{Z}/2.$

Wir wenden uns nun wieder der exakten Homologiesequenz aus Abschnitt 3.i zu:

$$\bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H_3(G_\mathfrak{p}) \to H_3(G) \to H^{-1}(G, K^\times) \to \bigoplus_{\mathfrak{p} \in \mathcal{P}(k)} H_2(G_\mathfrak{p}) \to H_2(G);$$

wie in Abschnitt 3.i bemerkt, werden die Abbildungen $i_* : H_q(G_\mathfrak{p}) \to H_q(G)$ von den Inklusionen $i : G_\mathfrak{p} \hookrightarrow G$ induziert.

Die lokalen Galoisgruppen $G_\mathfrak{p}$ sind zyklisch oder isomorph zu $G = (\mathbb{Z}/2)^2$. Bei der Bestimmung von $H^{-1}(G, K^\times)$ können nun zwei verschiedene Fälle auftreten, je nachdem ob eine der lokalen Galoisgruppen $G_\mathfrak{p}$ isomorph zu $G = (\mathbb{Z}/2)^2$ ist oder nicht, wobei der erste der einfachere ist und im folgenden der *nicht-singuläre* Fall genannt wird.

Im nicht-singulären Fall ist die Abbildung $\oplus_\mathfrak{p} H_3(G_\mathfrak{p}) \to H_3(G)$ offensichtlich surjektiv, und $H^{-1}(G, K^\times)$ ist daher isomorph zum Kern der Abbildung $\oplus_\mathfrak{p} H_2(G_\mathfrak{p}) \to H_2(G)$. Nun ist $H_2(\mathbb{Z}/2)$ trivial und $H_2(\mathbb{Z}/2)^2) \simeq \mathbb{Z}/2$. Bezeichnet $n \geq 1$ die Anzahl der Stellen $\mathfrak{p}$ von k mit $G_\mathfrak{p} \simeq (\mathbb{Z}/2)^2$, so gilt daher $\oplus_\mathfrak{p} H_2(G_\mathfrak{p}) \simeq (\mathbb{Z}/2)^n$, und es folgt $H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{n-1}$ (eine Untergruppe vom Index zwei in $\oplus_\mathfrak{p} H_2(G_\mathfrak{p})$). Die Aufgabe besteht demnach darin, die Anzahl der Stellen $\mathfrak{p}$ mit $G_\mathfrak{p} = G$ anzugeben. Sie ist stets endlich, kann jeden beliebigen Wert von n annehmen und ohne Schwierigkeiten für jede biquadratische Erweiterung über $\mathbb{Q}$ bestimmt werden (vgl. Kapitel 4). Insbesondere gilt Hilberts Satz 90 im nicht-singulären Fall genau dann, wenn genau eine der lokalen Galoisgruppen isomorph zu $(\mathbb{Z}/2)^2$ ist.

Soviel zum nicht-singulären Fall; nun soll der singuläre Fall behandelt werden, der dann vorliegt, wenn keine der lokalen Galoisgruppen isomorph zu $(\mathbb{Z}/2)^2$ ist. In dieser Situation ist jedes $G_\mathfrak{p}$ entweder trivial oder isomorph zu $\mathbb{Z}/2$. Dann ist $\oplus_\mathfrak{p} H_2(G_\mathfrak{p})$ trivial und $H^{-1}(G, K^\times)$ folglich isomorph zum Cokern der Abbildung $\oplus_\mathfrak{p} H_3(G_\mathfrak{p}) \to H_3(G) \simeq (\mathbb{Z}/2)^3$.

Wir bemerken zunächst, dass die von einer Inklusionen $i : G_\mathfrak{p} \hookrightarrow G$ induzierte Abbildung $i_* : H_3(G_\mathfrak{p}) \to H_3(G)$ injektiv ist für jede der lokalen Galoisgruppen $G_\mathfrak{p} \simeq \mathbb{Z}/2$. Dazu betrachte man eine Projektion $p : G \to G_\mathfrak{p}$, mit $p \circ i = id_{G_\mathfrak{p}}$. Aus der Funktorialität der gewöhnlichen Homologie von Gruppen ergibt sich dann für die induzierten Abbildungen der Homologiegruppen $(p \circ i)_* = p_* \circ i_* = (id_{G_\mathfrak{p}})_* = id_{H_3(G_\mathfrak{p})}$. Daher ist i_* injektiv.

Es stellt sich daher die Frage, wie $H_3(G_\mathfrak{p})$ für eine lokale Galoisgruppe $G_\mathfrak{p} \simeq \mathbb{Z}/2$ in die Gruppe $H_3(G) \simeq (\mathbb{Z}/2)^3$ abgebildet wird. Es seien U_1, U_2 und U_3 die drei Untergruppen der Ordnung zwei von $G \simeq U_1 \times U_2$. Nach der Künneth-Formel ist

$$H_3(U_1 \times U_2) \simeq H_3(U_1) \otimes H_0(U_2) \ \oplus \ H_0(U_1) \otimes H_3(U_2) \ \oplus \ \mathrm{Tor}(H_1(U_1), H_1(U_2)).$$

Nach [B, S. 120] wird $H_3(U_1)$ auf den Summanden $H_3(U_1) \otimes H_0(U_2) \simeq \mathbb{Z}/2$ abgebildet, $H_3(U_2)$ auf den Summanden $H_0(U_1) \otimes H_3(U_2) \simeq \mathbb{Z}/2$ (oder man verwende die Natürlichkeit der Künneth-Formel, angewandt auf die kanonischen Inklusionen $U_1 \times 0 \hookrightarrow U_1 \times U_2$ und $0 \times U_2 \hookrightarrow U_1 \times U_2$). Wir werden in Kapitel 4 zeigen, dass jede der drei Untergruppen U_1, U_2 und U_3 als lokale Galoisgruppe vorkommt. Das Bild der Abbildung $\oplus_\mathfrak{p} H_3(G_\mathfrak{p}) \to H_3(G)$ enthält daher die Untergruppe

$$H_3(U_1) \otimes H_0(U_2) \quad \oplus \quad H_0(U_1) \otimes H_3(U_2),$$

isomorph zu $(\mathbb{Z}/2)^2$, von $H_3(G) \simeq (\mathbb{Z}/2)^3$, und der Cokern dieser Abbildung ist daher entweder trivial oder isomorph zu $\mathbb{Z}/2$. Es stellt sich die Frage, wie $H_3(U_3)$ nach $H_3(G)$ abgebildet wird, oder genauer, ob das Bild von $H_3(U_3)$ nicht-trivial auf den Summmanden $\mathrm{Tor}(H_1(U_1), H_1(U_2))$ von $H_3(G)$ projeziert. Diese Frage werden wir später auf zwei verschiedene Arten direkt beantworten.

Es sei noch angemerkt, dass man das Ergebnis

$H_2(\mathbb{Z}/2) = 0, \quad H_2((\mathbb{Z}/2)^2) \simeq \mathbb{Z}/2,$

$H_3(\mathbb{Z}/2) \simeq \mathbb{Z}/2, \quad H_3((\mathbb{Z}/2)^2) \simeq (\mathbb{Z}/2)^3$

auch in der Form

$H^2(\mathbb{Z}/2, \mathbb{Q}/\mathbb{Z}) = 0, \quad H^2((\mathbb{Z}/2)^2, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/2,$

$H^3(\mathbb{Z}/2, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}/2, \quad H^3((\mathbb{Z}/2)^2, \mathbb{Q}/\mathbb{Z}) \simeq (\mathbb{Z}/2)^3$

schreiben kann. Dies werden wir in Abschnitt 3.iv gebrauchen. Zur Begründung sei erwähnt, dass für endliche Gruppen G und alle $p \in \mathbb{Z}$ aufgrund des in Abschnitt 3.iv formulierten Dualitätstheorems 3.3 (s. [AW],[B, S. 144ff]) Isomorphien

$$H^p(G, \mathbb{Z}) \simeq H^{-p}(G, \mathbb{Z})$$

bestehen, dass weiter für alle $p \geq 2$ per Definition die Gleichung

$$H^{-p}(G, \mathbb{Z}) = H_{p-1}(G)$$

gilt (s. [B, S. 128]) und dass aufgrund der exakten Sequenz

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

von G-Moduln wegen $H^p(G, \mathbb{Q}) = 0$ für alle $p \in \mathbb{Z}$ die Gleichungen

$$H^p(G, \mathbb{Z}) = H^{p-1}(G, \mathbb{Q}/\mathbb{Z})$$

folgen, $p \in \mathbb{Z}$.

3.iii Der zahlentheoretische Beweis

Nach den Betrachtungen des letzten Abschnittes wissen wir, dass im singulären Fall $n = 0$ entweder stets $H^{-1}(G, K^\times) = 1$ oder stets $H^{-1}(G, K^\times) \simeq \mathbb{Z}/2$ ist (unabhängig von der Erweiterung K/k). Es genügt daher, die Gruppe $H^{-1}(G, K^\times)$ im singulären Fall für eine spezielle Erweiterung zu kennen, um die Frage allgemein zu beantworten. Hier helfen uns nun die Ergebnisse von Kapitel 2, denn nach Satz 2.18 wissen wir, dass die Gruppe $H^{-1}(G, K^\times)$ der Erweiterung $K/\mathbb{Q}$ für $K = \mathbb{Q}(\sqrt{2}, \sqrt{17})$ und $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ trivial ist. Hier liegt jeweils der singuläre Fall vor, genauso wie für $K = \mathbb{Q}(\sqrt{5}, \sqrt{41})$, $K = \mathbb{Q}(\sqrt{13}, \sqrt{29})$ (s. die Tabellen in Kapitel 2). Wir können also schließen, dass die Gruppe $H^{-1}(G, K^\times)$ im singulären Fall stets trivial ist.

3.iv Ein Beweis per Funktorialität

In diesem Abschnitt soll der folgende Satz unter Verwendung allgemeiner kohomologischer Methoden bewiesen werden.

3.2 Satz. *Sei $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ und seien G_1, G_2, G_3 die drei Untergruppen der Ordnung 2 von G. Dann ist die Abbildung*

$$g : \coprod_{i=1}^{3} H^{-4}(G_i, \mathbb{Z}) \longrightarrow H^{-4}(G, \mathbb{Z}),$$

die für $\sum_i z_i \in \coprod_{i=1}^3 H^{-4}(G_i, \mathbb{Z})$ durch

$$g\left(\sum_i z_i\right) = \sum_i \mathrm{cor}_G^{G_i} z_i$$

gegeben ist, ein Isomorphismus.

Zu Satz 3.2 sei als erstes angemerkt, dass alle darin vorkommenden Kohomologiegruppen endliche Gruppen sind. Desweiteren sind sie, wie wir bereits gesehen haben, alle der Berechnung zugänglich: nach dem in Abschnitt 3.ii Gezeigten gilt

$$H^{-4}(G_i, \mathbb{Z}) = H_3(G_i, \mathbb{Z}) \simeq \mathbb{Z}/2$$
$$H^{-4}(G, \mathbb{Z}) = H_3(G, \mathbb{Z}) \simeq (\mathbb{Z}/2)^3$$

und demzufolge hat man

$$\coprod_{i=1}^{3} H^{-4}(G_i, \mathbb{Z}) \simeq H^{-4}(G, \mathbb{Z}) \simeq (\mathbb{Z}/2)^3.$$

Aus diesem Grund genügt es, die Surjektivität von g zu zeigen, d. h.

$$\mathrm{coker}\left(\coprod_{i=1}^{3} H^{-4}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cor}} H^{-4}(G, \mathbb{Z})\right) = 0. \tag{1}$$

Diese Aussage kann mithilfe eines fundamentalen Dualitätssatzes der Kohomologie von endlichen Gruppen wie folgt umgewandelt werden. Der Dualitätssatz lautet (s. [AW],[B, S. 144ff])

3.3 Theorem. *Sei A eine endliche Gruppe der Ordnung n. Dann ist für jedes $p \in \mathbb{Z}$ das cup-Produkt*

$$H^p(A, \mathbb{Z}) \times H^{-p}(A, \mathbb{Z}) \longrightarrow H^0(A, \mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$$

eine nicht-ausgeartete Paarung.

Insbesondere gilt nach diesem Satz, dass für alle $p \in \mathbb{Z}$ die Gruppen $H^p(A, \mathbb{Z})$ und $H^{-p}(A, \mathbb{Z})$ zueinander dual sind, wenn A eine endliche Gruppe ist. Darüber hinaus gilt für jede Untergruppe $A' \subset A$, dass die Restriktion

$$\mathrm{res}_{A'}^{A} : H^p(A, \mathbb{Z}) \longrightarrow H^p(A', \mathbb{Z})$$

dual ist zur Corestriktion

$$\mathrm{cor}_{A}^{A'} : H^{-p}(A', \mathbb{Z}) \longrightarrow H^{-p}(A, \mathbb{Z}).$$

Bezeichnet man die Inklusion $A' \hookrightarrow A$ mit ι, so heißt das für $p \geq 2$ anders gesagt, dass die funktorielle Abbildung

$$\iota^* : H^p(A, \mathbb{Z}) \longrightarrow H^p(A', \mathbb{Z})$$

der Kohomologiegruppen zur funktoriellen Abbildung

$$\iota_* : H_{p-1}(A', \mathbb{Z}) \longrightarrow H_{p-1}(A, \mathbb{Z})$$

der dualen Homologiegruppen dual ist. Weiter ist bekannt, dass die zu einer direkten Summe duale Gruppe das direkte Produkt der dualen Gruppen ist:

$$\left(\coprod_i A_i\right)^\wedge = \prod_i A_i^\wedge.$$

Die Aussage (1) ist aus Dualitätsgründen also gleichbedeutend mit der Aussage

$$\ker\left(H^4(G, \mathbb{Z}) \xrightarrow{\text{res}} \prod_{i=1}^{3} H^4(G_i, \mathbb{Z})\right) = 0, \tag{2}$$

vgl. [T, S. 198], wie durch Anwendung des folgenden Lemmas zu erkennen ist.

3.4 Lemma. *Es seien A und B endliche abelsche Gruppen und $\varphi : A \to B$ ein Gruppenhomomorphismus. Für den zu φ dualen Homomorphismus $\hat{\varphi} : B^\wedge \to A^\wedge$ gilt dann*

$$\ker(\hat{\varphi}) \simeq \operatorname{coker}(\varphi)^\wedge \simeq \operatorname{coker}(\varphi),$$

wobei die zweite Isomorphie nicht kanonisch ist.

Beweis: Nach Definition sind die dualen Gruppen durch

$$A^\wedge = \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}), \quad B^\wedge = \operatorname{Hom}(B, \mathbb{Q}/\mathbb{Z})$$

gegeben und die auf $B^\wedge$ definierte duale Abbildung $\hat{\varphi}$ durch

$$\hat{\varphi}(\chi)(a) = \chi(\varphi(a)), \quad a \in A$$

für $\chi \in B^\wedge$. Für den Kern von $\hat{\varphi}$ gilt damit

$$\begin{aligned}
&\ker(\hat{\varphi}) = \{\chi \in B^\wedge | \chi \circ \varphi = 0\} = \{\chi \in \operatorname{Hom}(B, \mathbb{Q}/\mathbb{Z}) | \chi_{|\operatorname{im}\varphi} = 0\}, \\
&\ker(\hat{\varphi}) \simeq \operatorname{Hom}(B/\operatorname{im}\varphi, \mathbb{Q}/\mathbb{Z}) = \operatorname{coker}(\varphi)^\wedge,
\end{aligned}$$

womit die erste Isomorphie gezeigt ist. Für jede endliche abelsche Gruppe besteht eine nicht kanonische Isomorphie zur dualen Gruppe; dies liefert angewandt auf $\operatorname{coker}(\varphi)$ die zweite Aussage des Lemmas. □

Im folgenden geht es darum, die Aussage (2) zu beweisen. Dazu soll diese noch einmal anders formuliert werden, indem wir zu Koeffizienten in $\mathbb{Q}/\mathbb{Z}$ übergehen. Zunächst stellen wir fest

3.5 Lemma. *Für alle $p \in \mathbb{Z}$ bestehen kommutative Diagramme*

$$\begin{array}{ccc}
H^{p-1}(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\text{res}} & \prod_{i=1}^3 H^{p-1}(G_i, \mathbb{Q}/\mathbb{Z}) \\
\downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\
H^p(G, \mathbb{Z}) & \xrightarrow{\text{res}} & \prod_{i=1}^3 H^p(G_i, \mathbb{Z})
\end{array}$$

mit natürlichen Isomorphismen δ.

Beweis: Für $A = G$ und $A = G_1, G_2, G_3$ gehen wir von der kurzen exakten Sequenz

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

von A-Moduln aus, wobei $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ jeweils mit der trivialen A-Modulstruktur versehen seien. Ein Stück der zugehörigen langen exakten Kohomologiesequenz lautet

$$H^{p-1}(A,\mathbb{Q}) \to H^{p-1}(A,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^p(A,\mathbb{Z}) \to H^p(A,\mathbb{Q})$$

mit der $(p-1)$-ten Randabbildung $\delta = \delta^{p-1}$. Wir wollen uns kurz überlegen, dass hierbei

$$H^{p-1}(A,\mathbb{Q}) = H^p(A,\mathbb{Q}) = 0$$

gilt, weil die Ordnung n von A in $\mathbb{Q}$ invertierbar ist. Die Multiplikation mit n stellt einen Isomorphismus der abelschen Gruppe $\mathbb{Q}$ dar, dessen Umkehrabbildung durch die Multiplikation mit $1/n$ gegeben ist. Anwendung der Funktoren $H^{p-1}(A,\cdot)$ und $H^p(A,\cdot)$ auf $n = n\cdot \mathrm{id}$ liefert daher Isomorphismen von $H^{p-1}(A,\mathbb{Q})$ bzw. $H^p(A,\mathbb{Q})$, wobei es sich wegen der Additivität von H in der zweiten Komponente wiederum um $n = n\cdot \mathrm{id}$, die Multiplikation mit n, handelt. Andererseits werden jedoch beide Gruppen durch n annulliert:

$$n \cdot H^{p-1}(A,\mathbb{Q}) = 0, \quad n \cdot H^p(A,\mathbb{Q}) = 0,$$

vgl. [B,S. 84], so dass $H^{p-1}(A,\mathbb{Q})$ und $H^p(A,\mathbb{Q})$ wie behauptet verschwinden. Es bezeichne ι_i die Inklusion $G_i \hookrightarrow G$. Aufgrund der Natürlichkeit aller vorkommenden Abbildungen erhalten wir für $i = 1,2,3$ kommutative Diagramme

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{p-1}(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & H^p(G,\mathbb{Z}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota_i^*} & & \downarrow{\scriptstyle \iota_i^*} & & \\ 0 & \longrightarrow & H^{p-1}(G_i,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & H^p(G_i,\mathbb{Z}) & \longrightarrow & 0 \end{array}$$

und weil es sich bei den funktoriellen Abbildungen ι_i^* gerade um die Restriktionen $\mathrm{res}^G_{G_i}$ handelt, vgl. [B, S. 80], folgt insgesamt die Behauptung. □

Nach Lemma 3.5 ist die Aussage (2) zu

$$\ker\left(H^3(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{res}} \prod_{i=1}^{3} H^3(G_i,\mathbb{Q}/\mathbb{Z}) \right) = 0 \tag{3}$$

äquivalent. Die Idee ist nun, zunächst Koeffizienten in $\mathbb{F}_2$ zu betrachten und den Kern der Abbildung

$$H^3(G,\mathbb{F}_2) \xrightarrow{\mathrm{res}} \prod_{i=1}^{3} H^3(G_i,\mathbb{F}_2)$$

zu bestimmen, um dann anschließend einen Vergleich mit der zu untersuchenden Abbildung anzustellen. Den Zusammenhang liefert das folgende

3.6 Lemma. *Für $A = \mathbb{Z}/2$ und $A = \mathbb{Z}/2 \times \mathbb{Z}/2$ bestehen natürliche kurze exakte Sequenzen*

$$0 \to H^2(A,\mathbb{Q}/\mathbb{Z}) \to H^3(A,\mathbb{F}_2) \to H^3(A,\mathbb{Q}/\mathbb{Z}) \to 0.$$

Beweis: Man betrachte die kurze exakte Sequenz

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{2} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Versieht man $\mathbb{F}_2$ und $\mathbb{Q}/\mathbb{Z}$ jeweils mit der trivialen A-Modulstruktur, so handelt es sich um eine kurze exakte Sequenz von A-Moduln. Diese vermittelt eine lange exakte Kohomologiesequenz (s. [AW] oder [B]); insbesondere erhält man die Teilsequenz

$$H^2(A,\mathbb{Q}/\mathbb{Z}) \xrightarrow{2} H^2(A,\mathbb{Q}/\mathbb{Z}) \to H^3(A,\mathbb{F}_2) \to H^3(A,\mathbb{Q}/\mathbb{Z}) \xrightarrow{2} H^3(A,\mathbb{Q}/\mathbb{Z}).$$

Hierzu sei angemerkt, dass der Funktor H in der zweiten Komponente additiv ist, weshalb die Abbildung $2 = \mathrm{id} + \mathrm{id}$ von $\mathbb{Q}/\mathbb{Z}$ für alle $p \in \mathbb{Z}$ unter $H^p(A, \cdot)$ auf die Abbildung $2 = \mathrm{id} + \mathrm{id}$ von $H^p(A, \mathbb{Q}/\mathbb{Z})$ abgebildet wird. Nach dem in Abschnitt 3.ii Gezeigten gilt für die erste Gruppe der Sequenz

$$H^2(A, \mathbb{Q}/\mathbb{Z}) \simeq \begin{cases} 0 & \text{für } A = \mathbb{Z}/2 \\ \mathbb{Z}/2 & \text{für } A = \mathbb{Z}/2 \times \mathbb{Z}/2 \end{cases}$$

und damit hat sie den Exponenten 2, so dass die Abbildung $2 = \mathrm{id} + \mathrm{id}$ die Nullabbildung von $H^2(A, \mathbb{Q}/\mathbb{Z})$ ist. Man erhält also die exakte Sequenz

$$0 \to H^2(A, \mathbb{Q}/\mathbb{Z}) \to H^3(A, \mathbb{F}_2) \to H^3(A, \mathbb{Q}/\mathbb{Z})_2 \to 0$$

mit

$$H^3(A, \mathbb{Q}/\mathbb{Z})_2 = \{\alpha \in H^3(A, \mathbb{Q}/\mathbb{Z}) | 2\alpha = 0\}.$$

Nach dem in Abschnitt 3.ii Gezeigten gilt

$$H^3(A, \mathbb{Q}/\mathbb{Z}) \simeq \begin{cases} \mathbb{Z}/2 & \text{für } A = \mathbb{Z}/2 \\ (\mathbb{Z}/2)^3 & \text{für } A = \mathbb{Z}/2 \times \mathbb{Z}/2 \end{cases}$$

und daher hat auch $H^3(A, \mathbb{Q}/\mathbb{Z})$ den Exponenten 2, woraus nun schließlich die Gleichheit $H^3(A, \mathbb{Q}/\mathbb{Z})_2 = H^3(A, \mathbb{Q}/\mathbb{Z})$ folgt. □

Das Lemma 3.6 stellt wie gesagt die Verbindung zu Koeffizienten in $\mathbb{F}_2$ her. Bevor wir mit dem Beweis von Satz 3.2 beginnen, formulieren wir

3.7 Satz. *Sei $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ und seien G_1, G_2, G_3 die drei Untergruppen der Ordnung 2 von G. Dann gilt*

$$\ker\left(H^3(G, \mathbb{F}_2) \xrightarrow{\text{res}} \prod_{i=1}^{3} H^3(G_i, \mathbb{F}_2) \right) \simeq \mathbb{Z}/2.$$

Den Beweis verschieben wir auf später. Mit dem soeben vorgeführten Satz 3.7 liegt alles bereit und wir widmen uns nunmehr dem

Beweis von Satz 3.2: Im folgenden geht es um Kohomologiegruppen von $U = \mathbb{Z}/2$ und $G = U \times U$ mit verschiedenen Koeffizienten. Es bezeichne ι_i die Inklusion $U = G_i \hookrightarrow G$ $(i = 1, 2, 3)$. Für die trivialen G-Moduln $M = \mathbb{F}_2$ und $M = \mathbb{Q}/\mathbb{Z}$ betrachte man die funktorielle Abbildung

$$H^3(G, M) \xrightarrow{\iota^* = (\iota_1^*, \iota_2^*, \iota_3^*)} H^3(U, M)^3$$

und für $M = \mathbb{Q}/\mathbb{Z}$ auch noch die Abbildung

$$H^2(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\iota^* = (\iota_1^*, \iota_2^*, \iota_3^*)} H^2(U, \mathbb{Q}/\mathbb{Z})^3.$$

Es handelt sich bei ι_i^* um die Restriktion

$$\mathrm{res}^G_{G_i} : H^p(G, M) \to H^p(G_i, M),$$

vgl. hierzu [AW, S. 99] oder [B, S. 80]. Desweiteren betrachte man für $A = G$ und $A = G_1, G_2, G_3$ die natürliche exakte Sequenz

$$0 \to H^2(A, \mathbb{Q}/\mathbb{Z}) \to H^3(A, \mathbb{F}_2) \to H^3(A, \mathbb{Q}/\mathbb{Z}) \to 0,$$

die nach Lemma 3.6 vorliegt. Per Funktorialität erhält man so die kommutativen Diagramme

$$\begin{array}{ccccc} H^2(G,\mathbb{Q}/\mathbb{Z}) & \hookrightarrow & H^3(G,\mathbb{F}_2) & \twoheadrightarrow & H^3(G,\mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \iota_i^*} & & \downarrow{\scriptstyle \iota_i^*} & & \downarrow{\scriptstyle \iota_i^*} \\ H^2(G_i,\mathbb{Q}/\mathbb{Z}) & \hookrightarrow & H^3(G_i,\mathbb{F}_2) & \twoheadrightarrow & H^3(G_i,\mathbb{Q}/\mathbb{Z}) \end{array}$$

und als deren Zusammensetzung schließlich mit

$$\begin{array}{ccccc} H^2(G,\mathbb{Q}/\mathbb{Z}) & \hookrightarrow & H^3(G,\mathbb{F}_2) & \twoheadrightarrow & H^3(G,\mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \iota^*} & & \downarrow{\scriptstyle \iota^*} & & \downarrow{\scriptstyle \iota^*} \\ H^2(U,\mathbb{Q}/\mathbb{Z})^3 & \hookrightarrow & H^3(U,\mathbb{F}_2)^3 & \twoheadrightarrow & H^3(U,\mathbb{Q}/\mathbb{Z})^3 \end{array}$$

ein einziges Diagramm. Nach dem in Abschnitt 3.ii Gezeigten gilt hierbei

$$H^2(U,\mathbb{Q}/\mathbb{Z}) = H^3(\mathbb{Z}/2,\mathbb{Z}) = H_2(\mathbb{Z}/2,\mathbb{Z}) = 0.$$

Wir betrachten jetzt die Kerne der vertikalen Abbildungen, die in dem erweiterten kommutativen Diagramm

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & H^2(G,\mathbb{Q}/\mathbb{Z}) & \to & \operatorname{Kern}\iota^* & \to & \operatorname{Kern}\iota^* & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & H^2(G,\mathbb{Q}/\mathbb{Z}) & \to & H^3(G,\mathbb{F}_2) & \to & H^3(G,\mathbb{Q}/\mathbb{Z}) & \to & 0 \\ & & \downarrow{\scriptstyle \iota^*=0} & & \downarrow{\scriptstyle \iota^*} & & \downarrow{\scriptstyle \iota^*} & & \\ 0 & \to & H^2(U,\mathbb{Q}/\mathbb{Z})^3 = 0 & \to & H^3(U,\mathbb{F}_2)^3 & \to & H^3(U,\mathbb{Q}/\mathbb{Z})^3 & \to & 0 \end{array}$$

ihren Platz finden. Nach Lemma 3.6 sind die unteren beiden Zeilen exakt. Per Diagrammjagd folgt das auch für die obere Zeile, vgl. das folgende Lemma 3.8. In dieser ersten Zeile ist nach dem in Abschnitt 3.ii Gezeigten nun

$$H^2(G,\mathbb{Q}/\mathbb{Z}) = H^3(G,\mathbb{Z}) = H_2(G,\mathbb{Z}) \simeq \mathbb{Z}/2$$

und wie in Satz 3.7 festgestellt gilt für den mittleren Kern

$$\ker\left(H^3(G,\mathbb{F}_2) \xrightarrow{\iota^*} \prod_{i=1}^{3} H^3(G_i,\mathbb{F}_2)\right) \simeq \mathbb{Z}/2.$$

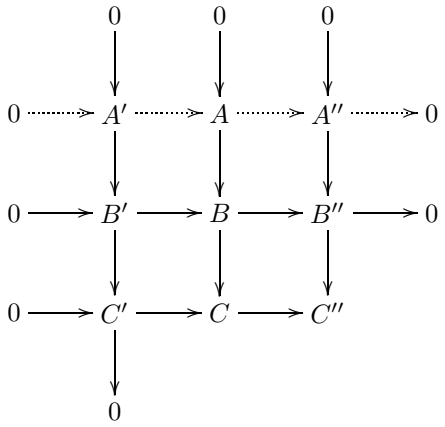
Also ist der dritte Kern gleich 0, oder anders gesagt folgt

$$\ker\left(H^3(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\text{res}} \prod_{i=1}^{3} H^3(G_i,\mathbb{Q}/\mathbb{Z})\right) = 0,$$

denn bekanntlich ist $\text{res} = \prod_i \text{res}^G_{G_i}$ hier gleich der funktoriellen Abbildung ι^*. □

Der Vollständigkeit halber sei jetzt noch die Diagrammjagd nachgetragen.

3.8 Lemma. *In einem kommutativen Diagramm*



von Gruppen und Gruppenhomomorphismen, in dem die Zeilen und Spalten mit durchgezogenen Pfeilen exakt sind, ist auch die Sequenz in der ersten Zeile exakt.

Beweis: Zu zeigen ist:

a) die Abbildung $A' \longrightarrow A$ ist injektiv;
b) $\mathrm{im}(A' \longrightarrow A) = \ker(A \longrightarrow A'')$;
c) die Abbildung $A \longrightarrow A''$ ist surjektiv.

Zu a): Das Element x von A' werde unter $A' \longrightarrow A$ auf 0 abgebildet. Dann wird es unter $A' \longrightarrow A \longrightarrow B$ auf 0 abgebildet und wegen der Kommutativität des Diagramms auch unter $A' \longrightarrow B' \longrightarrow B$. Weil $B' \longrightarrow B$ injektiv ist, ist bereits das Bild von x unter $A' \longrightarrow B'$ gleich 0, und weil $A' \longrightarrow B'$ ebenfalls injektiv ist, folgt $x = 0$.

Zu b): Die Verknüpfung $B' \longrightarrow B \longrightarrow B''$ ist aufgrund der Exaktheit der Sequenz die Nullabbildung. Also ist $A' \longrightarrow B' \longrightarrow B \longrightarrow B''$ die Nullabbildung und wegen der Kommutativität des Diagramms auch $A' \longrightarrow A \longrightarrow A'' \longrightarrow B''$. Dabei ist $A'' \longrightarrow B''$ injektiv, so dass bereits $A' \longrightarrow A \longrightarrow A''$ die Nullabbildung ist. Es folgt $\mathrm{im}(A' \longrightarrow A) \subset \ker(A \longrightarrow A'')$.

Sei nun $x \in \ker(A \longrightarrow A'')$. Dann wird x unter $A \longrightarrow A'' \longrightarrow B'' = A \longrightarrow B \longrightarrow B''$ auf 0 abgebildet, d. h. das Bild y von x unter $A \longrightarrow B$ liegt im Kern von $B \longrightarrow B''$. Aufgrund der Exaktheit der Sequenz $B' \longrightarrow B \longrightarrow B''$ ist y das Bild eines $z \in B'$. Weil auch die Sequenz $A \longrightarrow B \longrightarrow C$ exakt ist, wird y als Bild von x unter $A \longrightarrow B$ durch $B \longrightarrow C$ ebenfalls auf 0 abgebildet. Damit liegt z im Kern von $B' \longrightarrow B \longrightarrow C = B' \longrightarrow C' \longrightarrow C$, doch der Kern von $B' \longrightarrow C' \longrightarrow C$ ist wegen der Injektivität von $C' \longrightarrow C$ gleich dem von $B' \longrightarrow C'$. Die Exaktheit der Sequenz $A' \longrightarrow B' \longrightarrow C'$ liefert schließlich, dass z das Bild eines $t \in A'$ ist. Dieses $t \in A'$ wird unter $A' \longrightarrow A$ auf x abgebildet, denn das Bild von t unter $A' \longrightarrow A \longrightarrow B = A' \longrightarrow B' \longrightarrow B$ ist gleich dem Bild z von x unter $A \longrightarrow B$ und $A \longrightarrow B$ ist injektiv.

Zu c): Sei $x \in A''$. Weil die Sequenz $A'' \longrightarrow B'' \longrightarrow C''$ exakt ist, wird das Bild y von x unter $A'' \longrightarrow B''$ durch $B'' \longrightarrow C''$ auf 0 abgebildet. Wegen der Surjektivität der Abbildung besitzt y bzgl. $B \longrightarrow B''$ ein Urbild $z \in B$, das unter $B \longrightarrow B'' \longrightarrow C'' = B \longrightarrow C \longrightarrow C''$ auf 0 abgebildet wird. Das Bild s von z unter $B \longrightarrow C$ liegt also im Kern von $C \longrightarrow C''$, der aufgrund der Exaktheit von $C' \longrightarrow C \longrightarrow C''$ mit dem Bild von $C' \longrightarrow C$ übereinstimmt. Sei s das Bild von

$t \in C'$. Wegen der Surjektivität von $B' \longrightarrow C'$ ist t das Bild eines $u \in B'$, welches unter $B' \longrightarrow C' \longrightarrow C = B' \longrightarrow B \longrightarrow C$ auf s abgebildet wird. Da das Bild v von u unter $B' \longrightarrow B$ und z durch $B \longrightarrow C$ jeweils auf s abgebildet werden, liegt $z - v$ im Kern von $B \longrightarrow C$. Doch die Sequenz $A \longrightarrow B \longrightarrow C$ ist exakt, weshalb $z - v$ im Bild von $A \longrightarrow B$ liegt. Sei $z - v$ das Bild von $w \in A$. Dann ist das Bild von w unter $A \longrightarrow A'' \longrightarrow B'' = A \longrightarrow B \longrightarrow B''$, also das Bild von $z - v$ unter $B \longrightarrow B''$, gleich $y - 0 = y$. Doch auch x wird unter $A'' \longrightarrow B''$ auf y abgebildet, so dass x aufgrund der Injektivität von $A'' \longrightarrow B''$ mit dem Bild von w unter $A \longrightarrow A''$ übereinstimmt. □

Der Beweis von Satz 3.2 erfolgte durch Übergang zu Koeffizienten in $\mathbb{F}_2$. Hier ist alles übersichtlicher, wie das nachstehende Resultat auf eindrucksvolle Weise belegt (vgl. [AM, S. 69]).

3.9 Theorem. *Für alle $n \geq 0$ ist der Kohomologiering*

$$H^*((\mathbb{Z}/2)^n, \mathbb{F}_2) = \mathbb{F}_2[x_1, \cdots, x_n]$$

eine Polynomalgebra in n eindimensionalen Erzeugern.

Das Theorem hat mit der Künneth-Formel zu tun, die bei Koeffizienten in einem Körper eine einfachere Gestalt annimmt, weil die Torsionsanteile verschwinden. Das wollen wir uns jetzt für $n = 2$ genauer ansehen, und zwar mit

3.10 Satz. *Seien π_1 und π_2 die beiden Projektionen $\mathbb{Z}/2 \times \mathbb{Z}/2 \to \mathbb{Z}/2$, nämlich $(\sigma_1, \sigma_2) \mapsto \sigma_1$ und $(\sigma_1, \sigma_2) \mapsto \sigma_2$. Dann wird durch die Künneth-Formel für die Kohomologiegruppen $H^n(\mathbb{Z}/2 \times \mathbb{Z}/2, \mathbb{F}_2)$ $(n \geq 0)$ ein $\mathbb{F}_2$-Algebrenisomorphismus*

$$\begin{array}{ccc} H^*(\mathbb{Z}/2, \mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(\mathbb{Z}/2, \mathbb{F}_2) & \longrightarrow & H^*(\mathbb{Z}/2 \times \mathbb{Z}/2, \mathbb{F}_2) \\ \| & & \\ \mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] & & \end{array}$$

vermittelt, der für die Erzeuger $f \otimes g$ von $H^*(\mathbb{Z}/2, \mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(\mathbb{Z}/2, \mathbb{F}_2)$ durch

$$f \otimes g \longmapsto \pi_1^*(f) \cdot \pi_2^*(g) = \pi_1^*(f) \cup \pi_2^*(g)$$

gegeben ist, wobei $\cup$ das cup-Produkt bezeichnet.

Beweis: Sind G eine Gruppe und k ein mit der trivialen G-Operation versehener kommutativer Ring, so ist der Kohomologiering

$$H^*(G, k) = \bigoplus_{p \geq 0} H^p(G, k)$$

mit Multiplikation durch das cup-Produkt $\cup$ sowie

$$1 \in H^0(G, k) = k$$

eine graduierte anti-kommutative k-Algebra, vgl. [B, S. 112]. Dabei bedeutet anti-kommutativ, dass für $u \in H^p(G, k)$, $v \in H^q(G, k)$ die Gleichung

$$u \cup v = (-1)^{pq} v \cup u$$

in $H^{p+q}(G, k)$ erfüllt ist. Sei jetzt $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ und $U = \mathbb{Z}/2$. In unserem Fall liegt der Ring $k = \mathbb{F}_2$ vor und nach Theorem 3.9 wissen wir, dass

$$H^*(U, \mathbb{F}_2) = \mathbb{F}_2[x]$$

Polynomalgebra in x ist mit einem $x \in H^1(U, \mathbb{F}_2)$; für jedes $p \geq 0$ besteht also die Gleichung

$$H^p(U, \mathbb{F}_2) = \mathbb{F}_2 x^p.$$

Hierbei ist x das nicht-triviale Element von

$$H^1(U, \mathbb{F}_2) = \mathrm{Hom}(U, \mathbb{F}_2),$$

vgl. [AW, S. 97] oder [Ws, S. 29]. Wir betrachten nun die beiden Projektionen $\pi_i : G \to U$ $(i = 1, 2)$. Sie vermitteln die funktoriellen Abbildungen

$$\pi_i^* : H^*(U, \mathbb{F}_2) \to H^*(G, \mathbb{F}_2),$$

bei denen es sich um Homomorphismen von graduierten $\mathbb{F}_2$-Algebren handelt, vgl. [B, S. 112]. Desweiteren sind die π_i^* injektiv, denn bezeichnet ι_i die zu π_i gehörige Injektion $U \to G$, so hat man

$$\iota_i^* \pi_i^* = (\pi_i \iota_i)^* = \mathrm{id}_U^* = \mathrm{id}_{H^*(U, \mathbb{F}_2)}.$$

Folglich erhalten wir, dass

$$\pi_i^*(H^*(U, \mathbb{F}_2)) = \pi_i^*(\mathbb{F}_2[x]) = \mathbb{F}_2[\pi_i^* x] = \mathbb{F}_2[x_i]$$

Polynomalgebra in x_i ist, wenn wir $x_i = \pi_i^* x$ setzen. Genauer ist x_i das durch

$$x_i((\sigma_1, \sigma_2)) = x(\pi_i(\sigma_1, \sigma_2)) = x(\sigma_i)$$

definierte Element von $H^1(G, \mathbb{F}_2)$. Es gilt

$$H^1(G, \mathbb{F}_2) = \mathrm{Hom}(G, \mathbb{F}_2) = \mathbb{F}_2 x_1 + \mathbb{F}_2 x_2,$$

vgl. nochmals [AW, S. 97] bzw. [Ws, S. 29]. Schließlich gibt das Diagramm

$$\begin{array}{ccccc} \mathbb{F}_2[x] & \xhookrightarrow{\pi_1^*} & \mathbb{F}_2[x_1] & \hookrightarrow & H^*(G, \mathbb{F}_2) \\ & & & \nearrow & \\ \mathbb{F}_2[x] & \xhookrightarrow{\pi_2^*} & \mathbb{F}_2[x_2] & & \end{array}$$

von $\mathbb{F}_2$-Algebren Anlass zu dem $\mathbb{F}_2$-Algebrenhomomorphismus

$$\begin{array}{ccc} & & \mathbb{F}_2[x_1] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x_2] \xrightarrow{\cup} \mathbb{F}_2[x_1, x_2] \subset H^*(G, \mathbb{F}_2), \\ & \overset{\sim}{\nearrow} & \searrow^{\pi_1^* \otimes \pi_2^*} \\ \mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] & & \end{array}$$

wobei $\mathbb{F}_2[x_1, x_2]$ die von x_1 und x_2 erzeugte Teilalgebra von $H^*(G, \mathbb{F}_2)$ ist. Wir wollen im folgenden zeigen, dass dieser durch die Künneth-Formel vermittelt wird und einen Isomorphismus darstellt. Genauer gesagt heißt letzteres, dass

$$H^*(G, \mathbb{F}_2) = \mathbb{F}_2[x_1, x_2]$$

gilt und dies eine Polynomalgebra in den Erzeugern x_1 und x_2 ist. Ziehen wir also die Künneth-Formel für die Kohomologiegruppen $H^n(U \times U, \mathbb{F}_2)$ heran: nach dieser bestehen für alle $n \geq 0$ exakte Sequenzen

$$0 \longrightarrow \bigoplus_{p+q=n} H^p(U, \mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(U, \mathbb{F}_2) \xrightarrow{\times} H^n(U \times U, \mathbb{F}_2)$$
$$\longrightarrow \bigoplus_{p+q=n+1} \mathrm{Tor}_1^{\mathbb{F}_2}(H^p(U, \mathbb{F}_2), H^q(U, \mathbb{F}_2)) \longrightarrow 0$$

mit dem Kohomologie-Kreuzprodukt $\times$, vgl. [Wb,S. 166]; hierbei gilt

$$\bigoplus_{p+q=n+1} \operatorname{Tor}_1^{\mathbb{F}_2}(H^p(U,\mathbb{F}_2), H^q(U,\mathbb{F}_2)) = 0,$$

weil $\mathbb{F}_2$ ein Körper ist. Indem man die $\mathbb{F}_2$-linearen Abbildungen

$$\bigoplus_{p+q=n} H^p(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(U,\mathbb{F}_2) \xrightarrow{\times} H^n(G,\mathbb{F}_2)$$

für $n \geq 0$ addiert, erhält man einen $\mathbb{F}_2$-Algebrenhomomorphismus

$$H^*(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(U,\mathbb{F}_2) \xrightarrow{\times} H^*(G,\mathbb{F}_2),$$

vgl. [B,S. 120/121]. Dieser erweist sich nach Künneth-Formel als Isomorphismus, weil für jede der direkten Komponenten von

$$H^*(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(U,\mathbb{F}_2) = \bigoplus_{n\geq 0} \left(\bigoplus_{p+q=n} \mathbb{F}_2 x^p \otimes_{\mathbb{F}_2} \mathbb{F}_2 x^q \right)$$

mit dem Kreuzprodukt $\times$ eine exakte Sequenz

$$0 \longrightarrow \bigoplus_{p+q=n} \mathbb{F}_2 x^p \otimes_{\mathbb{F}_2} \mathbb{F}_2 x^q \xrightarrow{\times} H^n(G,\mathbb{F}_2) \longrightarrow 0$$

vorliegt. Auf der linken Seite steht hier eine direkte Summe von Teilvektorräumen der $\mathbb{F}_2$-Algebra $\mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x]$; es gilt

$$\bigoplus_{p+q=n} \mathbb{F}_2 x^p \otimes_{\mathbb{F}_2} \mathbb{F}_2 x^q = \bigoplus_{p+q=n} \mathbb{F}_2 (x\otimes 1)^p (1\otimes x)^q.$$

Unter dem Kreuzprodukt $\times$ wird diese Summe von Teilräumen von $\mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x]$ auf

$$\bigoplus_{p+q=n} \mathbb{F}_2 (x\times 1)^p (1\times x)^q = H^n(G,\mathbb{F}_2)$$

abgebildet. Wie wir zuletzt zeigen werden, folgt aus der Natürlichkeit der Künneth-Formel

$$x \times 1 = x_1, \quad 1 \times x = x_2$$

und man hat demnach für alle $n \geq 0$ exakte Sequenzen

$$0 \longrightarrow \bigoplus_{p+q=n} \mathbb{F}_2 x^p \otimes_{\mathbb{F}_2} \mathbb{F}_2 x^q \xrightarrow{\times} \bigoplus_{p+q=n} \mathbb{F}_2 x_1^p x_2^q \longrightarrow 0,$$

bei denen auf der rechten Seite der $\mathbb{F}_2$-Raum

$$\bigoplus_{p+q=n} \mathbb{F}_2 x_1^p x_2^q = H^n(G,\mathbb{F}_2)$$

als Bildbereich auftritt. Auf diese Weise haben wir den durch die Künneth-Formel vermittelten $\mathbb{F}_2$-Algebrenhomomorphismus

$$\mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] \xrightarrow{\times} H^*(G,\mathbb{F}_2)$$

genau beschrieben, da wir die Isomorphismen zwischen den direkten Komponenten explizit angegeben haben. Als letztes bleiben unter Verwendung der Natürlichkeit

der Künneth-Formel die Bilder von $x \otimes 1$ und $1 \otimes x$ zu bestimmen. Für alle $n \geq 0$ bestehen kommutative Diagramme

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bigoplus_{p+q=n} H^p(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(U,\mathbb{F}_2) & \xrightarrow{\times} & H^n(U\times U,\mathbb{F}_2) & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \bigoplus_{p+q=n} \mathrm{id}_U^* \otimes \mathrm{tr}_U^*} & & \uparrow{\scriptstyle (\mathrm{id}_U \times \mathrm{tr}_U)^*} & & \\
0 & \longrightarrow & \bigoplus_{p+q=n} H^p(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(1,\mathbb{F}_2) & \xrightarrow{\times} & H^n(U\times 1,\mathbb{F}_2) & \longrightarrow & 0 \\
 & & & \searrow & \uparrow{\scriptstyle \sim} & & \\
 & & & & H^n(U,\mathbb{F}_2) & &
\end{array}$$

mit der trivialen Abbildung $\mathrm{tr}_U : U \to 1$, oder etwas anders formuliert sind die Diagramme

$$\begin{array}{ccc}
\bigoplus_{p+q=n} H^p(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(U,\mathbb{F}_2) & \xrightarrow[\sim]{\times} & H^n(G,\mathbb{F}_2) \\
\uparrow{\scriptstyle \mathrm{id}_U^* \otimes \mathrm{tr}_U^*} & & \uparrow{\scriptstyle \pi_1^*} \\
H^n(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^0(1,\mathbb{F}_2) & \xrightarrow[\sim]{\times} & H^n(U,\mathbb{F}_2)
\end{array}$$

für alle $n \geq 0$ kommutativ. Sei $y = x^n$ das nicht-triviale Element von $H^n(U,\mathbb{F}_2)$. Dann wird das nicht-triviale Element $y \otimes 1$ von $H^n(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^0(1,\mathbb{F}_2)$ unter der vertikalen Abbildung

$$\mathrm{id}_U^* \otimes \mathrm{tr}_U^* : H^n(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^0(1,\mathbb{F}_2) \longrightarrow H^n(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^0(U,\mathbb{F}_2)$$

auf das nicht-triviale Element $y \otimes 1$ von $H^n(U,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^0(U,\mathbb{F}_2)$ abgebildet, weil

$$\mathrm{id}_U^* = \mathrm{id}_{H^n(U,\mathbb{F}_2)}, \quad \mathrm{tr}_U^* = \mathrm{id}_{\mathbb{F}_2}$$

gilt. Anwendung der horizontalen vom Kreuzprodukt vermittelten Abbildung auf $y \otimes 1$ liefert hingegen das nicht-triviale Element y von $H^n(U,\mathbb{F}_2)$. Insgesamt ergibt sich das Diagramm

$$\begin{array}{ccc}
y \otimes 1 & \xmapsto{\times} & y \times 1 = \pi_1^* y \\
{\scriptstyle \mathrm{id}_U^* \otimes \mathrm{tr}_U^*}\uparrow & & \uparrow{\scriptstyle \pi_1^*} \\
y \otimes 1 & \xmapsto{\times} & y
\end{array}$$

und es gilt also in $H^n(G,\mathbb{F}_2)$ die Gleichung

$$y \times 1 = \pi_1^* y,$$

was im Fall $n = 1$ wie behauptet

$$x \times 1 = \pi_1^* x = x_1$$

mit sich zieht. Auf analoge Weise zeigt man

$$1 \times x = \pi_2^* x = x_2,$$

indem man ganz entsprechend für die zweite Projektion argumentiert. Doch auch für den $\mathbb{F}_2$-Algebrenhomomorphismus $\pi_1^* \otimes \pi_2^*$ gilt

$$\begin{aligned}
x \otimes 1 &\longmapsto \pi_1^* x \cdot \pi_2^* 1 = \pi_1^* x \\
1 \otimes x &\longmapsto \pi_1^* 1 \cdot \pi_2^* x = \pi_2^* x
\end{aligned}$$

und weil die $\mathbb{F}_2$-Algebra

$$\mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] = \bigoplus_{n\geq 0} \Bigg(\bigoplus_{p+q=n} \mathbb{F}_2(x\otimes 1)^p (1\otimes x)^q \Bigg)$$

von $x\otimes 1$ und $1\otimes x$ erzeugt wird, folgt dass der von der Künneth-Formel vermittelte $\mathbb{F}_2$-Algebrenisomorphismus $\times$ mit $\pi_1^* \otimes \pi_2^*$ übereinstimmt. □

Wie wir gleich sehen werden, kann Satz 3.10 noch etwas anders formuliert werden. Das Tensorprodukt $H^*(\mathbb{Z}/2,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(\mathbb{Z}/2,\mathbb{F}_2)$ ist aufgrund der Isomorphieen

$$\mathbb{F}_2[x] \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] \;\simeq\; \mathbb{F}_2[X_1] \otimes_{\mathbb{F}_2} \mathbb{F}_2[X_2] \;\simeq\; \mathbb{F}_2[X_1, X_2]$$

eine Polynomalgebra in zwei unabhängigen Variablen X_1 und X_2. Auf ihm ist der $\mathbb{F}_2$-Algebrenhomomorphismus

$$\pi_1^* \otimes \pi_2^* : H^*(\mathbb{Z}/2,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(\mathbb{Z}/2,\mathbb{F}_2) \longrightarrow H^*(\mathbb{Z}/2\times\mathbb{Z}/2,\mathbb{F}_2)$$

definiert, der nach Satz 3.10 von der Künneth-Formel kommt und ein Isomorphismus ist. Auf den direkten Komponenten $H^p(\mathbb{Z}/2,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(\mathbb{Z}/2,\mathbb{F}_2)$ ist $\pi_1^* \otimes \pi_2^*$ also durch das Kreuzprodukt

$$\times : H^p(\mathbb{Z}/2,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^q(\mathbb{Z}/2,\mathbb{F}_2) \longrightarrow H^{p+q}(\mathbb{Z}/2\times\mathbb{Z}/2,\mathbb{F}_2)$$

gegeben. Das Kreuzprodukt wird bilinear auf ganz $H^*(\mathbb{Z}/2,\mathbb{F}_2)$ fortgesetzt, indem die Homomorphismen $\times$ auf den direkten Komponenten addiert werden. Für alle $f, g \in H^*(\mathbb{Z}/2,\mathbb{F}_2)$ gilt damit

$$\pi_1^* f \cup \pi_2^* g = f \times g$$

(Zusammenhang zwischen cup-Produkt und Kreuzprodukt der Künneth-Formel). Die zweite Aussage von Satz 3.10 lautet folgendermaßen. Der durch die Vorgaben

$$\begin{aligned} x\otimes 1 &\longmapsto X_1 \longmapsto \pi_1^* x \\ 1\otimes x &\longmapsto X_2 \longmapsto \pi_2^* x \end{aligned}$$

definierte Einsetzungshomomorphismus

$$H^*(\mathbb{Z}/2,\mathbb{F}_2) \otimes_{\mathbb{F}_2} H^*(\mathbb{Z}/2,\mathbb{F}_2) \xrightarrow{\sim} \mathbb{F}_2[X_1, X_2] \longrightarrow H^*(\mathbb{Z}/2\times\mathbb{Z}/2,\mathbb{F}_2)$$

ist ein Isomorphismus, oder anders formuliert weiß man über den Kohomologiering $H^*(\mathbb{Z}/2\times\mathbb{Z}/2,\mathbb{F}_2)$, dass

$$H^*(\mathbb{Z}/2\times\mathbb{Z}/2,\mathbb{F}_2) = \mathbb{F}_2[\pi_1^* x, \pi_2^* x]$$

eine Polynomalgebra in den eindimensionalen Erzeugern $\pi_1^* x$ und $\pi_2^* x$ ist.

Im folgenden sei stets $G = U \times U$ mit $U = \mathbb{Z}/2$; weiter seien G_1, G_2, G_3 der Reihe nach die drei von $(1,0)$, $(0,1)$ und $(1,1)$ erzeugten zweielementigen Untergruppen von G. Es seien

$$\iota_1 : G_1 \hookrightarrow G, \quad \iota_2 : G_2 \hookrightarrow G, \quad \iota_3 : G_3 \hookrightarrow G$$

die drei Inklusionen $U \to G$ und

$$\pi_1 : G = G_1 \times G_2 \to G_1, \quad \pi_2 : G = G_1 \times G_2 \to G_2$$

die beiden Projektionen $G = U \times U \to U$. Damit ist alles bereit und wir formulieren

3.11 Lemma. *Seien x das nicht-triviale Element von $H^1(U,\mathbb{F}_2)$ und x_1, x_2 die Bilder von x in $H^1(G,\mathbb{F}_2)$ unter den funktoriellen Abbildungen*

$$\pi_1^*, \pi_2^* : H^*(U,\mathbb{F}_2) \to H^*(G,\mathbb{F}_2).$$

Dann sind die zu den Inklusionen $\iota_1, \iota_2, \iota_3$ gehörigen funktoriellen Abbildungen

$$\iota_1^*, \iota_2^*, \iota_3^* : H^*(G,\mathbb{F}_2) \to H^*(U,\mathbb{F}_2)$$

gegeben durch die Homomorphismen

$$\begin{array}{lll} \mathbb{F}_2[x_1,x_2] \to \mathbb{F}_2[x], & \mathbb{F}_2[x_1,x_2] \to \mathbb{F}_2[x], & \mathbb{F}_2[x_1,x_2] \to \mathbb{F}_2[x], \\ f(x_1,x_2) \mapsto f(x,0) & f(x_1,x_2) \mapsto f(0,x) & f(x_1,x_2) \mapsto f(x,x). \end{array}$$

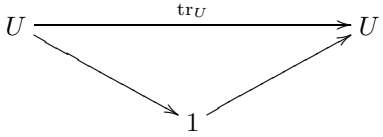
Beweis: Für die Erzeuger x_1 und x_2 von $H^*(G,\mathbb{F}_2) = \mathbb{F}_2[x_1,x_2]$ hat man

$$\begin{aligned} \iota_1^*(x_1) &= \iota_1^*(\pi_1^* x) = (\pi_1\,\iota_1)^* x = \mathrm{id}_U^* x = \mathrm{id}_{H^1(U,\mathbb{F}_2)} x = x \\ \iota_1^*(x_2) &= \iota_1^*(\pi_2^* x) = (\pi_2\,\iota_1)^* x = \mathrm{tr}_U^* x = \mathrm{tr}_{H^1(U,\mathbb{F}_2)} x = 0 \end{aligned}$$

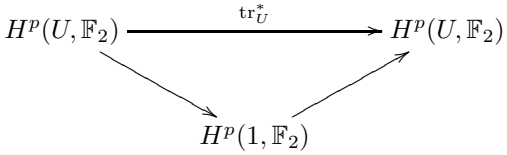
mit der trivialen Abbildung $\mathrm{tr}_U : U \to U$. Hierbei ist die funktorielle Abbildung

$$\mathrm{tr}_U^* : H^*(U,\mathbb{F}_2) \to H^*(U,\mathbb{F}_2)$$

gleich dem Einsetzungshomomorphismus $x \mapsto 0$ von $H^*(U,\mathbb{F}_2) = \mathbb{F}_2[x]$, weil das kommutative Diagramm



Anlass gibt zu kommutativen Diagrammen



und $H^p(1,\mathbb{F}_2)$ für $p \geq 1$ trivial ist. Ganz entsprechend erhält man

$$\iota_2^*(x_1) = 0, \quad \iota_2^*(x_2) = x.$$

Was schließlich die diagonale Einbettung $\iota_3 = \Delta$ betrifft, so gilt

$$\Delta^*(x_i) = \Delta^*(\pi_i^* x) = (\pi_i\,\Delta)^* x = \mathrm{id}_U^* x = \mathrm{id}_{H^1(U,\mathbb{F}_2)} x = x$$

für $i = 1, 2$. Also sind ι_1^*, ι_2^* und Δ^* gleich den oben angegebenen Abbildungen. □

Jetzt sind wir in der Lage, den Beweis von Satz 3.7 nachzutragen (den wir weiter oben zur Begründung unseres Hauptresultates 3.2 bereits herangezogen hatten).

Beweis von Satz 3.7: Es seien $x \in H^1(U,\mathbb{F}_2)$ der Erzeuger von $H^*(U,\mathbb{F}_2)$ und $x_1, x_2 \in H^1(G,\mathbb{F}_2)$ Erzeugende von $H^*(G,\mathbb{F}_2)$ wie in Lemma 3.11. Zu bestimmen ist der Kern der funktoriellen Abbildung

$$\iota^* : H^3(G,\mathbb{F}_2) \xrightarrow{(\iota_1^*,\iota_2^*,\iota_3^*)} H^3(U,\mathbb{F}_2) \times H^3(U,\mathbb{F}_2) \times H^3(U,\mathbb{F}_2).$$

Sie ist Einschränkung der funktoriellen Abbildung

$$\iota^* : H^*(G,\mathbb{F}_2) \xrightarrow{(\iota_1^*,\iota_2^*,\iota_3^*)} H^*(U,\mathbb{F}_2) \times H^*(U,\mathbb{F}_2) \times H^*(U,\mathbb{F}_2)$$

mit den Komponenten

$$\begin{aligned}
\iota_1^* : H^*(G,\mathbb{F}_2) &\longrightarrow H^*(U,\mathbb{F}_2) \quad \text{def. durch} \quad \iota_1^*(x_1) = x,\ \ \iota_1^*(x_2) = 0\\
\iota_2^* : H^*(G,\mathbb{F}_2) &\longrightarrow H^*(U,\mathbb{F}_2) \quad \text{def. durch} \quad \iota_2^*(x_1) = 0,\ \ \iota_2^*(x_2) = x\\
\iota_3^* : H^*(G,\mathbb{F}_2) &\longrightarrow H^*(U,\mathbb{F}_2) \quad \text{def. durch} \quad \iota_3^*(x_1) = x,\ \ \iota_3^*(x_2) = x
\end{aligned}$$

auf den direkten Summenden $H^3(G,\mathbb{F}_2)$ von $H^*(G,\mathbb{F}_2)$. Es handelt sich also um den $\mathbb{F}_2$-Algebrenhomomorphismus

$$\begin{aligned}
H^*(G,\mathbb{F}_2) &\longrightarrow H^*(U,\mathbb{F}_2) \times H^*(U,\mathbb{F}_2) \times H^*(U,\mathbb{F}_2)\\
\text{d. h. } \mathbb{F}_2[x_1,x_2] &\longrightarrow \mathbb{F}_2[x] \times \mathbb{F}_2[x] \times \mathbb{F}_2[x],\\
f(x_1,x_2) &\longmapsto (f(x,0), f(0,x), f(x,x))
\end{aligned}$$

und seine Einschränkung auf den Teilraum

$$H^3(G,\mathbb{F}_2) = \mathbb{F}_2 x_1^3 + \mathbb{F}_2 x_1^2 x_2 + \mathbb{F}_2 x_1 x_2^2 + \mathbb{F}_2 x_2^3,$$

wobei wir es hier mit einer direkten Summe zu tun haben. Für den Kern von ι^* gilt

$$\ker \iota^* = \ker \iota_1^* \cap \ker \iota_2^* \cap \ker \iota_3^*.$$

Nach Definition von ι_1^* und ι_2^* (s. auch Lemma 3.11) sind die Bilder eines Elementes

$$\gamma = a x_1^3 + b x_1^2 x_2 + c x_1 x_2^2 + d x_2^3$$

von $H^3(G,\mathbb{F}_2)$ unter diesen Abbildungen durch

$$\iota_1^*(\gamma) = a x^3, \quad \iota_2^*(\gamma) = d x^3$$

gegeben und man erhält deshalb

$$\begin{aligned}
\ker \iota_1^* &= \{\gamma = a x_1^3 + b x_1^2 x_2 + c x_1 x_2^2 + d x_2^3 \text{ aus } H^3(G,\mathbb{F}_2) \text{ mit } a = 0\}\\
&= \mathbb{F}_2 x_1^2 x_2 + \mathbb{F}_2 x_1 x_2^2 + \mathbb{F}_2 x_2^3,\\
\ker \iota_2^* &= \{\gamma = a x_1^3 + b x_1^2 x_2 + c x_1 x_2^2 + d x_2^3 \text{ aus } H^3(G,\mathbb{F}_2) \text{ mit } d = 0\}\\
&= \mathbb{F}_2 x_1^3 + \mathbb{F}_2 x_1^2 x_2 + \mathbb{F}_2 x_1 x_2^2.
\end{aligned}$$

Hieraus folgt

$$\begin{aligned}
\ker \iota_1^* \cap \ker \iota_2^* &= \{\gamma = b x_1^2 x_2 + c x_1 x_2^2 \text{ aus } H^3(G,\mathbb{F}_2)\}\\
&= \mathbb{F}_2 x_1^2 x_2 + \mathbb{F}_2 x_1 x_2^2.
\end{aligned}$$

Für $b, c \in \mathbb{F}_2$ wird das Element $b x_1^2 x_2 + c x_1 x_2^2$ von $\ker \iota_1^* \cap \ker \iota_2^*$ unter ι_3^* auf $b x^3 + c x^3$ abgebildet und es gilt

$$b x^3 + c x^3 = 0 \Leftrightarrow b = c;$$

darum hat man

$$\begin{aligned}
\ker \iota_1^* \cap \ker \iota_2^* \cap \ker \iota_3^* &= \{\gamma = b(x_1^2 x_2 + x_1 x_2^2) \text{ aus } H^3(G,\mathbb{F}_2)\}\\
&= \mathbb{F}_2(x_1^2 x_2 + x_1 x_2^2) \simeq \mathbb{F}_2,
\end{aligned}$$

so dass $\ker \iota^* \simeq \mathbb{F}_2$ ist. □

3.v Ein dritter Beweis von Theorem 3.1

Es sei $G = < t >$ eine zyklische Gruppe der Ordnung n. In diesem Abschnitt sollen die von den Inklusionen

$$\begin{array}{ccc} \iota_1 : G \longrightarrow G \times G, & \text{und} & \iota_2 : G \longrightarrow G \times G, \\ g \longmapsto (g, 1) & & g \longmapsto (1, g) \end{array}$$

sowie die von der diagonalen Einbettung

$$\begin{array}{c} \Delta : G \longrightarrow G \times G, \\ g \longmapsto (g, g) \end{array}$$

vermittelten Inklusionen $H_3(G, \mathbb{Z}) \to H_3(G \times G, \mathbb{Z})$ untersucht werden. Der folgende Satz wird auf sehr direktem Wege unter Rückgriff auf die Definition der Kohomologiegruppen und Morphismen seinen Beweis finden.

Satz 3.12 *Sei $G = < t >$ eine zyklische Gruppe der Ordnung n. Desweiteren seien G_1, G_2, G_3 die von $(t, 1)$, $(1, t)$ und (t, t) erzeugten zu G isomorphen Untergruppen von $G \times G$. Dann ist die Abbildung*

$$g : \coprod_{i=1}^{3} H_3(G_i, \mathbb{Z}) \longrightarrow H_3(G \times G, \mathbb{Z}),$$

die für $\sum_i z_i \in \coprod_{i=1}^3 H_3(G_i, \mathbb{Z})$ durch

$$g\Big(\sum_i z_i\Big) = \sum_i cor^{G_i}_{G\times G} z_i$$

gegeben ist, ein Isomorphismus.

Die in Satz 3.2 vorkommenden Kohomologiegruppen sind endlich, wie sich im Verlauf des Abschnitts noch herausstellen wird. Es bezeichne ι_3 die diagonale Einbettung $\Delta : G_3 \hookrightarrow G \times G$. Dann ist die Coresriktionsabbildung

$$\mathrm{cor}^{G_i}_{G\times G} : H_3(G_i, \mathbb{Z}) \longrightarrow H_3(G \times G, \mathbb{Z})$$

für $i = 1, 2, 3$ gleich der funktoriellen Abbildung

$$(\iota_i)_* : H_3(G_i, \mathbb{Z}) \longrightarrow H_3(G \times G, \mathbb{Z}).$$

Diese drei Inklusionen gilt es zu explizieren.

Projektive Auflösungen von $\mathbb{Z}$

Wir beginnen mit der Betrachtung projektiver Auflösungen von $\mathbb{Z}$ über $\mathbb{Z}[G]$ und über $\mathbb{Z}[G \times G]$. Ist allgemeiner G eine beliebige Gruppe, so nennt man für einen G-Modul M eine exakte Sequenz

$$\cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

von G-Moduln eine Auflösung von M, vgl. [B, S. 10], und spricht von einer projektiven Auflösung, wenn alle F_i projektive $\mathbb{Z}[G]$-Moduln sind. Versieht man $\mathbb{Z}$ mit der trivialen Operation, so ist $\mathbb{Z}$ ein G-Modul. Man definiert die Augmentation

$\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ als den durch $1 \mapsto 1$ definierten G-Modulhomomorphismus; die Augmentation ist also die Abbildung

$$\begin{aligned} \varepsilon \ : \ \mathbb{Z}[G] \ &\longrightarrow \ \mathbb{Z}\,, \\ \sum_{g\in G} n_g g &\longmapsto \sum_{g\in G} n_g. \end{aligned}$$

Dazu sei angemerkt, dass für jeden G-Modul M die Isomorphie

$$\begin{aligned} \mathrm{Hom}_G(\mathbb{Z}[G], M) &\longrightarrow M, \\ \varphi \qquad &\longmapsto \varphi(1) \end{aligned}$$

besteht; ein Element von $\mathrm{Hom}_G(\mathbb{Z}[G], M)$ anzugeben bedeutet also nichts anderes als das Bild von $1 \in \mathbb{Z}[G]$ zu nennen. Weiter wird durch $N = 1+t+\cdots+t^{n-1} \in \mathbb{Z}[G]$ die Norm definiert. Nachdem diese Begriffe eingeführt sind, formulieren wir (siehe [B, S. 35])

3.13 Lemma. *Für eine endliche zyklische Gruppe G mit erzeugendem Element t stellt die Sequenz*

$$\cdots \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{4}$$

eine projektive Auflösung von $\mathbb{Z}$ über $\mathbb{Z}[G]$ dar.

Beweis: Zunächst einmal ist mit $t-1$ der G-Homomorphismus $\mathbb{Z}[G] \to \mathbb{Z}[G]$ gemeint, unter dem 1 auf $t-1$ abgebildet wird, und ganz entsprechend ist die Normabbildung N definiert, d. h. es handelt sich um die $\mathbb{Z}[G]$-linearen Abbildungen

$$\begin{aligned} \mathbb{Z}[G] \ &\xrightarrow{t-1} \ \mathbb{Z}[G], \\ \sum_{g\in G} n_g g &\longmapsto \sum_{g\in G} n_g g(t-1) \\ &= \left(\sum_{g\in G} n_g g\right)(t-1) \end{aligned}$$

und

$$\begin{aligned} \mathbb{Z}[G] \ &\xrightarrow{N} \ \mathbb{Z}[G], \\ \sum_{g\in G} n_g g \longmapsto \sum_{g\in G} n_g gN = \sum_{g\in G} n_g N &= \left(\sum_{g\in G} n_g\right)N \\ &= \left(\sum_{g\in G} n_g g\right)N. \end{aligned}$$

Wir wollen uns kurz von der Exaktheit der Sequenz (4) überzeugen. Dass die Augmentation ε surjektiv ist, ist offensichtlich. Ihr Kern ist das Augmentationsideal

$$I_G = \mathbb{Z}[G](t-1),$$

denn wenn für ein Element $x = \sum n_k t^k$ von $\mathbb{Z}[G]$ die Augmentation $\varepsilon(x) = \sum n_k$ verschwindet, so gilt

$$\begin{aligned} x = \sum_k n_k t^k - \sum_k n_k = \sum_k n_k\big(t^k - 1\big) &= \sum_{k=1}^{n-1} n_k \sum_{i=0}^{k-1} t^i (t-1) \\ &= \left(\sum_{k=0}^{n-1} n_k \sum_{i=0}^{k-1} t^i\right)(t-1), \end{aligned}$$

und umgekehrt wird jedes Element vom Typ

$$\Big(\sum_{g\in G} n_g g\Big)(t-1) = \sum_{g\in G} n_g g(t-1)$$

unter der Augmentation auf 0 abgebildet, weil $t-1$ im Kern liegt und es sich um einen G-Homomorphismus handelt. Soviel zur Exaktheit an den letzten beiden Stellen. Weiter bestehen für jedes $x = \sum n_k t^k$ aus $\mathbb{Z}[G]$ die Äquivalenzen

$$\begin{aligned} x(t-1)=0 &\iff \Big(\sum_{k=0}^{n-1} n_k t^k\Big)(t-1)=0 \iff \sum_{k=0}^{n-1} n_k t^{k+1} - \sum_{k=0}^{n-1} n_k t^k = 0 \\ &\iff \sum_{k=1}^{n} n_{k-1} t^k - \sum_{k=0}^{n-1} n_k t^k = 0 \\ &\iff \forall\, k \in \{1,\dots,n-1\}\ n_{k-1} = n_k \\ &\iff x = \sum_{k=0}^{n-1} n_0 t^k = n_0 N, \end{aligned}$$

woraus $\ker(t-1) = \mathbb{Z}[G]N$ folgt, und für jedes $x = \sum n_g g$ aus $\mathbb{Z}[G]$ gilt

$$\begin{aligned} xN = 0 &\iff \sum n_g gN = \Big(\sum n_g g\Big)N = 0 \\ &\iff \sum n_g N = \Big(\sum n_g\Big)N = 0 \iff \sum n_g = 0, \end{aligned}$$

was $\ker N = I_G = \mathbb{Z}[G](t-1)$ zur Folge hat. Die Sequenz (4) ist demnach exakt und damit ist nachgewiesen, daß $\varepsilon : F \to \mathbb{Z}$ mit dem Komplex

$$F: \quad \cdots \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G],$$

also $F = \big((F_i)_i, (\partial_i : F_i \to F_{i-1})_i\big)$ wobei

$$F_i = \mathbb{Z}[G] \text{ für } i \geq 0 \quad \text{und} \quad \partial_i = \begin{cases} t-1 & \text{für ungerades } i > 0 \\ N & \text{für gerades } i > 0, \end{cases}$$

eine projektive Auflösung von $\mathbb{Z}$ durch freie, also insbesondere projektive $\mathbb{Z}[G]$-Moduln darstellt. □

Wir betrachten jetzt das Tensorprodukt $F \otimes F$ des Komplexes F mit sich selbst über dem Ring $\mathbb{Z}$. Für jedes $m \geq 0$ ist die Gruppe $(F \otimes F)_m$ per Definition durch die direkte Summe

$$(F \otimes F)_m = \bigoplus_{p+q=m} F_p \otimes F_q$$

gegeben und desweiteren ist für jedes $m > 0$ die Randabbildung $\mathcal{D}_m$ auf der direkten Komponente $F_p \otimes F_q$ von $(F \otimes F)_m$ durch

$$\mathcal{D}_m(x \otimes y) = (\partial_p x) \otimes y + (-1)^p x \otimes (\partial_q y)$$

definiert, vgl. [B, S. 7]. Die Gruppen $F_p \otimes F_q$ werden durch die Operation

$$(g,h) \cdot (x \otimes y) = (gx) \otimes (hy)$$

zu $(G \times G)$-Moduln, so dass auch die direkten Summen $(F \otimes F)_m$ mit komponentenweiser Operation $(G \times G)$-Moduln sind. Mit den wie oben definierten Randabbildungen $\mathcal{D}_m$ ist $F \otimes F$ also ein Komplex von $(G \times G)$-Moduln, denn wie man kann

leicht nachrechnen kann gilt für alle $m > 1$ die Gleichung $\mathcal{D}_{m-1} \circ \mathcal{D}_m = 0$. Der Isomorphismus

$$\begin{aligned} \mathbb{Z}[G] \otimes \mathbb{Z}[G] &\longrightarrow \mathbb{Z}[G \times G], \\ g \otimes h &\longmapsto (g, h) \end{aligned}$$

von $(G \times G)$-Moduln zeigt, dass alle $F_p \otimes F_q = \mathbb{Z}[G] \otimes \mathbb{Z}[G]$ freie und damit projektive $\mathbb{Z}[G \times G]$-Moduln sind. Als direkte Summen projektiver $\mathbb{Z}[G \times G]$-Moduln sind dann auch die $(F \otimes F)_m$ projektive $\mathbb{Z}[G \times G]$-Moduln. Wenn wir mit $\varepsilon \otimes \varepsilon$ die Augmentation

$$\begin{aligned} \mathbb{Z}[G] \otimes \mathbb{Z}[G] &\longrightarrow \mathbb{Z}, \\ g \otimes h &\longmapsto 1 \end{aligned}$$

von $(F \otimes F)_0 = F_0 \otimes F_0 = \mathbb{Z}[G] \otimes \mathbb{Z}[G]$ in den trivialen $(G \times G)$-Modul $\mathbb{Z}$ bezeichnen, so gilt weiter: Die projektive Auflösung $\varepsilon : F \to \mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G]$ liefert mit $\varepsilon \otimes \varepsilon : F \otimes F \to \mathbb{Z}$ eine projektive Auflösung von $\mathbb{Z}$ über $\mathbb{Z}[G \times G]$, vgl. [B, S. 107].

Bestimmung von $H_3(G, \mathbb{Z})$

Mit dem Ziel der Bestimmung von $H_3(G, \mathbb{Z})$ betrachten wir die projektive Auflösung $\varepsilon : F \to \mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G]$, bei der F ein Komplex von $\mathbb{Z}[G]$-Linksmoduln ist. Mit der trivialen Operation von G versehen wird $\mathbb{Z}$ zu einem $\mathbb{Z}[G]$-Rechtsmodul, und Tensorieren mit F über $\mathbb{Z}[G]$ liefert den Komplex

$$F_G : \quad \cdots \xrightarrow{1 \otimes \partial_3} \mathbb{Z} \otimes_{\mathbb{Z}[G]} F_2 \xrightarrow{1 \otimes \partial_2} \mathbb{Z} \otimes_{\mathbb{Z}[G]} F_1 \xrightarrow{1 \otimes \partial_1} \mathbb{Z} \otimes_{\mathbb{Z}[G]} F_0$$

von abelschen Gruppen. Für alle i ist dabei

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} F_i \;=\; \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \;\simeq\; \mathbb{Z},$$

denn der Homomorphismus

$$\begin{aligned} 1 \otimes \varepsilon \;:\; \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] &\longrightarrow \mathbb{Z}, \\ m \otimes \Big(\sum_{g \in G} n_g g \Big) &\longmapsto m \sum_{g \in G} n_g \end{aligned}$$

ist ein Isomorphismus mit der Umkehrabbildung $m \mapsto m \otimes 1$. Für ungerades i ist die Randabbildung $1 \otimes \partial_i$ des Komplexes F_G gleich $1 \otimes (t - 1)$ und bildet das Element $1 \otimes 1$ von $\mathbb{Z}[G]$ auf

$$1 \otimes (t-1) = 1 \otimes t - 1 \otimes 1 = 1 \otimes 1 - 1 \otimes 1 = 0$$

ab, für gerades i ist sie gleich $1 \otimes N$ und $1 \otimes 1$ wird auf

$$1 \otimes N = 1 \otimes \Big(\sum_{g \in G} g \Big) = \sum_{g \in G} 1 \otimes g = \sum_{g \in G} 1 \otimes 1 = n \otimes 1$$

abgebildet. Also ist F_G der Komplex

$$\cdots \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z}.$$

Per Definition sind für alle $i > 0$ die Homologiegruppen durch

$$H_i(G, \mathbb{Z}) = H_i(F_G)$$

gegeben, vgl. [B, S. 35], und es folgt

$$H_i(G,\mathbb{Z}) \simeq \begin{cases} \mathbb{Z} & \text{für } i = 0 \\ \mathbb{Z}/n & \text{für ungerades } i > 0 \\ 0 & \text{für gerades } i > 0. \end{cases}$$

Der Komplex $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)$

Wir kehren jetzt zur projektiven Auflösung $\varepsilon \otimes \varepsilon : F \otimes F \to \mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G \times G]$ zurück, um anhand dieser die Gruppe $H_3(G \times G, \mathbb{Z})$ zu bestimmen. Mit der trivialen Operation von $G \times G$ wird $\mathbb{Z}$ zu einem $\mathbb{Z}[G \times G]$-Rechtsmodul und $F \otimes F$ ist ein Komplex von $\mathbb{Z}[G \times G]$-Linksmoduln, so dass man durch Tensorisation von $\mathbb{Z}$ mit $F \otimes F$ über $\mathbb{Z}[G \times G]$ den Komplex

$$\cdots \xrightarrow{1\otimes\mathcal{D}_3} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)_2 \xrightarrow{1\otimes\mathcal{D}_2} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)_1 \xrightarrow{1\otimes\mathcal{D}_1} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)_0$$

von abelschen Gruppen erhält. Dabei ist für alle m nach Definition von $(F \otimes F)_m$

$$\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)_m = \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(\bigoplus_{p+q=m} F_p \otimes F_q \right)$$

und es bestehen die Isomorphien

$$\begin{aligned} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(\bigoplus_{p+q=m} F_p \otimes F_q \right) &\simeq \bigoplus_{p+q=m} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right) \\ \simeq \bigoplus_{p+q=m} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \mathbb{Z}[G \times G] &\simeq \bigoplus_{p+q=m} \mathbb{Z} \end{aligned}$$

von abelschen Gruppen. Beim ersten Isomorphismus wird ein Element vom Typ $m \otimes (x_{pq})_{p,q}$ auf $(m \otimes x_{pq})_{p,q}$ abgebildet, während der zweite durch die Isomorphie der $(G \times G)$-Moduln $F_p \otimes F_q$ und $\mathbb{Z}[G \times G]$ vermittelt wird. Für alle m gilt also

$$\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)_m \simeq \bigoplus_{p+q=m} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right) \simeq \mathbb{Z}^{m+1},$$

und um $H_3(G \times G, \mathbb{Z})$ zu bestimmen hat man die Randabbildungen

$$\begin{aligned} \bigoplus_{p+q=4} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right) &\longrightarrow \bigoplus_{p+q=3} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right) \\ &\longrightarrow \bigoplus_{p+q=2} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right) \end{aligned} \tag{5}$$

zu betrachten. Um diese zu verstehen, schauen wir zunächst die Randabbildungen

$$\bigoplus_{p+q=4} F_p \otimes F_q \xrightarrow{\mathcal{D}_4} \bigoplus_{p+q=3} F_p \otimes F_q \xrightarrow{\mathcal{D}_3} \bigoplus_{p+q=2} F_p \otimes F_q$$

des Komplexes $F \otimes F$ an, also die Homomorphismen von $\mathbb{Z}[G \times G]$-Moduln, aus denen durch Tensorieren mit $\mathbb{Z}$ über $\mathbb{Z}[G\times G]$ die Randabbildungen (5) hervorgehen.

Die Randabbildungen von $F \otimes F$

Da die $\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]} \left(F_p \otimes F_q\right)$ isomorph zu $\mathbb{Z}$ sind und jeweils vom Element $1\otimes(1\otimes 1)$ erzeugt werden, wollen wir sehen, wohin die Elemente $1 \otimes 1$ aus den einzelnen

direkten Summanden $F_p \otimes F_q$ unter $\mathcal{D}_4$ und $\mathcal{D}_3$ abgebildet werden. Betrachten wir als erstes die Einschränkungen von $\mathcal{D}_4$ auf die einzelnen direkten Summanden $F_p \otimes F_q$. Ausrechnen ergibt

$$\begin{aligned}
&F_0 \otimes F_4 \longrightarrow \big(F_0 \otimes F_3\big) \oplus \big(F_1 \otimes F_2\big) \oplus \big(F_2 \otimes F_1\big) \oplus \big(F_3 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (\textstyle\sum_{g\in G} 1 \otimes g,\;\; 0,\;\; 0,\;\; 0)
\end{aligned}$$

$$\begin{aligned}
&F_1 \otimes F_3 \longrightarrow \big(F_0 \otimes F_3\big) \oplus \big(F_1 \otimes F_2\big) \oplus \big(F_2 \otimes F_1\big) \oplus \big(F_3 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (t \otimes 1 - 1 \otimes 1,\;\; -1 \otimes t + 1 \otimes 1,\;\; 0,\;\; 0)
\end{aligned}$$

$$\begin{aligned}
&F_2 \otimes F_2 \longrightarrow \big(F_0 \otimes F_3\big) \oplus \big(F_1 \otimes F_2\big) \oplus \big(F_2 \otimes F_1\big) \oplus \big(F_3 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (0,\;\; \textstyle\sum_{g\in G} g \otimes 1,\;\; \sum_{g\in G} 1 \otimes g,\;\; 0)
\end{aligned}$$

$$\begin{aligned}
&F_3 \otimes F_1 \longrightarrow \big(F_0 \otimes F_3\big) \oplus \big(F_1 \otimes F_2\big) \oplus \big(F_2 \otimes F_1\big) \oplus \big(F_3 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (0,\;\; 0,\;\; t \otimes 1 - 1 \otimes 1,\;\; -1 \otimes t + 1 \otimes 1)
\end{aligned}$$

$$\begin{aligned}
&F_4 \otimes F_0 \longrightarrow \big(F_0 \otimes F_3\big) \oplus \big(F_1 \otimes F_2\big) \oplus \big(F_2 \otimes F_1\big) \oplus \big(F_3 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (0,\;\; 0,\;\; 0,\;\; \textstyle\sum_{g\in G} g \otimes 1)
\end{aligned}$$

Betrachtung der Einschränkungen von $\mathcal{D}_3$ auf die einzelnen direkten Summanden $F_p \otimes F_q$ liefert hingegen folgendes Ergebnis:

$$\begin{aligned}
&F_0 \otimes F_3 \longrightarrow \big(F_0 \otimes F_2\big) \oplus \big(F_1 \otimes F_1\big) \oplus \big(F_2 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (1 \otimes t - 1 \otimes 1,\;\; 0,\;\; 0)
\end{aligned}$$

$$\begin{aligned}
&F_1 \otimes F_2 \longrightarrow \big(F_0 \otimes F_2\big) \oplus \big(F_1 \otimes F_1\big) \oplus \big(F_2 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (t \otimes 1 - 1 \otimes 1,\;\; -\textstyle\sum_{g\in G} 1 \otimes g,\;\; 0)
\end{aligned}$$

$$\begin{aligned}
&F_2 \otimes F_1 \longrightarrow \big(F_0 \otimes F_2\big) \oplus \big(F_1 \otimes F_1\big) \oplus \big(F_2 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (0,\;\; \textstyle\sum_{g\in G} g \otimes 1,\;\; 1 \otimes t - 1 \otimes 1)
\end{aligned}$$

$$\begin{aligned}
&F_3 \otimes F_0 \longrightarrow \big(F_0 \otimes F_2\big) \oplus \big(F_1 \otimes F_1\big) \oplus \big(F_2 \otimes F_0\big),\\
&1 \otimes 1 \;\longmapsto (0,\;\; 0,\;\; t \otimes 1 - 1 \otimes 1)
\end{aligned}$$

Die Randabbildungen von $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} (F \otimes F)$

Nachdem geklärt ist, was mit den Elementen $1 \otimes 1$ der direkten Summanden von $\bigoplus_{p+q=4} F_p \otimes F_q$ und $\bigoplus_{p+q=3} F_p \otimes F_q$ unter den Randabbildungen $\mathcal{D}_4$ bzw. $\mathcal{D}_3$ geschieht, soll jetzt etwas zu den Bildern der Elemente $1 \otimes (1 \otimes 1)$ aus den direkten Summanden von $\bigoplus_{p+q=4} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big)$ und $\bigoplus_{p+q=3} \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big)$ unter den Abbildungen der Sequenz (5) gesagt werden. Man kann die $1 \otimes (1 \otimes 1)$ auch als Elemente von

$$\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \Big(\bigoplus_{p+q=4} F_p \otimes F_q \Big) \quad \text{bzw.} \quad \mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \Big(\bigoplus_{p+q=3} F_p \otimes F_q \Big)$$

auffassen. Da die auf diesen Gruppen definierten Randabbildungen nichts anderes sind als $\mathcal{D}_4$ und $\mathcal{D}_3$ von links mit der Identität von $\mathbb{Z}$ tensoriert, erhält man die Bilder der $1 \otimes (1 \otimes 1)$ ganz einfach indem man die Bilder der $1 \otimes 1$ unter $\mathcal{D}_4$ und $\mathcal{D}_3$ von links mit der 1 von $\mathbb{Z}$ tensoriert, und bei der Sequenz (5) wird sie in die einzelnen

Komponenetn gezogen. Zur expliziten Berechnung der Bilder der $1 \otimes (1 \otimes 1)$ ist nur noch zu sagen, dass für alle p, q und $g, h \in G$ im Tensorprodukt $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big)$ die Gleichung

$$1 \otimes (g \otimes h) = 1 \otimes ((g,h) \cdot (1 \otimes 1)) = (1 \cdot (g,h)) \otimes (1 \otimes 1) = 1 \otimes (1 \otimes 1),$$

erfüllt ist, d. h. die 1 von $\mathbb{Z}$ ergibt mit einem Element von $F_p \otimes F_q$ vom Typ $g \otimes h$ tensoriert das erzeugende Element von $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big)$. Es bleibt jetzt nichts weiter zu tun, als die oben angegebenen Bilder der $1 \otimes 1$ komponenentenweise von links mit 1 zu tensorieren, wobei die folgende Tensorprodukte vorkommen:

$$1 \otimes (1 \otimes t - 1 \otimes 1) = 1 \otimes (1 \otimes t) - 1 \otimes (1 \otimes 1) = 0$$

$$1 \otimes (t \otimes 1 - 1 \otimes 1) = 1 \otimes (t \otimes 1) - 1 \otimes (1 \otimes 1) = 0$$

$$1 \otimes \big(\textstyle\sum_{g\in G} 1 \otimes g\big) = \sum_{g\in G} 1 \otimes (1 \otimes g) = \sum_{g\in G} 1 \otimes (1 \otimes 1) = n \otimes (1 \otimes 1)$$

$$1 \otimes \big(\textstyle\sum_{g\in G} g \otimes 1\big) = \sum_{g\in G} 1 \otimes (g \otimes 1) = \sum_{g\in G} 1 \otimes (1 \otimes 1) = n \otimes (1 \otimes 1)$$

Weil die $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big)$ isomorph zu $\mathbb{Z}$ sind mit $1 \otimes (1 \otimes 1)$ als erzeugendem Element, handelt es sich bei der Sequenz (5) um eine Sequenz

$$\mathbb{Z}^5 \longrightarrow \mathbb{Z}^4 \longrightarrow \mathbb{Z}^3,$$

und die Einschränkungen der in ihr vorkommenden Homomorphismen auf die einzelnen direkten Summanden von $\mathbb{Z}^5$ und $\mathbb{Z}^4$ sind uns bekannt, da wir die Bilder der $1 \otimes (1 \otimes 1)$ unter den Abbildungen von Sequenz (5) angeben können, die aus den bereits angegebenen Bildern der $1 \otimes 1$ unter $\mathcal{D}_4$ und $\mathcal{D}_3$ resultieren, indem man komponentenweise von links mit 1 tensoriert. In derselben Reihenfolge wie oben ergeben sich also aus den Einschränkungen von $\mathcal{D}_4$ und $\mathcal{D}_3$ auf die direkten Summanden $F_p \otimes F_q$ von $\bigoplus_{p+q=4} F_p \otimes F_q$ bzw. $\bigoplus_{p+q=3} F_p \otimes F_q$ auf den $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(F_p \otimes F_q\big) \simeq \mathbb{Z}$ die folgenden Abbildungen:

Einschränkungen der Abbildung $\mathbb{Z}^5 \to \mathbb{Z}^4$

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$1 \longmapsto (n,\ 0,\ 0,\ 0)$$

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$1 \longmapsto (0,\ 0,\ 0,\ 0)$$

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$1 \longmapsto (0,\ n,\ n,\ 0)$$

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$1 \longmapsto (0,\ 0,\ 0,\ 0)$$

$$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$1 \longmapsto (0,\ 0,\ 0,\ n)$$

Bestimmung von $H_3(G \times G, \mathbb{Z})$

Zusammenfassend haben wir es demnach mit der Abbildung

$$\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \ \longrightarrow\ \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z},$$
$$(p_1,\ p_2,\ p_3,\ p_4,\ p_5) \longmapsto (p_1 \cdot n,\ p_3 \cdot n,\ p_3 \cdot n,\ p_5 \cdot n)$$

zu tun und ihr Bild ist $\mathbb{Z}(n,\ 0,\ 0,\ 0) + \mathbb{Z}(0,\ n,\ n,\ 0) + \mathbb{Z}(0,\ 0,\ 0,\ n)$.

Einschränkungen der Abbildung $\mathbb{Z}^4 \to \mathbb{Z}^3$

$$\begin{aligned}
&\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\
&1 \longmapsto (0,\ 0,\ 0) \\
&\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\
&1 \longmapsto (0,\ -n,\ 0) \\
&\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\
&1 \longmapsto (0,\ n,\ 0) \\
&\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\
&1 \longmapsto (0,\ 0,\ 0)
\end{aligned}$$

Hier haben wir es mit der Abbildung

$$\begin{aligned}
\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \ &\longrightarrow\ \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\
(p_1,\ p_2,\ p_3,\ p_4) &\longmapsto (0,\ (p_3 - p_2) \cdot n,\ 0)
\end{aligned}$$

tu tun, deren Kern $\mathbb{Z}(1,\ 0,\ 0,\ 0) + \mathbb{Z}(0,\ 1,\ 1,\ 0) + \mathbb{Z}(0,\ 0,\ 0,\ 1)$ ist.

Die Bestimmung von $H_3(G \times G, \mathbb{Z})$ erfolgt über die Sequenz (5) bzw. über die zuletzt betrachtete Sequenz $\mathbb{Z}^5 \to \mathbb{Z}^4 \to \mathbb{Z}^3$. Quotientenbildung ergibt

$$H_3(G \times G, \mathbb{Z}) \simeq \frac{\mathbb{Z}(1,\ 0,\ 0,\ 0) + \mathbb{Z}(0,\ 1,\ 1,\ 0) + \mathbb{Z}(0,\ 0,\ 0,\ 1)}{\mathbb{Z}(n,\ 0,\ 0,\ 0) + \mathbb{Z}(0,\ n,\ n,\ 0) + \mathbb{Z}(0,\ 0,\ 0,\ n)} \simeq (\mathbb{Z}/n)^3.$$

Die funktoriellen Abbildungen

Nachdem die Gruppen $H_3(G, \mathbb{Z})$ und $H_3(G \times G, \mathbb{Z})$ bestimmt sind, wollen wir im folgenden die von ι_1, ι_2 und Δ vermittelten Abbildungen $H_3(G, \mathbb{Z}) \to H_3(G \times G, \mathbb{Z})$ untersuchen. Dazu betrachten wir wieder die projektiven Auflösungen $\varepsilon : F \to \mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G]$ und $\varepsilon \otimes \varepsilon : F \otimes F \to \mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G \times G]$, also

$$\cdots \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

und

$$\cdots \xrightarrow{\mathcal{D}_3} \bigoplus_{p+q=2} F_p \otimes F_q \xrightarrow{\mathcal{D}_2} \bigoplus_{p+q=1} F_p \otimes F_q \xrightarrow{\mathcal{D}_1} F_0 \otimes F_0 \xrightarrow{\varepsilon\otimes\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Letztere Sequenz kann mittels ι_1, ι_2 und Δ ebenfalls als exakte Sequenz von G-Moduln und -Homomorphismen aufgefaßt werden, indem für $x \in (F \otimes F)_m$ und $g \in G$

$$g \cdot x = \iota_1(g) \cdot x, \quad g \cdot x = \iota_2(g) \cdot x \quad \text{bzw.} \quad g \cdot x = \Delta(g) \cdot x$$

gesetzt wird. Weil alle $F_i = \mathbb{Z}[G]$ projektive $\mathbb{Z}[G]$-Moduln sind und die Sequenz $\varepsilon \otimes \varepsilon : F \otimes F \to \mathbb{Z}$ azyklisch ist, gibt es eine G-Kettenabbildung τ, die das Diagramm

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{t-1} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{t-1} & \mathbb{Z}[G] & \xrightarrow{\varepsilon} & \mathbb{Z} \\
\downarrow & & \downarrow{\scriptstyle \tau_2} & & \downarrow{\scriptstyle \tau_1} & & \downarrow{\scriptstyle \tau_0} & & \downarrow{\scriptstyle 1} \\
\cdots & \xrightarrow{\mathcal{D}_3} & \bigoplus_{p+q=2} F_p \otimes F_q & \xrightarrow{\mathcal{D}_2} & \bigoplus_{p+q=1} F_p \otimes F_q & \xrightarrow{\mathcal{D}_1} & F_0 \otimes F_0 & \xrightarrow{\varepsilon\otimes\varepsilon} & \mathbb{Z}
\end{array}$$

kommutativ macht, vgl. [B, S. 22 u. S. 48]. Indem man die in der oberen Reihe stehende Sequenz F von links mit $\mathbb{Z}$ über $\mathbb{Z}[G]$ tensoriert, erhält man die Sequenz

zur Bestimmung der $H_p(G,\mathbb{Z})$, und entsprechend erhält man die Sequenz zur Bestimmung der $H_p(G\times G,\mathbb{Z})$, indem man die in der unteren Reihe stehende Sequenz $F\otimes F$ von links mit $\mathbb{Z}$ über $\mathbb{Z}[G\times G]$ tensoriert. Da die Sequenz $F\otimes F$ mittels ι_1, ι_2 und Δ auch eine Sequenz von G-Moduln ist, können die vertikalen Abbildungen τ_p ebenfalls von links über $\mathbb{Z}[G]$ mit der Identität von $\mathbb{Z}$ tensoriert werden. Dabei ist zu beachten, daß $\mathbb{Z}$ als G- wie als $(G\times G)$-Modul mit der trivialen Operation gedacht ist. Nach Tensorisation von links mit $\mathbb{Z}$ erhält man also das kommutative Diagramm

$$\begin{array}{ccccc}
\cdots & \xrightarrow{1\otimes N} & \mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G] & \xrightarrow{1\otimes(t-1)} & \mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G] \\
\downarrow & & \downarrow{\scriptstyle 1\otimes\tau_1} & & \downarrow{\scriptstyle 1\otimes\tau_0} \\
\cdots & \xrightarrow{1\otimes\mathcal{D}_2} & \mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\big(\bigoplus_{p+q=1}F_p\otimes F_q\big) & \xrightarrow{1\otimes\mathcal{D}_1} & \mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}(F_0\otimes F_0).
\end{array}$$

Die Abbildung $H_p(\iota_1,\mathbb{Z})$, $H_p(\iota_2,\mathbb{Z})$ bzw. $H_p(\Delta,\mathbb{Z})$ von $H_p(G,\mathbb{Z})$ nach $H_p(G\times G,\mathbb{Z})$ ist dann nichts anderes als die durch dieses Diagramm vermittelte Abbildung

$$H_p(1\otimes\tau): H_p(F_G)\to H_p\big((F\otimes F)_{G\times G}\big),$$

vgl. [B, S. 48].
Wir wollen als nächstes den Komplex $F\otimes F$ der Reihe nach mittels ι_1, ι_2 und Δ als Komplex von G-Moduln und -Homomorphismen auffassen und jeweils eine G-Kettenabbildung $\tau: F\to F\otimes F$ angeben, welche die Bestimmung der von ι_1, ι_2 bzw. Δ vermittelten Abbildung $H_3(G,\mathbb{Z})\to H_3(G\times G,\mathbb{Z})$ ermöglicht.

Die Kettenabbildung zu ι_1

Wir fassen als erstes $F\otimes F$ mittels ι_1 als Komplex von G-Moduln auf. Dann wird der $(G\times G)$-Modul $(F\otimes F)_m=\bigoplus_{p+q=m}F_p\otimes F_q$ durch die komponentenweise skalare Multiplikation

$$\begin{aligned}
G\times\big(F_p\otimes F_q\big)&\longrightarrow F_p\otimes F_q,\\
(g,\ x\otimes y)\quad&\longmapsto (gx)\otimes y
\end{aligned}$$

zum G-Modul, und es sei

$$\begin{aligned}
\tau_m\ :\ F_m\quad&\longrightarrow \big(F_m\otimes F_0\big)\oplus\big(F_{m-1}\otimes F_1\big)\oplus\cdots\oplus\big(F_0\otimes F_m\big),\\
1\quad&\longmapsto (1\otimes 1,\ 0,\ \ldots\ ,\ 0),\\
\sum_{g\in G}n_g g\quad&\longmapsto \sum_{g\in G}n_g g(1\otimes 1,\ 0,\ \ldots\ ,\ 0)\\
&=\sum_{g\in G}n_g(g\otimes 1,\ 0,\ \ldots\ ,\ 0)\\
&=\Big(\Big(\sum_{g\in G}n_g g\Big)\otimes 1,\ 0,\ \ldots\ ,\ 0\Big)
\end{aligned}$$

der G-Homomorphismus $F_m\to(F\otimes F)_m$, der $x\in F_m$ auf das Elemsent $x\otimes 1$ des direkten Summanden $F_m\otimes F_0$ von $(F\otimes F)_m$ abbildet. Es ist sofort zu erkennen, dass auf diese Weise ein G-Kettenabbildung $\tau: F\to F\otimes F$ definiert wird, denn für alle $m>0$ und $x\in F\otimes F$ gilt

$$\mathcal{D}_m\tau_m x=\mathcal{D}_m(x\otimes 1,0,\ldots,0)=\big((\partial_m x)\otimes 1,0,\ldots,0\big)=\tau_{m-1}\partial_m x.$$

Zuletzt ist noch zu überprüfen, dass $(\varepsilon \otimes \varepsilon)\tau_0 = \varepsilon$ gilt, d. h. die Verträglichkeit mit den Augmentationen. Tatsächlich ist $(\varepsilon \otimes \varepsilon)\tau_0$ gleich der Abbildung

$$\begin{array}{ccccc} F_0 & \longrightarrow & F_0 \otimes F_0 & \longrightarrow & \mathbb{Z}, \\ 1 & \longmapsto & 1 \otimes 1 & \longmapsto & 1, \\ \sum\limits_{g\in G} n_g g & \longmapsto & \sum\limits_{g\in G} n_g (g \otimes 1) & \longmapsto & \sum\limits_{g\in G} n_g, \end{array}$$

womit nachgewiesen ist, dass die wie oben definierte G-Kettenabbildung τ das Gewünschte leistet.

Die Kettenabbildung zu ι_2

Wenn wir jetzt $F \otimes F$ mittels ι_2 als Komplex von G-Moduln auffassen, so wird der $(G \times G)$-Modul $(F \otimes F)_m = \bigoplus_{p+q=m} F_p \otimes F_q$ durch die komponentenweise skalare Multiplikation

$$\begin{array}{c} G \times \big(F_p \otimes F_q\big) \longrightarrow F_p \otimes F_q, \\ (g,\ x \otimes y) \quad \longmapsto x \otimes (gy) \end{array}$$

zum G-Modul, und in diesem Fall sei

$$\begin{aligned} \tau_m \ :\ F_m \quad &\longrightarrow \big(F_m \otimes F_0\big) \oplus \big(F_{m-1} \otimes F_1\big) \oplus \cdots \oplus \big(F_0 \otimes F_m\big), \\ 1 \quad &\longmapsto (1 \otimes 1,\ 0,\ \ldots\ ,\ 0), \\ \sum_{g\in G} n_g g \quad &\longmapsto \sum_{g\in G} n_g g(1 \otimes 1,\ 0,\ \ldots\ ,\ 0) \\ &= \sum_{g\in G} n_g (1 \otimes g,\ 0,\ \ldots\ ,\ 0) \\ &= \Big(1 \otimes \Big(\sum_{g\in G} n_g g\Big),\ 0,\ \ldots\ ,\ 0\Big) \end{aligned}$$

der G-Homomorphismus $F_m \to (F \otimes F)_m$, der $x \in F_m$ auf das Elemsent $1 \otimes x$ des direkten Summanden $F_0 \otimes F_m$ von $(F \otimes F)_m$ abbildet. Es wird dann auf diese Weise ein G-Kettenkomplex $\tau : F \to F \otimes F$ definiert, denn für alle $m > 0$ und $x \in F \otimes F$ gilt

$$\mathcal{D}_m \tau_m x = \mathcal{D}_m(1 \otimes x, 0, \ldots, 0) = \big(1 \otimes (\partial_m x), 0, \ldots, 0\big) = \tau_{m-1}\partial_m x.$$

Auch hier bleibt die Verträglichkeit mit den Augmentationen zu überprüfen, d. h. daß $(\varepsilon \otimes \varepsilon)\tau_0 = \varepsilon$ gilt. Sie ist gegeben, denn $(\varepsilon \otimes \varepsilon)\tau_0$ ist gleich der Abbildung

$$\begin{array}{ccccc} F_0 & \longrightarrow & F_0 \otimes F_0 & \longrightarrow & \mathbb{Z}, \\ 1 & \longmapsto & 1 \otimes 1 & \longmapsto & 1, \\ \sum\limits_{g\in G} n_g g & \longmapsto & \sum\limits_{g\in G} n_g (1 \otimes g) & \longmapsto & \sum\limits_{g\in G} n_g, \end{array}$$

womit verifiziert ist, dass die zu ι_2 definierte G-Kettenabbildung τ das Gewünschte leistet.

Die Kettenabbildung zu Δ

Es sei schließlich $F \otimes F$ durch die diagonale Einbettung Δ ein Komplex von G-Moduln. In diesem Fall wird der $(G \times G)$-Modul $(F \otimes F)_m = \bigoplus_{p+q=m} F_p \otimes F_q$ durch die komponentenweise skalare Multiplikation

$$\begin{array}{c} G \times \big(F_p \otimes F_q\big) \longrightarrow F_p \otimes F_q, \\ (g,\ x \otimes y) \quad \longmapsto (gx) \otimes (gy) \end{array}$$

zum G-Modul, und wir definieren die G-Kettenabbildung τ wie folgt. Für ungerades m seien die Komponenten $\tau_{pq} : F_m \to F_p \otimes F_q$ von $\tau_m : F_m \to \bigoplus_{p+q=m} F_p \otimes F_q$ durch

$$\begin{aligned} F_m &\longrightarrow F_p \otimes F_q, \\ 1 &\longmapsto \begin{cases} 1 \otimes 1 & \text{falls } p \text{ gerade ist} \\ 1 \otimes t & \text{falls } p \text{ ungerade ist} \end{cases} \end{aligned}$$

gegeben und für gerades m durch

$$\begin{aligned} F_m &\longrightarrow F_p \otimes F_q, \\ 1 &\longmapsto \begin{cases} 1 \otimes 1 & \text{falls } p \text{ gerade ist} \\ \sum_{0 \le i < j \le m-1} t^i \otimes t^j & \text{falls } p \text{ ungerade ist,} \end{cases} \end{aligned}$$

vgl. [B, S. 108]. Wir wollen uns davon überzeugen, daß $\tau : F \to F \otimes F$ tatsächlich eine Kettenabbildung ist und desweiteren mit den Augmentationen verträglich, d.h. $(\varepsilon \otimes \varepsilon)\tau_0 = \varepsilon$. Um mit der Verträglichkeit mit den Augmentationen zu beginnen, $(\varepsilon \otimes \varepsilon)\tau_0$ ist der G-Homomorphismus

$$\begin{array}{ccccc} F_0 & \longrightarrow & F_0 \otimes F_0 & \longrightarrow & \mathbb{Z}, \\ 1 & \longmapsto & 1 \otimes 1 & \longmapsto & 1, \\ \sum\limits_{g \in G} n_g g & \longmapsto & \sum\limits_{g \in G} n_g (g \otimes g) & \longmapsto & \sum\limits_{g \in G} n_g, \end{array}$$

und stimmt also mit ε überein. Was die Behauptung betrifft, τ sei eine Kettenabbildung, so sind Fälle zu unterscheiden. Es geht darum, die Kommutativität des Diagramms

$$\begin{array}{ccc} F_m & \xrightarrow{\partial_m} & F_{m-1} \\ {\scriptstyle \tau_m}\downarrow & & \downarrow{\scriptstyle \tau_{m-1}} \\ \bigoplus_{p+q=m} F_p \otimes F_q & \xrightarrow{\mathcal{D}_m} & \bigoplus_{p+q=m-1} F_p \otimes F_q \end{array}$$

für alle $m > 0$ nachzuweisen, was anders gesagt heißt für alle p, q mit $p + q = m - 1$ die Kommutativität des Disgramms

$$\begin{array}{ccc} F_m & \xrightarrow{\partial_m} & F_{m-1} \\ {\scriptstyle \tau_m}\downarrow & & \downarrow{\scriptstyle \tau_{pq}} \\ \big(F_{p+1} \otimes F_q\big) \oplus \big(F_p \otimes F_{q+1}\big) & \xrightarrow{\mathcal{D}_m} & F_p \otimes F_q \end{array}$$

zu zeigen. Dabei ist mit $\tau_m : F_m \to (F_{p+1} \otimes F_q) \oplus (F_p \otimes F_{q+1})$ unter Missbrauch der Bezeichnung die Abbildung gemeint, die aus $\tau_m : F_m \to \bigoplus_{p+q=m} F_p \otimes F_q$ entsteht, wenn die Projektion auf $(F_{p+1} \otimes F_q) \oplus (F_p \otimes F_{q+1})$ hinterhergeschaltet wird, und ebenso ist $\mathcal{D}_m : (F_{p+1} \otimes F_q) \oplus (F_p \otimes F_{q+1}) \to F_p \otimes F_q$ die Abbildung, die aus $\mathcal{D}_m$ eingeschränkt auf $(F_{p+1} \otimes F_q) \oplus (F_p \otimes F_{q+1})$ entsteht, wenn anschließend auf $F_p \otimes F_q$ projiziert wird. Beginnen wir mit dem Fall, daß $p + q = m - 1$ gerade ist. Dann gilt

$$\begin{aligned} \tau_{pq}\partial_m 1 &= \tau_{pq}(t-1) = t \cdot \tau_{pq} 1 - \tau_{pq} 1 \\ &= \begin{cases} t \cdot (1 \otimes 1) - 1 \otimes 1 & \text{falls } p, q \text{ gerade} \\ t \cdot \Big(\sum_{0 \le i < j \le m-1} t^i \otimes t^j \Big) - \sum_{0 \le i < j \le m-1} t^i \otimes t^j & \text{falls } p, q \text{ ungerade} \end{cases} \\ &= \begin{cases} t \otimes t - 1 \otimes 1 & \text{falls } p, q \text{ gerade} \\ \sum_{0 \le i < j \le m-1} t^{i+1} \otimes t^{j+1} - \sum_{0 \le i < j \le m-1} t^i \otimes t^j & \text{falls } p, q \text{ ungerade} \end{cases} \end{aligned}$$

und Umformen des letzten Ausdruckes liefert

$$\sum_{0\le i<j\le m-1} t^{i+1}\otimes t^{j+1} - \sum_{0\le i<j\le m-1} t^i\otimes t^j = \sum_{1\le i<j\le m} t^i\otimes t^j - \sum_{0\le i<j\le m-1} t^i\otimes t^j$$
$$= \sum_{i=1}^{m-1} t^i\otimes 1 - \sum_{j=1}^{m-1} 1\otimes t^j = \sum_{i=0}^{m-1} t^i\otimes 1 - \sum_{j=0}^{m-1} 1\otimes t^j = N\otimes 1 - 1\otimes N;$$

zusammengefasst hat man also

$$\tau_{pq}\partial_m 1 = \begin{cases} t\otimes t - 1\otimes 1 & \text{falls } p,q \text{ gerade} \\ N\otimes t - 1\otimes N & \text{falls } p,q \text{ ungerade.} \end{cases}$$

Auf der anderen Seite gilt

$$F_m \xrightarrow{\tau_m} \big(F_{p+1}\otimes F_q\big)\oplus\big(F_p\otimes F_{q+1}\big),$$
$$1 \longmapsto \begin{cases} (1\otimes t,\ \ 1\otimes 1) & \text{falls } p,q \text{ gerade} \\ (1\otimes 1,\ \ 1\otimes t) & \text{falls } p,q \text{ ungerade} \end{cases}$$

und Hinterherschalten von $\mathcal{D}_m$ ergibt

$$\mathcal{D}_m\tau_m : F_m \longrightarrow F_p\otimes F_q,$$
$$1 \longmapsto \begin{cases} (t-1)\otimes t + 1\otimes(t-1) & \text{falls } p,q \text{ gerade} \\ N\otimes t - 1\otimes N & \text{falls } p,q \text{ ungerade} \end{cases}$$
$$= \begin{cases} t\otimes t - 1\otimes t + 1\otimes t - 1\otimes 1 & \text{falls } p,q \text{ gerade} \\ N\otimes t - 1\otimes N & \text{falls } p,q \text{ ungerade;} \end{cases}$$

demnach stimmt die Verknüpfung $\mathcal{D}_m\tau_m : F_m \to F_p\otimes F_q$ mit $\tau_{pq}\partial_m$ überein, was zu zeigen war. Sei nun die Summe $p+q = m-1$ ungerade. In diesem Fall ist

$$\tau_{pq}\partial_m 1 = \tau_{pq}N = \sum_{i=0}^{m-1} t^i\cdot\tau_{pq}1$$
$$= \begin{cases} \sum_{i=0}^{m-1} t^i\cdot(1\otimes 1) & \text{falls } p \text{ gerade, } q \text{ ungerade} \\ \sum_{i=0}^{m-1} t^i\cdot(1\otimes t) & \text{falls } p \text{ ungerade, } q \text{ gerade} \end{cases}$$
$$= \begin{cases} \sum_{i=0}^{m-1} t^i\otimes t^i & \text{falls } p \text{ gerade, } q \text{ ungerade} \\ \sum_{i=0}^{m-1} t^i\otimes t^{i+1} & \text{falls } p \text{ ungerade, } q \text{ gerade;} \end{cases}$$

andererseits gilt

$$F_m \xrightarrow{\tau_m} \big(F_{p+1}\otimes F_q\big)\oplus\big(F_p\otimes F_{q+1}\big),$$
$$1 \longmapsto \begin{cases} \big(\sum_{0\le i<j\le m-1} t^i\otimes t^j,\ \ 1\otimes 1\big) & \text{falls } p \text{ gerade, } q \text{ ungerade} \\ \big(1\otimes 1,\ \ \sum_{0\le i<j\le m-1} t^i\otimes t^j\big) & \text{falls } p \text{ ungerade, } q \text{ gerade} \end{cases}$$

und Hinterherschalten von $\mathcal{D}_m$ liefert

$$\begin{aligned}
F_m \longrightarrow & F_p \otimes F_q, \\
1 \longmapsto & \begin{cases} \sum_{0\le i<j\le m-1} t^i(t-1)\otimes t^j + 1\otimes N & \text{falls } p \text{ gerade, } q \text{ ungerade} \\ N\otimes 1 - \sum_{0\le i<j\le m-1} t^i \otimes t^j(t-1) & \text{falls } p \text{ ungerade, } q \text{ gerade} \end{cases} \\
= & \begin{cases} \sum_{0\le i<j\le m-1} t^{i+1}\otimes t^j - \sum_{0\le i<j\le m-1} t^i\otimes t^j + 1\otimes N & \text{falls } p \text{ gerade} \\ N\otimes 1 - \sum_{0\le i<j\le m-1} t^i\otimes t^{j+1} + \sum_{0\le i<j\le m-1} t^i\otimes t^j & \text{falls } p \text{ ungerade} \end{cases} \\
= & \begin{cases} \sum_{0<i\le j\le m-1} t^i\otimes t^j - \sum_{0\le i<j\le m-1} t^i\otimes t^j + \sum_{0\le j\le m-1} 1\otimes t^j \\ \sum_{0\le i\le m-1} t^i\otimes 1 - \sum_{0\le i<j\le m-1} t^i\otimes t^{j+1} + \sum_{0\le i\le j<m-1} t^i\otimes t^{j+1} \end{cases} \\
= & \begin{cases} \sum_{1\le i\le m-1} t^i\otimes t^i - \sum_{1\le j\le m-1} 1\otimes t^j + \sum_{0\le j\le m-1} 1\otimes t^j \\ \sum_{0\le i\le m-1} t^i\otimes 1 - \sum_{0\le i\le m-2} t^i\otimes 1 + \sum_{0\le i\le m-2} t^i\otimes t^{i+1} \end{cases} \\
= & \begin{cases} \sum_{i=0}^{m-1} t^i\otimes t^i \\ \sum_{i=0}^{m-1} t^i\otimes t^{i+1}, \end{cases}
\end{aligned}$$

so dass $\mathcal{D}_m\tau_m : F_m \to F_p\otimes F_q$ und $\tau_{pq}\partial_m$ wie behauptet übereinstimmen. Damit ist gezeigt, daß für alle $m>0$ die Abbildung $\mathcal{D}_m\tau_m : F_m \to \bigoplus_{p+q=m-1} F_p\otimes F_q$ gleich $\tau_{m-1}\partial_m$ ist, d. h. τ ist eine Kettenabbildung.

Die mit $\mathbb{Z}$ tensorierten Kettenabbildungen

Unser Ziel ist es, für eine zyklische Gruppe G der Ordnung n die von den Inklusionen $\iota_1, \iota_2 : G \to G\times G$ und von der diagonalen Einbettung $\Delta : G\to G\times G$ vermittelten Inklusionen $H_3(G,\mathbb{Z}) \to H_3(G\times G,\mathbb{Z})$ genauer zu beschreiben. Dazu betrachten wir die projektiven Auflösungen $\varepsilon : F\to\mathbb{Z}$ und $\varepsilon\otimes\varepsilon : F\otimes F\to\mathbb{Z}$ von $\mathbb{Z}$ über $\mathbb{Z}[G]$ bzw. über $\mathbb{Z}[G\times G]$, wobei F der Komplex

$$\cdots \xrightarrow{t-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{t-1} \mathbb{Z}[G]$$

mit der Norm $N = 1+t+\cdots+t^{n-1}$ ist und $F\otimes F$ der Komplex

$$\cdots \xrightarrow{\mathcal{D}_3} \bigoplus_{p+q=2} F_p\otimes F_q \xrightarrow{\mathcal{D}_2} \bigoplus_{p+q=1} F_p\otimes F_q \xrightarrow{\mathcal{D}_1} F_0\otimes F_0.$$

Mittels der Inklusionen ι_1, ι_2 und Δ wird $F\otimes F$ auf drei verschiedene Arten zu einem Komplex von G-Moduln, denn ist $\varphi : G\to G\times G$ ein Homomorphismus, so wird für $g\in G$ und $x\in (F\otimes F)_m = \bigoplus_{p+q=m} F_p\otimes F_q$

$$g\cdot x = \varphi(g)\cdot x$$

gesetzt. Weil alle F_i projektive $\mathbb{Z}[G]$-Moduln sind und der Komplex $F\otimes F$ azyklisch ist, gibt es G-Kettenabbildungen $\tau : F\to F\otimes F$, die mit den Augmentationen ε und $\varepsilon\otimes\varepsilon$ verträglich sind. Für die Homomorphismen ι_1, ι_2 und Δ haben wir derartige Kettenabbildungen explizit angegeben. Um ausgehend von diesen Kettenabbildungen die Abbildungen $H_3(G,\mathbb{Z}) \to H_3(G\times G,\mathbb{Z})$ zu bestimmen, betrachten wir jeweils das kommutative Diagramm

$$\begin{array}{ccccc}
\mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{t-1} & \mathbb{Z}[G] \\
\downarrow{\scriptstyle \tau_4} & & \downarrow{\scriptstyle \tau_3} & & \downarrow{\scriptstyle \tau_2} \\
\bigoplus_{p+q=4} F_p\otimes F_q & \xrightarrow{\mathcal{D}_4} & \bigoplus_{p+q=3} F_p\otimes F_q & \xrightarrow{\mathcal{D}_3} & \bigoplus_{p+q=3} F_p\otimes F_q
\end{array}$$

und tensorieren von links mit $\mathbb{Z}$, und zwar in der oberen Reihe über $\mathbb{Z}[G]$, in der unteren über $\mathbb{Z}[G\times G]$, während alle im Diagramm vorkommenden Abbildungen von links mit der Identität von $\mathbb{Z}$ tensoriert werden. Wegen der Isomorphien

$$\mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G]\simeq\mathbb{Z}$$

$$\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(\bigoplus_{p+q=m}F_p\otimes F_q\right)\simeq\bigoplus_{p+q=m}\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_p\otimes F_q\right)\simeq\mathbb{Z}^{m+1}$$

und der in $\mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G]$ gültigen Gleichungen

$$1\otimes N=\sum_{g\in G}1\otimes g=\sum_{g\in G}1\otimes 1=n\otimes 1$$
$$1\otimes(t-1)=1\otimes t-1\otimes 1=1\otimes 1-1\otimes 1=0$$

erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccc}\mathbb{Z} & \xrightarrow{\ n\ } & \mathbb{Z} & \xrightarrow{\ 0\ } & \mathbb{Z}\\ \downarrow & & \downarrow & & \downarrow\\ \mathbb{Z}^5 & \longrightarrow & \mathbb{Z}^4 & \longrightarrow & \mathbb{Z}^3.\end{array}$$

Das Bild des erzeugenden Elements $1\otimes 1$ von $\mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G]\simeq\mathbb{Z}$ unter $1\otimes\tau_m$ ist für jedes m

$$1\otimes\tau_m(1)\ \in\ \mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(\bigoplus_{p+q=m}F_p\otimes F_q\right),$$

welchem ein Element aus $\bigoplus_{p+q=m}\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_p\otimes F_q\right)$ entspricht, das aus

$$\tau_m(1)\in\bigoplus_{p+q=m}F_p\otimes F_q$$

entsteht, indem jede direkte Komponente von links mit 1 tensoriert wird. Da wir $\tau_m(1)$ explizit angeben können, erhalten wir auf diese Weise sofort das Bild von $1\otimes 1$ unter der durch τ_m vermittelten Abbildung

$$1\otimes\tau_m:\mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G]\to\bigoplus_{p+q=m}\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_p\otimes F_q\right)$$

und damit auch das Bild der 1 unter der Abbildung $\mathbb{Z}\to\mathbb{Z}^{m+1}$. Wir wollen jetzt konkret die zu ι_1, ι_2 und Δ gehörigen Abbildungen τ_3 ansehen. Es handelt sich um die G-Homomorphismen

$$\begin{aligned}F_3&\longrightarrow\left(F_0\otimes F_3\right)\oplus\left(F_1\otimes F_2\right)\oplus\left(F_2\otimes F_1\right)\oplus\left(F_3\otimes F_0\right),\\ 1&\longmapsto(0,\ 0,\ 0,\ 1\otimes 1)\quad(\text{zu }\iota_1)\\ 1&\longmapsto(1\otimes 1,\ 0,\ 0,\ 0)\quad(\text{zu }\iota_2)\\ 1&\longmapsto(1\otimes 1,\ 1\otimes t,\ 1\otimes 1,\ 1\otimes t)\quad(\text{zu }\Delta),\end{aligned}$$

so dass Tensorisation mit der Identität von $\mathbb{Z}$ die Gruppenhomomorphismen

$$\begin{aligned}\mathbb{Z}\otimes_{\mathbb{Z}[G]}F_3\longrightarrow&\Big(\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_0\otimes F_3\right)\Big)\oplus\Big(\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_1\otimes F_2\right)\Big)\\ &\oplus\Big(\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_2\otimes F_1\right)\Big)\oplus\Big(\mathbb{Z}\otimes_{\mathbb{Z}[G\times G]}\left(F_3\otimes F_0\right)\Big),\\ 1\otimes 1\ &\longmapsto(0,\ 0,\ 0,\ 1\otimes(1\otimes 1))\quad(\text{zu }\iota_1)\\ 1\otimes 1\ &\longmapsto(1\otimes(1\otimes 1),\ 0,\ 0,\ 0)\quad(\text{zu }\iota_2)\\ 1\otimes 1\ &\longmapsto(1\otimes(1\otimes 1),\ 1\otimes(1\otimes t),\ 1\otimes(1\otimes 1),\ 1\otimes(1\otimes t))\quad(\text{zu }\Delta)\end{aligned}$$

liefert, wobei

$$1 \otimes (1 \otimes t) = 1 \otimes ((1,\, t) \cdot (1 \otimes 1)) = (1 \cdot (1,\, t)) \otimes (1 \otimes 1) = 1 \otimes (1 \otimes 1)$$

das erzeugende Element von $\mathbb{Z} \otimes_{\mathbb{Z}[G\times G]} \big(\mathbb{Z}[G] \otimes \mathbb{Z}[G]\big) \simeq \mathbb{Z}$ ist. Man erhält also die Homomorphismen

$$\begin{aligned} &\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}, \\ &1 \longmapsto (0,\ 0,\ 0,\ 1) \quad (\text{zu } \iota_1) \\ &1 \longmapsto (1,\ 0,\ 0,\ 0) \quad (\text{zu } \iota_2) \\ &1 \longmapsto (1,\ 1,\ 1,\ 1) \quad (\text{zu } \Delta) \end{aligned}$$

als mittlere vertikale Abbildungen in den Diagrammen

$$\begin{array}{ccccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ {\scriptstyle \text{von } \tau_4}\big\downarrow & & {\scriptstyle \text{von } \tau_3}\big\downarrow & & {\scriptstyle \text{von } \tau_2}\big\downarrow \\ \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} & \xrightarrow[d_4]{} & \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} & \xrightarrow[d_3]{} & \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}. \end{array}$$

Bestimmung der Bilder von $H_3(G,\mathbb{Z})$ in $H_3(G\times G,\mathbb{Z})$

Wie wir bereits gezeigt haben, sind Kern bzw. Bild der von den Randabbildungen $\mathcal{D}_3$ und $\mathcal{D}_4$ vermittelten Homomorphismen d_3 und d_4 durch

$$\begin{aligned} \ker d_3 &= <(1,\ 0,\ 0,\ 0),\ (0,\ 1,\ 1,\ 0),\ (0,\ 0,\ 0,\ 1)> \\ \text{im } d_4 &= <(n,\ 0,\ 0,\ 0),\ (0,\ n,\ n,\ 0),\ (0,\ 0,\ 0,\ n)> \end{aligned}$$

gegeben, deren Quotient die Gruppe $H_3(G\times G,\mathbb{Z})$ liefert. Offenbar gilt auch

$$\begin{aligned} \ker d_3 &= <(1,\ 0,\ 0,\ 0),\ (1,\ 1,\ 1,\ 1),\ (0,\ 0,\ 0,\ 1)> \\ \text{im } d_4 &= <(n,\ 0,\ 0,\ 0),\ (n,\ n,\ n,\ n),\ (0,\ 0,\ 0,\ n)>, \end{aligned}$$

woraus sich die Isomorphien

$$H_3(G\times G,\mathbb{Z}) \simeq \frac{\mathbb{Z}(1,\ 0,\ 0,\ 0) + \mathbb{Z}(1,\ 1,\ 1,\ 1) + \mathbb{Z}(0,\ 0,\ 0,\ 1)}{\mathbb{Z}(n,\ 0,\ 0,\ 0) + \mathbb{Z}(n,\ n,\ n,\ n) + \mathbb{Z}(0,\ 0,\ 0,\ n)} \simeq (\mathbb{Z}/n)^3$$

ergeben. Die Bilder der von ι_1, ι_2 und Δ vermittelten Abbildungen

$$(\iota_1)_*,\ \ (\iota_2)_*,\ \ \Delta_* : H_3(G,\mathbb{Z}) \to H_3(G\times G,\mathbb{Z})$$

entsprechen hierbei den von $(1,\ 0,\ 0,\ 0)$, $(0,\ 0,\ 0,\ 1)$ und $(1,\ 1,\ 1,\ 1)$ erzeugten Restklassen, wie die Betrachtung der vertikalen Abbildungen $\mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ zu den τ_3 ergab, und daraus folgt schließlich

$$H_3(G\times G,\mathbb{Z}) = (\iota_1)_*\big(H_3(G,\mathbb{Z})\big) \ \oplus\ (\iota_2)_*\big(H_3(G,\mathbb{Z})\big) \ \oplus\ \Delta_*\big(H_3(G,\mathbb{Z})\big).$$

Jeder der drei direkten Summanden ist wie auch $H_3(G,\mathbb{Z})$ isomorph zu $\mathbb{Z}/n$.

4. Explizite Berechnung von $H^{-1}(G, K^\times)$ für biquadratische Erweiterungen von $\mathbb{Q}$

Gegeben sei eine biquadratische Erweiterung $K/\mathbb{Q}$ mit der Galoisgruppe G, und zwar sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ mit quadratfreien $a, b \in \mathbb{Z}$. Wie in Kapitel 3 gezeigt wurde, hängt der Isomorphietyp von $H^{-1}(G, K^\times)$ von den lokalen Galoisgruppen $G_\mathfrak{p}$ ab. Gibt es Stellen $\mathfrak{p}$ von $\mathbb{Q}$ mit $G_\mathfrak{p} = G$, so genügt es, deren Anzahl zu kennen. In jedem Fall soll gezeigt werden, dass jede der zweielementigen Untergruppen von G für ein geeignetes $\mathfrak{p}$ gleich der lokalen Galoisgruppe $G_\mathfrak{p}$ ist.

4.i Komplettierungen und lokale Galoisgruppen

In diesem Abschnitt werden wir den Begriff der Zerlegungsgruppe und der lokalen Galoisgruppe behandeln. Sei K/k eine galoissche Erweiterung algebraischer Zahlkörper mit der Galoisgruppe G; desweiteren sei $\mathfrak{p}$ eine endliche Stelle von k. Für jede Stelle $\mathfrak{P}$ von K, die über $\mathfrak{p}$ liegt, heißt

$$G_\mathfrak{P} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

die Zerlegungsgruppe von $\mathfrak{P}$ in Bezug auf die Erweiterung K/k. Sie hängt bei abelscher Gruppe G nicht von der Wahl der über $\mathfrak{p}$ liegenden Stelle $\mathfrak{P}$ von K ab und wird dann auch mit $G_\mathfrak{p}$ bezeichnet. Allgemein gilt nämlich für jedes $\sigma \in G$ die Gleichung

$$G_{\sigma\mathfrak{P}} = \sigma(G_\mathfrak{P})\sigma^{-1},$$

und die Galoisgruppe G operiert transitiv auf der Menge über $\mathfrak{p}$ liegenden Stellen von K (vgl. [N, S. 56-57]).

Sei nun $K_\mathfrak{P}$ eine Komplettierung von K bzgl. der Stelle $\mathfrak{P}$ und $k_\mathfrak{p}$ eine Komplettierung von k bzgl. der Stelle $\mathfrak{p}$. Bezeichnet weiter $k_\mathfrak{P}$ die in $K_\mathfrak{P}$ enthaltene Komplettierung von k bzgl. $\mathfrak{p}$, so besteht ein kanonischer Isomorphismus von $k_\mathfrak{p}$ nach $k_\mathfrak{P}$. Deshalb ist es sinnvoll, von der Erweiterung $K_\mathfrak{P}/k_\mathfrak{p}$ zu sprechen. Jedes $\sigma \in G_\mathfrak{P}$ kann als betragserhaltender k-Homomorphismus von K nach $K_\mathfrak{P}$ augefasst werden ([AZ, S. 103]) und besitzt somit eine eindeutige Fortsetzung zu einem Endomorphismus von $K_\mathfrak{P}$, der $k_\mathfrak{p}$ elementweise festhält ([A2, S .65]). Aufgrund der Eindeutigkeit sind diese Fortsetzungen ebenfalls Automorphismen, so dass man einen natürlichen Homomorphismus von $G_\mathfrak{P}$ nach $G(K_\mathfrak{P}/k_\mathfrak{p})$ erhält. Dieser ist sogar ein Isomorphismus, weil man umgekehrt jedem Element von $G(K_\mathfrak{P}/k_\mathfrak{p})$ seine Einschränkung auf K zuordnen kann und einen betragserhaltenden k-Automorphismus von K erhält (da die Erweiterung K/k normal ist). Ein betragserhaltender Automorphismus aus G ist aber offensichtlich ein Element von $G_\mathfrak{P}$. Die Gruppen $G_\mathfrak{P}$ und $G(K_\mathfrak{P}/k_\mathfrak{p})$ werden wegen ihrer natürlichen Isomorphie meist identifiziert. Im übrigen gilt $K_\mathfrak{P} = Kk_\mathfrak{p}$, was aufgrund des Translationssatzes der Galoistheorie die Gleichung $G_\mathfrak{P} = G(K/K\cap k_\mathfrak{p})$ zur Folge hat, so dass man insgesamt

$$G_{\mathfrak{P}} = G(K/K \cap k_{\mathfrak{p}}) = G(K_{\mathfrak{P}}/k_{\mathfrak{p}})$$

erhält, vgl. [AZ, S. 105].

Die Zerlegungsgruppe $G_{\mathfrak{P}}$ der über $\mathfrak{p}$ liegenden Stelle $\mathfrak{P}$ von K hat mit dem Zerlegungsverhalten von $\mathfrak{p}$ in K zu tun. Die Anzahl $g_{\mathfrak{p}}$ der über $\mathfrak{p}$ liegenden Stellen von K ist gleich dem Index von $G_{\mathfrak{P}}$ in G. Ist

$$\mathfrak{p} = (\mathfrak{P}_1 \dots \mathfrak{P}_{g_{\mathfrak{p}}})^{e_{\mathfrak{p}}}$$

die Zerlegung von $\mathfrak{p}$ in K, mit $e_{\mathfrak{p}}$ als dem gemeinsamen Verzweigungsindex der $\mathfrak{P}_i$ über $\mathfrak{p}$, so besteht mit dem Grad $n = K : k$ der Erweiterung K/k und mit dem gemeinsamen Restklassengrad $f_{\mathfrak{p}}$ der $\mathfrak{P}_i$ folgender Zusammenhang ([AZ, S. 70/71]):

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}.$$

Als letztes sei noch erwähnt, dass für einen biquadratischen Erweiterungskörper $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ von $\mathbb{Q}$ und jede Primzahl p der Körper $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})$ eine Komplettierung von K bzgl. einer der über p liegenden Stellen von K ist. Für jede Primzahl p ist die Gruppe G_p also gerade die Galoisgruppe der Erweiterung $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$, welche sich ohne Schwierigkeiten bestimmen lässt.

4.ii Quadratische Erweiterungen

Als nächstes sollen nun einige Ergebnisse über quadratische Erweiterungen $\mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$ angegeben werden, die über den Zerlegungstyp jeder endlichen Stelle p von $\mathbb{Q}$ Aufschluss geben. In dieser speziellen Situation ist eine der Zahlen $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ und $g_{\mathfrak{p}}$ gleich 2, während die restlichen den Wert 1 annehmen. Für eine Primzahl p sind in $L = \mathbb{Q}(\sqrt{d})$ demnach drei verschiedene Zerlegungstypen möglich:

p verzweigt: $\quad e_p = 2, \quad (p) = \mathfrak{P}^2, \quad G_p = G;$
p träge: $\quad f_p = 2, \quad (p) = \mathfrak{P}, \quad G_p = G;$
p voll zerlegt: $\quad g_p = 2, \quad (p) = \mathfrak{P}_1\mathfrak{P}_2, \quad \mathfrak{P}_1 \neq \mathfrak{P}_2, \quad G_p = 1.$

Die Diskriminante d_L von L ist gegeben durch $d_L = d$ falls $d \equiv 1(4)$, und $d_L = 4d$ sonst ([AZ, S. 50]). Ihre Primteiler sind gerade diejenigen Primzahlen, die in L verzweigt sind.

Für alle Primzahlen $p \neq 2$ gelten die folgenden Äquivalenzen ([AZ, S. 113]):

p verzweigt in $L \quad \Leftrightarrow \quad p \mid d$
p träge in $L \quad \Leftrightarrow \quad p \nmid d$ und $\left(\frac{d}{p}\right) = -1$
p voll zerlegt in $L \quad \Leftrightarrow \quad p \nmid d$ und $\left(\frac{d}{p}\right) = 1$

Im Falle $p = 2$ gilt hingegen

2 verzweigt in $L \Leftrightarrow d \not\equiv 1, 5\ (8)$
2 träge in $L \Leftrightarrow d \equiv 5\ (8)$
2 voll zerlegt in $L \Leftrightarrow d \equiv 1\ (8)$

Mit Hilfe dieser Resultate kann die Frage beantwortet werden, ob d für eine gegebene Primzahl p ein Quadrat in $\mathbb{Q}_p$ ist, oder anders ausgedrückt ermöglichen sie es, den Grad n_p der lokalen Erweiterung $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ anzugeben. Weil sich Restklassengrad und Verzweigungsindex bei Übergang zu den Kompletttierungen nicht ändern ([A2, S. 90]), und weil darüber hinaus $\mathbb{Q}_p$ und $\mathbb{Q}_p(\sqrt{d})$ lokale Körper sind ([A2, S. 114/115]), genügt der lokale Grad n_p der Gleichung $n_p = e_p f_p$ ([A2, S. 94]). Die Werte von e_p und f_p sind jedoch durch den Zerlegungstyp von p festgelegt; genau dann ist der lokale Grad n_p gleich 1, wenn Verzweigungsindex e_p und Trägheitsgrad f_p beide den Wert 1 annehmen. Die lokale Erweiterung $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$ ist demnach nur für in $L = \mathbb{Q}(\sqrt{d})$ voll zerlegtes p trivial.

4.iii Biquadratische Erweiterungen

Nachdem der Fall quadratischer Erweiterungen $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ geklärt ist, kann auch der lokale Grad der biquadratischen Erweiterung $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ für eine beliebige Primzahl p ermittelt werden, indem der Zerlegungstyp von p in $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ und $\mathbb{Q}(\sqrt{ab})$ unter Anwendung der oben genannten Resultate bestimmt wird (eventuell müssen für $p \neq 2$ einige der Legendre-Symbole $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$ und $\left(\frac{ab}{p}\right)$ unter Anwendung des quadratischen Reziprozitätsgesetzes und der beiden Zusätze ausgewertet werden). Für jede Primzahl p ist der Grad n_p der Erweiterung $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$ gleich 1, 2 oder 4.

Genau dann ist $n_p = 1$, wenn sowohl $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ als auch $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ den Grad 1 haben, d. h. wenn p in $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist.

Genau dann ist $n_p = 4$, wenn der Grad von $\mathbb{Q}_p(\sqrt{a})$ und von $\mathbb{Q}_p(\sqrt{b})$ über $\mathbb{Q}_p$ jeweils gleich 2 ist und außerdem $\mathbb{Q}_p(\sqrt{a}) \neq \mathbb{Q}_p(\sqrt{b})$ gilt; letztere Bedingung ist äquivalent dazu, dass a und b sich nicht um ein Quadrat in $\mathbb{Q}_p$ unterscheiden ([A1, S. 281]). Anders ausgedrückt ist n_p genau dann gleich 4, wenn die Erweiterungen $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$ jeweils den Grad 2 über $\mathbb{Q}_p$ haben, bzw. wenn p in keinem der Körper $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$ voll zerlegt ist.

Wenn der Grad von $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$ hingegen gleich 2 ist, so können drei Fälle unterschieden werden, je nachdem ob $\sqrt{a}$, $\sqrt{b}$ oder $\sqrt{ab}$ in $\mathbb{Q}_p$ liegt. Diese drei Fälle schließen sich gegenseitig aus, denn nur einer der Körper $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$ hat den Grad 1 über $\mathbb{Q}_p$ (weil $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})$ das Kompositum von zwei beliebigen unter den drei Körpern ist). Betrachtet man statt der lokalen Galoisgruppe $G(\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p)$ zu $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ die Zerlegungsgruppe $G(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{a}, \sqrt{b}) \cap \mathbb{Q}_p)$ von p, so ist G_p durch den zugehörigen

Fixkörper $F = \mathbb{Q}(\sqrt{a}, \sqrt{b}) \cap \mathbb{Q}_p$ in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ gekennzeichnet. Wenn der lokale Grad n_p gleich 2 ist, hat F den Grad 2 über $\mathbb{Q}$. Genauer ist $F = \mathbb{Q}(\sqrt{d})$ mit dem eindeutigen $d \in \{a, b, ab\}$, so dass $\sqrt{d}$ in $\mathbb{Q}_p$ liegt.

Die Zerlegungsgruppe G_p lässt sich nun für jede Primzahl p bestimmen. Nur wenn p in $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ verzweigt ist (d. h. wenn der gemeinsame Verzweigungsindex der über p liegenden Stellen von $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ nicht 1 ist), kann dabei $G_p = G$ herauskommen: für unverzweigtes p ist die lokale Erweiterung $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$ zyklisch, da sich der Verzweigungsindex bei Übergang zu den Komplettierungen nicht ändert und unverzweigte Erweiterungen lokaler Körper zyklisch sind ([A2, S. 97]).
Auch an der Stelle $\mathfrak{p} = \infty$ ist die lokale Galoisgruppe $G_\mathfrak{p}$ zyklisch, denn die Komplettierung von $\mathbb{Q}$ bzgl. $|\ |_\infty$ ist $\mathbb{R}$, und die Komplettierung von $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ bzgl. einer Fortsetzung von $|\ |_\infty$ ist ebenfalls $\mathbb{R}$, wenn $\sqrt{a}, \sqrt{b} \in \mathbb{R}$, und ansonsten $\mathbb{C}$. Um die Anzahl der Stellen $\mathfrak{p}$ mit $G_\mathfrak{p} = G$ herauszufinden, braucht man deshalb nur die endlichen Stellen p zu betrachten, für die p in einem der Körper $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ verzweigt ist. Es handelt sich um endlich viele Stellen, nämlich um die zu den Primteilern der Diskriminanten von $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$. Zusammen mit Abschnitt 4.ii ergibt sich nun

4.1 Satz. *Es sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ eine biquadratische Erweiterung von $\mathbb{Q}$, mit quadratfreien $a, b \in \mathbb{Z}$.*

Für eine Primzahl p gilt $G_p = G$ genau in den Fällen

i) $p \neq 2$, $p \mid a$, $p \nmid b$, $\left(\frac{b}{p}\right) = -1$
(p verzweigt in $\mathbb{Q}_p(\sqrt{a})$ und $\mathbb{Q}_p(\sqrt{ab})$, p träge in $\mathbb{Q}_p(\sqrt{b})$);

ii) $p \neq 2$, $p \nmid a$, $p \mid b$, $\left(\frac{a}{p}\right) = -1$
(p verzweigt in $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$, p träge in $\mathbb{Q}_p(\sqrt{a})$);

iii) $p \neq 2$, $p \mid a$, $p \mid b$, $\left(\frac{ab/p^2}{p}\right) = -1$
(p verzweigt in $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und p träge in $\mathbb{Q}_p(\sqrt{ab})$);

iv) $p = 2$, $a, b, (ab)_0 \not\equiv 1\ (8)$
(2 nicht voll zerlegt in $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$).
Hierbei bezeichnet $(ab)_0$ den quadratfreien Kern von ab.

Es ist $G_p = 1$ genau in den Fällen

i) $p \neq 2$, $p \nmid a$, $p \nmid b$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$
(p voll zerlegt in $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$);

ii) $p = 2$, $a, b \equiv 1\ (8)$
(2 voll zerlegt in $\mathbb{Q}_p(\sqrt{a})$, $\mathbb{Q}_p(\sqrt{b})$ und $\mathbb{Q}_p(\sqrt{ab})$).

4.2 Beispiel. (vgl. auch Abschnitte 4.x und 4.xi)

a) Es sei $a = 2$ und $b = p_1 \dots p_m$, mit paarweise verschiedenen Primzahlen $p_i \equiv 3\ (8)$. Dann ist $\left(\frac{a}{p_i}\right) = -1$, und nach Satz 4.1 gilt $G_p = G$ genau für die Primzahlen $p_1, \dots, p_m$, falls m gerade ist, und zusätzlich für die Primzahl 2, falls m ungerade ist. Nach Theorem 3.1 ist $H^{-1}(G, K^\times)$ gleich $(\mathbb{Z}/2)^{m-1}$ (m gerade) bzw. gleich $(\mathbb{Z}/2)^m$ (m ungerade).

b) Es sei $a = -1$ und $b = p_1 \dots p_m$, mit paarweise verschiedenen Primzahlen $p_i \equiv -1\ (8)$. Wieder ist $\left(\frac{a}{p_i}\right) = -1$, und in jedem Fall gilt nun $G_p = G$ genau für die n Primzahlen $p_1, \dots, p_m$. Nach Theorem 3.1 gilt $H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m-1}$.

c) Für $a = 2$, $b = 17$ sowie $a = -1$, $b = 17$ gilt $G_p \neq G$ für alle Primzahlen p.

4.iv Realisierung der Untergruppen der Galoisgruppe als Zerlegungsgruppen

Es soll der folgende Satz gezeigt werden.

4.3 Satz. *Es sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ eine biquadratische Erweiterung von $\mathbb{Q}$, mit quadratfreien $a, b \in \mathbb{Z}$ und Galoisgruppe $G = (\mathbb{Z}/2)^2$. Dann ist jede der drei zweielementigen Untergruppen von G für unendlich viele Primzahlen p gleich der Zerlegungsgruppe G_p.*

Für jede Stelle p von $\mathbb{Q}$ und jede über p liegende Stelle $\mathfrak{p}$ von $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ wird, wie bereits gesagt, die Zerlegungsgruppe $G_p = G_\mathfrak{p}$ mit der lokalen Galoisgruppe $G(K_\mathfrak{p}/\mathbb{Q}_p)$ identifiziert, womit also

$$G_p = G_\mathfrak{p} = G(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{a}, \sqrt{b}) \cap \mathbb{Q}_p) = G(\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p)$$

gilt. Die Gruppe G_p hat genau dann die Ordnung 2, wenn ihr Index in G gleich 2 ist; nach dem Hauptsatz der Galoistheorie ist dies äquivalent dazu, dass ihr Fixkörper $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \cap \mathbb{Q}_p$ den Grad 2 über $\mathbb{Q}$ hat. Demnach ist G_p genau dann gleich einer der zweielementigen Untergruppen von G, wenn nur eine der Wurzeln $\sqrt{a}$, $\sqrt{b}$, $\sqrt{ab}$ in $\mathbb{Q}_p$ liegt, und das heißt auf den Zerlegungstyp von p bezogen, dass p in genau einem der Körper $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ und $\mathbb{Q}(\sqrt{ab})$ voll zerlegt ist. Für $p \neq 2$ ist Letzteres schließlich gleichbedeutend damit, dass genau eines der Legendre-Symbole $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$ und $\left(\frac{ab}{p}\right)$ den Wert 1 annimmt. Wir setzen ab jetzt stets $p \neq 2$ voraus. Folgende drei Fälle können bei zweielementigem G_p auftreten:

1. Es gilt $\left(\frac{a}{p}\right) = 1$ und $\left(\frac{b}{p}\right) = -1$. Dann ist auch $\left(\frac{ab}{p}\right) = -1$, folglich liegt nur $\sqrt{a}$ in $\mathbb{Q}_p$. Identifiziert man wie gewöhnlich Zerlegungsgruppe und lokale Galoisgruppe an der Stelle p, so hat man

$$G_p = G(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{a})) = G(\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p) = G(\mathbb{Q}_p(\sqrt{ab})/\mathbb{Q}_p).$$

2. Es gilt $\left(\frac{a}{p}\right) = -1$ und $\left(\frac{b}{p}\right) = 1$. Daraus folgt weiter $\left(\frac{ab}{p}\right) = -1$, so dass nur $\sqrt{b}$ in $\mathbb{Q}_p$ enthalten ist. Für die Gruppe G_p gelten dann die Gleichungen

$$G_p = G(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{b})) = G(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p) = G(\mathbb{Q}_p(\sqrt{ab})/\mathbb{Q}_p).$$

3. Es gilt $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, woraus $\left(\frac{ab}{p}\right) = 1$ folgt. Nur $\sqrt{ab}$ liegt demnach in $\mathbb{Q}_p$, und

$$G_p = G(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}(\sqrt{ab})) = G(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p) = G(\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p).$$

Es soll nun gezeigt werden, dass jeder der genannten Fälle für unendlich viele Primzahlen p eintritt. Seien $\delta_a, \delta_b \in \{1, -1\}$ nicht beide gleich 1. Behauptet wird, dass es unendlich viele Primzahlen p gibt mit $\left(\frac{a}{p}\right) = \delta_a$ und $\left(\frac{b}{p}\right) = \delta_b$. Es sei $a = a'd$ und $b = b'd$, mit $d \in \mathbb{N}$ als dem größten gemeinsamen Teiler von a und b. Für alle Primzahlen p gilt $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)\left(\frac{d}{p}\right)$ und $\left(\frac{b}{p}\right) = \left(\frac{b'}{p}\right)\left(\frac{d}{p}\right)$, wobei a', b' und d quadratfrei und daher auch paarweise teilerfremd sind. Deshalb liegt es nahe, die Frage zu stellen, ob es unendlich viele Primzahlen p gibt mit $\left(\frac{a'}{p}\right) = \delta_a$, $\left(\frac{b'}{p}\right) = \delta_b$ und $\left(\frac{d}{p}\right) = 1$. Der Übersichtlichkeit halber werden bei der Beantwortung der Frage zwei Fälle unterschieden. Im ersten Fall haben a' und b' beide mindestens einen Primfaktor, während im zweiten $b = -1$ ist und $a = a'$ weiterhin mindestens einen Primfaktor besitzt. Diese beiden Fälle genügen, weil die restlichen darauf zurückgeführt werden können: im Falle $a', b' = \pm 1$ gilt $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{d}, \sqrt{-d}) = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$; ist hingegen nur $b' = \pm 1$, so kann a durch den Quotienten $a/b = a'/b' = \pm a' \neq \pm 1$ ersetzt werden und dann haben $\pm a'$ und $b = b' = \pm d$ beide mindestens einen Primfaktoren oder es ist $b' = -1$.

Es liege nun der erste Fall vor, und zwar sei

$$d = l_1 \dots l_r,\ r \geq 0$$
$$a' = \varepsilon_a p_1 \dots p_s,\ \varepsilon_a = \pm 1,\ s > 0$$
$$b' = \varepsilon_b q_1 \dots q_t,\ \varepsilon_b = \pm 1,\ t > 0$$

mit paarweise verschiedenen Primzahlen $l_1 \dots l_r, p_1 \dots p_s, q_1 \dots q_t$. Wir werden zunächst zeigen, dass es unendlich viele Primzahlen $p \neq l_1 \dots l_r, p_1 \dots p_s, q_1 \dots q_t$ gibt, welche den folgenden Bedingungen genügen.

1. $p \equiv 1(4)$, aäquivalent zu $\left(\frac{-1}{p}\right) = 1$;

für die ungeraden Primzahlen unter den l_i, p_j, q_k möge gelten:

2. $\left(\frac{l_i}{p}\right) = \left(\frac{p}{l_i}\right) = 1$ (die erste Gleichung fogt aus dem quadratischen Reziprozitätsgesetz) (z. B. sei $p \equiv 1(l_i)$);

3. $\left(\frac{p_1}{p}\right) = \left(\frac{p}{p_1}\right) = \delta_a$, $\left(\frac{p_j}{p}\right) = \left(\frac{p}{p_j}\right) = 1$ für alle $j > 1$;

4. $\left(\frac{q_1}{p}\right) = \left(\frac{p}{q_1}\right) = \delta_b$, $\left(\frac{q_k}{p}\right) = \left(\frac{p}{q_k}\right) = 1$ für alle $k > 1$.

Wir bemerken, dass höchstens eine der Primzahlen l_i, p_j, q_k gleich 2 ist; im folgenden kann dann $p \equiv 1(8)$ oder $p \equiv 5(8)$ gewählt werden, je nachdem ob $\left(\frac{2}{p}\right) = 1$ oder $\left(\frac{2}{p}\right) = -1$ erforderlich ist.

Für jede Primzahl p, die die Bedingungen 1.-4. erfüllt, gilt

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{p_1}{p}\right)\dots\left(\frac{p_s}{p}\right)\left(\frac{l_1}{p}\right)\dots\left(\frac{l_r}{p}\right) = \delta_a$$

$$\left(\frac{b}{p}\right) = \left(\frac{b'}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{q_1}{p}\right)\dots\left(\frac{q_t}{p}\right)\left(\frac{l_1}{p}\right)\dots\left(\frac{l_r}{p}\right) = \delta_b,$$

Für jede ungerade Primzahl l hängt der Wert ± 1 von $\left(\frac{p}{l}\right) = \left(\frac{l}{p}\right)$ nur von der Restklasse von p modulo l ab: nach Definition gilt $\left(\frac{p}{l}\right) = 1$ genau dann, wenn p ein Quadrat modulo l ist. Für jede ganze Zahl l in $\{4, l_1 \dots l_r, p_1 \dots p_s, q_1 \dots q_t\}$ wähle man nun eine Restklasse modulo l, so dass alle Bedingungen 1.-4. bzw. die entsprechenden Kongruenzen erfüllt sind. Nach dem Chinesischen Restsatz gibt es dann genau eine Restklasse modulo $4l_1 \dots l_r p_1 \dots p_s q_1 \dots q_t$, deren Vertreter diesen Kongruenzen genügen, und nach dem Primzahlsatz von Dirichlet (vgl. [N, S. 490]) liegen unendlich viele Primzahlen in dieser Restklasse (da jeder Vertreter der Restklasse nach Wahl der Kongruenzen prim ist zu allen l_i, p_j, q_t sowie 2).

Damit ist der erste Fall abgeschlossen, und nun soll auf den zweiten eingegangen werden. Es ist nun

$$a = \varepsilon p_1 \dots p_s,\ \varepsilon_a = \pm 1,\ s > 0,\ \ b = -1,$$

mit paarweise verschiedenen Primzahlen p_i. Wir haben die Existenz unendlich vieler Primzahlen p zu zeigen mit $\left(\frac{a}{p}\right) = \delta_a$ und $\left(\frac{-1}{p}\right) = \delta_b$ (in der Notation des ersten Falles). Ist $\delta_b = 1$, so ergibt sich die Behauptung mit $p \equiv 1(4)$ wie im ersten Fall. Ist $\delta_b = -1$, so sei $p \equiv 3(4)$; nach dem quadratischen Reziprozitätsgesetz gilt für ungerades p_i

$$\left(\frac{p_i}{p}\right) = (-1)^{\frac{p_i-1}{2}}\left(\frac{p}{p_i}\right).$$

Die Behauptung ergibt sich nun ebenfalls wie im ersten Fall (ist eines der p_i gleich 2, so gilt $\left(\frac{2}{p}\right) = 1$ für $p \equiv -1(8)$, und $\left(\frac{2}{p}\right) = -1$ für $p \equiv 3(8)$).

Damit ist der Beweis von Satz 4.3 beendet.

4.v Anwendung des Dichtigkeitssatzes von Tschebotarev

Aus dem Dichtigkeitssatz von Tschebotarev ergibt sich die folgende Verallgemeinerung von Satz 4.3.

4.4 Satz. *Es sei K/k eine galoissche Erweiterung algebraischer Zahlkörper mit abelscher Galoisgruppe G. Dann ist jede der zyklischen Untergruppen von G für unendlich viele Stellen $\mathfrak{p}$ von k gleich der Zerlegungsgruppe $G_\mathfrak{p}$.*

Es sei $\mathfrak{p}$ eine endliche Stelle von k, die in K unverzweigt ist, d.h. der gemeinsame Verzweigungsindex der über $\mathfrak{p}$ liegenden Stellen $\mathfrak{P}$ von K sei gleich 1. Die lokalen Erweiterungen $K_\mathfrak{P}/k_\mathfrak{p}$ sind dann alle unverzweigt, da die globale Erweiterung K/k an den $\mathfrak{p}$ teilenden Stellen $\mathfrak{P}$ von K unverzweigt ist. Über unverzweigte Erweiterungen lokaler Körper ist bekannt, dass sie zyklisch sind mit dem sog. Frobeniusautomorphismus als kanonischem Erzeugenden; dieser ist dadurch charakterisiert, dass er auf der Erweiterung der Restklassenkörper den zugehörigen Frobeniusautomorphismus vermittelt, vgl. [A2, S. 97]. Da die Restklassenkörper von k bzw. K für jedes $\mathfrak{P}/\mathfrak{p}$ mit denen von $k_\mathfrak{p}$ bzw. $K_\mathfrak{P}$ identifiziert werden können ([A2, S. 66]), gibt es also für jedes $\mathfrak{P}/\mathfrak{p}$ einen kanonischen Erzeuger der Zerlegungsgruppe $G_\mathfrak{P}$, nämlich den, der auf der Erweiterung $\bar{K}_\mathfrak{P}/\bar{k}_\mathfrak{p}$ den Frobeniusautomorphismus induziert. Er wird Frobeniusautomorphismus zu $\mathfrak{P}$ bzgl. der Erweiterung K/k genannt und mit

$$\varphi_\mathfrak{P} = \left(\frac{K/k}{\mathfrak{P}}\right)$$

bezeichnet, vgl. [AZ, S. 123]. Für alle $\sigma \in G(K/k)$ gilt

$$\left(\frac{K/k}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{K/k}{\mathfrak{P}}\right)\sigma^{-1},$$

vgl. [AZ, S. 124]. Wenn die Erweiterung K/k abelsch ist, hängt der Frobeniusautomorphismus $\left(\frac{K/k}{\mathfrak{P}}\right)$ deshalb nicht mehr von der über $\mathfrak{p}$ liegenden Stelle $\mathfrak{P}$ von K ab. So kann in diesem Fall jeder in K unverzweigten Stelle $\mathfrak{p}$ von k das Artinsymbol

$$\varphi_\mathfrak{p} = \left(\frac{K/k}{\mathfrak{p}}\right)$$

von $\mathfrak{p}$ bzgl. der abelschen Erweiterung K/k zugeordnet werden, mit $\left(\frac{K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{P}}\right)$, wenn $\mathfrak{P}$ eine $\mathfrak{p}$ teilende Stelle in K bezeichnet.

Aus dem Dichtigkeitssatz von Tschebotarev folgt für abelsches K/k, dass es zu jedem $\sigma \in G$ unendlich viele in K unverzweigte endliche Stellen $\mathfrak{p}$ von k gibt, so dass

$$\sigma = \left(\frac{K/k}{\mathfrak{p}}\right)$$

der Frobeniusautomorphismus zu jeder der über $\mathfrak{p}$ liegenden Stellen $\mathfrak{P}$ von K ist (vgl. [AZ, S. 290]). Für jedes solche $\mathfrak{p}$ ist dann

$$G_\mathfrak{p} = <\sigma>,$$

da der Frobeniusautomorphismus $\left(\frac{K/k}{\mathfrak{p}}\right)$ der über $\mathfrak{p}$ liegenden Stellen von K die Zerlegungsgruppe $G_{\mathfrak{p}}$ erzeugt. Demnach ist jede der zyklischen Untergruppen von $G(K/k)$ für unendlich viele Stellen $\mathfrak{p}$ gleich der Zerlegungsgruppe $G_{\mathfrak{p}}$.

Wir kommen nun zum zweiten Teil dieses Kapitels, in dem wir die Struktur der Gruppe $H^{-1}(G, K^\times)$ für gewisse Serien biquadratischer Erweiterungen $K/\mathbb{Q}$ explizit bestimmen wollen. Insbesondere wird dadurch gezeigt, dass alle Werte von n (vgl. Theorem 3.1) vorkommen können.

Im folgenden sei also $K/\mathbb{Q}$ eine biquadratische Erweiterung von $\mathbb{Q}$ mit Galoisgruppe G. Nach Theorem 3.1 ist $H^{-1}(G, K^\times)$ durch die Anzahl n der endlichen Stellen p von $\mathbb{Q}$ mit $G_p = G$ vollständig bestimmt. Zur Bestimmung von n genügt es nach Abschnitt 4.iii, die Gruppen G_p für alle Primteiler p der Diskriminanten der quadratischen Teilkörper von K zu berechnen. Es sollen nun zuerst für biquadratische Erweiterungen $K/\mathbb{Q}$, bei denen K aus $\mathbb{Q}$ durch Adjunktion der Wurzeln $\sqrt{a}, \sqrt{b}$ zweier ungerader Primzahlen entsteht, alle Fälle klassifiziert werden, die bei derartigen Erweiterungen auftreten können, und später auch für einige andere Werte von a, b.

4.vi Es sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, mit ungeraden Primzahlen $a \neq b$. Die Erweiterung ist dann biquadratisch, weil $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}(\sqrt{b})$ gilt (vgl. [A1, S. 281]). Bei der Bestimmung der lokalen Galoisgruppen G_p sind folgende Fälle zu unterscheiden.

1. $p \neq 2, a, b$. Da p die Diskriminanten von $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ nicht teilt, ist p in jedem dieser Körper träge oder voll zerlegt. Die Erweiterungen $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ und $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ sind damit unverzweigt, so dass folglich auch die Erweiterung $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$ unverzweigt ist und demnach höchstens den Grad 2 hat. Genau dann ist der Grad von $\mathbb{Q}_p(\sqrt{a}, \sqrt{b})/\mathbb{Q}_p$ gleich 1, wenn p sowohl in $\mathbb{Q}(\sqrt{a})$ als auch in $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist. Es folgt

$$G_p = 1 \text{ falls } \left(\tfrac{a}{p}\right) = \left(\tfrac{b}{p}\right) = 1$$
$$G_p \simeq \mathbb{Z}/2 \text{ sonst.}$$

2. Es sei $p = a$. Dann teilt p die Diskriminante von $\mathbb{Q}(\sqrt{a})$, die von $\mathbb{Q}(\sqrt{b})$ hingegen nicht. Anders ausgedrückt ist p nur in $\mathbb{Q}(\sqrt{a})$ verzweigt, so dass die Erweiterung $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ rein verzweigt ist vom Grade 2, während die Erweiterung $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ unverzweigt ist. Deshalb gilt $\mathbb{Q}_p(\sqrt{a}) \neq \mathbb{Q}_p(\sqrt{b})$, und das Kompositum hat den Grad 4 über $\mathbb{Q}$ genau dann, wenn wenn nicht $\mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p$ gilt. Dabei ist $\mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p$ äquivalent dazu, dass p in $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist. Also hat man

$$G_a \simeq \mathbb{Z}/2 \text{ falls } \left(\tfrac{b}{a}\right) = 1$$

$$G_a = G \text{ falls } \left(\tfrac{b}{a}\right) = -1.$$

3. Im Falle $p = b$ gilt entsprechend

$$G_b \simeq \mathbb{Z}/2 \text{ falls } \left(\tfrac{a}{b}\right) = 1$$
$$G_b = G \text{ falls } \left(\tfrac{a}{b}\right) = -1.$$

4. Es sei $p = 2$. Der Grad der Erweiterung $\mathbb{Q}_2(\sqrt{a}, \sqrt{b})/\mathbb{Q}_2$ ist genau dann gleich 4, wenn die Teilerweiterungen $\mathbb{Q}_2(\sqrt{a})/\mathbb{Q}_2$, $\mathbb{Q}_2(\sqrt{b})/\mathbb{Q}_2$ und $\mathbb{Q}_2(\sqrt{ab})/\mathbb{Q}_2$ alle den Grad 2 haben; das wiederum ist äquivalent dazu, dass die Primzahl 2 in keinem der Körper $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ und $\mathbb{Q}(\sqrt{ab})$ voll zerlegt ist. Die Primzahl 2 ist in einem quadratischen Teilkörper $\mathbb{Q}(\sqrt{d})$ genau dann voll zerlegt, wenn $d \equiv 1\ (8)$ gilt. Dabei ist $ab \equiv 1\ (8)$ äquivalent zu $a \equiv b\ (8)$, denn in der Einheitengruppe von $\mathbb{Z}/8$ ist jedes Element zu sich selbst invers. Weiter ist der Grad der Erweiterung $\mathbb{Q}_2(\sqrt{a}, \sqrt{b})/\mathbb{Q}_2$ genau dann gleich 1, wenn die Teilerweiterungen $\mathbb{Q}_2(\sqrt{a})/\mathbb{Q}_2$ und $\mathbb{Q}_2(\sqrt{b})/\mathbb{Q}_2$ beide den Grad 1 haben, d.h. wenn die Primzahl 2 in $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist. Zusammenfassend gilt

$$G_2 = 1 \text{ falls } a, b \equiv 1\ (8)$$
$$G_2 = G \text{ falls } a, b \not\equiv 1\ (8),\ a \not\equiv b\ (8).$$
$$G_2 \simeq \mathbb{Z}/2 \text{ sonst.}$$

Für eine beliebige Primzahl p kann die lokale Galoisgruppe G_p also leicht bestimmt werden, wobei für $p \neq 2$ mindestens eines der Legendre-Symbole $\left(\frac{a}{p}\right)$ oder $\left(\frac{b}{p}\right)$ sinnvoll ist und ausgewertet werden muss, was aber Dank dem quadratischen Reziprozitätsgesetz und der Ergänzungssätze keine Schwierigkeit darstellt. Ist man jedoch nur an $H^{-1}(G, K^\times)$ interessiert, so genügt es wie gesagt, die Anzahl der endlichen Stellen p von $\mathbb{Q}$ mit $G_p = G$ zu kennen. Dies ist nun für Primzahlen p möglich, die Primteiler von einer der Diskriminanten der Körper $\mathbb{Q}(\sqrt{a})$ und $\mathbb{Q}(\sqrt{b})$ sind. Es genügt deshalb, die Zerlegungsgruppen G_2, G_a und G_b zu betrachten. Der Übersichtlichkeit halber soll kurz festgehalten werden, wann genau eine jede unter diesen Gruppen mit der Galoisgruppe G übereinstimmt. Die vorangegangenen Überlegungen haben gezeigt, dass folgendes gilt.

$$G_a = G \ \Leftrightarrow\ \left(\tfrac{b}{a}\right) = -1$$
$$G_b = G \ \Leftrightarrow\ \left(\tfrac{a}{b}\right) = -1$$
$$G_2 = G \ \Leftrightarrow\ a, b \not\equiv 1\ (8),\ a \not\equiv b\ (8).$$

Die Fälle, die für ein Primzahlpaar (a, b) auftreten können, lassen sich nun wie folgt klassifizieren.

4.5 Satz. *Es sei $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, mit ungeraden Primzahlen $a \neq b$, und es sei G die Galoisgruppe der biquadratischen Erweiterung $K/\mathbb{Q}$. Dann gilt*

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^2$ in den Fällen

1) $a \equiv 3\ (4)$, $b \equiv 5\ (8)$ oder umgekehrt, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = -1 \quad (G_a = G_b = G_2 = G)$;
Beispiele: $(a, b) = (3, 5),\ (7, 5)$;

$H^{-1}(G, K^\times) \simeq \mathbb{Z}/2$ in den Fällen

2) $a \equiv 1\ (8)$ oder $b \equiv 1\ (8)$ oder $a \equiv b\ (8)$, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = -1 \quad (G_a = G_b = G, G_2 \neq G)$
Beispiele: $(a, b) = (3, 17),\ (5, 17),\ (7, 17),\ (41, 17),\ (5, 13)$;

3) $a, b \equiv 3\ (4)$, $a \not\equiv b\ (8)$, d. h. $a \equiv 3\ (8)$, $b \equiv 7\ (8)$ oder umgekehrt, $(G_a = G,\ G_b \simeq \mathbb{Z}/2$ oder umgekehrt, $G_2 = G)$
Beispiele: $(a, b) = (3, 7),\ (3, 23)$;

$H^{-1}(G, K^\times) = 1$ in den Fällen

4) $a \equiv 3\ (4)$, $b \equiv 5\ (8)$ oder umgekehrt, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = 1 \quad (G_a = G_b \simeq \mathbb{Z}/2,\ G_2 = G)$
Beispiele: $(a, b) = (3, 13),\ (7, 29),\ (11, 5),\ (31, 5)$;

5) $a, b \equiv 3\ (4)$, $a \equiv b\ (8)$, d. h. $a, b \equiv 3\ (8)$ oder $a, b \equiv 7\ (8) \quad (G_a = G,\ G_b \simeq \mathbb{Z}/2$ oder umgekehrt, $G_2 \simeq \mathbb{Z}/2)$
Beispiele: $(a, b) = (3, 11),\ (7, 23)$;

der singuläre Fall $G_p \neq G$ für alle p hingegen liegt vor falls

6) $a \equiv 1\ (8)$ oder $b \equiv 1\ (8)$ oder $a \equiv b\ (8)$, $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = 1 \quad (G_a = G_b \simeq \mathbb{Z}/2,\ G_2 \simeq \mathbb{Z}/2$ oder $G_2 = 1)$
Beispiele: $(a, b) = (3, 73),\ (5, 41),\ (7, 113),\ (13, 17),\ (19, 17),\ (31, 17),\ (89, 17),\ (5, 29)$;

im singulären Fall gilt ebenfalls $H^{-1}(G, K^\times) = 1$.

Dies sind sämtliche Fälle, die bei einer Erweiterung vom Typ $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ mit voneinander verschiedenen, ungeraden Primzahlen a, b vorkommen können.

4.vii Es sei nun $a = 2$, d.h. $K = \mathbb{Q}(\sqrt{2}, \sqrt{b})$, wobei b weiterhin eine ungerade Primzahl bezeichnet.

1. Es sei $p \neq 2, b$. Dann ist p kein Teiler der Diskriminanten von $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{b})$, so dass p in diesen Körpern nicht verzweigt, d. h. träge oder voll zerlegt ist. Die lokalen Erweiterungen $\mathbb{Q}_p(\sqrt{2})/\mathbb{Q}_p$ und $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ sind demnach unverzweigt, weshalb auch das Kompositum $\mathbb{Q}_p(\sqrt{2}, \sqrt{b})/\mathbb{Q}_p$ unverzweigt ist und somit höchstens den Grad 2 hat. Genauer gilt

$$G_p = 1 \text{ falls } \left(\frac{2}{p}\right) = \left(\frac{b}{p}\right) = 1$$

$$G_p \simeq \mathbb{Z}/2 \text{ sonst.}$$

2. Es sei $p = b$. Da p die Diskriminante von $\mathbb{Q}(\sqrt{b})$ teilt, die von $\mathbb{Q}(\sqrt{2})$ hingegen nicht, ist p in $\mathbb{Q}(\sqrt{b})$ verzweigt und in $\mathbb{Q}(\sqrt{2})$ träge oder voll zerlegt. Die Erweiterung $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ ist rein verzweigt ist vom Gerade 2, während die Erweiterung $\mathbb{Q}_p(\sqrt{2})/\mathbb{Q}_p$ unverzweigt ist. Man erhält

$$G_b \simeq \mathbb{Z}/2 \text{ falls } \left(\tfrac{2}{b}\right) = 1$$
$$G_b = G \text{ falls } \left(\tfrac{2}{b}\right) = -1.$$

3. Es sei $p = 2$. Dann ist p Teiler der Diskriminante 8 von $\mathbb{Q}(\sqrt{2})$, oder anders gesagt ist p in $\mathbb{Q}(\sqrt{2})$ verzweigt, d. h. die Erweiterung $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ ist rein verzweigt vom Grade 2. Die Erweiterung $\mathbb{Q}_2(\sqrt{b})/\mathbb{Q}_2$ kann hingegen von beliebigem Typus sein, denn bekanntlich hängt der Zerlegungstyp von 2 in $\mathbb{Q}(\sqrt{b})$ nur von der Restklasse von b modulo 8 ab. Weil $p = 2$ Teiler von $2b$ ist, kann jedenfalls gesagt werden, dass 2 in $\mathbb{Q}(\sqrt{2b})$ verzweigt ist. Es stellt sich somit die Frage, wann 2 in $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist und demzufolge $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2b})$ ist, oder wann andererseits 2 in $\mathbb{Q}(\sqrt{b})$ nicht voll zerlegt ist und damit alle drei Erweiterungen $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{b})$ und $\mathbb{Q}(\sqrt{2b})$ voneinander verschieden sind. Es ergibt sich

$$G_2 \simeq \mathbb{Z}/2 \text{ falls } b \equiv 1\ (8)$$
$$G_2 = G \text{ falls } b \not\equiv 1\ (8).$$

Nach 2. und 3. gilt daher

$$G_b = G \ \Leftrightarrow\ \left(\tfrac{2}{b}\right) = -1$$
$$G_2 = G \ \Leftrightarrow\ b \not\equiv 1\ (8)$$

und man erhält den folgenden

4.6 Satz. *Es sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{b})$, mit einer ungeraden Primzahl b, und G die Galoisgruppe der biquadratischen Erweiterung $K/\mathbb{Q}$. Dann gilt im nichtsingulären Fall*

$H^{-1}(G, K^\times) \simeq \mathbb{Z}/2$ falls $b \equiv \pm 3\ (8)$ $\quad (G_b = G_2 = G)$
Beispiele: $(a, b) = (2, 3),\ (2, 5)$;

$H^{-1}(G, K^\times) = 1$ falls $b \equiv 7\ (8)$ $\quad (G_b \simeq \mathbb{Z}/2,\ G_2 = G)$
Beispiele: $(a, b) = (2, 7),\ (2, 23)$;

der singuläre Fall liegt vor für $b \equiv 1\ (8)$ $\quad (G_b = G_2 \simeq \mathbb{Z}/2)$
Beispiele: $(a, b) = (2, 17),\ (2, 41)$;
im singulären Fall gilt $H^{-1}(G, K^\times) = 1$.

4.viii Es sei nun $a = -1$, d.h. $K = \mathbb{Q}(\sqrt{-1}, \sqrt{b})$, mit beliebiger Primzahl b. Die Situation ist wie folgt.

1. Es sei $p \neq 2, b$. Weil p in $\mathbb{Q}(\sqrt{-1})$ und $\mathbb{Q}(\sqrt{b})$ nicht verzweigt ist, sind die Erweiterungen $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt{b})/\mathbb{Q}$ und damit auch die Erweiterungen $\mathbb{Q}_p(\sqrt{-1})/\mathbb{Q}_p$, $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ unverzweigt. Folglich ist auch $\mathbb{Q}_p(\sqrt{-1}, \sqrt{b})/\mathbb{Q}_p$ unverzweigt, weshalb der Grad nur 1 oder 2 sein kann. Genau dann ist der Grad gleich 1, wenn p sowohl in $\mathbb{Q}(\sqrt{-1})$ als auch in $\mathbb{Q}(\sqrt{b})$ voll zerlegt ist, d.h. wenn $\left(\frac{-1}{p}\right) = \left(\frac{b}{p}\right) = 1$ gilt. Hierbei ist $\left(\frac{-1}{p}\right) = 1$ äquivalent zu $p \equiv 1\ (4)$, so dass man erhält

$$G_p = 1 \text{ falls } p \equiv 1\ (4) \text{ und } \left(\tfrac{b}{p}\right) = 1$$
$$G_p \simeq \mathbb{Z}_2 \text{ sonst.}$$

2. Es sei $p \neq 2$ und $p = b$. Bekanntlich ist p in $\mathbb{Q}(\sqrt{p})$ verzweigt, während p in $\mathbb{Q}(\sqrt{-1})$ nur träge oder voll zerlegt sein kann. Nur dann stimmt G_p mit G überein, wenn p in $\mathbb{Q}(\sqrt{-1})$ träge ist, d.h. wenn $\left(\frac{-1}{p}\right) = -1$ gilt. Demnach hat man

$$G_b \simeq \mathbb{Z}/2 \text{ falls } b \equiv 1\ (4)$$
$$G_b = G \text{ falls } b \equiv 3\ (4).$$

3. Es sei $p = 2$. Nun ist 2 in $\mathbb{Q}(\sqrt{-1})$ verzweigt, doch in $\mathbb{Q}(\sqrt{b})$ sind alle Zerlegungstypen möglich. Die Aussage $G_2 = G$ ist äquivalent dazu, dass 2 weder in $\mathbb{Q}(\sqrt{b})$ noch in $\mathbb{Q}(\sqrt{-b})$ voll zerlegt ist. Dabei ist 2 genau dann in $\mathbb{Q}(\sqrt{b})$ voll zerlegt, wenn $b \equiv 1\ (8)$ ist, und in $\mathbb{Q}(\sqrt{-b})$ ist 2 genau dann voll zerlegt, wenn $-b \equiv 1\ (8)$ ist. Zusammenfassend heisst das

$$G_2 \simeq \mathbb{Z}/2 \text{ falls } b \equiv \pm 1\ (8)$$
$$G_2 = G \text{ falls } b \equiv \pm 3\ (8).$$

Damit erhält man

$$G_b = G \quad \Leftrightarrow \quad b \equiv 3\ (4),$$
$$G_2 = G \quad \Leftrightarrow \quad b \equiv \pm 3\ (8)$$

sowie den folgenden

4.7 Satz. *Es sei $K = \mathbb{Q}(\sqrt{-1}, \sqrt{b})$, mit einer beliebigen Primzahl b, und G die Galoisgruppe der biquadratischen Erweiterung $K/\mathbb{Q}$. Dann gilt im nicht-singulären Fall*

$H^{-1}(G, K^\times) \simeq \mathbb{Z}/2$ *falls* $b \equiv 3\ (8)$ $\quad (G_b = G_2 = G)$
Beispiele: $(a, b) = (-1, 3),\ (-1, 11)$*;*

$H^{-1}(G, K^\times) = 1$ *falls* $b \equiv 5, 7\ (8)$ $\quad (G_b \simeq \mathbb{Z}/2,\ G_2 = G$ *oder umgekehrt),*
oder falls $b = 2$ $\quad (G_2 = G)$
Beispiele: $(a, b) = (-1, 5),\ (-1, 7),\ (-1, 2)$*;*

der singuläre Fall liegt vor für $b \equiv 1\ (8)$ $\quad (G_b = G_2 \simeq \mathbb{Z}/2)$
Beispiele: $(a, b) = (-1, 17),\ (-1, 41)$*;*
im singulären Fall gilt $H^{-1}(G, K^\times) = 1$.

4.ix Es sei $K = \mathbb{Q}(\sqrt{3}, \sqrt{b})$, $b \neq 2, 3$ prim (dies ist ein Spezialfall der in Satz 4.5 betrachteten Situation).

Es ist 2 verzweigt in $\mathbb{Q}(\sqrt{3})$, voll zerlegt in $\mathbb{Q}(\sqrt{b})$ genau für $b \equiv 1\ (8)$, und voll zerlegt in $\mathbb{Q}(\sqrt{3b})$ genau für $3b \equiv 1\ (8)$ bzw. $b \equiv 3\ (8)$. Es folgt

$$G_2 \simeq \mathbb{Z}/2 \text{ falls } b \equiv 1, 3\ (8)$$
$$G_2 \simeq (\mathbb{Z}/2)^2 \text{ falls } b \equiv 5, 7\ (8).$$

Weiter ist 3 verzweigt in $\mathbb{Q}(\sqrt{3})$, voll zerlegt in $\mathbb{Q}(\sqrt{b})$ für $\left(\frac{b}{3}\right) = 1$ und träge in $\mathbb{Q}(\sqrt{b})$ für $\left(\frac{b}{3}\right) = -1$. Daher gilt

$$G_3 \simeq \mathbb{Z}/2 \text{ falls } b \equiv 1\ (3)$$
$$G_3 \simeq (\mathbb{Z}/2)^2 \text{ falls } b \equiv -1\ (3).$$

Schließlich ist b voll zerlegt in $\mathbb{Q}(\sqrt{3})$ für $\left(\frac{3}{b}\right) = 1$, d.h. für $b \equiv \pm 1\ (12)$, und träge in $\mathbb{Q}(\sqrt{3})$ für $\left(\frac{3}{b}\right) = -1$ bzw. $b \equiv \pm 5\ (12)$, und daher

$$G_b \simeq \mathbb{Z}/2 \text{ falls } b \equiv \pm 1\ (12)$$
$$G_2 \simeq (\mathbb{Z}/2)^2 \text{ falls } b \equiv \pm 5\ (12).$$

Damit ergibt sich

4.8 Satz. *Es sei $\mathbb{Q}(\sqrt{3}, \sqrt{b})/\mathbb{Q}$ eine biquadratische Erweiterung, mit $p \neq 2, 3$ prim und Galoisgruppe G. Dann gilt im nicht-singulären Fall*

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^2$ *für* $b \equiv 5\ (24)$

$H^{-1}(G, K^\times) \simeq \mathbb{Z}/2$ *für* $b \equiv 7, 17, 23\ (24)$

$H^{-1}(G, K^\times) = 1$ *für* $b \equiv 11, 13, 19\ (24)$

während der singuläre Fall für $b \equiv 1\ (24)$ *vorliegt; im singulären Fall gilt ebenfalls* $H^{-1}(G, K^\times) = 1$.

4.x Es sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{p_1 \dots p_m})$, mit paarweise verschiedenen, ungeraden Primzahlen $p_1, \dots, p_m$.

Es ist 2 verzweigt in $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2p_1 \dots p_m})$, und 2 ist voll zerlegt in $\mathbb{Q}(\sqrt{p_1 \dots p_m})$ genau für $p_1 \dots p_m \equiv 1\ (8)$. Daher gilt

$$G_2 \simeq \mathbb{Z}/2 \text{ falls } p_1 \dots p_m \equiv 1\ (8)$$
$$G_2 \simeq (\mathbb{Z}/2)^2 \text{ sonst.}$$

Weiter ist p_i voll zerlegt in $\mathbb{Q}(\sqrt{2})$ falls $\left(\frac{2}{p_i}\right) = 1$, träge in $\mathbb{Q}(\sqrt{2})$ falls $\left(\frac{2}{p_i}\right) = -1$, und in jedem Fall verzweigt in $\mathbb{Q}(\sqrt{p_1 \dots p_m})$. Es folgt

$$G_{p_i} \simeq \mathbb{Z}/2 \text{ falls } p_i \equiv \pm 1\ (8)$$
$$G_{p_i} \simeq (\mathbb{Z}/2)^2 \text{ falls } p_i \equiv \pm 3\ (8).$$

Damit erhält man

4.9 Satz. *Es sei $\mathbb{Q}(\sqrt{2}, \sqrt{p_1 \dots p_m})/\mathbb{Q}$ eine biquadratische Erweiterung, mit paarweise verschiedenen, ungeraden Primzahlen $p_1, \dots, p_m$ und Galoisgruppe G. Es sei m_1 die Anzahl der p_i mit $p_i \equiv \pm 3\ (8)$. Dann liegt der singuläre Fall vor für $m_1 = 0$, $p_1 \dots p_m \equiv 1\ (8)$. Im nicht-singulären Fall gilt*

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1 - 1}$ falls $m_1 > 0$, $p_1 \dots p_m \equiv 1\ (8)$;

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1}$ falls $p_1 \dots p_m \not\equiv 1\ (8)$.

Im singulären Fall gilt $H^{-1}(G, K^\times) = 1$.

4.xi Schließlich sei $K = \mathbb{Q}(\sqrt{-1}, \sqrt{p_1 \dots p_m})$, mit paarweise verschiedenen Primzahlen $p_1, \dots, p_m$.

Es ist 2 verzweigt in $\mathbb{Q}(\sqrt{-1})$. Für $p_1 \dots p_m \equiv \pm 1\ (8)$ ist 2 in $\mathbb{Q}(\sqrt{p_1 \dots p_m})$ bzw. in $\mathbb{Q}(\sqrt{-p_1 \dots p_m})$ voll zerlegt, für $p_1 \dots p_m \equiv \pm 3\ (8)$ ist 2 in $\mathbb{Q}(\sqrt{-p_1 \dots p_m})$ bzw. in $\mathbb{Q}(\sqrt{p_1 \dots p_m})$ träge. Für $p_1 \dots p_m \equiv \pm 2, 3, -1\ (8)$ ist 2 in $\mathbb{Q}(\sqrt{p_1 \dots p_m})$ verzweigt und für $p_1 \dots p_m \equiv \mp 2, -3, 1\ (8)$ ist 2 in $\mathbb{Q}(\sqrt{-p_1 \dots p_m})$ verzweigt. Es folgt

$$G_2 \simeq \mathbb{Z}/2 \text{ für } p_1 \dots p_m \equiv \pm 1\ (8)$$
$$G_2 \simeq (\mathbb{Z}/2)^2 \text{ sonst.}$$

Für $p_i \neq 2$ ist p_i voll zerlegt in $\mathbb{Q}(\sqrt{-1})$ falls $\left(\frac{-1}{p_i}\right) = 1$ bzw. $p_i \equiv 1\ (4)$, und träge in $\mathbb{Q}(\sqrt{-1})$ falls $\left(\frac{-1}{p_i}\right) = -1$ bzw. $p_i \equiv 3\ (4)$. In jedem Fall ist p_i verzweigt in $\mathbb{Q}(\sqrt{\pm p_1 \dots p_m})$.

$$G_{p_i} \simeq \mathbb{Z}/2 \text{ falls } p_i \equiv 1\ (4)$$

$$G_{p_i} \simeq (\mathbb{Z}/2)^2 \text{ falls } p_i \equiv 3\ (4).$$

Damit ergibt sich

4.10 Satz. *Es sei $\mathbb{Q}(\sqrt{-1}, \sqrt{p_1 \dots p_m})/\mathbb{Q}$ eine biquadratische Erweiterung, mit paarweise verschiedenen Primzahlen $p_1, \dots, p_m$ und Galoisgruppe G. Es sei m_1 die Anzahl der p_i mit $p_i \equiv 3, 7\ (8)$. Dann liegt der singuläre Fall vor für $m_1 = 0$, $p_1 \dots p_m \equiv \pm 1\ (8)$. Im nicht-singulären Fall gilt*

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1 - 1}$ *falls* $m_1 > 0$, $p_1 \dots p_m \equiv \pm 1\ (8)$;

$H^{-1}(G, K^\times) \simeq (\mathbb{Z}/2)^{m_1}$ *falls* $p_1 \dots p_m \not\equiv \pm 1\ (8)$.

Im singulären Fall gilt $H^{-1}(G, K^\times) = 1$.

Literatur

[AM] A. Adem, R. J. Milgram, *Cohomology of Finite Groups.* Grundlehren der mathematischen Wissenschaften 309, Springer 1994

[B] K. S. Brown, *Cohomology of Groups.* Graduate Texts in Mathematics 87, Springer 1982

[CF], [AW], [T] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory.* Academic Press 1967

[H] D. Hilbert, *Die Theorie der algebraischen Zahlkörper.* Jahresberichte der DMV 4 (1997), 175-546 (in David Hilbert, Gesammelte Abhandlungen Bd. 1, Springer 1970)

[HS] P. J. Hilton, U. Stammbach, *A Course in Homological Algebra.* Graduate Texts in Mathematics 4, Springer 1971

[A1] F. Lorenz, *Einführung in die Algebra I.* Spektrum Akademischer Verlag, 3. Auflage 1996

[A2] F. Lorenz, *Einführung in die Algebra II.* Spektrum Akademischer Verlag, 2. Auflage 1997

[AZ] F. Lorenz, *Algebraische Zahlentheorie.* BI-Wissenschaftsverlag 1993

[L] F. Lorenz, *Ein Scholion zum Satz 90 von Hilbert.* Abh. Math. Sem. Univ. Hamburg 68 (1998), 347-362

[N] J. Neukirch, *Algebraische Zahlentheorie.* Springer 1992

[SZ] R. Stöcker, H. Zieschang, *Algebraische Topologie.* 2. Auflage, Teubner 1994

[Wb] C. A. Weibel, *An Introduction to Homological Algebra.* Cambridge Studies in Advanced Mathematics 1994

[Ws] E. Weiss, *Cohomology of Groups.* Academic Press 1969

Dank

Mein herzlicher Dank gilt Herrn Professor Lorenz, der mich aufs Beste betreut hat, sowie Herrn T. Bauer für wichtige Hinweise. Weiter danke ich in besonderer Weise Herrn M. Wiegard.

Curriculum Vitae

Persönliche Daten

Name:	Nadja Zimmermann
Geburtsdatum:	15.10.1977
Geburtsort:	Bonn
Staatsbürgerschaft:	Deutsch
Familienstand:	ledig
Name des Vaters:	Bruno P. Zimmermann
Name der Mutter:	Gisela A. G. Zimmermann, geb. Riggert

Bildungsgang

1983/84	Wines School, Ann Arbor (Michigan, USA)
1984/85 bis 1986/87	Hufelandschule, Bochum
1987/88	Schillerschule, Bochum
1988/89 bis 1990/91	Scuola Media Statale ai Campi Elisi, Trieste (Italien)
1991/92 bis 1995/96	Liceo Scientifico Statale Guglielmo Oberdan, Trieste
23.12.1996	Abschluss: Abitur am Liceo Gulielmo Oberdan
WS 1996/97 bis WS 1998/99	Studium an der Westf. Wilhelms-Universität Münster
SS 1999	Semester an der Ruprecht-Karls-Universität Heidelberg
WS 1999/2000 bis WS 2003/04	Studium an der Westf. Wilhelms-Universität Münster
16.06.2004	Abschluss: Diplom in Mathematik an der Westfälischen Wilhelms-Universität Münster
WS 2004/05 bis SS 2006	Promotionsstudium der Mathematik an der Westfälischen Wilhelms-Universität Münster unter der Betreuung von Prof. Dr. Falko Lorenz

Tätigkeiten

WS 1998/99 bis WS 2004/05	Studentische Hilfskraft, wissenschaftliche Hilfskraft