

Hecke-Algebren zu unimodularen
und unitären Matrixgruppen
über Dedekind-Ringen

HECKE-ALGEBREN ZU UNIMODULAREN UND UNITÄREN MATRIXGRUPPEN ÜBER DEDEKIND-RINGEN

VON DER FAKULTÄT FÜR MATHEMATIK,
INFORMATIK UND NATURWISSENSCHAFTEN DER
RHEINISCH-WESTFÄLISCHEN TECHNISCHEN HOCHSCHULE
AACHEN ZUR ERLANGUNG DES AKADEMISCHEN GRADES
EINES DOKTORS DER NATURWISSENSCHAFTEN
GENEHMIGTE DISSERTATION

VORGELEGT VON

DIPLOM-MATHEMATIKER MARC ENSENBACH

AUS BOCHOLT

BERICHTER:

UNIVERSITÄTSPROFESSOR DR. RER. NAT. ALOYS KRIEG
UNIVERSITÄTSPROFESSOR DR. RER. NAT. HERBERT PAHLINGS

TAG DER MÜNDLICHEN PRÜFUNG: 17. OKTOBER 2008

DIESE DISSERTATION IST AUF DEN INTERNETSEITEN
DER HOCHSCHULBIBLIOTHEK ONLINE VERFÜGBAR.

VORWORT

Diese Dissertation entstand von 2004 bis 2008 am Lehrstuhl A für Mathematik der RWTH Aachen.

Für die Betreuung der Arbeit möchte ich mich bei Herrn Professor Krieg bedanken. Er hat mich durch viele wertvolle Anregungen unterstützt und war bei fachlichen Problemen stets ansprechbar.

Für die Übernahme der Zweitbetreuung danke ich Herrn Professor Pahlings.

Meinen derzeitigen und ehemaligen Kollegen am Lehrstuhl A für Mathematik möchte ich für die gute Arbeitsatmosphäre, die vielen interessanten mathematischen und nicht-mathematischen Unterhaltungen und die Versorgung mit Kuchen danken. Mein besonderer Dank gilt Frau Morton und Frau Giese, die mir bei verwaltungs- und organisationstechnischen Fragen stets geholfen haben.

Mein Dank gilt auch dem Graduiertenkolleg »Hierarchie und Symmetrie in mathematischen Modellen«. Ohne dessen Unterstützung wäre diese Dissertation zu diesem Zeitpunkt wohl noch nicht fertiggestellt. Danken möchte ich dabei besonders dem Sprecher, Herrn Professor Hiß, und den anderen Stipendiaten für die vielen anregenden Gespräche und Vorträge.

Abschließend gilt meinen Eltern und meinen Freunden und allen, die dafür gesorgt haben, dass auch außerhalb des Institutes meine

Vorwort

Promotionsphase eine sehr angenehme Zeit geworden ist – alle hier namentlich aufzuzählen würde den Rahmen sprengen – mein allerherzlichster Dank für diese schönen vier Jahre.

Aachen, im Juni 2008

Marc Ensenbach

INHALTSVERZEICHNIS

Zusammenfassung	9
Summary	11
Einleitung	13
1 Grundlagen	19
1.1 Die abstrakte Theorie der Hecke-Algebren	19
1.2 Dedekind-Ringe	28
2 Hecke-Algebren zu unimodularen Gruppen	39
2.1 Wohldefiniertheit	39
2.2 Grundlagen der Elementarteilertheorie	42
2.3 Maßformeln	53
2.4 Ein Reduktionssatz	75
2.5 Methoden zur Berechnung konkreter Produkte	78
2.6 Elementarteiler von Matrixprodukten	94
2.7 Tensorproduktzerlegungen	108
2.8 Zerlegbare Matrizen	115
2.9 Minimale Erzeugendensysteme	134
3 Hecke-Algebren zu unitären Gruppen	143
3.1 Wohldefiniertheit	143
3.2 Rechtsnebenklassenvertreter	150

Inhaltsverzeichnis

3.3	Tensorproduktzerlegungen	154
3.4	Simultane Vertretersysteme	161
	Ausblick	167
	Lebenslauf	169
	Literaturverzeichnis	171
	Symbolverzeichnis	175
	Index	177

ZUSAMMENFASSUNG

In dieser Dissertation wird die Struktur der Hecke-Algebren zu unimodularen Matrixgruppen über Dedekind-Ringen und zu unitären Matrixgruppen über Ganzheitsringen imaginär-quadratischer Zahlkörper untersucht.

Erstes Hauptresultat der Untersuchung der unimodularen Gruppen über einem Dedekind-Ring $\mathfrak{o}$ ist eine Maßformel, die es gestattet, im Falle von (2×2) -Matrizen die Anzahl der in einer Doppelnebenklasse der Form $GL_2(\mathfrak{o})A GL_2(\mathfrak{o})$ enthaltenen Rechtsnebenklassen der Form $GL_2(\mathfrak{o})A_i$ als

$$\mu(A) = N(\mathfrak{f}_2(A)) \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} | \mathfrak{f}_2(A)}} (1 + N(\mathfrak{p})^{-1})$$

zu berechnen, wobei $N(\cdot)$ die Norm eines Ideals und $\mathfrak{f}_2(A)$ den zweiten Grundfaktor von A bezeichnet, der als $\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}$ definiert ist, wenn $\mathfrak{d}_i(A)$ für den i -ten Determinantenteiler von A steht. Als Anwendung dieser Maßformel erhält man für das Produkt in der Hecke-Algebra die Reduktionsformel

$$(\llbracket \text{diag}(1, a) \rrbracket * \llbracket \text{diag}(1, b) \rrbracket)(\text{diag}(1, c)) = \begin{cases} 1, & \text{falls } c \in ab\mathfrak{o}^*, \\ 0 & \text{sonst.} \end{cases}$$

Das zweite zentrale Ergebnis ist eine Tensorproduktzerlegung. Bezeichnet H^* die Hecke-Algebra auf der Menge aller Matrizen aus

$\mathfrak{o}^{n \times n}$ mit Determinante in $\mathbb{Z} \setminus \{0\}$ zu der Untergruppe $\mathrm{GL}_n(\mathfrak{o})$ und H_p^* für jede Primzahl $p \in \mathbb{N}$ die Hecke-Algebra auf der Menge aller Matrizen aus $\mathfrak{o}^{n \times n}$ mit einer Determinante der Form $\pm p^k$ für ein $k \in \mathbb{N}_0$ ebenfalls zur Untergruppe $\mathrm{GL}_n(\mathfrak{o})$, so hat man

$$H^* \cong \bigotimes_{p \text{ Primzahl in } \mathbb{N}} H_p^*.$$

Weiter wird gezeigt werden, dass die H_p^* stets endlich erzeugte Algebren sind. Für $n = 2$ liefert die explizite Konstruktion einiger Erzeugendensysteme und die Untersuchung auf Minimalität, dass in den Fällen, dass $p\mathfrak{o}$ die Primidealzerlegung $\mathfrak{p}$ oder $\mathfrak{p}^2$ über $\mathfrak{o}$ hat, sogar algebraisch unabhängige Erzeugendensysteme existieren – genauer, dass in diesen Fällen $H_p^* \cong \mathbb{C}[X_1, X_2]$ gilt – und im Falle der Primidealzerlegung $p\mathfrak{o} = \mathfrak{p}\mathfrak{q}$ stets eine Relatorenmenge $R(p)$ existiert, so dass $H_p^* \cong \mathbb{C}[X_1, X_2, X_3, X_4] // R(p)$ gilt, was für den Fall, dass $\mathfrak{o}$ Ganzheitsring eines quadratischen Zahlkörpers ist, auf die Formel

$$H^* \cong \bigotimes_{p \text{ träge oder verzweigt}} \mathbb{C}[X_1, X_2] \otimes \bigotimes_{p \text{ zerlegt}} \mathbb{C}[X_1, X_2, X_3, X_4] // R(p)$$

führt.

Die Untersuchung der unitären Matrixgruppen liefert ausgezeichnete Vertreter von Rechtsnebenklassen (solche, deren C-Block die Nullmatrix ist) und die Existenz von simultanen Vertretersystemen von Rechts- und Linksnebenklassen. Hauptresultat ist die Beziehung

$$T_n(p^l) * T_n(m) = T_n(p^l m)$$

für den Fall, dass p eine träge Primzahl ist und $l, m, n \in \mathbb{N}$ mit $p \nmid m$ gilt, wobei $T_n(m)$ ein Element der Hecke-Algebra bezeichnet, das für alle Matrizen mit einer gewissen Determinante den Koeffizient 1 und sonst überall den Koeffizient 0 hat. Als Negativresultat wird bewiesen, dass im allgemeinen eine Tensorproduktzerlegung wie im Falle der unimodularen Gruppen hier nicht möglich ist.

SUMMARY

In this thesis the structure of the Hecke algebras related to unimodular matrix groups over Dedekind domains and to unitary matrix groups over the ring of integers of an imaginary quadratic number field is being analysed.

The first main result of the analysis of the unimodular groups over a Dedekind domain $\mathfrak{o}$ is a measure formula which in the case of (2×2) matrices allows to calculate the number of right cosets of type $\mathrm{GL}_2(\mathfrak{o})A_i$ contained in a double coset of type $\mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})$ by means of the formula

$$\mu(A) = N(\mathfrak{f}_2(A)) \prod_{\substack{\mathfrak{p} \text{ prime ideal} \\ \mathfrak{p} | \mathfrak{f}_2(A)}} (1 + N(\mathfrak{p})^{-1}),$$

where $N(\cdot)$ denotes the norm of an ideal and $\mathfrak{f}_2(A)$ denotes the second fundamental factor of A , which by definition equals to $\mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}$ when $\mathfrak{d}_i(A)$ stands for the i -th determinantal divisor of A . As an application of this measure formula to the product in the Hecke algebra one obtains the reduction formula

$$(\llbracket \mathrm{diag}(1, a) \rrbracket * \llbracket \mathrm{diag}(1, b) \rrbracket)(\mathrm{diag}(1, c)) = \begin{cases} 1, & \text{if } c \in ab\mathfrak{o}^*, \\ 0 & \text{otherwise.} \end{cases}$$

The second central result is a tensor product decomposition. Denote by H^* the Hecke algebra on the set of all matrices from $\mathfrak{o}^{n \times n}$ with

Summary

determinant in $\mathbb{Z} \setminus \{0\}$ with respect to the subgroup $\mathrm{GL}_n(\mathfrak{o})$ and by H_p^* for every prime $p \in \mathbb{N}$ the Hecke algebra on the set of all matrices from $\mathfrak{o}^{n \times n}$ with a determinant of type $\pm p^k$ for some $k \in \mathbb{N}_0$, likewise with respect to the subgroup $\mathrm{GL}_n(\mathfrak{o})$. Then one has

$$H^* \cong \bigotimes_{p \text{ prime in } \mathbb{N}} H_p^*.$$

Furthermore, it will be proven that the H_p^* are always finitely generated algebras. For the case $n = 2$ the explicit construction of some systems of generators and the analysis of minimality show that in those cases in which $p\mathfrak{o}$ has the prime ideal decomposition $\mathfrak{p}$ or $\mathfrak{p}^2$ over $\mathfrak{o}$ there even exist algebraically independent systems of generators – more precisely, that $H_p^* \cong \mathbb{C}[X_1, X_2]$ holds in those cases –, and that in those cases of prime ideal composition $p\mathfrak{o} = \mathfrak{p}\mathfrak{q}$ there always exists a set of relators $R(p)$ such that $H_p^* \cong \mathbb{C}[X_1, X_2, X_3, X_4] // R(p)$ holds, which in the case that $\mathfrak{o}$ is the ring of integers of a quadratic number field yields the formula

$$H^* \cong \bigotimes_{p \text{ inert or ramified}} \mathbb{C}[X_1, X_2] \otimes \bigotimes_{p \text{ split}} \mathbb{C}[X_1, X_2, X_3, X_4] // R(p).$$

The analysis of the unitary matrix groups yields distinguished representatives of right cosets (those whose C-block is the zero matrix) and the existence of simultaneous sets of representatives of right and left cosets. The main result is the relation

$$T_n(p^l) * T_n(m) = T_n(p^l m)$$

for the case that p is an inert prime and $l, m, n \in \mathbb{N}$ holds with $p \nmid m$, where $T_n(m)$ denotes an element of the Hecke algebra which for all matrices with a certain determinant has the coefficient 1 and otherwise has the coefficient 0. As a negative result it is proven that in general a tensor product decomposition similar to the one for the case of a unimodular group does not exist here.

EINLEITUNG

Ausgangspunkt der Hecke-Theorie für Modulformen ist der 1920 von Mordell geführte Beweis der Formel

$$\tau(m)\tau(n) = \sum_{\substack{d|\operatorname{ggT}(m,n) \\ d>0}} d^{11} \tau(mnd^{-2}),$$

die das Produkt zweier Fourierkoeffizienten der normierten Diskriminante Δ^* (einer Spitzenform vom Gewicht 12) als gewichtete Summe von Fourierkoeffizienten darstellt (Proc. Cambridge Phil. Soc. 19, S. 117–124). In moderner Sprechweise benutzte Mordell dabei implizit Hecke-Operatoren vom Gewicht 12.

Im Jahre 1940 erkannte Hecke, dass die von Mordell verwendete Konstruktion – die im wesentlichen einer Durchschnittsbildung über transformierte Modulformen entsprach – verallgemeinert werden konnte, und definierte eine Klasse von Operatoren (*Math. Werke*, S. 644–707), die heute Hecke-Operatoren genannt werden.

In der Form, wie sie von Hecke definiert wurden, entsprachen die Hecke-Operatoren bestimmten Mengen von Matrizen, wobei diese Mengen invariant unter der Links- und Rechtsmultiplikation mit Modulmatrizen (den (2×2) -Matrizen mit Determinante 1) waren. Aus dieser Darstellung ergab sich eine weitere Verallgemeinerung: Es wurden nun Operatoren zu allen (nichtleeren) Mengen, die invariant unter Links- und Rechtsmultiplikation mit Modulmatrizen waren,

definiert. Als elementaren Bestandteil erhielt man so die minimalen Mengen mit dieser Eigenschaft, die Doppelnebenklassen.

Die grundlegende Bedeutung der Doppelnebenklassen für die Hecke-Operatoren führte zu der Idee, zur Untersuchung der Relationen zwischen diesen (verallgemeinerten) Operatoren eine »abstrakte Hecke-Algebra« auf dem Vektorraum der formalen Summen von Doppelnebenklassen zu definieren und diese mit Hilfsmitteln der linearen Algebra zu analysieren. Die Erfolge dieses Ansatzes führten zu einem größeren Bekanntheitsgrad der abstrakten Hecke-Algebren, und die Tatsache, dass diese Algebren nicht nur in der Theorie der Modulformen Verwendung fanden, sondern auch Konzepte der Darstellungstheorie verallgemeinerten (vergleiche die Einführung in Abschnitt 1.1), führten zu einer Etablierung als Gegenstand eigenständiger Forschungen.

Die abstrakte Hecke-Algebra kann so allgemein formuliert werden, dass sie nicht nur für Doppelnebenklassen bezüglich der Gruppe der Modulmatrizen, sondern auch für Doppelnebenklassen bezüglich weiteren Gruppen, die eine bestimmte Endlichkeitsbedingung erfüllen, definiert werden können. Die wohlbekannten Grundlagen der sich daraus ergebenden allgemeinen Theorie werden in Abschnitt 1.1 aus der Literatur zusammengestellt.

Die in dieser Dissertation zu untersuchenden Hecke-Algebren sind in enger Anlehnung an die aus der Theorie der Modulformen bekannten »klassischen« Algebren solche, die über Doppelnebenklassen zu bestimmten Matrixgruppen definiert sind, nämlich den Doppelnebenklassen zu unimodularen und unitären Gruppen.

Die Theorie der Hecke-Algebren zu unimodularen Gruppen (also den Gruppen der über gegebenen Ringen invertierbaren Matrizen) ist für den Fall, dass der zugrundeliegende Ring ein Hauptidealring ist, wohlbekannt und wurde in [Enso4] aus Arbeiten von Freitag, Krieg und Tamagawa zusammengestellt. Als Verallgemeinerung werden nun in dieser Dissertation als zugrundeliegende Ringe nicht nur

Hauptidealringe, sondern beliebige normendliche Dedekind-Ringe betrachtet, was insbesondere alle Ganzheitsringe algebraischer Zahlkörper abdeckt.

Die Grundlagen der Theorie der Dedekind-Ringe werden in Abschnitt 1.2 dargestellt, bevor dann im zweiten Kapitel die Struktur der abstrakten Hecke-Algebren zu unimodularen Gruppen über diesen Ringen untersucht wird. In Abschnitt 2.1 wird dabei zunächst gezeigt, dass die interessierenden Hecke-Algebren unter den gegebenen Voraussetzungen tatsächlich wohldefiniert sind. Abschnitt 2.2 legt die Grundlagen für genauere algebraische Untersuchungen, indem für den zu betrachtenden Fall eine einfache Charakterisierung der Gleichheit von Doppelnebenklassen gegeben wird und deren Konsequenzen untersucht werden.

Im klassischen Fall von einiger Bedeutung sind Formeln zur Bestimmung der Anzahl von Rechtsnebenklassen in gegebenen Doppelnebenklassen, da es diese erlauben, bestimmte formale Potenzreihen als Quotient von Polynomen darzustellen; in Abschnitt 2.3 wird eine solche Formel für den Fall von (2×2) -Matrizen über Dedekind-Ringen hergeleitet, und in Abschnitt 2.4 findet diese Formel Anwendung im Beweis eines Reduktionssatzes, der es gestattet, Teile der Struktur einer gegebenen Hecke-Algebra durch die Struktur einer Hecke-Algebra zu Matrizen eines einfacheren Formats zu beschreiben. Der Abschnitt 2.5 stellt eine weitere Anwendung der Formel zur Berechnung der Anzahl von Rechtsnebenklassen in Doppelnebenklassen vor, die es erlaubt, Produkte von konkret gegebenen Doppelnebenklassen von Matrizen in der Hecke-Algebra explizit algorithmisch zu berechnen; neben dem auf dieser Anwendung beruhenden Algorithmus werden darüberhinausgehend auch weitere Methoden zur Berechnung konkreter Produkte behandelt.

In Abschnitt 2.6 wird die bereits aus Abschnitt 2.2 bekannte Elementarteilertheorie dahingehend vertieft, dass der Zusammenhang zwischen dem Produkt in der Hecke-Algebra und den Determinantenteilern

im Detail untersucht wird. Diese Ergebnisse finden in Abschnitt 2.7 bei der Tensorproduktzerlegung von Hecke-Algebren Anwendung. Für den klassischen Fall kennt man das Ergebnis, dass die Hecke-Algebra sich als Tensorprodukt gewisser zu Primzahlen gehöriger Unteralegebren schreiben lässt; in dem hier betrachteten allgemeinen Fall lässt sich jedoch nur eine leicht schwächere Aussage beweisen. Eine weitere Anwendung der Ergebnisse aus Abschnitt 2.6 findet sich im Abschnitt 2.8 bei der Charakterisierung und expliziten Beschreibung von Erzeugendensystemen der in der Tensorproduktdarstellung auftretenden Unteralegebren; auch hier erhält man eine wesentlich kompliziertere Struktur als im klassischen Fall, in dem jede dieser Unteralegebren isomorph zu einem Polynomring in mehreren Variablen ist. In Abschnitt 2.9 schließlich werden die zuvor konstruierten Erzeugendensysteme auf Minimalität untersucht.

Nachdem im zweiten Kapitel die Hecke-Algebra zu unimodularen Gruppen über Dedekind-Ringen untersucht wurde, behandelt das dritte Kapitel den Fall unitärer Gruppen über Ganzheitsringen imaginär-quadratische Zahlkörper. Die unitären Gruppen werden in Abschnitt 3.1 als Gruppen von Matrizen, die eine bestimmte Invarianzbedingung erfüllen, eingeführt. Eine leichte Modifikation der Bedingung an das Transformationsverhalten liefert die Menge, auf der – wie gezeigt wird – in wohldefinierter Weise eine Hecke-Algebra definiert werden kann.

Wie auch im zweiten Kapitel sollen die hier definierten Hecke-Algebren auf die Möglichkeit einer Tensorproduktzerlegung untersucht werden. Als Vorbereitung werden dazu im Abschnitt 3.2 ausgezeichnete Vertreter von Rechtsnebenklassen bestimmt. In Abschnitt 3.3 wird dann unter Verwendung dieser ausgezeichneten Vertreter gezeigt, dass in Spezialfällen gewisse Multiplikativitäten in der Hecke-Algebra gelten, im allgemeinen aber eine vollständige Tensorproduktzerlegung nicht möglich ist.

Das dritte Kapitel schließt in Abschnitt 3.4 mit dem Nachweis, dass

sich bezüglich der unitären Gruppe Vertretersysteme der in einer Doppelnebenklasse enthaltenen Rechtsnebenklassen finden lassen, die zugleich auch Vertretersysteme der in der Doppelnebenklasse enthaltenen Linksnebenklassen sind.

KAPITEL EINS

GRUNDLAGEN

Dieses Kapitel gibt einen Überblick über die benötigten Grundlagen aus der Theorie der Hecke-Algebren (wie sie etwa in [Kri90] dargestellt ist) und der Theorie der Dedekind-Ringe und führt dabei die hier verwendete Notation ein.

§ 1.1

DIE ABSTRAKTE THEORIE DER HECKE-ALGEBREN

Algebraisch motiviert sich die Betrachtung von Hecke-Algebren aus dem in der Darstellungstheorie wichtigen Begriff der Gruppenalgebra.

Ist G eine Gruppe, so bildet die Menge

$$\mathbb{C}^{(G)} = \{f : G \rightarrow \mathbb{C} \mid f(g) \neq 0 \text{ nur für endlich viele } g \in G\}$$

der Abbildungen von G nach $\mathbb{C}$ mit endlichem Träger einen $\mathbb{C}$ -Vektorraum, der eine Basis der Form $\{1_g \mid g \in G\}$ besitzt, wobei

$$1_g : G \rightarrow \mathbb{C}, \quad h \mapsto \begin{cases} 1, & \text{falls } g = h, \\ 0 & \text{sonst} \end{cases}$$

die Indikatorfunktion von g (beziehungsweise der Menge $\{g\}$) bezeichnet. Versieht man diesen Vektorraum zusätzlich mit der durch

$$1_g * 1_h = 1_{gh} \quad \text{für alle } g, h \in G$$

eindeutig bestimmten bilinearen Verknüpfung, so wird er zu einer $\mathbb{C}$ -Algebra. Diese Algebra wird *Gruppenalgebra* zu G genannt.

Hecke-Algebren entstehen als Verallgemeinerungen von Gruppenalgebren dadurch, dass als Basis des zu betrachtenden $\mathbb{C}$ -Vektorraums Indikatorfunktionen nicht zu Gruppenelementen, sondern zu Nebenklassen betrachtet werden. Nachfolgend werden die hierbei verwendeten Bezeichnungen eingeführt.

1.1.1 BEZEICHNUNGEN: Ist G eine (multiplikativ geschriebene) Gruppe, so führt man für beliebige $g \in G$ und $M, N \subseteq G$ die Bezeichnungen

$$\begin{aligned} Mg &= \{mg \mid m \in M\}, \\ gN &= \{gn \mid n \in N\}, \\ MN &= \{mn \mid m \in M, n \in N\} \end{aligned}$$

ein. Ist U eine Untergruppe von G , so heißt Ug die *Rechtsnebenklasse* von g bezüglich U ; analog wird gU als *Links-* und UgU als *Doppelnebenklasse* bezeichnet. Ist M eine Vereinigung von Rechtsnebenklassen bezüglich U , so bezeichnet

$$U \backslash M = \{Ug \mid g \in M\}$$

die Menge der in M enthaltenen Rechtsnebenklassen (die aufgrund der Voraussetzung, dass U eine Untergruppe ist, paarweise disjunkt

sind). Analog definiert man $M // U$ und $U \backslash M // U$ als Menge der in M enthaltenen Links- beziehungsweise Doppelnebenklassen, wenn M eine Vereinigung solcher Nebenklassen ist.

Mit $|M|$ für eine beliebige Menge M wird die Kardinalität von M bezeichnet. Insbesondere steht also $|U \backslash M|$ für die Anzahl der in M enthaltenen verschiedenen Rechtsnebenklassen bezüglich U , falls M eine Vereinigung solcher Rechtsnebenklassen ist. Analoge Bezeichnungen werden auch für die Anzahlen von Links- beziehungsweise Doppelnebenklassen verwendet.

Ist $\mathfrak{M}$ ein System von paarweise disjunkten Mengen (etwa eine Nebenklassenmenge), so bedeutet die Bezeichnung $x :: \mathfrak{M}$, dass x ein *Vertretersystem* der Mengen in $\mathfrak{M}$ durchläuft, also für jede in $\mathfrak{M}$ enthaltene Menge M genau einmal einen (nicht näher bestimmten) Wert aus M annimmt. $\diamond$

Mit den gerade eingeführten Bezeichnungen lässt sich nun der Übergang von der Gruppenalgebra zur Hecke-Algebra vollziehen. Würde man dabei allerdings in natürlicher Weise das Produkt zweier Indikatorfunktionen 1_{Ug} und 1_{Uh} durch $1_{Ug} * 1_{Uh} = 1_{U(gh)}$ definieren, wäre im allgemeinen Fall, nämlich wenn U kein Normalteiler von G ist, keine Wohldefiniertheit gegeben. Hier wird dieses Problem nicht durch die Forderung gelöst, dass U ein Normalteiler sein soll; statt dessen definiert man nicht beliebige Produkte der Form $1_{Ug} * 1_{Uh}$, sondern nur solche vom Typ $(1_{Ug_1} + \dots + 1_{Ug_m}) * 1_{Uh}$, bei denen es ein $g \in G$ gibt, das $1_{Ug_1} + \dots + 1_{Ug_m} = 1_{UgU}$ erfüllt. Dann kann nämlich die natürliche Definition $(1_{Ug_1} + \dots + 1_{Ug_m}) * 1_{Uh} = 1_{Ug_1h} + \dots + 1_{Ug_mh}$ ohne Wohldefiniertheitsprobleme vorgenommen werden, wie das folgende Lemma zeigt.

1.1.2 LEMMA: Sei G eine Gruppe und U eine Untergruppe von G sowie $g, h \in G$ und $h' \in Uh$. Weiter gebe es $g_1, \dots, g_r, g'_1, \dots, g'_r \in UgU$, so dass

$$UgU = Ug_1 \cup \dots \cup Ug_r = Ug'_1 \cup \dots \cup Ug'_r$$

gilt, wobei die Notation mit $\dot{\cup}$ ausdrücken soll, dass alle vereinigten Mengen paarweise disjunkt sind. Unter diesen Voraussetzungen ist

$$Ug_1h \dot{\cup} \dots \dot{\cup} Ug_rh = Ug'_1h' \dot{\cup} \dots \dot{\cup} Ug'_rh'$$

erfüllt. ◇

BEWEIS:

vergleiche [Fre83] nach IV.1.5 (S. 228) □

Dieses Lemma liefert die Begründung dafür, dass nachher Indikatorfunktionen zu Doppelnebenklassen – und nicht zu Rechtsnebenklassen – als Basiselemente der zu konstruierenden Hecke-Algebra herangezogen werden. Dies hat jedoch zur Folge, dass verlangt werden muss, dass die zu betrachtenden Doppelnebenklassen UgU nur aus endlich vielen Rechtsnebenklassen bestehen, da in der obigen Definition von $1_{UgU} * 1_{Uh}$ das Auftreten unendlicher Summen vermieden werden soll. Vor der formalen Einführung des Hecke-Produkts wird daher zunächst ein Kriterium zur Überprüfung dieser Bedingung vorgestellt.

1.1.3 LEMMA: Sei G eine Gruppe, U eine Untergruppe von G und $g \in G$. Dann gilt $|U \parallel UgU| = |U \cap g^{-1}Ug \parallel U|$, also lässt sich UgU genau dann als Vereinigung endlich vieler Rechtsnebenklassen bezüglich U darstellen, wenn $|U \cap g^{-1}Ug \parallel U|$ endlich ist. ◇

BEWEIS:

Sind $u, v \in U$ mit $Ugu = Ug v$, so gibt es ein $w \in U$ mit $gu = wgv$. Mit dieser Wahl von w folgt $g^{-1}wg = uv^{-1} \in U$. Setzt man nun also $x = g^{-1}wg$, so ist $x \in U$ und $x \in g^{-1}Ug$, und es gilt $xv = u$, woraus die Gleichheit der Rechtsnebenklassen $(U \cap g^{-1}Ug)u$ und $(U \cap g^{-1}Ug)v$ folgt. Demzufolge ist die Abbildungsvorschrift

$$\begin{aligned} \varphi : U \parallel UgU &\rightarrow U \cap g^{-1}Ug \parallel U, \\ Ugu &\mapsto (U \cap g^{-1}Ug)u \quad \text{für jedes } u \in U, \end{aligned}$$

wohldefiniert. Die so erklärte Abbildung φ ist injektiv, da für $u, v \in U$ mit $(U \cap g^{-1}Ug)u = (U \cap g^{-1}Ug)v$ die Existenz eines $y \in U \cap g^{-1}Ug$ mit $u = yv$ folgt und man insbesondere $gu = gyv \in gg^{-1}Ugv = Ug v$ und somit $Ugu = Ug v$ erhält. Die Surjektivität von φ schließlich ist klar, da man für jedes beliebige $u \in U$ die Nebenklasse Ugu als Urbild von $(U \cap g^{-1}Ug)u$ hat. Insgesamt ist φ also eine Bijektion, was die Behauptung beweist. $\square$

Es folgt die angekündigte Definition des Hecke-Produktes.

1.1.4 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Sei G eine Gruppe und U eine Untergruppe von G . Weiter stehe M für ein Untermonoid von G mit $U \subseteq M$ und der Eigenschaft, dass es für alle $g \in M$ ein $m \in \mathbb{N} = \{1, 2, \dots\}$ und $g_1, \dots, g_m \in M$ gibt mit

$$UgU = Ug_1 \dot{\cup} \dots \dot{\cup} Ug_m.$$

Es bezeichne $[g]$ die Doppelnebenklasse UgU , und die Indikatorfunktionen $\llbracket g \rrbracket, \llbracket g \rrbracket_R, \llbracket g \rrbracket_L : G \rightarrow \mathbb{C}$ seien definiert durch

$$\llbracket g \rrbracket(h) = \begin{cases} 1, & \text{falls } h \in UgU, \\ 0 & \text{sonst} \end{cases}$$

und

$$\llbracket g \rrbracket_R(h) = \begin{cases} 1, & \text{falls } h \in Ug, \\ 0 & \text{sonst,} \end{cases} \quad \llbracket g \rrbracket_L(h) = \begin{cases} 1, & \text{falls } h \in gU, \\ 0 & \text{sonst.} \end{cases}$$

Für $g, g_1, \dots, g_m, h \in M$ mit $[g] = Ug_1 \dot{\cup} \dots \dot{\cup} Ug_m$ (also mit anderen Worten $\llbracket g \rrbracket = \llbracket g_1 \rrbracket_R + \dots + \llbracket g_m \rrbracket_R$) setze

$$\llbracket g \rrbracket * \llbracket h \rrbracket_R = \llbracket g_1 h \rrbracket_R + \dots + \llbracket g_m h \rrbracket_R,$$

und erhalte durch bilineare Fortsetzung eine Verknüpfung, die insbesondere $f_1 * f_2$ für zwei Elemente f_1 und f_2 aus H erklärt, wobei H

den $\mathbb{C}$ -Vektorraum, der von der Menge $\{\llbracket g \rrbracket \mid g \in M\}$ erzeugt wird, bezeichnet. Zuletzt definiere das Maß $\mu(V) := |U \backslash V|$ für alle Teilmengen V von G , die sich als Vereinigungen von Rechtsnebenklassen bezüglich U schreiben lassen. $\diamond$

Die folgende Bemerkung stellt eine alternative Möglichkeit der Definition von $*$ vor.

1.1.5 BEMERKUNG: Die Bezeichnungen aus 1.1.4 seien hier übernommen. Für alle Funktionen $f_1, f_2 \in H$ gilt dann

$$(f_1 * f_2)(g) = \int_G f_1(gt^{-1})f_2(t) \, d\mu(t),$$

wobei die rechte Seite ein Integral im allgemeinen maßtheoretischen Sinne bezeichnet, da μ ein Maß auf der σ -Algebra aller Teilmengen von G ist, die Vereinigungen von Rechtsnebenklassen bezüglich U sind.

Die Definition als eine solche Faltung ist insbesondere dann von Interesse, wenn auf G ein Haar-Maß existiert, von dem μ eine Vergrößerung darstellt. Dies ist beispielsweise der Fall, wenn man G als allgemeine lineare Gruppe über dem Körper der p -adischen Zahlen und U als allgemeine lineare Gruppe über dem Ring der ganzen p -adischen Zahlen wählt. Genauer zu diesem maßtheoretischen Zugang (insbesondere ein Beweis der hier behaupteten Gleichheit) kann in [Enso4] nachgelesen werden. $\diamond$

Bevor nun H als Hecke-Algebra definiert werden kann, muss zunächst sichergestellt sein, dass die Verknüpfung $f_1 * f_2$ zweier Elemente von H wieder ein Element in H liefert und die Verknüpfung assoziativ ist. Dies ist neben einer weiteren wichtigen Eigenschaft dieser Verknüpfung Inhalt des folgenden Lemmas.

1.1.6 LEMMA: Es seien die Bezeichnungen aus 1.1.4 übernommen.

- a) Für alle $f_1, f_2 \in H$ gilt $f_1 * f_2 \in H$.
- b) Für alle $f_1, f_2, f_3 \in H$ gilt $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$.
- c) Ist e das neutrale Element von G , so gilt $f * \llbracket e \rrbracket = f = \llbracket e \rrbracket * f$ für alle $f \in H$. $\diamond$

BEWEIS:

[Fre83] IV.1.7 (S. 228) $\square$

Der Frage nach der Kommutativität von $*$ wird später in diesem Abschnitt noch nachgegangen (vergleiche 1.1.12). Zunächst soll nun jedoch die Hecke-Algebra formal eingeführt werden.

1.1.7 DEFINITION (Hecke-Algebra): Die Bezeichnungen aus 1.1.4 seien hier übernommen. Die Menge H zusammen mit $*$ und den üblichen Verknüpfungen auf $\mathbb{C}$ -Vektorräumen von Funktionen heißt *Hecke-Algebra* zum *Hecke-Tripel* (G, M, U) . Diese Algebra (und auch die Menge H) wird mit $H(G, M, U)$ bezeichnet. $\diamond$

Eine alternative Definition von H beschreibt dieses als Menge aller Funktionen $f : G \rightarrow \mathbb{C}$, die $f(ugv) = f(g)$ für alle $g \in G$ und $u, v \in U$ erfüllen, und für die der sogenannte Träger Vereinigung endlicher vieler Doppelnebenklassen der Form $[h]$ für $h \in M$ ist. Da auch in einigen der folgenden Untersuchungen der Träger eine Rolle spielt, wird hier eine formale Definition gegeben und dann sein Verhalten unter der Verknüpfung $*$ betrachtet.

1.1.8 DEFINITION (Träger): Ist (G, M, U) ein Hecke-Tripel und $f \in H(G, M, U)$, so definiert man den *Träger* von f als

$$\{g \in G \mid f(g) \neq 0\}$$

und bezeichnet ihn mit $\text{Tr } f$. $\diamond$

Eigenschaften des Trägers der Verknüpfung zweier Elemente aus der Hecke-Algebra beschreibt das folgende Lemma.

1.1.9 LEMMA: Mit den Bezeichnungen aus 1.1.4 gilt für Funktionen $f_1, f_2 \in H$ stets

$$\text{Tr}(f_1 * f_2) \subseteq (\text{Tr } f_1)(\text{Tr } f_2).$$

Ist zusätzlich $f_i(g) \geq 0$ für alle $i \in \{1, 2\}$ und $g \in M$ erfüllt, so gilt sogar

$$\text{Tr}(f_1 * f_2) = (\text{Tr } f_1)(\text{Tr } f_2),$$

insbesondere gilt für alle $g, h \in M$, dass $\llbracket g \rrbracket * \llbracket h \rrbracket$ den Träger $UgUhU$ hat. $\diamond$

BEWEIS:

Sei $f_1 = a_1 \llbracket g_1 \rrbracket_{\mathbb{R}} + \cdots + a_m \llbracket g_m \rrbracket_{\mathbb{R}}$ und $f_2 = b_1 \llbracket h_1 \rrbracket_{\mathbb{R}} + \cdots + b_n \llbracket h_n \rrbracket_{\mathbb{R}}$ mit $a_i \neq 0$ und $b_j \neq 0$ für alle $1 \leq i \leq m$ und $1 \leq j \leq n$. Dann ist $f_1 * f_2$ eine Summe von Funktionen der Form $a_i b_j \llbracket g_i h_j \rrbracket_{\mathbb{R}}$ mit Träger $Ug_i h_j$, wobei $Ug_i \subseteq \text{Tr } f_1$ und $h_j \in \text{Tr } f_2$ gilt. Daraus folgt die erste Teilaussage, nämlich $\text{Tr}(f_1 * f_2) \subseteq (\text{Tr } f_1)(\text{Tr } f_2)$.

Nun sei zusätzlich $f_1 \geq 0$ und $f_2 \geq 0$ angenommen, was äquivalent dazu ist, dass in obiger Darstellung von f_1 und f_2 alle auftretenden Koeffizienten a_i und b_j positiv sind. Sei weiter $k_1 \in \text{Tr } f_1$ und $k_2 \in \text{Tr } f_2$. Dann gibt es ein $1 \leq i \leq m$ und ein $1 \leq j \leq n$, so dass $k_1 \in Ug_i$ und $k_2 \in Uh_j$ gilt. Wähle $u \in U$ so, dass $k_2 = uh_j$ erfüllt ist. Da $g_i u \in [g_i] \subseteq \text{Tr } f_1$ gilt, gibt es ein $1 \leq r \leq m$ mit $g_i u \in Ug_r$. Es folgt $k_1 k_2 \in Ug_i u h_j = Ug_r h_j$, also $(f_1 * f_2)(k_1 k_2) \geq a_r b_j > 0$, da $a_r > 0$ und $b_j > 0$ vorausgesetzt wurde und auch sonst in der Darstellung von $f_1 * f_2$ als Linearkombination von Indikatorfunktionen nur positive Koeffizienten auftraten. Aus $(f_1 * f_2)(k_1 k_2) > 0$ erhält man die Beziehung $k_1 k_2 \in \text{Tr}(f_1 * f_2)$, woraus sich die Behauptung ergibt, da $k_1 \in \text{Tr } f_1$ und $k_2 \in \text{Tr } f_2$ beliebig gewählt waren. $\square$

Für viele Zwecke genügt es nicht, nur den Träger von $f_1 * f_2$ zu kennen, sondern man benötigt oft noch zusätzlich Informationen über

die genauen Funktionswerte – unter anderem deshalb, weil die Funktionswerte nach 1.1.6 (a) und der Definition von H als Koeffizienten in der Darstellung von $f_1 * f_2$ als Linearkombination von (paarweise verschiedenen) Indikatorfunktionen des Typs $\llbracket g \rrbracket$ für $g \in M$ auftreten. Das folgende Lemma stellt Formeln zur Berechnung dieser Funktionswerte beziehungsweise Koeffizienten für die elementaren Produkte der Form $\llbracket g_1 \rrbracket * \llbracket g_2 \rrbracket$ für $g_1, g_2 \in M$ vor.

1.1.10 LEMMA: Es seien die Bezeichnungen aus 1.1.4 übernommen und $g, g_1, \dots, g_m, h, h_1, \dots, h_n \in M$, so dass $\llbracket g \rrbracket = \llbracket g_1 \rrbracket_R + \dots + \llbracket g_m \rrbracket_R$ und $\llbracket h \rrbracket = \llbracket h_1 \rrbracket_R + \dots + \llbracket h_n \rrbracket_R$ gilt. Dann hat man

$$\begin{aligned} (\llbracket g \rrbracket * \llbracket h \rrbracket)(k) &= |\{(i, j) \mid g_i h_j \in Uk, 1 \leq i \leq m, 1 \leq j \leq n\}| \\ &= |\{(g', h') \mid Uk = Ug'h', g' :: U \setminus \llbracket g \rrbracket, h' :: U \setminus \llbracket h \rrbracket\}| \end{aligned}$$

und

$$\begin{aligned} \mu([k])(\llbracket g \rrbracket * \llbracket h \rrbracket)(k) &= |\{(i, j) \mid g_i h_j \in UkU, 1 \leq i \leq m, 1 \leq j \leq n\}| \\ &= |\{(g', h') \mid UkU = Ug'h'U, g' :: U \setminus \llbracket g \rrbracket, \\ &\quad h' :: U \setminus \llbracket h \rrbracket\}| \end{aligned}$$

für alle $k \in M$. ◇

BEWEIS:

[Kri90] 1.4.4 (S. 14 f.) □

Als nächstes soll in diesem Abschnitt die schon früher angesprochene Frage nach der Kommutativität von Hecke-Algebren untersucht werden. Zur Formulierung eines hinreichenden Kriteriums wird der Begriff des Antiautomorphismus benötigt.

1.1.11 DEFINITION (Antiautomorphismus): Es sei G eine Gruppe. Eine bijektive Abbildung $\varphi : G \rightarrow G$ heißt *Antiautomorphismus*, wenn $\varphi(gh) = \varphi(h)\varphi(g)$ für alle $g, h \in G$ gilt. ◇

Wenn nun auf G ein Antiautomorphismus existiert, der gewisse Bedingungen erfüllt, kann die Kommutativität der Hecke-Algebra gefolgert werden.

1.1.12 SATZ: Es seien die Bezeichnungen aus 1.1.4 übernommen. Existiert ein Antiautomorphismus $\varphi : G \rightarrow G$, der $\varphi(U) = U$ und $[\varphi(g)] = [g]$ für alle $g \in M$ erfüllt, so ist die Hecke-Algebra $H(G, M, U)$ kommutativ. $\diamond$

BEWEIS:

[Kri90] I.7.2 (S. 27)

□

Bislang wurde fast ausschließlich die Zerlegung von Doppelnebenklassen in Rechtsnebenklassen betrachtet. Da gegebenenfalls auch die Zerlegung in Linksnebenklassen von Interesse ist, wird noch eine Charakterisierung der Existenz eines simultanen Vertretersystems von $U \backslash UgU$ und $UgU // U$ angegeben.

1.1.13 LEMMA: Es seien die Bezeichnungen aus 1.1.4 übernommen und $g \in M$ gegeben. Gilt dann für die Mächtigkeiten von Vertretersystemen $|U \backslash UgU| = |UgU // U|$, so gibt es $g_1, \dots, g_m \in M$ mit

$$Ug_1 \dot{\cup} \dots \dot{\cup} Ug_m = UgU = g_1U \dot{\cup} \dots \dot{\cup} g_mU. \quad \diamond$$

BEWEIS:

[Fre83] IV.1.9 (S. 230)

□

§ 1.2

DEDEKIND-RINGE

Die Hecke-Algebren, die in den nachfolgenden Kapiteln genauer untersucht werden sollen, sind allesamt Matrixgruppen über sogenannten Dedekind-Ringen, die eine Verallgemeinerung von Ganzheitsringen algebraischer Zahlkörper darstellen. In diesem Abschnitt

werden deshalb Dedekind-Ringe formal definiert und ihre wichtigsten Eigenschaften aufgeführt; schließlich wird noch auf das später verwendete Konzept der Lokalisierung eingegangen. Da dazu Begriffe und Bezeichnungen aus der allgemeinen Idealtheorie über Integritätsringen benötigt werden, folgt zunächst eine kurze Zusammenfassung, die vor allem die hier verwendete Notation einführen soll.

1.2.1 DEFINITION: Sei $\mathfrak{o}$ ein Integritätsring und K dessen Quotientenkörper. Eine nichtleere Teilmenge $\mathfrak{a} \subseteq \mathfrak{o}$ heißt *ganzes Ideal* von K oder Ideal in $\mathfrak{o}$, wenn für alle $a, b \in \mathfrak{a}$ und $r \in \mathfrak{o}$ stets $a + b \in \mathfrak{a}$ und $ra \in \mathfrak{a}$ folgt. Die Mengen der Form $\{ca \mid a \in \mathfrak{a}\}$ für ein ganzes Ideal $\mathfrak{a} \neq \{0\}$ und ein $c \in K \setminus \{0\}$ heißen (*gebrochene*) *Ideale* von K . Die Menge aller gebrochenen Ideale von K wird mit $\mathfrak{I}(K)$ bezeichnet.

Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von K und $c \in K$, so sei

$$\begin{aligned} c\mathfrak{a} &= \{ca \mid a \in \mathfrak{a}\}, \\ \mathfrak{a} + \mathfrak{b} &= \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}, \\ \mathfrak{a} \cdot \mathfrak{b} &= \sum_{\substack{a \in \mathfrak{a} \\ b \in \mathfrak{b}}} ab\mathfrak{o}. \end{aligned}$$

Die Summe $\mathfrak{a} + \mathfrak{b}$ heißt auch *größter gemeinsamer Teiler* von $\mathfrak{a}$ und $\mathfrak{b}$. Unter dem größten gemeinsamen Teiler zweier Elemente $a, b \in K$ wird die Summe $a\mathfrak{o} + b\mathfrak{o}$ verstanden. Ist der größte gemeinsame Teiler zweier Ideale oder Elemente von K gleich $\mathfrak{o}$, so heißen die Ideale oder Elemente *teilerfremd*. Mit $\mathfrak{a}^{-1}$ für $\mathfrak{a} \neq \{0\}$ schließlich wird das gebrochene Ideal von K bezeichnet, das der Bedingung $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$ genügt.

Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$, so heißt $N_{\mathfrak{o}}(\mathfrak{a}) := |\mathfrak{o} // \mathfrak{a}|$ (wenn man $\mathfrak{o}$ und $\mathfrak{a}$ als additive Gruppen auffasst) die *Norm* von $\mathfrak{a}$. Wenn klar ist, auf welchen Ring die Norm bezogen ist, wird die vereinfachte Schreibweise $N(\mathfrak{a})$ verwendet. Der Ring $\mathfrak{o}$ heißt *normendlich*, wenn $N(\mathfrak{a})$ für jedes Ideal $\mathfrak{a}$ in $\mathfrak{o}$ endlich ist.

Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von K , zu denen es ein Ideal $\mathfrak{c}$ von $\mathfrak{o}$ mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ gibt, so heißt $\mathfrak{b}$ *Teiler* von $\mathfrak{a}$, was mit $\mathfrak{b} \mid \mathfrak{a}$ bezeichnet wird. Wie üblich bedeutet dann $\mathfrak{b} \nmid \mathfrak{a}$, dass $\mathfrak{b}$ kein Teiler von $\mathfrak{a}$ ist. Gilt bei $\mathfrak{b} \mid \mathfrak{a}$ zusätzlich noch $\mathfrak{b} \neq \mathfrak{a}$, so heißt $\mathfrak{b}$ *echter Teiler* von $\mathfrak{a}$. Dies wird mit $\mathfrak{b} \parallel \mathfrak{a}$ bezeichnet. Die hier definierten Begriffe werden auf Elemente von K übertragen, indem man $a \in K$ durch $a\mathfrak{o}$ ersetzt.

Ein Ideal $\mathfrak{a}$ von K heißt *Hauptideal*, wenn es ein $a \in K$ gibt mit $\mathfrak{a} = a\mathfrak{o}$. Die Menge aller von $\{0\}$ verschiedenen Hauptideale von K wird mit $\mathfrak{H}(K)$ bezeichnet. Ist $\mathfrak{b}$ ein Ideal von K , so heißt $\mathfrak{b}\mathfrak{H}(K)$ (als Teilmenge der multiplikativen Gruppe $\mathfrak{I}(K)$) die *Idealklasse* von $\mathfrak{b}$, und die Menge aller Idealklassen in $\mathfrak{I}(K)$, also $\mathfrak{I}(K) \parallel \mathfrak{H}(K)$, wird mit $\mathfrak{C}(K)$ bezeichnet und heißt *Klassengruppe* von K . Die *Klassenzahl* von K schließlich ist definiert als die Mächtigkeit von $\mathfrak{C}(K)$ und wird mit $h(K)$ bezeichnet.

Ein Ideal $\mathfrak{p}$ von $\mathfrak{o}$, das $\mathfrak{p} \neq \{0\}$ und $\mathfrak{p} \neq \mathfrak{o}$ erfüllt, heißt *Primideal*, wenn für alle $a, b \in \mathfrak{o}$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ gilt.

Die multiplikative Gruppe $\{a \in \mathfrak{o} \mid a\mathfrak{o} = \mathfrak{o}\}$ schließlich heißt *Einheitengruppe* von $\mathfrak{o}$ und wird mit $\mathfrak{o}^*$ bezeichnet. $\diamond$

Die nun folgende Definition von Dedekind-Ringen ist eine von verschiedenen äquivalenten Formulierungen (vergleiche etwa [Koc97] nach Satz 3.1.1 (S. 63) und Satz 3.4.1 (S. 69)).

1.2.2 DEFINITION (Dedekind-Ring): Ist $\mathfrak{o}$ ein Integritätsring, so wird er *Dedekind-Ring* genannt, wenn die folgenden beiden Bedingungen erfüllt sind:

- (i) Jedes Ideal $\mathfrak{a} \neq \{0\}$ im Quotientenkörper K von $\mathfrak{o}$ besitzt eine Darstellung der Form

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_m^{v_m}$$

mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$ und Exponenten $v_i \in \mathbb{Z} \setminus \{0\}$, und diese Darstellung ist bis auf Reihenfolge der $\mathfrak{p}_i$ eindeutig.

- (ii) Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale in $\mathfrak{o}$, so gilt $\mathfrak{a} \subseteq \mathfrak{b}$ genau dann, wenn $\mathfrak{b} \mid \mathfrak{a}$ gilt (also ein Ideal $\mathfrak{c}$ in $\mathfrak{o}$ existiert mit $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$). $\diamond$

Die Betrachtung von Dedekind-Ringen wurde durch die folgende wichtige Beispielklasse motiviert.

1.2.3 SATZ: Ist K ein algebraischer Zahlkörper und $\mathfrak{o}$ dessen Ganzheitsring, so ist $\mathfrak{o}$ ein Dedekind-Ring mit Quotientenkörper K . $\diamond$

BEWEIS:

[Neu92] 1(3.1) (S. 18 f.) zusammen mit [Koc97] nach Satz 3.1.1 (S. 63) und Satz 3.4.1 (S. 69) $\square$

Die Eindeutigkeit der Primidealzerlegung in Dedekind-Ringen gibt Anlass zur Definition von Vielfachheiten.

1.2.4 DEFINITION (Vielfachheit): Sei $\mathfrak{o}$ ein Dedekind-Ring, K dessen Quotientenkörper und $\mathfrak{a}$ ein Ideal in K mit Primidealzerlegung wie in 1.2.2 (i). Dann definiert man $v_{p_i}(\mathfrak{a}) = v_i$ für alle $1 \leq i \leq m$ und $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ für alle Primideale $\mathfrak{p}$ von $\mathfrak{o}$, die nicht unter den $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ vorkommen. Man nennt $v_{\mathfrak{p}}(\mathfrak{a})$ die *Vielfachheit* von $\mathfrak{p}$ in $\mathfrak{a}$. Für alle $a \in K$ definiert man $v_{\mathfrak{p}}(a)$, die Vielfachheit von $\mathfrak{p}$ in a , durch $v_{\mathfrak{p}}(a\mathfrak{o})$.

Für beliebige Ideale $\mathfrak{b}$ in $\mathfrak{o}$ definiert man die Vielfachheit von $\mathfrak{b}$ in einem Ideal $\mathfrak{a}$ von K durch $\sup\{i \in \mathbb{Z} \mid \mathfrak{b}^i \text{ teilt } \mathfrak{a}\}$ und bezeichnet sie mit $v_{\mathfrak{b}}(\mathfrak{a})$. Wie oben überträgt man die Definition auf Elemente von K , indem man von diesen Elementen zu den von ihnen erzeugten Hauptidealen übergeht. $\diamond$

Der Vollständigkeit halber sei an dieser Stelle bemerkt, dass es nun für Primideale $\mathfrak{p}$ zwei verschiedene Definitionen der $\mathfrak{p}$ -Vielfachheit gibt, wobei diese aber gleichwertig sind.

Für die Vielfachheiten gelten Rechenregeln, die das folgende Lemma zusammenfasst.

1.2.5 LEMMA: Sei $\mathfrak{o}$ ein Dedekind-Ring mit Quotientenkörper K und $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Weiter seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale von K . Dann gilt:

- a) $v_{\mathfrak{p}}(\mathfrak{a}_1 \cdots \mathfrak{a}_n) = v_{\mathfrak{p}}(\mathfrak{a}_1) + \cdots + v_{\mathfrak{p}}(\mathfrak{a}_n)$.
- b) $v_{\mathfrak{p}}(\mathfrak{a}_1^{-1}) = -v_{\mathfrak{p}}(\mathfrak{a}_1)$.
- c) $v_{\mathfrak{p}}(\mathfrak{a}_1 + \cdots + \mathfrak{a}_n) = \min\{v_{\mathfrak{p}}(\mathfrak{a}_1), \dots, v_{\mathfrak{p}}(\mathfrak{a}_n)\}$.
- d) Es gilt $\mathfrak{a}_1 \mid \mathfrak{a}_2$ genau dann, wenn $v_{\mathfrak{q}}(\mathfrak{a}_1) \leq v_{\mathfrak{q}}(\mathfrak{a}_2)$ für alle Primideale $\mathfrak{q}$ von $\mathfrak{o}$ gilt.
- e) $v_{\mathfrak{p}}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n) = \max\{v_{\mathfrak{p}}(\mathfrak{a}_1), \dots, v_{\mathfrak{p}}(\mathfrak{a}_n)\}$.

Die Aussagen (a) und (b) gelten auch, wenn die $\mathfrak{a}_i$ durch Elemente a_i von K ersetzt werden, die Aussage (c) muss bei dieser Ersetzung zu $v_{\mathfrak{p}}(a_1 + \cdots + a_n) \geq \min\{v_{\mathfrak{p}}(a_1), \dots, v_{\mathfrak{p}}(a_n)\}$ modifiziert werden. $\diamond$

BEWEIS:

[Koc97] 3.3 (S. 67 ff.), für die Vielfachheiten bei einem Schnitt von Idealen beachte, dass sich $\mathfrak{b} \subseteq \mathfrak{a}_i$ nach der Definition von Dedekind-Ringen und Teil (d) dadurch charakterisieren lässt, dass $v_{\mathfrak{q}}(\mathfrak{b}) \geq v_{\mathfrak{q}}(\mathfrak{a}_i)$ für alle Primideale $\mathfrak{q}$ von $\mathfrak{o}$ gilt $\square$

Der Schnitt von Idealen lässt sich nach den gerade angegebenen Rechenregeln für Vielfachheiten auch durch Produkt- und Summenbildung ausdrücken.

1.2.6 LEMMA: Sei $\mathfrak{o}$ ein Dedekind-Ring und K dessen Quotientenkörper. Weiter seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale von K . Dann gilt $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}(\mathfrak{a} + \mathfrak{b})^{-1}$, und $\mathfrak{b}\mathfrak{a}^{-1} \cap \mathfrak{a}\mathfrak{b}^{-1}$ ist ein Ideal in $\mathfrak{o}$. Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale in $\mathfrak{o}$, so gilt $\mathfrak{b}\mathfrak{a}^{-1} \cap \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}$ und $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ sowie $\mathfrak{a}^{-1} \cap \mathfrak{b}^{-1} = \mathfrak{o}$ und $\mathfrak{o} \cap \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}$. $\diamond$

BEWEIS:

Für jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$ gilt

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}(\mathfrak{a} + \mathfrak{b})^{-1}) &= v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}) - \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\} \\ &= \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}, \end{aligned}$$

was $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}(\mathfrak{a} + \mathfrak{b})^{-1}$ beweist. Ebenso hat man

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{b}\mathfrak{a}^{-1} \cap \mathfrak{a}\mathfrak{b}^{-1}) &= \max\{v_{\mathfrak{p}}(\mathfrak{b}) - v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{a}) - v_{\mathfrak{p}}(\mathfrak{b})\} \\ &= |v_{\mathfrak{p}}(\mathfrak{b}) - v_{\mathfrak{p}}(\mathfrak{a})| \geq 0, \end{aligned}$$

für alle Primideale $\mathfrak{p}$ von $\mathfrak{o}$, also liegt $\mathfrak{b}\mathfrak{a}^{-1} \cap \mathfrak{a}\mathfrak{b}^{-1}$ in $\mathfrak{o}$. Falls $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale von $\mathfrak{o}$ sind, müssen auch $\mathfrak{a}^2$ und $\mathfrak{b}^2$ teilerfremd sein, also gilt $\mathfrak{a}^2 + \mathfrak{b}^2 = \mathfrak{o}$, woraus

$$\begin{aligned} \mathfrak{b}\mathfrak{a}^{-1} \cap \mathfrak{a}\mathfrak{b}^{-1} &= \mathfrak{b}\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b}^{-1}(\mathfrak{b}\mathfrak{a}^{-1} + \mathfrak{a}\mathfrak{b}^{-1})^{-1} = (\mathfrak{b}\mathfrak{a}^{-1} + \mathfrak{a}\mathfrak{b}^{-1})^{-1} \\ &= \mathfrak{a}\mathfrak{b}(\mathfrak{b}^2 + \mathfrak{a}^2)^{-1} = \mathfrak{a}\mathfrak{b}\mathfrak{o}^{-1} = \mathfrak{a}\mathfrak{b} \end{aligned}$$

folgt. Weiter hat man hier $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}(\mathfrak{a} + \mathfrak{b})^{-1} = \mathfrak{a}\mathfrak{b}\mathfrak{o}^{-1} = \mathfrak{a}\mathfrak{b}$ wegen $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$, und genauso berechnet man

$$\begin{aligned} \mathfrak{a}^{-1} \cap \mathfrak{b}^{-1} &= \mathfrak{a}^{-1}\mathfrak{b}^{-1}(\mathfrak{a}^{-1} + \mathfrak{b}^{-1})^{-1} = (\mathfrak{a}\mathfrak{b}(\mathfrak{a}^{-1} + \mathfrak{b}^{-1}))^{-1} \\ &= (\mathfrak{b} + \mathfrak{a})^{-1} = \mathfrak{o}^{-1} = \mathfrak{o}. \end{aligned}$$

Schließlich hat man noch

$$\begin{aligned} \mathfrak{o} \cap \mathfrak{a}\mathfrak{b}^{-1} &= \mathfrak{o}\mathfrak{a}\mathfrak{b}^{-1}(\mathfrak{o} + \mathfrak{a}\mathfrak{b}^{-1})^{-1} = (\mathfrak{a}^{-1}\mathfrak{b}(\mathfrak{o} + \mathfrak{a}\mathfrak{b}^{-1}))^{-1} \\ &= (\mathfrak{a}^{-1}(\mathfrak{b} + \mathfrak{a}))^{-1} = (\mathfrak{a}^{-1}\mathfrak{o})^{-1} = \mathfrak{a} \end{aligned}$$

was auch die letzte Behauptung beweist. $\square$

Dedekind-Ringe müssen nicht zwangsläufig Hauptidealringe sein, was bedeutet, dass im allgemeinen nicht jedes Ideal von $\mathfrak{o}$ durch genau ein Element erzeugt ist. Man kann jedoch zeigen, dass man immer mit zwei Erzeugern auskommen kann. Grundlage dafür ist das folgende allgemeinere Resultat.

1.2.7 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring. Weiter seien $\mathfrak{a}$ und $\mathfrak{b}$ von $\{0\}$ verschiedene Ideale in $\mathfrak{o}$. Dann gibt es ein $a \in \mathfrak{a}$ mit $a\mathfrak{b} + a\mathfrak{o} = \mathfrak{a}$ und $a\mathfrak{b} \cap a\mathfrak{o} = a\mathfrak{b}$. $\diamond$

BEWEIS:

[Koc97] Satz 3.3.5 (S. 69) $\square$

Eine Spezialisierung liefert nun den angekündigten Zwei-Erzeuger-Satz.

1.2.8 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring, K dessen Quotientenkörper und $\mathfrak{a}$ ein Ideal von K sowie $a_1 \in \mathfrak{a} \setminus \{0\}$. Dann gibt es ein $a_2 \in \mathfrak{a}$, das $a_1\mathfrak{o} + a_2\mathfrak{o} = \mathfrak{a}$ erfüllt. $\diamond$

BEWEIS:

Wähle gemäß [Koc97] Satz 3.2.2 (S. 65) ein $m \in K$, so dass $m\mathfrak{a}$ ein ganzes Ideal ist. Da wegen $a_1 \in \mathfrak{a}$ das Ideal $a_1\mathfrak{a}^{-1}$ ganz ist, liefert die erste Aussage aus 1.2.7 ein $a \in m\mathfrak{a}$ mit $(m\mathfrak{a})(a_1\mathfrak{a}^{-1}) + a\mathfrak{o} = m\mathfrak{a}$, also $ma_1\mathfrak{o} + a\mathfrak{o} = m\mathfrak{a}$. Die Wahl $a_2 = m^{-1}a$ beweist dann die Behauptung wegen $a_1\mathfrak{o} + a_2\mathfrak{o} = m^{-1}(ma_1\mathfrak{o} + a\mathfrak{o}) = m^{-1}m\mathfrak{a} = \mathfrak{a}$. $\square$

Wie in allen Ringen gilt auch in Dedekind-Ringen ein chinesischer Restsatz. Da nach 1.2.6 der Schnitt teilerfremder Ideale mit ihrem Produkt übereinstimmt, hat man hier auch eine Fassung für Produkte von Idealen.

1.2.9 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring. Weiter seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ paarweise teilerfremde Ideale von $\mathfrak{o}$ sowie $a_1, \dots, a_n \in \mathfrak{o}$. Dann gibt es ein $a \in \mathfrak{o}$ mit

$$\{x \in \mathfrak{o} \mid x \in \mathfrak{a}_i + \mathfrak{a}_i \text{ für alle } 1 \leq i \leq n\} = a + \mathfrak{a}_1 \cdots \mathfrak{a}_n. \quad \diamond$$

BEWEIS:

Dies ist eine leichte Umformulierung von [Koc97] Satz 3.6.3 (S. 73). $\square$

Für spätere Beweise werden noch bestimmte von einem Dedekind-Ring abgeleitete Ringe benötigt.

1.2.10 DEFINITION (Lokalisierung): Sei $\mathfrak{o}$ ein Dedekind-Ring mit Quotientenkörper K und $\mathfrak{M}$ eine endliche Menge von Primidealen von $\mathfrak{o}$. Dann heißt

$$\mathfrak{o}_{\mathfrak{M}} := \{x \in K \mid v_p(x) \geq 0 \text{ für alle } p \in \mathfrak{M}\}$$

die *Lokalisierung* von $\mathfrak{o}$ an $\mathfrak{M}$. Für Primideale p von $\mathfrak{o}$ setzt man abkürzend $\mathfrak{o}_p = \mathfrak{o}_{\{p\}}$. $\diamond$

Das folgende Lemma beinhaltet die wichtigsten Eigenschaften von Lokalisierungen.

1.2.11 LEMMA: Sei $\mathfrak{o}$ Dedekind-Ring mit Quotientenkörper K und $\mathfrak{M}$ eine endliche Menge Primidealen von $\mathfrak{o}$.

- a) Die Menge $\mathfrak{o}_{\mathfrak{M}}$ ist eine Teilmenge von K und mit den dadurch induzierten Verknüpfungen ein Hauptidealring.
- b) Für jedes $a \in K$ gilt

$$a\mathfrak{o}_{\mathfrak{M}} = \{u \in K \mid v_p(u) \geq v_p(a) \text{ für alle } p \in \mathfrak{M}\}.$$

- c) Für $a, b \in K$ gilt $a\mathfrak{o}_{\mathfrak{M}} = b\mathfrak{o}_{\mathfrak{M}}$ genau dann, wenn $v_p(a) = v_p(b)$ für alle $p \in \mathfrak{M}$ erfüllt ist. Weiter gilt $a\mathfrak{o}_{\mathfrak{M}} \mid b\mathfrak{o}_{\mathfrak{M}}$ genau dann, wenn $v_p(a) \leq v_p(b)$ für alle $p \in \mathfrak{M}$ erfüllt ist.
- d) Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}_{\mathfrak{M}}$ und $\mathfrak{b}$ ein gebrochenes Ideal in K , so ist $\mathfrak{a} \cap \mathfrak{b}$ ein gebrochenes Ideal in K oder gleich $\{0\}$. Ist $a \in K$ so gewählt, dass $\mathfrak{a} = a\mathfrak{o}_{\mathfrak{M}}$ gilt, so hat man $v_p(\mathfrak{a} \cap \mathfrak{b}) = \max\{v_p(a), v_p(\mathfrak{b})\}$ für alle $p \in \mathfrak{M}$ und $v_p(\mathfrak{a} \cap \mathfrak{b}) = v_p(\mathfrak{b})$ für alle Primideale p von $\mathfrak{o}$ mit $p \notin \mathfrak{M}$.
- e) Für alle $a \in \mathfrak{o}$ und Primideale p von $\mathfrak{o}$ gilt $v_p(a\mathfrak{o}_p \cap \mathfrak{o}) = v_p(a)$.

1 Grundlagen

- f) Ist $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$ und $\mathfrak{a}$ ein Ideal von $\mathfrak{o}_{\mathfrak{p}}$ mit $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) \geq 0$, so gibt es ein $a \in \mathfrak{o}$ mit $\mathfrak{a} = a\mathfrak{o}_{\mathfrak{p}}$.
- g) Ist $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$, und sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von $\mathfrak{o}_{\mathfrak{p}}$ mit $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) \geq 0$ und $v_{\mathfrak{p}}(\mathfrak{b} \cap \mathfrak{o}) \geq 0$, so gilt $\mathfrak{a} = \mathfrak{b}$ genau dann, wenn $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) = v_{\mathfrak{p}}(\mathfrak{b} \cap \mathfrak{o})$ erfüllt ist. Weiter ist $\mathfrak{a} \mid \mathfrak{b}$ äquivalent zu $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) \leq v_{\mathfrak{p}}(\mathfrak{b} \cap \mathfrak{o})$.
- h) Ist $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$, und sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von $\mathfrak{o}_{\mathfrak{p}}$ mit $v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) \geq 0$ und $v_{\mathfrak{p}}(\mathfrak{b} \cap \mathfrak{o}) \geq 0$, so gilt

$$v_{\mathfrak{p}}((\mathfrak{a}\mathfrak{b}) \cap \mathfrak{o}) = v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{o}) + v_{\mathfrak{p}}(\mathfrak{b} \cap \mathfrak{o}).$$

- i) Sind $a_1, \dots, a_n$ aus $\mathfrak{o}$ gegeben, so hat man

$$v_{\mathfrak{p}}((a_1\mathfrak{o}_{\mathfrak{p}} + \dots + a_n\mathfrak{o}_{\mathfrak{p}}) \cap \mathfrak{o}) = \min\{v_{\mathfrak{p}}(a_1), \dots, v_{\mathfrak{p}}(a_n)\}$$

für alle Primideale $\mathfrak{p}$ von $\mathfrak{o}$.

◇

BEWEIS:

- a) [Koc97] Satz 3.7.2 (S. 75)

- b) Anwendung der Definition von $\mathfrak{o}_{\mathfrak{M}}$ im Fall $a \neq 0$ liefert

$$\begin{aligned} a\mathfrak{o}_{\mathfrak{M}} &= \{ax \mid x \in K \text{ mit } v_{\mathfrak{p}}(x) \geq 0 \text{ für alle } \mathfrak{p} \in \mathfrak{M}\} \\ &= \{u \in K \mid v_{\mathfrak{p}}(\frac{u}{a}) \geq 0 \text{ für alle } \mathfrak{p} \in \mathfrak{M}\} \\ &\stackrel{1.2.5}{=} \{u \in K \mid v_{\mathfrak{p}}(u) - v_{\mathfrak{p}}(a) \geq 0 \text{ für alle } \mathfrak{p} \in \mathfrak{M}\} \\ &= \{u \in K \mid v_{\mathfrak{p}}(u) \geq v_{\mathfrak{p}}(a) \text{ für alle } \mathfrak{p} \in \mathfrak{M}\}, \end{aligned}$$

und für $a = 0$ sind wegen $v_{\mathfrak{p}}(0) = \infty$ beide Seiten der behaupteten Gleichung gleich $\{0\}$.

c) Man hat

$$\begin{aligned}
 a\mathfrak{o}_{\mathfrak{M}} &= b\mathfrak{o}_{\mathfrak{M}} && \stackrel{(b)}{\Leftrightarrow} \\
 \{u \in K \mid v_p(u) \geq v_p(a) \text{ für alle } p \in \mathfrak{M}\} \\
 &= \{u \in K \mid v_p(u) \geq v_p(b) \text{ für alle } p \in \mathfrak{M}\} && \Leftrightarrow \\
 v_p(a) &= v_p(b) \text{ für alle } p \in \mathfrak{M},
 \end{aligned}$$

und

$$\begin{aligned}
 a\mathfrak{o}_{\mathfrak{M}} &\mid b\mathfrak{o}_{\mathfrak{M}} && \stackrel{(b)}{\Leftrightarrow} \\
 \{u \in K \mid v_p(u) \geq v_p(a) \text{ für alle } p \in \mathfrak{M}\} \\
 &\supseteq \{u \in K \mid v_p(u) \geq v_p(b) \text{ für alle } p \in \mathfrak{M}\} && \Leftrightarrow \\
 v_p(a) &\leq v_p(b) \text{ für alle } p \in \mathfrak{M}.
 \end{aligned}$$

d) Da $\mathfrak{o}_{\mathfrak{M}}$ nach Teil (a) ein Hauptidealring ist, existiert zu a stets ein $\mathfrak{a} \in \mathfrak{o}_{\mathfrak{M}} \subseteq K$ mit $\mathfrak{a} = a\mathfrak{o}_{\mathfrak{M}}$. Dann gilt

$$\mathfrak{a} = a\mathfrak{o}_{\mathfrak{M}} \stackrel{(b)}{=} \{u \in K \mid v_p(u) \geq v_p(a) \text{ für alle } p \in \mathfrak{M}\},$$

also

$$\mathfrak{a} \cap \mathfrak{b} = \{u \in \mathfrak{b} \mid v_p(u) \geq v_p(a) \text{ für alle } p \in \mathfrak{M}\}.$$

Nun ist $u \in \mathfrak{b}$ nach 1.2.5 gleichbedeutend mit $\mathfrak{b} \mid u\mathfrak{o}$ und damit äquivalent dazu, dass $v_p(u) \geq v_p(\mathfrak{b})$ für alle Primideale p von $\mathfrak{o}$ gilt. Somit besteht $\mathfrak{a} \cap \mathfrak{b}$ genau aus den Elementen u von K , für die $v_p(u) \geq v_p(a)$ für alle $p \in \mathfrak{M}$ und $v_p(u) \geq v_p(\mathfrak{b})$ für alle Primideale p von $\mathfrak{o}$ gilt. Dies beweist alle Behauptungen.

e) Die Aussage erhält man mit $\mathfrak{b} = \mathfrak{o}$ und $\mathfrak{M} = \{p\}$ aus Teil (d), indem man $v_p(a) \geq 0$ und $v_p(\mathfrak{o}) = 0$ benutzt.

f) Da $\mathfrak{o}_p$ nach Teil (a) ein Hauptidealring ist, gibt es ein $a' \in K$ mit $\mathfrak{a} = a'\mathfrak{o}_p$. Nun setze $v = v_p(a')$ und wähle ein a aus $\mathfrak{p}^v \setminus \mathfrak{p}^{v+1}$. Da nach Teil (e) $v = v_p(a') = v_p(a'\mathfrak{o}_p \cap \mathfrak{o}) = v_p(\mathfrak{a} \cap \mathfrak{o})$ gilt und

$v_p(a \cap \mathfrak{o}) \geq 0$ nach Voraussetzung erfüllt ist, liegt a dann in $\mathfrak{o}$, und es gilt weiter $v_p(a) = v = v_p(a')$ und somit nach Teil (c) $a\mathfrak{o}_p = a'\mathfrak{o}_p = \mathfrak{a}$, was die Behauptung beweist.

g) Nach Teil (f) gibt es $a, b \in \mathfrak{o}$ mit $\mathfrak{a} = a\mathfrak{o}_p$ und $\mathfrak{b} = b\mathfrak{o}_p$, und nach Teil (e) gilt dann $v_p(\mathfrak{a} \cap \mathfrak{o}) = v_p(a)$ und $v_p(\mathfrak{b} \cap \mathfrak{o}) = v_p(b)$, so dass man mit Teil (c) die Behauptungen erhält.

h) Nach Teil (f) gibt es $a, b \in \mathfrak{o}$ mit $\mathfrak{a} = a\mathfrak{o}_p$ und $\mathfrak{b} = b\mathfrak{o}_p$. Nun folgt

$$\begin{aligned} v_p((\mathfrak{ab}) \cap \mathfrak{o}) &= v_p((ab\mathfrak{o}_p) \cap \mathfrak{o}) \stackrel{(e)}{=} v_p(ab) = v_p(a) + v_p(b) \\ &\stackrel{(e)}{=} v_p(a\mathfrak{o}_p \cap \mathfrak{o}) + v_p(b\mathfrak{o}_p \cap \mathfrak{o}) \\ &= v_p(\mathfrak{a} \cap \mathfrak{o}) + v_p(\mathfrak{b} \cap \mathfrak{o}). \end{aligned}$$

i) Da $\mathfrak{o}_p$ nach Teil (a) ein Hauptidealring ist, gibt es ein $a_0 \in \mathfrak{o}_p$ mit $a_1\mathfrak{o}_p + \dots + a_n\mathfrak{o}_p = a_0\mathfrak{o}_p$. Nun ist nach Teil (b)

$$a_i\mathfrak{o}_p = \{u \in K \mid v_p(u) \geq v_p(a_i)\}$$

für alle $0 \leq i \leq n$. Nach Wahl von a_0 gilt $a_i \in a_0\mathfrak{o}_p$ und damit auch $v_p(a_i) \geq v_p(a_0)$ für alle $1 \leq i \leq n$, also

$$v_p(a_0) \leq \min\{v_p(a_1), \dots, v_p(a_n)\}.$$

Nach Wahl von a_0 gibt es darüberhinaus $a'_1, \dots, a'_n$ mit $a'_i \in a_i\mathfrak{o}_p$ für alle $1 \leq i \leq n$ und $a_0 = a'_1 + \dots + a'_n$. Damit erhält man nach 1.2.5 zunächst $v_p(a_0) \geq \min\{v_p(a'_1), \dots, v_p(a'_n)\}$, und da $a'_i \in a_i\mathfrak{o}_p$ und somit $v_p(a'_i) \geq v_p(a_i)$ für alle $1 \leq i \leq n$ gilt, kann man weiter $\min\{v_p(a'_1), \dots, v_p(a'_n)\} \geq \min\{v_p(a_1), \dots, v_p(a_n)\}$ abschätzen. Dies zeigt

$$v_p(a_0) \geq \min\{v_p(a_1), \dots, v_p(a_n)\},$$

also hat man insgesamt

$$\min\{v_p(a_1), \dots, v_p(a_n)\} = v_p(a_0) \stackrel{(e)}{=} v_p(a_0\mathfrak{o}_p \cap \mathfrak{o}),$$

was die Behauptung beweist. □

KAPITEL ZWEI

HECKE-ALGEBREN ZU UNIMODULAREN GRUPPEN

In diesem Kapitel wird für beliebige Dedekind-Ringe $\mathfrak{o}$ die Struktur von Hecke-Algebren $H(G, M, U)$ untersucht, bei denen U die Menge aller invertierbaren Matrizen über $\mathfrak{o}$ mit einem vorgeschriebenem Format ist. Diese Algebren stellen eine Verallgemeinerung der in [Hei90] betrachteten Hecke-Algebren dar.

§ 2.1

WOHLDEFINIERTHEIT

In diesem Abschnitt werden die zur Definition der zu betrachtenden Hecke-Algebren nötigen Bezeichnungen eingeführt und dann diese Algebren auf Wohldefiniertheit untersucht. Zunächst werden dazu die hier verwendeten Notationen für Matrizen vorgestellt.

2.1.1 BEZEICHNUNGEN: Es sei $\mathfrak{o}$ ein Integritätsring. Sind $m, n \in \mathbb{N}$, so bezeichnet $\mathfrak{o}^{m \times n}$ die Menge der Matrizen mit m Zeilen und n Spalten mit Einträgen in $\mathfrak{o}$, also die Menge der $(m \times n)$ -Matrizen über $\mathfrak{o}$.

Ist $A \in \mathfrak{o}^{m \times n}$, so definiert man $(A)_{IJ}$ für Mengen $I \subseteq \{1, \dots, m\}$ und $J \subseteq \{1, \dots, n\}$ als diejenige Matrix, die aus A entsteht, indem man alle Zeilen streicht, deren Nummern nicht I vorkommen, und alle Spalten streicht, deren Nummern nicht in J vorkommen. Weiter bezeichnet $(A)_{ij}$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ den Eintrag von A im Schnittpunkt der i -ten Zeile mit der j -ten Spalte.

Das Symbol A^T steht für die Transponierte und A^{adj} für die Adjunkte einer Matrix A .

Der Rang einer Matrix $A \in \mathfrak{o}^{m \times n}$, also das maximale $r \in \mathbb{N}_0$ (wobei $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$) mit $r \leq n$, für das es ein $J \subseteq \{1, \dots, n\}$ mit $|J| = r$ gibt, so dass die Spalten von $(A)_{IJ}$ für $I = \{1, \dots, m\}$ linear unabhängig sind, wird mit $\text{Rang } A$ bezeichnet. Ist $A \in \mathfrak{o}^{n \times n}$ eine quadratische Matrix, so steht $\det A$ für die Determinante von A .

Für $n \in \mathbb{N}$ bezeichnet man die $(n \times n)$ -Einheitsmatrix mit E_n und definiert die *allgemeine lineare Gruppe* $\text{GL}_n(\mathfrak{o})$ durch

$$\begin{aligned} \text{GL}_n(\mathfrak{o}) &= \{A \in \mathfrak{o}^{n \times n} \mid \exists A' \in \mathfrak{o}^{n \times n} : AA' = E_n\} \\ &= \{A \in \mathfrak{o}^{n \times n} \mid \det A \in \mathfrak{o}^*\}. \end{aligned}$$

Zuletzt wird noch das Monoid $\text{IL}_n(\mathfrak{o})$ durch

$$\text{IL}_n(\mathfrak{o}) = \{A \in \mathfrak{o}^{n \times n} \mid \det A \neq 0\}$$

definiert. ◇

Nun werden die in diesem Abschnitt benötigten Grundvoraussetzungen angegeben.

2.1.2 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Sei $\mathfrak{o}$ ein normendlicher Dedekind-Ring und K dessen Quotientenkörper. Setze $G_n = \text{GL}_n(K)$ und $I_n = \text{IL}_n(\mathfrak{o})$ sowie $U_n = \text{GL}_n(\mathfrak{o})$ für jedes $n \in \mathbb{N}$ und

$$U_n[\mathfrak{a}] = \{M \in U_n \mid M - E_n \in \mathfrak{a}^{n \times n}\}$$

für alle $n \in \mathbb{N}$ und Ideale $\mathfrak{a}$ in $\mathfrak{o}$. ◇

Für den Beweis, dass (G_n, I_n, U_n) ein Hecke-Tripel ist, wird gezeigt, dass jede Hauptkongruenzgruppe $U_n[\mathfrak{a}]$ in U_n endlichen Index hat und jede Untergruppe vom Typ $U_n \cap A^{-1}U_nA$ für $A \in I_n$ eine Hauptkongruenzgruppe enthält, so dass dann mit 1.1.3 die Behauptung gefolgt werden kann.

2.1.3 LEMMA: Es seien die Bezeichnungen aus 2.1.2 übernommen und $n \in \mathbb{N}$. Für jedes Ideal $\mathfrak{a}$ von $\mathfrak{o}$ ist dann $|U_n[\mathfrak{a}] \backslash U_n| < \infty$. $\diamond$

BEWEIS:

Die Abbildung

$$\varphi : U_n \rightarrow \mathrm{GL}_n(\mathfrak{o} // \mathfrak{a}), \quad M \mapsto M + \mathfrak{a}^{n \times n}$$

ist ein Gruppenhomomorphismus: Dass $\varphi(MN) = \varphi(M)\varphi(N)$ für alle $M, N \in U_n$ gilt, erhält man sofort, indem man die Einträge des Matrixprodukts betrachtet, also ist nur noch die Wohldefiniertheit der Abbildung zu beweisen, wofür hier genügt, für jedes $M \in U_n$ die Invertierbarkeit von $M + \mathfrak{a}^{n \times n}$ in $(\mathfrak{o} // \mathfrak{a})^{n \times n}$ zu zeigen. Aus

$$(M + \mathfrak{a}^{n \times n})(M^{-1} + \mathfrak{a}^{n \times n}) = E_n + \mathfrak{a}^{n \times n}$$

erhält man diese direkt.

Nach dem Homomorphiesatz ist nun $\mathrm{Kern} \varphi \backslash U_n \cong \mathrm{Bild} \varphi$, und da $\mathrm{Kern} \varphi = \{M \in U_n \mid M + \mathfrak{a}^{n \times n} = E_n + \mathfrak{a}^{n \times n}\} = U_n[\mathfrak{a}]$ gilt, folgt

$$|U_n[\mathfrak{a}] \backslash U_n| = |\mathrm{Bild} \varphi| \leq |\mathrm{GL}_n(\mathfrak{o} // \mathfrak{a})| \leq |(\mathfrak{o} // \mathfrak{a})^{n \times n}| = |\mathfrak{o} // \mathfrak{a}|^{n^2} < \infty$$

wegen der Normendlichkeit von $\mathfrak{o}$. $\square$

Nun kann die Wohldefiniertheit von $H(G_n, I_n, U_n)$ bewiesen werden.

2.1.4 SATZ: Es seien die Bezeichnungen aus 2.1.2 übernommen und $n \in \mathbb{N}$. Dann ist (G_n, I_n, U_n) ein Hecke-Tripel. $\diamond$

BEWEIS:

Es genügt zu zeigen, dass $U_n A U_n$ für jedes $A \in I_n$ in endlich viele Rechtsnebenklassen bezüglich U_n zerfällt, da die anderen Eigenschaften eines Hecke-Tripels für (G_n, I_n, U_n) klarerweise erfüllt sind.

Sei $A \in I_n$ und $m = \det A$. Jedes $M \in U_n[m\mathfrak{o}]$ besitzt eine Darstellung der Form $M = E_n + mM'$ für ein $M' \in \mathfrak{o}^{n \times n}$. Damit folgt

$$A M A^{-1} = A(E_n + mM')A^{-1} = E_n + AM'mA^{-1},$$

wobei $E_n + AM'mA^{-1}$ zu $\mathfrak{o}^{n \times n}$ gehört, da mA^{-1} als Adjunkte von A auch zu $\mathfrak{o}^{n \times n}$ gehört und alle anderen auftretenden Matrizen ebenfalls in $\mathfrak{o}^{n \times n}$ liegen. Es ist also $A M A^{-1} \in \mathfrak{o}^{n \times n}$. Wegen

$$\det(A M A^{-1}) = (\det A)(\det M)(\det A)^{-1} = \det M \stackrel{M \in U_n}{\in} \mathfrak{o}^*$$

liegt $A M A^{-1}$ sogar in U_n , und es folgt daraus $M \in A^{-1}U_n A$. Da M ein beliebiges Element von $U_n[m\mathfrak{o}]$ war, zeigt dies $U_n[m\mathfrak{o}] \subseteq A^{-1}U_n A$, und da $U_n[m\mathfrak{o}] \subseteq U_n$ gilt, hat man auch $U_n[m\mathfrak{o}] \subseteq U_n \cap A^{-1}U_n A$. Zusammen mit $|U_n[m\mathfrak{o}] \setminus U_n| < \infty$ nach 2.1.3 folgt dann erst recht $|U_n \cap A^{-1}U_n A \setminus U_n| < \infty$, und da A ein beliebiges Element von I_n war, ergibt sich mit 1.1.3 die Behauptung. $\square$

§ 2.2

GRUNDLAGEN DER ELEMENTARTEILERTHEORIE

Aus der Definition von Produkten von Elementen von Hecke-Algebren ist ersichtlich, dass Charakterisierungen der Gleichheit von Doppelnebenklassen für Strukturuntersuchungen hilfreich sein können. Für den Fall der in diesem Kapitel zu untersuchenden Hecke-Algebren zu unimodularen Matrixgruppen erhält man ein solches Kriterium aus der Elementarteilertheorie. Nachfolgend werden die benötigten Aussagen dieser Theorie für Dedekind-Ringe vorgestellt. Die Begriffe und

Resultate sind größtenteils den Arbeiten [Ste12], [Fra34] und [Kru32] entnommen.

Grundlegend für die Einführung von Elementarteilern ist das Konzept der Ableitung einer Matrix.

2.2.1 DEFINITION (Ableitung): Fixiere für alle $k, n \in \mathbb{N}$ mit $k \leq n$ eine Aufzählung $I_{n,k,1}, \dots, I_{n,k,\binom{n}{k}}$ der k -elementigen Teilmengen von $\{1, \dots, n\}$. Bezeichne $\mathfrak{o}$ einen Dedekind-Ring und K dessen Quotientenkörper. Sei $A \in K^{m \times n}$ und $1 \leq k \leq \min\{m, n\}$. Die Matrix $B \in K^{\binom{m}{k} \times \binom{n}{k}}$ mit

$$(B)_{zs} = \det((A)_{I_{m,k,z}, I_{n,k,s}}) \quad \text{für alle } 1 \leq z \leq \binom{m}{k} \text{ und } 1 \leq s \leq \binom{n}{k}$$

heißt k -te *Ableitung* von A und wird auch mit $A^{[k]}$ bezeichnet. $\diamond$

Mit diesem Konzept lassen sich nun Determinantenteiler und davon abgeleiteten Begriffe wie Elementarteiler definieren.

2.2.2 DEFINITION (Determinantenteiler): Die Bezeichnungen aus 2.2.1 seien übernommen. Der größte gemeinsame Teiler

$$\sum_{\substack{1 \leq z \leq \binom{m}{k} \\ 1 \leq s \leq \binom{n}{k}}} (A^{[k]})_{zs} \mathfrak{o} = \sum_{\substack{1 \leq z \leq \binom{m}{k} \\ 1 \leq s \leq \binom{n}{k}}} (\det(A)_{I_{m,k,z}, I_{n,k,s}}) \mathfrak{o}$$

aller Einträge von $A^{[k]}$ heißt k -ter *Determinantenteiler* von A und wird mit $\mathfrak{d}_k(A)$ bezeichnet. Weiter definiert man $\mathfrak{d}_i(A) = \mathfrak{o}$ für alle $i \leq 0$ und $\mathfrak{d}_j(A) = \{0\}$ für alle $j > \min\{m, n\}$.

Für alle $k \in \mathbb{Z}$ mit $\mathfrak{d}_k(A) \neq \{0\}$ definiere $\mathfrak{e}_k(A) = \mathfrak{d}_k(A) \mathfrak{d}_{k-1}(A)^{-1}$ und $\mathfrak{f}_k(A) = \mathfrak{e}_k(A) \mathfrak{e}_{k-1}(A)^{-1}$ und setze weiter $\mathfrak{e}_k(A) = \{0\}$ sowie $\mathfrak{f}_k(A) = \{0\}$ für alle $k \in \mathbb{Z}$ mit $\mathfrak{d}_k(A) = \{0\}$. Dann heißt $\mathfrak{e}_k(A)$ der k -te *Elementarteiler* und $\mathfrak{f}_k(A)$ der k -te *Grundfaktor* von A . $\diamond$

Es sei bemerkt, dass mit diesen Bezeichnungen $\mathfrak{d}_1(A) = \mathfrak{e}_1(A) = \mathfrak{f}_1(A)$ der größte gemeinsame Teiler der Einträge von A ist, da man $A^{[1]}$ aus A durch Zeilen- und Spaltenvertauschungen erhalten kann.

Da Dedekind-Ringe nicht zwangsläufig Hauptidealringe sein müssen, werden für die spätere Anwendung neben den gerade definierten noch zwei weitere Begriffe benötigt.

2.2.3 DEFINITION (Zeilenklasse, Spaltenklasse): Seien die Bezeichnungen aus 2.2.1 übernommen, $r = \text{Rang } A$ und $1 \leq i \leq \binom{m}{r}$ so gewählt, dass die i -te Zeile von $A^{[r]}$ nicht die Nullzeile ist. Dann heißt

$$\left(\sum_{k=1}^{\binom{m}{r}} (A^{[r]})_{ik} \mathfrak{o} \right) \cdot \mathfrak{H}(K)$$

die *Zeilenklasse* von A und wird mit $\mathfrak{Z}(A)$ bezeichnet. Ist $1 \leq j \leq \binom{n}{r}$ so gewählt, dass die j -te Spalte von $A^{[r]}$ nicht die Nullspalte ist, dann heißt

$$\left(\sum_{k=1}^{\binom{n}{r}} (A^{[r]})_{kj} \mathfrak{o} \right) \cdot \mathfrak{H}(K)$$

die *Spaltenklasse* von A und wird mit $\mathfrak{S}(A)$ bezeichnet. ◇

Zunächst noch einige Anmerkungen zur Wohldefiniertheit: Da die Matrix $A^{[r]}$ von den gewählten Anordnungen $I_{n,k,1}, I_{n,k,2}, \dots$ abhängt, wird gefordert, dass bei jedem Auftreten eines solchen Ausdrucks dieselbe Anordnung gewählt wird. Um welche es sich konkret handelt, ist für das Folgende nicht relevant. Bei den Determinantenteilern (und damit auch bei den Elementarteilern und Grundfaktoren) ist das Ideal $\mathfrak{d}_k(A)$ (genauso $\mathfrak{e}_k(A)$ und $\mathfrak{f}_k(A)$) unabhängig von der konkreten Anordnung der Einträge von $A^{[k]}$; deshalb sind diese Ideale sogar ohne weitere Einschränkungen wohldefiniert. Zuletzt kann man zeigen, dass Zeilenklasse und Spaltenklasse von A unabhängig von der Wahl der Zeile i beziehungsweise der Spalte j sind (und dass es stets vom Nullvektor verschiedene Zeilen und Spalten gibt), so dass auch diese Begriffe wohldefiniert sind (vergleiche etwa [Ste12] § 2, 11. (S. 331)).

Der nachfolgende Satz fasst nun einige der grundlegenden Eigenschaften der gerade neu eingeführten Begriffe zusammen, beschränkt sich

dabei jedoch auf den uns hier interessierenden Fall von quadratischen Matrizen.

2.2.4 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring, K dessen Quotientenkörper, $n \in \mathbb{N}$ und $A \in K^{n \times n}$ vom Rang r . Dann gilt:

- a) $\mathfrak{d}_k(A) = \mathfrak{d}_1(A^{[k]})$ für alle $1 \leq k \leq n$.
- b) $\mathfrak{d}_r(A) \neq \{0\}$, $\mathfrak{e}_r(A) \neq \{0\}$ und $\mathfrak{f}_r(A) \neq \{0\}$.
- c) $\mathfrak{d}_k(A) = \mathfrak{e}_k(A) = \mathfrak{f}_k(A) = \{0\}$ für alle $k > r$.
- d) $(\det A)\mathfrak{o} = \mathfrak{d}_n(A) = \mathfrak{e}_1(A) \cdots \mathfrak{e}_n(A)$
 $= \mathfrak{f}_1(A)^n \mathfrak{f}_2(A)^{n-1} \cdots \mathfrak{f}_{n-1}(A)^2 \mathfrak{f}_n(A).$
- e) Ist $r = n$, so gilt $\mathfrak{Z}(A) = \mathfrak{S}(A) = \mathfrak{H}(K)$.
- f) $\mathfrak{e}_k(A) \mid \mathfrak{e}_{k+1}(A)$ für alle $k \in \mathbb{Z}$.
- g) Ist $A \in \mathfrak{o}^{n \times n}$, so sind alle Grundfaktoren, Elementarteiler und Determinantenteiler von A Ideale in $\mathfrak{o}$.
- h) Gibt es $s, t \in \mathbb{N}$, so dass A von der Form $\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$ ist für ein $B \in K^{s \times t}$ und ein $C \in K^{(n-s) \times (n-t)}$, so gilt $\mathfrak{Z}(A) = \mathfrak{Z}(B) \cdot \mathfrak{Z}(C)$.
- i) Für alle $B \in K^{n \times n}$ und $1 \leq k \leq r$ gilt $A^{[k]}B^{[k]} = (AB)^{[k]}$. ◇

BEWEIS:

Die Aussagen (a)–(e) sind einfache Folgerungen aus den Definitionen, (f) und (h) findet man in [Kru32] nach Satz 10 (S. 25), Teil (g) folgt aus den Definitionen und Teil (f), und (i) ist der Satz von Binet-Cauchy ([Ait69] 39. (S. 92)). □

Die Bedeutung der Elementarteilertheorie für die Behandlung von Hecke-Algebren besteht – wie schon zu Anfang dieses Abschnitts erwähnt – darin, dass sich mit Hilfe der Elementarteiler charakterisieren lässt, wann zwei Doppelnebenklassen bezüglich $\mathrm{GL}_n(\mathfrak{o})$ übereinstimmen.

2.2.5 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring, K dessen Quotientenkörper, $n \in \mathbb{N}$ und $A, B \in K^{n \times n}$. Dann sind äquivalent:

- (i) Es gibt $P, Q \in \mathrm{GL}_n(\mathfrak{o})$ mit $B = PAQ$.
- (ii) Es gilt $\mathfrak{z}(A) = \mathfrak{z}(B)$, und für alle $1 \leq k \leq n$ ist $\mathfrak{e}_k(A) = \mathfrak{e}_k(B)$.

Falls $\mathrm{Rang} A = n$ gilt (also A in $\mathrm{GL}_n(K)$ liegt), ist (i) bereits äquivalent dazu, dass $\mathfrak{e}_k(A) = \mathfrak{e}_k(B)$ für alle $1 \leq k \leq n$ gilt.

Sämtliche Aussagen gelten genauso, wenn man überall $\mathfrak{e}_k$ durch $\mathfrak{d}_k$ oder überall $\mathfrak{e}_k$ durch $\mathfrak{f}_k$ ersetzt. $\diamond$

BEWEIS:

[Kru32] Satz 11 (S. 25) für die Äquivalenz von (i) und (ii), der Zusatz für $\mathrm{Rang} A = n$ folgt mit 2.2.4 (e), die Möglichkeit des Übergangs zu Determinantenteilern oder Grundfaktoren ergibt sich direkt aus den Definitionen. $\square$

Aus diesem Satz lassen sich mehrere wichtige Folgerungen ziehen.

2.2.6 FOLGERUNG: Sei $\mathfrak{o}$ ein Dedekind-Ring und K dessen Quotientenkörper. Ist $A \in \mathrm{GL}_n(K)$, so liegt A^T in der Doppelnebenklasse $\mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})$. $\diamond$

BEWEIS:

Da die Determinante invariant unter Transposition ist, enthalten für jedes $1 \leq k \leq n$ die Matrizen $A^{[k]}$ und $(A^T)^{[k]}$ dieselben Einträge (wenn auch an verschiedenen Stellen). Daraus folgt

$$\mathfrak{d}_k(A^T) = \mathfrak{d}_1((A^T)^{[k]}) = \mathfrak{d}_1(A^{[k]}) = \mathfrak{d}_k(A),$$

also auch $\mathfrak{e}_k(A^T) = \mathfrak{e}_k(A)$ für alle $1 \leq k \leq n$, so dass sich mit 2.2.5 die Behauptung ergibt. $\square$

Als Anwendung dieser Folgerung lässt sich die Kommutativität der Hecke-Algebra $H(G_n, I_n, U_n)$ feststellen.

2.2.7 SATZ: Es seien die Bezeichnungen aus 2.1.2 übernommen und $n \in \mathbb{N}$. Dann ist die Hecke-Algebra $H(G_n, I_n, U_n)$ kommutativ. $\diamond$

BEWEIS:

Betrachte die Abbildung $\varphi : G_n \rightarrow G_n, A \mapsto A^T$. Aus der elementaren Matrix-Theorie erhält man, dass diese Abbildung ein wohldefinierter Antiautomorphismus ist, der darüberhinaus $\varphi(U_n) = U_n$ erfüllt. Für jedes $A \in I_n$ gilt weiter $\varphi(A) = A^T \in U_n A U_n$ nach 2.2.6, also auch $U_n \varphi(A) U_n = U_n A U_n$, so dass man mit 1.1.12 nun die Kommutativität von $H(G_n, I_n, U_n)$ erhält. $\square$

Aus 2.2.5 erhält man eine weitere Aussage, die später bei der Bestimmung von Normalformen wichtig wird.

2.2.8 FOLGERUNG: Für $a_1, \dots, a_n, b_1, \dots, b_n \in \mathfrak{o}$ sind äquivalent:

(i) Es gilt $a_1 \mathfrak{o} + \dots + a_n \mathfrak{o} = b_1 \mathfrak{o} + \dots + b_n \mathfrak{o}$.

(ii) Es gibt eine Matrix $R \in \mathrm{GL}_n(\mathfrak{o})$ mit

$$R(a_1 \quad \dots \quad a_n)^T = (b_1 \quad \dots \quad b_n)^T. \quad \diamond$$

BEWEIS:

(ii) $\Rightarrow$ (i): Ist (ii) erfüllt, so liefert 2.2.5 die Gleichung

$$\mathfrak{e}_1((a_1 \quad \dots \quad a_n)^T) = \mathfrak{e}_1((b_1 \quad \dots \quad b_n)^T),$$

was nach Definition der Elementarteiler äquivalent zur Aussage (i) ist.

(i) $\Rightarrow$ (ii): Es gelte $a_1 \mathfrak{o} + \dots + a_n \mathfrak{o} = b_1 \mathfrak{o} + \dots + b_n \mathfrak{o}$. Nehme zunächst an, dass $b_i \neq 0$ für mindestens ein $1 \leq i \leq n$ gilt. Definiere

$$A = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ a_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \dots & 0 \end{pmatrix} \in \mathfrak{o}^{n \times n}, \quad B = \begin{pmatrix} b_1 & 0 & \dots & 0 \\ b_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_n & 0 & \dots & 0 \end{pmatrix} \in \mathfrak{o}^{n \times n}.$$

Da

$$\epsilon_1(A) = a_1\mathfrak{o} + \cdots + a_n\mathfrak{o} = b_1\mathfrak{o} + \cdots + b_n\mathfrak{o} = \epsilon_1(B)$$

nach Voraussetzung gilt, $\epsilon_k(A) = \{0\} = \epsilon_k(B)$ für alle $2 \leq k \leq n$ erfüllt ist und darüberhinaus die Zeilenklasse von A als Idealklasse des größten gemeinsamen Teilers der Einträge einer Zeile von $A^{[1]} = A$, also einer Zeile der Form $(a_i \ 0 \ \cdots \ 0)$, die Hauptklasse ist und Gleiches für B gilt, womit insbesondere $\mathfrak{Z}(A) = \mathfrak{Z}(B)$ erfüllt ist, gibt es nach 2.2.5 Matrizen $P, Q \in \mathrm{GL}_n(\mathfrak{o})$ mit $B = PAQ$, also $BQ^{-1} = PA$. Schreibe

$$Q^{-1} = \begin{pmatrix} q & \tilde{q} \\ q' & Q' \end{pmatrix} \quad \text{für } q \in \mathfrak{o}, \tilde{q} \in \mathfrak{o}^{1 \times (n-1)}, q' \in \mathfrak{o}^{(n-1) \times 1}, \\ Q' \in \mathfrak{o}^{(n-1) \times (n-1)},$$

und setze $a = (a_1 \ \cdots \ a_n)^T$ sowie $b = (b_1 \ \cdots \ b_n)^T$ und weiter $b' = (b_2 \ \cdots \ b_n)^T$. Dann gilt

$$BQ^{-1} = \begin{pmatrix} b_1 & 0 \\ b' & 0 \end{pmatrix} \begin{pmatrix} q & \tilde{q} \\ q' & Q' \end{pmatrix} = \begin{pmatrix} b_1q & b_1\tilde{q} \\ b'q & b'Q' \end{pmatrix}$$

und

$$PA = P(a \ 0) = (Pa \ 0),$$

so dass mit $BQ^{-1} = PA$ die Beziehungen

$$bq = \begin{pmatrix} b_1q \\ b'q \end{pmatrix} = Pa \quad \text{und} \quad b\tilde{q} = \begin{pmatrix} b_1\tilde{q} \\ b'Q' \end{pmatrix} = 0$$

folgen. Da nach Annahme nicht alle Einträge von b gleich 0 sind und $\mathfrak{o}$ ein Integritätsring ist, erhält man aus $b\tilde{q} = 0$, dass $\tilde{q} = 0$ gelten muss. Daher gilt nun $q \det Q' = \det Q^{-1} \in \mathfrak{o}^*$ wegen $Q^{-1} \in \mathrm{GL}_n(\mathfrak{o})$, also folgt insbesondere $q \in \mathfrak{o}^*$. Setzt man nun $R = q^{-1}P$, so gilt $R \in \mathrm{GL}_n(\mathfrak{o})$ wegen $P \in \mathrm{GL}_n(\mathfrak{o})$ und $q^{-1} \in \mathfrak{o}^*$, und aus $bq = Pa$ folgt $b = q^{-1}Pa = Ra$, was die Behauptung für diesen Fall liefert.

Es verbleibt, den Fall $b_1 = \cdots = b_n = 0$ zu betrachten. Hier muss wegen $a_1\mathfrak{o} + \cdots + a_n\mathfrak{o} = b_1\mathfrak{o} + \cdots + b_n\mathfrak{o}$ auch $a_1 = \cdots = a_n = 0$ gelten, so dass man etwa $R = E_n$ wählen kann. Dies vervollständigt den Beweis. $\square$

Für das Folgende ebenfalls von Interesse ist nun, wann zu vorgeschriebenen Elementarteilern (oder Determinantenteilern oder Grundfaktoren) und vorgeschriebener Zeilenklasse (oder Spaltenklasse) eine Matrix existiert. Dabei wird zunächst der Fall betrachtet, dass n gegebene Elementarteiler durch eine Matrix in $\mathfrak{o}^{2n \times 2n}$ realisiert werden sollen, da dies eine einfache Normalform erlaubt.

2.2.9 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring, K dessen Quotientenkörper und $n \in \mathbb{N}$. Weiter seien $\mathfrak{b}_1, \dots, \mathfrak{b}_n$ Ideale in $\mathfrak{o}$ mit $\{0\} \neq \mathfrak{b}_1 \mid \mathfrak{b}_2 \mid \dots \mid \mathfrak{b}_n$ und $\mathfrak{K}$ eine Idealklasse, wobei $\mathfrak{K} = \mathfrak{H}(K)$ gelte, falls $\mathfrak{b}_n$ nicht das Nullideal ist. Bestimme $1 \leq r \leq n$ so, dass $\mathfrak{b}_r \neq \{0\}$ und $\mathfrak{b}_k = \{0\}$ für alle $r < k \leq n$ gilt. Dann gibt es eine Matrix $A \in \mathfrak{o}^{2n \times 2n}$, die von der Form

$$A = \begin{pmatrix} a_1 & & & & 0 & \cdots & 0 \\ & b_1 & & & \vdots & & \vdots \\ & & a_2 & & & & \\ & & & b_2 & & & \\ & & & & \ddots & & \\ & & & & & a_{r-1} & \\ & & & & & & b_{r-1} \\ & & & & & a_r & c_r \\ & & & & & b_r & d_r \\ & & & & & & \vdots \\ & & & & & & \vdots \\ 0 & \cdots & & & & \cdots & 0 & \cdots & 0 \\ \vdots & & & & & & \vdots & \ddots & \vdots \\ 0 & \cdots & & & & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

ist, Zeilenklasse $\mathfrak{K}$ hat und $\mathfrak{e}_k(A) = \mathfrak{b}_k$ für alle $1 \leq k \leq n$ erfüllt. Weiter kann man fordern, dass $a_k \mathfrak{o} + b_k \mathfrak{o} = \mathfrak{b}_k$ für alle $1 \leq k < r$ gilt und die Matrix $\begin{pmatrix} a_r & c_r \\ b_r & d_r \end{pmatrix}$ vom Rang 1 ist und Zeilenklasse $\mathfrak{K}$ sowie ersten Elementarteiler $\mathfrak{b}_r$ hat; ist $\mathfrak{K} = \mathfrak{H}(K)$, darf darüberhinaus $c_r = d_r = 0$ gefordert werden. $\diamond$

BEWEIS:

[Kru32] vor Satz 11 (S. 25) für die allgemeine Form und [Kru32] nach Satz 9 (S. 24) für $c_r = d_r = 0$ falls $\mathfrak{K} = \mathfrak{H}(K)$ $\square$

Dieses Ergebnis wird nun auf die Realisierbarkeit von n vorgeschriebenen Determinantenteilern, Elementarteilern beziehungsweise Grundfaktoren in $\mathfrak{o}^{n \times n}$ übertragen. Dabei wird im folgenden nur noch auf den hier interessierenden Fall von Matrizen mit vollem Rang eingegangen.

2.2.10 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n, \mathfrak{b}_1, \dots, \mathfrak{b}_n$ und $\mathfrak{c}_1, \dots, \mathfrak{c}_n$ von $\{0\}$ verschiedene Ideale in $\mathfrak{o}$. Dann gilt:

- a) Ist $A \in \mathfrak{o}^{m \times m}$ mit $m \geq n$ eine Matrix vom Rang n mit $\mathfrak{d}_n(A) \in \mathfrak{H}(K)$ und $\mathfrak{Z}(A) = \mathfrak{H}(K)$, so gibt es eine Matrix $B \in \mathfrak{o}^{n \times n}$, die die gleichen Determinantenteiler, Elementarteiler und Grundfaktoren hat wie A .
- b) Es gibt genau dann eine Matrix $B \in \mathfrak{o}^{n \times n}$ mit $\mathfrak{e}_k(A) = \mathfrak{b}_k$ für alle $1 \leq k \leq n$, wenn $\mathfrak{b}_1 \cdots \mathfrak{b}_n$ ein Hauptideal ist und $\mathfrak{b}_{k-1} \mid \mathfrak{b}_k$ für alle $2 \leq k \leq n$ gilt.
- c) Es gibt genau dann eine Matrix $A \in \mathfrak{o}^{n \times n}$ mit $\mathfrak{d}_k(A) = \mathfrak{a}_k$ für alle $1 \leq k \leq n$, wenn $\mathfrak{a}_n$ ein Hauptideal ist und $\mathfrak{a}_{k-1}^2 \mathfrak{a}_{k-2}^{-1} \mid \mathfrak{a}_k$ für alle $2 \leq k \leq n$ gilt (dabei sei $\mathfrak{a}_0 = \mathfrak{o}$ gesetzt).
- d) Es gibt genau dann eine Matrix $C \in \mathfrak{o}^{n \times n}$ mit $\mathfrak{f}_k(A) = \mathfrak{c}_k$ für alle $1 \leq k \leq n$, wenn $\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \cdots \mathfrak{c}_{n-1}^2 \mathfrak{c}_n$ ein Hauptideal ist. $\diamond$

BEWEIS:

- a) Nach [Fra34] Satz 1 (S. 150) gilt $\mathfrak{S}(A)\mathfrak{Z}(A) = \mathfrak{d}_n(A)\mathfrak{H}(K)$, also gilt mit $\mathfrak{d}_n(A) \in \mathfrak{H}(K)$ und $\mathfrak{Z}(A) = \mathfrak{H}(A)$ auch $\mathfrak{S}(A) = \mathfrak{H}(K)$; mit [Fra34] Satz 6 (S. 155) folgt nun die Behauptung. (Die Resultate in [Fra34] sind explizit für den Fall von Ganzheitsringen algebraischer Zahlkörper formuliert, doch die Übertragung auf beliebige Dedekind-Ringe ist wortwörtlich möglich.)

- b) Die Existenz der Matrix B für gegebene $\mathfrak{b}_1, \dots, \mathfrak{b}_n$, die die genannten Bedingungen erfüllen, folgt aus 2.2.9 und Teil (a), dass umgekehrt für gegebenes B die Elementarteiler die genannten Bedingungen erfüllen, steht in 2.2.4 (d) und 2.2.4 (f)
- c) ist eine Umformulierung von Teil (b)
- d) ist eine Umformulierung von Teil (b) □

Der gerade bewiesene Satz besagt zusammen mit 2.2.5, dass es eine Bijektion zwischen den in $\text{IL}_n(\mathfrak{o})$ enthaltenen Doppelnebenklassen bezüglich $\text{GL}_n(\mathfrak{o})$ und den n -Tupeln $(\mathfrak{b}_1, \dots, \mathfrak{b}_n)$ von Idealen mit $\mathfrak{b}_1, \dots, \mathfrak{b}_n$ in $\mathfrak{o}$ mit $\mathfrak{b}_1 \mid \dots \mid \mathfrak{b}_n$ und $\mathfrak{b}_1 \cdots \mathfrak{b}_n \in \mathfrak{H}(K)$ gibt. In analoger Weise existieren auch Bijektionen zwischen diesen Doppelnebenklassen und Determinantenteilertupeln beziehungsweise Grundfaktorentupeln.

Eine weitere Anwendung von 2.2.9 liefert für jede Matrix in $\mathfrak{o}^{n \times n}$ eine Normalform, die allerdings nicht mehr im gleichen Matrixring liegt.

2.2.11 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring, $n \in \mathbb{N}$ und $A \in \mathfrak{o}^{n \times n}$ eine Matrix vom Rang n . Setze $A' = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n}$. Dann gibt es Matrizen $A_1, \dots, A_n \in \mathfrak{o}^{2 \times 2}$, wobei A_k für jedes $1 \leq k \leq n$ von der Form $\begin{pmatrix} a_k & 0 \\ b_k & 0 \end{pmatrix}$ ist mit $\mathfrak{e}_1(A_k) = \mathfrak{e}_k(A)$, so dass

$$\text{diag}(A_1, \dots, A_n) \in \text{GL}_{2n}(\mathfrak{o}) A' \text{GL}_{2n}(\mathfrak{o})$$

gilt, wobei $\text{diag}(A_1, \dots, A_n)$ die Blockdiagonalmatrix mit den Blöcken $A_1, \dots, A_n$ auf der Diagonalen bezeichnet. ◇

BEWEIS:

Anwendung von 2.2.9 unter Berücksichtigung von $\text{Rang } A = n$ und

somit $\mathfrak{e}_n(A) \neq \{0\}$ liefert die Existenz einer Matrix der Form

$$A'' = \begin{pmatrix} a_1 & & & 0 & \cdots & 0 \\ b_1 & & & \vdots & & \vdots \\ & a_2 & & & & \\ & b_2 & & & & \\ & & \ddots & & & \\ & & & a_{n-1} & & \\ & & & b_{n-1} & & \\ & & & & a_n & \vdots \\ & & & & b_n & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n},$$

die die Beziehungen $\mathfrak{e}_k(A'') = \mathfrak{e}_k(A)$ und $a_k\mathfrak{o} + b_k\mathfrak{o} = \mathfrak{e}_k(A)$ für alle $1 \leq k \leq n$ erfüllt. (Die Anwendung von 2.2.9 ist nach 2.2.4 (f) möglich.) Definiert man nun $A_i = \begin{pmatrix} a_i & 0 \\ b_i & 0 \end{pmatrix}$ für alle $1 \leq i \leq n$, so kann man $\text{diag}(A_1, \dots, A_n)$ aus A'' durch Vertauschung von Spalten erhalten, also gilt insbesondere $\text{diag}(A_1, \dots, A_n) \in A'' \text{GL}_{2n}(\mathfrak{o})$. Andererseits gilt $\mathfrak{Z}(A'') = \mathfrak{H}(K) = \mathfrak{Z}(A')$ und $\mathfrak{e}_k(A'') = \mathfrak{e}_k(A) = \mathfrak{e}_k(A')$ für alle $1 \leq k \leq n$, also erhält man mit 2.2.5, dass $A'' \in \text{GL}_{2n}(\mathfrak{o})A'\text{GL}_{2n}(\mathfrak{o})$ gilt. Insgesamt ist also

$$\text{diag}(A_1, \dots, A_n) \in A'' \text{GL}_{2n}(\mathfrak{o}) \subseteq \text{GL}_{2n}(\mathfrak{o})A' \text{GL}_{2n}(\mathfrak{o}),$$

was zu zeigen war. □

Die gerade konstruierte Normalform wird in einem späteren Abschnitt noch wichtig werden, wenn es darum geht, Aussagen über die Determinantenteiler von Produkten von Matrizen zu machen. Diese Aussagen werden benötigt, um den Träger von Produkten von Elementen der zu untersuchenden Hecke-Algebra genauer zu beschreiben.

§ 2.3

MASSFORMELN

In der Definition von Hecke-Algebren im ersten Kapitel war gefordert, dass jede Doppelnebenklasse bezüglich U Vereinigung endlich vieler Rechtsnebenklassen bezüglich U ist. In diesem Abschnitt soll es nun darum gehen, die Anzahl der benötigten Rechtsnebenklassen exakt zu berechnen. Ebenso von Interesse ist eine Formel, die für eine Doppelnebenklasse die Anzahl bestimmter ausgezeichneteter Rechtsnebenklassen angibt. Zunächst werden die Bezeichnungen für die zu berechnenden Größen eingeführt.

2.3.1 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Sei $\mathfrak{o}$ ein normendlicher Dedekind-Ring und K dessen Quotientenkörper. Für jedes $n \in \mathbb{N}$ sei $G_n = \mathrm{GL}_n(K)$ und $U_n = \mathrm{GL}_n(\mathfrak{o})$ sowie $I_n = \mathrm{IL}_n(\mathfrak{o})$. Weiter seien die sich daraus ergebenden Bezeichnungen aus 1.1.4 übernommen (mit G_n anstelle von G und U_n anstelle von U sowie I_n anstelle von M).

Ein Analogon zum Maß μ , das auf Vereinigungen von Rechtsnebenklassen bezüglich U_n definiert ist, wird nun auch für Elemente der Hecke-Algebra $H(G_n, I_n, U_n)$ eingeführt: Für jedes $A \in I_n$ definiere $\mu(\llbracket A \rrbracket) = \mu([A])$ und setze die Abbildung μ linear auf $H(G_n, I_n, U_n)$ fort. Zur Vereinfachung der Notation setze noch $\mu([A]) = \mu(A)$ für alle $A \in I_n$.

Für $A \in I_n$ und $1 \leq i \leq n$ setze weiter

$$\mathfrak{g}_i(A) = (A)_{1i}\mathfrak{o} + \cdots + (A)_{ni}\mathfrak{o},$$

und für Ideale $\mathfrak{a}$ von $\mathfrak{o}$ definiere

$$\mu_{\mathfrak{a}}(\llbracket A \rrbracket) = |\{U_n A' \mid A' \in U_n A U_n, \mathfrak{g}_1(A') = \mathfrak{a}\}| = \mu_{\mathfrak{a}}([A]) = \mu_{\mathfrak{a}}(A).$$

Setze auch die Abbildung $\mu_{\mathfrak{a}}$ linear auf $H(G_n, I_n, U_n)$ fort. $\diamond$

Die hier vorgestellte Definition von μ_a verlangt eine Anmerkung zur Wohldefiniertheit: Diese ist gegeben, da $\mathfrak{g}_1(A'') = \mathfrak{g}_1(A')$ für alle $A'' \in U_n A'$ gilt (nach 2.2.8).

Zur Abzählung der in einer Doppelnebenklasse enthaltenen verschiedenen Rechtsnebenklassen mit vorgeschriebenem größten gemeinsamen Teiler der ersten Spalte wird folgendes Vorgehen gewählt: Bestimme zunächst für jede Rechtsnebenklasse mit vorgeschriebenem größten gemeinsamen Teiler der ersten Spalte einen ausgezeichneten Vertreter (2.3.2), und zähle dann diejenigen, die in der gegebenen Doppelnebenklasse liegen (2.3.3 beziehungsweise 2.3.6). Die nachfolgenden Analysen beschränken sich dabei auf den Fall $n = 2$.

2.3.2 LEMMA: Es seien die Bezeichnungen aus 2.3.1 übernommen, $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$ und $b \in \mathfrak{a}$. Weiter sei gemäß 1.2.8 ein $a \in \mathfrak{a} \setminus \{0\}$ gewählt, das $a\mathfrak{o} + b\mathfrak{o} = \mathfrak{a}$ erfüllt, und V ein Vertretersystem von $(\mathfrak{o} \cap ab^{-1}\mathfrak{o}) // (ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o})$. Dann hat jede Rechtsnebenklasse $U_2 A$ für $A \in I_2$ mit $\mathfrak{g}_1(A) = \mathfrak{a}$ und $\mathfrak{d}_2(A) = b\mathfrak{o}$ einen eindeutig bestimmten Vertreter der Form

$$\begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix} \quad \text{für ein } c \in V.$$

Das Vertretersystem V ist endlich. ◇

BEWEIS:

Für die Eindeutigkeit des Vertreters zeige, dass für $c, d \in V$ mit

$$U_2 \underbrace{\begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix}}_{=:C} = U_2 \underbrace{\begin{pmatrix} a & d-1 \\ b & ba^{-1}d \end{pmatrix}}_{=:D}$$

stets $c = d$ gilt. Wegen $U_2 C = U_2 D$ gibt es ein $P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \in U_2$ mit

$$\begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix} = \begin{pmatrix} a & d-1 \\ b & ba^{-1}d \end{pmatrix},$$

also

$$\begin{pmatrix} p_1a + p_2b & p_1(c-1) + p_2ba^{-1}c \\ p_3a + p_4b & p_3(c-1) + p_4ba^{-1}c \end{pmatrix} = \begin{pmatrix} a & d-1 \\ b & ba^{-1}d \end{pmatrix}.$$

Daraus liest man zunächst $p_1a + p_2b = a$ und $p_3a + p_4b = b$ ab und folgert $p_2 = ab^{-1}(1 - p_1)$ sowie $p_3 = ba^{-1}(1 - p_4)$. Da die Determinanten von C und D übereinstimmen (beide sind gleich b) und $PC = D$ gilt, hat man $\det P = 1$, also $p_1p_4 - p_2p_3 = 1$. Einsetzen der Gleichungen für p_2 und p_3 liefert $p_1p_4 - (1 - p_1)(1 - p_4) = 1$, woraus nach Auflösen $p_4 = 2 - p_1$ folgt. Aus der letzten Matrixgleichung liest man weiter $p_3(c-1) + p_4ba^{-1}c = ba^{-1}d$ ab. Zusammen mit den Gleichungen für p_2 , p_3 und p_4 folgt daraus nun

$$\begin{aligned} d - c &= ab^{-1}(ba^{-1}d) - c = ab^{-1}(p_3(c-1) + p_4ba^{-1}c) - c \\ &= ab^{-1}p_3(c-1) + p_4c - c \\ &= ab^{-1}(ba^{-1}(1 - p_4))(c-1) + p_4c - c \\ &= (1 - p_4)(c-1) + p_4c - c = p_4 - 1 = (2 - p_1) - 1 \\ &= 1 - p_1 = ba^{-1}(ab^{-1}(1 - p_1)) = ba^{-1}p_2 \in ba^{-1}\mathfrak{o} \end{aligned}$$

folgt. Da c und d als Elemente von V beide in $ab^{-1}\mathfrak{o}$ liegen, gilt auch $d - c \in ab^{-1}\mathfrak{o}$, also insgesamt $d - c \in ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$. Da V als Vertretersystem modulo $ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ gewählt wurde, muss daher $d = c$ gelten.

Existenz des Vertreters: Sei $A \in I_2$ mit $\mathfrak{g}_1(A) = \mathfrak{a}$ und $\mathfrak{d}_2(A) = b\mathfrak{o}$. Da $a\mathfrak{o} + b\mathfrak{o} = \mathfrak{a} = \mathfrak{g}_1(A)$ gilt, gibt es nach 2.2.8 ein $P_1 \in U_2$ mit

$$P_1A = \begin{pmatrix} a & * \\ b & * \end{pmatrix}.$$

Setze $\varepsilon = b(\det(P_1A))^{-1}$. Wegen $\mathfrak{d}_2(P_1A) = \mathfrak{d}_2(A) = b\mathfrak{o}$ gilt dann $\varepsilon \in \mathfrak{o}^*$. Weiter sei $P_2 = \text{diag}(\varepsilon, 1) \in U_2$. Dann gilt

$$\begin{aligned} \det(P_2P_1A) &= (\det P_2) \det(P_1A) = \varepsilon \det(P_1A) \\ &= b(\det(P_1A))^{-1} \det(P_1A) = b. \end{aligned}$$

Die Ideale $\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ und $\mathfrak{o} \cap ba^{-1}\mathfrak{o}$ sind teilerfremd, denn für jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$ gilt

$$\begin{aligned} & v_{\mathfrak{p}}((\mathfrak{o} \cap ab^{-1}\mathfrak{o}) + (\mathfrak{o} \cap ba^{-1}\mathfrak{o})) \\ & \stackrel{1.2.5}{=} \min\{\max\{0, v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)\}, \max\{0, v_{\mathfrak{p}}(b) - v_{\mathfrak{p}}(a)\}\} \\ & = 0, \end{aligned}$$

also $(\mathfrak{o} \cap ab^{-1}\mathfrak{o}) + (\mathfrak{o} \cap ba^{-1}\mathfrak{o}) = \mathfrak{o}$. Nach dem chinesischen Restsatz (1.2.9) gibt es dann ein $p \in \mathfrak{o}$ mit $p \in (\mathfrak{o} \cap ba^{-1}\mathfrak{o}) + \varepsilon^{-1}$ und gleichzeitig $p \in (\mathfrak{o} \cap ab^{-1}\mathfrak{o}) + 1$. Die Matrix

$$P_3 = \begin{pmatrix} p & ab^{-1}(1 - \varepsilon p) \\ ba^{-1}(p - 1) & \varepsilon + 1 - \varepsilon p \end{pmatrix}$$

liegt in $\mathfrak{o}^{2 \times 2}$, denn aus $p \in (\mathfrak{o} \cap ba^{-1}\mathfrak{o}) + \varepsilon^{-1}$ folgt $\varepsilon p \in \varepsilon ba^{-1}\mathfrak{o} + 1$ und damit $ab^{-1}(1 - \varepsilon p) \in \varepsilon \mathfrak{o} = \mathfrak{o}$, und aus $p \in (\mathfrak{o} \cap ab^{-1}\mathfrak{o}) + 1$ folgt $p - 1 \in ab^{-1}\mathfrak{o}$ und damit $ba^{-1}(p - 1) \in \mathfrak{o}$, für die übrigen Einträge ist offensichtlich, dass sie in $\mathfrak{o}$ liegen. Darüberhinaus hat man $\det P_3 = 1$, also insbesondere $P_3 \in U_2$. Nun ist

$$\begin{aligned} P_3 P_2 P_1 A &= P_3 \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & * \\ b & * \end{pmatrix} \\ &= \begin{pmatrix} p & ab^{-1}(1 - \varepsilon p) \\ ba^{-1}(p - 1) & \varepsilon + 1 - \varepsilon p \end{pmatrix} \begin{pmatrix} a\varepsilon & * \\ b & * \end{pmatrix} \\ &= \begin{pmatrix} pa\varepsilon + a(1 - \varepsilon p) & * \\ b\varepsilon(p - 1) + \varepsilon b + b - \varepsilon pb & * \end{pmatrix} = \begin{pmatrix} a & * \\ b & * \end{pmatrix}. \end{aligned}$$

Setze $r = (P_3 P_2 P_1 A)_{12}$ und $s = (P_3 P_2 P_1 A)_{22}$, dann ist

$$as - br = \det(P_3 P_2 P_1 A) = (\det P_3) \det(P_2 P_1 A) = 1 \cdot b = b,$$

und es folgt $as = br + b = b(1 + r)$ und damit $1 + r = ab^{-1}s \in ab^{-1}\mathfrak{o}$. Da zudem $1 + r \in \mathfrak{o}$ gilt, gibt es nach Wahl von V dann ein $c \in V$ mit $1 + r \in c + (ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o})$. Setze nun

$$P_4 = \begin{pmatrix} ab^{-1}s - c + 1 & ab^{-1}(c - r - 1) \\ s - ba^{-1}c & c - r \end{pmatrix}.$$

Diese Matrix liegt in $\mathfrak{o}^{2 \times 2}$: Zunächst gilt $1 + r - c \in ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ nach Wahl von c , also ist insbesondere $ab^{-1}(c - r - 1) \in ab^{-1}(-ba^{-1}\mathfrak{o}) = \mathfrak{o}$; weiter gilt

$$\begin{aligned} ab^{-1}s - c + 1 &= (ab^{-1}s - r) + (r - c + 1) = \frac{1}{b}(as - br) + (r - c + 1) \\ &= \frac{1}{b} \cdot b + (r - c + 1), \end{aligned}$$

also liegt $ab^{-1}s - c + 1$ in $\mathfrak{o}$, da dies bereits für 1 sowie r und c gilt; ebenso liegt

$$s - ba^{-1}c = s + ba^{-1}(1 + r - c) - ba^{-1}(1 + r)$$

in $\mathfrak{o}$, denn einerseits wurde bereits $1 + r \in ab^{-1}\mathfrak{o}$ gezeigt, woraus $ba^{-1}(1 + r) \in \mathfrak{o}$ folgt, andererseits folgt aus

$$1 + r - c \in ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$$

insbesondere $ba^{-1}(1 + r - c) \in ba^{-1}(ab^{-1}\mathfrak{o}) = \mathfrak{o}$; schließlich liegt auch $c - r$ in $\mathfrak{o}$, da bereits c und r aus $\mathfrak{o}$ gewählt wurden. Man rechnet nun nach, dass

$$\det P_4 = -r + ab^{-1}s = \frac{1}{b}(as - br) = \frac{1}{b} \cdot b = 1$$

gilt, was insbesondere $P_4 \in U_2$ beweist. Dann ist $P_4P_3P_2P_1A \in U_2A$, da die Matrizen $P_1, \dots, P_4$ alle in U_2 liegen. Verwendet man zur Verkürzung der Schreibweise $t = c - r - 1$, so ist nun

$$\begin{aligned} P_4P_3P_2P_1A &= P_4 \begin{pmatrix} a & r \\ b & s \end{pmatrix} \\ &= \begin{pmatrix} ab^{-1}s - c + 1 & ab^{-1}t \\ s - ba^{-1}c & c - r \end{pmatrix} \begin{pmatrix} a & r \\ b & s \end{pmatrix} \\ &= \begin{pmatrix} a^2b^{-1}s - ac + a + at & ab^{-1}sr - cr + r + ab^{-1}st \\ as - bc + bc - br & sr - ba^{-1}cr + cs - rs \end{pmatrix}, \end{aligned}$$

und indem man $t = c - r - 1$ einsetzt, erhält man weiter

$$\begin{aligned}
 & \begin{pmatrix} a^2b^{-1}s - ac + a + at & ab^{-1}sr - cr + r + ab^{-1}st \\ as - bc + bc - br & sr - ba^{-1}cr + cs - rs \end{pmatrix} \\
 &= \begin{pmatrix} a^2b^{-1}s - ar & -cr + r + ab^{-1}s(c-1) \\ as - br & -ba^{-1}cr + cs \end{pmatrix} \\
 &= \begin{pmatrix} a(ab^{-1}s - r) & (ab^{-1}s - r)(c-1) \\ b(ab^{-1}s - r) & ba^{-1}c(-r + ab^{-1}s) \end{pmatrix} \\
 &= \begin{pmatrix} a & c-1 \\ b & ba^{-1}c \end{pmatrix},
 \end{aligned}$$

da oben bereits gezeigt wurde, dass $ab^{-1}s - r = 1$ gilt. Dies beweist, dass es in U_2A einen Vertreter der gewünschten Form gibt.

Die Endlichkeit von V folgt aus der Endlichkeit eines Vertretersystems von $\mathfrak{o} \parallel (ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o})$, die sich wiederum aus der Normendlichkeit von $\mathfrak{o}$ ergibt, da $ba^{-1}\mathfrak{o} \cap ab^{-1}\mathfrak{o}$ nach 1.2.6 ein Ideal in $\mathfrak{o}$ ist. $\square$

Nun wird eine erste Formel für die Anzahl von Rechtsnebenklassen mit vorgeschriebenem größten gemeinsamen Teiler der ersten Spalte angegeben.

2.3.3 LEMMA: Es seien die Bezeichnungen aus 2.3.1 übernommen. Darüberhinaus sei $A \in I_2$ und $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$ mit $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)$. Wähle ein $a \in \mathfrak{a}$ mit $ao + (\det A)\mathfrak{o} = \mathfrak{a}$ (möglich nach 1.2.8, da $\det A \in \mathfrak{a}$ wegen $\mathfrak{a} \mid \mathfrak{d}_2(A) = (\det A)\mathfrak{o}$), setze $\mathfrak{q} = \mathfrak{a}^{-1}a$ sowie $\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{d}_2(A)$ und wähle ein Vertretersystem V von $\mathfrak{q} \parallel \mathfrak{qb}$. Dann gilt

$$\mu_{\mathfrak{a}}(A) = |\{c \in V \mid \mathfrak{a} + (c-1)\mathfrak{o} + cq^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}|. \quad \diamond$$

BEWEIS:

Zeige zunächst, dass V ein Vertretersystem von

$$(\mathfrak{o} \cap a(\det A)^{-1}\mathfrak{o}) \parallel ((\det A)a^{-1}\mathfrak{o} \cap a(\det A)^{-1}\mathfrak{o})$$

ist. Die Ideale $\mathfrak{q}$ und $\mathfrak{b}$ sind teilerfremd, denn es gilt

$$\mathfrak{a} = \mathfrak{a}\mathfrak{o} + (\det A)\mathfrak{o} = \mathfrak{a}\mathfrak{q} + \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{q} + \mathfrak{b}),$$

also $\mathfrak{q} + \mathfrak{b} = \mathfrak{o}$. Deswegen erhält man

$$\mathfrak{o} \cap a(\det A)^{-1}\mathfrak{o} = \mathfrak{o} \cap \mathfrak{a}\mathfrak{q}(\mathfrak{a}\mathfrak{b})^{-1} = \mathfrak{o} \cap \mathfrak{q}\mathfrak{b}^{-1} \stackrel{1.2.6}{=} \mathfrak{q}$$

und

$$(\det A)a^{-1}\mathfrak{o} \cap a(\det A)^{-1}\mathfrak{o} = \mathfrak{b}\mathfrak{q}^{-1} \cap \mathfrak{q}\mathfrak{b}^{-1} \stackrel{1.2.6}{=} \mathfrak{b}\mathfrak{q},$$

woraus sich die Behauptung dieser Vorüberlegung ergibt.

Ist U_2B für ein $B \in I_2$ eine Rechtsnebenklasse in U_2AU_2 mit $\mathfrak{g}_1(B) = \mathfrak{a}$, so gilt insbesondere $\mathfrak{d}_2(B) = \mathfrak{d}_2(A)$. Nach 2.3.2 besitzt U_2B dann einen eindeutigen Vertreter von der dort beschriebenen Form (mit $b = \det A$). Zur Berechnung von $\mu_{\mathfrak{a}}(A)$ bestimme also die Anzahl der Vertreter C in der Form von 2.3.2 mit $b = \det A$ (das V ist gemäß Vorüberlegung bereits korrekt gewählt), die $\mathfrak{d}_1(C) = \mathfrak{d}_1(A)$ erfüllen (denn genau dann liegt dieser Vertreter nach 2.2.5 in U_2AU_2 , da zusätzlich $\mathfrak{d}_2(C) = b\mathfrak{o} = \mathfrak{d}_2(A)$ gilt). Bestimme dazu die Anzahl der $c \in V$ mit

$$\mathfrak{d}_1 \left(\begin{pmatrix} a & c-1 \\ \det A & (\det A)a^{-1}c \end{pmatrix} \right) = \mathfrak{d}_1(A).$$

Nun ist

$$\begin{aligned} \mathfrak{d}_1 \left(\begin{pmatrix} a & c-1 \\ \det A & (\det A)a^{-1}c \end{pmatrix} \right) &= \mathfrak{a}\mathfrak{o} + (\det A)\mathfrak{o} + (c-1)\mathfrak{o} \\ &\quad + ((\det A)a^{-1}c)\mathfrak{o} \\ &= \mathfrak{a} + (c-1)\mathfrak{o} + \mathfrak{d}_2(A)a^{-1}c \\ &= \mathfrak{a} + (c-1)\mathfrak{o} + (\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{q})^{-1}c \\ &= \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{b}\mathfrak{q}^{-1}. \end{aligned}$$

Dies schließt den Beweis ab. □

Diese erste elementare Anzahlformel kann noch vereinfacht werden und auf eine »geschlossene Form« gebracht werden. Als Vorbereitung werden einige Hilfslemmata benötigt.

2.3.4 LEMMA: Es seien die Bezeichnungen aus 2.3.1 und 2.3.3 übernommen. Für $c \in q$ und Ideale $\mathfrak{c}$ von $\mathfrak{o}$ sind dann äquivalent:

$$(i) \quad \mathfrak{c} \mid \mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b}.$$

$$(ii) \quad \mathfrak{c} \mid \mathfrak{a} \text{ und } ac \mid \mathfrak{d}_2(A) \text{ und } \mathfrak{c} \mid c - 1. \quad \diamond$$

BEWEIS:

(i) $\Rightarrow$ (ii): Aus (i) erhält man sofort $\mathfrak{c} \mid \mathfrak{a}$ und $\mathfrak{c} \mid c - 1$. Es verbleibt nun $ac \mid \mathfrak{d}_2(A)$ zu zeigen. Zeige dazu $v_p(ac) \leq v_p(\mathfrak{d}_2(A))$ für alle Primideale p . Ist p ein Primideal mit $p \nmid \mathfrak{c}$, so folgt wegen $\mathfrak{a} \mid \mathfrak{d}_2(A)$ die behauptete Ungleichung:

$$v_p(ac) = v_p(\mathfrak{a}) + v_p(\mathfrak{c}) = v_p(\mathfrak{a}) + 0 \leq v_p(\mathfrak{d}_2(A)).$$

Sei nun p ein Primideal mit $p \mid \mathfrak{c}$. Wegen $\mathfrak{c} \mid c - 1$ ist $v_p(c - 1) \geq 1$, und da $c - 1$ und c stets teilerfremd sind, muss $v_p(c) = 0$ gelten. Nach (i) gilt $\mathfrak{c} \mid cq^{-1}\mathfrak{b}$, also

$$1 \leq v_p(\mathfrak{c}) \leq v_p(cq^{-1}\mathfrak{b}) = v_p(c) - v_p(q) + v_p(\mathfrak{b}) = -v_p(q) + v_p(\mathfrak{b}).$$

Nun kann nicht $v_p(q) \geq 1$ gelten, denn da q und $\mathfrak{b}$ teilerfremd sind (vergleiche den Beweis von 2.3.3), würde $v_p(\mathfrak{b}) = 0$ und daraus mit der gerade gezeigten Ungleichung $1 \leq -v_p(q) \leq -1$ folgen. Daher muss $v_p(q) = 0$ gelten, da q ein Ideal in $\mathfrak{o}$ ist. Aus obiger Ungleichung erhält man dann $v_p(\mathfrak{c}) \leq v_p(\mathfrak{b})$ und somit

$$v_p(ac) = v_p(\mathfrak{a}) + v_p(\mathfrak{c}) \leq v_p(\mathfrak{a}) + v_p(\mathfrak{b}) = v_p(\mathfrak{ab}) = v_p(\mathfrak{d}_2(A)).$$

Die bewiesenen Aussagen zusammengenommen liefern nun (ii).

(ii) $\Rightarrow$ (i): Zum Beweis dieser Richtung genügt es, $\mathfrak{c} \mid cq^{-1}\mathfrak{b}$ zu zeigen, falls (ii) gilt. Aus $ac \mid \mathfrak{d}_2(A)$ folgt $\mathfrak{c} \mid \mathfrak{a}^{-1}\mathfrak{d}_2(A) = \mathfrak{b}$, und wegen $c \in q$ ist $cq^{-1} \subseteq \mathfrak{o}$, also gilt erst recht $\mathfrak{c} \mid cq^{-1}\mathfrak{b}$. $\square$

Auch das nachfolgende Lemma wird als Hilfsmittel im Beweis einer Vereinfachung von 2.3.3 benötigt.

2.3.5 LEMMA: Es seien die Bezeichnungen aus 2.3.1 und 2.3.3 übernommen. Für jedes Ideal $\mathfrak{c}$ von $\mathfrak{o}$ mit $\mathfrak{c} \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{c}^{-1}$ gilt dann

$$|\{c \in V \mid c - 1 \in \mathfrak{c}\}| = N(\mathfrak{b})N(\mathfrak{c})^{-1}. \quad \diamond$$

BEWEIS:

(1) Es gilt $\mathfrak{c} \mid \mathfrak{b}$: Wegen $\mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{c}^{-1}$ existiert ein Ideal $\mathfrak{a}'$ in $\mathfrak{o}$ mit $\mathfrak{a}\mathfrak{a}' = \mathfrak{d}_2(A)\mathfrak{c}^{-1}$; es folgt $\mathfrak{b} = \mathfrak{d}_2(A)\mathfrak{a}^{-1} = \mathfrak{d}_2(A)\mathfrak{d}_2(A)^{-1}\mathfrak{c}\mathfrak{a}' = \mathfrak{c}\mathfrak{a}'$, also $\mathfrak{c} \mid \mathfrak{b}$.

(2) Wegen der Teilerfremdheit von $\mathfrak{b}$ und $\mathfrak{q}$ (vergleiche den Beweis von 2.3.3) müssen nach (1) auch $\mathfrak{q}$ und $\mathfrak{c}$ teilerfremd sein. Daher existiert nach 1.2.9 ein $d \in \mathfrak{o}$ mit

$$\{x \in \mathfrak{o} \mid x \in \mathfrak{q}, x \in 1 + \mathfrak{c}\} = d + \mathfrak{c}\mathfrak{q}.$$

(3) Es sei $\{c \in V \mid c - 1 \in \mathfrak{c}\} = \{d_1, \dots, d_k\}$ und $V = \{d_1, \dots, d_m\}$ mit $m \geq k$. Dann bilden die $d_1 - d, \dots, d_k - d$ ein Vertretersystem von $\mathfrak{c}\mathfrak{q} // \mathfrak{b}\mathfrak{q}$:

(3a) Wegen $d \in \mathfrak{q}$ und $d \in 1 + \mathfrak{c}$ nach (2) sowie $d_i - 1 \in \mathfrak{c}$ nach Wahl von $d_1, \dots, d_k$ gilt $d_i - d \in d_i + \mathfrak{q} = \mathfrak{q}$ und $d_i - d \in (d_i - 1) + \mathfrak{c} = \mathfrak{c}$, also $d_i - d \in \mathfrak{c} \cap \mathfrak{q} = \mathfrak{c}\mathfrak{q}$ für alle $1 \leq i \leq k$ (dabei gilt $\mathfrak{c} \cap \mathfrak{q} = \mathfrak{c}\mathfrak{q}$ nach 1.2.6 aufgrund der Teilerfremdheit).

(3b) Da die d_i Elemente eines Vertretersystems von $\mathfrak{q} // \mathfrak{b}\mathfrak{q}$ sind, müssen die $d_i + \mathfrak{b}\mathfrak{q}$ für $1 \leq i \leq m$ und damit auch die $(d_i - d) + \mathfrak{b}\mathfrak{q}$ für $1 \leq i \leq m$ paarweise verschieden sein.

(3c) Für jedes $x \in \mathfrak{c}\mathfrak{q}$ gibt es ein $1 \leq j \leq k$ mit $x \in (d_j - d) + \mathfrak{b}\mathfrak{q}$: Ist $x \in \mathfrak{c}\mathfrak{q} = \mathfrak{c} \cap \mathfrak{q}$, also $x \in \mathfrak{c}$ und $x \in \mathfrak{q}$, so gilt nach (2) $x + d \in x + \mathfrak{q} = \mathfrak{q}$ und $x + d \in x + 1 + \mathfrak{c} = 1 + \mathfrak{c}$, also $x + d \in \mathfrak{q} \cap (\mathfrak{c} + 1)$. Wegen $x + d \in \mathfrak{q}$ gibt es ein $1 \leq j \leq m$ mit $x + d \in d_j + \mathfrak{b}\mathfrak{q}$. Es gilt sogar $j \leq k$, denn

nach (1) gilt $\mathfrak{c} \mid \mathfrak{b} \mid \mathfrak{b}\mathfrak{q}$, womit aus $x + d \in d_j + \mathfrak{b}\mathfrak{q}$ auch $x + d \in d_j + \mathfrak{c}$ folgt, was $d_j - 1 \in x + d - 1 + \mathfrak{c} = \mathfrak{c}$ liefert, da bereits $x + d \in \mathfrak{c} + 1$ gezeigt wurde. Damit ist Punkt (3) vollständig bewiesen.

(4) Es gilt $|\mathfrak{c}\mathfrak{q} // \mathfrak{b}\mathfrak{q}| = N(\mathfrak{b})N(\mathfrak{c})^{-1}$: Man hat

$$\begin{aligned} N(\mathfrak{c})N(\mathfrak{q}) \cdot |\mathfrak{c}\mathfrak{q} // \mathfrak{b}\mathfrak{q}| &= N(\mathfrak{c}\mathfrak{q}) \cdot |\mathfrak{c}\mathfrak{q} // \mathfrak{b}\mathfrak{q}| \\ &= |\mathfrak{o} // \mathfrak{c}\mathfrak{q}| \cdot |\mathfrak{c}\mathfrak{q} // \mathfrak{b}\mathfrak{q}| \\ &= |\mathfrak{o} // \mathfrak{b}\mathfrak{q}| = N(\mathfrak{b}\mathfrak{q}) \\ &= N(\mathfrak{b})N(\mathfrak{q}), \end{aligned}$$

woraus man nach Division durch $N(\mathfrak{c})N(\mathfrak{q})$ die Behauptung aus (4) erhält.

Die Punkte (3) und (4) liefern zusammengekommen den Beweis des Lemmas. $\square$

Mit diesen Lemmata ist nun eine Vereinfachung der Maßformel aus 2.3.3 möglich.

2.3.6 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen. Weiter sei $A \in I_2$ und $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$. Gilt nun $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$, so ist

$$\mu_{\mathfrak{a}}(A) = \frac{N(\mathfrak{d}_2(A))}{N(\mathfrak{a})N(\mathfrak{d}_1(A))} \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} \mid \mathfrak{a}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}}} (1 - N(\mathfrak{p})^{-1}),$$

andernfalls ist $\mu_{\mathfrak{a}}(A) = 0$. $\diamond$

BEWEIS:

(1) In 2.3.3 wurde gezeigt, dass mit den dort eingeführten Bezeichnungen

$$\mu_{\mathfrak{a}}(A) = |\{c \in V \mid \mathfrak{a} + (c - 1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}|$$

gilt. Ist $\mathfrak{a}$ ein Ideal von $\mathfrak{o}$ mit $\mu_{\mathfrak{a}}(A) \geq 1$, so gibt es ein $c \in V$ mit $\mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)$, also insbesondere

$$\mathfrak{d}_1(A) \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b}.$$

Mit 2.3.4 folgt $\mathfrak{d}_1(A) \mid \mathfrak{a}$ und $\mathfrak{a}\mathfrak{d}_1(A) \mid \mathfrak{d}_2(A)$, also zusammengenommen $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$. Daher ist nun $\mu_{\mathfrak{a}}(A) = 0$, falls diese Bedingung nicht erfüllt ist.

(2) Es sei

$$\Omega = \{\mathfrak{q} \text{ Primideal von } \mathfrak{o} \mid \mathfrak{q} \text{ teilt } \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-2}\} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_m\}.$$

Im folgenden gelte stets $\mathfrak{d}_1(A) \mid \mathfrak{a} \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}$. Definiere nun $M = \{c \in V \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}$. Für Ideale $\mathfrak{c}$ von $\mathfrak{o}$ setze $M(\mathfrak{c}) = \{c \in V \mid \mathfrak{c} \text{ teilt } \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b}\}$. Dann gilt zunächst

$$\begin{aligned} & \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)| \\ &= \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} \sum_{c \in M(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)} (-1)^k. \end{aligned}$$

Es bezeichne $\chi_{\mathfrak{c}}$ die Indikatorfunktion von $M(\mathfrak{c})$. Da für jedes Ideal $\mathfrak{c}'$ in $\mathfrak{o}$ offenbar $M(\mathfrak{d}_1(A)) \supseteq M(\mathfrak{d}_1(A)\mathfrak{c}')$ gilt, hat man weiter

$$\begin{aligned} & \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} \sum_{c \in M(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)} (-1)^k \\ &= \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} \sum_{c \in M(\mathfrak{d}_1(A))} (-1)^k \chi_{\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k}(c) \\ &= \sum_{c \in M(\mathfrak{d}_1(A))} \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k \chi_{\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k}(c). \end{aligned}$$

Für jedes $c \in M(\mathfrak{d}_1(A))$ sei $\Omega(c)$ die Menge aller Primideale von $\mathfrak{o}$, die das Ideal $(\mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b})\mathfrak{d}_1(A)^{-1}$ teilen. Sind nun $\mathfrak{q}_1, \dots, \mathfrak{q}_k$ paarweise verschiedene Primideale von $\mathfrak{o}$, so gilt $c \in M(\mathfrak{d}_1(A)\mathfrak{q}_1 \cdots \mathfrak{q}_k)$ nach Definition von $M(c)$ und $\Omega(c)$ genau dann, wenn $\{\mathfrak{q}_1, \dots, \mathfrak{q}_k\}$ eine Teilmenge von $\Omega(c)$ ist. Daher gilt weiter

$$\begin{aligned}
 & \sum_{c \in M(\mathfrak{d}_1(A))} \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k \chi_{\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k}(c) \\
 &= \sum_{c \in M(\mathfrak{d}_1(A))} \sum_{k=0}^{|\Omega(c)|} \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega(c) \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k \\
 &= \sum_{c \in M(\mathfrak{d}_1(A))} \sum_{k=0}^{|\Omega(c)|} \binom{|\Omega(c)|}{k} (-1)^k \\
 &= \sum_{c \in M(\mathfrak{d}_1(A))} 0^{|\Omega(c)|} = |\{c \in M(\mathfrak{d}_1(A)) \mid \Omega(c) = \emptyset\}|.
 \end{aligned}$$

Für $c \in M(\mathfrak{d}_1(A))$ gilt $\Omega(c) = \emptyset$ nach Definition von $\Omega(c)$ genau dann, wenn $\mathfrak{d}_1(A) = \mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b}$ gilt (beachte, dass das in der Definition von $\Omega(c)$ auftretende Ideal $(\mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b})\mathfrak{d}_1(A)^{-1}$ für jedes $c \in M(\mathfrak{d}_1(A))$ ein ganzes Ideal ist und somit $\Omega(c) = \emptyset$ nur gelten kann, wenn dieses Ideal gleich $\mathfrak{o}$ ist), also erhält man insgesamt

$$\begin{aligned}
 & \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)| \\
 &= |\{c \in M(\mathfrak{d}_1(A)) \mid \mathfrak{d}_1(A) = \mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b}\}| \\
 &= |\{c \in V \mid \mathfrak{d}_1(A) = \mathfrak{a} + (c - 1)\mathfrak{o} + cq^{-1}\mathfrak{b}\}|.
 \end{aligned}$$

(3) Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ Primideale. Falls

$$\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)^{-1}$$

nicht gilt, ist für $c = \mathfrak{d}_1(A)p_1 \cdots p_k$ die erste oder die zweite Bedingung der Aussage aus 2.3.4 (ii) verletzt und folglich nach diesem Lemma $|M(\mathfrak{d}_1(A)p_1 \cdots p_k)| = 0$, ansonsten hat man

$$\begin{aligned} |M(\mathfrak{d}_1(A)p_1 \cdots p_k)| &\stackrel{2.3.4}{=} |\{c \in V \mid \mathfrak{d}_1(A)p_1 \cdots p_k \text{ teilt } c - 1\}| \\ &\stackrel{2.3.5}{=} N(\mathfrak{b})N(\mathfrak{d}_1(A)p_1 \cdots p_k)^{-1}. \end{aligned}$$

(4) Für Primideale $p_1, \dots, p_k$ definiere

$$\psi(p_1, \dots, p_k) = \begin{cases} 1, & \text{falls } \mathfrak{d}_1(A)p_1 \cdots p_k \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)p_1 \cdots p_k)^{-1}, \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt

$$\begin{aligned} &\sum_{k=0}^m \sum_{\substack{\{p_1, \dots, p_k\} \subseteq \Omega \\ |\{p_1, \dots, p_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)p_1 \cdots p_k)| \\ &\stackrel{(3)}{=} \sum_{k=0}^m \sum_{\substack{\{p_1, \dots, p_k\} \subseteq \Omega \\ |\{p_1, \dots, p_k\}|=k}} (-1)^k N(\mathfrak{b})N(\mathfrak{d}_1(A)p_1 \cdots p_k)^{-1} \psi(p_1, \dots, p_k), \end{aligned}$$

also

$$\begin{aligned} &N(\mathfrak{b})^{-1}N(\mathfrak{d}_1(A)) \sum_{k=0}^m \sum_{\substack{\{p_1, \dots, p_k\} \subseteq \Omega \\ |\{p_1, \dots, p_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)p_1 \cdots p_k)| \\ &= \sum_{k=0}^m \sum_{\substack{\{p_1, \dots, p_k\} \subseteq \Omega \\ |\{p_1, \dots, p_k\}|=k}} (-1)^k N(p_1)^{-1} \cdots N(p_k)^{-1} \psi(p_1, \dots, p_k). \end{aligned}$$

Nun gilt $\mathfrak{d}_1(A)p_1 \cdots p_k \mid \mathfrak{a} \mid \mathfrak{d}_2(A)(\mathfrak{d}_1(A)p_1 \cdots p_k)^{-1}$ genau dann, wenn $p_1 \cdots p_k \mid \mathfrak{a}\mathfrak{d}_1(A)^{-1}$ und $p_1 \cdots p_k \mid \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$ gilt, was wiederum äquivalent dazu ist, dass $p_1 \cdots p_k$ den größten gemeinsamen Teiler $\mathfrak{a}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$ teilt. Daher sind in obiger Summe

genau die Summanden von Null verschieden, bei denen die $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ alle das Ideal $\mathfrak{a}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$ teilen. Es bezeichne nun Ω' die Menge aller Primideale, die $\mathfrak{a}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{a}^{-1}$ teilen. Dann erhält man folgende Vereinfachung:

$$\begin{aligned}
 & \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k N(\mathfrak{p}_1)^{-1} \dots N(\mathfrak{p}_k)^{-1} \psi(\mathfrak{p}_1, \dots, \mathfrak{p}_k) \\
 &= \sum_{k=0}^{|\Omega'|} \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega' \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k N(\mathfrak{p}_1)^{-1} \dots N(\mathfrak{p}_k)^{-1} \\
 &= \sum_{k=0}^{|\Omega'|} \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega' \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-N(\mathfrak{p}_1)^{-1}) \dots (-N(\mathfrak{p}_k)^{-1}),
 \end{aligned}$$

und nach dem allgemeinen Distributivgesetz gilt

$$\begin{aligned}
 & \sum_{k=0}^{|\Omega'|} \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega' \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-N(\mathfrak{p}_1)^{-1}) \dots (-N(\mathfrak{p}_k)^{-1}) \\
 &= \prod_{\mathfrak{q} \in \Omega'} (1 - N(\mathfrak{q})^{-1}).
 \end{aligned}$$

Fügt man nun alle Umformungen in diesem Absatz zusammen und ergänzt den Faktor $N(\mathfrak{b})N(\mathfrak{d}_1(A))^{-1}$ wieder, so ergibt sich die Gleichung

$$\begin{aligned}
 & \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)\mathfrak{p}_1 \dots \mathfrak{p}_k)| \\
 &= N(\mathfrak{b})N(\mathfrak{d}_1(A))^{-1} \prod_{\mathfrak{q} \in \Omega'} (1 - N(\mathfrak{q})^{-1}).
 \end{aligned}$$

(5) Zusammengefasst gilt

$$\begin{aligned}
 \mu_{\mathfrak{a}}(A) &\stackrel{(1)}{=} |\{c \in V \mid \mathfrak{a} + (c-1)\mathfrak{o} + c\mathfrak{q}^{-1}\mathfrak{b} = \mathfrak{d}_1(A)\}| \\
 &\stackrel{(2)}{=} \sum_{k=0}^m \sum_{\substack{\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \Omega \\ |\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}|=k}} (-1)^k |M(\mathfrak{d}_1(A)\mathfrak{p}_1 \cdots \mathfrak{p}_k)| \\
 &\stackrel{(4)}{=} N(\mathfrak{b})N(\mathfrak{d}_1(A))^{-1} \prod_{\mathfrak{q} \in \Omega'} (1 - N(\mathfrak{q})^{-1}) \\
 &\stackrel{\mathfrak{b}=\mathfrak{d}_2(A)\mathfrak{a}^{-1}}{=} \frac{N(\mathfrak{d}_2(A))}{N(\mathfrak{a})N(\mathfrak{d}_1(A))} \prod_{\mathfrak{q} \in \Omega'} (1 - N(\mathfrak{q})^{-1}),
 \end{aligned}$$

was die Behauptung beweist. $\square$

Diese Formel für $\mu_{\mathfrak{a}}(A)$ wird im nächsten Abschnitt noch im Beweis eines Reduktionssatzes relevant. Zunächst soll jedoch auch eine Maßformel für die Anzahl aller in einer Doppelnebenklasse enthaltenen Rechtsnebenklassen gezeigt werden.

2.3.7 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen und $A \in I_2$. Dann gilt

$$\mu(A) = N(\mathfrak{f}_2(A)) \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} \mid \mathfrak{f}_2(A)}} (1 + N(\mathfrak{p})^{-1}).$$

$\diamond$

BEWEIS:

(1) Zur Berechnung von $\mu(A)$ müssen alle $\mu_{\mathfrak{a}}(A)$ aufsummiert werden, da dies dann die Anzahl der Rechtsnebenklassen U_2B in U_2AU_2 mit beliebigem größten gemeinsamen Teiler der Einträge der ersten Spalte von B beschreibt; definiert man für Primideale $\mathfrak{p}$ und Ideale $\mathfrak{c}$ von $\mathfrak{o}$ zur Abkürzung

$$\psi_{\mathfrak{p}}(\mathfrak{c}) = \begin{cases} 1 - N(\mathfrak{p})^{-1}, & \text{falls } \mathfrak{p} \mid \mathfrak{c}\mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A)\mathfrak{d}_1(A)^{-1}\mathfrak{c}^{-1}, \\ 1 & \text{sonst,} \end{cases}$$

so gilt

$$\begin{aligned} \mu(A) &= \sum_{\mathfrak{a} \text{ Ideal in } \mathfrak{o}} \mu_{\mathfrak{a}}(A) \\ &\stackrel{2.3.6}{=} \sum_{\mathfrak{d}_1(A) | \mathfrak{a} | \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-1}} \frac{N(\mathfrak{d}_2(A))}{N(\mathfrak{a})N(\mathfrak{d}_1(A))} \prod_{\mathfrak{p} \text{ Primideal}} \psi_{\mathfrak{p}}(\mathfrak{a}). \end{aligned}$$

Verwende als neuen Summationsindex $\mathfrak{a}' = \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-1} \mathfrak{a}^{-1}$ anstelle von $\mathfrak{a}$. Dann ist die Bedingung $\mathfrak{d}_1(A) | \mathfrak{a} | \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-1}$ gleichbedeutend mit $\mathfrak{o} | \mathfrak{a}' | \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-2} = \mathfrak{f}_2(A)$, und $\psi_{\mathfrak{p}}(\mathfrak{a}) = 1 - N(\mathfrak{p})^{-1}$, das heißt $\mathfrak{p} | \mathfrak{a} \mathfrak{d}_1(A)^{-1} + \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-1} \mathfrak{a}^{-1}$, ist äquivalent zur Bedingung $\mathfrak{p} | (\mathfrak{a}')^{-1} \mathfrak{d}_1(A)^{-2} \mathfrak{d}_2(A) + \mathfrak{a}' = (\mathfrak{a}')^{-1} \mathfrak{f}_2(A) + \mathfrak{a}'$, und es gilt $\psi_{\mathfrak{p}}(\mathfrak{a}) = 1$ für alle Primideale $\mathfrak{p}$, die diese Bedingung nicht erfüllen. Darüberhinaus gilt $N(\mathfrak{a}') = N(\mathfrak{d}_2(A))N(\mathfrak{d}_1(A))^{-1}N(\mathfrak{a})^{-1}$, also hat man insgesamt

$$\begin{aligned} &\sum_{\mathfrak{d}_1(A) | \mathfrak{a} | \mathfrak{d}_2(A) \mathfrak{d}_1(A)^{-1}} \frac{N(\mathfrak{d}_2(A))}{N(\mathfrak{a})N(\mathfrak{d}_1(A))} \prod_{\mathfrak{p} \text{ Primideal}} \psi_{\mathfrak{p}}(\mathfrak{a}) \\ &= \sum_{\mathfrak{o} | \mathfrak{a}' | \mathfrak{f}_2(A)} N(\mathfrak{a}') \prod_{\substack{\mathfrak{q} \text{ Primideal} \\ \mathfrak{q} | (\mathfrak{a}')^{-1} \mathfrak{f}_2(A) + \mathfrak{a}'}} (1 - N(\mathfrak{q})^{-1}). \end{aligned}$$

(2) Für Ideale $\mathfrak{c}$ von $\mathfrak{o}$ bezeichne $\mathfrak{Q}_{\mathfrak{c}}$ die Menge aller Primideale $\mathfrak{q}$, die $\mathfrak{c}^{-1} \mathfrak{f}_2(A) + \mathfrak{c}$ teilen. Sei nun $\mathfrak{p}$ ein Primideal, $k \in \mathbb{N}_0$ und $\mathfrak{c}$ ein Ideal von $\mathfrak{o}$ mit $\mathfrak{p} \nmid \mathfrak{c}$. Dann gilt

$$\begin{aligned} \mathfrak{p} &\in \mathfrak{Q}_{\mathfrak{p}^k \mathfrak{c}} && \Leftrightarrow \\ \mathfrak{p} &| (\mathfrak{p}^k \mathfrak{c})^{-1} \mathfrak{f}_2(A) + \mathfrak{p}^k \mathfrak{c} && \Leftrightarrow \\ \mathfrak{v}_{\mathfrak{p}}((\mathfrak{p}^k \mathfrak{c})^{-1} \mathfrak{f}_2(A)) &> 0 \text{ und } \mathfrak{v}_{\mathfrak{p}}(\mathfrak{p}^k \mathfrak{c}) \geq 1 && \Leftrightarrow \\ -k + \mathfrak{v}_{\mathfrak{p}}(\mathfrak{f}_2(A)) &> 0 \text{ und } k \geq 1 && \Leftrightarrow \\ 1 &\leq k < \mathfrak{v}_{\mathfrak{p}}(\mathfrak{f}_2(A)), && \end{aligned}$$

und für jedes Primideal $\mathfrak{p}' \neq \mathfrak{p}$ ist

$$\begin{aligned}
 \mathfrak{p}' &\in \Omega_{\mathfrak{p}^k \mathfrak{c}} && \Leftrightarrow \\
 \mathfrak{p}' &\mid (\mathfrak{p}^k \mathfrak{c})^{-1} f_2(A) + \mathfrak{p}^k \mathfrak{c} && \Leftrightarrow \\
 v_{\mathfrak{p}'}((\mathfrak{p}^k \mathfrak{c})^{-1} f_2(A)) &> 0 \text{ und } v_{\mathfrak{p}'}(\mathfrak{p}^k \mathfrak{c}) \geq 1 && \Leftrightarrow \\
 v_{\mathfrak{p}'}(\mathfrak{c}^{-1} f_2(A)) &> 0 \text{ und } v_{\mathfrak{p}'}(\mathfrak{c}) \geq 1 && \Leftrightarrow \\
 \mathfrak{p}' &\in \Omega_{\mathfrak{c}}.
 \end{aligned}$$

(3) Beweise nun die Behauptung durch vollständige Induktion nach der Anzahl der Primteiler von $f_2(A)$. Ist diese Anzahl gleich 0, so gilt $f_2(A) = \mathfrak{o}$ und damit

$$\begin{aligned}
 \mu(A) &\stackrel{(1)}{=} \sum_{\mathfrak{o} \mid \mathfrak{a}' \mid f_2(A)} N(\mathfrak{a}') \prod_{\mathfrak{q} \in \Omega_{\mathfrak{a}'}} (1 - N(\mathfrak{q})^{-1}) \\
 &= N(\mathfrak{o}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{o}}} (1 - N(\mathfrak{q})^{-1}) = 1 \cdot 1 = 1,
 \end{aligned}$$

was mit der zu zeigenden Formel übereinstimmt. Nun werde $f_2(A)$ von mindestens einem Primideal $\mathfrak{p}$ geteilt. Es gilt

$$\begin{aligned}
 \mu(A) &\stackrel{(1)}{=} \sum_{\mathfrak{o} \mid \mathfrak{a}' \mid f_2(A)} N(\mathfrak{a}') \prod_{\mathfrak{q} \in \Omega_{\mathfrak{a}'}} (1 - N(\mathfrak{q})^{-1}) \\
 &= \sum_{k=0}^{v_{\mathfrak{p}}(f_2(A))} \sum_{\substack{\mathfrak{o} \mid \mathfrak{c} \mid f_2(A) \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{p}^k \mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{p}^k \mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\
 &\stackrel{(2)}{=} \sum_{k=1}^{v_{\mathfrak{p}}(f_2(A))-1} \sum_{\substack{\mathfrak{o} \mid \mathfrak{c} \mid f_2(A) \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{p})^k N(\mathfrak{c}) (1 - N(\mathfrak{p})^{-1}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\
 &\quad + \sum_{\substack{\mathfrak{o} \mid \mathfrak{c} \mid f_2(A) \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\
 &\quad + \sum_{\substack{\mathfrak{o} \mid \mathfrak{c} \mid f_2(A) \\ \mathfrak{p} \mid \mathfrak{c}}} N(\mathfrak{p})^{v_{\mathfrak{p}}(f_2(A))} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}).
 \end{aligned}$$

Da

$$\begin{aligned}
 & \sum_{k=1}^{v_p(f_2(A))-1} \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^k N(c) (1 - N(p))^{-1} \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 = & \sum_{k=1}^{v_p(f_2(A))-1} \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^k N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 & - \sum_{k=1}^{v_p(f_2(A))-1} \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^{k-1} N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 = & \sum_{k=1}^{v_p(f_2(A))-1} \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^k N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 & - \sum_{k=0}^{v_p(f_2(A))-2} \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^k N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 = & \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^{v_p(f_2(A))-1} N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 & - \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1}
 \end{aligned}$$

gilt, vereinfacht sich die Formel für $\mu(A)$ zu

$$\begin{aligned}
 \mu(A) = & \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^{v_p(f_2(A))} N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1} \\
 & + \sum_{\substack{o|c|f_2(A) \\ p \nmid c}} N(p)^{v_p(f_2(A))-1} N(c) \prod_{q \in \Omega_c} (1 - N(q))^{-1}
 \end{aligned}$$

$$= N(\mathfrak{p})^{v_{\mathfrak{p}}(f_2(A))} (1 + N(\mathfrak{p})^{-1}) \sum_{\substack{\mathfrak{o}|\mathfrak{c}|f_2(A) \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}).$$

Wähle nun eine Matrix $A' \in I_n$ mit $\mathfrak{d}_i(A') = \mathfrak{d}_i(A)\mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{d}_i(A))}$ für jedes $i \in \{1, 2\}$; dies ist möglich nach 2.2.10, denn für alle Primideale $\mathfrak{q}$ von $\mathfrak{o}$ gilt

$$\begin{aligned} v_{\mathfrak{q}}((\mathfrak{d}_1(A)\mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{d}_1(A))})^2) &= \begin{cases} 2v_{\mathfrak{q}}(\mathfrak{d}_1(A)), & \text{falls } \mathfrak{q} \neq \mathfrak{p}, \\ 0 & \text{sonst} \end{cases} \\ &\stackrel{2.2.4(f)}{\leq} \begin{cases} v_{\mathfrak{q}}(\mathfrak{d}_2(A)), & \text{falls } \mathfrak{q} \neq \mathfrak{p}, \\ 0 & \text{sonst} \end{cases} \\ &= v_{\mathfrak{q}}(\mathfrak{d}_2(A)\mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{d}_2(A))}), \end{aligned}$$

also $(\mathfrak{d}_1(A)\mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{d}_1(A))})^2 \mid \mathfrak{d}_2(A)\mathfrak{p}^{-v_{\mathfrak{p}}(\mathfrak{d}_2(A))}$. Mit dieser Wahl tritt $\mathfrak{p}$ nicht als Primteiler von $f_2(A')$ auf, also kann die Induktionsvoraussetzung auf A' angewendet werden. Berücksichtige nun noch, dass mit der Definition von $\Omega'_{\mathfrak{c}}$ als Menge aller Primideale, die $\mathfrak{c}^{-1}f_2(A') + \mathfrak{c}$ teilen, für ein Ideal $\mathfrak{c}$ von $\mathfrak{o}$ mit $\mathfrak{p} \nmid \mathfrak{c}$ stets $\Omega_{\mathfrak{c}} = \Omega'_{\mathfrak{c}}$ gilt, da wegen $\mathfrak{p} \nmid \mathfrak{c}$ sowohl $\mathfrak{p} \notin \Omega_{\mathfrak{c}}$ als auch $\mathfrak{p} \notin \Omega'_{\mathfrak{c}}$ nach Definition dieser Mengen gelten muss und für jedes Primideal $\mathfrak{q} \neq \mathfrak{p}$ die Bedingungen $\mathfrak{p} \mid \mathfrak{c}^{-1}f_2(A) + \mathfrak{c}$ und $\mathfrak{p} \mid \mathfrak{c}^{-1}f_2(A') + \mathfrak{c}$ wegen $v_{\mathfrak{q}}(f_2(A')) = v_{\mathfrak{q}}(f_2(A))$ äquivalent sind. Somit erhält man

$$\begin{aligned} &\sum_{\substack{\mathfrak{o}|\mathfrak{c}|f_2(A) \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\ &= \sum_{\substack{\mathfrak{o}|\mathfrak{c}|f_2(A') \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega'_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\ &\stackrel{(1)}{=} \mu(A') \stackrel{(IV)}{=} N(f_2(A')) \prod_{\substack{\mathfrak{p}' \text{ Primideal} \\ \mathfrak{p}' \mid f_2(A')}} (1 + N(\mathfrak{p}')^{-1}) \end{aligned}$$

und damit insgesamt

$$\begin{aligned}
 \mu(A) &= N(\mathfrak{p})^{v_{\mathfrak{p}}(f_2(A))} (1 + N(\mathfrak{p})^{-1}) \sum_{\substack{\mathfrak{o}|\mathfrak{c} \\ \mathfrak{p} \nmid \mathfrak{c}}} N(\mathfrak{c}) \prod_{\mathfrak{q} \in \Omega_{\mathfrak{c}}} (1 - N(\mathfrak{q})^{-1}) \\
 &= N(\mathfrak{p})^{v_{\mathfrak{p}}(f_2(A))} (1 + N(\mathfrak{p})^{-1}) N(f_2(A')) \prod_{\substack{\mathfrak{p}' \text{ Primideal} \\ \mathfrak{p}' | f_2(A')}} (1 + N(\mathfrak{p}')^{-1}) \\
 &= N(f_2(A)) \prod_{\substack{\mathfrak{p}' \text{ Primideal} \\ \mathfrak{p}' | f_2(A)}} (1 + N(\mathfrak{p}')^{-1}),
 \end{aligned}$$

was zu zeigen war. □

Die folgende Bemerkung stellt einige bereits bekannte vergleichbare Ergebnisse zur Berechnung der Anzahl von Rechtsnebenklassen zusammen.

2.3.8 **BEMERKUNG:** Wird der Fall $K = \mathbb{Q}$ untersucht, so lässt sich eine Aussage beweisen, die eine bestimmte formale Potenzreihe über der Hecke-Algebra als Quotient von Polynomen darstellt (zu diesem Rationalitätssatz vergleiche etwa [Kri90] v (9.3)). In den Beweis dieser Aussage geht ein, dass für jede Primzahl p die Doppelnebenklasse $\text{GL}_n(\mathbb{Q}) \text{diag}(1, \dots, 1, p, \dots, p) \text{GL}_n(\mathbb{Q})$, bei der das p genau j -mal auftritt, nach einer leichten Umformulierung der Indexformel aus [Kri90] v (7.2) in genau

$$p^{-\frac{j(j+1)}{2}} \sum_{1 \leq v_1 < \dots < v_j \leq n} p^{v_1 + \dots + v_j}$$

Rechtsnebenklassen bezüglich $\text{GL}_n(\mathbb{Z})$ zerfällt. Man rechnet leicht nach, dass dieses Resultat im Falle $n = 2$ (und folglich $j \in \{0, 1, 2\}$) mit dem Ergebnis aus 2.3.7 übereinstimmt.

Ist man für einen Hauptidealring $\mathfrak{o}$ mit der Notation aus 2.3.1 nicht an $\mu([A])$ für jedes $A \in I_n$ interessiert, sondern für jedes $d \in \mathfrak{o} \setminus \{0\}$ nur

an der Anzahl der in der Menge $\{A \in I_n \mid \det A \in d\mathfrak{o}^*\}$ enthaltenen Rechtsnebenklassen bezüglich U_n , so erhält man diese gemäß [New72] Satz II.4 (S. 20) über

$$\prod_{\substack{p \in P \\ p \mid d}} \prod_{j=1}^{n-1} \frac{N(p)^{v_{p\mathfrak{o}}(d)+j} - 1}{N(p)^j - 1},$$

wenn P ein Vertretersystem von $\{p \mid p \text{ Primelement in } \mathfrak{o}\} // \mathfrak{o}^*$ bezeichnet. Im Falle $n = 2$ vereinfacht sich die an gleicher Stelle gegebene alternative Formel für diese Rechtsnebenklassenzahl zu

$$\sum_{\substack{c \in \mathfrak{o} \\ c \mid d}} N(c),$$

was mit der für die klassische Theorie der Hecke-Operatoren wichtigen Anzahl der Rechtsnebenklassen in $T_1 // T_d$ übereinstimmt, wenn T_m für alle $m \in \mathbb{Z}$ die Menge der Matrizen $A \in \mathbb{Z}^{2 \times 2}$ mit $\det A = m$ bezeichnet (vergleiche [Koe07] Korollar IV.1.2 (S. 209)). $\diamond$

Zum Abschluss dieses Abschnitts steht noch eine elementare Anwendung des Hauptresultats 2.3.7.

2.3.9 FOLGERUNG: Sei $\mathfrak{o}$ ein normendlicher Dedekind-Ring und $U = \mathrm{GL}_2(\mathfrak{o})$ sowie

$$U^0[\mathfrak{a}] = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U \mid b \in \mathfrak{a} \right\}$$

für jedes Ideal $\mathfrak{a}$ von $\mathfrak{o}$. Für jedes $m \in \mathfrak{o}$ gilt dann

$$|U^0[m\mathfrak{o}] // U| = N(m\mathfrak{o}) \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} \mid m}} (1 + N(\mathfrak{p})^{-1}).$$

$\diamond$

2 Hecke-Algebren zu unimodularen Gruppen

BEWEIS:

Sei $m \in \mathfrak{o}$ und $A = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$. Für $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U$ gilt

$$B \in A^{-1}UA \quad \Leftrightarrow$$

$$ABA^{-1} \in U \quad \Leftrightarrow$$

$$\begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & m^{-1} \end{pmatrix} \in U \quad \Leftrightarrow$$

$$\begin{pmatrix} a & m^{-1}b \\ mc & d \end{pmatrix} \in U,$$

und da bereits

$$\det \begin{pmatrix} a & m^{-1}b \\ mc & d \end{pmatrix} = ad - bc = \det B \stackrel{B \in U}{\in} \mathfrak{o}^*$$

und $a, m, c, d \in \mathfrak{o}$ gilt, hat man

$$\begin{pmatrix} a & m^{-1}b \\ mc & d \end{pmatrix} \in U \quad \Leftrightarrow \quad m^{-1}b \in \mathfrak{o} \quad \Leftrightarrow \quad b \in m\mathfrak{o},$$

also ist insgesamt $B \in U^0[m\mathfrak{o}]$ äquivalent zu $B \in U$ und $B \in A^{-1}UA$. Somit gilt $U^0[m\mathfrak{o}] = U \cap A^{-1}UA$. Mit den Bezeichnungen aus 2.3.1 ist nun

$$\begin{aligned} |U^0[m\mathfrak{o}] \backslash U| &= |U \cap A^{-1}UA \backslash U| \stackrel{1.1.3}{=} |U \backslash UAU| \\ &= \mu(A) \stackrel{2.3.7}{=} N(f_2(A)) \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} | f_2(A)}} (1 + N(\mathfrak{p})^{-1}) \\ &= N(m\mathfrak{o}) \prod_{\substack{\mathfrak{p} \text{ Primideal} \\ \mathfrak{p} | m}} (1 + N(\mathfrak{p})^{-1}), \end{aligned}$$

was die Behauptung beweist. □

§ 2.4

EIN REDUKTIONSSATZ

Die im letzten Abschnitt hergeleiteten Anzahlformeln für Rechtsnebenklassen gestatten für einen Spezialfall (nämlich $n = 2$) den Beweis einer Vermutung, die bestimmte Produkte in der Hecke-Algebra $H(G_n, I_n, U_n)$ auf Produkte in $H(G_{n-1}, I_{n-1}, U_{n-1})$ zurückführt. Als Vorbereitung dieses Reduktionssatzes muss zunächst als Hilfsaussage die Multiplikativität von μ_o bewiesen werden.

2.4.1 LEMMA: Es seien die Bezeichnungen aus 2.3.1 übernommen und zwei Elemente $f, g \in H(G_2, I_2, U_2)$ gegeben. Dann gilt $\mu_o(f * g) = \mu_o(f)\mu_o(g)$. $\diamond$

BEWEIS:

Aufgrund der Definition von μ_o genügt es, diese Aussage für den Fall $f = \llbracket A \rrbracket$ und $g = \llbracket B \rrbracket$ für Matrizen $A, B \in I_2$ zu zeigen. Für alle $C \in \text{Tr}(f * g) = U_2 A U_2 B U_2$ (nach 1.1.9) gilt $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C)$ nach 2.6.2, also auch $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{g}_1(C)$. Daher gilt $\mu_o(f * g) = 0$, falls $\mathfrak{d}_1(A) \neq o$ oder $\mathfrak{d}_1(B) \neq o$; da dann wegen $\mathfrak{d}_1(A) \mid \mathfrak{g}_1(A)$ beziehungsweise $\mathfrak{d}_1(B) \mid \mathfrak{g}_1(B)$ auch $\mu_o(A) = 0$ oder $\mu_o(B) = 0$ gilt, ist die Behauptung in diesem Fall erfüllt. Betrachte nun den verbleibenden Fall $\mathfrak{d}_1(A) = o = \mathfrak{d}_1(B)$. Sei $A_1, \dots, A_k$ ein Vertretersystem der Rechtsnebenklassen bezüglich U_2 von $U_2 A U_2$ und $B_1, \dots, B_m$ ein Vertretersystem der Rechtsnebenklassen bezüglich U_2 von $U_2 B U_2$. Dabei seien die B_j nach 2.2.8 ohne Beschränkung der Allgemeinheit so gewählt, dass die Vertreter mit o als größtem gemeinsamen Teiler der Einträge der ersten Spalte die Form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ haben. Nach Definition von μ_o und $*$ ist

$$\mu_o(\llbracket A \rrbracket * \llbracket B \rrbracket) = |\{(i, j) \mid 1 \leq i \leq k, 1 \leq j \leq m, \mathfrak{g}_1(A_i B_j) = o\}|.$$

Sei $1 \leq i \leq k$ und $1 \leq j \leq m$. Ist $\mathfrak{g}_1(B_j) \neq o$, so gilt auch $\mathfrak{g}_1(A_i B_j) \neq o$, denn in der ersten Spalte von $A_i B_j$ stehen Linearkombinationen der

Einträge der ersten Spalte von B_j . Ist $\mathfrak{g}_1(B_j) = \mathfrak{o}$, so gilt

$$A_i B_j = \begin{pmatrix} (A_i)_{11} & (A_i)_{12} \\ (A_i)_{21} & (A_i)_{22} \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} (A_i)_{11} & * \\ (A_i)_{21} & * \end{pmatrix}.$$

Daher gilt $\mathfrak{g}_1(A_i B_j) = \mathfrak{o}$ genau dann, wenn $(A_i)_{11}$ und $(A_i)_{21}$ teilerfremd sind, also wenn $\mathfrak{g}_1(A_i) = \mathfrak{o}$ ist. Insgesamt erhält man

$$\begin{aligned} \mu_{\mathfrak{o}}(f * g) &= |\{(i, j) \mid 1 \leq i \leq k, 1 \leq j \leq m, \mathfrak{g}_1(A_i B_j) = \mathfrak{o}\}| \\ &= |\{(i, j) \mid 1 \leq i \leq k, 1 \leq j \leq m, \mathfrak{g}_1(A_i) = \mathfrak{o}, \mathfrak{g}_1(B_j) = \mathfrak{o}\}| \\ &= |\{1 \leq i \leq k \mid \mathfrak{g}_1(A_i) = \mathfrak{o}\}| \cdot |\{1 \leq j \leq m \mid \mathfrak{g}_1(B_j) = \mathfrak{o}\}| \\ &= \mu_{\mathfrak{o}}(f) \mu_{\mathfrak{o}}(g), \end{aligned}$$

was die Behauptung beweist. □

Nun lässt sich der angekündigte Reduktionssatz aufschreiben und beweisen. Dabei wird eine Formulierung gewählt, die die einfache Struktur der Hecke-Algebra $H(G_1, I_1, U_1)$ ausnutzt.

2.4.2 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen und $a, b, c \in \mathfrak{o}$. Setze $A = \text{diag}(1, a)$ und $B = \text{diag}(1, b)$ sowie $C = \text{diag}(1, c)$. Dann gilt

$$(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) = \begin{cases} 1, & \text{falls } c \in ab\mathfrak{o}^*, \\ 0 & \text{sonst.} \end{cases} \quad \diamond$$

BEWEIS:

Nach Definition von $\mu_{\mathfrak{o}}$ und $*$ gilt

$$\begin{aligned} &\sum_{D::U_2 \setminus I_2 // U_2} (\llbracket A \rrbracket * \llbracket B \rrbracket)(D) \cdot \mu_{\mathfrak{o}}(\llbracket D \rrbracket) \\ &= \mu_{\mathfrak{o}}(\llbracket A \rrbracket * \llbracket B \rrbracket) \stackrel{2.4.1}{=} \mu_{\mathfrak{o}}(\llbracket A \rrbracket) \mu_{\mathfrak{o}}(\llbracket B \rrbracket) \stackrel{2.3.6}{=} N(\mathfrak{d}_2(A)) N(\mathfrak{d}_2(B)) \\ &= N(a\mathfrak{o}) N(b\mathfrak{o}) = N(ab\mathfrak{o}) = N(\mathfrak{d}_2(AB)) \stackrel{2.3.6}{=} \mu_{\mathfrak{o}}(\llbracket AB \rrbracket). \end{aligned}$$

Es ist $AB \in \text{Tr}(\llbracket A \rrbracket * \llbracket B \rrbracket)$ nach 1.1.9, und wegen $(\llbracket A \rrbracket * \llbracket B \rrbracket)(D) \in \mathbb{N}_0$ für jedes $D \in I_2$ nach Definition von $*$ gilt sogar $(\llbracket A \rrbracket * \llbracket B \rrbracket)(AB) \geq 1$. Es folgt

$$\begin{aligned}
 0 &\leq \sum_{\substack{D::U_2 \setminus I_2 // U_2 \\ D \notin U_2 AB U_2}} (\llbracket A \rrbracket * \llbracket B \rrbracket)(D) \cdot \mu_{\mathfrak{o}}(\llbracket D \rrbracket) \\
 &= \sum_{D::U_2 \setminus I_2 // U_2} (\llbracket A \rrbracket * \llbracket B \rrbracket)(D) \cdot \mu_{\mathfrak{o}}(\llbracket D \rrbracket) \\
 &\quad - (\llbracket A \rrbracket * \llbracket B \rrbracket)(AB) \cdot \mu_{\mathfrak{o}}(\llbracket AB \rrbracket) \\
 &= \mu_{\mathfrak{o}}(\llbracket AB \rrbracket) - (\llbracket A \rrbracket * \llbracket B \rrbracket)(AB) \cdot \mu_{\mathfrak{o}}(\llbracket AB \rrbracket) \\
 &= (1 - (\llbracket A \rrbracket * \llbracket B \rrbracket)(AB)) \cdot \mu_{\mathfrak{o}}(\llbracket AB \rrbracket) \leq 0,
 \end{aligned}$$

also

$$\sum_{\substack{D::U_2 \setminus I_2 // U_2 \\ D \notin U_2 AB U_2}} (\llbracket A \rrbracket * \llbracket B \rrbracket)(D) \cdot \mu_{\mathfrak{o}}(\llbracket D \rrbracket) = 0$$

und

$$(1 - (\llbracket A \rrbracket * \llbracket B \rrbracket)(AB)) \cdot \mu_{\mathfrak{o}}(\llbracket AB \rrbracket) = 0.$$

Mit 2.3.6 folgt $\mu_{\mathfrak{o}}(\llbracket AB \rrbracket) = \mu_{\mathfrak{o}}(\llbracket \text{diag}(1, ab) \rrbracket) > 0$, also erhält man aus der letzten abgesetzten Gleichung $(\llbracket A \rrbracket * \llbracket B \rrbracket)(AB) = 1$. Da in der vorletzten abgesetzten Gleichung auf der linken Seite alle Summanden nichtnegativ sind, müssen sie alle gleich 0 sein. Insbesondere muss $(\llbracket A \rrbracket * \llbracket B \rrbracket)(D) = 0$ gelten, falls $\mu_{\mathfrak{o}}(\llbracket D \rrbracket) > 0$ gilt. Für alle $d \in \mathfrak{o}$ hat man aber $\mu_{\mathfrak{o}}(\llbracket \text{diag}(1, d) \rrbracket) = N(d\mathfrak{o}) > 0$ nach 2.3.6, also gilt $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) = 0$, falls $C \notin U_2 AB U_2$. Da $C \in U_2 AB U_2$ nach 2.2.5 äquivalent zu $c \in ab\mathfrak{o}^*$ ist, folgt nun die Behauptung. $\square$

Zum Abschluss dieses Abschnitts steht noch eine Bemerkung zu einer Verallgemeinerung von 2.4.2.

2.4.3 BEMERKUNG: Der gerade bewiesene Satz ist ein Spezialfall der folgenden aus der klassischen Hecke-Theorie

motivierten Vermutung, die für $n > 2$ noch nicht bewiesen werden konnte: Sind $A', B', C' \in I_{n-1}$ gegeben (wieder mit den Bezeichnungen aus 2.3.1) und $A = \text{diag}(1, A')$ sowie $B = \text{diag}(1, B')$ und $C = \text{diag}(1, C')$ gesetzt, dann gilt

$$(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) = (\llbracket A' \rrbracket * \llbracket B' \rrbracket)(C').$$

Diese Aussage wird für den klassischen Fall, dass $\mathfrak{o}$ ein Hauptidealring ist, in [Fre83] IV.2.5 (S. 240) formuliert und bewiesen. $\diamond$

§ 2.5

METHODEN ZUR BERECHNUNG KONKRETER PRODUKTE

In diesem Abschnitt werden deterministische und probabilistische Algorithmen zur Berechnung von konkreten Produkten in Hecke-Algebren zu unimodularen Gruppen vorgestellt. Die wichtigsten Bestandteile dabei sind algorithmisch überprüfbare Kriterien für die Gleichheit von Doppelnebenklassen und Methoden zur Zerlegung von Doppelnebenklassen in Rechtsnebenklassen. Sind diese gegeben, kann der im folgende Satz formulierte allgemeine Algorithmus zur Produktberechnung verwendet werden.

2.5.1 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen und der folgende Algorithmus gegeben, der auf Matrizen $A, B \in I_n$ arbeitet:

- (1) Bestimme durch Zerlegung von $[A]$ und $[B]$ in Rechtsnebenklassen Matrizen $A_1, \dots, A_k \in [A]$ und $B_1, \dots, B_m \in [B]$, die ein Vertretersystem von $U_n \backslash [A]$ beziehungsweise $U_n \backslash [B]$ bilden.
- (2) Setze $D = \{\}$.

- (3) Für jedes Paar (i, j) mit $1 \leq i \leq k$ und $1 \leq j \leq m$ überprüfe, ob es ein $C' \in D$ mit $[A_i B_j] = [C']$ gibt; falls dies nicht der Fall ist, füge $A_i B_j$ als Element zu D hinzu und setze $c_{A_i B_j} = 1$; gibt es hingegen ein $C' \in D$ mit $[A_i B_j] = [C']$, das zudem noch $U_n C' = U_n A_i B_j$ erfüllt, so erhöhe $c_{C'}$ um 1.

Terminiert dieser Algorithmus, erhält man $D \subseteq I_n$ und $c_C \in \mathbb{N}$ für alle $C \in D$, so dass

$$[A] * [B] = \sum_{C \in D} c_C [C]$$

gilt. ◇

BEWEIS:

Die Aussage folgt aus 1.1.10. □

Das in dem gerade aufgestellten Algorithmus benötigte Gleichheitskriterium für Doppelnebenklassen ist hier durch 2.2.5 gegeben, so dass nur die Zerlegung in Rechtsnebenklassen zu untersuchen bleibt.

Verwendet man die für den Fall $n = 2$ bereits hergeleiteten Formeln für die Anzahl von Rechtsnebenklassen in einer gegebenen Doppelnebenklasse, lässt sich der folgende Algorithmus vom Las-Vegas-Typ zur Zerlegung beliebiger Doppelnebenklassen der Form $U_2 A U_2$ formulieren.

2.5.2 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen und der folgende Algorithmus gegeben, der auf einer Matrix $A \in I_2$ arbeitet und ein endliches Erzeugendensystem S von U_2 benötigt:

- (1) Berechne $k = \mu(A)$ gemäß 2.3.7.
- (2) Setze $R = \{A\}$.
- (3) Wähle »zufällig« ein $l \in \mathbb{N}$ (»nicht zu groß«).

- (4) Setze $Q = E_2$. Wiederhole nun l -mal den folgenden Schritt: Wähle zufällig ein Element C von $S \cup \{P^{-1} \mid P \in S\}$ und verwende bei der nächsten Wiederholung $Q \cdot C$ anstelle von Q .
- (5) Wenn es kein $B \in R$ mit $U_2 A Q = U_2 B$ gibt, füge AQ als Element zu R hinzu.
- (6) Wenn $|R| < k$ gilt, gehe zu Schritt (3), ansonsten Ende.

Terminiert dieser Algorithmus, erhält man mit R ein Vertretersystem von $U_n \backslash [A]$. $\diamond$

BEWEIS:

Gemäß Schritt (5) enthält R nie zwei verschiedene Matrizen, die in derselben Rechtsnebenklasse bezüglich U_2 liegen. Weiter werden höchstens Elemente von $[A]$ zu R hinzugefügt. Da nun gemäß Schritt (6) der Algorithmus nur terminiert, wenn R dieselbe Mächtigkeit wie ein Vertretersystem von $U_2 \backslash [A]$ erreicht, muss in diesem Fall dann auch R ein Vertretersystem von $U_2 \backslash [A]$ sein. $\square$

Ein für die Durchführung einer Zerlegung in Rechtsnebenklassen nach diesem Algorithmus benötigtes Erzeugendensystem von U_2 lässt sich in Spezialfällen einfach angeben.

2.5.3 SATZ: Sei K ein algebraischer Zahlkörper und $\mathfrak{o}$ dessen Ganzheitsring. Weiter seien $\omega_1, \dots, \omega_n \in \mathfrak{o}$ und Einheiten $\varepsilon_1, \dots, \varepsilon_t \in \mathfrak{o}^*$ so gewählt, dass $\mathfrak{o} = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$ gilt und $\{\varepsilon_1, \dots, \varepsilon_t\}$ ein Gruppenerzeugendensystem von $\mathfrak{o}^*$ darstellt. Ist nun entweder

- (i) K kein imaginärquadratischer Zahlkörper oder
- (ii) $K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11})\}$ (also K imaginärquadratischer Zahlkörper und $\mathfrak{o}$ zusammen mit der üblichen Norm N ein Euklidischer Ring),

so ist

$$\left\{ \begin{pmatrix} 1 & \omega_k \\ 0 & 1 \end{pmatrix} \mid 1 \leq k \leq n \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ \omega_k & 1 \end{pmatrix} \mid 1 \leq k \leq n \right\} \\ \cup \left\{ \begin{pmatrix} \varepsilon_k & 0 \\ 0 & 1 \end{pmatrix} \mid 1 \leq k \leq t \right\}$$

ein Erzeugendensystem von $\mathrm{GL}_2(\mathfrak{o})$. ◇

BEWEIS:

Setze

$$S_1 = \left\{ \begin{pmatrix} 1 & \omega_k \\ 0 & 1 \end{pmatrix} \mid 1 \leq k \leq n \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ \omega_k & 1 \end{pmatrix} \mid 1 \leq k \leq n \right\} \quad \text{und} \\ S_2 = \left\{ \begin{pmatrix} \varepsilon_k & 0 \\ 0 & 1 \end{pmatrix} \mid 1 \leq k \leq t \right\},$$

und sei $Q \in \mathrm{GL}_2(\mathfrak{o})$. Setzt man $\varepsilon = \det Q$ und $P_1 = \mathrm{diag}(\varepsilon, 1)$, so ist $P_1^{-1}Q \in \mathrm{GL}_2(\mathfrak{o})$ mit $\det P_1^{-1}Q = \varepsilon^{-1}\varepsilon = 1$. Nach [Hah89] 4.3.10 und den nachfolgenden Bemerkungen (S. 173) gibt es unter den gemachten Voraussetzungen an K Matrizen $P_2, \dots, P_m \in \mathfrak{o}^{2 \times 2}$ mit $P_1^{-1}Q = P_2 \cdots P_m$, so dass für jedes $1 \leq j \leq m$ entweder $P_j = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ oder $P_j = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ gilt. Für jedes $r \in \mathfrak{o} = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ gibt es nun $a_1, \dots, a_s \in \{\omega_1, \dots, \omega_n\}$ und $v_1, \dots, v_s \in \{1, -1\}$, so dass $r = v_1a_1 + \cdots + v_sa_s$ und folglich

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix}^{v_1} \cdots \begin{pmatrix} 1 & a_s \\ 0 & 1 \end{pmatrix}^{v_s} \quad \text{sowie} \\ \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a_1 & 1 \end{pmatrix}^{v_1} \cdots \begin{pmatrix} 1 & 0 \\ a_s & 1 \end{pmatrix}^{v_s}$$

gilt. Demnach lässt sich P_j für jedes $2 \leq j \leq m$ als Produkt von Matrizen aus S_1 und Inversen von Matrizen aus S_1 darstellen. Da zu ε nach Wahl der $\varepsilon_1, \dots, \varepsilon_t$ ganze Zahlen $w_1, \dots, w_t$ mit $\varepsilon = \varepsilon_1^{w_1} \cdots \varepsilon_t^{w_t}$ existieren, liegt P_1 im Erzeugnis von S_2 . Somit folgt insgesamt aus

$Q = P_1 \cdots P_m$ (was man aus $P_1^{-1}Q = P_2 \cdots P_m$ erhält), dass Q in der von $S_1 \cup S_2$ erzeugten Gruppe liegt. Da Q aus $\mathrm{GL}_2(\mathfrak{o})$ beliebig gewählt war und zudem $S_1 \cup S_2 \subseteq \mathrm{GL}_2(\mathfrak{o})$ gilt, erhält man, dass das Gruppenerzeugnis von $S_1 \cup S_2$ genau gleich $\mathrm{GL}_2(\mathfrak{o})$ ist. $\square$

Ein erstes Beispiel für den Algorithmus aus 2.5.2 verwendet den gerade bewiesenen Satz zur Angabe des benötigten Erzeugendensystems von U_2 .

2.5.4 BEISPIEL: Sei $\omega = \sqrt{10}$ und $K = \mathbb{Q}(\omega)$ sowie $\mathfrak{o}$ der Ganzheitsring von K . Aus der algebraischen Zahlentheorie ist bekannt, dass $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega$ gilt und $\mathfrak{o}^*$ von -1 und $3 + \omega$ erzeugt wird (Spezialfall des Dirichletschen Einheitsensatzes). Somit kann man nach 2.5.3 in dem Algorithmus aus 2.5.2 die Menge S als

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3+\omega & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

wählen.

Verwende nun die Bezeichnungen aus 1.1.4 mit $G = \mathrm{GL}_2(K)$ und $U = \mathrm{GL}_2(\mathfrak{o})$ sowie $M = \mathrm{IL}_2(\mathfrak{o})$. Der Algorithmus aus 2.5.2 liefert beispielsweise die Zerlegungen

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right]_{\mathbb{R}} + \left[\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right]_{\mathbb{R}} + \left[\begin{pmatrix} 1 & \omega \\ 0 & 2 \end{pmatrix} \right]_{\mathbb{R}} \\ &\quad + \left[\begin{pmatrix} 1 & 1+\omega \\ 0 & 2 \end{pmatrix} \right]_{\mathbb{R}} + \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right]_{\mathbb{R}} + \left[\begin{pmatrix} 2 & 0 \\ \omega & 1 \end{pmatrix} \right]_{\mathbb{R}} \end{aligned}$$

und

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] &= \sum_{b=0}^9 \left[\begin{pmatrix} 1 & b \\ 0 & \omega \end{pmatrix} \right]_{\mathbb{R}} + \sum_{c \in \{0,2,4,5,6,8\}} \left[\begin{pmatrix} \omega & 0 \\ c & 1 \end{pmatrix} \right]_{\mathbb{R}} \\ &\quad + \left[\begin{pmatrix} \omega+5 & 2 \\ 5 & 2-\omega \end{pmatrix} \right]_{\mathbb{R}} + \left[\begin{pmatrix} 2 & \omega+5 \\ 4-\omega & 5 \end{pmatrix} \right]_{\mathbb{R}}. \end{aligned}$$

Mit 2.5.1 und den gerade berechneten Zerlegungen erhält man beispielsweise die Produkte

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \right] + 6 \left[\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right] + \left[\begin{pmatrix} 2 & \omega \\ 0 & 2 \end{pmatrix} \right]$$

und

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix} \right] + 3 \left[\begin{pmatrix} \omega & 2 \\ 0 & \omega \end{pmatrix} \right] \\ &\quad + 6 \left[\begin{pmatrix} \omega & 5 \\ 0 & \omega \end{pmatrix} \right] + 18 \left[\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} \right] \end{aligned}$$

sowie

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 0 \\ 0 & 2\omega \end{pmatrix} \right] + \left[\begin{pmatrix} 2 & 0 \\ 0 & \omega \end{pmatrix} \right]. \quad \diamond$$

Der vorgestellte Zerlegungsalgorithmus kann leicht modifiziert auch in den Fällen benutzt werden, in denen 2.5.3 keine Aussage über die Erzeuger von U_2 liefert, indem man anstelle eines Erzeugendensystems von U_2 eine beliebige Teilmenge S von U_2 verwendet. Die Terminierung ist dann im allgemeinen weniger wahrscheinlich, aber falls diese eintritt, wird immer noch eine korrekte Zerlegung geliefert. Das folgende Beispiel zeigt, dass man auch in den Fällen, in denen die in 2.5.3 angegebene Menge kein Erzeugendensystem ist, mit dieser Menge S im Algorithmus gute Ergebnisse erzielen kann.

2.5.5 BEISPIEL: Sei $\omega = \sqrt{-5}$ und $K = \mathbb{Q}(\omega)$ sowie $\mathfrak{o}$ der Ganzheitsring von K . Aus der algebraischen Zahlentheorie ist bekannt, dass $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega$ und $\mathfrak{o}^* = \{1, -1\}$ gilt. Somit kann man mit der gerade diskutierten Modifikation von 2.5.2 in dem Algorithmus

$$S = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \omega & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

wählen.

Verwende nun die Bezeichnungen aus 1.1.4 mit $G = \mathrm{GL}_2(K)$ und $U = \mathrm{GL}_2(\mathfrak{o})$ sowie $M = \mathrm{IL}_2(\mathfrak{o})$. Der Algorithmus aus 2.5.2 liefert beispielsweise die Zerlegungen

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 1 & \omega \\ 0 & 2 \end{pmatrix} \right]_{\mathrm{R}} \\ &\quad + \left[\begin{pmatrix} 1 & 1+\omega \\ 0 & 2 \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 2 & 0 \\ 1+\omega & 1 \end{pmatrix} \right]_{\mathrm{R}} \end{aligned}$$

und

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] &= \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 1 & 1 \\ 0 & \omega \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 1 & -1 \\ 0 & \omega \end{pmatrix} \right]_{\mathrm{R}} \\ &\quad + \left[\begin{pmatrix} 1 & 2 \\ 0 & \omega \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} 1 & -2 \\ 0 & \omega \end{pmatrix} \right]_{\mathrm{R}} + \left[\begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \right]_{\mathrm{R}}. \end{aligned}$$

Mit 2.5.1 und den gerade berechneten Zerlegungen erhält man beispielsweise die Produkte

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \right] + 6 \left[\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right] \\ &\quad + \left[\begin{pmatrix} 2 & 1+\omega \\ 0 & 2 \end{pmatrix} \right] \end{aligned}$$

und

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \right] + 6 \left[\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} \right]$$

sowie

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right] * \left[\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \right] = \left[\begin{pmatrix} 1 & 0 \\ 0 & 2\omega \end{pmatrix} \right].$$

Für eine Übersicht weiterer Produkte verwende für Ideale $\mathfrak{b}_1, \mathfrak{b}_2$ von $\mathfrak{o}$ die Notation $[\mathfrak{b}_1, \mathfrak{b}_2]$ zur Beschreibung von $[B]$ für eine Matrix

$B \in \text{IL}_2(\mathfrak{o})$ mit $\mathfrak{e}_i(\mathfrak{b}_i) = \mathfrak{b}_i$ für alle $i \in \{1, 2\}$ (sofern eine solche Matrix existiert), und erlaube, dass in dieser Notation Hauptideale der Form $\mathfrak{b}_i\mathfrak{o}$ abkürzend durch $\mathfrak{b}_i$ angegeben werden können (so dass etwa $\llbracket 1, 2 \rrbracket$ dasselbe bedeutet wie $\llbracket \mathfrak{o}, 2\mathfrak{o} \rrbracket$). Weiter führe die Bezeichnungen

$$\mathfrak{p}_2 = 2\mathfrak{o} + (1 + \omega)\mathfrak{o}$$

$$\mathfrak{p}_{31} = 3\mathfrak{o} + (1 + \omega)\mathfrak{o}$$

$$\mathfrak{p}_{32} = 3\mathfrak{o} + (2 + \omega)\mathfrak{o}$$

ein (so dass $\mathfrak{p}_2^2 = 2\mathfrak{o}$ und $\mathfrak{p}_{31}\mathfrak{p}_{32} = 3\mathfrak{o}$ gilt). Dann erhält man als Produkte der Form $\llbracket A \rrbracket * \llbracket B \rrbracket$ mit $\llbracket A \rrbracket * \llbracket B \rrbracket \neq \llbracket AB \rrbracket$ und in der Menge $\{C \in \text{IL}_2(\mathfrak{o}) \mid \det C \in 4\mathfrak{o}^*\}$ enthaltenem Träger

$$\llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket 1, \mathfrak{p}_2^2 \rrbracket = \llbracket 1, \mathfrak{p}_2^4 \rrbracket + \llbracket \mathfrak{p}_2, \mathfrak{p}_2^3 \rrbracket + 6\llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^2 \rrbracket,$$

mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 5\mathfrak{o}^*\}$ enthaltenem Träger

$$\llbracket 1, \omega \rrbracket * \llbracket 1, \omega \rrbracket = \llbracket 1, \omega^2 \rrbracket + 6\llbracket \omega, \omega \rrbracket,$$

mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 6\mathfrak{o}^*\}$ enthaltenem Träger

$$\llbracket 1, \mathfrak{p}_2\mathfrak{p}_{31} \rrbracket * \llbracket 1, \mathfrak{p}_2\mathfrak{p}_{32} \rrbracket = \llbracket 1, \mathfrak{p}_2^2\mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket + 3\llbracket \mathfrak{p}_2, \mathfrak{p}_2\mathfrak{p}_{31}, \mathfrak{p}_{32} \rrbracket,$$

mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 8\mathfrak{o}^*\}$ enthaltenem Träger

$$\llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket 1, \mathfrak{p}_2^4 \rrbracket = \llbracket 1, \mathfrak{p}_2^6 \rrbracket + \llbracket \mathfrak{p}_2, \mathfrak{p}_2^5 \rrbracket + 4\llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^4 \rrbracket,$$

$$\llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket \mathfrak{p}_2, \mathfrak{p}_2^3 \rrbracket = \llbracket \mathfrak{p}_2, \mathfrak{p}_2^5 \rrbracket + \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^4 \rrbracket + 6\llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^3 \rrbracket,$$

mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 9\mathfrak{o}^*\}$ enthaltenem Träger

$$\begin{aligned} \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket * \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket &= \llbracket 1, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket + 4\llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}\mathfrak{p}_{32}^2 \rrbracket \\ &\quad + 4\llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32} \rrbracket + 16\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket, \end{aligned}$$

mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 16\mathfrak{o}^*\}$ enthaltenem Träger

$$\begin{aligned}
 \llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket 1, \mathfrak{p}_2^6 \rrbracket &= \llbracket 1, \mathfrak{p}_2^8 \rrbracket + \llbracket \mathfrak{p}_2, \mathfrak{p}_2^7 \rrbracket + 4\llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket \mathfrak{p}_2, \mathfrak{p}_2^5 \rrbracket &= \llbracket \mathfrak{p}_2, \mathfrak{p}_2^7 \rrbracket + \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket + 4\llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^5 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_2^2 \rrbracket * \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^4 \rrbracket &= \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket + \llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^5 \rrbracket + 6\llbracket \mathfrak{p}_2^4, \mathfrak{p}_2^4 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_2^4 \rrbracket * \llbracket 1, \mathfrak{p}_2^4 \rrbracket &= \llbracket 1, \mathfrak{p}_2^8 \rrbracket + \llbracket \mathfrak{p}_2, \mathfrak{p}_2^7 \rrbracket + 2\llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket \\
 &\quad + 4\llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^5 \rrbracket + 24\llbracket \mathfrak{p}_2^4, \mathfrak{p}_2^4 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_2^4 \rrbracket * \llbracket \mathfrak{p}_2, \mathfrak{p}_2^3 \rrbracket &= \llbracket \mathfrak{p}_2, \mathfrak{p}_2^7 \rrbracket + \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket + 4\llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^5 \rrbracket, \\
 \llbracket \mathfrak{p}_2, \mathfrak{p}_2^3 \rrbracket * \llbracket \mathfrak{p}_2, \mathfrak{p}_2^3 \rrbracket &= \llbracket \mathfrak{p}_2^2, \mathfrak{p}_2^6 \rrbracket + \llbracket \mathfrak{p}_2^3, \mathfrak{p}_2^5 \rrbracket + 6\llbracket \mathfrak{p}_2^4, \mathfrak{p}_2^4 \rrbracket,
 \end{aligned}$$

und mit in $\{A \in \text{IL}_2(\mathfrak{o}) \mid \det A \in 27\mathfrak{o}^*\}$ enthaltenem Träger

$$\begin{aligned}
 \llbracket 1, \mathfrak{p}_{31}^2 \rrbracket * \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32}^3 \rrbracket &= \llbracket 1, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^3 \rrbracket + 3\llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^3 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{31}^2 \rrbracket * \llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}\mathfrak{p}_{32}^2 \rrbracket &= \llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^2 \rrbracket + 3\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket * \llbracket 1, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket &= \llbracket 1, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^3 \rrbracket + 3\llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^3 \rrbracket \\
 &\quad + 3\llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^2 \rrbracket + 9\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket * \llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}\mathfrak{p}_{32}^2 \rrbracket &= \llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^3 \rrbracket + 3\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{31}\mathfrak{p}_{32} \rrbracket * \llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32} \rrbracket &= \llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^2 \rrbracket + 3\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{32}^2 \rrbracket * \llbracket 1, \mathfrak{p}_{31}^3\mathfrak{p}_{32} \rrbracket &= \llbracket 1, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^3 \rrbracket + 3\llbracket \mathfrak{p}_{32}, \mathfrak{p}_{31}^3\mathfrak{p}_{32}^2 \rrbracket, \\
 \llbracket 1, \mathfrak{p}_{32}^2 \rrbracket * \llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}^2\mathfrak{p}_{32} \rrbracket &= \llbracket \mathfrak{p}_{31}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^3 \rrbracket + 3\llbracket \mathfrak{p}_{31}\mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}^2 \rrbracket.
 \end{aligned}$$

Um auch ein Beispiel für das Verhalten einer trägen Primzahl zu geben, wird noch das Produkt

$$\llbracket 1, 11 \rrbracket * \llbracket 1, 11 \rrbracket = \llbracket 1, 121 \rrbracket + 122\llbracket 11, 11 \rrbracket$$

berechnet.

◇

Möchte man nun Produkte in $H(G_n, I_n, U_n)$ für $n \geq 3$ berechnen, steht bislang ein zu 2.3.7 analoges Ergebnis nicht zu Verfügung. Für die Zerlegung von Doppelnebenklassen in Rechtsnebenklassen wird daher ein anderes Kriterium benötigt, das garantiert, dass zu einem bestimmten Zeitpunkt bereits alle möglichen Rechtsnebenklassen gefunden wurden. Ein solches Kriterium kann aus der folgenden hinreichenden Bedingung für die Gleichheit zweier Rechtsnebenklassen für den Fall von Diagonalmatrizen hergeleitet werden.

2.5.6 SATZ: Es sei $\mathfrak{o}$ ein normendlicher Dedekind-Ring und $n \in \mathbb{N}$. Weiter sei $U_n = \text{GL}_n(\mathfrak{o})$ und die Diagonalmatrix $A = \text{diag}(a_1, \dots, a_n) \in \text{IL}_n(\mathfrak{o})$ gegeben. Ist für $P, Q \in U_n$ dann

$$(Q - P)_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \dots \cap a_n\mathfrak{o})$$

für alle $1 \leq i, j \leq n$ erfüllt, so gilt bereits $U_n A P = U_n A Q$. $\diamond$

BEWEIS:

Setze $R = QP^{-1}$. Dann gilt

$$R - E_n = QP^{-1} - E_n = (Q - P)P^{-1}.$$

Da mit P auch $(P^{-1})^T$ in U_n liegt, erhält man

$$\begin{aligned} \sum_{j=1}^n ((Q - P)P^{-1})_{ij}\mathfrak{o} &= \sum_{j=1}^n (((Q - P)P^{-1})^T)_{ji}\mathfrak{o} \\ &= \sum_{j=1}^n ((P^{-1})^T(Q - P)^T)_{ji}\mathfrak{o} \\ &\stackrel{2.2.8}{=} \sum_{j=1}^n ((Q - P)^T)_{ji}\mathfrak{o} \\ &= \sum_{j=1}^n (Q - P)_{ij}\mathfrak{o}. \end{aligned}$$

Da nach Voraussetzung

$$a_i^{-1}(a_1\mathfrak{o} \cap \dots \cap a_n\mathfrak{o}) \mid (Q - P)_{i1}\mathfrak{o} + \dots + (Q - P)_{in}\mathfrak{o}$$

gilt, folgt somit insbesondere $(R - E_n)_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \dots \cap a_n\mathfrak{o})$ für alle $1 \leq i, j \leq n$. Definiere nun $D \in K^{n \times n}$ durch $(D)_{ij} = a_i(R - E_n)_{ij}a_j^{-1}$ für alle $1 \leq i, j \leq n$. Dann gilt sogar $D \in \mathfrak{o}^{n \times n}$, denn für alle $1 \leq i, j \leq n$ hat man

$$\begin{aligned}(D)_{ij} &= a_i(R - E_n)_{ij}a_j^{-1} \in a_i a_i^{-1}(a_1\mathfrak{o} \cap \dots \cap a_n\mathfrak{o})a_j^{-1} \\ &= (a_1\mathfrak{o} \cap \dots \cap a_n\mathfrak{o})a_j^{-1} \subseteq a_j\mathfrak{o}a_j^{-1} = \mathfrak{o}.\end{aligned}$$

Weiter gilt nun

$$\begin{aligned}(A^{-1}DA)_{ij} &= (\text{diag}(a_1^{-1}, \dots, a_n^{-1})D \text{diag}(a_1, \dots, a_n))_{ij} \\ &= a_i^{-1}(D)_{ij}a_j = a_i^{-1}a_i(R - E_n)_{ij}a_j^{-1}a_j = (R - E_n)_{ij}\end{aligned}$$

für alle $1 \leq i, j \leq n$, also hat man $A^{-1}DA = R - E_n$ und folglich

$$ARA^{-1} - E_n = A(R - E_n)A^{-1} = D \in \mathfrak{o}^{n \times n},$$

woraus man auch $ARA^{-1} \in \mathfrak{o}^{n \times n}$ erhält. Da wegen $P, Q \in U_n$ auch $R = QP^{-1} \in U_n$ und damit $R \in \mathfrak{o}^*$ gilt, ist

$$\det(ARA^{-1}) = (\det A)(\det R)(\det A)^{-1} = \det R \in \mathfrak{o}^*,$$

also erhält man zusammen mit $ARA^{-1} \in \mathfrak{o}^{n \times n}$, dass $ARA^{-1} \in U_n$ und somit $R \in A^{-1}U_nA$ gilt. Da schon gezeigt wurde, dass $R \in U_n$ gilt, hat man insgesamt $R \in U_n \cap (A^{-1}U_nA)$, und aus $R = QP^{-1}$ folgt damit $(U_n \cap (A^{-1}U_nA))P = (U_n \cap (A^{-1}U_nA))Q$. Gemäß dem Beweis von 1.1.3 ist dies äquivalent zu $U_nAP = U_nAQ$, was die zu zeigende Aussage war. $\square$

Mit dem geraden bewiesene Satz lässt sich ein Algorithmus zur Zerlegung von $U_n \text{diag}(a_1, \dots, a_n)U_n$ in Rechtsnebenklassen für beliebige $n \in \mathbb{N}$ formulieren.

2.5.7 SATZ: Es seien die Bezeichnungen aus 2.3.1 übernommen und der folgende Algorithmus gegeben, der auf einer Matrix $A = \text{diag}(a_1, \dots, a_n) \in I_n$ arbeitet:

- (1) Wähle für jedes $1 \leq i \leq n$ ein Vertretersystem V_i der Restklassenmenge $\mathfrak{o} \parallel a_i^{-1}(a_1\mathfrak{o} \cap \cdots \cap a_n\mathfrak{o})$.
- (2) Setze $W = \{Q' \in \mathfrak{o}^{n \times n} \mid (Q')_{ij} \in V_i \text{ für alle } 1 \leq i, j \leq n\}$ und $R = \emptyset$.
- (3) Wähle ein $Q' \in W$.
- (4) Finde – sofern möglich – ein $Q \in U_n$ mit

$$(Q - Q')_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \cdots \cap a_n\mathfrak{o})$$

für alle $1 \leq i, j \leq n$. Falls ein solches Q nicht existiert, entferne Q' aus W und gehe zurück zu Schritt (3).

- (5) Wenn es kein $B \in R$ mit $U_2AQ = U_2B$ gibt, füge AQ als Element zu R hinzu.
- (6) Entferne Q' aus W . Wenn $W \neq \emptyset$ gilt, gehe zurück zu Schritt (3), ansonsten Ende.

Terminiert dieser Algorithmus, erhält man mit R ein Vertretersystem von $U_n \parallel [A]$. $\diamond$

BEWEIS:

Gemäß Schritt (5) enthält R nie zwei verschiedene Matrizen, die in derselben Rechtsnebenklasse bezüglich U_2 liegen. Weiter werden höchstens Elemente von $[A]$ zu R hinzugefügt. Somit verbleibt nur noch zu zeigen, dass die Vereinigung aller Mengen der Form U_nA' für $A' \in R$ die Menge $[A]$ enthält. Sei $B \in [A]$. Dann gibt es ein $P \in U_n$ mit $B \in U_nAP$. Ist W wie in Schritt (2) gewählt, so gibt es nach Definition dieser Menge ein $Q' \in W$ mit $(P - Q')_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \cdots \cap a_n\mathfrak{o})$ für alle $1 \leq i, j \leq n$. Konstruiert man zu Q' wie in Schritt (4) ein $Q \in U_n$ mit $(Q - Q')_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \cdots \cap a_n\mathfrak{o})$ für alle $1 \leq i, j \leq n$, so gilt auch $(P - Q)_{ij} \in a_i^{-1}(a_1\mathfrak{o} \cap \cdots \cap a_n\mathfrak{o})$ für alle $1 \leq i, j \leq n$ und folglich $U_nAP = U_nAQ$ nach 2.5.6. Da nun wegen $Q' \in W$ mindestens einmal in Schritt (5) ein Vertreter der Rechtsnebenklasse U_nAQ zu R hinzugefügt wird, gibt es also ein $B' \in R$ mit $U_nB' = U_nAQ = U_nAP$, also ist

wegen $B \in U_n AP$ die Matrix B in der Vereinigung aller Rechtsnebenklassen der Form $U_n A'$ für $A' \in R$ enthalten. Da B beliebig aus $[A]$ gewählt werden kann, schließt dies den Beweis ab. $\square$

Bei der Durchführung von Schritt (4) im letzten Algorithmus hilft folgende Charakterisierung von Teilmatrizen von Matrizen aus $\mathrm{GL}_n(\mathfrak{o})$.

2.5.8 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring und $A' \in \mathfrak{o}^{n \times k}$ für ein $1 \leq k \leq n$ gegeben. Dann sind äquivalent:

- (i) Es gilt $\mathfrak{d}_j(A') = \mathfrak{o}$ für alle $1 \leq j \leq k$.
- (ii) Es gibt ein $R \in \mathrm{GL}_n(\mathfrak{o})$ mit $(R)_{ij} = (A')_{ij}$ für alle $1 \leq i \leq n$ und $1 \leq j \leq k$. $\diamond$

BEWEIS:

(i) $\Rightarrow$ (ii): Es gelte $\mathfrak{d}_j(A') = \mathfrak{o}$ für alle $1 \leq j \leq k$. Setze

$$A = \begin{pmatrix} A_1 & 0 \\ A_3 & 0 \end{pmatrix} \in \mathfrak{o}^{n \times n} \quad \text{und} \quad B = \begin{pmatrix} E_k & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{o}^{n \times n}$$

mit

$$A_1 = \begin{pmatrix} (A)_{11} & \cdots & (A)_{1k} \\ \vdots & \ddots & \vdots \\ (A)_{k1} & \cdots & (A)_{kk} \end{pmatrix}$$

und

$$A_3 = \begin{pmatrix} (A)_{k+1,1} & \cdots & (A)_{k+1,k} \\ \vdots & \ddots & \vdots \\ (A)_{n1} & \cdots & (A)_{nk} \end{pmatrix}.$$

Gemäß Voraussetzung gilt nun $\mathfrak{d}_j(A) = \mathfrak{d}_j(A') = \mathfrak{o} = \mathfrak{d}_j(B)$ für jedes $1 \leq j \leq k$ sowie $\mathfrak{d}_j(A) = \{0\} = \mathfrak{d}_j(B)$ für jedes $k < j \leq n$, und darüberhinaus tritt in jeder Zeile von $A^{[k]}$ nur höchstens ein von 0 verschiedener Eintrag auf (nämlich in der Spalte, die der Spaltenauswahl $\{1, \dots, k\}$ von A entspricht), also gilt $\mathfrak{z}(A) = \mathfrak{h}(K)$, und analog zeigt

man $\mathfrak{J}(B) = \mathfrak{H}(K)$. Nun erhält man aus 2.2.5, dass $P, Q \in \mathrm{GL}_n(\mathfrak{o})$ mit $B = PAQ$ existieren. Schreibe

$$P = \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} \quad \text{und} \quad Q^{-1} = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix} \quad \text{mit} \quad P_1, Q_1 \in \mathfrak{o}^{k \times k}.$$

Aus $B = PAQ$ erhält man $BQ^{-1} = PA$, also

$$\begin{pmatrix} E_k & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix} = \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} \begin{pmatrix} A_1 & 0 \\ A_3 & 0 \end{pmatrix}$$

und damit

$$\begin{pmatrix} Q_1 & Q_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1 A_1 + P_2 A_3 & 0 \\ P_3 A_1 + P_4 A_3 & 0 \end{pmatrix}.$$

Diese Gleichung liefert insbesondere $Q_2 = 0$, und zusammen mit $Q^{-1} \in \mathrm{GL}_n(\mathfrak{o})$ erhält man die Invertierbarkeit von Q_1 in $\mathfrak{o}^{k \times k}$. Setzt man $R = P^{-1} \mathrm{diag}(Q_1, E_{n-k})$, so gilt $R \in \mathrm{GL}_n(\mathfrak{o})$ wegen $Q_1 \in \mathrm{GL}_k(\mathfrak{o})$ und $P \in \mathrm{GL}_n(\mathfrak{o})$, und man hat

$$\begin{aligned} A &= P^{-1} B Q^{-1} = P^{-1} \begin{pmatrix} Q_1 & 0 \\ 0 & 0 \end{pmatrix} = R \begin{pmatrix} Q_1^{-1} & 0 \\ 0 & E_{n-k} \end{pmatrix} \begin{pmatrix} Q_1 & 0 \\ 0 & 0 \end{pmatrix} \\ &= R \begin{pmatrix} E_k & 0 \\ 0 & 0 \end{pmatrix}, \end{aligned}$$

also stimmen die ersten k Spalten von A und R überein, womit R die gewünschten Bedingungen erfüllt.

(ii) $\Rightarrow$ (i): Sei $R \in \mathrm{GL}_n(\mathfrak{o})$ mit $(R)_{ij} = (A')_{ij}$ für alle $1 \leq i \leq n$ und $1 \leq j \leq k$. Fixiere ein $1 \leq j \leq k$, und verwende die Bezeichnungen

$$\begin{aligned} S &= \{f : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid f \text{ injektiv}\}, \\ S_j &= \{f : \{j+1, \dots, n\} \rightarrow \{1, \dots, n\} \mid f \text{ injektiv}\}, \\ S_{j,\tau} &= \{f : \{1, \dots, j\} \rightarrow \{1, \dots, n\} \setminus \mathrm{Bild} \, \tau \mid f \text{ injektiv}\} \end{aligned}$$

für $\tau \in S_j$, und für jedes $\sigma \in S$ sei $\varepsilon(\sigma) \in \{\pm 1\}$ das Vorzeichen der Permutation σ . Dann gilt

$$\begin{aligned} \det R &= \sum_{\sigma \in S} \varepsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n} \\ &= \sum_{\tau \in S_j} \sum_{\varrho \in S_{j,\tau}} \varepsilon(\rho \circ \tau) a_{(\rho \circ \tau)(1),1} \cdots a_{(\rho \circ \tau)(n),n} \\ &= \sum_{\tau \in S_j} \varepsilon(\tau) a_{\tau(j+1),j+1} \cdots a_{\tau(n),n} \underbrace{\sum_{\varrho \in S_{j,\tau}} \varepsilon(\rho) a_{\rho(1),1} \cdots a_{\rho(j),j}}_{=: D(\tau)}. \end{aligned}$$

Nun ist $D(\tau)$ die Determinante der $(j \times j)$ -Untermatrix von A' , die durch Auswahl der Zeilen entsteht, deren Nummern in der Menge $\{1, \dots, n\} \setminus \text{Bild } \tau$ enthalten sind. Da für $\tau \in S_j$ stets $D(\tau) \in \mathfrak{d}_j(A')$ gilt, folgt nun insgesamt $\det R \in \mathfrak{d}_j(A')$, so dass man wegen $\det R \in \mathfrak{o}^*$ dann $\mathfrak{d}_j(A') = \mathfrak{o}$ erhält. Da $1 \leq j \leq k$ beliebig gewählt war, zeigt dies, dass (i) gilt. $\square$

Mit den eingeführten Hilfsmitteln können nun einige Beispiele für den Fall $n = 3$ berechnet werden.

2.5.9 BEISPIEL: Sei $\omega = \sqrt{-5}$ und $K = \mathbb{Q}(\omega)$ sowie $\mathfrak{o}$ der Ganzheitsring von K . Verwende nun die Bezeichnungen aus 1.1.4 mit $G = \text{GL}_3(K)$ und $U = \text{GL}_3(\mathfrak{o})$ sowie $M = \text{IL}_3(\mathfrak{o})$. Zur Berechnung der Zerlegung von $[\text{diag}(1, 1, 2)]$ wird algorithmisch gemäß 2.5.7 vorgegangen, wobei nur dann versucht wird, zu $Q' \in W$ ein zugehöriges $Q \in U_3$ zu finden, wenn Q' die im nächsten Absatz hergeleitete notwendige Bedingung für die Existenz von einem solchen Q erfüllt.

Es existiere zu $Q' \in W$ ein zugehöriges $Q \in U_3$. Da gemäß 2.5.7

$(Q - Q')_{ij} \in 2\mathfrak{o}$ für alle $i \in \{1, 2\}$ und $j \in \{1, 2, 3\}$ gilt, hat man

$$\begin{aligned} \mathfrak{o} &\stackrel{2,5,8}{=} \mathfrak{d}_2 \left(\begin{pmatrix} (Q)_{11} & (Q)_{12} & (Q)_{13} \\ (Q)_{21} & (Q)_{22} & (Q)_{23} \end{pmatrix} \right) \\ &\subseteq \mathfrak{d}_2 \left(\begin{pmatrix} (Q')_{11} & (Q')_{12} & (Q')_{13} \\ (Q')_{21} & (Q')_{22} & (Q')_{23} \end{pmatrix} \right) + 2\mathfrak{o} \subseteq \mathfrak{o}. \end{aligned}$$

Ist also der größte gemeinsame Teiler von $2\mathfrak{o}$ mit dem zweiten Determinantenteiler von $(Q')_{\{1,2\},\{1,2,3\}}$ nicht gleich $\mathfrak{o}$, kann zu Q' kein $Q \in U_3$ existieren.

Ist die hergeleitete notwendige Bedingung für die Existenz einer zu Q' gehörigen Matrix $Q \in U_3$ nicht erfüllt, wird dieses Q' im Algorithmus verworfen; ansonsten werden systematisch Matrizen, die die Kongruenzbedingungen für Q erfüllen, darauf getestet, ob ihre Determinante in $\mathfrak{o}^*$ liegt, und im Erfolgsfall als Wert für Q verwendet. In diesem Beispiel ist dieses Vorgehen stets erfolgreich, so dass man folgende Zerlegung erhält:

$$\begin{aligned} &\llbracket \text{diag}(1, 1, 2) \rrbracket \\ &= \sum_{a,b \in \{0,1,\omega,1+\omega\}} \left\llbracket \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 2 \end{pmatrix} \right\rrbracket_{\mathbb{R}} + \sum_{a \in \{0,1,\omega,1+\omega\}} \left\llbracket \begin{pmatrix} 1 & a & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}} \\ &\quad + \sum_{a,b \in \{0,1\}} \left\llbracket \begin{pmatrix} 1 & a & b \\ 0 & 2 & 0 \\ 0 & 1+\omega & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}} \\ &\quad + \left\llbracket \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}} + \left\llbracket \begin{pmatrix} 2 & 0 & 0 \\ 1+\omega & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}} \\ &\quad + \left\llbracket \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1+\omega & 0 & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}} + \left\llbracket \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 1+\omega & 0 & 1 \end{pmatrix} \right\rrbracket_{\mathbb{R}}. \end{aligned}$$

Analog kann man Zerlegungen von weiteren Doppelnebenklassen der Form $[\text{diag}(1, 1, m)]$ für $m \in \mathfrak{o}$ berechnen. Dabei erhält man etwa, dass $[\text{diag}(1, 1, \omega)]$ in 31 und $[\text{diag}(1, 1, 3)]$ in 169 Rechtsnebenklassen bezüglich U_3 zerfällt. Zur übersichtlicheren Darstellung von sich daraus ergebenden Produkten führe wie in 2.5.5 die Bezeichnungen $\mathfrak{p}_2$ und $\mathfrak{p}_{31}$ sowie $\mathfrak{p}_{32}$ ein (so dass $\mathfrak{p}_2^2 = 2\mathfrak{o}$ und $\mathfrak{p}_{31}\mathfrak{p}_{32} = 3\mathfrak{o}$ gilt) und verwende in analoger Weise die Notation $[[\cdot, \cdot, \cdot]]$ zur Bezeichnung von $[[B]]$ für eine Matrix B mit vorgeschriebenen Elementarteilern. Dann gilt etwa

$$[[1, 1, 2]] * [[1, 1, 2]] = [[1, 1, 4]] + [[1, \mathfrak{p}_2, \mathfrak{p}_2^3]] + 6[[1, 2, 2]],$$

$$[[1, 1, \omega]] * [[1, 1, \omega]] = [[1, 1, 5]] + 6[[1, \omega, \omega]],$$

$$[[1, 1, 2]] * [[1, 1, \omega]] = [[1, 1, 2\omega]],$$

$$\begin{aligned} [[1, 1, 3]] * [[1, 1, 3]] &= [[1, 1, 9]] + 4[[1, \mathfrak{p}_{31}, \mathfrak{p}_{31}\mathfrak{p}_{32}^2]] + 4[[1, \mathfrak{p}_{32}, \mathfrak{p}_{31}^2\mathfrak{p}_{32}]] \\ &\quad + 16[[1, 3, 9]], \end{aligned}$$

$$[[1, 1, 2]] * [[1, 1, 3]] = [[1, 1, 6]],$$

$$[[1, 1, \omega]] * [[1, 1, 3]] = [[1, 1, 3\omega]].$$

◇

§ 2.6

ELEMENTARTEILER VON MATRIXPRODUKTEN

Nachdem im letzten Abschnitt konkrete Produkte der Form $[[A]] * [[B]]$ algorithmisch berechnet wurden, soll es nun darum gehen, theoretische Aussagen über Funktionswerte der Form $([[A]] * [[B]])(C)$ herzuleiten.

Aus 1.1.9 ist bekannt, dass $([[A]] * [[B]])(C)$ genau dann von 0 verschieden ist, wenn $C \in U_n A U_n B U_n$ gilt. Daher sollen nun Aussagen

über die Elementarteiler (beziehungsweise Determinantenteiler) der in $U_n A U_n B U_n$ auftretenden Matrizen getroffen werden.

2.6.1 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien $A, B \in \text{IL}_n(\mathfrak{o})$. Dann gilt $\mathfrak{d}_k(A)\mathfrak{d}_k(B) \mid \mathfrak{d}_k(AB)$ für alle $1 \leq k \leq n$. $\diamond$

BEWEIS:

Zunächst gilt für zwei beliebige Matrizen $A', B' \in \mathfrak{o}^{m \times m}$ stets die Beziehung $\mathfrak{d}_1(A')\mathfrak{d}_1(B') \mid \mathfrak{d}_1(A'B')$: Die Einträge von $A'B'$ sind Summen von Produkten der Form $a'b'$, wobei a' ein Eintrag von A' und b' ein Eintrag von B' ist. Allgemein gilt $\mathfrak{d}_1(A') \mid a'$ und $\mathfrak{d}_1(B') \mid b'$ (denn die ersten Determinantenteiler sind genau die größten gemeinsamen Teiler aller Einträge einer Matrix), so dass für das Produkt $\mathfrak{d}_1(A')\mathfrak{d}_1(B') \mid a'b'$ folgt. Die Summen solcher Produkte werden dann ebenfalls von $\mathfrak{d}_1(A')\mathfrak{d}_1(B')$ geteilt, also gilt $\mathfrak{d}_1(A')\mathfrak{d}_1(B') \mid c'$ für alle Einträge c' von $A'B'$, woraus $\mathfrak{d}_1(A')\mathfrak{d}_1(B') \mid \mathfrak{d}_1(A'B')$ folgt.

Für $1 \leq k \leq n$ erhält man durch Anwendung des gerade Bewiesenen

$$\begin{aligned} \mathfrak{d}_k(A)\mathfrak{d}_k(B) &\stackrel{2.2.4(a)}{=} \mathfrak{d}_1(A^{[k]})\mathfrak{d}_1(B^{[k]}) \mid \mathfrak{d}_1(A^{[k]}B^{[k]}) \\ &\stackrel{2.2.4(i)}{=} \mathfrak{d}_1((AB)^{[k]}) \stackrel{2.2.4(a)}{=} \mathfrak{d}_k(AB), \end{aligned}$$

was zu zeigen war. $\square$

Für die Anwendung auf die zu betrachtende Hecke-Algebra wird aus dem Satz eine etwas allgemeinere Aussage abgeleitet.

2.6.2 FOLGERUNG: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien Matrizen $A, B \in \text{IL}_n(\mathfrak{o})$ gegeben. Für jede Matrix $C \in \text{GL}_n(\mathfrak{o})A\text{GL}_n(\mathfrak{o})B\text{GL}_n(\mathfrak{o})$ und jedes $1 \leq k \leq n$ gilt dann $\mathfrak{d}_k(A)\mathfrak{d}_k(B) \mid \mathfrak{d}_k(C)$. $\diamond$

BEWEIS:

Ist $C \in \text{GL}_n(\mathfrak{o})A\text{GL}_n(\mathfrak{o})B\text{GL}_n(\mathfrak{o})$, so gibt es $P, Q, R \in \text{GL}_n(\mathfrak{o})$ mit

$C = PAQBR$. Dann gilt

$$\mathfrak{d}_k(A)\mathfrak{d}_k(B) \stackrel{2.2.5}{=} \mathfrak{d}_k(PA)\mathfrak{d}_k(QBR) \stackrel{2.6.1}{=} \mathfrak{d}_k(PAQBR) = \mathfrak{d}_k(C). \quad \square$$

Mit der gerade bewiesenen Folgerung lassen sich über die Determinantenteiler der beteiligten Matrizen Aussagen treffen, dass in der zu untersuchenden Hecke-Algebra bestimmte Funktionswerte der Form $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C)$ gleich 0 sind (nämlich solche, für die die angegebene Determinantenteilerrelation zwischen A , B und C nicht erfüllt ist). Es werden zusätzlich aber auch Aussagen benötigt, die garantieren, dass bestimmte Funktionswerte für über ihre Determinantenteiler spezifizierte Matrizen von Null verschieden sind. Ein Satz, der dieses leistet, wird nachfolgend vorgestellt. Zum Beweis werden Normalformen und ein Hilfslemma benötigt.

2.6.3 LEMMA: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien $A_1, \dots, A_n$ in $\mathfrak{o}^{2 \times 2}$ Matrizen vom Rang 1 mit $\mathfrak{d}_1(A_1) \mid \mathfrak{d}_1(A_2) \mid \dots \mid \mathfrak{d}_1(A_n)$. Setze $A = \text{diag}(A_1, \dots, A_n)$. Dann gilt $\mathfrak{e}_k(A) = \mathfrak{d}_1(A_k)$ für alle $1 \leq k \leq n$ und $\mathfrak{z}(A) = \mathfrak{z}(A_1) \cdots \mathfrak{z}(A_n)$. $\diamond$

BEWEIS:

Die Aussage $\mathfrak{z}(A) = \mathfrak{z}(A_1) \cdots \mathfrak{z}(A_n)$ folgt aus 2.2.4 (h). Zeige daher nur noch, dass $\mathfrak{e}_k(A) = \mathfrak{d}_1(A_k)$ für alle $1 \leq k \leq n$ gilt. Sei $k \in \mathbb{N}$ mit $k \leq n$ und A' eine $(k \times k)$ -Untermatrix von A mit von 0 verschiedener Determinante. Sei $Z = \{z_1, \dots, z_k\}$ mit $z_1 < \dots < z_k$ die zugehörige Zeilenauswahl und $S = \{s_1, \dots, s_k\}$ mit $s_1 < \dots < s_k$ die zugehörige Spaltenauswahl.

Da die Untermatrix eine von 0 verschiedene Determinante hat, muss $z_i > 2(i-1)$ für alle $1 \leq i \leq k$ gelten, denn jede Auswahl von mehr als $i-1$ Zeilen aus den ersten $2(i-1)$ Zeilen von A ist linear abhängig, da für alle $1 \leq j \leq k$ die Zeilen $2j-1$ und $2j$ nach Konstruktion von A stets Vielfache voneinander sind.

Ist a ein Eintrag aus der i -ten Zeile von $(A)_{ZS}$, dann ist a ein Eintrag der z_i -ten Zeile von A . Sei zunächst $a \neq 0$. Dann gehört a nach

Konstruktion von A zu A_j für $j = [\frac{z_i+1}{2}]$ (wobei $[x]$ für $x \in \mathbb{R}$ die Gauß-Klammer von x , also $\sup\{y \in \mathbb{Z} \mid y \leq x\}$, bezeichnet), liegt also in $\mathfrak{d}_1(A_j)$; wegen $z_i > 2(i-1)$ gilt $j \geq i$, also $\mathfrak{d}_1(A_i) \mid \mathfrak{d}_1(A_j)$ aufgrund der Teilbarkeitsbeziehung aus den Voraussetzungen, so dass aus $a \in \mathfrak{d}_1(A_j)$ auch $a \in \mathfrak{d}_1(A_i)$ folgt. Da $a \in \mathfrak{d}_1(A_i)$ auch für $a = 0$ gilt, liegen die Einträge der i -ten Zeile der Untermatrix $(A)_{ZS}$ alle in $\mathfrak{d}_1(A_i)$. Hat man nun ein Produkt aus k Faktoren, bei dem jeweils der i -te Faktor aus der i -ten Zeile von $(A)_{ZS}$ stammt, liegt dieses Produkt folglich in $\mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$. Da sich die Determinante von $(A)_{ZS}$ als Summe und Differenz solcher Produkte schreiben lässt, liegt auch sie in $\mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$.

Der k -te Determinantenteiler von A als größter gemeinsamer Teiler aller $(k \times k)$ -Unterdeterminanten wird von $\mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$ geteilt, da dies nach dem gerade Bewiesenen bereits für alle betrachteten Unterdeterminanten gilt. Es verbleibt, die umgekehrte Teilbarkeitsbeziehung $\mathfrak{d}_k(A) \mid \mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$ zu zeigen, denn dann gilt $\mathfrak{d}_k(A) = \mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$ für alle $1 \leq k \leq n$ und folglich $\mathfrak{e}_k(A) = \mathfrak{d}_k(A) \mathfrak{d}_{k-1}(A)^{-1} = \mathfrak{d}_1(A_k)$ für alle $1 \leq k \leq n$. Unter den $(k \times k)$ -Untermatrizen von A treten speziell alle Matrizen der Form $\text{diag}(a_1, \dots, a_k)$ auf, bei denen jeweils a_i ein Eintrag von A_i ist, also liegen alle Produkte der Form $a_1 \cdots a_k$ in $\mathfrak{d}_k(A)$. Das von diesen Produkten erzeugte Teilideal von $\mathfrak{d}_k(A)$ ist genau gleich $\mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$, denn die Einträge einer A_i bilden jeweils ein Erzeugendensystem von $\mathfrak{d}_1(A_i)$. Es folgt $\mathfrak{d}_k(A) \mid \mathfrak{d}_1(A_1) \cdots \mathfrak{d}_1(A_k)$, was den Beweis abschließt. $\square$

Mit diesem Hilfslemma kann nun der Beweis des folgenden Satzes über die »Realisierbarkeit« bestimmter Determinantenteiler in der Menge $\text{GL}_n(\mathfrak{o}) A \text{GL}_n(\mathfrak{o}) B \text{GL}_n(\mathfrak{o})$ angegangen werden.

2.6.4 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien A und B Matrizen aus $\text{IL}_n(\mathfrak{o})$. Dann gibt es eine Matrix $C \in \text{GL}_n(\mathfrak{o}) A \text{GL}_n(\mathfrak{o}) B \text{GL}_n(\mathfrak{o})$ mit $\mathfrak{d}_k(C) = \mathfrak{d}_k(A) \mathfrak{d}_k(B)$ für alle $k \in \mathbb{N}$ mit $k \leq n$. $\diamond$

2 Hecke-Algebren zu unimodularen Gruppen

BEWEIS:

Setze $U_n = \text{GL}_n(\mathfrak{o})$ und $U_{2n} = \text{GL}_{2n}(\mathfrak{o})$ sowie

$$E' = \begin{pmatrix} E_n \\ 0 \end{pmatrix} \in \mathfrak{o}^{2n \times n}, \quad \tilde{E} = \begin{pmatrix} E_n & 0 \end{pmatrix} \in \mathfrak{o}^{n \times 2n}.$$

Seien

$$A' = E' A \tilde{E} = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n} \quad \text{und} \quad B' = E' B \tilde{E} = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n}$$

sowie $A^* = \text{diag}(A_1, \dots, A_n)$ und $B^* = \text{diag}(B_1, \dots, B_n)$ Normalformen von A' und B' aus 2.2.11. Setze

$$C^* = A^* (B^*)^T = \text{diag}(A_1 B_1^T, \dots, A_n B_n^T)$$

und wähle gemäß 2.2.10 eine Matrix $C \in \mathfrak{o}^{n \times n}$ mit $f_k(C) = f_k(A) f_k(B)$ für alle $1 \leq k \leq n$. Dies ist möglich, da

$$\begin{aligned} f_1(C)^n f_2(C)^{n-1} \cdots f_n(C) &= (f_1(A) f_1(B))^n \cdots (f_n(A) f_n(B)) \\ &= (f_1(A)^n \cdots f_n(A)) (f_1(B)^n \cdots f_n(B)) \\ &= \mathfrak{d}_n(A) \mathfrak{d}_n(B) \end{aligned}$$

als Produkt zweier Hauptideale wieder ein Hauptideal ist. Mit dieser Wahl gilt auch $\mathfrak{e}_k(C) = \mathfrak{e}_k(A) \mathfrak{e}_k(B)$ und $\mathfrak{d}_k(C) = \mathfrak{d}_k(A) \mathfrak{d}_k(B)$ für alle $1 \leq k \leq n$. Setze

$$C' = E' C \tilde{E} = \begin{pmatrix} C & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n}.$$

Zeige nun, dass $C' \in U_{2n} C^* U_{2n}$ gilt. Betrachte zunächst $A_k B_k^T$ für $1 \leq k \leq n$. Sei $A_k = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ und $B_k = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$. Dann hat

$$A_k B_k^T = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$$

Rang 1, den ersten Determinantenteiler

$$\begin{aligned} aco + ado + bco + bdo &= (ao + bo)(co + do) = \mathfrak{d}_1(A_k) \mathfrak{d}_1(B_k) \\ &= \mathfrak{e}_k(A) \mathfrak{e}_k(B) \end{aligned}$$

und die Zeilenklasse $(aco + ado)\mathfrak{H}(K) = a\mathfrak{d}_1(B_k)\mathfrak{H}(K) = \mathfrak{d}_1(B_k)\mathfrak{H}(K)$. Weiter folgt dann

$$\mathfrak{d}_1(A_{k-1}B_{k-1}^T) = \mathfrak{e}_{k-1}(A)\mathfrak{e}_{k-1}(B) \stackrel{2.2.4(f)}{=} \mathfrak{e}_k(A)\mathfrak{e}_k(B) = \mathfrak{d}_1(A_kB_k^T)$$

für alle $1 \leq k \leq n$. Damit sind die Voraussetzungen von 2.6.3 erfüllt; man erhält $\mathfrak{e}_k(C^*) = \mathfrak{d}_1(A_kB_k^T)$ wegen $C^* = \text{diag}(A_1B_1^T, \dots, A_nB_n^T)$, also $\mathfrak{e}_k(C^*) = \mathfrak{e}_k(A)\mathfrak{e}_k(B) = \mathfrak{e}_k(C)$ und damit $\mathfrak{d}_k(C^*) = \mathfrak{d}_k(C)$ für alle $1 \leq k \leq n$ (für $j > n$ ist $\mathfrak{d}_j(C^*) = \{0\} = \mathfrak{d}_j(C')$). Für den Beweis von $C' \in U_{2n}C^*U_{2n}$ verbleibt gemäß 2.2.5 daher nur noch $\mathfrak{Z}(C^*) = \mathfrak{Z}(C')$ zu zeigen. Zunächst ist $\mathfrak{Z}(C') = \mathfrak{Z}(C) = \mathfrak{H}(K)$ nach 2.2.4 (e). Weiter ist $\mathfrak{Z}(C^*) = \mathfrak{Z}(A^*(B^*)^T) = \mathfrak{Z}(A_1B_1^T) \cdots \mathfrak{Z}(A_nB_n^T)$ nach 2.6.3 aufgrund der Struktur von $A^*(B^*)^T$. Da bereits gezeigt wurde, dass

$$\mathfrak{Z}(A_kB_k^T) = \mathfrak{d}_1(B_k)\mathfrak{H}(K) = \mathfrak{e}_k(B)\mathfrak{H}(K)$$

gilt, erhält man

$$\begin{aligned} \mathfrak{Z}(A_1B_1^T) \cdots \mathfrak{Z}(A_nB_n^T) &= \mathfrak{e}_1(B) \cdots \mathfrak{e}_n(B)\mathfrak{H}(K) = \mathfrak{d}_n(B)\mathfrak{H}(K) \\ &= \mathfrak{H}(K) = \mathfrak{Z}(C'). \end{aligned}$$

Dies schließt den Beweis von $C' \in U_{2n}C^*U_{2n}$ ab.

Aus der gerade bewiesenen Tatsache $C' \in U_{2n}C^*U_{2n}$ folgt, dass es $P, Q \in U_{2n}$ mit $C' = PC^*Q = PA^*(B^*)^TQ$ gibt. Mit 2.2.11 erhält man, dass es Matrizen $P_1, Q_1, P_2, Q_2 \in U_{2n}$ gibt mit $A^* = P_1A'Q_1$ sowie $B^* = P_2B'Q_2$. Darüberhinaus gilt $C = \tilde{E}C'E'$ sowie $A' = E'A\tilde{E}$ und $B' = E'B\tilde{E}$. Insgesamt erhält man so

$$\begin{aligned} C &= \tilde{E}C'E' = \tilde{E}PA^*(B^*)^TQE' = \tilde{E}PP_1A'Q_1(P_2B'Q_2)^TQE' \\ &= \tilde{E}PP_1E'A\tilde{E}Q_1(P_2E'B\tilde{E}Q_2)^TQE' \\ &= \tilde{E}PP_1E'A\tilde{E}Q_1Q_2^T\tilde{E}^TB^T(E')^TP_2^TQE'. \end{aligned}$$

Setzt man $R_1 = \tilde{E}PP_1E' \in \mathfrak{o}^{n \times n}$ und $R_2 = \tilde{E}Q_1Q_2^T\tilde{E}^T \in \mathfrak{o}^{n \times n}$ sowie $R_3 = (E')^TP_2^TQE' \in \mathfrak{o}^{n \times n}$, so hat man $C = R_1AR_2B^TR_3$. Insbesondere

gilt

$$\det C = (\det R_1)(\det A)(\det R_2)(\det B)(\det R_3),$$

und da sich $(\det A)(\det B)$ und $\det C$ wegen $\mathfrak{d}_n(A)\mathfrak{d}_n(B) = \mathfrak{d}_n(C)$ nur um einen Faktor aus der Einheitengruppe $\mathfrak{o}^*$ unterscheiden können, folgt $(\det R_1)(\det R_2)(\det R_3) \in \mathfrak{o}^*$, also $\det R_1, \det R_2, \det R_3 \in \mathfrak{o}^*$, und damit insgesamt $R_1, R_2, R_3 \in U_n$. Daraus erhält man nun, dass

$$C \in U_n A U_n B^T U_n \stackrel{2.2.6}{=} C \in U_n A U_n B U_n$$

gilt, und da C nach Konstruktion darüberhinaus die geforderten Bedingungen an die Determinantenteiler erfüllt, ist damit die Aussage bewiesen. $\square$

Eine leichte Modifikation des Beweises liefert eine Verallgemeinerung:

2.6.5 BEMERKUNG: Durch Einfügen geeigneter Permutationsmatrizen im Beweis von 2.6.4 erhält man folgende stärkere Aussage: Ist $\mathfrak{o}$ ein Dedekind-Ring, $n \in \mathbb{N}$, und sind A und B Matrizen aus $\text{IL}_n(\mathfrak{o})$, so gibt es für jede Permutation π auf $\{1, \dots, n\}$ eine Matrix $C \in \text{GL}_n(\mathfrak{o}) A \text{GL}_n(\mathfrak{o}) B \text{GL}_n(\mathfrak{o})$, deren Elementarteiler $\mathfrak{e}_1(A)\mathfrak{e}_{\pi(1)}(B), \dots, \mathfrak{e}_n(A)\mathfrak{e}_{\pi(n)}(B)$ sind (bis auf Sortierung). $\diamond$

Zu gegebenen $A, B \in \text{IL}_n(\mathfrak{o})$ liefern die bislang bewiesenen Aussagen $M, N \subseteq \text{IL}_n(\mathfrak{o})$ mit $M \subseteq \text{Tr}(\llbracket A \rrbracket * \llbracket B \rrbracket) \subseteq N$. Ist $\mathfrak{o}$ ein Hauptidealring, lässt sich zumindest im Fall $n = 2$ eine Verschärfung zu $M = N$, also eine genaue Charakterisierung des Trägers, erreichen.

2.6.6 SATZ: Sei $\mathfrak{o}$ ein Hauptidealring. Weiter seien A, B und C Matrizen aus $\text{IL}_2(\mathfrak{o})$. Dann sind äquivalent:

- (i) Es gilt $C \in \text{GL}_2(\mathfrak{o}) A \text{GL}_2(\mathfrak{o}) B \text{GL}_2(\mathfrak{o})$.
- (ii) Es gilt $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C) \mid (\mathfrak{d}_1(A)\mathfrak{d}_1(B))(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))$ und $\mathfrak{d}_2(C) = \mathfrak{d}_2(A)\mathfrak{d}_2(B)$. $\diamond$

BEWEIS:

Wähle $a, b, c, d \in \mathfrak{o}$ mit $a\mathfrak{o} = \mathfrak{d}_1(A)$ und $b\mathfrak{o} = \mathfrak{d}_1(B)$ sowie $c\mathfrak{o} = \mathfrak{f}_2(A)$ und $d\mathfrak{o} = \mathfrak{f}_2(B)$ (möglich wegen 2.2.4 (g) und der Tatsache, dass $\mathfrak{o}$ ein Hauptidealring ist). Setze $A' = \text{diag}(a, ac)$ und $B' = \text{diag}(b, bd)$. Dann gilt $\mathfrak{d}_1(A') = a\mathfrak{o} = \mathfrak{d}_1(A)$ sowie $\mathfrak{d}_2(A') = a^2c\mathfrak{o} = \mathfrak{d}_1(A)^2\mathfrak{f}_2(A) = \mathfrak{d}_2(A)$ und genauso $\mathfrak{d}_k(B') = \mathfrak{d}_k(B)$ für alle $k \in \{1, 2\}$. Wähle nun gemäß 2.2.5 Matrizen $P, Q_1, Q_2, R \in \text{GL}_2(\mathfrak{o})$ mit $A = PA'Q_1$ und $B = Q_2B'R$.

(i) $\Rightarrow$ (ii): Es gebe $P', Q', R' \in \text{GL}_2(\mathfrak{o})$ mit $C = P'AQ'BR'$. Dann gilt $\det C = (\det P')(\det A)(\det Q')(\det B)(\det R') \in (\det A)(\det B)\mathfrak{o}^*$, also $\mathfrak{d}_2(C) = \mathfrak{d}_2(A)\mathfrak{d}_2(B)$. Weiter gilt $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C)$ nach 2.6.2. Somit verbleibt nur noch $\mathfrak{d}_1(C) \mid (\mathfrak{d}_1(A)\mathfrak{d}_1(B))(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))$ zu zeigen. Mit den oben eingeführten allgemeinen Bezeichnungen ist $C = P'PA'Q_1Q'Q_2B'RR'$ und damit $\mathfrak{d}_1(C) = \mathfrak{d}_1(A'Q_1Q'Q_2B')$ nach 2.2.5 wegen $P'P \in \text{GL}_2(\mathfrak{o})$ und $RR' \in \text{GL}_2(\mathfrak{o})$. Setze zur Abkürzung

$$Q_1Q'Q_2 = Q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}.$$

Dann gilt

$$A'QB' = \begin{pmatrix} a & 0 \\ 0 & ac \end{pmatrix} \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} aq_1b & aq_2bd \\ acq_3b & acq_4bd \end{pmatrix},$$

also $\mathfrak{d}_1(C) = \mathfrak{d}_1(A'QB') = ab(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o})$. Sei nun $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Gilt $\mathfrak{p} \nmid q_1$, so ist $v_{\mathfrak{p}}(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o}) = 0$, also

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}_1(C)) &= v_{\mathfrak{p}}(ab(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o})) \\ &= v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(\mathfrak{d}_1(A)\mathfrak{d}_1(B)) \\ &\leq v_{\mathfrak{p}}(\mathfrak{d}_1(A)\mathfrak{d}_1(B)(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))). \end{aligned}$$

Gilt hingegen $\mathfrak{p} \mid q_1$, so folgt $\mathfrak{p} \nmid q_2$ und $\mathfrak{p} \nmid q_3$, da man andernfalls mit $\mathfrak{p} \mid q_1q_4 - q_2q_3 = \det Q$ einen Widerspruch zu $Q \in \text{GL}_2(\mathfrak{o})$ erhalten

würde. Somit gilt dann

$$\begin{aligned}
 v_p(\mathfrak{d}_1(C)) &= v_p(ab(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o})) \\
 &= v_p(ab) + \min\{v_p(q_1), v_p(d), v_p(c), v_p(cq_4d)\} \\
 &\leq v_p(ab) + \min\{v_p(d), v_p(c)\} = v_p(ab) + v_p(d\mathfrak{o} + c\mathfrak{o}) \\
 &= v_p(ab(d\mathfrak{o} + c\mathfrak{o})),
 \end{aligned}$$

und da nach Wahl von a, b, c und d nun $a\mathfrak{o} = \mathfrak{d}_1(A)$ sowie $b\mathfrak{o} = \mathfrak{d}_1(B)$ und $c\mathfrak{o} = \mathfrak{f}_2(A)$ sowie $d\mathfrak{o} = \mathfrak{f}_2(B)$ gilt, hat man auch in diesem Fall

$$v_p(\mathfrak{d}_1(C)) \leq v_p(\mathfrak{d}_1(A)\mathfrak{d}_1(B)(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))),$$

so dass insgesamt $\mathfrak{d}_1(C) \mid \mathfrak{d}_1(A)\mathfrak{d}_1(B)(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))$ folgt.

(ii) $\Rightarrow$ (i): Sei C eine Matrix aus $IL_2(\mathfrak{o})$, die die Aussage in (ii) erfüllt. Definiere $\mathfrak{a} = \mathfrak{d}_1(C)\mathfrak{d}_1(A)^{-1}\mathfrak{d}_1(B)^{-1}$. Da dann nach Voraussetzung $\mathfrak{a} \mid \mathfrak{f}_2(A) + \mathfrak{f}_2(B) = c\mathfrak{o} + d\mathfrak{o}$ und somit erst recht $c \in \mathfrak{a}$ gilt, gibt es nach 1.2.8 ein $q_1 \in \mathfrak{a}$ mit $q_1\mathfrak{o} + c\mathfrak{o} = \mathfrak{a}$. Weiter gilt aufgrund der Voraussetzungen $\mathfrak{a} \subseteq \mathfrak{o}$ und somit $q_1 \in \mathfrak{o}$. Daher gibt es nach 1.2.8 ein $q_2 \in \mathfrak{o}$ mit $q_1\mathfrak{o} + q_2\mathfrak{o} = \mathfrak{o}$. Demzufolge existieren dann $q_3, q_4 \in \mathfrak{o}$ mit $q_1q_4 - q_2q_3 = 1$. Setzt man also $Q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$, so gilt $\det Q = 1$ und folglich $Q \in GL_2(\mathfrak{o})$. Definiert man weiter $C' = A'QB'$, so ist dann $\det C' = (\det A')(\det Q)(\det B') = (\det A')(\det B')$ und somit

$$\begin{aligned}
 \mathfrak{d}_2(C') &= \mathfrak{d}_2(A')\mathfrak{d}_2(B') \stackrel{2.2.5}{=} \mathfrak{d}_2(PA'Q_1)\mathfrak{d}_2(Q_2B'R) \\
 &= \mathfrak{d}_2(A)\mathfrak{d}_2(B) = \mathfrak{d}_2(C)
 \end{aligned}$$

erfüllt. Weiter gilt

$$C' = A'QB' = \begin{pmatrix} a & 0 \\ 0 & ac \end{pmatrix} \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} aq_1b & aq_2bd \\ acq_3b & acq_4bd \end{pmatrix},$$

also $\mathfrak{d}_1(C') = ab(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o})$. Sei nun $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Gilt $\mathfrak{p} \nmid q_1$, so ist $v_p(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o}) = 0$ und somit

$v_p(\mathfrak{d}_1(C')) = v_p(ab)$, und wegen $q_1 \in \mathfrak{a}$ folgt aus $p \nmid q_1$ erst recht $p \nmid \mathfrak{a}$ und damit

$$\begin{aligned} v_p(\mathfrak{d}_1(C)) &= v_p(\mathfrak{d}_1(A)\mathfrak{d}_1(B)\mathfrak{a}) = v_p(\mathfrak{d}_1(A)\mathfrak{d}_1(B)) \\ &= v_p(ab) = v_p(\mathfrak{d}_1(C')). \end{aligned}$$

Gilt hingegen $p \mid q_1$, so folgt $p \nmid q_2$ und $p \nmid q_3$ wie im ersten Teil des Beweises, woraus man

$$\begin{aligned} v_p(\mathfrak{d}_1(C')) &= v_p(ab(q_1\mathfrak{o} + q_2d\mathfrak{o} + cq_3\mathfrak{o} + cq_4d\mathfrak{o})) \\ &= v_p(ab) + \min\{v_p(q_1), v_p(d), v_p(c), v_p(cq_4d)\} \\ &= v_p(ab) + \min\{v_p(q_1), v_p(d), v_p(c)\} \\ &= v_p(ab) + v_p(q_1\mathfrak{o} + d\mathfrak{o} + c\mathfrak{o}) \end{aligned}$$

erhält. Nach Wahl von q_1 gilt nun $q_1\mathfrak{o} + c\mathfrak{o} = \mathfrak{a}$, und da wie oben gesehen $\mathfrak{a} \mid c\mathfrak{o} + d\mathfrak{o}$ gilt, hat man dann auch $q_1\mathfrak{o} + c\mathfrak{o} + d\mathfrak{o} = \mathfrak{a}$. Somit erhält man

$$\begin{aligned} v_p(\mathfrak{d}_1(C')) &= v_p(ab) + v_p(q_1\mathfrak{o} + d\mathfrak{o} + c\mathfrak{o}) = v_p(ab) + v_p(\mathfrak{a}) \\ &= v_p(\mathfrak{d}_1(A)\mathfrak{d}_1(B)\mathfrak{a}) = v_p(\mathfrak{d}_1(C)). \end{aligned}$$

Da also $v_p(\mathfrak{d}_1(C')) = v_p(\mathfrak{d}_1(C))$ für alle Primideale p von $\mathfrak{o}$ gilt, hat man $\mathfrak{d}_1(C') = \mathfrak{d}_1(C)$. Zusammen mit der bereits gezeigten Aussage $\mathfrak{d}_2(C') = \mathfrak{d}_2(C)$ und 2.2.5 folgt, dass $P', R' \in \mathrm{GL}_2(\mathfrak{o})$ mit $C = P'C'R'$ existieren. Somit folgt

$$C = P'C'R' = P'A'QB'R' = P'P^{-1}AQ_1^{-1}QQ_2^{-1}BR^{-1}R',$$

und da $P'P^{-1}$ und $Q_1^{-1}QQ_2^{-1}$ sowie $R^{-1}R'$ als Produkte von Matrizen aus $\mathrm{GL}_2(\mathfrak{o})$ selbst wieder in $\mathrm{GL}_2(\mathfrak{o})$ liegen, folgt insgesamt $C \in \mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o})$. $\square$

Die Aussage (i) $\Rightarrow$ (ii) aus 2.6.6 lässt sich durch Lokalisierung auf beliebige Dedekind-Ringe verallgemeinern.

2.6.7 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring. Weiter seien A und B Matrizen aus $\text{IL}_2(\mathfrak{o})$. Für jedes $C \in \text{GL}_2(\mathfrak{o}) A \text{GL}_2(\mathfrak{o}) B \text{GL}_2(\mathfrak{o})$ gilt dann $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C) \mid (\mathfrak{d}_1(A)\mathfrak{d}_1(B))(\mathfrak{f}_2(A) + \mathfrak{f}_2(B))$ sowie $\mathfrak{d}_2(C) = \mathfrak{d}_2(A)\mathfrak{d}_2(B)$. $\diamond$

BEWEIS:

Es gelte $C \in \text{GL}_2(\mathfrak{o}) A \text{GL}_2(\mathfrak{o}) B \text{GL}_2(\mathfrak{o})$. Sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Für Matrizen $D \in \mathfrak{o}^{n \times n}$ und $k \in \{1, 2\}$ verwende die Bezeichnung

$$\mathfrak{d}_{\mathfrak{p},k}(D) = \sum_{i=1}^{\binom{2}{k}} \sum_{j=1}^{\binom{2}{k}} (D^{[k]})_{ij} \mathfrak{o}_{\mathfrak{p}}.$$

Dann ist $\mathfrak{d}_{\mathfrak{p},k}(D)$ der k -te Determinantenteiler von D , wenn man diese Matrix als Element von $\mathfrak{o}_{\mathfrak{p}}^{2 \times 2}$ auffasst. Da $\mathfrak{o}_{\mathfrak{p}}$ nach 1.2.11 (a) ein Hauptidealring ist, erhält man aus 2.6.6, dass

$$\mathfrak{d}_{\mathfrak{p},1}(C) \mid \mathfrak{d}_{\mathfrak{p},1}(A)\mathfrak{d}_{\mathfrak{p},1}(B)(\mathfrak{d}_{\mathfrak{p},1}(A)^{-2}\mathfrak{d}_{\mathfrak{p},2}(A) + \mathfrak{d}_{\mathfrak{p},1}(B)^{-2}\mathfrak{d}_{\mathfrak{p},2}(B))$$

und somit

$$\mathfrak{d}_{\mathfrak{p},1}(A)\mathfrak{d}_{\mathfrak{p},1}(B)\mathfrak{d}_{\mathfrak{p},1}(C) \mid \mathfrak{d}_{\mathfrak{p},1}(B)^2\mathfrak{d}_{\mathfrak{p},2}(A) + \mathfrak{d}_{\mathfrak{p},1}(A)^2\mathfrak{d}_{\mathfrak{p},2}(B)$$

gilt. Zur Abkürzung definiere $\mathfrak{c}_1 = \mathfrak{d}_{\mathfrak{p},1}(C)$ und $\mathfrak{a}_k = \mathfrak{d}_{\mathfrak{p},k}(A)$ sowie $\mathfrak{b}_k = \mathfrak{d}_{\mathfrak{p},k}(B)$ für jedes $k \in \{1, 2\}$. Nun gilt

$$\begin{aligned} \mathfrak{v}_{\mathfrak{p}}(\mathfrak{a}_1 \cap \mathfrak{o}) &= \mathfrak{v}_{\mathfrak{p}}(((A)_{11}\mathfrak{o}_{\mathfrak{p}} + (A)_{12}\mathfrak{o}_{\mathfrak{p}} + (A)_{21}\mathfrak{o}_{\mathfrak{p}} + (A)_{22}\mathfrak{o}_{\mathfrak{p}}) \cap \mathfrak{o}) \\ &\stackrel{1.2.11(i)}{=} \min_{i,j \in \{1,2\}} \mathfrak{v}_{\mathfrak{p}}((A)_{ij}) \geq 0, \end{aligned}$$

da die Einträge von A alle in $\mathfrak{o}$ liegen. Genauso erhält man weiter $\mathfrak{v}_{\mathfrak{p}}(\mathfrak{b}_1 \cap \mathfrak{o}) \geq 0$ und $\mathfrak{v}_{\mathfrak{p}}(\mathfrak{c}_1 \cap \mathfrak{o}) \geq 0$. Dass auch $\mathfrak{v}_{\mathfrak{p}}(\mathfrak{a}_2 \cap \mathfrak{o}) \geq 0$ und $\mathfrak{v}_{\mathfrak{p}}(\mathfrak{b}_2 \cap \mathfrak{o}) \geq 0$ gilt, erhält man aus der Tatsache, dass die Determinanten von A und B in $\mathfrak{o}$ liegen. Daher erhält man mit den Rechenregeln

aus 1.2.11

$$\begin{aligned}
 v_p(a_1 b_1 c_1 \cap o) &= v_p(a_1 \cap o) + v_p(b_1 \cap o) + v_p(c_1 \cap o) \\
 &= \min_{i,j \in \{1,2\}} v_p((A)_{ij}) + \min_{i,j \in \{1,2\}} v_p((B)_{ij}) \\
 &\quad + \min_{i,j \in \{1,2\}} v_p((C)_{ij}) \\
 &= v_p(d_1(A)) + v_p(d_1(B)) + v_p(d_1(C)) \\
 &= v_p(d_1(A) d_1(B) d_1(C))
 \end{aligned}$$

und genauso

$$\begin{aligned}
 v_p((b_1^2 a_2 + a_1^2 b_2) \cap o) \\
 &= \min\{v_p((b_1^2 a_2) \cap o), v_p((a_1^2 b_2) \cap o)\} \\
 &= \min\{2v_p(b_1 \cap o) + v_p(a_2 \cap o), 2v_p(a_1 \cap o) + v_p(b_2 \cap o)\} \\
 &= \min\{2v_p(d_1(B)) + v_p(d_2(A)), 2v_p(d_1(A)) + v_p(d_2(B))\} \\
 &= \min\{v_p(d_1(B)^2 d_2(A)), v_p(d_1(A)^2 d_2(B))\} \\
 &= v_p(d_1(B)^2 d_2(A) + d_1(A)^2 d_2(B)).
 \end{aligned}$$

Nun gilt wie oben gesehen $a_1 b_1 c_1 \mid b_1^2 a_2 + a_2^2 b_2$ und folglich nach 1.2.11 (g)

$$v_p((a_1 b_1 c_1) \cap o) \leq v_p((b_1^2 a_2 + a_2^2 b_2) \cap o),$$

so man zusammen mit den durchgeführten Umformungen

$$v_p(d_1(A) d_1(B) d_1(C)) \leq v_p(d_1(B)^2 d_2(A) + d_1(A)^2 d_2(B))$$

erhält. Da p ein beliebiges Primideal von o war, folgt insgesamt

$$d_1(A) d_1(B) d_1(C) \mid d_1(B)^2 d_2(A) + d_1(A)^2 d_2(B)$$

und somit

$$\begin{aligned}
 d_1(C) &\mid d_1(A)^{-1} d_1(B) d_2(A) + d_1(A) d_1(B)^{-1} d_2(B) \\
 &= d_1(A) d_1(B) (d_1(A)^{-2} d_2(A) + d_1(B)^{-2} d_2(B)) \\
 &= d_1(A) d_1(B) (f_2(A) + f_2(B)),
 \end{aligned}$$

was eine der zu beweisenden Behauptungen war. Die noch fehlenden Behauptungen $\mathfrak{d}_1(A)\mathfrak{d}_1(B) \mid \mathfrak{d}_1(C)$ und $\mathfrak{d}_2(C) = \mathfrak{d}_2(A)\mathfrak{d}_2(B)$ erhält man aus 2.6.1 und der Multiplikativität der Determinante. $\square$

Sind A und B zwei Matrizen aus $\mathrm{IL}_2(\mathfrak{o})$ mit $\mathfrak{d}_2(A) + \mathfrak{d}_2(B) = \mathfrak{o}$, so gilt erst recht $\mathfrak{f}_2(A) + \mathfrak{f}_2(B) = \mathfrak{o}$, da $\mathfrak{f}_2(A)$ ein Teiler von $\mathfrak{d}_2(A)$ und $\mathfrak{f}_2(B)$ ein Teiler von $\mathfrak{d}_2(B)$ ist. In diesem Fall schließt man mit 2.6.7, dass $\mathfrak{d}_1(C) = \mathfrak{d}_1(A)\mathfrak{d}_1(B)$ und $\mathfrak{d}_2(C) = \mathfrak{d}_2(A)\mathfrak{d}_2(B)$ für alle $C \in \mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o})$ gelten muss. Mit 2.2.5 folgt dann, dass $\mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o})$ aus genau einer Doppelnebenklasse besteht, und da $AB \in \mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o})$ gilt, folgt

$$\mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o}) = \mathrm{GL}_2(\mathfrak{o})AB\mathrm{GL}_2(\mathfrak{o}).$$

Diese Aussage lässt sich nicht nur für $n = 2$, sondern für beliebiges $n \in \mathbb{N}$ beweisen. Dazu wird als Vorbereitung der folgende Satz benötigt.

2.6.8 SATZ: Sei $\mathfrak{o}$ ein Dedekind-Ring und $n \in \mathbb{N}$. Weiter seien $A, B \in \mathrm{IL}_n(\mathfrak{o})$ mit $\mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{o}$. Dann gilt $\mathfrak{d}_k(AB) = \mathfrak{d}_k(A)\mathfrak{d}_k(B)$ für alle $1 \leq k \leq n$. $\diamond$

BEWEIS:

Sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$. Für Matrizen $D \in \mathfrak{o}^{n \times n}$ verwende die Bezeichnung $\mathfrak{d}_{\mathfrak{p},k}(D)$ wie im Beweis von 2.6.7, und definiere analog $\mathfrak{e}_{\mathfrak{p},k}(D) = \mathfrak{d}_{\mathfrak{p},k}(D)\mathfrak{d}_{\mathfrak{p},k-1}(D)^{-1}$.

Da $\mathfrak{o}_{\mathfrak{p}}$ nach 1.2.11 (a) ein Hauptidealring ist, gibt es nach [New72] Satz II.9 (S. 26) $a'_1, \dots, a'_n \in \mathfrak{o}_{\mathfrak{p}}$ und $b'_1, \dots, b'_n \in \mathfrak{o}_{\mathfrak{p}}$, so dass $a'_1 \mid \dots \mid a'_n$ sowie $b'_1 \mid \dots \mid b'_n$ und $A' := \mathrm{diag}(a'_1, \dots, a'_n) \in \mathrm{GL}_n(\mathfrak{o}_{\mathfrak{p}})A\mathrm{GL}_n(\mathfrak{o}_{\mathfrak{p}})$ sowie $B' := \mathrm{diag}(b'_1, \dots, b'_n) \in \mathrm{GL}_n(\mathfrak{o}_{\mathfrak{p}})B\mathrm{GL}_n(\mathfrak{o}_{\mathfrak{p}})$ gilt. Die Bemerkung nach [New72] Satz II.9 (S. 26 f.) besagt nun, dass $\mathfrak{e}_{\mathfrak{p},k}(A') = a'_k\mathfrak{o}_{\mathfrak{p}}$ und $\mathfrak{e}_{\mathfrak{p},k}(B') = b'_k\mathfrak{o}_{\mathfrak{p}}$ für alle $1 \leq k \leq n$ gilt, und für das Produkt $A'B' = \mathrm{diag}(a'_1b'_1, \dots, a'_nb'_n)$ folgt $\mathfrak{e}_{\mathfrak{p},k}(A'B') = a'_kb'_k\mathfrak{o}_{\mathfrak{p}}$ für alle $k \in \mathbb{N}$ mit $k \leq n$. Somit erhält man

$$\mathfrak{e}_{\mathfrak{p},k}(AB) = a'_kb'_k\mathfrak{o}_{\mathfrak{p}} = \mathfrak{e}_{\mathfrak{p},k}(A)\mathfrak{e}_{\mathfrak{p},k}(B)$$

für alle $1 \leq k \leq n$ und damit auch $\mathfrak{d}_{\mathfrak{p},k}(AB) = \mathfrak{d}_{\mathfrak{p},k}(A)\mathfrak{d}_{\mathfrak{p},k}(B)$ für alle $1 \leq k \leq n$. Für jedes $1 \leq k \leq n$ hat man nun wie im Beweis von 2.6.7

$$\begin{aligned} \mathfrak{v}_{\mathfrak{p}}(\mathfrak{d}_k(A)\mathfrak{d}_k(B)) &= \mathfrak{v}_{\mathfrak{p}}((\mathfrak{d}_{\mathfrak{p},k}(A)\mathfrak{d}_{\mathfrak{p},k}(B)) \cap \mathfrak{o}) = \mathfrak{v}_{\mathfrak{p}}((\mathfrak{d}_{\mathfrak{p},k}(AB)) \cap \mathfrak{o}) \\ &= \mathfrak{v}_{\mathfrak{p}}(\mathfrak{d}_k(AB)), \end{aligned}$$

und da diese Gleichung für jedes beliebige Primideale $\mathfrak{p}$ von $\mathfrak{o}$ gilt, folgt $\mathfrak{d}_k(A)\mathfrak{d}_k(B) = \mathfrak{d}_k(AB)$, was zu beweisen war. $\square$

Mit diesem Satz kann die für den Fall $\mathfrak{d}_2(A) + \mathfrak{d}_2(B) = \mathfrak{o}$ bereits hergeleitete Gleichung $\mathrm{GL}_2(\mathfrak{o})A\mathrm{GL}_2(\mathfrak{o})B\mathrm{GL}_2(\mathfrak{o}) = \mathrm{GL}_2(\mathfrak{o})AB\mathrm{GL}_2(\mathfrak{o})$ auf $(n \times n)$ -Matrizen verallgemeinert werden.

2.6.9 FOLGERUNG: Sei $\mathfrak{o}$ ein Dedekind-Ring. Weiter seien $A, B \in \mathrm{IL}_n(\mathfrak{o})$ mit $\mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{o}$. Dann gilt

$$\mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})B\mathrm{GL}_n(\mathfrak{o}) = \mathrm{GL}_n(\mathfrak{o})AB\mathrm{GL}_n(\mathfrak{o}). \quad \diamond$$

BEWEIS:

Sei $C \in \mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})B\mathrm{GL}_n(\mathfrak{o})$. Dann gibt es $P, Q, R \in \mathrm{GL}_n(\mathfrak{o})$ mit $C = PAQBR$. Da nach 2.2.5 $\mathfrak{d}_n(PAQ) + \mathfrak{d}_n(BR) = \mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{o}$ gilt, erhält man für jedes $1 \leq k \leq n$, dass

$$\mathfrak{d}_k(C) = \mathfrak{d}_k(PAQBR) \stackrel{2.6.8}{=} \mathfrak{d}_k(PAQ)\mathfrak{d}_k(BR) \stackrel{2.2.5}{=} \mathfrak{d}_k(A)\mathfrak{d}_k(B)$$

gilt. Da C aus $\mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})B\mathrm{GL}_n(\mathfrak{o})$ beliebig gewählt war, folgt so mit 2.2.5, dass $\mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})B\mathrm{GL}_n(\mathfrak{o})$ nur aus höchstens einer Doppelnebenklasse bezüglich $\mathrm{GL}_n(\mathfrak{o})$ besteht. Die Behauptung erhält man nun aus $AB \in \mathrm{GL}_n(\mathfrak{o})A\mathrm{GL}_n(\mathfrak{o})B\mathrm{GL}_n(\mathfrak{o})$. $\square$

Die in diesem Abschnitt bewiesenen Sätze finden im folgenden Anwendung, wenn es darum geht, Hecke-Algebren als Tensorprodukte zu schreiben und die Struktur der einzelnen Faktoren genauer zu untersuchen.

§ 2.7

TENSORPRODUKTZERLEGUNGEN

Die »klassische« Hecke-Algebra $H(\mathrm{GL}_n(\mathbb{Q}), \mathrm{IL}_n(\mathbb{Z}), \mathrm{GL}_n(\mathbb{Z}))$ lässt sich bis auf Isomorphie als Tensorprodukt über alle Teilalgebren der Form $H(\mathrm{GL}_n(\mathbb{Q}), I_{n,p}, \mathrm{GL}_n(\mathbb{Z}))$ für Primzahlen $p \in \mathbb{N}$ schreiben, wobei $I_{n,p}$ die Menge aller $(n \times n)$ -Matrizen über $\mathbb{Z}$ mit Determinante aus $\{\pm 1, \pm p, \pm p^2, \pm p^3, \dots\}$ bezeichnet (vergleiche etwa [Fre83] IV.2.2 (S. 238)). Im hier betrachteten allgemeinen Fall ist eine solche Tensorproduktarstellung weder über Primelemente noch über Primideale von $\mathfrak{o}$ möglich. Hauptgründe dafür sind die Tatsachen, dass einerseits die Primelementzerlegung in $\mathfrak{o}$ nicht immer eindeutig zu sein braucht und andererseits nicht für jeden Dedekind-Ring jede Primidealpotenz $\mathfrak{p}^k$ als Determinante einer Matrix auftreten kann, denn dies würde erfordern, dass $\mathfrak{p}^k$ stets ein Hauptideal ist. Indem die Menge der möglichen Determinanten eingeschränkt wird, erhält man jedoch zumindest für eine Teilalgebra eine zum klassischen Fall analoge Zerlegung. Zunächst werden die benötigten Voraussetzungen dargestellt.

2.7.1 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Sei $\mathfrak{o}$ ein normendlicher Dedekind-Ring und K dessen Quotientenkörper. Für jedes $n \in \mathbb{N}$ sei $G_n = \mathrm{GL}_n(K)$ und $U_n = \mathrm{GL}_n(\mathfrak{o})$ sowie $I_n = \mathrm{IL}_n(\mathfrak{o})$. Weiter seien die sich daraus ergebenden Bezeichnungen aus 1.1.4 übernommen (mit G_n anstelle von G und U_n anstelle von U sowie I_n anstelle von M).

Definiere nun weiter

$$I_n^* = \{A \in I_n \mid \mathfrak{d}_n(A) = a\mathfrak{o} \text{ für ein } a \in \mathbb{Z}\},$$

und für jede Primzahl $p \in \mathbb{N}$ setze

$$I_{n,p}^* = \{A \in I_n^* \mid \mathfrak{d}_n(A) = p^k \mathfrak{o} \text{ für ein } k \in \mathbb{N}_0\}. \quad \diamond$$

Mit diesen Bezeichnungen kann man nun zusätzlich die Hecke-Algebren $H(G_n, I_n^*, U_n)$ und $H(G_n, I_{n,p}^*, U_n)$ bilden und untersuchen.

2.7.2 DEFINITION: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und $p \in \mathbb{N}$ eine Primzahl. Dann heit $H(G_n, I_{n,p}^*, U_n)$ *Primrkomponente* von $H(G_n, I_n^*, U_n)$ bezglich p . $\diamond$

Um die Wohldefiniertheit der angestrebten Tensorproduktdarstellung zu zeigen, bentigt man zunchst eine Aussage, die $\llbracket A \rrbracket * \llbracket B \rrbracket$ fr den Fall von teilerfremden Determinanten beschreibt. In deren Beweis wird die folgende Charakterisierung der Tatsache, dass smtliche Eintrge einer ber K gegebenen Matrix bereits in $\mathfrak{o}$ liegen, verwendet.

2.7.3 LEMMA: Sei $\mathfrak{o}$ ein Dedekind-Ring mit Quotientenkrper K und $n \in \mathbb{N}$. Weiter seien $l, m \in \mathfrak{o}$ teilerfremd und $M \in K^{n \times n}$ mit $lM \in \mathfrak{o}^{n \times n}$ und $mM \in \mathfrak{o}^{n \times n}$. Dann gilt $M \in \mathfrak{o}^{n \times n}$. $\diamond$

BEWEIS:

Sei x ein beliebiger Eintrag von M . Dann gilt $lx \in \mathfrak{o}$ und $mx \in \mathfrak{o}$, also $x \in l^{-1}\mathfrak{o} \cap m^{-1}\mathfrak{o}$. Da l und m teilerfremd sind, gilt nach 1.2.6 $l^{-1}\mathfrak{o} \cap m^{-1}\mathfrak{o} = \mathfrak{o}$. Dies beweist die Behauptung. $\square$

Nun kann im Falle von teilerfremden Determinanten das Produkt $\llbracket A \rrbracket * \llbracket B \rrbracket$ auf ein Matrixprodukt zurckgefhrt werden.

2.7.4 SATZ: Es seien die Bezeichnungen aus 2.7.1 bernommen und $n \in \mathbb{N}$. Weiter seien Matrizen $A, B \in I_n$ gegeben mit $\mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{o}$. Dann gilt $\llbracket A \rrbracket * \llbracket B \rrbracket = \llbracket AB \rrbracket$. $\diamond$

BEWEIS:

Nach 2.6.9 gilt $U_n A U_n B U_n = U_n A B U_n$, also muss nach 1.1.9 ein $c \in \mathbb{C}$ mit $\llbracket A \rrbracket * \llbracket B \rrbracket = c \llbracket AB \rrbracket$ existieren. Sei $\{A_1, \dots, A_r\}$ ein Vertretersystem von $U_n \setminus [A]$ und $\{B_1, \dots, B_s\}$ ein Vertretersystem von $U_n \setminus [B]$. Fr $c = 1$ gengt es nach 1.1.10 zu zeigen, dass die Rechtsnebenklassen $U_n A_i B_j$ fr $1 \leq i \leq r$ und $1 \leq j \leq s$ paarweise verschieden sind. Seien

nun $1 \leq i, k \leq r$ und $1 \leq j, l \leq s$ mit $U_n A_i B_j = U_n A_k B_l$. Dann existiert ein $P \in U_n$ mit $PA_i B_j = A_k B_l$, und es folgt $A_k^{-1} P A_i = B_l B_j^{-1}$ woraus man mit $\varepsilon := (\det A)(\det A_k)^{-1}$ die Gleichungskette

$$(\det A) B_l B_j^{-1} = \varepsilon (\det A_k) B_l B_j^{-1} = \varepsilon (\det A_k) A_k^{-1} P A_i = \varepsilon A_k^{\text{adj}} P A_i$$

erhält, wobei der rechtsstehende Ausdruck ein Produkt von ε mit Matrizen aus $\mathfrak{o}^{n \times n}$ ist und $\varepsilon = (\det A)(\det A_k)^{-1} \in \mathfrak{o}^*$ wegen $A_k \in [A]$ nach 2.2.5 gilt, was insgesamt beweist, dass $(\det A) B_l B_j^{-1} \in \mathfrak{o}^{n \times n}$ gilt. Andererseits hat man mit $\varepsilon' := (\det B)(\det B_j)^{-1} \in \mathfrak{o}^*$ auch

$$(\det B) B_l B_j^{-1} = \varepsilon' (\det B_j) B_l B_j^{-1} = \varepsilon' B_l B_j^{\text{adj}} \in \mathfrak{o}^{n \times n},$$

so dass man aus der wegen $\mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{o}$ gegebenen Teilerfremdheit von $\det A$ und $\det B$ nach 2.7.3 erhält, dass $B_l B_j^{-1} \in \mathfrak{o}^{n \times n}$ gilt. Wegen $\det(B_l B_j^{-1}) = (\det B_l)(\det B_j)^{-1} = \varepsilon' \in \mathfrak{o}^*$ hat man sogar $B_l B_j^{-1} \in U_n$, also erhält man $U_n B_l = U_n B_j$, und da B_l und B_j aus einem Vertretersystem von $U_n \setminus [B]$ gewählt wurden, muss dann sogar $B_l = B_j$ gelten. Analog erhält man $A_i = A_k$, denn aus $PA_i B_j = A_k B_l$ folgt wegen $B_j = B_l$ und $B_j, B_l \in I_n$ zunächst $PA_i = A_k$ und damit $U_n A_i = U_n A_k$. Damit wurde gezeigt, dass $U_n A_i B_j = U_n A_k B_l$ nur für $(i, j) = (k, l)$ gelten kann, was beweist, dass die $U_n A_i B_j$ paarweise verschieden sind. Dies schließt den Beweis ab. $\square$

Nachdem nun bewiesen wurde, dass in bestimmten Spezialfällen $\llbracket A \rrbracket * \llbracket B \rrbracket = \llbracket AB \rrbracket$ gilt, stellt sich die Frage, wann sich umgekehrt zu einem $C \in I_n$ Matrizen A und B finden lassen, die gewissen Nebenbedingungen genügen und $\llbracket C \rrbracket = \llbracket A \rrbracket * \llbracket B \rrbracket$ erfüllen.

2.7.5 SATZ: Es seien die Bezeichnungen aus 2.7.1 übernommen. Weiter sei $n \in \mathbb{N}$ und $C \in I_n$. Gibt es Hauptideale $\mathfrak{a}, \mathfrak{b}$ in $\mathfrak{o}$ mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ und $\mathfrak{d}_n(C) = \mathfrak{a}\mathfrak{b}$, so gibt es Matrizen $A, B \in I_n$ mit $\mathfrak{d}_n(A) = \mathfrak{a}$ und $\mathfrak{d}_n(B) = \mathfrak{b}$ sowie $\llbracket C \rrbracket = \llbracket A \rrbracket * \llbracket B \rrbracket$. Die Doppelnebenklassen $[A]$ und $[B]$ sind durch diese Bedingungen eindeutig bestimmt. $\diamond$

BEWEIS:

Existenz: Für jedes $1 \leq k \leq n$ definiere Ideale $\mathfrak{a}_k$ und $\mathfrak{b}_k$ durch

$$\mathfrak{v}_{\mathfrak{p}}(\mathfrak{a}_k) = \begin{cases} \mathfrak{v}_{\mathfrak{p}}(\mathfrak{e}_k(C)), & \text{falls } \mathfrak{p} \mid \mathfrak{a}, \\ 0 & \text{sonst} \end{cases}$$

und

$$\mathfrak{v}_{\mathfrak{p}}(\mathfrak{b}_k) = \begin{cases} \mathfrak{v}_{\mathfrak{p}}(\mathfrak{e}_k(C)), & \text{falls } \mathfrak{p} \mid \mathfrak{b}, \\ 0 & \text{sonst} \end{cases}$$

für alle Primideale $\mathfrak{p}$ von $\mathfrak{o}$. Da die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind und $\mathfrak{e}_k(C) \mid \mathfrak{d}_n(C) = \mathfrak{a}\mathfrak{b}$ gilt (2.2.4 (d), (g)), hat man mit dieser Wahl $\mathfrak{a}_k\mathfrak{b}_k = \mathfrak{e}_k(C)$ (1.2.5). Wegen $\mathfrak{e}_1(C) \mid \cdots \mid \mathfrak{e}_n(C)$ (2.2.4 (f)) gilt dann auch $\mathfrak{a}_1 \mid \cdots \mid \mathfrak{a}_n$ und $\mathfrak{b}_1 \mid \cdots \mid \mathfrak{b}_n$, und da $\mathfrak{e}_1(C) \cdots \mathfrak{e}_n(C) = \mathfrak{d}_n(C) = \mathfrak{a}\mathfrak{b}$ gilt, hat man $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}$ sowie $\mathfrak{b}_1 \cdots \mathfrak{b}_n = \mathfrak{b}$, also sind diese Produkte Hauptideale. Damit existieren nach 2.2.10 Matrizen $A, B \in I_n$, die $\mathfrak{e}_k(A) = \mathfrak{a}_k$ und $\mathfrak{e}_k(B) = \mathfrak{b}_k$ für alle $1 \leq k \leq n$ erfüllen. Für diese Matrizen gilt $\mathfrak{d}_n(A) + \mathfrak{d}_n(B) = \mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ und $\llbracket A \rrbracket * \llbracket B \rrbracket = \llbracket AB \rrbracket$ nach 2.7.4 sowie $\mathfrak{d}_k(AB) = \mathfrak{d}_k(A)\mathfrak{d}_k(B) = \mathfrak{a}_1 \cdots \mathfrak{a}_k \cdot \mathfrak{b}_1 \cdots \mathfrak{b}_k = \mathfrak{d}_k(C)$ nach 2.6.8 für alle $1 \leq k \leq n$. Mit 2.2.5 erhält man aus der letzten Aussage $\llbracket AB \rrbracket = \llbracket C \rrbracket$, womit insgesamt $\llbracket C \rrbracket = \llbracket A \rrbracket * \llbracket B \rrbracket$ gezeigt ist.

Eindeutigkeit: Sind $A, A', B, B' \in I_n$ mit $\mathfrak{d}_n(A) = \mathfrak{a} = \mathfrak{d}_n(A')$ und $\mathfrak{d}_n(B) = \mathfrak{b} = \mathfrak{d}_n(B')$ sowie $\llbracket A \rrbracket * \llbracket B \rrbracket = \llbracket C \rrbracket = \llbracket A' \rrbracket * \llbracket B' \rrbracket$, so gilt

$$\mathfrak{d}_k(A)\mathfrak{d}_k(B) \stackrel{2.6.8}{=} \mathfrak{d}_k(AB) \stackrel{2.7.4}{\stackrel{2.2.5}{=}} \mathfrak{d}_k(C) \stackrel{2.7.4}{\stackrel{2.2.5}{=}} \mathfrak{d}_k(A'B') \stackrel{2.6.8}{=} \mathfrak{d}_k(A')\mathfrak{d}_k(B')$$

für alle $1 \leq k \leq n$. Da $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind und $\mathfrak{d}_k(A), \mathfrak{d}_k(A') \mid \mathfrak{a}$ sowie $\mathfrak{d}_k(B), \mathfrak{d}_k(B') \mid \mathfrak{b}$ gilt, folgt $\mathfrak{d}_k(A') = \mathfrak{d}_k(A)$ und $\mathfrak{d}_k(B) = \mathfrak{d}_k(B')$ für alle $1 \leq k \leq n$, was mit 2.2.5 $\llbracket A \rrbracket = \llbracket A' \rrbracket$ und $\llbracket B \rrbracket = \llbracket B' \rrbracket$ zeigt und die Eindeutigkeit beweist. $\square$

Als Vorstufe zur Zerlegung von $H(G_n, I_n^*, U_n)$ beschreibt das folgende Lemma das Tensorprodukt zweier Teilalgebren.

2.7.6 LEMMA: Es seien die Bezeichnungen aus 2.7.1 übernommen und $n \in \mathbb{N}$. Ist $\mathfrak{M}$ eine multiplikativ abgeschlossene Menge von Hauptidealen in $\mathfrak{o}$ (insbesondere gelte $\mathfrak{o} \in \mathfrak{M}$), so sei $M_{\mathfrak{M}} = \{A \in I_n \mid \mathfrak{d}_n(A) \in \mathfrak{M}\}$. Seien nun $\mathfrak{A}$ und $\mathfrak{B}$ zwei multiplikativ abgeschlossene Mengen von Hauptidealen in $\mathfrak{o}$, so dass $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ für alle $\mathfrak{a} \in \mathfrak{A}$ und $\mathfrak{b} \in \mathfrak{B}$ gilt, und $\mathfrak{A}\mathfrak{B}$ bezeichne die Menge $\{\mathfrak{a}\mathfrak{b} \mid \mathfrak{a} \in \mathfrak{A}, \mathfrak{b} \in \mathfrak{B}\}$. Dann gilt

$$H(G_n, M_{\mathfrak{A}\mathfrak{B}}, U_n) \cong H(G_n, M_{\mathfrak{A}}, U_n) \otimes H(G_n, M_{\mathfrak{B}}, U_n). \quad \diamond$$

BEWEIS:

Da die $\llbracket A \rrbracket$ für $A :: U_n \setminus M_{\mathfrak{A}} // U_n$ eine Vektorraumbasis der Hecke-Algebra $H(G_n, M_{\mathfrak{A}}, U_n)$ bilden und Analoges für $B :: U_n \setminus M_{\mathfrak{B}} // U_n$ gilt, genügt es zu zeigen, dass die $\llbracket A \rrbracket * \llbracket B \rrbracket$ für $A :: U_n \setminus M_{\mathfrak{A}} // U_n$ und $B :: U_n \setminus M_{\mathfrak{B}} // U_n$ eine Basis von $H(G_n, M_{\mathfrak{A}\mathfrak{B}}, U_n)$ darstellen.

Zeige zunächst, dass die Elemente $\llbracket A \rrbracket * \llbracket B \rrbracket$ für $A :: U_n \setminus M_{\mathfrak{A}} // U_n$ und $B :: U_n \setminus M_{\mathfrak{B}} // U_n$ ein Vektorraum-Erzeugendensystem von $H(G_n, M_{\mathfrak{A}\mathfrak{B}}, U_n)$ bilden. Dazu weise nach, dass sich jedes $\llbracket C \rrbracket$ für $C \in M_{\mathfrak{A}\mathfrak{B}}$ als Linearkombination solcher Produkte schreiben lässt. Ist $C \in M_{\mathfrak{A}\mathfrak{B}}$, so gilt $\mathfrak{d}_2(C) \in \mathfrak{A}\mathfrak{B}$, also gibt es dann ein $\mathfrak{a} \in \mathfrak{A}$ und ein $\mathfrak{b} \in \mathfrak{B}$ mit $\mathfrak{d}_2(C) = \mathfrak{a}\mathfrak{b}$, und es gilt $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$. Nach 2.7.5 existiert dann ein $A \in M_{\mathfrak{A}}$ und ein $B \in M_{\mathfrak{B}}$ mit $\llbracket C \rrbracket = \llbracket A \rrbracket * \llbracket B \rrbracket$, wobei man ohne Einschränkung A aus einem vorgegebenen Vertretersystem von $U_n \setminus M_{\mathfrak{A}} // U_n$ wählen kann und Analoges für B gilt.

Nun verbleibt zu zeigen, dass die $\llbracket A \rrbracket * \llbracket B \rrbracket$ für $A :: U_n \setminus M_{\mathfrak{A}} // U_n$ und $B :: U_n \setminus M_{\mathfrak{B}} // U_n$ linear unabhängig sind. Da A und B teilerfremde Determinanten haben, gilt nach 2.7.4 $\llbracket A \rrbracket * \llbracket B \rrbracket = \llbracket AB \rrbracket$. Da die $\llbracket C \rrbracket$ mit $C \in I_n$ und $\mathfrak{d}_n(C) \in \mathfrak{A}\mathfrak{B}$ eine Basis von $H(G_n, M_{\mathfrak{A}\mathfrak{B}}, U_n)$ bilden, genügt es zu zeigen, dass aus $\llbracket A'B' \rrbracket = \llbracket AB \rrbracket$ für $A, A' \in M_{\mathfrak{A}}$ und $B, B' \in M_{\mathfrak{B}}$ stets $\llbracket A \rrbracket = \llbracket A' \rrbracket$ und $\llbracket B \rrbracket = \llbracket B' \rrbracket$ folgt. Setze

$$\mathfrak{a} = \mathfrak{d}_n(A), \quad \mathfrak{a}' = \mathfrak{d}_n(A'), \quad \mathfrak{b} = \mathfrak{d}_n(B), \quad \mathfrak{b}' = \mathfrak{d}_n(B').$$

Dann gilt $ab = a'b'$ und $a, a' \in \mathfrak{A}$ sowie $b, b' \in \mathfrak{B}$. Für jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$ folgt $v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a') + v_{\mathfrak{p}}(b')$ (1.2.5). Betrachte als ersten Fall, dass $v_{\mathfrak{p}}(a) = 0$ und $v_{\mathfrak{p}}(b) = 0$ gilt. Dann muss auch $v_{\mathfrak{p}}(a') = 0$ und $v_{\mathfrak{p}}(b') = 0$ gelten, da alle auftretenden Vielfachheiten wegen $a, b \subseteq \mathfrak{o}$ nichtnegativ sein müssen. Als zweiten Fall betrachte $v_{\mathfrak{p}}(a) = 0$ und $v_{\mathfrak{p}}(b) > 0$. Da nach Wahl von $\mathfrak{A}$ und $\mathfrak{B}$ die Ideale a' und b teilerfremd sind, folgt $v_{\mathfrak{p}}(a') = 0 = v_{\mathfrak{p}}(a)$, und daraus erhält man $v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(b')$ wegen $v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a') + v_{\mathfrak{p}}(b')$. Im verbleibenden Fall ist $v_{\mathfrak{p}}(a) > 0$. Wegen $a + b = \mathfrak{o}$ und $a + b' = \mathfrak{o}$ folgt $v_{\mathfrak{p}}(b) = 0 = v_{\mathfrak{p}}(b')$ und somit auch $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(a')$. Insgesamt wurde damit in allen Fällen $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(a')$ und $v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(b')$ gezeigt, und da dies für jedes Primideal $\mathfrak{p}$ gilt, muss $a = a'$ und $b = b'$ gelten. Mit der Eindeutigkeit der Zerlegung aus 2.7.5 erhält man nun $[A] = [A']$ und $[B] = [B']$, was den Beweis abschließt. $\square$

Es folgt die angekündigte Tensorproduktzerlegung. Die Aussage wird dabei etwas allgemeiner formuliert und bewiesen, so dass die Zerlegung von $H(G_n, I_n^*, U_n)$ eine einfache Folgerung aus diesem Satz ist.

2.7.7 SATZ: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und R ein faktorieller Teilring von $\mathfrak{o}$ sowie

$$M_n = \{A \in I_n \mid \mathfrak{d}_n(A) = r\mathfrak{o} \text{ für ein } r \in R\}.$$

Weiter sei $P(R)$ die Menge der Primelemente von R und P ein Vertretersystem von $P(R) // R^*$. Für jedes $p \in P$ setze

$$M_{n,p} = \{A \in M_n \mid \mathfrak{d}_n(A) = p^k \mathfrak{o} \text{ für ein } k \in \mathbb{N}_0\}.$$

Dann gilt

$$H(G_n, M_n, U_n) \cong \bigotimes_{p \in P} H(G_n, M_{n,p}, U_n).$$

$\diamond$

BEWEIS:

Sei $p_1, p_2, \dots$ eine Abzählung von P und

$$\mathfrak{A} = \{p_1^v \mathfrak{o} \mid v \in \mathbb{N}_0\}$$

sowie

$$\mathfrak{B} = \{p_{i_1}^{v_1} \cdots p_{i_k}^{v_k} \mathfrak{o} \mid k \in \mathbb{N}_0, 2 \leq i_1 < \cdots < i_k, v_1, \dots, v_k \in \mathbb{N}\}.$$

Diese Mengen erfüllen die Voraussetzungen von 2.7.6 (Teilerfremdheit über R impliziert Teilerfremdheit über $\mathfrak{o}$, da aus $aR + bR = R$ stets $\mathfrak{o} = R\mathfrak{o} = (aR + bR)\mathfrak{o} \subseteq a\mathfrak{o} + b\mathfrak{o}$ folgt), und $\mathfrak{A}\mathfrak{B}$ ist die Menge aller Ideale der Form $r\mathfrak{o}$ mit $r \in R$. Mit den Bezeichnungen aus dem letzten Lemma ist also

$$\begin{aligned} H(G_n, M_n, U_n) &= H(G_n, M_{\mathfrak{A}\mathfrak{B}}, U_n) \\ &\cong H(G_n, M_{\mathfrak{A}}, U_n) \otimes H(G_n, M_{\mathfrak{B}}, U_n) \\ &= H(G_n, M_{n,p_1}, U_n) \otimes H(G_n, M_{\mathfrak{B}}, U_n). \end{aligned}$$

Spaltet man nun analog $H(G_n, M_{n,p_2}, U_n)$ von $H(G_n, M_{\mathfrak{B}}, U_n)$ ab und setzt diese Abspaltung mit $p_3, p_4, \dots$ fort, erhält man induktiv die Behauptung. $\square$

2.7.8 FOLGERUNG: Es seien die Bezeichnungen aus 2.7.1 übernommen und $n \in \mathbb{N}$. Dann gilt

$$H(G_n, I_n^*, U_n) \cong \bigotimes_{p \text{ Primzahl in } \mathbb{N}} H(G_n, I_{n,p}^*, U_n).$$

$\diamond$

Die gerade gezeigte Zerlegung von $H(G_n, I_n^*, U_n)$ zieht nun die Frage nach der Struktur der Primärkomponenten dieser Hecke-Algebra nach sich. Erste Aussagen in diese Richtung liefert der übernächste Abschnitt, in dem endliche Erzeugendensysteme von $H(G_n, I_{n,p}^*, U_n)$ bestimmt werden. Zunächst müssen jedoch noch einige Vorbereitungen getroffen werden.

§ 2.8

ZERLEGBARE MATRIZEN

Als Vorbereitung zur Bestimmung von Erzeugendensystemen von Primärkomponenten wird in diesem Abschnitt das Konzept der zerlegbaren und unzerlegbaren Matrizen eingeführt und untersucht. Es wird sich herausstellen, dass man Erzeugendensysteme von Hecke-Algebren dadurch charakterisieren kann, dass sie alle Funktionen $\llbracket C \rrbracket$ für unzerlegbare $C \in I_n$ erzeugen, was die Überprüfung dieser Eigenschaft vereinfacht, da es nur endlich viele unzerlegbare Matrizen gibt.

Bevor der Begriff der zerlegbaren Matrizen definiert werden kann, müssen zunächst zwei Größenrelationen im Determinantenteilersinne eingeführt werden.

2.8.1 DEFINITION: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und $A, B \in I_n$. Gilt $\mathfrak{d}_i(A) \mid \mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$, so heißt A im Determinantenteilersinne kleiner/gleich B ; dies wird mit $A \trianglelefteq B$ bezeichnet. Gibt es zusätzlich ein $1 \leq i \leq n$ mit $\mathfrak{d}_i(A) \nmid \mathfrak{d}_i(B)$, so heißt A im Determinantenteilersinne (echt) kleiner als B ; dies wird mit $A \triangleleft B$ bezeichnet. $\diamond$

Diese Größenrelation wird zunächst im folgenden Lemma benötigt, das Aussagen über das Verschwinden und Nichtverschwinden von Koeffizienten in einem Produkt der Form $\llbracket A \rrbracket * \llbracket B \rrbracket$ macht.

2.8.2 LEMMA: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und $A, B, C \in I_n$ mit $\mathfrak{d}_k(C) = \mathfrak{d}_k(A)\mathfrak{d}_k(B)$ für alle $1 \leq k \leq n$. Dann gilt $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) \neq 0$, und für alle $C' \in I_n$ mit $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C') \neq 0$ folgt $C \trianglelefteq C'$. $\diamond$

BEWEIS:

Diese Aussagen folgen mit 1.1.9 aus 2.6.4 beziehungsweise 2.6.2. $\square$

Weiter kann nun auch der für diesen Abschnitt titelgebende Begriff eingeführt werden.

2.8.3 DEFINITION (zerlegbar, unzerlegbar): Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und M_n ein Untermonoid von I_n mit $U_n \subseteq M_n$ sowie $C \in M_n$. Gibt es $A, B \in M_n$ mit $\mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B) \parallel \mathfrak{d}_n(C)$, so dass $C \in U_n A U_n B U_n$ gilt und für $C' \in U_n A U_n B U_n$ stets $C \leq C'$ folgt, so heißt C in M_n *zerlegbar* mit A und B . Ist C nicht zerlegbar, so heißt es *unzerlegbar*. Ist $f \in H(G_n, M_n, U_n)$ mit $f(C) \neq 0$ nur für unzerlegbare $C \in M_n$, so heißt auch f *unzerlegbar*. $\diamond$

Erstes Ziel dieses Abschnitts ist der Beweis der Tatsache, dass eine Menge, die alle $\llbracket C \rrbracket$ für unzerlegbare Matrizen C erzeugt, bereits ein Erzeugendensystem der Hecke-Algebra $H(G_n, M_n, U_n)$ ist. Dieser Beweis – und auch der Nachweis eines vorbereitenden Lemmas – lässt sich mit dem Begriff des harmonischen Elements für Hecke-Algebren leichter formulieren.

2.8.4 DEFINITION (harmonisch): Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und M_n ein Untermonoid von I_n mit $U_n \subseteq M_n$ sowie $f \in H(G_n, M_n, U_n)$ und $\mathfrak{a}$ ein Ideal von $\mathfrak{o}$. Ist $f(C) = 0$ für alle $C \in M_n$ mit $\mathfrak{d}_n(C) \neq \mathfrak{a}$, so heißt f *harmonisch* zur Determinante $\mathfrak{a}$.

Ist $f \in H(G_n, M_n, U_n)$ beliebig, so definiere $f_{\mathfrak{a}} \in H(G_n, M_n, U_n)$ durch

$$f_{\mathfrak{a}} : C \mapsto \begin{cases} f(C), & \text{falls } \mathfrak{d}_n(C) = \mathfrak{a}, \\ 0 & \text{sonst.} \end{cases}$$

Dieses $f_{\mathfrak{a}}$ heißt *$\mathfrak{a}$ -harmonischer Teil* von f . $\diamond$

Es folgt das angekündigte vorbereitende Lemma für den Beweis von 2.8.6.

2.8.5 LEMMA: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und M_n Untermonoid von I_n mit $U_n \subseteq M_n$ sowie $f \in H(G_n, M_n, U_n)$ und $\mathfrak{a}$ ein Ideal von $\mathfrak{o}$. Dann gibt es ein $k \in \mathbb{N}_0$ und $c_1, \dots, c_k \in \mathbb{C}$ sowie Matrizen $A_1, \dots, A_k, B_1, \dots, B_k \in M_n$ mit $\mathfrak{d}_n(A_i) \parallel \mathfrak{a}$ und $\mathfrak{d}_n(B_i) \parallel \mathfrak{a}$ sowie $\mathfrak{d}_n(A_i B_i) = \mathfrak{a}$ für alle $1 \leq i \leq k$, so dass der $\mathfrak{a}$ -harmonische Teil von $f + c_1 \llbracket A_1 \rrbracket * \llbracket B_1 \rrbracket + \dots + c_k \llbracket A_k \rrbracket * \llbracket B_k \rrbracket$ unzerlegbar ist. $\diamond$

BEWEIS:

Mit 2.2.5 folgt, dass es nur endlich viele Doppelnebenklassen der Form $[C]$ mit $\mathfrak{d}_n(C) = \mathfrak{a}$ gibt, da nur endlich viele Möglichkeiten für die $\mathfrak{d}_1(C), \dots, \mathfrak{d}_{n-1}(C)$ existieren (denn sie müssen nach 2.2.4 (f) alle Teiler von $\mathfrak{d}_n(C) = \mathfrak{a}$ sein). Daher ist für jedes $C \in M_n$ mit $\mathfrak{d}_n(C) = \mathfrak{a}$ die Zahl

$$d(C) = \max\{l \in \mathbb{N}_0 \mid \exists C_1, \dots, C_l \in M_n : C = C_0 \triangleleft \dots \triangleleft C_l, \\ \mathfrak{d}_n(C_1) = \dots = \mathfrak{d}_n(C_l) = \mathfrak{a}\}$$

wohldefiniert, und es gibt ein $D \in \mathbb{N}_0$ mit $d(C) \leq D$ für alle $C \in M_n$ mit $\mathfrak{d}_n(C) = \mathfrak{a}$. Für jedes $C' \in M_n$ mit $\mathfrak{d}_n(C') = \mathfrak{a}$ und $C \triangleleft C'$ gilt $d(C) > d(C')$, denn man kann stets $C' \triangleleft \dots \triangleleft C_l$ zu $C \triangleleft C' \triangleleft \dots \triangleleft C_l$ erweitern. Für jedes $s \in \mathbb{N}_0$ und $g \in H(G_n, M_n, U_n)$ definiere nun noch

$$Z_s(g) = \{[C] \mid g(C) \neq 0, C \text{ zerlegbar}, \mathfrak{d}_n(C) = \mathfrak{a}, d(C) = s\}.$$

(1) Es gebe ein $s \in \mathbb{N}_0$ mit $Z_s(f) \neq \emptyset$. Zeige, dass man dann ein $c \in \mathbb{C}$ und $A, B \in M_n$ mit $\mathfrak{d}_n(A) \parallel \mathfrak{a}$ und $\mathfrak{d}_n(B) \parallel \mathfrak{a}$ sowie $\mathfrak{d}_n(AB) = \mathfrak{a}$ findet, so dass $f^* := f + c \llbracket A \rrbracket * \llbracket B \rrbracket$ die Inklusion $Z_s(f^*) \subsetneq Z_s(f)$ und für alle $t > s$ die Gleichung $Z_t(f^*) = Z_t(f)$ erfüllt. Wähle ein $C \in Z_s(f)$. Dann ist C zerlegbar, also existieren $A, B \in M_n$ mit $\mathfrak{d}_n(A) \parallel \mathfrak{a}$ und $\mathfrak{d}_n(B) \parallel \mathfrak{a}$, so dass $C \in U_n A U_n B U_n$ gilt. Aus Letzterem folgt bereits $\mathfrak{d}_n(AB) = \mathfrak{d}_n(A) \mathfrak{d}_n(B) = \mathfrak{d}_n(C) = \mathfrak{a}$, so dass nur noch zu zeigen verbleibt, dass ein $c \in \mathbb{C}$ existiert, so dass $f^* := f + c \llbracket A \rrbracket * \llbracket B \rrbracket$ die Inklusion $Z_s(f^*) \subsetneq Z_s(f)$ erfüllt und für alle $t > s$ die Gleichung

$Z_t(f^*) = Z_t(f)$ gilt. Wähle nun $c = -f(C)(([A] * [B])(C))^{-1}$, was möglich ist, da nach 1.1.9 $C \in U_n A U_n B U_n = \text{Tr}([A] * [B])$ und somit $([A] * [B])(C) \neq 0$ gilt. Dann hat man

$$\begin{aligned} f^*(C) &= f(C) + c([A] * [B])(C) \\ &= f(C) - f(C)(([A] * [B])(C))^{-1}([A] * [B])(C) \\ &= f(C) - f(C) = 0, \end{aligned}$$

also $[C] \notin Z_s(f^*)$. Sei $C' \in M_n$ mit $[C'] \in Z_s(f^*)$. Aus $[C] \notin Z_s(f^*)$ folgt dann insbesondere $[C'] \neq [C]$, also gibt es nach 2.2.5 ein $k \in \mathbb{N}$ mit $k \leq n$ und $\mathfrak{d}_k(C') \neq \mathfrak{d}_k(C)$. Wäre $C' \in \text{Tr}([A] * [B])$, so erhielte man mit 2.8.2, dass $C \leq C'$ gelten würde, und wegen $\mathfrak{d}_k(C') \neq \mathfrak{d}_k(C)$ hätte man sogar $C \triangleleft C'$, woraus wie oben gesehen $d(C) > d(C')$ folgte, was wegen $[C] \in Z_s(f)$ und $[C'] \in Z_s(f^*)$ den Widerspruch $s > s$ liefern würde. Somit kann nicht $C' \in \text{Tr}([A] * [B])$ gelten; da nach Definition von f^* aber $[C'] \in Z_s(f)$ oder $C' \in \text{Tr}([A] * [B])$ gelten muss, folgt $[C'] \in Z_s(f)$, und wegen $[C'] \neq [C]$ hat man sogar $[C'] \in Z_s(f) \setminus \{[C]\}$. Dies beweist $Z_s(f^*) \subsetneq Z_s(f)$. Da f und f^* sich nach Definition höchstens auf $\text{Tr}([A] * [B])$ unterscheiden, für jedes $C' \in \text{Tr}([A] * [B])$ mit $[C'] \neq [C]$ wie oben gesehen $d(C') < d(C) = s$ gilt und man im Falle $[C'] = [C]$ klarerweise $d(C') = d(C) = s$ hat, stimmen $Z_t(f)$ und $Z_t(f^*)$ für alle $t \in \mathbb{N}_0$ mit $t > s$ überein.

(2) Es gebe ein $s \in \mathbb{N}_0$ mit $Z_t(f) = \emptyset$ für alle $t \in \mathbb{N}_0$ mit $t > s$. Sei $|Z_s(f)| = k$. Setze $f_k = f$. Für jedes $i = k, k-1, \dots, 1$ existieren nach (1) $c_i \in \mathbb{C}$ und $A_i, B_i \in M_n$ mit $\mathfrak{d}_n(A_i) \parallel \mathfrak{a}$ und $\mathfrak{d}_n(B_i) \parallel \mathfrak{a}$ sowie $\mathfrak{d}_n(A_i B_i) = \mathfrak{a}$, so dass $f_{i-1} := f_i + c_i [A_i] * [B_i]$ die Inklusion $Z_s(f_{i-1}) \subsetneq Z_s(f_i)$ und für alle $t > s$ die Gleichung $Z_t(f_{i-1}) = Z_t(f_i)$ erfüllt. Wegen $|Z_s(f)| = k$ hat man so schließlich $Z_s(f_0) = \emptyset$ und weiter $Z_t(f_0) = Z_t(f_k) = Z_t(f) = \emptyset$ für alle $t > s$, also insgesamt $Z_t(f_0) = \emptyset$ für alle $t \geq s$.

(3) Nach Wahl von D ist die Voraussetzung von (2) für $s = D$ erfüllt. Bezeichne mit $\tilde{f}_{D-1}$ das zu $\tilde{f}_D := f$ gemäß (2) konstruierte f_0 .

Dann gilt $Z_t(\tilde{f}_{D-1}) = \emptyset$ für alle $t > D - 1$, also erfüllt $\tilde{f}_{D-1}$ die Voraussetzungen an f in (2) für $s = D - 1$, so dass sich analog zum Übergang von $\tilde{f}_D$ zu $\tilde{f}_{D-1}$ ein $\tilde{f}_{D-2}$ zu $\tilde{f}_{D-1}$ konstruieren lässt und man dann auch weiter $\tilde{f}_{D-3}, \dots, \tilde{f}_0$ analog erhält. Man hat schließlich $Z_t(\tilde{f}_0) = \emptyset$ für alle $t \in \mathbb{N}_0$, was nach der Definition der Z_t bedeutet, dass der α -harmonische Teil von $\tilde{f}_0$ unzerlegbar ist. Darüberhinaus ist nach Konstruktion $\tilde{f}_0 - f$ eine Linearkombination von Funktionen der Form $\llbracket A \rrbracket * \llbracket B \rrbracket$ mit $A, B \in M_n$ und $\mathfrak{d}_n(A) \parallel \alpha$ sowie $\mathfrak{d}_n(B) \parallel \alpha$ und $\mathfrak{d}_n(AB) = \alpha$, womit die Behauptung bewiesen ist. $\square$

Damit sind die Vorbereitungen zum Beweis der Charakterisierung von Erzeugendensystemen von Hecke-Algebren abgeschlossen.

2.8.6 SATZ: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und M_n ein Untermonoid von I_n , das $U_n \subseteq M_n$ erfüllt. Weiter seien $f_1, \dots, f_k \in H(G_n, M_n, U_n)$. Gilt dann $\llbracket C \rrbracket \in \mathbb{C}[f_1, \dots, f_k]$ für alle in M_n unzerlegbaren $C \in M_n$, so ist $\mathbb{C}[f_1, \dots, f_k] = H(G_n, M_n, U_n)$. $\diamond$

BEWEIS:

Zeige, dass $\llbracket C \rrbracket \in \mathbb{C}[f_1, \dots, f_k]$ für alle $C \in M_n$ gilt. Für $\llbracket E_n \rrbracket$ gilt dies nach Voraussetzung, da E_n unzerlegbar ist. Sei nun $C \in M_n$, und es sei bereits gezeigt, dass $\llbracket C' \rrbracket \in \mathbb{C}[f_1, \dots, f_k]$ für alle C' mit $\mathfrak{d}_n(C') \parallel \mathfrak{d}_n(C)$ gilt. Da $\llbracket C \rrbracket$ harmonisch zur Determinante $\mathfrak{d}_n(C)$ ist, gibt es nach dem letzten Lemma ein $k \in \mathbb{N}_0$ und $c_1, \dots, c_k \in \mathbb{C}$ sowie Matrizen $A_1, \dots, A_k, B_1, \dots, B_k \in M_n$ mit $\mathfrak{d}_n(A_i) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B_i) \parallel \mathfrak{d}_n(C)$ sowie $\mathfrak{d}_n(A_i B_i) = \mathfrak{d}_n(C)$ für alle $1 \leq i \leq k$, so dass der $\mathfrak{d}_n(C)$ -harmonische Teil von $f^* := \llbracket C \rrbracket + c_1 \llbracket A_1 \rrbracket * \llbracket B_1 \rrbracket + \dots + c_k \llbracket A_k \rrbracket * \llbracket B_k \rrbracket$ unzerlegbar ist. Da die $\llbracket A_i \rrbracket * \llbracket B_i \rrbracket$ nach 1.1.9 wegen $\mathfrak{d}_n(A_i B_i) = \mathfrak{d}_n(C)$ stets $\mathfrak{d}_n(C)$ -harmonisch sind und selbiges für $\llbracket C \rrbracket$ gilt, ist auch f^* als Linearkombination dieser Funktionen $\mathfrak{d}_n(C)$ -harmonisch. Zusammengefasst erhält man also, dass f^* unzerlegbar und damit eine Linearkombination von Funktionen der Form $\llbracket D \rrbracket$ für unzerlegbare $D \in M_n$ ist. Nach Voraussetzung ist jedes solche $\llbracket D \rrbracket$ ein Element von $\mathbb{C}[f_1, \dots, f_k]$, also gilt dies dann auch für f^* . Da nach Induktionsvoraussetzung wegen

$\mathfrak{d}_n(A_i) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B_i) \parallel \mathfrak{d}_n(C)$ auch $\llbracket A_i \rrbracket, \llbracket B_i \rrbracket \in \mathbb{C}[f_1, \dots, f_k]$ gilt, kann nun

$$\llbracket C \rrbracket = f^{*} - c_1 \llbracket A_1 \rrbracket * \llbracket B_1 \rrbracket - \dots - c_k \llbracket A_k \rrbracket * \llbracket B_k \rrbracket \in \mathbb{C}[f_1, \dots, f_k]$$

gefolgert werden. Da die $\llbracket C \rrbracket$ für $C \in M_n$ eine $\mathbb{C}$ -Vektorraum-Basis von $H(G_n, M_n, U_n)$ bilden, erhält man damit die Behauptung. $\square$

Das nächste Ziel ist nun, die Zerlegbarkeit von Matrizen durch einfachere Bedingungen zu charakterisieren, damit die Anwendung des gerade bewiesenen Satzes leichter möglich ist.

2.8.7 LEMMA: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und M_n ein Untermonoid von I_n mit $U_n \subseteq M_n$. Ein $C \in M_n$ ist genau dann zerlegbar, wenn es $A, B \in M_n$ gibt mit $\mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B) \parallel \mathfrak{d}_n(C)$ sowie $\mathfrak{d}_i(C) = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$. $\diamond$

BEWEIS:

Nach der Definition von Zerlegbarkeit und 1.1.9 genügt es, die Äquivalenz folgender Aussagen zu beweisen:

- (i) Es gilt $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) \neq 0$, und aus $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C') \neq 0$ folgt stets $C \leq C'$.
- (ii) Es gilt $\mathfrak{d}_i(C) = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$.

(ii) $\Rightarrow$ (i): Diese Richtung ist die Aussage von 2.8.2.

(i) $\Rightarrow$ (ii): Nach 2.6.4 und 2.8.2 existiert eine Matrix $C' \in M_n$, die $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C') \neq 0$ und $\mathfrak{d}_i(C') = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$ erfüllt. Demzufolge muss für jedes $C \in M_n$, das der Bedingung (i) genügt, $\mathfrak{d}_i(C) \mid \mathfrak{d}_i(C') = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$ gelten (wegen $C \leq C'$). Aus $(\llbracket A \rrbracket * \llbracket B \rrbracket)(C) \neq 0$ folgt mit 1.1.9 und 2.6.2 darüberhinaus $\mathfrak{d}_i(A)\mathfrak{d}_i(B) \mid \mathfrak{d}_i(C)$, also hat man insgesamt gezeigt, dass $\mathfrak{d}_i(A)\mathfrak{d}_i(B) \mid \mathfrak{d}_i(C) \mid \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ und damit $\mathfrak{d}_i(C) = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ für alle $1 \leq i \leq n$ gilt. $\square$

Das nachfolgende Lemma vereinfacht die Charakterisierung aus 2.8.7, indem die Existenz einer Zerlegung in Matrizen in eine Aussage über Ideale umformuliert wird.

2.8.8 LEMMA: Es seien die Bezeichnungen aus 2.7.1 übernommen, $n \in \mathbb{N}$ und $\mathfrak{T}$ eine multiplikativ abgeschlossene Menge von Hauptidealen von $\mathfrak{o}$ mit der Eigenschaft, dass für alle $\mathfrak{a}, \mathfrak{b} \in \mathfrak{T}$ mit $\mathfrak{a} \mid \mathfrak{b}$ auch $\mathfrak{b}\mathfrak{a}^{-1} \in \mathfrak{T}$ gilt. Setze $M_n = \{C \in I_n \mid \mathfrak{d}_n(C) \in \mathfrak{T}\}$. Für ein $C \in M_n$ sind dann äquivalent:

- (i) Die Matrix C ist in M_n zerlegbar.
- (ii) Es gibt Ideale $\mathfrak{c}_1, \dots, \mathfrak{c}_n$ in $\mathfrak{o}$ mit $\mathfrak{c}_i \mid \mathfrak{f}_i(C)$ für alle $1 \leq i \leq n$, so dass $\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \dots \mathfrak{c}_{n-1}^2 \mathfrak{c}_n \in \mathfrak{T} \setminus \{\mathfrak{o}, \mathfrak{d}_n(C)\}$ gilt. $\diamond$

BEWEIS:

(i) $\Rightarrow$ (ii): Sei C in M_n zerlegbar. Dann gibt es nach 2.8.7 $A, B \in M_n$ mit $\mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B) \parallel \mathfrak{d}_n(C)$ sowie $\mathfrak{d}_i(C) = \mathfrak{d}_i(A)\mathfrak{d}_i(B)$ (und damit auch $\mathfrak{e}_i(C) = \mathfrak{e}_i(A)\mathfrak{e}_i(B)$ und $\mathfrak{f}_i(C) = \mathfrak{f}_i(A)\mathfrak{f}_i(B)$) für alle $1 \leq i \leq n$. Definiere $\mathfrak{c}_i = \mathfrak{f}_i(A)$ für alle $1 \leq i \leq n$. Da Grundfaktoren nach 2.2.4 (g) hier stets Ideale in $\mathfrak{o}$ sind, hat man

$$\mathfrak{c}_i = \mathfrak{f}_i(A) \mid \mathfrak{f}_i(A)\mathfrak{f}_i(B) = \mathfrak{f}_i(C).$$

Weiter gilt dann

$$\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \dots \mathfrak{c}_{n-1}^2 \mathfrak{c}_n = \mathfrak{f}_1(A)^n \mathfrak{f}_2(A)^{n-1} \dots \mathfrak{f}_{n-1}(A)^2 \mathfrak{f}_n(A) \stackrel{2.2.4(d)}{=} \mathfrak{d}_n(A),$$

also ist dieses Produkt ein Hauptideal aus $\mathfrak{T}$. Da $\mathfrak{d}_n(A)\mathfrak{d}_n(B) = \mathfrak{d}_n(C)$ mit $\mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ und $\mathfrak{d}_n(B) \parallel \mathfrak{d}_n(C)$ gilt, muss $\mathfrak{o} \parallel \mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ und damit $\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \dots \mathfrak{c}_n \notin \{\mathfrak{o}, \mathfrak{d}_n(C)\}$ erfüllt sein.

(ii) $\Rightarrow$ (i): Seien $\mathfrak{c}_1, \dots, \mathfrak{c}_n$ gegeben, die die in (ii) geforderten Bedingungen erfüllen. Dann existiert nach 2.2.10 eine Matrix $A \in I_n$ mit $\mathfrak{f}_i(A) = \mathfrak{c}_i$ für alle $1 \leq i \leq n$. Setze nun $\mathfrak{c}'_i = \mathfrak{f}_i(C)\mathfrak{c}_i^{-1}$ für alle $1 \leq i \leq n$.

Dann sind die $\mathfrak{c}'_i$ wegen $\mathfrak{c}_i \mid f_i(C)$ Ideale in $\mathfrak{o}$. Weiter gilt

$$\begin{aligned} (\mathfrak{c}'_1)^n (\mathfrak{c}'_2)^{n-1} \cdots \mathfrak{c}'_n &= f_1(C)^n \mathfrak{c}_1^{-n} f_2(C)^{n-1} \mathfrak{c}_2^{-(n-1)} \cdots f_n(C) \mathfrak{c}_n^{-1} \\ &\stackrel{2.2.4(d)}{=} \mathfrak{d}_n(C) (\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \cdots \mathfrak{c}_n)^{-1}, \end{aligned}$$

was ein Hauptideal ist, da bereits $\mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \cdots \mathfrak{c}_n$ nach Voraussetzung ein Hauptideal ist. Gemäß 2.2.10 existiert daher eine Matrix $B \in I_n$ mit $f_i(B) = \mathfrak{c}'_i$ für alle $1 \leq i \leq n$.

Nach Konstruktion gilt nun $f_i(A)f_i(B) = f_i(C)$ und folglich auch $\mathfrak{e}_i(A)\mathfrak{e}_i(B) = \mathfrak{e}_i(C)$ und $\mathfrak{d}_i(A)\mathfrak{d}_i(B) = \mathfrak{d}_i(C)$ für alle $1 \leq i \leq n$. Darüberhinaus war $\mathfrak{d}_n(A) = \mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \cdots \mathfrak{c}_n$ ein Ideal aus $\mathfrak{T}$, ebenso $\mathfrak{d}_n(B) = \mathfrak{d}_n(C)\mathfrak{d}_n(A)^{-1}$ (nach Wahl von $\mathfrak{T}$, da $\mathfrak{d}_n(A) \mid \mathfrak{d}_n(C)$), also liegen A und B sogar in M_n . Wegen $\mathfrak{d}_n(A) = \mathfrak{c}_1^n \mathfrak{c}_2^{n-1} \cdots \mathfrak{c}_n \notin \{\mathfrak{o}, \mathfrak{d}_2(C)\}$ kann weder $\mathfrak{d}_n(A) = \mathfrak{d}_n(C)$ noch $\mathfrak{d}_n(B) = \mathfrak{d}_n(C)$ gelten, also gilt sowohl $\mathfrak{d}_n(A) \parallel \mathfrak{d}_n(C)$ als auch $\mathfrak{d}_n(B) \parallel \mathfrak{d}_n(C)$. Nach 2.8.7 ist damit die Zerlegbarkeit von C in M_n bewiesen. $\square$

Im letzten Teil dieses Abschnitts sollen nun die unzerlegbaren Matrizen für Primärkomponenten beschrieben werden. Dort kann die Bestimmung algorithmisiert werden.

2.8.9 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Übernehme die Bezeichnungen aus 2.7.1. Weiter sei $p \in \mathbb{N}$ eine Primzahl mit Primidealzerlegung

$$p\mathfrak{o} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_m^{v_m}$$

über $\mathfrak{o}$. Für jedes $n \in \mathbb{N}$ und $C \in I_{n,p}^*$ sowie $1 \leq i \leq n$ und $1 \leq j \leq m$ sei

$$V_{ji}(C) = v_{\mathfrak{p}_j}(f_i(C))$$

und $V_j(C) = (V_{j1}(C), \dots, V_{jn}(C))$. Für n -Tupel $b = (b_1, \dots, b_n) \in \mathbb{N}_0^n$ definiere $D(b) = nb_1 + (n-1)b_2 + \cdots + 2b_{n-1} + b_n$ (so dass nach 1.2.5 und 2.2.4 (d) insbesondere $D(V_j(C)) = v_{\mathfrak{p}_j}(\mathfrak{d}_n(C))$ für alle $1 \leq j \leq m$

gilt). Ist zusätzlich $b' = (b'_1, \dots, b'_n) \in \mathbb{N}_0^n$, so schreibe $b' \leq b$, falls $b'_i \leq b_i$ für alle $1 \leq i \leq n$ gilt, und $b' < b$, falls $b' \leq b$ und $b' \neq b$ gilt. Weiter definiere

$$L(b) = \{D(b') \mid b' \in \mathbb{N}_0^n, b' \leq b\}.$$

Sind $b_1, \dots, b_n$ Ideale in $\mathfrak{o}$, die die entsprechende Bedingung aus 2.2.5 erfüllen, so setze $[b_1, \dots, b_n] = [C]$ für eine beliebige Matrix $C \in I_n$, die $e_i(C) = b_i$ für alle $1 \leq i \leq n$ erfüllt, weiter setze $\llbracket b_1, \dots, b_n \rrbracket = \llbracket C \rrbracket$. Anstelle von $a\mathfrak{o}$ für ein $a \in \mathfrak{o}$ wird in dieser Schreibweise auch einfach a verwendet. $\diamond$

Mit diesen Bezeichnungen kann man nun eine Charakterisierung der Zerlegbarkeit durch eine rein kombinatorische Bedingung formulieren.

2.8.10 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen. Weiter seien $n, k \in \mathbb{N}$ und $C \in I_{n,p}^*$ mit $\mathfrak{o}_n(C) = p^k \mathfrak{o}$. Dann sind äquivalent:

- (i) C ist in $I_{n,p}^*$ zerlegbar.
- (ii) Es gibt ein $1 \leq l < k$, so dass $lv_j \in L(V_j(C))$ für alle $1 \leq j \leq m$ gilt. $\diamond$

BEWEIS:

Man erhält $I_{n,p}^*$ mit der Konstruktion für M_n aus 2.8.8, indem man $\mathfrak{T} = \{p^l \mathfrak{o} \mid l \in \mathbb{N}_0\}$ setzt. Nach 2.8.8 genügt es daher, die Äquivalenz folgender Aussagen zu zeigen:

- (i') Es gibt ein $1 \leq l < k$ und Ideale $c_1, \dots, c_n$ in $\mathfrak{o}$ mit $c_i \mid f_i(C)$ für alle $1 \leq i \leq n$, so dass $c_1^n c_2^{n-1} \dots c_{n-1}^2 c_n = p^l$ gilt.
- (ii) Es gibt ein $1 \leq l < k$, so dass $lv_j \in L(V_j(C))$ für alle $1 \leq j \leq m$ gilt.

(i') $\Rightarrow$ (ii): Ist (i') erfüllt, so definiere $b_{ji} = v_{p_j}(c_i)$ und $b_j = (b_{j1}, \dots, b_{jn})$ für alle $1 \leq i \leq n$ und $1 \leq j \leq m$. Wegen $c_i \mid f_i(C)$ für alle $1 \leq i \leq n$ gilt $b_j \leq V_j(C)$ für alle $1 \leq j \leq m$ (1.2.5). Nach Definition folgt $D(b_j) \in L(V_j(C))$ für alle $1 \leq j \leq m$. Nun ist

$$\begin{aligned} D(b_j) &= nb_{j1} + (n-1)b_{j2} + \dots + b_{jn} \\ &= nv_{p_j}(c_1) + (n-1)v_{p_j}(c_2) + \dots + v_{p_j}(c_n) \\ &\stackrel{1.2.5}{=} v_{p_j}(c_1^n c_2^{n-1} \dots c_n) = v_{p_j}(p^l) = lv_j \end{aligned}$$

für alle $1 \leq j \leq m$, was (ii) beweist.

(ii) $\Rightarrow$ (i'): Ist nun (ii) erfüllt, so gibt es für jedes $1 \leq j \leq m$ ein $b_j = (b_{j1}, \dots, b_{jn}) \in \mathbb{N}_0^n$ mit $b_j \leq V_j(C)$ und $D(b_j) = lv_j$. Definiere

$$c_i = p_1^{b_{1i}} \dots p_m^{b_{mi}}$$

für alle $1 \leq i \leq n$. Dann gilt $c_i \mid f_i(C)$ für alle $1 \leq i \leq n$, denn für alle $1 \leq j \leq m$ ist

$$v_{p_j}(c_i) = b_{ji} \leq V_{ji}(C) = v_{p_j}(f_i(C)).$$

Weiter ist

$$\begin{aligned} c_1^n c_2^{n-1} \dots c_n &= (p_1^{b_{11}} \dots p_m^{b_{m1}})^n (p_1^{b_{12}} \dots p_m^{b_{m2}})^{n-1} \dots (p_1^{b_{1n}} \dots p_m^{b_{mn}}) \\ &= p_1^{nb_{11} + (n-1)b_{12} + \dots + b_{1n}} \dots p_m^{nb_{m1} + (n-1)b_{m2} + \dots + b_{mn}} \\ &= p_1^{D(b_1)} \dots p_m^{D(b_m)} = p_1^{lv_1} \dots p_m^{lv_m} = p^l o, \end{aligned}$$

was nun (i') beweist. □

Die Bedingung (ii) von 2.8.10 kann dabei als rein kombinatorische Bedingung aufgefasst werden, da nach Bestimmung der $V_j(C)$ alle weiteren Berechnungen in $\mathbb{N}_0$ stattfinden.

In den zwei Spezialfällen $m = 1$ und $v_1 = 1$ beziehungsweise $m = 1$ und $v_1 = 2$ lassen sich die unzerlegbaren Matrizen der Primärkomponente für beliebiges n in einfacher geschlossener Form angeben.

2.8.11 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen mit $m = 1$ und $v_1 = 1$. Weiter sei $n \in \mathbb{N}$ und $C \in I_{n,p}^*$. Dann sind äquivalent:

- (i) C ist unzerlegbar.
- (ii) Es gilt $[C] = [1, \dots, 1, p, \dots, p]$, wobei die Anzahl der p im zwischen 0 und n (jeweils einschließlich) liegt. $\diamond$

BEWEIS:

Sei $C \in I_{n,p}^*$ und $b = (b_1, \dots, b_n) = V_1(C)$. Die Zerlegbarkeit von C ist nach 2.8.10 äquivalent zur Existenz eines $l \in \mathbb{N}$ mit

$$l < v_{p_1}(\partial_n(C)) = nb_1 + (n-1)b_2 + \dots + b_n \quad \text{und} \quad l \in L(V_1(C)),$$

was nach Definition von $L(V_1(C))$ wiederum äquivalent zur Existenz eines $a \in \mathbb{N}_0^n$ mit $a \leq b$ und $1 \leq D(a) < nb_1 + (n-1)b_2 + \dots + b_n$ ist. Fasst man die letzten beiden Bedingungen zusammen, erhält man als äquivalente Bedingung für die Zerlegbarkeit von C die Existenz eines $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$.

1. Fall: $b_1 = \dots = b_n = 0$, also $[C] = [1, \dots, 1]$. Dann kann es kein $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ geben, also ist C unzerlegbar.
2. Fall: Es gibt ein i mit $b_i = 1$ und $b_j = 0$ für alle $j \neq i$, es ist also $[C] = [1, \dots, 1, p, p, \dots, p]$. Da es auch hier kein $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ gibt, kann C nicht zerlegbar sein.
3. Fall: Es gibt ein i mit $b_i \geq 2$. In diesem Fall gibt es ein $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$, also ist dann C zerlegbar.
4. Fall: Es gibt $i \neq j$ mit $b_i \geq 1$ und $b_j \geq 1$. Mit der gleichen Begründung wie im dritten Fall ist C zerlegbar. $\square$

Den Fall $m = 1$ und $v_1 = 2$ behandelt man analog.

2.8.12 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen mit $m = 1$ und $v_1 = 2$. Dann sind die $[C]$ für unzerlegbare $C \in I_{n,p}^*$ genau diejenigen von einer der folgenden Formen:

- (i) $[1, \dots, 1, p, p, \dots, p]$, wobei die Anzahl der p gerade ist,
- (ii) $[1, \dots, 1, p, p, \dots, p, p^2, p^2, \dots, p^2]$, wobei die Anzahl der p gerade und die Anzahl der p^2 ungerade ist. $\diamond$

BEWEIS:

Sei $C \in I_{n,p}^*$ und $b = (b_1, \dots, b_n) = V_1(C)$. Weiter sei $k \in \mathbb{N}_0$ mit $\vartheta_n(C) = p^k o$ gewählt. Dann gilt

$$k = \frac{1}{2} v_{p_1}(\vartheta_n(C)) = \frac{1}{2} (nb_1 + (n-1)b_2 + \dots + b_n),$$

also ist insbesondere $D(b) = nb_1 + (n-1)b_2 + \dots + b_n$ eine gerade Zahl.

Die Zerlegbarkeit von C ist nach 2.8.10 äquivalent zur Existenz eines $1 \leq l < k$ mit $2l \in L(V_1(C))$, was nach Definition von $L(V_1(C))$ gleichbedeutend mit der Existenz eines $a \in \mathbb{N}_0^n$ mit $a \leq b$ und $D(a)$ gerade sowie $1 \leq \frac{1}{2}D(a) < k$ ist. Wegen $D(b) = 2k$ erhält man als weitere äquivalente Umformulierung die Existenz eines $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ und geradem $D(a)$.

Fall 1: Alle Einträge von b sind gleich Null. Dann gilt $[C] = [1, \dots, 1]$ (Fall (i)). Da es kein $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ gibt, ist C unzerlegbar.

Fall 2: Genau ein Eintrag von b ist von Null verschieden.

Fall 2.1: Der von Null verschiedene Eintrag von b ist gleich 1. Sei $1 \leq i \leq n$ mit $b_i = 1$. Dann muss $n - i + 1$ eine gerade Zahl sein, sonst hätte man einen Widerspruch zur Vorüberlegung, wo gezeigt wurde, dass $D(b)$ gerade ist. Es folgt nun $[C] = [1, \dots, 1, p, p, \dots, p]$, wobei die Anzahl der p gleich $n - i + 1$, also gerade ist (Fall (i)). Da es hier kein

$a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ gibt, kann ein solches C nicht zerlegbar sein.

Fall 2.2: Der von Null verschiedene Eintrag von b ist gleich 2.

Fall 2.2.1: Für das i mit $b_i = 2$ ist $n - i + 1$ ungerade. Dann ist also $[C] = [1, \dots, 1, p^2, p^2, \dots, p^2]$, wobei die Anzahl der p^2 ungerade ist (Fall (ii)). Für die Wahl eines $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ gibt es nur die Möglichkeit $a = (a_1, \dots, a_n)$ mit $a_i = 1$ und $a_j = 0$ für $j \neq i$. Dann aber ist $D(a) = n - i + 1$ ungerade, so dass man auch hier keine Zerlegung hat.

Fall 2.2.2: Für das i mit $b_i = 2$ ist $n - i + 1$ gerade. Dann ist also $[C] = [1, \dots, 1, p^2, p^2, \dots, p^2]$, wobei die Anzahl der p^2 gerade ist. Hier hat man eine Zerlegung, denn man kann $a = (a_1, \dots, a_n)$ mit $a_i = 1$ und $a_j = 0$ für $j \neq i$ wählen und hat dann $(0, \dots, 0) < a < b$ und $D(a) = n - i + 1$ gerade.

Fall 2.3: Der von Null verschiedene Eintrag von b ist größer als 2. Auch hier ist $[C]$ nicht von der Form (i) oder (ii). Sei $1 \leq i \leq n$ mit $b_i \geq 3$. Dann hat man eine Zerlegung, denn man kann $a = (a_1, \dots, a_n)$ mit $a_i = 2$ und $a_j = 0$ für $j \neq i$ wählen und hat dann $(0, \dots, 0) < a < b$ und $D(a) = 2(n - i + 1)$ gerade.

Fall 3: Genau zwei Einträge von b sind von Null verschieden.

Fall 3.1: Die von 0 verschiedenen Einträge von b sind beide gleich 1.

Fall 3.1.1: Für $r, s \in \mathbb{N}$ mit $r < s$ und $b_r = b_s = 1$ sind $n - r + 1$ und $n - s + 1$ ungerade. Dann ist $[C] = [1, \dots, 1, p, p, \dots, p, p^2, p^2, \dots, p^2]$, wobei die Anzahl der p gleich $s - r$ und damit gerade ist; die Anzahl der p^2 ist gleich $n - s + 1$ und damit ungerade (Fall (ii)). Hier ist C unzerlegbar, denn die einzigen $a \in \mathbb{N}_0^n$ mit $(0, \dots, 0) < a < b$ erfüllen $D(a) \in \{n - r + 1, n - s + 1\}$ und sind somit ungerade.

Fall 3.1.2: Für $r, s \in \mathbb{N}$ mit $r < s$ und $b_r = b_s = 1$ ist $n - r + 1$ oder $n - s + 1$ gerade. Dann ist $[C] = [1, \dots, 1, p, p, \dots, p, p^2, p^2, \dots, p^2]$, wobei die Anzahl der p^2 gerade ist (falls $n - s + 1$ gerade ist) oder

die Anzahl der p ungerade ist (falls $n - s + 1$ ungerade und folglich $n - r + 1$ gerade ist). In diesem Fall hat man eine Zerlegung, denn für $a = (a_1, \dots, a_n)$ wählt man entweder $a_r = 1$ und $a_j = 0$ für alle $j \neq r$ (im Falle, dass $n - r + 1$ gerade ist) oder $a_s = 1$ und $a_j = 0$ für alle $j \neq s$ (im Falle, dass $n - s + 1$ gerade ist); dann ist $(0, \dots, 0) < a < b$ und $D(a)$ gerade.

Fall 3.2: Von den beiden von Null verschiedenen Einträgen von b ist einer größer als 1. Hier ist $[C]$ nicht von der Form (i) oder (ii). In diesem Fall hat man eine Zerlegung: Sei $1 \leq i \leq n$ mit $b_i \geq 2$. Wählt man $a = (a_1, \dots, a_n)$ mit $a_i = 2$ und $a_j = 0$ für $j \neq i$, so gilt $(0, \dots, 0) < a < b$, und $D(a) = 2(n - i + 1)$ ist gerade.

Fall 4: Mindestens drei Einträge von b sind von Null verschieden. Auch hier ist $[C]$ nicht von der Form (i) oder (ii). Seien $r, s, t \in \mathbb{N}$ paarweise verschieden mit $b_r, b_s, b_t \geq 1$. Von den Zahlen $n - r + 1$ und $n - s + 1$ sowie $n - t + 1$ sind entweder mindestens zwei gerade oder mindestens zwei ungerade. In beiden Fällen seien dies ohne Beschränkung der Allgemeinheit $n - r + 1$ und $n - s + 1$. Definiere $a = (a_1, \dots, a_n)$ durch $a_r = 1$ und $a_s = 1$ sowie $a_j = 0$ für alle $j \notin \{r, s\}$. Dann hat man $(0, \dots, 0) < a < b$ mit $D(a) = (n - r + 1) + (n - s + 1)$ gerade als Summe entweder zweier ungerader oder zweier gerader Zahlen. Daher ist C zerlegbar. $\square$

Anstatt für eine feste Primidealzerlegung von $p\mathfrak{o}$ die unzerlegbaren Matrizen für alle $n \in \mathbb{N}$ zu bestimmen, kann man auch versuchen, für festes n die unzerlegbaren Matrizen für alle Primidealzerlegungen zu beschreiben.

2.8.13 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen und $C \in I_{2,p}^*$. Ist $\mathfrak{d}_2(C) = \mathfrak{o}$ oder $\mathfrak{d}_2(C) = p\mathfrak{o}$, so ist C unzerlegbar. Gilt hingegen $p^3 \mid \mathfrak{d}_2(C)$, so ist C zerlegbar. Im verbleibenden Fall $\mathfrak{d}_2(C) = p^2\mathfrak{o}$ ist C genau dann unzerlegbar, wenn ein $1 \leq j \leq m$ existiert, für das v_j ungerade ist und $V_{j1}(C) = v_j$ gilt

(äquivalent: C ist genau dann zerlegbar, wenn $V_{j1}(C) \leq 2\lfloor \frac{v_j}{2} \rfloor$ für alle $1 \leq j \leq m$ gilt). $\diamond$

BEWEIS:

Sei $k \in \mathbb{N}_0$ mit $\mathfrak{d}_2(C) = p^k \mathfrak{o}$. Die Zerlegbarkeit von C ist nach 2.8.10 äquivalent zur Existenz eines $1 \leq l < k$ mit $lv_j \in L(V_j(C))$ für alle $1 \leq j \leq m$. Ist $k = 0$ oder $k = 1$, so kann C also nicht zerlegbar sein. Betrachte nun den Fall $k \geq 3$. Zum Nachweis der Zerlegbarkeit von C zeige, dass für $1 \leq j \leq m$ stets $2v_j \in L(V_j(C))$ gilt. Sei $1 \leq j \leq m$. Wähle $a = (a_1, a_2)$ mit

$$a_2 = 2 \min \left\{ v_j, \left\lfloor \frac{V_{j2}(C)}{2} \right\rfloor \right\}, \quad a_1 = v_j - \frac{1}{2}a_2.$$

Dann sind a_1 und a_2 ganzzahlig, und es gilt $0 \leq a_2 \leq 2v_j$. Weiter folgt $a_1 = v_j - \frac{1}{2}a_2 \geq 0$, also insgesamt $a \in \mathbb{N}_0^2$. Nach Wahl von a_2 gilt $a_2 \leq V_{j2}(C)$. Ist $a_2 = 2v_j$, so gilt

$$a_1 = v_j - \frac{1}{2}a_2 = 0 \leq V_{j1}(C).$$

Andernfalls ist

$$a_2 = 2 \left\lfloor \frac{V_{j2}(C)}{2} \right\rfloor \geq V_{j2}(C) - 1,$$

und mit $2V_{j1}(C) + V_{j2}(C) = \mathfrak{v}_{p_j}(\mathfrak{d}_2(C)) = kv_j$ folgt

$$\begin{aligned} a_1 &= v_j - \frac{1}{2}a_2 \leq v_j - \frac{1}{2}(V_{j2}(C) - 1) = v_j - \frac{1}{2}(kv_j - 2V_{j1}(C) - 1) \\ &= v_j(1 - \frac{1}{2}k) + V_{j1}(C) + \frac{1}{2} \stackrel{k \geq 3}{\leq} -\frac{1}{2}v_j + V_{j1}(C) + \frac{1}{2} \stackrel{v_j \geq 1}{\leq} V_{j1}(C), \end{aligned}$$

so dass man insgesamt $a \leq V_j(C)$ erhält. Daher ist $D(a) \in L(V_j(C))$, und mit $D(a) = 2a_1 + a_2 = 2v_j$ folgt die hier zu zeigende Aussage.

Untersuche nun den verbleibenden Fall, sei also $k = 2$. Dann gilt $2V_{j1}(C) + V_{j2}(C) = \mathfrak{v}_{p_j}(\mathfrak{d}_2(C)) = 2v_j$, also hat man $V_{j1}(C) \leq v_j$ für alle $1 \leq j \leq m$. Betrachte zunächst den Unterfall, dass es kein $1 \leq j \leq m$ gibt mit v_j ungerade und $V_{j1}(C) = v_j$. Zeige die Zerlegbarkeit von C

durch Nachweis von $v_j \in L(V_j(C))$ für alle $1 \leq j \leq m$. Sei $1 \leq j \leq m$. Setze $a = (a_1, a_2)$ mit

$$a_1 = \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor, \quad a_2 = v_j - 2a_1.$$

Dann sind a_1 und a_2 ganzzahlig, und es gilt $0 \leq a_1 \leq V_{j1}(C)$. Weiter ist

$$a_2 = v_j - 2 \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor \geq 0$$

wegen $V_{j1}(C) \leq v_j$, und es gilt

$$\begin{aligned} a_2 &= v_j - 2 \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor = \frac{1}{2}(2V_{j1}(C) + V_{j2}(C)) - 2 \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor \\ &= V_{j1}(C) - 2 \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor + \frac{1}{2}V_{j2}(C); \end{aligned}$$

ist $V_{j1}(C)$ gerade, so folgt aus dieser Rechnung $a_2 = \frac{1}{2}V_{j2}(C) \leq V_{j2}(C)$, ist $V_{j1}(C)$ ungerade, so muss in diesem Unterfall $V_{j1}(C) < v_j$ gelten, und es folgt $V_{j2}(C) = 2v_j - 2V_{j1}(C) \geq 2$, also

$$\begin{aligned} V_{j1}(C) - 2 \left\lfloor \frac{V_{j1}(C)}{2} \right\rfloor + \frac{1}{2}V_{j2}(C) &= 1 + \frac{1}{2}V_{j2}(C) = \frac{1}{2}(V_{j2}(C) + 2) \\ &\leq \frac{1}{2}(2V_{j2}(C)) = V_{j2}(C). \end{aligned}$$

Insgesamt erhält man also $a \in \mathbb{N}_0^n$ mit $a \leq V_j(C)$. Darüberhinaus gilt $D(a) = 2a_1 + a_2 = v_j$, so dass $v_j \in L(V_j(C))$ folgt, was die Untersuchung dieses Unterfalls abschließt. Nun gebe es ein $1 \leq j \leq m$ mit v_j ungerade und $V_{j1}(C) = v_j$. Zeige die Unzerlegbarkeit von C durch den Nachweis der Tatsache, dass es kein $a \leq V_j(C)$ mit $D(a) = v_j$ gibt. Sei $a = (a_1, a_2)$ mit $a \leq V_j(C)$. Aus $V_{j1}(C) = v_j$ folgt mit $2V_{j1}(C) + V_{j2}(C) = 2v_j$, dass $V_{j2}(C) = 0$ gilt. Es folgt $a_2 = 0$ nach Wahl von a . Dann ist $D(a) = 2a_1 + a_2 = 2a_1$ gerade, kann also nicht gleich v_j sein. Dies schließt den Beweis ab. $\square$

Im allgemeinen Fall gestaltet sich eine geschlossene Beschreibung der unzerlegbaren Matrizen sehr viel komplexer. Daher wird hier darauf verzichtet; stattdessen sollen im folgenden obere Schranken für die Determinanten unzerlegbarer Matrizen hergeleitet werden, die es ermöglichen, alle unzerlegbaren Matrizen in $I_{n,p}^*$ durch Überprüfung endlich vieler Fälle zu bestimmen.

2.8.14 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen, $n \in \mathbb{N}$ mit $n \geq 2$ und $C \in I_{n,p}^*$ so, dass $p^{nk} \mid \mathfrak{d}_n(C)$ gilt, wobei k das kleinste gemeinsame Vielfache der Zahlen $1, \dots, n$ bezeichnet. Dann ist C in $I_{n,p}^*$ zerlegbar. $\diamond$

BEWEIS:

Sei $1 \leq j \leq m$. Wegen $p^{nk} \mid \mathfrak{d}_n(C)$ gilt

$$nk v_j = v_{p_j}(p^{nk}) \leq v_{p_j}(\mathfrak{d}_n(C)) = D(V_j(C)) = \sum_{i=1}^n (n-i+1) V_{ji}(C).$$

Einer der n Summanden muss mindestens gleich kv_j sein, da sonst die Ungleichung nicht gelten würde. Es existiert also ein $1 \leq i \leq n$ mit $(n-i+1)V_{ji}(C) \geq kv_j$. Setzt man nun $a = (a_1, \dots, a_n)$ mit

$$a_r = \begin{cases} \frac{kv_j}{n-i+1}, & \text{falls } r = i, \\ 0 & \text{sonst,} \end{cases}$$

so ist $\frac{kv_j}{n-i+1} \in \mathbb{N}$ wegen $n-i+1 \in \{1, \dots, n\}$, da k das kleinste gemeinsame Vielfache von $1, \dots, n$ ist. Weiter gilt mit dieser Wahl $a \leq V_j(C)$. Insgesamt folgt damit $D(a) \in L(V_j(C))$. Wegen

$$D(a) = (n-i+1) \frac{kv_j}{n-i+1} = kv_j$$

folgt nun mit 2.8.10 die Behauptung wegen $1 \leq k < nk$. $\square$

Diese Schranke genügt für die Folgerung, dass jede Primärkomponente von $H(G_n, I_n^*, U_n)$ ein endliches Erzeugendensystem hat (Anwendung von 2.8.6). Für praktische Zwecke zur expliziten Bestimmung

aller unzerlegbaren Matrizen ist diese Aussage aus Komplexitätsgründen jedoch nicht gut geeignet. Mit weiteren Hilfsaussagen lässt sich die Schranke jedoch so weit drücken, dass man computergestützt für mehrere nichttriviale Fälle die jeweilige maximale p -Potenz von $\mathfrak{d}_n(C)$ für unzerlegbare $C \in I_{n,p}^*$ berechnen kann.

2.8.15 BEISPIEL: Es seien die Bezeichnungen aus 2.8.9 übernommen. Berechne nun für einige Fälle

$$\max\{k \in \mathbb{N}_0 \mid \text{Es gibt ein unzerlegbares } C \in I_{n,p}^* \text{ mit } \mathfrak{d}_n(C) = p^k \mathfrak{o}\}.$$

Der folgenden Tabelle kann man diese Werte in Abhängigkeit von n und der Primidealzerlegung (PIZ) von p entnehmen.

PIZ	$n = 2$	$n = 3$	$n = 4$	$n = 5$
$\mathfrak{p}_1$	2	3	4	5
$\mathfrak{p}_1^2$	1	3	3	5
$\mathfrak{p}_1 \mathfrak{p}_2$	2	6	12	20
$\mathfrak{p}_1^3$	2	2	4	
$\mathfrak{p}_1^2 \mathfrak{p}_2$	2	6	12	
$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$	2	6	12	
$\mathfrak{p}_1^4$	1	3	3	
$\mathfrak{p}_1^3 \mathfrak{p}_2$	2	6	12	
$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	1	3	6	
$\mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3$	2	6	12	
$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4$	2	6	12	

◇

Durch systematisches Durchprobieren aller Möglichkeiten kann man nun jeweils alle unzerlegbaren Matrizen bestimmen.

2.8.16 BEISPIEL: Es seien die Bezeichnungen aus 2.8.9 übernommen. Berechne für einige Spezialfälle alle unzerlegbare Matrizen in $I_{n,p}^*$.

n	PIZ	Klassen unzerlegbarer Matrizen
2	p_1	$[1, 1], [1, p_1], [p_1, p_1]$
2	p_1^2	$[1, 1], [1, p_1^2], [p_1, p_1]$
2	$p_1 p_2$	$[1, 1], [1, p_1 p_2], [p_1, p_1 p_2^2], [p_2, p_1^2 p_2], [p_1 p_2, p_1 p_2]$
2	p_1^3	$[1, 1], [1, p_1^3], [p_1, p_1^2], [p_1^3, p_1^3]$
2	$p_1^2 p_2$	$[1, 1], [1, p_1^2 p_2], [p_1, p_1 p_2], [p_2, p_1^4 p_2], [p_1 p_2, p_1^3 p_2], [p_1^2 p_2, p_1^2 p_2]$
2	$p_1 p_2 p_3$	$[1, 1], [1, p_1 p_2 p_3], [p_1, p_1 p_2^2 p_3^2], [p_2, p_1^2 p_2 p_3^2], [p_1 p_2, p_1 p_2 p_3^2], [p_3, p_1^2 p_2^2 p_3], [p_1 p_3, p_1 p_2^2 p_3], [p_2 p_3, p_1^2 p_2 p_3], [p_1 p_2 p_3, p_1 p_2 p_3]$
2	p_1^4	$[1, 1], [1, p_1^4], [p_1, p_1^3], [p_1^2, p_1^2]$

n	PIZ	Klassen unzerlegbarer Matrizen
3	p_1	$[1, 1, 1], [1, 1, p_1], [1, p_1, p_1], [p_1, p_1, p_1]$
3	p_1^2	$[1, 1, 1], [1, 1, p_1^2], [1, p_1, p_1], [p_1, p_1, p_1^2], [p_1^2, p_1^2, p_1^2]$
3	$p_1 p_2$	$[1, 1, 1], [1, 1, p_1 p_2], [1, p_1, p_1 p_2^2], [1, p_2, p_1^2 p_2], [1, p_1 p_2, p_1 p_2], [p_1, p_1, p_1 p_2^3], [p_2, p_2, p_1^3 p_2], [p_1 p_2, p_1 p_2, p_1 p_2], [p_2, p_1 p_2, p_1^2 p_2], [p_1, p_1 p_2, p_1 p_2^2], [p_2, p_1^2 p_2, p_1^2 p_2^2], [p_1, p_1 p_2^2, p_1^2 p_2^2], [p_2^2, p_1^3 p_2^2, p_1^3 p_2^2], [p_1^2, p_1^2 p_2^3, p_1^2 p_2^3]$
3	p_1^3	$[1, 1, 1], [1, 1, p_1^3], [1, p_1, p_1^2], [p_1, p_1, p_1], [1, p_1^3, p_1^3]$

n	PIZ	Klassen unzerlegbarer Matrizen
4	p_1	$[1, 1, 1, 1], [1, 1, 1, p_1], [1, 1, p_1, p_1], [1, p_1, p_1, p_1], [p_1, p_1, p_1, p_1]$
4	p_1^2	$[1, 1, 1, 1], [1, 1, 1, p_1^2], [1, 1, p_1, p_1], [1, p_1, p_1, p_1^2], [p_1, p_1, p_1, p_1], [1, p_1^2, p_1^2, p_1^2]$

◇

§ 2.9

MINIMALE ERZEUGENDENSYSTEME

Nachdem im letzten Abschnitt unzerlegbare Matrizen bestimmt wurden, stellt sich nun die Frage, ob die daraus gemäß 2.8.6 ableitbaren Erzeugendensysteme der Form $\{\llbracket C \rrbracket \mid C \in I_{n,p}^* \text{ unzerlegbar}\} \setminus \{\llbracket 1, 1 \rrbracket\}$ von Primärkomponenten minimal sind.

Im Falle $n = 2$ lässt sich eine nicht zu komplizierte untere Schranke für die Mächtigkeit von Erzeugendensystemen von Primärkomponenten angeben.

2.9.1 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen. Setze

$$d = \prod_{i=1}^m (v_i + 1) \quad \text{und} \quad r = \prod_{i=1}^m \left(\left\lceil \frac{v_i}{2} \right\rceil + 1 \right).$$

Dann besteht jedes Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$ als $\mathbb{C}$ -Algebra aus mindestens $\max\{r, d - \binom{r}{2}\}$ Elementen. $\diamond$

BEWEIS:

Allgemein gilt: Ist $\{f_1, \dots, f_k\}$ ein Erzeugendensystem einer $\mathbb{C}$ -Algebra und $F \in \mathbb{C}[X_2, \dots, X_k]$, so ist auch $\{f_1 + F(f_2, \dots, f_k), f_2, \dots, f_k\}$ ein Erzeugendensystem derselben Algebra, denn für alle Polynome $G \in \mathbb{C}[X_1, \dots, X_k]$ ist auch

$$H = G(X_1 - F(X_2, \dots, X_k), X_2, \dots, X_k)$$

ein Polynom, und es gilt

$$H(f_1 + F(f_2, \dots, f_k), f_2, \dots, f_k) = G(f_1, \dots, f_k).$$

Sei nun $\{f_1, \dots, f_k\}$ ein Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$ als $\mathbb{C}$ -Algebra. Dann ist auch $\{f_1, \dots, f_k, \llbracket 1, 1 \rrbracket\}$ ein Erzeugendensystem, und

mit den im letzten Absatz beschriebenen Transformationen kann man ein Erzeugendensystem der Form $\{g_1, \dots, g_k, \llbracket 1, 1 \rrbracket\}$ erhalten, bei dem für $1 \leq i \leq n$ stets $g_i = f_i - f_i(E_2)\llbracket 1, 1 \rrbracket$, also insbesondere $g_i(E_2) = 0$ gilt. Wegen $g_1^0 = \llbracket 1, 1 \rrbracket$ kann man $\llbracket 1, 1 \rrbracket$ aus obigem Erzeugendensystem streichen, so dass man $\{g_1, \dots, g_k\}$ als Erzeugendensystem der Hecke-Algebra erhält.

Setze

$$M_1 = \{C \in I_{2,p}^* \mid \mathfrak{d}_2(C) = p\mathfrak{o}\}$$

und

$$H_1 = \{f|_{M_1} \mid f \in H(G_2, I_{2,p}^*, U_2)\}.$$

Mit 2.2.4 (f) und 2.2.5 folgt, dass die Menge $\{\llbracket a, pa^{-1} \rrbracket|_{M_1} \mid a^2 \text{ teilt } p\}$ eine Basis von H_1 ist. Nun gilt $a^2 \mid p$ genau dann, wenn in der Primidealzerlegung von a jeder Exponent eines Primideals höchstens halb so groß ist wie der entsprechende Exponent in der Primidealzerlegung von p . Demnach besteht diese Basis aus genau $(\lfloor \frac{v_1}{2} \rfloor + 1) \cdots (\lfloor \frac{v_m}{2} \rfloor + 1)$ Elementen. Die Dimension von H_1 als $\mathbb{C}$ -Vektorraum ist also gleich r . Da $\{g_1, \dots, g_k\}$ ein Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$ als $\mathbb{C}$ -Algebra ist, erzeugen die Monome $g_1^{v_1} * \cdots * g_k^{v_k}$ mit $v_1, \dots, v_k \in \mathbb{N}_0$ diese Menge als $\mathbb{C}$ -Vektorraum. Folglich ist H_1 das $\mathbb{C}$ -Vektorraum-Erzeugnis der $g_1^{v_1} * \cdots * g_k^{v_k}|_{M_1}$ mit $v_1, \dots, v_k \in \mathbb{N}_0$. Da für alle $1 \leq i \leq k$ nach Konstruktion aus $g_i(C) \neq 0$ stets $p \mid \det C$ folgt, muss $(g_i * g_j)(C) \neq 0$ für beliebige $1 \leq i, j \leq k$ stets $p^2 \mid \det C$ implizieren (1.1.9), also ist $g_i * g_j|_{M_1} = 0$ für alle diese i, j . Daher ist H_1 bereits das $\mathbb{C}$ -Vektorraum-Erzeugnis von $g_1|_{M_1}, \dots, g_k|_{M_1}$. Indem man gegebenenfalls umsortiert, kann man ohne Beschränkung der Allgemeinheit annehmen, dass $\{g_1|_{M_1}, \dots, g_r|_{M_1}\}$ eine Basis von H_1 ist, da dieser Vektorraum die Dimension r hat. Es folgt nun insbesondere $k \geq r$, was bereits einen Teil der Behauptung beweist. Durch Addition geeigneter Vielfache der $g_1, \dots, g_r$ zu $g_{r+1}, \dots, g_k$ kann man ein Erzeugendensystem $\{g_1, \dots, g_r, h_{r+1}, \dots, h_k\}$ von $H(G_2, I_{2,p}^*, U_2)$ als $\mathbb{C}$ -Algebra erhalten, für das $h_i(C) \neq 0$ für $r < i \leq k$ stets $p^2 \mid \det C$ impliziert.

Setze nun

$$M_2 = \{C \in I_{2,p}^* \mid \mathfrak{d}_2(C) = p\mathfrak{o} \text{ oder } \mathfrak{d}_2(C) = p^2\mathfrak{o}\}$$

und

$$H_2 = \{f|_{M_2} \mid f \in H(G_2, I_{2,p}^*, U_2)\}.$$

Die Menge $\{\llbracket \mathfrak{a}, pa^{-1} \rrbracket|_{M_2} \mid \mathfrak{a}^2 \text{ teilt } p\} \cup \{\llbracket \mathfrak{b}, p^2\mathfrak{b}^{-1} \rrbracket|_{M_2} \mid \mathfrak{b}^2 \text{ teilt } p^2\}$ ist eine Basis von H_2 (nach 2.2.4 (f) und 2.2.5). Es wurde bereits gezeigt, dass die Bedingung $\mathfrak{a}^2 \mid p$ von genau r verschiedenen ganzen Idealen erfüllt wird; weiter gilt $\mathfrak{b}^2 \mid p^2$ genau dann, wenn in der Primidealzerlegung von $\mathfrak{b}$ jeder Exponent eines Primideals höchstens so groß ist wie der entsprechende Exponent in der Primidealzerlegung von p . Demnach enthält diese Basis genau $r + (v_1 + 1) \cdots (v_m + 1)$ Elemente. Die Dimension von H_2 als $\mathbb{C}$ -Vektorraum ist also gleich $r + d$. Da $\{g_1, \dots, g_r, h_{r+1}, \dots, h_k\}$ ein Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$ als Algebra ist, erzeugen die Monome $g_1^{v_1} \cdots g_r^{v_r} * h_{r+1}^{v_{r+1}} \cdots h_k^{v_k}$ mit $v_1, \dots, v_k \in \mathbb{N}_0$ diese Menge als $\mathbb{C}$ -Vektorraum. Folglich ist H_2 das $\mathbb{C}$ -Vektorraum-Erzeugnis der $g_1^{v_1} \cdots g_r^{v_r} * h_{r+1}^{v_{r+1}} \cdots h_k^{v_k}|_{M_2}$ mit $v_1, \dots, v_k \in \mathbb{N}_0$. Da nach Konstruktion für alle $1 \leq i \leq r$ aus $g_i(C) \neq 0$ stets $p \mid \det C$ und für alle $r < i \leq k$ aus $h_i(C) \neq 0$ stets $p^2 \mid \det C$ folgt, implizieren sowohl $(g_i * g_j * g_l)(C) \neq 0$ (für beliebige $1 \leq i, j, l \leq r$) als auch $(g_i * h_j)(C) \neq 0$ (für beliebige $1 \leq i \leq r$ und $r < j \leq k$) und $(h_i * h_j)(C) \neq 0$ (für beliebige $r < i, j \leq k$) stets $p^3 \mid \det C$ (nach 1.1.9), also muss für $g_1^{v_1} \cdots g_r^{v_r} * h_{r+1}^{v_{r+1}} \cdots h_k^{v_k}|_{M_2} \neq 0$ genau einer der folgenden Fälle auftreten: (i) Es gibt genau ein $1 \leq i \leq k$ mit $v_i = 1$, für alle $j \neq i$ gilt $v_j = 0$. (ii) Es gibt genau ein $1 \leq i \leq r$ mit $v_i = 2$, für alle $j \neq i$ gilt $v_j = 0$. (iii) Es gibt $1 \leq i < j \leq r$ mit $v_i = 1$ und $v_j = 1$, für alle $l \neq i, j$ ist $v_l = 0$. Indem man die Anzahl der Möglichkeiten für die einzelnen Fälle addiert, erhält man, dass das oben angegebene $\mathbb{C}$ -Vektorraum-Erzeugendensystem für H_2 aus genau $k + r + \binom{r}{2}$ von 0 verschiedenen Elementen besteht. Diese Anzahl muss mindestens so groß sein wie die Dimension von H_2 , also folgt $k + r + \binom{r}{2} \geq r + d$ und damit $k \geq d - \binom{r}{2}$, was nun auch den noch fehlenden Teil der Behauptung beweist. $\square$

Nun können die aus den Ergebnissen des letzten Abschnitts ableitbaren Erzeugendensysteme von Primärkomponenten auf Minimalität untersucht werden.

2.9.2 BEISPIEL: Die Bezeichnungen seien zunächst aus 2.7.1 übernommen. Wähle als Erzeugendensystem der Algebra $H(G_2, I_{2,p}^*, U_2)$ gemäß 2.8.6 alle Funktionen der Form $\llbracket C \rrbracket$ für unzerlegbare $C \in I_{2,p}^*$ mit $\llbracket C \rrbracket \neq \llbracket 1, 1 \rrbracket$ (die Funktion $\llbracket 1, 1 \rrbracket$ wird im Erzeugendensystem nicht benötigt, da sie sich stets als g^0 für ein $g \in H(G_2, I_{2,p}^*, U_2)$ darstellen lässt). Alle in 2.8.16 vorgestellten Beispiele für $n = 2$ liefern so Erzeugendensysteme, deren Mächtigkeit gleich der in 2.9.1 berechneten Schranke ist, also sind alle diese Erzeugendensysteme minimal.

Betrachte nun (mit den Voraussetzungen aus 2.8.9) den Fall $m = 1$ und $v_1 = 5$. Als von $\llbracket 1, 1 \rrbracket$ verschiedene Klassen unzerlegbarer Matrizen erhält man mit 2.8.13

$$\llbracket 1, p^5 \rrbracket, \quad \llbracket p, p^4 \rrbracket, \quad \llbracket p^2, p^3 \rrbracket, \quad \llbracket p^5, p^5 \rrbracket,$$

während 2.9.1 als untere Schranke für die Mächtigkeit eines Erzeugendensystems 3 liefert. Daher gestattet dieses Lemma hier keinen Beweis der Minimalität des aus den unzerlegbaren Matrizen ableitbaren Erzeugendensystems. Als Ursache für die Nichtverwendbarkeit der Schranke aus 2.9.1 kann man die Tatsache ausmachen, dass es Beispiele gibt, in denen die im Beweis auftretenden Monome $g_1^2, g_2^2, g_3^2, g_1 * g_2, g_1 * g_3$ und $g_2 * g_3$ linear abhängig sind. Ob dies immer so ist, also ob das oben herleitbare Erzeugendensystem mit 4 Elementen dennoch minimal ist, kann derzeit weder bewiesen noch widerlegt werden. $\diamond$

In zu 2.9.1 analoger Weise lassen sich auch Schranken für den Fall $n \geq 3$ herleiten. Es stellt sich jedoch heraus, dass diese Schranke kaum brauchbar ist, da sie nur in wenigen Fällen mit der Mächtigkeit des aus den unzerlegbaren Matrizen herleitbaren Erzeugendensystems übereinstimmt. Als nächstes soll daher eine andere Fragestellung

untersucht werden, nämlich ob die als minimal identifizierten Erzeugendensysteme sogar algebraisch unabhängig sind. Im Fall der Primidealzerlegung $p_0 = p_1$ kann der Beweis der algebraischen Unabhängigkeit nahezu wortwörtlich aus dem klassischen Fall (etwa aus [Fre83] 2.9 (S. 244)) übernommen werden. Einige interessantere Spezialfälle werden im folgenden betrachtet.

2.9.3 LEMMA: Es seien die Bezeichnungen aus 2.8.9 übernommen mit $m = 1$ und $v_1 = 2$. Dann bilden $\llbracket 1, p_1^2 \rrbracket$ und $\llbracket p_1, p_1 \rrbracket$ ein algebraisch unabhängiges $\mathbb{C}$ -Algebren-Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$. Es gilt also $H(G_2, I_{2,p}^*, U_2) \cong \mathbb{C}[X_1, X_2]$, wobei X_1 und X_2 Unbestimmte sind. $\diamond$

Beweis:

Setze zur Vereinfachung der Schreibweisen $p = p_1$. Es genügt nun zu zeigen, dass $\llbracket 1, p^2 \rrbracket$ und $\llbracket p, p \rrbracket$ algebraisch unabhängig sind. Es sei angenommen, diese beiden Elemente seien algebraisch abhängig. Dann gibt es ein Polynom $F \in \mathbb{C}[X_1, X_2]$ mit $F \neq 0$ und $F(\llbracket 1, p^2 \rrbracket, \llbracket p, p \rrbracket) = 0$. Dies ist äquivalent dazu, dass es eine endliche nichtleere Teilmenge M von $\mathbb{N}_0 \times \mathbb{N}_0$ und Koeffizienten $c_{m_1 m_2} \in \mathbb{C} \setminus \{0\}$ für alle $(m_1, m_2) \in M$ gibt mit

$$f := \sum_{(m_1, m_2) \in M} c_{m_1 m_2} \llbracket 1, p^2 \rrbracket^{m_1} * \llbracket p, p \rrbracket^{m_2} = 0.$$

Wähle nun (k_1, k_2) so, dass

$$k_2 = \min\{m_2 \mid (m_1, m_2) \in M\}$$

und

$$k_1 = \min\{m_1 \mid (m_1, k_2) \in M\}$$

gilt. Dann hat man $(k_1, k_2) \in M$, und für jedes Paar $(m_1, m_2) \in M$ mit $(m_1, m_2) \neq (k_1, k_2)$ folgt $k_2 < m_2$ (falls $m_2 \neq k_2$) oder $k_1 < m_1$ (falls $m_2 = k_2$ und $m_1 \neq k_1$), also $k_2 < m_2$ oder $2k_1 + 2k_2 < 2m_1 + 2m_2$. Wählt man nun gemäß 2.2.10 ein $C \in I_{2,p}^*$ mit $\mathfrak{d}_1(C) = p^{k_1}$ und $\mathfrak{d}_2(C) = p^{2k_1+2k_2}$, so gilt $\mathfrak{d}_1(C) \parallel p^{m_2}$ oder $\mathfrak{d}_2(C) \parallel p^{2m_1+2m_2}$. In einem Produkt der Form $\llbracket 1, p^2 \rrbracket^{l_1} * \llbracket p, p \rrbracket^{l_2}$ haben aber nur solche $C \in I_{2,p}^*$

einen von 0 verschiedenen Funktionswert, für die $p^{l_2} \mid \mathfrak{d}_1(C)$ und $p^{2l_1+2l_2} \mid \mathfrak{d}_2(C)$ gilt (induktive Anwendung von 2.8.2), also gilt hier

$$(\llbracket 1, p^2 \rrbracket^{l_1} * \llbracket p, p \rrbracket^{l_2})(C) = 0 \quad \text{für alle } (l_1, l_2) \in M \setminus \{(k_1, k_2)\},$$

so dass

$$\begin{aligned} 0 = f(C) &= \sum_{(m_1, m_2) \in M} c_{m_1 m_2} (\llbracket 1, p^2 \rrbracket^{m_1} * \llbracket p, p \rrbracket^{m_2})(C) \\ &= c_{k_1 k_2} (\llbracket 1, p^2 \rrbracket^{k_1} * \llbracket p, p \rrbracket^{k_2})(C) \end{aligned}$$

folgt. Nach 2.8.2 (induktiv angewendet) ist $(\llbracket 1, p^2 \rrbracket^{k_1} * \llbracket p, p \rrbracket^{k_2})(C) \neq 0$, so dass man aus der letzten Gleichung $c_{k_1 k_2} = 0$ erhält, was einen Widerspruch zu $(k_1, k_2) \in M$ darstellt. Daher können $\llbracket 1, p^2 \rrbracket$ und $\llbracket p, p \rrbracket$ nicht algebraisch abhängig sein. $\square$

Es gibt auch Fälle, in denen minimale Erzeugendensysteme von Primärkomponenten nicht algebraisch unabhängig sind, wie das folgende Lemma zeigt.

2.9.4 LEMMA: Seien die Voraussetzungen 2.8.9 mit $m = 2$ und $v_1 = v_2 = 1$ erfüllt. Dann ist

$$\{\llbracket 1, p_1 p_2 \rrbracket, \llbracket p_1, p_1 p_2^2 \rrbracket, \llbracket p_2, p_1^2 p_2 \rrbracket, \llbracket p_1 p_2, p_1 p_2 \rrbracket\}$$

ein minimales Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$, aber algebraisch abhängig. $\diamond$

BEWEIS:

Dass die gegebene Menge ein minimales Erzeugendensystem von $H(G_2, I_{2,p}^*, U_2)$ ist, wurde bereits in 2.9.2 bewiesen, zeige also nur noch die algebraische Abhängigkeit.

Die folgenden Monome können nach 1.1.9 (induktiv angewendet) aufgrund der Multiplikativität der Determinante jeweils nur auf den

Matrizen $C \in I_{2,p}^*$ mit $\mathfrak{d}_2(C) = p^4 \mathfrak{o}$ einen von Null verschiedenen Wert annehmen:

$$\begin{aligned} & \llbracket 1, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket^4, & \llbracket 1, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket^2 * \llbracket \mathfrak{p}_1, \mathfrak{p}_1 \mathfrak{p}_2^2 \rrbracket, \\ & \llbracket 1, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket^2 * \llbracket \mathfrak{p}_2, \mathfrak{p}_1^2 \mathfrak{p}_2 \rrbracket, & \llbracket 1, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket^2 * \llbracket \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket, \\ & \llbracket \mathfrak{p}_1, \mathfrak{p}_1 \mathfrak{p}_2^2 \rrbracket^2, & \llbracket \mathfrak{p}_1, \mathfrak{p}_1 \mathfrak{p}_2^2 \rrbracket * \llbracket \mathfrak{p}_2, \mathfrak{p}_1^2 \mathfrak{p}_2 \rrbracket, \\ & \llbracket \mathfrak{p}_1, \mathfrak{p}_1 \mathfrak{p}_2^2 \rrbracket * \llbracket \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket, & \llbracket \mathfrak{p}_2, \mathfrak{p}_1^2 \mathfrak{p}_2 \rrbracket^2, \\ & \llbracket \mathfrak{p}_2, \mathfrak{p}_1^2 \mathfrak{p}_2 \rrbracket * \llbracket \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket, & \llbracket \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1 \mathfrak{p}_2 \rrbracket^2. \end{aligned}$$

Nun hat $\{f|_M \mid f \in H(G_2, I_{2,p}^*, U_2)\}$ für $M = \{C \in I_{2,p}^* \mid \mathfrak{d}_n(C) = p^4 \mathfrak{o}\}$ die $\mathbb{C}$ -Vektorraum-Dimension 9, eine Basis dieses Vektorraumes wird nach 2.2.4 (f) und 2.2.5 beispielsweise von

$$\begin{aligned} & \llbracket 1, \mathfrak{p}_1^4 \mathfrak{p}_2^4 \rrbracket, & \llbracket \mathfrak{p}_1, \mathfrak{p}_1^3 \mathfrak{p}_2^4 \rrbracket, & \llbracket \mathfrak{p}_1^2, \mathfrak{p}_1^2 \mathfrak{p}_2^4 \rrbracket, & \llbracket \mathfrak{p}_2, \mathfrak{p}_1^4 \mathfrak{p}_2^3 \rrbracket, & \llbracket \mathfrak{p}_1 \mathfrak{p}_2, \mathfrak{p}_1^3 \mathfrak{p}_2^3 \rrbracket, \\ & \llbracket \mathfrak{p}_1^2 \mathfrak{p}_2, \mathfrak{p}_1^2 \mathfrak{p}_2^3 \rrbracket, & \llbracket \mathfrak{p}_2^2, \mathfrak{p}_1^4 \mathfrak{p}_2^2 \rrbracket, & \llbracket \mathfrak{p}_1 \mathfrak{p}_2^2, \mathfrak{p}_1^3 \mathfrak{p}_2^2 \rrbracket, & \llbracket \mathfrak{p}_1^2 \mathfrak{p}_2^2, \mathfrak{p}_1^2 \mathfrak{p}_2^2 \rrbracket \end{aligned}$$

gebildet. Daher müssen die 10 oben aufgelisteten Monome linear abhängig sein, also existiert eine nichttriviale Linearkombination der 0. Dies beweist auch die algebraische Abhängigkeit, da eine Linearkombination von Monomen ein Polynom ist. $\square$

Der Fall der Primidealzerlegung $p\mathfrak{o} = \mathfrak{p}^2$ kann vollständig analysiert werden.

2.9.5 LEMMA: Seien die Voraussetzungen 2.8.9 mit $m = 1$ und $v_1 = 2$ erfüllt. Dann ist

$$\{\llbracket C \rrbracket \mid C \in I_{n,p}^* \text{ unzerlegbar}\} \setminus \{\llbracket 1, 1 \rrbracket\}$$

für $n = 2$ ein algebraisch unabhängiges und für $n \geq 3$ ein algebraisch abhängiges Erzeugendensystem von $H(G_n, I_{n,p}^*, U_n)$. $\diamond$

BEWEIS:

Nach 2.8.6 und 2.9.3 verbleibt zu zeigen, dass für $n \geq 3$ die gegebene Menge algebraisch abhängig ist. Berechne dazu die Dimension

des Untervektorraums V_n von $H(G_n, I_{n,p}^*, U_n)$, der alle Funktionen enthält, die nur auf den Matrizen C mit $\mathfrak{d}_n(C) = \mathfrak{p}_1^8$ einen von Null verschiedenen Wert annehmen. Diese Dimension ist gleich der Anzahl der Elemente der Form $\llbracket a_1, \dots, a_n \rrbracket$ mit $a_1 \cdots a_n = \mathfrak{p}_1^8$, da diese eine Basis des Untervektorraums bilden. Die Dimensionsberechnung für festes n ist also durch kombinatorische Überlegungen durchführbar. Berechne nun weiter p_n , die Anzahl der Produkte von Elementen aus der gegebenen Menge, die in diesem Unterraum liegen, also nur auf den Matrizen C mit $\mathfrak{d}_n(C) = \mathfrak{p}_1^8$ einen von Null verschiedenen Wert annehmen. Dies ist ebenfalls durch endlich viele Produktbildungen durchführbar. Man erhält

n	$\dim V_n$	p_n
3	10	11
4	15	16
5	18	19
6	20	21
7	21	22
8	22	23

Da hier jeweils die Anzahl der Produkte größer ist als die Untervektorraumdimension, müssen die Produkte linear abhängig sein, womit die Menge algebraisch abhängig ist. Im Fall $n > 8$ gilt nun ebenfalls $\dim V_n = 22$, da aufgrund der Bedingung $\mathfrak{d}_n(C) = \mathfrak{p}_1^8$ in der Darstellung $\llbracket C \rrbracket = \llbracket a_1, \dots, a_n \rrbracket$ nur die letzten 8 Einträge von $\mathfrak{o}$ verschieden sein dürfen und man für eine Basis B_8 von V_8 somit

$$\{\llbracket \text{diag}(1, \dots, 1, C) \rrbracket \in H(G_n, I_{n,p}^*, U_n) \mid \llbracket C \rrbracket \in B_8\}$$

als eine Basis von V_n erhält. Analog kann man die Produkte für $n = 8$ zu Produkten für $n > 8$ erweitern und erhält für die Anzahl der Produkte $p_n \geq p_8 = 23 > 22 = \dim V_n$. Insgesamt liegt algebraische Abhängigkeit also für alle $n \in \mathbb{N}$ mit $n \geq 3$ vor. $\square$

Für weitere Spezialfälle kann die Untersuchung von minimalen Erzeugendensystemen auf algebraische Abhängigkeit in ähnlicher Form

geführt werden. Eine allgemeine Charakterisierung der algebraisch unabhängigen minimalen Erzeugendensysteme ist allerdings bislang nicht bekannt.

KAPITEL DREI

HECKE-ALGEBREN ZU UNITÄREN GRUPPEN

Nachdem im letzten Kapitel für beliebige Dedekind-Ringe $\mathfrak{o}$ die Struktur von Hecke-Algebren $H(G, M, U)$ untersucht wurde, bei denen U die Menge aller invertierbaren Matrizen über $\mathfrak{o}$ mit einem vorgeschriebenem Format ist, sollen nun in Teilen vergleichbare Resultate für den Fall hergeleitet werden, dass U eine unitäre Gruppe zu einem Ganzheitsring eines imaginär-quadratischen Zahlkörper ist. Auch diese Algebren kann man als Verallgemeinerungen der in [Heig0] betrachteten Hecke-Algebren bezüglich Gruppen von (2×2) -Matrizen auffassen.

§ 3.1

WOHLDEFINIERTHEIT

In diesem Abschnitt werden die zur Definition der zu betrachtenden Hecke-Algebren nötigen Bezeichnungen eingeführt und dann diese Algebren auf Wohldefiniertheit untersucht. Dazu werden Matrixtransformationen definiert und dann Mengen von Matrizen betrachtet, die ein spezielles Transformationsverhalten zeigen.

3.1.1 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Sei K ein imaginär-quadratischen Zahlkörper und $\mathfrak{o}$ dessen Ganzheitsring. Ist $n \in \mathbb{N}$ und sind $L, M \in K^{n \times n}$, so definiere

$$M^* = \overline{M}^T \quad \text{und} \quad L[M] = M^*LM,$$

wobei $\overline{M}$ die Matrix bezeichnet, die man aus M erhält, indem man alle Einträge komplex konjugiert. Setze

$$J_n = \begin{pmatrix} 0 & -E_n \\ E_n & 0 \end{pmatrix} \in \mathfrak{o}^{2n \times 2n}$$

sowie $U_n = \text{GL}_n(\mathfrak{o})$. Für jedes $m \in K$ führe weiter die Bezeichnungen

$$\Delta_n(m) = \{M \in \mathfrak{o}^{2n \times 2n} \mid J_n[M] = mJ_n\}$$

und

$$\Delta'_n(m) = \{M \in K^{2n \times 2n} \mid J_n[M] = mJ_n\}$$

ein. Setze nun $\Gamma_n = \Delta_n(1)$ und

$$\Delta_n = \bigcup_{m=1}^{\infty} \Delta_n(m) \quad \text{sowie} \quad \Delta'_n = \bigcup_{m \in \mathbb{Q} \setminus \{0\}} \Delta'_n(m).$$

Für jedes $M \in \Delta'_n$ sei $w(M) \in K$ definiert durch die Gleichung $J_n[M] = w(M)J_n$. Weiter definiere $\Gamma_n[\mathfrak{a}] = \{M \in \Gamma_n \mid M - E_n \in \mathfrak{a}^{n \times n}\}$ für alle $n \in \mathbb{N}$ und Ideale $\mathfrak{a}$ in $\mathfrak{o}$.

Zuletzt wird noch eine Konvention eingeführt: Wird für eine Matrix $M \in K^{2n \times 2n}$ eine Schreibweise der Form $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ ohne weitere Spezifikation von A, B, C und D verwendet, so beinhaltet dies, dass die Blöcke A, B, C und D alle das Format $n \times n$ haben. $\diamond$

Zunächst beweise einige elementare Eigenschaften von $\Delta'_n(m)$ und $\Delta_n(m)$.

3.1.2 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$.

- a) Ist $m \in K \setminus \mathbb{Q}$, so gilt $\Delta'_n(m) = \emptyset$.
- b) Ist $m \in \mathbb{Q}$ und $M \in \Delta'_n(m)$, so gilt $|\det M| = |m|^n$.
- c) Ist $m \in \mathbb{Q} \setminus \{0\}$, so ist $M \in \Delta'_n(m)$ äquivalent zu $M^* \in \Delta'_n(m)$, und $M \in \Delta_n(m)$ ist äquivalent zu $M^* \in \Delta_n(m)$. $\diamond$

BEWEIS:

- a) Sei $m \in K$ und $M \in \Delta_n(m)$. Wegen $J_n^* = J_n^T = -J_n$ und $M^{**} = M$ gilt

$$\begin{aligned} mJ_n &= J_n[M] = M^*J_nM = (M^*J_nM)^{**} = (M^*J_n^*M^{**})^* \\ &= (-M^*J_nM)^* = (-mJ_n)^* = -\overline{m}J_n^* = \overline{m}J_n, \end{aligned}$$

also $m = \overline{m}$ und somit $m \in \mathbb{R}$, also insgesamt $m \in K \cap \mathbb{R} = \mathbb{Q}$ (da K imaginär-quadratischer Zahlkörper). Daraus folgt die Behauptung.

- b) Sei $m \in \mathbb{Q}$ und $M \in \Delta'_n(m)$. Dann gilt $M^*J_nM = J_n[M] = mJ_n$, also

$$(\det M^*)(\det J_n)(\det M) = \det(mJ_n) = m^{2n} \det J_n,$$

woraus man mit $\det J_n = 1$ die Gleichung $(\det M^*)(\det M) = m^{2n}$ erhält. Wegen $\det M^* = \det \overline{M} = \overline{\det M}$ hat man

$$|\det M|^2 = (\overline{\det M})(\det M) = (\det M^*)(\det M) = m^{2n},$$

was die Behauptung liefert.

- c) Sei $M \in \Delta'_n(m)$. Dann gilt $M^*J_nM = J_n[M] = mJ_n$, also

$$\begin{aligned} J_n[M^*]J_nM &= M^{**}J_nM^*J_nM = MJ_nM^*J_nM = MJ_nmJ_n \\ &= mM(-E_{2n}) = -mM. \end{aligned}$$

Da $|\det M| = |m|^n \neq 0$ nach Teil (b) gilt, ist M in $K^{2n \times 2n}$ invertierbar. Weiter gilt $J_n^{-1} = -J_n$, so dass man aus dieser Gleichung

$$J_n[M^*] = J_n[M^*]J_nMM^{-1}J_n^{-1} = -mMM^{-1}J_n^{-1} = -mJ_n^{-1} = mJ_n,$$

also $M^* \in \Delta'_n(m)$ erhält. Ist $M \in \Delta_n(m) = \Delta'_n(m) \cap \mathfrak{o}^{2n \times 2n}$, so liefert das bereits Bewiesene zunächst $M^* \in \Delta'_n(m)$, und da mit M auch M^* in $\mathfrak{o}^{2n \times 2n}$ liegt, gilt in diesem Fall sogar $M^* \in \Delta_n(m)$. Von den behaupteten Äquivalenzen wurde somit jeweils eine Richtung bewiesen; die jeweils andere erhält man nun mit $M^{**} = M$ durch erneute Anwendung des bewiesenen Teils. $\square$

Hilfreich für weiterführende Untersuchungen ist die nachfolgende Charakterisierung der Elemente von $\Delta'_n(m)$ und $\Delta_n(m)$.

3.1.3 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$. Weiter sei $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in K^{2n \times 2n}$. Für jedes $m \in \mathbb{Q}$ sind dann äquivalent:

- (i) Es gilt $M \in \Delta'_n(m)$.
 - (ii) Es gilt $C^*A = A^*C$ und $D^*B = B^*D$ sowie $A^*D - C^*B = mE_n$.
 - (iii) Es gilt $BA^* = AB^*$ und $DC^* = CD^*$ sowie $AD^* - BC^* = mE_n$.
- Gilt $M \in \mathfrak{o}^{2n \times 2n}$, so ist (ii) und auch (iii) äquivalent zu $M \in \Delta_n(m)$. $\diamond$

BEWEIS:

Die Äquivalenz (i) $\Leftrightarrow$ (ii) erhält man aus der Definition von $\Delta'_n(m)$ und

$$J_n[M] = \begin{pmatrix} C^*A - A^*C & C^*B - A^*D \\ D^*A - B^*C & D^*B - B^*D \end{pmatrix}.$$

Die Aussage (i) $\Leftrightarrow$ (ii) liefert die Äquivalenz von $M^* \in \Delta'_n(m)$ und (iii). Mit 3.1.2 (c) erhält man daraus (i) $\Leftrightarrow$ (iii).

Der Zusatz ist nach Definition von $\Delta'_n(m)$ und $\Delta_n(m)$ klar. $\square$

Die gerade bewiesene Charakterisierung liefert eine explizite Formel zur Berechnung einer Inversen.

3.1.4 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$.

a) Ist $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Delta'_n$ und setzt man

$$M' = \frac{1}{w(M)} \begin{pmatrix} D^* & -B^* \\ -C^* & A^* \end{pmatrix} \in K^{2n \times 2n},$$

so gilt $M'M = E_{2n}$.

b) Es gilt $\Delta'_n \subseteq \text{GL}_{2n}(K)$.

c) Es gilt $\Gamma_n \subseteq U_{2n}$. ◇

BEWEIS:

a) Ausmultiplizieren liefert

$$M'M = \frac{1}{w(M)} \begin{pmatrix} D^*A - B^*C & D^*B - B^*D \\ A^*C - C^*A & A^*D - C^*B \end{pmatrix} \stackrel{3.1.3}{=} \begin{pmatrix} E_n & 0 \\ 0 & E_n \end{pmatrix},$$

was genau die Behauptung ist.

b) folgt aus (a)

c) Für jedes $M \in \Gamma_n = \Delta_n(1) \subseteq \mathfrak{o}^{2n \times 2n}$ liegt das gemäß Teil (a) konstruierte M' wegen $w(M) = 1$ in $\mathfrak{o}^{2n \times 2n}$, und da $M'M = E_{2n}$ nach Teil (a) gilt, folgt die Behauptung. □

Die algebraische Struktur der Menge Δ'_n und einiger spezieller Teilmengen wird im folgenden Lemma genauer untersucht.

3.1.5 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$.

a) Für alle $l, m \in \mathbb{Q}$ gilt

$$\Delta'_n(l) \cdot \Delta'_n(m) \subseteq \Delta'_n(lm) \quad \text{und} \quad \Delta_n(l) \cdot \Delta_n(m) \subseteq \Delta_n(lm).$$

b) Für alle $m \in \mathbb{Q} \setminus \{0\}$ gilt $\Delta'_n(m)^{-1} = \Delta'_n(\frac{1}{m})$.

c) Mit der Matrixmultiplikation ist Δ'_n eine Untergruppe von $\text{GL}_{2n}(K)$.

d) Mit der Matrixmultiplikation ist Γ_n eine Untergruppe von U_{2n} . $\diamond$

BEWEIS:

a) Sei $L \in \Delta'_n(l)$ und $M \in \Delta'_n(m)$. Dann gilt

$$J_n[LM] = (LM)^* J_n LM = M^* L^* J_n LM = LM^* J_n M = lm J_n,$$

also $LM \in \Delta'_n(lm)$, was die erste Behauptung liefert. Zum Nachweis von $\Delta_n(l) \cdot \Delta_n(m) \subseteq \Delta_n(lm)$ verwende den bereits bewiesenen Teil und die Tatsache, dass hier alle Matrizen in $\mathfrak{o}^{2n \times 2n}$ liegen.

b) Sei $M \in \Delta'_n(m)^{-1}$. Dann gilt $M^{-1} \in \Delta'_n(m)$ und somit

$$m J_n = J_n[M^{-1}] = (M^{-1})^* J_n M^{-1},$$

also $m^{-1} J_n^{-1} = M J_n^{-1} M^*$. Mit $J_n^{-1} = -J_n$ hat man dann

$$-m^{-1} J_n = M J_n^{-1} M^* = -M^{**} J_n M^* = -J_n[M^*],$$

also $m^{-1} J_n = J_n[M^*]$ und folglich $M^* \in \Delta'_n(m^{-1})$, woraus man $M \in \Delta'_n(\frac{1}{m})$ nach 3.1.2 (c) erhält. Dies beweist $\Delta'_n(m)^{-1} \subseteq \Delta'_n(\frac{1}{m})$; indem man m durch $\frac{1}{m}$ ersetzt, erhält man $\Delta'_n(\frac{1}{m})^{-1} \subseteq \Delta'_n(m)$ und daraus dann $\Delta'_n(\frac{1}{m}) = (\Delta'_n(\frac{1}{m})^{-1})^{-1} \subseteq \Delta'_n(m)^{-1}$, so dass man insgesamt die zu zeigende Gleichheit bewiesen hat.

c) Nach Teil (a) und Teil (b) sowie 3.1.4 (b) ist Δ'_n eine bezüglich Multiplikation und Inversenbildung abgeschlossene Teilmenge von $GL_{2n}(K)$, die darüberhinaus wegen $J_n[E_{2n}] = E_{2n}^* J_n E_{2n} = J_n$ die Einheitsmatrix enthält. Dies beweist die Behauptung.

d) Nach Teil (a) und 3.1.4 (c) ist $\Gamma_n = \Delta_n(1)$ eine bezüglich Multiplikation abgeschlossene Teilmenge von U_{2n} , die darüberhinaus wegen $J_n[E_{2n}] = E_{2n}^* J_n E_{2n} = J_n$ die Einheitsmatrix enthält. Ist $M \in \Gamma_n$, so ist $M^{-1} \in \mathfrak{o}^{2n \times 2n}$ wegen $\Gamma_n \subseteq U_{2n}$; weiter gilt $M^{-1} \in \Delta'_n(1)$ nach Teil (b), also insgesamt

$$M^{-1} \in \Delta'_n(1) \cap \mathfrak{o}^{2n \times 2n} = \Delta_n(1) = \Gamma_n.$$

Das beweist die Abgeschlossenheit von Γ_n bezüglich Inversenbildung und schließt den Beweis der Behauptung ab. $\square$

Im letzten Kapitel wurde die Wohldefiniertheit der Hecke-Algebra über die Tatsache gezeigt, dass jede Hauptkongruenzgruppe $U_n[\mathfrak{a}]$ in U_n endlichen Index hat und jede Untergruppe $U_n \cap A^{-1}U_nA$ für $A \in I_n$ eine Hauptkongruenzgruppe enthält. Für den Nachweis, dass $(\Delta'_n, \Delta_n, \Gamma_n)$ ein Hecke-Tripel ist, kann analog vorgegangen werden.

3.1.6 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$. Für jedes Ideal $\mathfrak{a}$ von $\mathfrak{o}$ ist dann $|\Gamma_n[\mathfrak{a}] \backslash \Gamma_n| < \infty$. $\diamond$

BEWEIS:

Die Abbildung $\varphi : \Gamma_n \rightarrow \mathrm{GL}_{2n}(\mathfrak{o} // \mathfrak{a})$, $M \mapsto M + \mathfrak{a}^{2n \times 2n}$ ist ein Gruppenhomomorphismus: Die Beziehung $\varphi(MN) = \varphi(M)\varphi(N)$ für alle $M, N \in \Gamma_n$ erhält man sofort, indem man man die Einträge des Matrixprodukts betrachtet, also ist nur noch die Wohldefiniertheit der Abbildung zu beweisen, wofür hier genügt, für jedes $M \in \Gamma_n$ die Invertierbarkeit von $M + \mathfrak{a}^{2n \times 2n}$ in $(\mathfrak{o} // \mathfrak{a})^{2n \times 2n}$ zu zeigen. Aus

$$(M + \mathfrak{a}^{2n \times 2n})(M^{-1} + \mathfrak{a}^{2n \times 2n}) = E_{2n} + \mathfrak{a}^{2n \times 2n}$$

erhält man diese direkt, da M^{-1} wegen $M \in \Gamma_n \subseteq U_{2n}$ (letzteres gemäß 3.1.5 (d)) existiert und in $\mathfrak{o}^{2n \times 2n}$ liegt.

Nach dem Homomorphiesatz ist nun $\mathrm{Kern} \varphi \backslash \Gamma_n \cong \mathrm{Bild} \varphi$, und da $\mathrm{Kern} \varphi = \{M \in \Gamma_n \mid M + \mathfrak{a}^{2n \times 2n} = E_{2n} + \mathfrak{a}^{2n \times 2n}\} = \Gamma_n[\mathfrak{a}]$ gilt, folgt

$$\begin{aligned} |\Gamma_n[\mathfrak{a}] \backslash \Gamma_n| &= |\mathrm{Bild} \varphi| \leq |\mathrm{GL}_{2n}(\mathfrak{o} // \mathfrak{a})| \leq |(\mathfrak{o} // \mathfrak{a})^{2n \times 2n}| \\ &= |\mathfrak{o} // \mathfrak{a}|^{4n^2} < \infty, \end{aligned}$$

da $\mathfrak{o}$ als Ganzheitsring eines algebraischen Zahlkörpers normendlich ist (vergleiche [Neu92] I (2.5)). $\square$

Nun kann die Wohldefiniertheit von $H(\Delta'_n, \Delta_n, \Gamma_n)$ bewiesen werden.

3.1.7 SATZ: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$. Dann ist $(\Delta'_n, \Delta_n, \Gamma_n)$ ein Hecke-Tripel. $\diamond$

BEWEIS:

Es genügt zu zeigen, dass $\Gamma_n M \Gamma_n$ für jedes $M \in \Delta_n$ in endlich viele Rechtsnebenklassen bezüglich Γ_n zerfällt, da die anderen Eigenschaften eines Hecke-Tripels für $(\Delta'_n, \Delta_n, \Gamma_n)$ nach 3.1.5 erfüllt sind.

Sei $M \in \Delta_n$ und $m = w(M)$. Jedes $L \in \Gamma_n[m\mathfrak{o}]$ besitzt eine Darstellung der Form $L = E_{2n} + mL'$ für ein $L' \in \mathfrak{o}^{2n \times 2n}$. Damit folgt

$$MLM^{-1} = M(E_{2n} + mL')M^{-1} = E_{2n} + ML'mM^{-1},$$

wobei $E_{2n} + ML'mM^{-1}$ zu $\mathfrak{o}^{2n \times 2n}$ gehört, da mM^{-1} nach 3.1.4 (a) auch zu $\mathfrak{o}^{2n \times 2n}$ gehört und alle anderen auftretenden Matrizen ebenfalls in $\mathfrak{o}^{2n \times 2n}$ liegen. Es ist also $MLM^{-1} \in \mathfrak{o}^{2n \times 2n}$. Wegen $M \in \Delta_n(m)$ und $L \in \Gamma_n = \Delta_n(1)$ gilt $MLM^{-1} \in \Delta'_n(m \cdot 1 \cdot \frac{1}{m}) = \Delta'_n(1)$ nach 3.1.5 (a), (b). Somit liegt MLM^{-1} sogar in $\Delta'_n(1) \cap \mathfrak{o}^{2n \times 2n} = \Delta_n(1) = \Gamma_n$, und es folgt daraus $L \in M^{-1}\Gamma_n M$. Da L ein beliebiges Element von $\Gamma_n[m\mathfrak{o}]$ war, zeigt dies $\Gamma_n[m\mathfrak{o}] \subseteq M^{-1}\Gamma_n M$, und da $\Gamma_n[m\mathfrak{o}] \subseteq \Gamma_n$ gilt, hat man auch $\Gamma_n[m\mathfrak{o}] \subseteq \Gamma_n \cap M^{-1}\Gamma_n M$. Zusammen mit $|\Gamma_n[m\mathfrak{o}] \setminus \Gamma_n| < \infty$ nach 3.1.6 folgt dann erst recht $|\Gamma_n \cap M^{-1}\Gamma_n M \setminus \Gamma_n| < \infty$, und da M ein beliebiges Element von Δ_n war, ergibt sich mit 1.1.3 die Behauptung. $\square$

§ 3.2

RECHTSNEBENKLASSENVERTRETER

Für die folgende Untersuchung der Hecke-Algebra zum Hecke-Tripel $(\Delta'_n, \Delta_n, \Gamma_n)$ werden ausgezeichnete Vertreter von Rechtsnebenklassen bezüglich Γ_n benötigt. Bei dem Beweis der Existenz der gewünschten Vertreter wird von der Theorie der Hermiteschen Paare Gebrauch gemacht.

3.2.1 DEFINITION (Hermitesche Paare): Es sei K ein imaginär-quadratischer Zahlkörper, $\mathfrak{o}$ sein Ganzheitsring und $n \in \mathbb{N}$. Ein Paar (A, B) von Matrizen $A, B \in \mathfrak{o}^{n \times n}$ heißt *Hermitesches Paar*, wenn $\text{Rang}(A \ B) = n$ und $AB^* = BA^*$ gilt.

Ein Hermitesches Paar (A, B) heißt *teilerfremd*, wenn für alle $x \in K^{1 \times n}$ mit $xA \in \mathfrak{o}^{1 \times n}$ und $xB \in \mathfrak{o}^{1 \times n}$ auch $x \in \mathfrak{o}^{1 \times n}$ gilt.

Zwei Hermitesche Paare (A_1, B_1) und (A_2, B_2) heißen *assoziiert*, wenn $A_1 B_2^* = B_1 A_2^*$ gilt. $\diamond$

Zunächst werden einige grundlegende Eigenschaften Hermitescher Paare zitiert.

3.2.2 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$.

- a) Ist $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Delta_n$, so sind (A, B) und (C, D) sowie (A^*, C^*) und (B^*, D^*) Hermitesche Paare.
- b) Ein Hermitesches Paar (A, B) ist genau dann teilerfremd, wenn $\mathfrak{d}_n((A \ B)) = \mathfrak{o}$ gilt.
- c) Ist $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n$, so sind (A, B) und (C, D) teilerfremde Hermitesche Paare.
- d) Ist (A, B) ein teilerfremdes Hermitesches Paar, so gibt es in Γ_n eine Matrix der Form $\begin{pmatrix} A & B \\ * & * \end{pmatrix}$. $\diamond$

BEWEIS:

- a) Dies erhält man aus 3.1.3, wenn man für die Paare (A^*, C^*) und (B^*, D^*) berücksichtigt, dass $A^* C^{**} = C^* A^{**}$ zu $A^* C = C^* A$ und $B^* D^{**} = D^* B^{**}$ zu $B^* D = D^* B$ äquivalent ist.
- b) [Bra51] vor Lemma 1 (S. 144)
- c) [Bra51] vor Lemma 1 (S. 144)
- d) [Bra51] Lemma 1 (S. 144) $\square$

Wichtig für das weitere Vorgehen ist der folgende Satz, der es für bestimmte Betrachtungen gestattet, von beliebigen Hermiteschen Paaren zu teilerfremden Hermiteschen Paaren überzugehen.

3.2.3 SATZ: Sei K ein imaginär-quadratischer Zahlkörper und $\mathfrak{o}$ sein Ganzheitsring. Ist dann (A, B) ein Hermitesches Paar, so gibt es ein teilerfremdes Hermitesches Paar (A', B') , das zu (A, B) assoziiert ist. $\diamond$

BEWEIS:

[Bra49] Satz I (S. 831) $\square$

Mit dem gerade zitierten Satz lässt sich nun die Existenz eines ausgezeichneten Vertreters in jeder Rechtsnebenklasse der Form $\Gamma_n M$ für $M \in \Delta_n$ beweisen.

3.2.4 SATZ: Es seien die Bezeichnungen aus 3.1.1 übernommen und $n \in \mathbb{N}$. Ist $M \in \Delta_n$, so gibt es in $\Gamma_n M$ ein Element der Form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. $\diamond$

BEWEIS:

Sei $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Delta_n$. Dann ist (A^*, C^*) nach 3.2.2 (a) ein Hermitesches Paar, zu dem es nach 3.2.3 ein assoziiertes teilerfremdes Hermitesches Paar (F, G) gibt, so dass insbesondere $FC = FC^{**} = GA^{**} = GA$ gilt. Das teilerfremde Hermitesche Paar (F, G) lässt sich nach 3.2.2 (d) zu einer Matrix $P = \begin{pmatrix} F & G \\ * & * \end{pmatrix} \in \Gamma_n$ ergänzen. Wegen $J_n \in \Gamma_n$ gilt dann auch $J_n P J_n \in \Gamma_n$. Zusammen mit

$$\begin{aligned} J_n P J_n M &= \begin{pmatrix} 0 & -E_n \\ E_n & 0 \end{pmatrix} \begin{pmatrix} F & G \\ * & * \end{pmatrix} \begin{pmatrix} 0 & -E_n \\ E_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} * & * \\ G & -F \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} * & * \\ GA - FC & GB - FD \end{pmatrix} \\ &\stackrel{GA=FC}{=} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \end{aligned}$$

folgt nun die Behauptung. $\square$

Nun lassen sich Vertretersysteme von $\Gamma_n \parallel \Delta_n(m)$ angeben.

3.2.5 SATZ: Es seien die Bezeichnungen aus 3.1.1 übernommen, $n \in \mathbb{N}$ und V_n ein Vertretersystem von $U_n \parallel \mathfrak{o}^{n \times n}$. Weiter sei

$$X'_{n,m} = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(m) \mid D \in V_n \right\}.$$

Dann gilt $\Delta_n(m) = \Gamma_n X$. Insbesondere lässt sich aus $X'_{n,m}$ ein Vertretersystem $X_{n,m}$ von $\Gamma_n \parallel \Delta_n(m)$ auswählen. $\diamond$

BEWEIS:

Zeige, dass zu jedem $M \in \Delta_n(m)$ ein $P \in \Gamma_n$ und ein $M' \in X'_{n,m}$ existiert man $M = PM'$. Nach 3.2.4 existiert ein $P' \in \Gamma_n$ und ein $R \in \mathfrak{o}^{n \times n}$ mit $P'M = \begin{pmatrix} * & * \\ 0 & R \end{pmatrix}$. Wähle nun $Q \in U_n$ so, dass $QR \in V$ gilt. Wie man mit 3.1.3 nachrechnet, gilt $\text{diag}(Q^*, Q^{-1}) \in \Gamma_n$. Setzt man also $P = (P')^{-1} \text{diag}(Q^*, Q^{-1})$ und $M' = P^{-1}M$, so gilt $P \in \Gamma_n$ und $M' \in \Delta_n(m)$ nach 3.1.5 (a), (b) sowie $M = PM'$ und

$$\begin{aligned} M' &= P^{-1}M = \text{diag}(Q^*, Q^{-1})^{-1}P'M = \begin{pmatrix} (Q^*)^{-1} & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} * & * \\ 0 & R \end{pmatrix} \\ &= \begin{pmatrix} * & * \\ 0 & QR \end{pmatrix} \stackrel{QR \in V_n}{\in} X'_{n,m}, \end{aligned}$$

was $M \in \Gamma_n X'_{n,m}$ beweist. Somit gilt also $\Delta_n(m) \subseteq \Gamma_n X'_{n,m}$. Die Inklusion $\Gamma_n X'_{n,m} \subseteq \Delta_n(m)$ erhält man aus 3.1.5 (a), womit insgesamt die behauptete Gleichheit gezeigt ist. Der Zusatz ist klar. $\square$

Die hier gezeigten Sätze finden im nächsten Abschnitt Anwendung, wo die Frage nach einer Tensorproduktzerlegung von $H(\Delta'_n, \Delta_n, \Gamma_n)$ untersucht wird.

§ 3.3

TENSORPRODUKTZERLEGUNGEN

In diesem Abschnitt wird gezeigt, dass es ein Analogon zu 2.7.8 für $H(\Delta'_n, \Delta_n, \Gamma_n)$ nicht geben kann. Darüberhinaus werden einige dennoch geltende schwächere Resultate bewiesen. Als Vorbereitung wird gezeigt, dass die $\Gamma_n LM$ für $L :: \Gamma_n \parallel \Delta_n(l)$ und $M :: \Gamma_n \parallel \Delta_n(m)$ paarweise verschieden sind, wenn l und m teilerfremde natürliche Zahlen sind.

3.3.1 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen, $l, m \in \mathbb{N}$ teilerfremd und $n \in \mathbb{N}$. Weiter seien $X_{n,l}$ und $X_{n,m}$ gemäß 3.2.5 konstruiert. Sind dann $L, L' \in X_{n,l}$ und $M, M' \in X_{n,m}$ mit $\Gamma_n LM = \Gamma_n L'M'$ gegeben, so gilt bereits $L = L'$ und $M = M'$. $\diamond$

BEWEIS:

Wegen $\Gamma_n LM = \Gamma_n L'M'$ gibt es ein $P \in \Gamma_n$ mit $L'M' = PLM$, und es folgt $M'M^{-1} = (L')^{-1}PL$. Wegen $M \in X_{n,m} \subseteq \Delta_n(m)$ folgt mit 3.1.4 (a), dass $mM^{-1} \in \mathfrak{o}^{2n \times 2n}$ und somit auch $mM'M^{-1} \in \mathfrak{o}^{2n \times 2n}$ gilt. Ebenso erhält man aus $L \in X_{n,l} \subseteq \Delta_n(l)$, dass $lL^{-1} \in \mathfrak{o}^{2n \times 2n}$ gilt, woraus $lM'M^{-1} = l(L')^{-1}PL \in \mathfrak{o}^{2n \times 2n}$ folgt. Insgesamt erhält man nun $M'M^{-1} \in \mathfrak{o}^{2n \times 2n}$ nach 2.7.3 aufgrund der Teilerfremdheit von l und m . Darüberhinaus gilt $M'M^{-1} \in \Delta'_n(1)$ nach 3.1.5 (a) wegen $M, M' \in \Delta_n(m)$, also insgesamt $M'M^{-1} \in \Delta'_n(1) \cap \mathfrak{o}^{2n \times 2n} = \Gamma_n$, woraus $\Gamma_n M' = \Gamma_n M$ folgt. Da M und M' als Elemente von $X_{n,m}$ zu einem Vertretersystem von $\Gamma_n \parallel \Delta_n(m)$ gehören, erhält man aus $\Gamma_n M' = \Gamma_n M$ bereits $M' = M$. Somit wird die Voraussetzung $\Gamma_n LM = \Gamma_n L'M'$ zu $\Gamma_n LM = \Gamma_n L'M$, und Multiplikation mit M^{-1} von rechts auf beiden Seiten liefert $\Gamma_n L' = \Gamma_n L$ und damit wegen $L, L' \in X_{n,l}$ auch $L' = L$, womit nun die Behauptung vollständig bewiesen ist. $\square$

In Analogie zu 2.7.5 stellt sich nun die Frage, ob sich unter bestimmten Voraussetzungen jedes gegebene $N \in \Delta_n(lm)$ als Produkt zweier

Matrizen $L \in \Delta_n(l)$ und $M \in \Delta_n(m)$ schreiben lässt.

3.3.2 LEMMA: Es seien die Bezeichnungen aus 3.1.1 übernommen, $l, m \in \mathbb{N}$ teilerfremd und $n \in \mathbb{N}$. Zu jeder Matrix $N = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(lm)$, für die $\mathfrak{d}_n(A) + l^n \mathfrak{o}$ ein Hauptideal ist, gibt es dann Matrizen $L \in \Delta_n(l)$ und $M \in \Delta_n(m)$ mit $N = LM$. $\diamond$

BEWEIS:

Setze $\mathfrak{a} = \mathfrak{d}_n(A) + l^n \mathfrak{o}$ und $\mathfrak{b} = \mathfrak{a}^{-1} \mathfrak{d}_n(A)$. Da $\mathfrak{a}$ nach Voraussetzung ein Hauptideal ist, muss auch $\mathfrak{b}$ ein Hauptideal in $\mathfrak{o}$ sein. Wegen $N \in \Delta_n(lm)$ folgt $AD^* = lmE_n$ nach 3.1.3, also $(\det A)(\det D) = l^n m^n$ und damit $\{0\} \neq \mathfrak{d}_n(A) \mid l^n m^n \mathfrak{o}$. Da l und m teilerfremd sind, gibt es dann (teilerfremde) Ideale $\mathfrak{a}'$ und $\mathfrak{b}'$ in $\mathfrak{o}$ mit $\mathfrak{d}_n(A) = \mathfrak{a}' \mathfrak{b}'$ und $\mathfrak{a}' \mid l^n$ sowie $\mathfrak{b}' \mid m^n$. Da dann auch $\mathfrak{b}'$ und l^n teilerfremd sind, gilt

$$\mathfrak{a} = \mathfrak{d}_n(A) + l^n \mathfrak{o} = \mathfrak{a}' \mathfrak{b}' + l^n \mathfrak{o} = \mathfrak{a}' + l^n \mathfrak{o} = \mathfrak{a}',$$

womit wegen $\mathfrak{a} \mathfrak{b} = \mathfrak{d}_n(A) = \mathfrak{a}' \mathfrak{b}'$ auch $\mathfrak{b} = \mathfrak{b}'$ folgt. Insgesamt sind also $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Hauptideale in $\mathfrak{o}$ mit $\mathfrak{d}_n(A) = \mathfrak{a} \mathfrak{b}$. In Verbindung mit 1.1.9 liefert 2.7.5 nun Matrizen $A'_1, A'_2 \in \mathfrak{o}^{n \times n}$ mit $\mathfrak{d}_n(A'_1) = \mathfrak{a}$ und $\mathfrak{d}_n(A'_2) = \mathfrak{b}$ sowie $A \in U_n A'_1 U_n A'_2 U_n$. Wähle nun $A_1 \in U_n A'_1$ und $A_2 \in U_n A'_2 U_n$ mit $A = A_1 A_2$.

Aus 3.1.3 folgt $A^* D = lmE_n$ und damit

$$lmA^{-1} = (lmA^{-1})^{**} = (\bar{l} \bar{m} (A^{-1})^*)^* = (lm(A^*)^{-1})^* = D^*.$$

Somit gilt insbesondere $lmA^{-1} \in \mathfrak{o}^{n \times n}$. Man erhält $lmA_2^{-1} A_1^{-1} \in \mathfrak{o}^{n \times n}$, und daraus ergibt sich $lmA_2^{-1} \in \mathfrak{o}^{n \times n} A_1 \subseteq \mathfrak{o}^{n \times n}$. Andererseits hat man $(\det A_2) A_2^{-1} = A_2^{\text{adj}} \in \mathfrak{o}^{n \times n}$ und somit wegen

$$(\det A_2) \mathfrak{o} = \mathfrak{d}_n(A_2) \stackrel{2.2.5}{=} \mathfrak{d}_n(A'_2) = \mathfrak{b} \mid m^n$$

erst recht $m^n A_2^{-1} \in \mathfrak{o}^{n \times n}$. Insgesamt gilt also $lmA_2^{-1} \in \mathfrak{o}^{n \times n}$ und $m^{n-1} mA_2^{-1} \in \mathfrak{o}^{n \times n}$, und da l und m und damit auch l und m^{n-1} teilerfremd sind, liefert 2.7.3 nun, dass $mA_2^{-1} \in \mathfrak{o}^{n \times n}$ gilt. Analog zeigt man $lA_1^{-1} \in \mathfrak{o}^{n \times n}$. Setzt man also $D_1 = (lA_1^{-1})^*$ und $D_2 = (mA_2^{-1})^*$,

so gilt $D_1, D_2 \in \mathfrak{o}^{n \times n}$ und $A_1^* D_1 = A_1^* (lA_1^{-1})^* = lE_n$ sowie analog $A_2^* D_2 = mE_n$. Mit der oben gezeigten Gleichung $lmA^{-1} = D^*$ gilt weiter

$$\begin{aligned} D_1 D_2 &= (lA_1^{-1})^* (mA_2^{-1})^* = lm(A_2^{-1} A_1^{-1})^* = lm((A_1 A_2)^{-1})^* \\ &= (lmA^{-1})^* = (D^*)^* = D. \end{aligned}$$

Wähle nun ein $x \in l\mathbb{Z} \cap (1 + m\mathbb{Z})$, was wegen der Teilerfremdheit von l und m nach 1.2.9 möglich ist. Setze dann $B_1 = (1 - x)BD_2^{-1}$ und $B_2 = xA_1^{-1}B$. Wegen $D_2 = (mA_2^{-1})^*$ ist $D_2^{-1} = \frac{1}{m}A_2^*$, also ist $B_1 = (1 - x)BD_2^{-1}$ wegen $m \mid 1 - x$ ein Element von $\mathfrak{o}^{n \times n}$. Da vorhin bereits bewiesen wurde, dass lA_1^{-1} in $\mathfrak{o}^{n \times n}$ liegt, folgt wegen $x \mid l$ auch $B_2 = xA_1^{-1}B \in \mathfrak{o}^{n \times n}$.

Setze

$$L = \begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix} \quad \text{und} \quad M = \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix}.$$

Dann gilt $L, M \in \mathfrak{o}^{2n \times 2n}$, da für alle Teilmatrizen gezeigt wurde, dass sie in $\mathfrak{o}^{n \times n}$ liegen. Wegen $N \in \Delta_n(lm)$ gilt $(BA^*)^* = AB^* = BA^*$ sowie $A^*D = lmE_n$ nach 3.1.3, und oben wurde zudem $D = D_1 D_2$ gezeigt. Somit erhält man

$$\begin{aligned} B_1^* D_1 &= (D_1^* B_1)^* = (D_1^* (1 - x)BD_2^{-1})^* = (D_1^* (1 - x)BD^{-1}DD_2^{-1})^* \\ &= (1 - x)(D_1^* (BD^{-1})D_1)^* = (1 - x)D_1^* (BD^{-1})^* D_1 \\ &= (1 - x)D_1^* (B \frac{1}{lm} A^*)^* D_1 = (1 - x)D_1^* \frac{1}{lm} (BA^*)^* D_1 \\ &= (1 - x)D_1^* \frac{1}{lm} BA^* D_1 = (1 - x)D_1^* BD^{-1} D_1 \\ &= D_1^* (1 - x)BD_2^{-1} = D_1^* B_1. \end{aligned}$$

Da zudem $A_1^* D_1 = lE_n$ bereits gezeigt wurde, folgt $L \in \Delta_n(l)$ mit 3.1.3. Für den Nachweis von $M \in \Delta_n(m)$ gehe analog vor: Aus 3.1.3 erhält man wegen $N \in \Delta_n(lm)$, dass $(D^* B)^* = B^* D = D^* B$ und

$AD^* = lmE_n$ gilt, woraus $(A^{-1}B)^* = (\frac{1}{lm}D^*B)^* = \frac{1}{lm}D^*B = A^{-1}B$ folgt, und oben wurde bereits $A_2^*D_2 = mE_n$ gezeigt. Somit erhält man

$$\begin{aligned} B_2^*D_2 &= (D_2^*B_2)^* = (D_2^*xA_1^{-1}B)^* = x(D_2^*A_1^{-1}AA^{-1}B)^* \\ &= x(D_2^*A_2(A^{-1}B))^* = x(A^{-1}B)^*A_2^*D_2 = x(A^{-1}B)mE_n \\ &= x(mE_n)^*(A^{-1}B) = x(A_2^*D_2)^*(A^{-1}B) = xD_2^*A_2A^{-1}B \\ &= D_2^*xA_1^{-1}B = D_2^*B_2. \end{aligned}$$

Zusammen mit $A_2^*D_2 = mE_n$ folgt $M \in \Delta_n(M)$ mit 3.1.3. Zuletzt hat man

$$LM = \begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix} \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix} = \begin{pmatrix} A_1A_2 & A_1B_2 + B_1D_2 \\ 0 & D_1D_2 \end{pmatrix}$$

mit $A_1A_2 = A$ und $D_1D_2 = D$ sowie

$$A_1B_2 + B_1D_2 = A_1xA_1^{-1}B + (1-x)BD_2^{-1}D_2 = xB + B - xB = B,$$

also $LM = N$. Dies schließt den Beweis ab. $\square$

In dem gerade bewiesenen Lemma wurde ein hinreichendes Kriterium dafür formuliert, dass eine gegebene Matrix aus $\Delta_n(lm)$ sich als Produkt von Matrizen aus $\Delta_n(l)$ und $\Delta_n(m)$ schreiben lässt. Nun soll eine ganze Klasse von Matrizen, die diesen Bedingungen genügt, angegeben werden.

3.3.3 SATZ: Es seien die Bezeichnungen aus 3.1.1 übernommen, p eine in $\mathfrak{o}$ träge Primzahl und $l, m, n \in \mathbb{N}$ mit $p \nmid m$. Dann gibt es zu jedem $N \in \Delta_n(p^l m)$ Matrizen $L \in \Delta_n(p^l)$ und $M \in \Delta_n(m)$ mit $N = LM$. $\diamond$

BEWEIS:

Sei $P \in \Gamma_n$ gemäß 3.2.4 so gewählt, dass $N' := PN = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ gilt. Da $p\mathfrak{o}$ ein Primideal und gleichzeitig ein Hauptideal in $\mathfrak{o}$ ist, sind alle Teiler von $p^{ln}\mathfrak{o}$ Hauptideale, also ist insbesondere $\mathfrak{d}_n(A) + p^{ln}\mathfrak{o}$ ein

Hauptideal. Da $p \nmid m$ gilt, sind p^l und m teilerfremd, also folgt mit 3.3.2, dass es ein $L' \in \Delta_n(p^l)$ und ein $M \in \Delta_n(m)$ gibt mit $N' = L'M$. Setzt man $L = P^{-1}L'$, so ist nach 3.1.5 (a), (d) auch L ein Element von $\Delta_n(p^l)$, und es gilt $LM = P^{-1}L'M = P^{-1}N' = N$, was zu beweisen war. $\square$

Die Aussage aus 3.3.3 soll nun in eine Aussage über die Hecke-Algebra $H(\Delta'_n, \Delta_n, \Gamma_n)$ übersetzt werden. Dazu werden zunächst die verwendeten Bezeichnungen eingeführt.

3.3.4 VORAUSSSETZUNGEN UND BEZEICHNUNGEN: Die Bezeichnungen aus 3.1.1 seien übernommen. Darüberhinaus verwende für jedes $n \in \mathbb{N}$ die Bezeichnungen, die sich mit Δ'_n anstelle von G und Γ_n anstelle von U sowie Δ_n anstelle von M aus 1.1.4 ergeben. Für alle $m, n \in \mathbb{N}$ definiere zuletzt

$$T_n(m) = \sum_{M::\Gamma_n \backslash \Delta_n(m) // \Gamma_n} \llbracket M \rrbracket. \quad \diamond$$

Nun folgt die angekündigte Übertragung der Aussage von 3.3.3 auf $H(\Delta'_n, \Delta_n, \Gamma_n)$.

3.3.5 SATZ: Es seien die Bezeichnungen aus 3.3.4 übernommen, $p \in \mathbb{N}$ eine in $\mathfrak{o}$ träge Primzahl und $l, m, n \in \mathbb{N}$ mit $p \nmid m$. Dann gilt $T_n(p^l) * T_n(m) = T_n(p^l m)$. $\diamond$

BEWEIS:

Stellt man $T_n(p^l) * T_n(m)$ als Linearkombination von Funktionen der Form $\llbracket N \rrbracket$ für $N :: \Gamma_n \backslash \Delta_n // \Gamma_n$ dar, so liefert 3.3.1 aufgrund der Teilerfremdheit von p^l und m in Verbindung mit 1.1.10, dass die dort auftretenden Koeffizienten alle jeweils nur 0 oder 1 sein können. Für $N \notin \Delta_n(p^l m)$ muss der zugehörige Koeffizient gleich 0 sein, da für $L \in \Delta_n(p^l)$ und $M \in \Delta_n(m)$ der Träger von $\llbracket L \rrbracket * \llbracket M \rrbracket$ nach 1.1.9 und 3.1.5 (a) stets eine Teilmenge von $\Delta_n(p^l m)$ ist. Für jedes $N \in \Delta_n(p^l m)$ hingegen gibt es nach 3.3.3 Matrizen $L \in \Delta_n(p^l)$ und $M \in \Delta_n(m)$

mit $LM = N$, so dass insbesondere $N \in \Gamma_n L \Gamma_n M \Gamma_n$ und somit nach 1.1.9 $N \in \text{Tr}(\llbracket L \rrbracket * \llbracket M \rrbracket)$ folgt, was beweist, dass N im Träger von $T_n(p^l) * T_n(m)$ enthalten ist. Da für jedes $N \in \Delta_n$ wie bereits gesehen $(T_n(p^l) * T_n(m))(N) \in \{0, 1\}$ gilt, hat man insgesamt

$$(T_n(p^l) * T_n(m))(N) = \begin{cases} 1, & \text{falls } N \in \Delta_n(p^l m), \\ 0 & \text{sonst,} \end{cases}$$

was die zu beweisenden Aussage liefert. $\square$

Es stellt sich nun die Frage, ob in 3.3.5 auf die Bedingung, dass p in $\mathfrak{o}$ träge ist, verzichtet werden kann.

3.3.6 BEMERKUNG: Auf die Trägheitsbedingung in 3.3.5 kann nicht verzichtet werden.

Die Voraussetzungen und Bezeichnungen aus 3.3.4 seien übernommen für $K = \mathbb{Q}(\omega)$ mit $\omega = \sqrt{-5}$. Weiter sei $p = 2$ und $q = 3$ sowie

$$N = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \quad \text{mit} \quad A = \begin{pmatrix} 1 & 0 \\ 0 & 1 + \omega \end{pmatrix} \quad \text{und} \quad D = \begin{pmatrix} 6 & 0 \\ 0 & 1 + \omega \end{pmatrix}.$$

Dann gilt $AD^* = 6E_2$, also $N \in \Delta_2(6) = \Delta_2(pq)$ nach 3.1.3. Es sei angenommen, es würde $T_2(2) * T_2(3) = T_2(6)$ gelten, also insbesondere $(T_2(2) * T_2(3))(N) = 1$ erfüllt sein. Mit den Bezeichnungen aus 3.2.5 existieren dann nach 1.1.10 $L \in X_{2,2}$ und $M \in X_{2,3}$ mit $\Gamma_2 N = \Gamma_2 LM$. Somit folgt, dass ein $P \in \Gamma_2$ mit $PN = LM$ existiert. Da dann $P = LMN^{-1}$ ein Produkt von Matrizen der Form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ ist, hat auch P diese Form. Schreibt man $P = \begin{pmatrix} F & G \\ 0 & W \end{pmatrix}$, so folgt, da nach 3.1.3 $FW^* = E_n$ gilt, dass F in U_2 liegen muss. Weiter sei nun

$$L = \begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix} \quad \text{und} \quad M = \begin{pmatrix} A_2 & B_2 \\ 0 & D_2 \end{pmatrix}.$$

Aus $PN = LM$, also

$$\begin{pmatrix} FA & GD \\ 0 & WD \end{pmatrix} = \begin{pmatrix} A_1 A_2 & A_1 B_2 + B_1 D_2 \\ 0 & D_1 D_2 \end{pmatrix},$$

folgt man insbesondere $A_1 A_2 = FA$, und wegen $F \in U_2$ erhält man daraus $(\det A_1)(\det A_2) \in (\det A)\mathfrak{o}^*$, also $\mathfrak{d}_2(A_1)\mathfrak{d}_2(A_2) = \mathfrak{d}_2(A)$. Da nun $\mathfrak{d}_2(A) = (1 + \omega)\mathfrak{o}$ nicht als Produkt zweier von $(1 + \omega)\mathfrak{o}$ verschiedener Hauptideale geschrieben werden kann, muss ein $i \in \{1, 2\}$ mit $\mathfrak{d}_2(A_i) = (1 + \omega)\mathfrak{o}$ existieren. Aus $L \in X_{2,2} \subseteq \Delta_2(2)$ folgt $A_1 D_1^* = 2E_2$ nach 3.1.3, also $(\det A_1)(\det \overline{D_1}) = 4$. Da aber $1 + \omega$ kein Teiler von 4 ist, kann nicht $\mathfrak{d}_2(A_1) = (1 + \omega)\mathfrak{o}$ gelten. Analog erhält man aber, dass wegen $A_2 D_2^* = 3E_2$ auch $\mathfrak{d}_2(A_2) = (1 + \omega)\mathfrak{o}$ nicht möglich ist. Dieser Widerspruch zeigt, dass die Annahme $T_2(2) * T_2(3) = T_2(6)$ falsch war, was nicht nur beweist, dass die Trägheitsbedingung in 3.3.5 notwendig ist, sondern auch zeigt, dass eine zu 2.7.8 analoge Zerlegung von $H(\Delta'_n, \Delta_n, \Gamma_n)$ im allgemeinen nicht angegeben werden kann. $\diamond$

Trotz dieser negativen Beantwortung der Frage nach einer Tensorproduktzerlegung für den allgemeinen Fall lässt sich dennoch für einen Spezialfall eine solche Zerlegung angeben.

3.3.7 SATZ: Es seien die Bezeichnungen aus 3.3.4 übernommen, wobei K Klassenzahl 1 habe, also $\mathfrak{o}$ ein Hauptidealring sei. Dann ist die Hecke-Algebra $H(\Delta'_n, \Delta_n, \Gamma_n)$ kommutativ, und es gilt

$$H(\Delta'_n, \Delta_n, \Gamma_n) \cong \bigotimes_{p \text{ Primzahl in } \mathbb{N}} H(\Delta'_n, \Delta_{n,p}, \Gamma_n),$$

wenn man $\Delta_{n,p} = \Delta_n(1) \cup \Delta_n(p) \cup \Delta_n(p^2) \cup \dots$ setzt. Definiert man

$$T_n(p) = \llbracket \text{diag}(E_n, pE_n) \rrbracket$$

für alle Primzahlen $p \in \mathbb{N}$ und

$$T_{n,l}(a) = \llbracket \text{diag}(E_{n-l}, aE_l, N(a)E_{n-l}, aE_l) \rrbracket$$

für alle $0 \leq l \leq n$ und $a \in \mathfrak{o} \setminus \{0\}$, so gilt für in $\mathfrak{o}$ träge Primzahlen $p \in \mathbb{N}$ stets

$$H(\Delta'_n, \Delta_{n,p}, \Gamma_n) = \mathbb{C}[T_n(p), T_{n,1}(p), \dots, T_{n,n}(p)] \cong \mathbb{C}[X_1, \dots, X_{n+1}],$$

für in $\mathfrak{o}$ zerlegte Primzahlen $p \in \mathbb{N}$ mit $p = q\bar{q}$ (für $q \in \mathfrak{o}$) stets

$$\begin{aligned} H(\Delta'_n, \Delta_{n,p}, \Gamma_n) &= \mathbb{C}[T_n(p), T_{n,1}(q), \dots, T_{n,n}(q), T_{n,1}(\bar{q}), \dots, T_{n,n}(\bar{q})] \\ &\cong \mathbb{C}[X_1, \dots, X_{2n+1}] \end{aligned}$$

und für in $\mathfrak{o}$ verzweigte Primzahlen $p \in \mathbb{N}$ mit $p = q^2$ (für $q \in \mathfrak{o}$) stets

$$H(\Delta'_n, \Delta_{n,p}, \Gamma_n) = \mathbb{C}[T_{n,0}(q), \dots, T_{n,n}(q)] \cong \mathbb{C}[X_1, \dots, X_{n+1}],$$

wobei die X_i in allen Fällen Unbestimmte bezeichnen. $\diamond$

BEWEIS:

[Kri87] Satz 5 (S. 217) $\square$

§ 3.4

SIMULTANE VERTRETERSYSTEME

Für theoretische Untersuchungen in einer Hecke-Algebra $H(G, M, U)$ sind für gegebenes $g \in M$ Teilmengen von M interessant, die sowohl Vertretersystem von $U \backslash [g]$ als auch Vertretersystem von $[g] \backslash U$ sind. In diesem Abschnitt wird gezeigt, dass solche simultanen Vertretersysteme für $H(\Delta'_n, \Delta_n, \Gamma_n)$ existieren.

3.4.1 VORAUSSETZUNGEN UND BEZEICHNUNGEN: Die Bezeichnungen aus 3.1.1 seien übernommen. Für jedes $n \in \mathbb{N}$ bezeichne $\tilde{\Gamma}_n$ die Faktorgruppe $\Gamma_n \backslash \mathfrak{o}^* E_{2n}$ und $\tilde{\Delta}'_n$ die Faktorgruppe $\Delta'_n \backslash \mathfrak{o}^* E_{2n}$; weiter sei

$$\operatorname{Im} Z = \frac{1}{2i}(Z - Z^*)$$

für alle $Z \in \mathbb{C}^{n \times n}$ und

$$\mathcal{H}_n = \{Z \in \mathbb{C}^{n \times n} \mid \operatorname{Im} Z > 0\},$$

wobei $\text{Im } Z > 0$ bedeutet, dass $z^*(\text{Im } Z)z > 0$ für alle $z \in \mathbb{C}^{n \times 1} \setminus \{0\}$ gilt (also $\text{Im } Z$ positiv definit ist).

Für $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Delta'_n$ und $Z \in \mathcal{H}_n$ definiere über

$$M \langle Z \rangle = (AZ + B)(CZ + D)^{-1}$$

eine Linksooperation von Δ'_n auf $\mathcal{H}_n$. Ist $\tilde{L} \in \tilde{\Delta}'_n$, so sei $\tilde{L} \langle Z \rangle$ definiert durch $L \langle Z \rangle$, wenn L ein Element von Δ'_n mit $\tilde{L} = L\sigma^*E_{2n}$ ist. $\diamond$

Die Wohldefiniertheit von $\tilde{L} \langle Z \rangle$ für $\tilde{L} \in \tilde{\Delta}'_n$ entnimmt man [Bra51] Abschnitt 4 (S. 148).

Der Beweis der Existenz eines simultanen Vertretersystems wird später gemäß 1.1.13 über $|\Gamma_n \backslash [M]| = |[M] / \Gamma_n|$ geführt. Letzteres erhält man wiederum über einen Vergleich von Volumina bestimmter Fundamentalbereiche. Deshalb wird zunächst der Begriff des Fundamentalbereiches eingeführt und untersucht.

3.4.2 DEFINITION (Fundamentalbereich): Sei G eine Gruppe und X eine mit einer Topologie versehene Menge. Die Gruppe G operiere vermöge $\circledast$ (von links) auf X . Eine Teilmenge F von X heißt *Fundamentalbereich* von X zu G , wenn die folgenden Bedingungen erfüllt sind:

- (i) Die Menge F ist abgeschlossen in X .
- (ii) Zu jedem $x \in X$ gibt es ein $g \in G$ mit $g \circledast x \in F$.
- (iii) Sind x_1, x_2 im offenen Kern von F und ist $g \in G$ mit $g \circledast x_1 = x_2$, so gilt $g \circledast x = x$ für alle $x \in X$. $\diamond$

Dass in dem hier interessierenden Fall tatsächlich ein Fundamentalbereich existiert, entnimmt man [Bra51].

3.4.3 SATZ: Es seien die Bezeichnungen aus 3.4.1 übernommen und $n \in \mathbb{N}$, wobei $\mathcal{H}_n$ mit der Relativtopologie zur natürlichen Topologie auf $\mathbb{C}^{n \times n}$ versehen sei. Dann gibt es einen Fundamentalbereich von $\mathcal{H}_n$ zu Γ_n . $\diamond$

BEWEIS:

[Bra51] Lemma 2 (S. 151) $\square$

Das folgende Lemma beschreibt Fundamentalbereiche von $\mathcal{H}_n$ zu Untergruppen von Γ_n .

3.4.4 LEMMA: Es seien die Bezeichnungen aus 3.4.1 übernommen und $n \in \mathbb{N}$ sowie $\mathcal{F}$ ein Fundamentalbereich von $\mathcal{H}_n$ zu Γ_n und Λ eine Untergruppe von Γ_n von endlichem Index mit $o^*E_{2n} \cap \Gamma_n \subseteq \Lambda$.

a) Bilden $M_1, \dots, M_k$ ein Vertretersystem von $\Lambda \parallel \Gamma_n$, so ist

$$\bigcup_{i=1}^k M_i \langle \mathcal{F} \rangle$$

ein Fundamentalbereich von $\mathcal{H}_n$ zu Λ , und die offenen Kerne der $M_i \langle \mathcal{F} \rangle$ sind paarweise disjunkt.

b) Ist $M \in \Gamma_n$ und F ein Fundamentalbereich von $\mathcal{H}_n$ zu Λ , so ist $M \langle F \rangle$ ein Fundamentalbereich von $\mathcal{H}_n$ zu $M\Lambda M^{-1}$. $\diamond$

BEWEIS:

a) Dies ist eine Verallgemeinerung von [Koe07] Satz II.3.1 und lässt sich analog beweisen.

b) Ist $\{M_1, \dots, M_k\}$ ein Vertretersystem von $\Lambda \parallel \Gamma_n$, so ist die Menge $\{MM_1M^{-1}, \dots, MM_kM^{-1}\}$ und somit nach 1.1.2 auch die Menge $\{MM_1, \dots, MM_k\}$ ein Vertretersystem von $M\Lambda M^{-1} \parallel \Gamma_n$; Teil (a) liefert nun die Behauptung, da $M \langle M_i \langle \mathcal{F} \rangle \rangle = (MM_i) \langle \mathcal{F} \rangle$ für alle $1 \leq i \leq k$ gemäß [Bra51] Abschnitt 4 gilt. $\square$

Die Aussage 3.4.4 (b) wird nun auf den zu untersuchenden Spezialfall übertragen.

3.4.5 FOLGERUNG: Es seien die Bezeichnungen aus 3.4.1 übernommen. Ist dann $M \in \Delta'_n$ und F ein Fundamentalbereich von $\mathcal{H}_n$ zu $\Gamma_n \cap (M^{-1}\Gamma_n M)$, so ist $M \langle F \rangle$ ein Fundamentalbereich von $\mathcal{H}_n$ zu $\Gamma_n \cap (M\Gamma_n M^{-1})$. $\diamond$

BEWEIS:

Im Beweis von 3.1.7 wurde gezeigt, dass $\Gamma_n \cap (M^{-1}\Gamma_n M)$ in Γ_n endlichen Index hat. Daher kann 3.4.4 (b) angewendet werden; man erhält, dass $M \langle F \rangle$ ein Fundamentalbereich von $M(\Gamma_n \cap (M^{-1}\Gamma_n M))M^{-1}$ ist. Mit

$$L \in M(\Gamma_n \cap (M^{-1}\Gamma_n M))M^{-1} \quad \Leftrightarrow$$

$$M^{-1}LM \in \Gamma_n \cap (M^{-1}\Gamma_n M) \quad \Leftrightarrow$$

$$M^{-1}LM \in \Gamma_n \text{ und } M^{-1}LM \in M^{-1}\Gamma_n M \quad \Leftrightarrow$$

$$L \in M^{-1}\Gamma_n M \text{ und } L \in \Gamma_n \quad \Leftrightarrow$$

$$L \in \Gamma_n \cap (M^{-1}\Gamma_n M)$$

erhält man die Behauptung. $\square$

Auf $\mathcal{H}_n$ wird nun ein Maß eingeführt.

3.4.6 SATZ: Es seien die Bezeichnungen aus 3.4.1 übernommen, $n \in \mathbb{N}$ und $\mathcal{F}$ ein Fundamentalbereich von $\mathcal{H}_n$ bezüglich Γ_n . Dann gibt es ein Maß μ auf $\mathcal{H}_n$, das den folgenden Bedingungen genügt:

- (i) Das Maß μ ist invariant unter den Operationen aus Γ_n , das heißt, für jedes $M \in \Gamma_n$ und μ -messbares $V \subseteq \mathcal{H}_n$ ist auch $M \langle V \rangle$ messbar bezüglich μ mit $\mu(M \langle V \rangle) = \mu(V)$.

- (ii) Es gilt $\mu(\mathcal{F}) = \mu(\overset{\circ}{\mathcal{F}}) = 1$. $\diamond$

BEWEIS:

[Bra51] Satz III (S. 157) und Normierung □

Nun wird die bereits angekündigte Hauptaussage dieses Abschnitts formuliert und bewiesen.

3.4.7 SATZ: Es seien die Bezeichnungen aus 3.4.1 übernommen und $n \in \mathbb{N}$. Für jedes $M \in \Delta_n$ gibt es $M_1, \dots, M_k \in [M]$, so dass $\{M_1, \dots, M_k\}$ sowohl ein Vertretersystem von $\Gamma_n \backslash [M]$ als auch ein Vertretersystem von $[M] // \Gamma_n$ ist. ◇

BEWEIS:

Sei $M \in \Delta_n$ und $r = |\Gamma_n \backslash [M]|$ sowie $s = |[M] // \Gamma_n|$. Gemäß 1.1.3 gilt $r = |\Gamma_n \cap (M^{-1}\Gamma_n M) \backslash \Gamma_n|$, und mit einer leichten Modifikation des Beweises von 1.1.3 erhält man, dass analog $s = |\Gamma_n \cap (M\Gamma_n M^{-1}) \backslash \Gamma_n|$ gilt. Bilden nun $M_1, \dots, M_r \in \Gamma_n$ ein Vertretersystem der Nebenklassenmenge $\Gamma_n \cap (M^{-1}\Gamma_n M) \backslash \Gamma_n$, so ist nach 3.4.4 (a)

$$F := \bigcup_{i=1}^r M_i \langle \mathcal{F} \rangle$$

ein Fundamentalbereich von $\mathcal{H}_n$ zu $\Gamma_n \cap (M^{-1}\Gamma_n M)$, wenn $\mathcal{F}$ einen Fundamentalbereich von $\mathcal{H}_n$ zu Γ_n bezeichnet. Da die in der Definition von F auftretende Vereinigung mit dem invarianten Maß μ aus 3.4.6 nach 3.4.4 (a) bis auf Nullmengen disjunkt ist, folgt

$$\mu(F) = \sum_{i=1}^r \mu(M_i \langle \mathcal{F} \rangle) = \sum_{i=1}^r \mu(\mathcal{F}) = \sum_{i=1}^r 1 = r.$$

Analog folgt $\mu(F') = s$ wegen der Invarianz von μ für jeden Fundamentalbereich F' von $\mathcal{H}_n$ zu $\Gamma_n \cap (M\Gamma_n M^{-1})$. Da nach 3.4.5 $M \langle F \rangle$ ein solcher Fundamentalbereich ist, folgt wieder mit der Invarianz von μ , dass $s = \mu(M \langle F \rangle) = \mu(F) = r$ gilt. Somit zerfällt $[M]$ in gleichviele Rechts- wie Linksnebenklassen bezüglich Γ_n , also existiert nach 1.1.13 ein simultanes Vertretersystem. □

AUSBLICK

Eines der Hauptresultate des zweiten Kapitels war eine Formel zur Berechnung der Anzahl der in einer Doppelnebenklasse enthaltenen Rechtsnebenklassen für den Fall der Gruppe $GL_2(\mathfrak{o})$ (vergleiche 2.3.7). Als Verallgemeinerung kann die Frage untersucht werden, wie sich diese Anzahlen für $GL_n(\mathfrak{o})$ mit $n \geq 3$ berechnen lassen; eine solche Formel würde in Analogie zu 2.5.2 einen Algorithmus zur Berechnung konkreter Produkte in weiteren Hecke-Algebren liefern. Der Ansatz der expliziten Konstruktion von Normalformen wie in 2.3.2 erscheint dabei weniger zielführend zu sein. Vielversprechender stellt sich der Ansatz dar, die Mächtigkeit von Vertretersystemen über Lokalisierungen $\mathfrak{o}_{\mathfrak{p}}$ auszurechnen (was aufgrund der Struktur der Lokalisierungen einfacher möglich ist) und aus diesen einzelnen Kardinalitäten auf die Mächtigkeit des Vertretersystems über $\mathfrak{o}$ schließen zu wollen.

In diesem Zusammenhang bleibt auch noch zu untersuchen, ob die in 2.4.3 formulierte Vermutung über eine Verallgemeinerung des Reduktionssatzes (2.4.2) gültig ist. Ein Beweis könnte mit den Ideen oder den Ergebnissen aus der gerade angesprochenen Herleitung verallgemeinerter Maßformeln möglich sein.

Bei der Untersuchung von Erzeugendensystemen von Primärkomponenten im zweiten Kapitel spielte der neu eingeführte Begriff der unzerlegbaren Matrizen eine wichtige Rolle. In einigen Spezialfällen konnte eine geschlossene Beschreibung all dieser Matrizen angegeben

werden (2.8.11, 2.8.11, 2.8.13), eine generische Beschreibung wurde jedoch nicht gefunden. Als offenes Problem verbleibt somit das Finden einer solchen generischen Beschreibung oder zumindest die Analyse weiterer Spezialfälle.

Weitere Betrachtungen in diesem Bereich lieferten in einigen Spezialfällen das Ergebnis, dass die aus der Menge der unzerlegbaren Matrizen ableitbaren Erzeugendensysteme minimal sind (2.9.2). Zu beantworten bleibt die Frage, ob dies immer gilt. Ebenfalls in diesem Kontext wurde gezeigt, dass bestimmte minimale Erzeugendensysteme algebraisch abhängig sind (2.9.4, 2.9.5). In diesen Fällen kann noch untersucht werden, welchen Relationen die Erzeuger unterliegen.

Die im dritten Kapitel erhaltenen Ergebnisse über Hecke-Algebren zu unitären Gruppen werfen ebenfalls weitere offene Fragen auf. So konnte nicht allgemein geklärt werden, ob die Hecke-Algebren in dem hier betrachteten Fall stets kommutativ sind. Als Hilfsmittel zur Klärung dieser Frage könnte eine zum Determinantenteilerkriterium (2.2.5) analoge Charakterisierung von Doppelnebenklassen dienen; es wird vermutet, dass auch im Fall der unitären Gruppe die Überstimmung aller Determinantenteiler zur Gleichheit der zugehörigen Doppelnebenklassen äquivalent ist. Mit einem solchen Kriterium könnten wie im zweiten Kapitel Maßformeln, Reduktionssätze und Erzeugendensysteme hergeleitet werden.

Die Nichtexistenz einer Tensorproduktzerlegung im unitären Fall wurde bewiesen, indem gezeigt wurde, dass ein Tensorprodukt von Primärkomponenten nicht alle zur Erzeugung der gesamten Hecke-Algebra benötigten Basiselemente hätte (3.3.6). Noch offen ist die Frage, ob nicht als schwächere Aussage zumindest $[[L]] * [[M]] = [[LM]]$ für $L \in \Delta_n(l)$ und $M \in \Delta_n(m)$ mit teilerfremden $l, m \in \mathbb{N}$ gilt.

Weitere offene Fragen aus dem Bereich der Hecke-Theorie ergeben sich natürlich aus der Möglichkeit, neben den unimodularen und unitären Gruppen noch weitere Gruppen zu untersuchen.

LEBENS LAUF

PERSÖNLICHE DATEN

Name:	Marc Ensenbach
Geburtsdatum:	23. Juni 1979
Geburtsort:	Bocholt
Familienstand:	ledig
Staatsangehörigk.:	deutsch

SCHULBILDUNG

08.1985 – 07.1986	Josefschule, Bocholt
08.1986 – 06.1989	Biemenhorster Schule, Bocholt
08.1989 – 06.1998	St.-Georg-Gymnasium, Bocholt (Allgemeine Hochschulreife vom 3. Juni 1998)

ZIVILDIENTST

07.1998 – 07.1999	Fahrdienst an der Zivildienstschule Bocholt
-------------------	--

STUDIUM

10.1999 – 09.2001	Grundstudium Mathematik an der RWTH Aachen (Vordiplom vom 21. September 2001)
10.2002 – 02.2003	Grundstudium Informatik an der RWTH Aachen (Vordiplom vom 22. Februar 2003)
10.2001 – 06.2004	Hauptstudium Mathematik an der RWTH Aachen (Diplom vom 7. Juni 2004), Diplomarbeit zum Thema »Algebraische und maßtheoretische Strukturuntersuchungen in Hecke-Algebren«
06.2004 –	Promotionsstudium Mathematik an der RWTH Aachen (Betreuung der Arbeit durch Prof. Dr. A. Krieg, Lehrstuhl A für Mathematik)

TÄTIGKEITEN

10.2000 – 06.2004	Studentische Hilfskraft an den mathematischen Instituten der RWTH Aachen
06.2004 – 10.2004	Wissenschaftlicher Angestellter am Lehrstuhl A für Mathematik der RWTH Aachen
11.2004 – 10.2007	Stipendiat des Graduiertenkollegs »Hierarchie und Symmetrie in mathematischen Modellen«
11.2004 – 10.2007	Wissenschaftliche Hilfskraft am Lehrstuhl A für Mathematik der RWTH Aachen
11.2007 –	Wissenschaftlicher Angestellter am Lehrstuhl A für Mathematik der RWTH Aachen

LITERATURVERZEICHNIS

- [Ait69] Aitken, Alexander C.
Determinanten und Matrizen
B. I. Hochschultaschenbücher 293*
Bibliographisches Institut, Mannheim 1969
- [And87] Andrianov, Anatolij N.
Quadratic Forms and Hecke Operators
Grundlehren der mathematischen Wissenschaften 286
Springer-Verlag, Berlin · Heidelberg · New York 1987
- [Bra49] Braun, Hel
Hermitian Modular Functions
Ann. Math. (2) 50, S. 827–855 (1949)
- [Bra51] Braun, Hel
Hermitian Modular Functions. III
The Hermitian Modular Group
Ann. Math. (2) 53, S. 143–160 (1951)
- [Enso4] Ensenbach, Marc
*Algebraische und maßtheoretische Strukturuntersuchungen
in Hecke-Algebren*
Diplomarbeit RWTH Aachen 2004

- [Fra34] Franz, Wolfgang
Elementarteilertheorie in algebraischen Zahlkörpern
 J. Reine Angew. Math. 171, S. 149–161 (1934)

- [Fre83] Freitag, Eberhard
Siegelsche Modulfunktionen
 Grundlehren der mathematischen Wissenschaften 254
 Springer-Verlag, Berlin · Heidelberg · New York 1983

- [Hah89] Hahn, Alexander J.; O’Meara, O. Timothy
The Classical Groups and K-Theory
 Grundlehren der mathematischen Wissenschaften 291
 Springer-Verlag, Berlin · Heidelberg · New York 1989

- [Hei90] Heitkamp, Dieter
Hecke-Theorie zur $SL(2; \mathfrak{o})$
 Dissertation an der Universität Münster 1990

- [Kli56] Klingen, Helmut
Über die Erzeugenden gewisser Modulgruppen
 Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl.,
 Math.-Phys.-Chem. Abt. 1956, S. 173–183 (1956)

- [Koc97] Koch, Helmut
Zahlentheorie
Algebraische Zahlen und Funktionen
 Vieweg, Braunschweig · Wiesbaden 1997

- [Koe07] Koecher, Max; Krieg, Aloys
Elliptische Funktionen und Modulformen
 Springer-Verlag, Berlin · Heidelberg · New York 2007

- [Kri85] Krieg, Aloys
Modular Forms on Half-Spaces of Quaternions
 Lecture Notes in Mathematics 1143
 Springer-Verlag, Berlin · Heidelberg · New York 1985

- [Kri87] Krieg, Aloys
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions
 Proc. Indian Acad. Sci. (Math. Sci.) 97, No. 1–3,
 S. 201–229 (1987)
- [Kri90] Krieg, Aloys
Hecke algebras
 Memoirs of the American Mathematical Society 435
 American Mathematical Society, Providence 1990
- [Kru32] Krull, Wolfgang
Matrizen, Moduln und verallgemeinerte Abelsche Gruppen im Bereich der ganzen algebraischen Zahlen
 (Beitr. z. Algebra Nr. 19)
 Sitzungsber. Heidelberger Akad. Wiss. 1932 No. 2,
 S. 13–38 (1932)
- [Neu92] Neukirch, Jürgen
Algebraische Zahlentheorie
 Springer-Verlag, Berlin · Heidelberg · New York 1992
- [New72] Newman, Morris
Integral matrices
 Academic Press, London 1972
- [Red52] Rédei, László
Über die Determinantenteiler
 Acta Math. Acad. Sci. Hung. 3, S. 143–150 (1952)
- [Ste12] Steinitz, Ernst
Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. I
 Math. Ann. 71, S. 328–354 (1912)

SYMBOLVERZEICHNIS

In diesem Verzeichnis sind nur die »global« definierten Symbole aufgeführt. Die Auflösung weiterer Bezeichnungen ist jeweils in den Voraussetzungen der Aussage zu finden.

BUCHSTABENBASIERTE SYMBOLE

.adj	2.1.1	Adjunkte einer Matrix
$\mathbb{C}$		Menge der komplexen Zahlen
$\mathfrak{C}(K)$	1.2.1	Klassengruppe
$\mathfrak{d}_k(A)$	2.2.2	Determinantenteiler
$\det A$	2.1.1	Determinante einer Matrix
$\text{diag}(\dots)$	2.2.11	(Block-)Diagonalmatrix
$\mathfrak{e}_k(A)$	2.2.2	Elementarteiler
E_n	2.1.1	$(n \times n)$ -Einheitsmatrix
$\mathfrak{f}_k(A)$	2.2.2	Grundfaktor
$\text{GL}_n(\mathfrak{o})$	2.1.1	allgemeine lineare Gruppe
$h(K)$	1.2.1	Klassenzahl
$H(G, M, U)$	1.1.7	Hecke-Algebra
$\mathfrak{h}(K)$	1.2.1	Menge der Hauptideale $\neq \{0\}$
$\mathfrak{I}(K)$	1.2.1	Menge der gebrochenen Ideale
$\text{IL}_n(\mathfrak{o})$	2.1.1	Monoid der Matrizen $A \in \mathfrak{o}^{n \times n}$ mit $\det A \neq 0$
$\mathbb{N}$	1.1.4	Menge der natürlichen Zahlen $\{1, 2, \dots\}$
$\mathbb{N}_0$	2.1.1	Zahlenmenge $\mathbb{N} \cup \{0\} = \{0, 1, 2, \dots\}$

$N(\mathfrak{a})$	1.2.1	Norm eines Ideals
$N_o(\mathfrak{a})$	1.2.1	Norm eines Ideals
$\mathbb{Q}$		Menge der rationalen Zahlen
$\mathbb{R}$		Menge der reellen Zahlen
$\text{Rang } A$	2.1.1	Rang einer Matrix
$\mathfrak{S}(A)$	2.2.3	Spaltenklasse einer Matrix
$\cdot^T$	2.1.1	Transponierte einer Matrix
$\text{Tr } f$	1.1.8	Träger
$v_p(\mathfrak{a})$	1.2.4	Vielfachheit
$\mathbb{Z}$		Menge der ganzen Zahlen
$\mathfrak{Z}(A)$	2.2.3	Zeilenklasse einer Matrix

SONSTIGE BEZEICHNUNGEN

Ug	1.1.1	Rechtsnebenklasse
gU	1.1.1	Linksnebenklasse
UgU	1.1.1	Doppelnebenklasse
$U \parallel M$	1.1.1	Rechtsnebenklassensystem
$M \parallel U$	1.1.1	Linksnebenklassensystem
$U \parallel M \parallel U$	1.1.1	Doppelnebenklassensystem
$ M $	1.1.1	Kardinalität
$x :: \mathfrak{M}$	1.1.1	Durchlaufen eines Vertretersystems
$\mathfrak{a} \mid \mathfrak{b}$	1.2.1	$\mathfrak{a}$ teilt $\mathfrak{b}$
$\mathfrak{a} \nmid \mathfrak{b}$	1.2.1	$\mathfrak{a}$ teilt $\mathfrak{b}$ nicht
$\mathfrak{a} \parallel \mathfrak{b}$	1.2.1	$\mathfrak{a}$ ist echter Teiler von $\mathfrak{b}$
$\mathfrak{a}\mathfrak{S}(K)$	1.2.1	Idealklasse
$\mathfrak{o}^*$	1.2.1	Einheitengruppe
$\mathfrak{o}_{\mathfrak{M}}, \mathfrak{o}_p$	1.2.10	Lokalisierung
$\mathfrak{o}^{m \times n}$	2.1.1	Matrixring
$(A)_{IJ}$	2.1.1	Zeilen- und Spaltenauswahl einer Matrix
$A^{[k]}$	2.2.1	Ableitung einer Matrix
$A \trianglelefteq B, A \triangleleft B$	2.8.1	Relation zwischen Matrizen auf Basis der $\mathfrak{d}_k$
$f_{\mathfrak{a}}$	2.8.4	$\mathfrak{a}$ -harmonischer Teil von f

INDEX

- Ableitung, 43
- Algebra
 - Hecke-, 25
- algebraischer Zahlkörper, 31
- Algorithmus
 - zur DNK-Zerlegung, 79, 88
 - zur Produktberechnung, 78
- allgemeine lin. Gruppe, 24, 40
- Antiautomorphismus, 27, 47
- Assoziativität, 24
- chinesischer Restsatz, 34
- Dedekind-Ring, 30
- Determinantenteiler, 43, 95
 - Realisierbarkeit, 50, 97
- Doppelnebenklasse, 20
- echter Teiler, 30
- Einheitengruppe, 30
- Element
 - neutrales, 25
- Elementarteiler, 43, 95
 - Realisierbarkeit, 50
- Erzeugendensystem
 - algebraisch unabhängig, 138
 - minimal, 134
- Erzeuger
 - eines Ideals, 33
 - von $GL_2(\mathfrak{o})$, 81
 - von Hecke-Algebren, 119
- Faltung, 24
- Fundamentalebereich, 162
- ganzes Ideal, 29
- Ganzheitsring, 31
- gebrochenes Ideal, 29
- Größenrelation
 - im Det.teilersinne, 115
- größter gemeinsamer Teiler, 29
- Grundfaktor, 43
 - Realisierbarkeit, 50
- Gruppe
 - allgemeine lineare, 24, 40
 - unimodulare, 39
- Gruppenalgebra, 20
- Haar-Maß, 24
- harmonisch, 116
- harmonischer Teil, 116
- Hauptideal, 30

- Hauptidealring, 33, 35, 100, 160
- Hauptkongruenzgruppe, 41, 149
- Hecke-Algebra, 25
- Hecke-Tripel, 25, 41, 150
- Hermiteches Paar, 151
- Ideal
 - ganzes, 29
 - gebrochenes, 29
 - in $\mathfrak{o}$, 29
 - von K , 29
- Idealklasse, 30
- imag.-quadrat. Zahlkörper, 143
- Index, 41
- Indikatorfunktion, 20, 23
- Integritätsring, 29
- invariantes Maß, 164
- Kardinalität, 21
- Klassengruppe, 30
- Klassenzahl, 30
- Koeffizient, 27, 115
- Kommutativität, 28, 47, 160
- Linearkombination, 27
- Linksnebenklasse, 20
- Lokalisierung, 35, 103
- Maß, 24, 164
 - Haar-, 24
 - invariantes, 164
- Maßformel, 62, 67
- Matrixtransformation, 143
- minimales Erzeug.system, 134
- neutrales Element, 25
- Norm, 29
- Normalform, 51, 98
- normendlich, 29
- p -adische Zahl, 24
- Paar
 - Hermiteches, 151
- Primärkomponente, 109, 122
- Primideal, 30
- Primidealzerlegung, 31
- Quotientenkörper, 29
- Rechtsnebenklasse, 20
- Reduktionssatz, 76
- Restsatz
 - chinesischer, 34
- Ring
 - Dedekind-, 30
- simultanes Vertr.system, 28, 161
- Spaltenklasse, 44
- Teiler, 30
 - echter, 30
 - größter gemeinsamer, 29
- teilerfremd, 29
- Tensorprodukt, 108, 154
- Träger, 20, 25, 100
- Tripel
 - Hecke-, 25, 41, 150
- unimodulare Gruppe, 39
- unzerlegbar, 116

Vertretersystem, 21
 simultanes, 28, 161
 von Rechtsnebenkl., 54, 150

Vielfachheit, 31

Wohldefiniertheit, 41, 149

Zahl

p -adische, 24

Zahlkörper

 algebraischer, 31

 imaginär-quadratischer, 143

Zeilenklasse, 44

zerlegbar, 116