Ringe mit einer Theorie des größten gemeinsamen Teilers

Dissertation
zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultäten
der Georg-August-Universität zu Göttingen

vorgelegt von
Friedemann Lucius
aus Stade

Göttingen 1996

D 7
Referent: Prof. Dr. Eckart Maus
Korreferent: Prof. Dr. Ulrich Stuhler
Tag der mündlichen Prüfung: 30. Januar 1997

Inhaltsverzeichnis

Einleitung 2

1. Idealoperationen und Idealsysteme 7
1.1. Der Begriff der $*$-Idealoperation und des $*$-Idealsystems 7
1.2. $*$-Multiplikation und $*$-Invertierbarkeit von $*$-Idealen 10
1.3. $*$-prime und $*$-maximale $*$-Ideale 12

2. Ringe mit ggT-Theorie 15
2.1. Ringe mit ggT 15
2.2. Der Begriff des Ringes mit ggT-Theorie 16
2.3. Die Idealstruktur von Ringen mit ggT-Theorie 18
2.4. Ganzabgeschlossenheit und Multiplikativität des Inhalts 20
2.5. Die Konstruktion einer ggT-Theorie nach Kronecker 23
2.6. Verschiedene Charakterisierungen für Ringe mit ggT-Theorie 26
2.7. Der ganze Abschluß von Ringen mit ggT-Theorie 28

3. Ringe mit ggT-Theorie endlichen Typs 31
3.1. Das Axiom (G 2) und der Begriff des Ringes mit ggT-Theorie e. T. 32
3.2. Idealtheoretische Charakterisierung von Ringen mit ggT-Theorie e. T. 34
3.3. Divisorentheoretische Charakterisierung von Ringen mit ggT-Theorie e. T. 37
3.4. Der ganze Abschluß von Ringen mit ggT-Theorie e. T. 39
3.5. Der bewertungstheoretische Zugang 41

4. Der Begriff des „algebraischen Divisors“ bei Kronecker 44
4.1. Zur algebraischen Ausgangssituation bei Kronecker 45
4.2. Kroneckers Divisor- und Teilbarkeitsbegriff 47
4.3. „Algebraische Divisoren“ als größte gemeinsame Teiler von „algebraischen Grössen“ 52
4.4. Zu einem zeitgemäßen Verständnis des Kroneckerschen Divisorbegriffs 58
4.5. Dedekinds Ideale und Kroneckers Divisoren im Vergleich 64

Literaturverzeichnis 68

Einleitung

Das Grundproblem, von dem die Entwicklung der algebraischen Zahlentheorie im letzten Jahrhundert ihren Ausgang nahm, war die Frage nach der Zerlegbarkeit von Elementen in Primfaktoren. Dabei standen zunächst Zahlbereichserweiterungen über den ganzrationalen Zahlen, zunehmend aber auch allgemeinere Integritätsringe im Mittelpunkt des Interesses. Aus heutiger Sicht ging es darum, durch Einführung eines geeigneten Divisorensystems einen Ersatz für die i. a. fehlende Faktorialität zu schaffen.

Eine überaus suggestive axiomatische Beschreibung dieser Vorgehensweise stellt der Begriff eines *Ringes mit Divisorentheorie* dar, der in seiner ursprünglichen Definition nach Borewicz-Šafarevič folgende Gestalt hat:

> Wir sprechen von einer Divisorentheorie für den Ring [= Integritätsring] $\mathfrak{O}$, wenn eine Halbgruppe $\mathfrak{D}$ mit eindeutiger Primfaktorzerlegung und ein Homomorphismus $\alpha \to (\alpha)$ der Halbgruppe $\mathfrak{O}^*$ in $\mathfrak{D}$ mit folgenden Eigenschaften gegeben sind:
> 1°. Ein Element $\alpha \in \mathfrak{O}^*$ ist dann und nur dann durch $\beta \in \mathfrak{O}^*$ teilbar, wenn (α) durch (β) in $\mathfrak{D}$ teilbar ist.
> 2°. Wenn α und β aus $\mathfrak{O}^*$ durch ein $\mathfrak{a} \in \mathfrak{D}$ teilbar sind, so ist auch $\alpha \pm \beta$ durch $\mathfrak{a}$ teilbar.
> 3°. Seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Elemente aus $\mathfrak{D}$ mit der Eigenschaft, daß die Gesamtheit aller $\alpha \in \mathfrak{O}$, die durch $\mathfrak{a}$ teilbar sind, übereinstimmt mit der Gesamtheit aller $\beta \in \mathfrak{O}$, die durch $\mathfrak{b}$ teilbar sind. Dann ist $\mathfrak{a} = \mathfrak{b}$.[1]

Das erste Axiom stellt sicher, daß die Teilbarkeitseigenschaften des Integritätsringes $\mathfrak{O}$ in der Divisorenhalbgruppe $\mathfrak{D}$ treu wiedergegeben werden; Axiom 3° entspricht der Forderung, daß die Divisorenhalbgruppe $\mathfrak{D}$ minimal gewählt ist, also keine überflüssigen Divisoren enthält. Von dem zweiten Axiom — es besagt, daß die Vielfachen eines Divisors ein Ideal bilden — weiß man inzwischen, daß es aus den anderen beiden gefolgert werden kann und somit entbehrlich ist.[2]

In der Literatur hat sich für Ringe mit Divisorentheorie heutzutage die Bezeichnung *Krullbereich* eingebürgert.[3] Als solche sind sie relativ gut erforscht. Es gibt eine Vielzahl äquivalenter Charakterisierungen, man überblickt die Situation bei Ringerweiterungen (Polynomringe, Lokalisierungen, allgemeine Quotientenringe, ganzer Abschluß in endlichen Körpererweiterungen) und kennt, je nach methodischem Ansatz, unterschiedliche Beschreibungen der Divisorenhalbgruppe in Abhängigkeit vom betrachteten Grundring D.[4]

Es scheint historisch bedingt — genauer gesagt: dem übermächtigen Einfluß der Dedekindschen Idealtheorie zuzuschreiben — daß sich Untersuchungen über die Arithmetik in beliebigen Integritätsringen meistens an der Grundfrage der Primfaktorzerlegung orientieren oder zumindest in deren Umfeld einzuordnen sind. Dabei tritt oftmals in den Hintergrund, daß die Frage nach der Primfaktorzerlegung lediglich als Spezialfall einer sehr viel allgemeineren arithmetischen Eigenschaft anzusehen ist, nämlich der Existenz eines größten gemeinsamen Teilers.

Die Borewicz-Šafarevičsche Definition für Ringe mit Divisorentheorie eignet sich gut, um axiomatisch zu beschreiben, was es heißen soll, daß zwei Elemente eines Integritätsringes so etwas wie einen größten gemeinsamen Teiler besitzen: Man ersetze in der oben genannten Definition einfach den Begriff „Halbgruppe $\mathfrak{D}$ mit eindeutiger Primfaktorzerlegung“ durch „Monoid

---

[1] *Borewicz et al. 1966*, S. 189.

[2] *Skula 1970*, S. 119. Vgl. hierzu auch die Ergebnisse von Abschnitt 2.3, insbesondere Anmerkung 40, S. 19, sowie Korollar 2.7, S. 19.

[3] Krull war der erste, der Ringe mit Divisorentheorie im Rahmen seiner Arbeiten zur allgemeinen Bewertungstheorie untersucht und bewertungstheoretisch charakterisiert hat. Vgl. hierzu auch Abschnitt 3.5.

[4] Einen guten Überblick über Ringe mit Divisorentheorie/Krullbereiche verschafft *Bourbaki 1989*, Chapter VII.

(d. h. Halbgruppe mit Kürzungsregel) $\mathfrak{D}$ mit ggT“ und nenne den so definierten Integritätsbereich entsprechend *Ring mit ggT-Theorie*.

Offensichtlich handelt es sich hierbei um eine Verallgemeinerung der Ringe mit Divisorentheorie/Krullbereiche. Daß die Situation bei Ringen mit ggT-Theorie aber eine wesentlich andere ist, wird bereits deutlich, wenn man die multiplikative Struktur eines ggT-Monoiden genau unter die Lupe nimmt. Die bloße Existenz von Kürzungsregel und größtem gemeinsamen Teiler impliziert nämlich noch keineswegs die Existenz einer Zerlegung in *endlich viele* irreduzible Faktoren. Der Verzicht auf die eindeutige Primfaktorzerlegung in der Divisorenhalbgruppe $\mathfrak{D}$ bedeutet somit den Verzicht auf eine entscheidende Endlichkeitsvoraussetzung. Man muß sich zunächst an den Gedanken gewöhnen, daß es in Ringen mit ggT-Theorie unter Umständen Elemente gibt, deren zugehörige Hauptdivisoren durch beliebig hohe Divisorpotenzen teilbar sind.

In der vorliegenden Arbeit sollen Ringe mit ggT-Theorie näher untersucht werden. Welche Kriterien sind notwendig, welche hinreichend für die Existenz einer ggT-Theorie? Ist eine ggT-Theorie, sofern sie existiert, (bis auf Isomorphie) eindeutig bestimmt? Ist es möglich, die Elemente des ggT-Monoiden $\mathfrak{D}$, also die Divisoren, in kanonischer Weise zu konstruieren? Welche Eigenschaften eines Ringes mit ggT-Theorie bleiben bei Ringerweiterung erhalten? Besitzt der ganze Abschluß eines Ringes mit ggT-Theorie in einer algebraischen Körpererweiterung wieder eine ggT-Theorie?

Es erscheint naheliegend, sich diesen Fragen methodisch auf die gleiche Weise zu nähern wie bei den Ringen mit Divisorentheorie. Man macht allerdings bald die Erfahrung, daß sich die beiden am weitesten verbreiteten Ansätze, nämlich der bewertungstheoretische (auf Krull zurückgehende) und der idealtheoretische (auf Dedekind und Artin/van der Waerden zurückgehende)[5], nicht ohne weiteres auf die Situation der Ringe mit ggT-Theorie übertragen und verallgemeinern lassen. Bei einem dritten, heutzutage nur wenig beachteten Zugang scheint die Lage hingegen weniger hoffnungslos: Gemeint ist das auf Kronecker zurückgehende Verfahren zur expliziten Konstruktion einer Divisorentheorie.

In seiner Abhandlung „Grundzüge einer arithmetischen Theorie der algebraischen Grössen“[6] aus dem Jahre 1882 entwickelte Kronecker in bewußter Abgrenzung zur Dedekindschen Idealtheorie eine eigene Theorie der algebraischen Divisoren. Kronecker selbst beschrieb die Grundidee seines Ansatzes mit folgenden Worten:

> [. . .], dass mit jenen Divisoren das Gebiet der algebraischen Grössen, welche den Ausgangspunkt bilden, genügend erweitert wird, um den bei ganzen Zahlen und bei ganzen rationalen Funktionen von Variabeln geltenden einfachen Gesetzen der Theilbarkeit, welche beim Uebergang zu den ganzen algebraischen Grössen modifiziert werden, wiederum Raum zur vollen Wirksamkeit zu verschaffen.[7]

Mit den „ganzen rationalen Funktionen von Variabeln“ bezeichnete Kronecker Polynome über den ganzrationalen Zahlen $\mathbb{Z}$ in beliebig vielen Unbestimmten. Demzufolge verstand er unter „ganzen algebraischen Grössen“ auch nicht nur die ganzen Elemente aus dem algebraischen Abschluß der rationalen Zahlen $\mathbb{Q}$, sondern allgemeiner Elemente, die einer Ganzheitsbedingung über Polynomringen der Gestalt $\mathbb{Z}[X]$ ($X = \{X_i\}_{i \in I}$ beliebige Familie von Unbestimmten) genügten. Wie im Zitat bereits angedeutet, ging es Kronecker darum, die für die Grundringe $\mathbb{Z}$ bzw. $\mathbb{Z}[X]$ geltenden Teilbarkeitsalgorithmen — das vor allem ist mit den „einfachen Gesetzen der Teilbarkeit“ gemeint — in den ganzen Abschluß dieser Ringe hinüberzuretten. Dies gelingt im wesentlichen

[5] Zum bewertungstheoretischen Ansatz vgl. *Borewicz et al. 1966*, zum idealtheoretischen *Bourbaki 1989*.

[6] *Kronecker 1882*. Es handelt sich um eine Festschrift, die Kronecker anläßlich des 50-jährigen Doktorjubiläums seines Doktorvaters Kummer publizierte. In der Literatur wird auf diese Arbeit Kroneckers daher häufig unter der Bezeichnung „Kummer-Festschrift“ Bezug genommen.

[7] *Kronecker 1882*, S. 300.

durch die „Association neuer Grössengebilde“[8]: Durch Einbettung in einen geeigneten (nicht algebraischen) Erweiterungskörper von $\mathbb{Q}$ bzw. $\mathbb{Q}(X)$ macht Kronecker die ganzen Abschließungen von $\mathbb{Z}$ bzw. $\mathbb{Z}[X]$ zu Integritätsbereichen, in denen es ein Verfahren gibt, mit dessen Hilfe entschieden werden kann, ob eine (ganze) algebraische Größe durch eine andere teilbar ist oder nicht. Die Elemente dieser Erweiterungsringe sind genau die Kroneckerschen Divisoren. Ihr entscheidender Vorzug liegt Kronecker zufolge darin, daß sie „concrete algebraische Gebilde“ in „einfacher, übersichtlicher, naturgemässer Gestalt“ darstellen, die der „abstracten Eigenschaften“ der Kummerschen *idealen Zahlen* oder der Dedekindschen *Ideale* entbehren.

Aus heutiger Sicht, vor allem im Hinblick auf die hier zu behandelnde Thematik, kommt ein weiterer Punkt hinzu: Kroneckers Ansatz führt über den klassischen Dedekindschen auch insofern hinaus, als er im Grunde nicht so sehr auf eine Theorie der Primzerlegung, sondern vielmehr auf eine Theorie des größten gemeinsamen Teilers abzielt. Zumindest hat es im Laufe des 20. Jahrhunderts immer wieder Mathematiker gegeben, die Kroneckers arithmetische Theorie genau in diesem Sinne verstanden wissen wollten. Stellvertretend für diese Minderheit, sei in diesem Zusammenhang H. M. Edwards zitiert, der in der Einleitung zu seinem Buch „Divisor Theory“ schreibt:

> Today most mathematicians who know about Kronecker's theory of divisors know about it from having read Hermann Weyl's lectures on algebraic number theory [...], and regard it, as Weyl did, as an alternative to Dedekind's theory of ideals. Weyl's axiomatization of what he calls „Kronecker's“ theory is built — as Dedekind's theory was built — around unique factorization. However, in presenting the theory in this way Weyl overlooks one of Kronecker's most valuable ideas, namely, the idea that the objective of the theory is to define greatest common divisors, *not* to achieve factorization into primes. [9]

Wie kommen diese unterschiedlichen Interpretationen zustande? Es ist in erster Linie die Kroneckersche Darstellung selbst, die das Verständnis seiner Theorie so ungemein schwierig macht. Bis auf den heutigen Tag bleiben die Ausführungen an vielen Stellen undurchsichtig, ja fast kryptisch; hinzu kommen einige Fehler, zahlreiche Ungenauigkeiten und eine umständliche Syntax. Erschwerend kommt hinzu, daß leider auch das, was über oder in Anknüpfung an Kronecker geschrieben wurde, nur selten zur Klarheit beiträgt. Selbst die enthusiastischen Kronecker-Verehrer können in dieser Beziehung nicht halten, was sie versprechen.

Es fällt auf, daß die ersten 50 bis 60 Jahre nach Veröffentlichung der Kummer-Festschrift von jenen Mathematikern, die sich heutzutage mit Kronecker beschäftigen und auf ihn berufen, m. E. nicht ausreichend rezipiert werden. Ein möglicher Grund mag darin liegen, daß nicht wenige Mathematiker nach der Lektüre von Weyls „Algebraische Zahlentheorie“[10] darauf verzichtet haben, ältere Literatur zu Rate zu ziehen in dem Glauben, Weyl habe die Kroneckerschen Ideen adäquat erfaßt und in der bestmöglichen Weise dargestellt. Gerade diese Annahme bedeutet m. E. jedoch eine Fehleinschätzung; denn für eine wirklich klare Sicht der Dinge ist der Weylsche Beitrag noch allzusehr der Kroneckerschen Diktion verhaftet und nicht strukturell genug. Tatsächlich hat es vor Weyl bereits Mathematiker gegeben, deren Verständnis wesentlich tiefer ging, die jedoch nach dem ersten Erscheinen von Weyls Buch im Jahre 1940 offenbar nur noch schwer durchdringen konnten.

Den Schlüssel zu einem strukturellen Verständnis der Kroneckerschen Divisorentheorie liefert in meinen Augen eine Arbeit von Heinz Prüfer aus dem Jahre 1932. Sie trägt den Titel „Untersuchungen über Teilbarkeitseigenschaften in Körpern“ und setzt sich u. a. zum Ziel, „die zweite der klassischen Theorien der algebraischen Zahlen, die von Kronecker, in möglichster Allgemeinheit

[8] *Kronecker 1882*, S. 300.
[9] *Edwards 1990*, S. v.
[10] *Weyl 1966*; vgl. das oben angeführte Zitat von Edwards.

abstrakt“ darzustellen.[11] Diesem Anspruch werden die Ausführungen Prüfers tatsächlich in vollem Umfang gerecht. Doch worum geht es genau?

Prüfers Interesse galt allgemein den Teilbarkeitsverhältnissen in Körpern, die sich als Quotientenkörper von Integritätsringen darstellen lassen. Ein Körperelement α heißt dann durch ein anderes Körperelement β teilbar, wenn $\alpha\beta^{-1}$ ein *ganzes* Element, d. h. ein Element des zugrundeliegenden Integritätsringes, ist. Teilbarkeit in einem Körper meint immer Teilbarkeit in diesem Sinne, und Begriffe wie der des größten gemeinsamen Teilers, die zunächst nur für Ringelemente definiert sind, verallgemeinern sich entsprechend.

Nun hatten die Untersuchungen Dedekinds für den Fall algebraischer Zahlkörper gezeigt, daß es für Integritätsbereiche, in denen der Satz von der eindeutigen Primfaktorzerlegung nicht mehr gilt, unter Umständen Divisorensysteme gibt — bei Dedekind eben die Menge der Ideale — , die eine eindeutige Primzerlegung ermöglichen. Der Dedekindsche Idealbegriff ist allerdings für die Situation algebraischer Zahlkörper maßgeschneidert. I. a. liefert die Menge der (gebrochenen) Ideale eines Körpers *kein* geeignetes Divisorensystem. Lediglich wenn der Grundring ein Dedekindbereich ist, also die Ideale bzgl. der üblichen Idealmultiplikation eine Gruppe bilden, läßt sich die Situation übertragen. Für beliebige Integritätsringe ist die Dedekindsche Idealstruktur noch zu „fein“, um auf ihrer Grundlage eine allgemeine „Theorie der Primzerlegung“, geschweige denn eine allgemeine „Theorie der Teilbarkeit“ zu entwickeln.

Zur Lösung dieses Problems schlug Prüfer eine axiomatische Neufassung des Dedekindschen Idealbegriffs vor. Die Definition, so Prüfer, komme „darauf hinaus, daß gewisse Dedekindsche Ideale ausgezeichnet und nur diese betrachtet werden.“[12] Für den Auswahlprozeß wird lediglich die Gültigkeit einiger grundlegender Axiome gefordert. Auf diese Weise hält Prüfer sich die Möglichkeit zur Bildung einer Vielzahl unterschiedlicher sogenannter „Idealsysteme“ offen, unter denen das Dedekindsche Idealsystem nur als Spezialfall, nämlich als Idealsystem mit dem höchsten „Feinheitsgrad“, vorkommt. Damit gelingt es ihm nunmehr, Kriterien für bestimmte arithmetische Eigenschaften eines gegebenen Grundringes (bzw. seines Quotientenkörpers) sowie gewisser Erweiterungen herzuleiten.

Der unschätzbare Wert, den die Prüfersche Arbeit für die vorliegende Problemstellung hat, liegt jedoch darin, daß sie Kroneckers Divisorentheorie und Dedekinds Idealtheorie gewissermaßen auf einer höheren Ebene zusammenführt. Genauer gesagt: Mit Hilfe des verallgemeinerten Idealbegriffs deckt Prüfer die hinter der Kroneckerschen Theorie stehenden algebraischen Strukturen auf und macht diese dadurch transparent.

Ausgehend von einem (ganzabgeschlossenen) Grundring D mit Quotientenkörper K, beschreibt Prüfer das Kroneckersche Verfahren zur Konstruktion von Divisoren als Einbettung eben dieses Grundringes in einen Erweiterungsring, der genau jene Eigenschaft besitzt (z. B. eindeutige Primfaktorzerlegung, Existenz eines ggT), deren Vorhandensein man sich für den gegebenen Ring D wünscht. Vor allen anderen kommt Prüfer das Verdienst zu, diesen Erweiterungsring mit Hilfe seines neuen Idealbegriffs als ausgezeichneten Unterring des rationalen Funktionenkörpers $K(X)$ charakterisiert zu haben. Heutzutage werden Integritätsbereiche dieser Bauart auch als *Kroneckersche Funktionalringe* bezeichnet.[13]

Die Kroneckerschen Funktionalringe werden sich tatsächlich als Schlüsselobjekte erweisen, wenn es darum geht, für einen Ring D eine ggT-Theorie im oben definierten Sinne zu konstruieren. Im Grunde hat sich auch Prüfer mit diesem Problem bereits beschäftigt, dabei allerdings nur die Gültigkeit des ersten Borewicz-Šafarevičschen Axioms verlangt. Gerade das dritte Axiom ist

[11] *Prüfer 1932*, S. 2. Der letzte Paragraph dieser Untersuchung (§ 12) behandelt die Kroneckersche Theorie.

[12] *Prüfer 1932*, S. 1.

[13] Die Terminologie geht wohl auf Krull zurück. In der Prüferschen Arbeit kommt dieser Begriff noch nicht vor. Vgl. hierzu auch Abschnitt 2.5.

jedoch ein Stolperstein auf dem Weg zu einer allgemeinen Theorie des größten gemeinsamen Teilers. Zumindest verhindert es eine unmittelbare Übertragung der Prüferschen Ergebnisse auf den hier interessierenden Fall eines Ringes mit ggT-Theorie. Eine Hauptaufgabe der vorliegenden Arbeit besteht darin, eben diesen Stolperstein aus dem Wege zu räumen, was wesentlich zur Klarheit der Begriffsbildung beitragen wird.

Um eine in sich geschlossene Darstellung zu erreichen, wird im ersten Kapitel die Prüfersche Theorie der *Idealsysteme* bzw. *Idealoperationen* noch einmal zusammenfassend dargestellt und anhand der wichtigsten Beispiele erläutert. Im zweiten Kapitel wird der Begriff eines Ringes mit ggT-Theorie genauer untersucht. Insbesondere werden einige wichtige Aussagen über die Idealstruktur solcher Ringe bewiesen und in Anlehnung an die Kroneckersche Methode erläutert, wie sich die Divisoren einer ggT-Theorie explizit darstellen lassen. Außerdem wird gezeigt, daß der ganze Abschluß eines Ringes mit ggT-Theorie in einer algebraischen Körpererweiterung wieder eine ggT-Theorie besitzt. Im dritten Kapitel werden Ringe mit ggT-Theorie endlichen Typs — das sind Ringe mit ggT-Theorie, in denen jeder Divisor größter gemeinsamer Teiler von endlich vielen Hauptdivisoren ist — eingehend untersucht und ideal– sowie divisorentheoretisch charakterisiert. In diesem Zusammenhang gehen wir außerdem auf Ringe mit Divisorentheorie als Spezialfall der Ringe mit ggT-Theorie näher ein. Das letzte Kapitel schließlich stellt den Versuch dar, jene Passagen der Kummer-Festschrift, in denen Kronecker den Begriff des „algebraischen Divisors“ entwickelt, mit Hilfe der Ergebnisse der vorangegangenen Kapitel zeitgemäß darzustellen und einem tieferen Verständnis zugänglich zu machen.

Die vorliegende Arbeit entstand im Rahmen eines von der Deutschen Forschungsgemeinschaft geförderten Projekts an der Universität Göttingen. Für die gewährte finanzielle Unterstützung bin ich der Deutschen Forschungsgemeinschaft zu großem Dank verpflichtet. Außerdem möchte ich all jenen Menschen danken, die mir bei der Fertigstellung meiner Dissertation geholfen haben. Mein besonderer Dank gilt M. Denker, von dem die Initiative zu dieser Arbeit ausging, U. Stuhler, der sich selbstlos für meine Förderung durch die Deutsche Forschungsgemeinschaft eingesetzt hat, sowie vor allem meinem Lehrer E. Maus, der die Themenstellung angeregt und mit seinem beständigen Interesse sowie seiner betreuerischen Erfahrung wesentlich zum Gelingen der Arbeit beigetragen hat. Sein kritischer Blick hat mich vor zahlreichen gedanklichen und begrifflichen Ungenauigkeiten bewahrt. Viele Gespräche mit R. Haubrich haben mir geholfen, Probleme deutlicher zu erkennen und die Gedankenführung zu schärfen. Auch ihm sei hierfür gedankt. Ohne den Rückhalt meiner Familie, insbesondere das liebevolle Verständnis, das meine Frau Katja für die wöchentliche räumliche Trennung und andere damit verbundene Unannehmlichkeiten gezeigt hat, hätte ich diese Arbeit nicht so schnell zum Abschluß bringen können. Ich danke ihr von ganzem Herzen.

Göttingen, im Dezember 1996 *Friedemann Lucius*

Kapitel 1

Idealoperationen und Idealsysteme

1.1. Der Begriff der $*$-Idealoperation und des $*$-Idealsystems

Im folgenden sei D stets ein Integritätsbereich mit Quotientenkörper K. Für die multiplikative Halbgruppe von D schreiben wir D^*, für die multiplikative Gruppe von K entsprechend K^*. $D^\times$ stehe für die Einheitengruppe von D. In Anlehnung an die englischsprachige Literatur bezeichne $\mathsf{F}(D)$ die Menge *aller*, $\mathsf{f}(D)$ die Menge aller *endlich erzeugten* gebrochenen D-Ideale. Für Ideale (bzw. Divisoren) verwenden wir die klassische Notation der deutschen Frakturbuchstaben.

Am Anfang steht die Definition der grundlegenden, auf Prüfer und Krull zurückgehenden Begriffe.[14]

Definition 1.1. *Eine Abbildung*

$$\begin{aligned}(\cdot)_* : \mathsf{F}(D) &\longrightarrow \mathsf{F}(D)\\ \mathfrak{a} &\longmapsto \mathfrak{a}_* := (\mathfrak{a})_*\end{aligned}$$

heißt ***$*$-Idealoperation*** *von D (sprich: „Stern-Idealoperation“)*[15]*, wenn sie folgende Bedingungen erfüllt:*

(I 1) $(\mathfrak{a}_*)_* = \mathfrak{a}_*$.

(I 2) $\mathfrak{a} \subseteq \mathfrak{a}_*$*, und es gilt* $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow \mathfrak{a}_* \subseteq \mathfrak{b}_*$.

(I 3) $(\alpha)_* := (\alpha D)_* = \alpha D$ *und* $(\alpha\mathfrak{a})_* = \alpha\mathfrak{a}_*$ *für alle* $\alpha \in K^*$.

Das Bild eines ganzen bzw. gebrochenen D-Ideals $\mathfrak{a}$ unter der $*$-Idealoperation $(\cdot)_*$ heißt das ***zu*** *$\mathfrak{a}$* ***gehörige*** *ganze bzw. gebrochene* ***$*$-Ideal****. Ein D-Ideal $\mathfrak{a}$ mit $\mathfrak{a} = \mathfrak{a}_*$ wird auch* ***$*$-Ideal*** *genannt. Die Urbilder eines $*$-Ideals $\mathfrak{a} = \mathfrak{a}_*$ heißen* ***$*$-erzeugende Ideale*** *von $\mathfrak{a}$. Das $*$-Ideal $\mathfrak{a}$ heißt* ***$*$-endlich****, wenn es ein endlich erzeugtes Ideal $\mathfrak{b} \in \mathsf{f}(D)$ mit $\mathfrak{a} = \mathfrak{b}_*$ gibt.*[16] *Die Menge aller $*$-Ideale heißt* ***$*$-Idealsystem*** *von D und wird mit $\mathsf{F}_*(D)$ bezeichnet. Betrachtet man nur $*$-endliche Ideale, so spricht man genauer von dem* ***Idealsystem der $*$-endlichen $*$-Ideale*** *$\mathsf{f}_*(D)$.*

Genau genommen bilden die $*$-Ideale nichts anderes als ein ausgezeichnetes Repräsentantensystem der Äquivalenzrelation „$\sim$“, die von der $*$-Idealoperation $(\cdot)_*$ auf der Menge der gebrochenen Ideale $\mathsf{F}(D)$ vermöge

$$\mathfrak{a} \sim \mathfrak{b} \quad :\Leftrightarrow \quad \mathfrak{a}_* = \mathfrak{b}_*$$

induziert wird.

Die einfachste aller denkbaren Idealoperationen ist die Identität auf den gebrochenen D-Idealen. Die Menge aller gebrochenen bzw. aller endlich erzeugten D-Ideale wird — vermutlich zu Ehren Dedekinds — auch als *d-Idealsystem* $\mathsf{F}_d(D)$ bzw. als System der d-endlichen d-Ideale $\mathsf{f}_d(D)$ bezeichnet, um sie mit anderen $*$-Idealsystemen besser vergleichen zu können. Unter allen $*$-Idealsystemen besitzt das d-Idealsystem die feinste Struktur.

---

[14] Die Begriffsbildungen und Ergebnisse dieses Kapitels sind, von einigen Ausnahmen abgesehen (vgl. Anmerkung 21), weitgehend der einschlägigen Literatur entnommen. Hauptquelle sind die Werke „Multiplicative Ideal Theory“ von Gilmer (dort vor allem §32), 1992 bei Queen's Papers im Nachdruck erschienen, und „Les Systèmes d'Idéaux“ von Jaffard aus dem Jahre 1960 (dort vor allem Chapitre I).

[15] Die Bezeichnung $*$-Idealoperation geht auf *Krull 1936a*, S. 556, zurück, der allerdings die Kennzeichnung „$'$“ benutzt, um die gewöhnlichen von den $*$-Idealen zu unterscheiden. Die $*$-Notation hat sich heutzutage (vor allem in der englischsprachigen Literatur, wo von sogenannten „*star-operations*“ die Rede ist) gegenüber der Krullschen sowie der Prüferschen Kennzeichnung mit dem Indexbuchstaben „r“ durchgesetzt.

[16] Man beachte: Wenn $\mathfrak{a}$ ein endlich erzeugtes D-Ideal ist, so muß das zugehörige $*$-Ideal $\mathfrak{a}_*$ keineswegs mehr ein endlich erzeugtes D-Ideal sein.

Definition 1.2. *Sei $\mathfrak{a}$ ein gebrochenes D-Ideal in K. Dann heißt*

$$\mathfrak{a}_v := \bigcap_{\substack{\mu \in K^* \\ \mathfrak{a} \subseteq \mu D}} \mu D$$

*das zu $\mathfrak{a}$ gehörige v-**Ideal**.*[17]

Man zeigt, daß die v-Ideale eines Integritätsbereiches D ein Idealsystem bilden, das sogenannte v-*Idealsystem* $\mathsf{F}_v(D)$. Es besitzt unter allen $*$-Idealsystemen die gröbste Struktur. Denn ist $\mathfrak{a}$ ein beliebiges D-Ideal, $\mathfrak{a}_*$ sein zugehöriges $*$-Ideal unter irgendeiner $*$-Idealoperation, so ist für ein $\mu \in K^*$ aufgrund der Axiome (I 2) und (I 3) die Aussage $\mathfrak{a} \subseteq \mu D$ äquivalent zu $\mathfrak{a}_* \subseteq \mu D$. Daraus folgt jedoch $(\mathfrak{a}_*)_v = \mathfrak{a}_v$, also $\mathfrak{a}_* \subseteq \mathfrak{a}_v$. Nicht zuletzt aufgrund dieser Eigenschaft ist das v-Idealsystem zusammen mit dem d-Idealsystem das wohl wichtigste Idealsystem überhaupt.

In der Literatur werden die v-Ideale bisweilen auch in der bequemen *Idealquotienten*-Schreibweise eingeführt. Ist $(\mathfrak{b} : \mathfrak{a}) = \{\mu \in K : \mu\mathfrak{a} \subseteq \mathfrak{b}\}$ und verwendet man für $(D : \mathfrak{a})$ die ebenfalls gebräuchliche Notation $\mathfrak{a}^{-1}$, dann wird häufig auch $\mathfrak{a}_v := (D : (D : \mathfrak{a})) = (\mathfrak{a}^{-1})^{-1}$ das zu $\mathfrak{a}$ gehörige v-Ideal genannt. Man zeigt jedoch, daß beide Definitionen völlig gleichwertig sind.[18] Als Folgerung ergibt sich, daß für jedes gebrochene D-Ideal $\mathfrak{a}$ stets $\mathfrak{a}^{-1} = \left((\mathfrak{a}^{-1})^{-1}\right)^{-1} = (\mathfrak{a}^{-1})_v$ gilt, also $\mathfrak{a}^{-1}$ stets ein v-Ideal ist.[19]

Der Gedanke, aus einem bestehenden $*$-Idealsystem ein neues Idealsystem herzuleiten, erscheint naheliegend.

Definition 1.3. *Sei $\mathfrak{a}$ ein gebrochenes D-Ideal und $(\cdot)_*$ eine beliebige Idealoperation von D. Dann heißt*

$$\mathfrak{a}_{*_s} = \bigcup_{\substack{\mathfrak{e} \in \mathfrak{f}(D) \\ \mathfrak{e} \subseteq \mathfrak{a}}} \mathfrak{e}_*$$

*das zu $\mathfrak{a}$ gehörige $*_s$-**Ideal**.*

Für die Menge der $*_s$-Ideale weist man ohne Schwierigkeiten die Axiome (I 1) – (I 3) nach. Idealsysteme bzw. Idealoperationen, die sich auf diese Weise aus einem $*$-Idealsystem herleiten lassen, heißen mit Lorenzen auch *endlichartig*.[20]

Aus der Definition der $*_s$-Ideale geht hervor, daß das Idealsystem der $*$-endlichen $*$-Ideale und das zugehörige Idealsystem der $*_s$-endlichen $*_s$-Ideale stets miteinander identisch sind. Darüber hinaus stellt man fest, daß d-Idealsystem und d_s-Idealsystem vollkommen übereinstimmen.

---

[17] Der Begriff des v-Ideals geht auf Prüfer zurück. In der Literatur werden v-Ideale mit *Bourbaki 1989*, S. 476, bisweilen auch als *divisorielle Ideale* („*divisorial ideals*“, „*idéaux divisoriels*“) bezeichnet. Anschaulich gesagt, ist das zu $\mathfrak{a}$ gehörige v-Ideal $\mathfrak{a}_v$ ein gebrochenes D-Ideal, das genau aus den gemeinsamen Vielfachen der gemeinsamen Teiler von allen Elementen aus $\mathfrak{a}$ besteht. Denn die Bedingung „$\mathfrak{a} \subseteq \mu D$“ läßt sich ja auch schreiben als „$\mu^{-1}\alpha \in D$ für alle $\alpha \in \mathfrak{a}$“, was bedeutet, daß μ alle Elemente aus $\mathfrak{a}$ teilt. Genau so findet sich die Definition bei *Prüfer 1932*, S. 18, dort allerdings nur für den Fall, daß das Ideal $\mathfrak{a}$ endlich erzeugt ist.

[18] Siehe *Jaffard 1960*, S. 19, Théorème 1.

[19] Siehe *Jaffard 1960*, S. 20, Corollaire zu Théorème 1. Etwa zeitgleich mit Prüfer führten Artin/van der Waerden die sogenannte *Quasigleichheitsrelation* für gebrochene Ideale ein. Dabei heißen nach *van der Waerden 1967*, S. 194, zwei gebrochene D-Ideale $\mathfrak{a}$ und $\mathfrak{b}$ *quasigleich*, wenn $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ gilt. Da diese Bedingung wiederum äquivalent zu $\mathfrak{a}_v = \mathfrak{b}_v$ ist, ist die Quasigleichheitsrelation nichts anderes als jene Äquivalenzrelation, die von der v-Idealoperation in der oben beschriebenen Weise auf der Menge der gebrochenen D-Ideale induziert wird. Beide Ansätze wurden offenbar unabhängig voneinander entwickelt. Dies geht aus einer Anmerkung bei *Prüfer 1932*, S. 18, hervor, in der auf die Darstellung bei van der Waerden verwiesen wird. Die Anmerkung ist ausdrücklich als „Zusatz bei der Korrektur“ gekennzeichnet.

[20] *Lorenzen 1939*, S. 540. Die in der englischsprachigen Literatur verbreitete Terminologie „*ideal system of finite character*“ ist m. E. nicht ganz glücklich, da es leicht zu Verwechslungen mit dem ebenfalls gebräuchlichen Begriff „*ideal system of finite type*“ kommen kann, mit dem die Idealsysteme $*$-endlicher $*$-Ideale bezeichnet werden.

Eine besondere Rolle unter den $*_s$-Idealsystemen spielt das v_s-Idealsystem, auch t-*Idealsystem* genannt. Das t-Idealsystem ist das gröbste endlichartige Idealsystem überhaupt und wird sich im weiteren Verlauf als Schlüsselobjekt erweisen.

Eine zweite Möglichkeit, aus einem gegebenen $*$-Idealsystem ein neues zu konstruieren, liefert die sogenannte *Spuridealoperation*. Dazu folgende Vorüberlegung. In der Einleitung wurde bereits angedeutet, daß Kroneckers Verfahren zur Konstruktion einer Divisorentheorie im wesentlichen darin besteht, den zu untersuchenden Grundring D in einen Erweiterungsring T (mit eindeutiger Primfaktorzerlegung, mit ggT) einzubetten und dessen Elemente als Divisoren der Elemente von D aufzufassen. Dabei muß man an die Ringerweiterung die grundlegende Forderung stellen, daß die Teilbarkeitsrelation auf T mit der Teilbarkeitsrelation auf D verträglich ist, oder anders gesagt: Wenn K der Quotientenkörper von D und L der Quotientenkörper von T ist, dann darf ein $\alpha \in K^*$ bzgl. D dann und nur dann durch ein $\beta \in K^*$ teilbar sein, wenn es auch bzgl. T durch β teilbar ist. Wie man sich leicht klarmacht, ist dazu wiederum die Forderung $T \cap K = D$ äquivalent. Genau dieser Situation werden wir im Verlauf der vorliegenden Untersuchung an mehreren Stellen begegnen.

Satz und Definition 1.4. *Seien D ein Integritätsbereich mit Quotientenkörper K und T ein Erweiterungsring von D mit Quotientenkörper L derart, daß $T \cap K = D$ gilt. Auf T sei ein beliebiges $*$-Idealsystem $\mathsf{F}_*(T)$ gegeben. Dann ist die Abbildung*

$$\begin{aligned}(\cdot)_{*_p} : \mathsf{F}(D) &\longrightarrow \mathsf{F}(D)\\ \mathfrak{a} &\longmapsto \mathfrak{a}_{*_p} := (\mathfrak{a}T)_* \cap K\end{aligned}$$

*eine Idealoperation von D, die sogenannte $*_p$-**Idealoperation** oder auch $*$-**Spuridealoperation** von D bzgl. $\mathsf{F}_*(T)$. Das Idealsystem der $*_p$-Ideale heißt auch $*$-**Spuridealsystem** von D bzgl. $\mathsf{F}_*(T)$, das zu $\mathfrak{a} \in \mathsf{F}(D)$ gehörige $*_p$-Ideal auch $*$-**Spurideal** von $\mathfrak{a}$ bzgl. $\mathsf{F}_*(T)$.*[21]

Die Axiome (I 1) – (I 3) prüft man ohne Schwierigkeiten nach. Der Zusammenhang zwischen einer Idealoperation $(\cdot)_*$ von T, ihrer zugehörigen endlichartigen Idealoperation $(\cdot)_{*_s}$ sowie den entsprechenden Spuroperationen von D wird durch folgenden Satz beschrieben. Er besagt im wesentlichen, daß $*_p$-Idealbildung und $*_s$-Idealbildung miteinander vertauschbar sind.

Satz 1.5. *Seien $(\cdot)_*$ eine Idealoperation von T, $(\cdot)_{*_s}$ die von ihr induzierte endlichartige Idealoperation und $(\cdot)_{*_p}$ bzw. $(\cdot)_{*_{s_p}}$ die zugehörigen Spuroperationen auf D. Dann ist $(\cdot)_{*_{p_s}}$ die von $(\cdot)_{*_p}$ induzierte endlichartige Idealoperation auf T, d. h. für ein beliebiges gebrochenes D-Ideal $\mathfrak{a}$ gilt $\mathfrak{a}_{*_{s_p}} = \mathfrak{a}_{*_{p_s}}$.*

Beweis: Der Satz ergibt sich unmittelbar aus den Definitionen für $*_p$- und $*_s$-Ideale:

$$\mathfrak{a}_{*_{s_p}} = K \cap \bigcup_{\substack{\mathfrak{e}\in \mathsf{f}(T),\\ \mathfrak{e}\subseteq \mathfrak{a}T}} \mathfrak{e}_* = \bigcup_{\substack{\mathfrak{e}\in \mathsf{f}(D),\\ \mathfrak{e}\subseteq \mathfrak{a}}} (\mathfrak{e}T)_* \cap K = \bigcup_{\substack{\mathfrak{e}\in \mathsf{f}(D),\\ \mathfrak{e}\subseteq \mathfrak{a}}} \mathfrak{e}_{*_p} = \mathfrak{a}_{*_{p_s}}. \qquad \square$$

[21] Spurideale kommen, soweit ich sehe, erstmals bei *Jaffard 1960*, S. 52ff., vor (dort heißen sie „*empreintes d'un système d'idéaux*“). Ansonsten tauchen sie in der Literatur meines Wissens nur noch bei *Aubert 1983* auf. Beide Autoren sind im wesentlichen an rein multiplikativen Strukturen interessiert, d. h. ihre Untersuchungsgegenstände sind nicht Integritätsbereiche und deren Quotientenkörper, sondern (multiplikative) Monoide und deren Quotientengruppen. Für diese entwickelt vor allem Jaffard, in Anlehnung an die in dieser Hinsicht grundlegende Dissertation von *Lorenzen 1939*, eine rein multiplikative Idealtheorie, deren Ergebnisse sich weitgehend auch auf Integritätsbereiche übertragen lassen. In einem rein ringtheoretischen Kontext sind mir Spurideale bislang noch nicht begegnet. Insbesondere Satz 1.12 im nächsten Abschnitt ist in dieser Form in der Literatur (*Jaffard 1960* und *Aubert 1983* eingeschlossen) nicht zu finden. Die Bezeichnung $*_p$-Ideale („p“ für „Projektion“) wurde von mir gewählt, um die Einheitlichkeit der Terminologie zu wahren.

Mit Satz 1.5 weiß man zwar, daß das Spursystem eines endlichartigen Idealsystems auf T wieder endlichartig ist. Dies bedeutet aber beispielsweise im konkreten Fall der t-Idealoperation noch lange nicht, daß die Spurideale ebenfalls wieder t-Ideale sind.

1.2. $*$-Multiplikation und $*$-Invertierbarkeit von $*$-Idealen

Aufgrund von Axiom (I 2) bilden die Ideale eines beliebigen $*$-Idealsystems (sei es $*$-endlich oder nicht) bzgl. Inklusion eine teilweise geordnete Menge. Damit ist allerdings noch nicht viel gewonnen, solange auf $\mathsf{F}_*(D)$ keine Verknüpfung definiert ist.

Definition 1.6. *Es seien $(\cdot)_*$ eine beliebige $*$-Idealoperation von D und $\mathfrak{a}, \mathfrak{b} \in \mathsf{F}_*(D)$ zwei $*$-Ideale, die von den gebrochenen D-Idealen $\mathfrak{a}'$ bzw. $\mathfrak{b}'$ erzeugt werden, d. h. $\mathfrak{a} = \mathfrak{a}_* = (\mathfrak{a}')_*$, $\mathfrak{b} = \mathfrak{b}_* = (\mathfrak{b}')_*$. Dann wird auf dem System der $*$-Ideale $\mathsf{F}_*(D)$ eine $*$-Multiplikation „$\times$“ definiert vermöge $\mathfrak{a}_* \times \mathfrak{b}_* := (\mathfrak{a}' \cdot \mathfrak{b}')_*$.*[22] *Das $*$-Ideal $\mathfrak{a}_*$ heißt durch das $*$-Ideal $\mathfrak{b}_*$ **$*$-teilbar** oder teilbar bzgl. der $*$-Multiplikation — in Zeichen: $\mathfrak{a}_* \mid \mathfrak{b}_*$ —, wenn ein ganzes D-Ideal $\mathfrak{g}_*$ mit $\mathfrak{a}_* \times \mathfrak{g}_* = \mathfrak{b}_*$ existiert.*

Die $*$-Multiplikation macht jedes $*$-Idealsystem zu einer (bzgl. Inklusion teilweise geordneten) Halbgruppe mit dem Einheitsideal $(1)_* = D$ als Einselement. Von besonderem Interesse sind jene $*$-Ideale, die in dieser Halbgruppe ein Inverses besitzen.

Definition 1.7. *Existiert zu einem beliebigen gebrochenen D-Ideal $\mathfrak{a}$ (das nicht als $*$-Ideal vorausgesetzt werden muß) ein gebrochenes D-Ideal $\mathfrak{b}$ mit $\mathfrak{a}_* \times \mathfrak{b}_* = (1)_* = D$, so heißt $\mathfrak{a}$ **$*$-invertierbar** und das zu $\mathfrak{b}$ gehörige $*$-Ideal $\mathfrak{b}_*$ das **$*$-Inverse** zu $\mathfrak{a}$.*

Mit diesen Bezeichnungen erhält man folgendes Lemma, bei dem es sich um eine Verallgemeinerung jener aus der algebraischen Zahlentheorie vertrauten Formel handelt, nach der „Teilbarkeit“ von Idealen nichts anderes bedeutet als „Enthaltensein“.

Lemma 1.8. *Seien $\mathfrak{a}, \mathfrak{b}$ zwei gebrochene D-Ideale und $(\cdot)_*$ eine beliebige $*$-Idealoperation von D. Dann folgt aus $\mathfrak{a}_* \mid \mathfrak{b}_*$ stets $\mathfrak{b}_* \subseteq \mathfrak{a}_*$. Ist $\mathfrak{a}$ zudem $*$-invertierbar, so ist auch die Umkehrung richtig: $\mathfrak{a}_* \mid \mathfrak{b}_* \Leftrightarrow \mathfrak{b}_* \subseteq \mathfrak{a}_*$.*

Beweis: Wegen $\mathfrak{a}_* \mid \mathfrak{b}_*$ existiert ein ganzes D-Ideal $\mathfrak{g}$ mit $\mathfrak{b}_* = (\mathfrak{a}_* \cdot \mathfrak{g}_*)_* \subseteq (\mathfrak{a}_* D)_* = \mathfrak{a}_*$. Damit ist die erste Aussage klar. Für die Implikation „$\Leftarrow$“ der zweiten Aussage sei $\mathfrak{b}_* \subseteq \mathfrak{a}_*$. Aufgrund der $*$-Invertierbarkeit von $\mathfrak{a}$ existiert ein $*$-Ideal $\mathfrak{a}'_*$ mit $\mathfrak{a}_* \times \mathfrak{a}'_* = D$. Damit ist aber das $*$-Ideal $\mathfrak{b}_* \times \mathfrak{a}'_* \subseteq \mathfrak{a}_* \times \mathfrak{a}'_* = D$ ganz, und man erhält $\mathfrak{b}_* = \mathfrak{b}_* \times (\mathfrak{a}_* \times \mathfrak{a}'_*) = (\mathfrak{b}_* \times \mathfrak{a}'_*) \times \mathfrak{a}_*$, d. h. $\mathfrak{b}_*$ ist durch $\mathfrak{a}_*$ $*$-teilbar. □

In der Dedekindschen Idealtheorie hat man sich daran gewöhnt, daß das Inverse eines endlich erzeugten Ideals stets wieder ein endlich erzeugtes Ideal ist. In beliebigen $*$-Idealsystemen gilt eine entsprechende Aussage nicht. So ist nicht auszuschließen, daß ein $*$-endliches $*$-Ideal zwar $*$-invertierbar, das $*$-Inverse jedoch nicht mehr $*$-endlich ist. Für $*_s$-Idealsysteme, also für endlichartige Idealsysteme, bleibt diese Aussage aber richtig.

Satz 1.9. *Gegeben sei eine endlichartige $*$-Idealoperation von D. Ist das gebrochene D-Ideal $\mathfrak{a}$ $*$-invertierbar, so ist das $*$-Inverse von $\mathfrak{a}$ (und damit auch $\mathfrak{a}_*$) ein $*$-endliches $*$-Ideal, d. h. es existiert ein endlich erzeugtes D-Ideal $\mathfrak{b}$ mit $\mathfrak{a}_* \times \mathfrak{b}_* = (\mathfrak{a}\mathfrak{b})_* = D$. Insbesondere ist also jedes $*$-invertierbare $*$-Ideal $*$-endlich.*[23]

[22] „ $\cdot$ “ bezeiche die übliche Idealmultiplikation mit $\mathfrak{a} \cdot \mathfrak{b} = \{\alpha_1\beta_1 + \ldots + \alpha_n\beta_n \in K : \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}, n \in \mathbb{N}\}$. Man zeigt, daß die Definition der $*$-Multiplikation wohldefiniert ist, also nicht von der Wahl der $*$-erzeugenden Ideale $\mathfrak{a}'$ und $\mathfrak{b}'$ abhängt. Siehe *Gilmer 1992*, S. 393, Proposition 32.2.(c).

[23] Siehe *Jaffard 1960*, S. 30, Théorème 8.

Wenn es um Strukturaussagen über endlichartige Idealsysteme geht, ist Satz 1.9 von nicht zu unterschätzender Wichtigkeit. Ist nämlich bekannt, daß sämtliche $*_s$-Ideale eines gegebenen $*_s$-Systems $*_s$-invertierbar sind, so weiß man, daß es für jedes $*_s$-Ideal ein endliches $*_s$-Erzeugendensystem gibt und somit die $*_s$-Ideale ein Gruppe bzgl. der $*_s$-Multiplikation bilden, die mit der Gruppe der $*_s$-endlichen $*_s$-Ideale $\mathfrak{f}_{*_s}(D)$ übereinstimmt. Das folgende Lemma impliziert sogar, daß dann auch die t-Ideale bzgl. der t-Multiplikation eine Gruppe bilden und $*_s$- und t-Idealsystem miteinander identisch sind.

Lemma 1.10. *Es sei $(\cdot)_*$ eine beliebige $*$-Idealoperation von D. Ist das gebrochene D-Ideal $\mathfrak{a}$ $*$-invertierbar mit $\mathfrak{a}_* \times \mathfrak{b}_* = D$, $\mathfrak{b} \in \mathfrak{F}(D)$, so folgt*

$$\mathfrak{b}_* = \mathfrak{a}^{-1} = (\mathfrak{a}_*)^{-1} \quad \textit{und} \quad \mathfrak{a}_* = \mathfrak{b}^{-1} = (\mathfrak{b}_*)^{-1}.$$

Insbesondere sind $\mathfrak{a}_*$ und $\mathfrak{b}_*$ v-Ideale von D.[24]

Alle $*$-invertierbaren $*$-Ideale sind also v-Ideale. Falls die Idealoperation $(\cdot)_*$ darüber hinaus endlichartig ist, werden aufgrund von Satz 1.9 die $*$-invertierbaren $*$-Ideale zu $*$-endlichen $*$-Idealen, also — wegen $\mathfrak{a}_v = \mathfrak{a}_t$ für alle $\mathfrak{a} \in \mathfrak{f}(D)$ — zu t-endlichen t-Idealen. Damit erhält man folgende wichtige Aussage über das Idealsystem der v- bzw. t-Ideale.

Korollar 1.11. *Gegeben sei eine beliebige $*$-Idealoperation $(\cdot)_*$ von D. Ist jedes gebrochene $*$-Ideal von D $*$-invertierbar, d. h. bilden die $*$-Ideale von D eine Gruppe bzgl. der $*$-Multiplikation, so stimmen $*$- und v-Idealoperation miteinander überein, und es gilt $\mathfrak{F}_*(D) = \mathfrak{F}_v(D)$. Insbesondere wird damit die Gruppe der $*$-Ideale zur Gruppe der v-Ideale. Ist die Idealoperation $(\cdot)_*$ darüber hinaus endlichartig, so stimmen $*$- und t-Idealoperation miteinander überein, und es gilt $\mathfrak{F}_*(D) = \mathfrak{f}_*(D) = \mathfrak{f}_t(D) = \mathfrak{F}_t(D)$. Insbesondere wird damit die Gruppe der $*$-Ideale zur Gruppe der t-endlichen t-Ideale.*

Zum Abschluß dieses Abschnittes wollen wir noch eine Aussage über Spuridealsysteme beweisen, die in der Literatur nicht zu finden ist, auf die wir jedoch im folgenden gelegentlich zurückgreifen müssen. Dazu sei wieder T ein Erweiterungsring von D mit $T \cap K = D$. Man wird i. a. nicht davon ausgehen können, daß sich die Eigenschaften eines $*$-Idealsystems von T auf das zugehörige Spuridealsystem von D übertragen. Bilden beispielsweise die $*$-Ideale von T bzgl. der $*$-Multiplikation eine Gruppe, so ist nicht zwingend, das die Spurideale auf D bzgl. der $*_p$-Multiplikation ebenfalls diese Eigenschaft besitzen.

Im folgenden wird uns die Situation begegnen, daß der Erweiterungsring T Polynomring über D oder Quotientenring[25] eines solchen Polynomringes ist. In diesem Fall übertragen sich Gruppeneigenschaft und t-Idealeigenschaft auch auf die Spurideale. Genauer gilt:

Satz 1.12. *Es seien $D \subseteq T$ Integritätsbereiche mit Quotientenkörper K bzw. L dergestalt, daß T ein freier D-Modul ist. Ferner bezeichne N eine multiplikativ abgeschlossene Teilmenge von T. Für den Quotientenring T_N von T nach N gelte $T_N \cap K = D$. Ist $(\cdot)_*$ eine endlichartige Idealoperation des Quotientenringes T_N und bilden die $*$-endlichen $*$-Ideale von T_N eine Gruppe bzgl. der $*$-Multiplikation, so bilden die $*_p$-endlichen $*$-Spurideale von D eine Gruppe bzgl. der $*_p$-Multiplikation. Diese ist mit der Gruppe der t-endlichen t-Ideale identisch.*

Für den Beweis dieses Satzes erweist sich das folgende Lemma als hilfreich.

---

[24] Siehe *Jaffard 1960*, S. 23, Lemme 1.

[25] In dieser Arbeit werden Ringe der Gestalt $D_N = N^{-1}D = \{\frac{a}{b} \in L : a \in D, b \in N\}$, N multiplikativ abgeschlossene Teilmenge von D, als *Quotientenringe* bezeichnet, nicht zu verwechseln mit den *Restklassenringen* der Gestalt D/N, N Ideal von D. Ist N das Komplement eines Primideals $\mathfrak{p}$ von D, so nennen wir, wie allgemein üblich, D_N auch die *Lokalisierung von D bei $\mathfrak{p}$*.

Lemma 1.13. *Es seien $D \subseteq T$ Integritätsbereiche mit Quotientenkörper K bzw. L dergestalt, daß T ein freier D-Modul ist. Ferner bezeichne N eine beliebige multiplikativ abgeschlossene Teilmenge von T und T_N den zugehörigen Quotientenring. Dann gilt*
(1) $(\mathfrak{a}T)^{-1} = \mathfrak{a}^{-1}T$ *für alle gebrochenen D-Ideale $\mathfrak{a}$.*
(2) $(\mathfrak{a}T_N)^{-1} = \mathfrak{a}^{-1}T_N$ *für alle endlich erzeugten gebrochenen D-Ideale $\mathfrak{a}$.*

Beweis: Ad (1) Sei $\mathfrak{a}$ ein gebrochenes D-Ideal. Die Inklusion $\mathfrak{a}^{-1}T \subseteq (\mathfrak{a}T)^{-1}$ ist wegen $\mathfrak{a}^{-1}(\mathfrak{a}T) \subseteq T$, d. h. $\mathfrak{a}^{-1} \subseteq (\mathfrak{a}T)^{-1}$, immer erfüllt — unabhängig davon, ob T ein freier D-Modul ist oder nicht. Seien also $\gamma \in (\mathfrak{a}T)^{-1}$ und $\{\omega_i\}_{i\in I}$ eine D-Modulbasis von T. Wegen

$$\begin{aligned}(\mathfrak{a}T)^{-1} &= \{\mu \in L : \mu\mathfrak{a}T \subseteq T\} = \{\mu \in L : \mu\alpha \in T \text{ für alle } \alpha \in \mathfrak{a}\}\\ &= \{\mu \in L : \mu \in \alpha^{-1}T \text{ für alle } \alpha \in \mathfrak{a}\}\\ &= \bigcap_{\alpha\in\mathfrak{a}} \frac{1}{\alpha}T\end{aligned}$$

existiert eine Familie $\{\tau_\alpha\}_{\alpha\in\mathfrak{a}}$ von Elementen aus T mit $\gamma = \frac{1}{\alpha}\tau_\alpha$. Da T ein freier D-Modul ist, läßt sich jedes τ_α eindeutig als D-Linearkombination von endlich vielen ω_i darstellen. Zu jedem τ_α existiert also eine eindeutig bestimmte Familie $\{d_{\alpha,i}\}_{i\in I}$ von Elementen aus D mit $\tau_\alpha = \sum_{i\in I} d_{\alpha,i}\cdot\omega_i$ und $d_{\alpha,i} = 0$ für fast alle $i \in I$. Für jedes $\alpha \in \mathfrak{a}$ gibt es somit eine Darstellung $\gamma = \sum_{i\in I} \frac{1}{\alpha}d_{\alpha,i}\cdot\omega_i$. Da die Basiselemente ω_i insbesondere über L linear unabhängig sind, müssen die Koeffizienten $\frac{1}{\alpha}d_{\alpha,i}$ von ω_i für jedes $\alpha \in \mathfrak{a}$ in den einzelnen Darstellungen gleich sein. Also ist für ein festes $i \in I$ jeder der auftretenden Koeffizienten in dem D-Ideal $\bigcap_{\alpha\in\mathfrak{a}} \frac{1}{\alpha}D = \mathfrak{a}^{-1}$ enthalten. Insgesamt folgt daher $\gamma \in \mathfrak{a}^{-1}T$.

Ad (2) Für alle gebrochenen T-Ideale $\mathfrak{a}, \mathfrak{b} \in \mathsf{F}(T)$ gilt $(\mathfrak{a} : \mathfrak{b})T_N \subseteq (\mathfrak{a}T_N : \mathfrak{b}T_N)$, und es herrscht Gleichheit, wenn man darüber hinaus $\mathfrak{b}$ als endlich erzeugt annimmt.[26] Übertragen auf den vorliegenden Fall, folgt hieraus zusammen mit Aussage (1)

$$\mathfrak{a}^{-1}T_N = (\mathfrak{a}^{-1}T)T_N = (\mathfrak{a}T)^{-1}T_N = (T : \mathfrak{a}T)T_N = (T_N : \mathfrak{a}T_N) = (\mathfrak{a}T_N)^{-1}. \qquad \square$$

Beweis von Satz 1.12: Es sei $\mathfrak{a}$ ein endlich erzeugtes gebrochenes D-Ideal. Aufgrund von Lemma 1.13.(2) gilt $(\mathfrak{a}T_N)^{-1} = \mathfrak{a}^{-1}T_N$. Da nach Voraussetzung jedes $*$-endliche $*$-Ideal von T_N $*$-invertierbar ist, erhält man $T_N = (\mathfrak{a}T_N \cdot (\mathfrak{a}T_N)^{-1})_* = (\mathfrak{a}\mathfrak{a}^{-1}T_N)_*$, woraus sofort $D = T_N \cap K = (\mathfrak{a}\mathfrak{a}^{-1}T_N)_* \cap K = (\mathfrak{a}\mathfrak{a}^{-1})_{*_p}$ folgt. Damit ist $\mathfrak{a}$ als $*_p$-invertierbar nachgewiesen. Da aufgrund von Satz 1.5 die $*$-Spuroperation $(\cdot)_{*_p}$ von D wiederum endlichartig ist, muß das $*_p$-Inverse von $\mathfrak{a}$ $*_p$-endlich sein. Insgesamt folgt also, daß die $*_p$-endlichen $*_p$-Ideale von D bzgl. der $*_p$-Multiplikation eine Gruppe bilden, die nach Korollar 1.11 mit der Gruppe der t-endlichen t-Ideale übereinstimmt. $\square$

1.3. $*$-prime und $*$-maximale $*$-Ideale

Es sei $(\cdot)_*$ eine beliebige Idealoperation. Da das Idealsystem der $*$-Ideale mit der $*$-Multiplikation eine bzgl. Inklusion teilweise geordnete Halbgruppe bildet, können in gewohnter Weise gewisse $*$-Ideale als *prim* oder *maximal* ausgezeichnet werden.

Definition 1.14. *Seien D ein Integritätsbereich und $\mathfrak{p}_*$ ein ganzes $*$-Ideal von D. $\mathfrak{p}_*$ heißt **$*$-prim**, wenn für alle $*$-Ideale $\mathfrak{a}_*, \mathfrak{b}_*$ aus $\mathfrak{a}_* \times \mathfrak{b}_* \subseteq \mathfrak{p}_*$ stets $\mathfrak{a}_* \subseteq \mathfrak{p}_*$ oder $\mathfrak{b}_* \subseteq \mathfrak{p}_*$ folgt. $\mathfrak{p}_*$ heißt **$*$-maximal**, wenn für jedes $*$-Ideal $\mathfrak{a}_*$ mit $\mathfrak{p}_* \subseteq \mathfrak{a}_*$ stets $\mathfrak{a}_* = \mathfrak{p}_*$ oder $\mathfrak{a}_* = D$ folgt.*

[26] Siehe *Gilmer 1992*, S. 37, Theorem 4.3.(7), und Theorem 4.4.(4).

Aus den Axiomen (I 1) – (I 3) für $*$-Idealoperationen folgt leicht, daß ein D-Ideal genau dann $*$-prim ist, wenn es ein primes $*$-Ideal ist. Wird die Idealoperation $(\cdot)_*$ als endlichartig vorausgesetzt, so läßt sich, ähnlich wie in der Dedekindschen Idealtheorie, zeigen, daß jedes $*$-maximale D-Ideal $\neq \{0\}$ $*$-prim ist, ebenso jedes über einem Hauptideal $\neq \{0\}$ minimale D-Ideal.[27] Für t-invertierbare t-Ideale ist auch die Umkehrung richtig. Genauer gilt:

Satz 1.15. *Es sei $(\cdot)_*$ eine endlichartige Idealoperation von D. Ist $\mathfrak{p} \neq \{0\}$ ein $*$-invertierbares D-Ideal, so sind folgende Bedingungen äquivalent:*
(1) $\mathfrak{p}$ *ist $*$-prim.*
(2) $\mathfrak{p}$ *ist t-prim.*
(3) $\mathfrak{p}$ *ist t-maximal.*
(4) $\mathfrak{p}$ *ist ein über einem Hauptideal $\neq \{0\}$ minimales D-Primideal.*

Beweis: Für die Implikationen (3) $\Rightarrow$ (2) sowie (4) $\Rightarrow$ (2) sei auf Jaffard verwiesen.

(1) $\Leftrightarrow$ (2) Jedes $*$-invertierbare $*$-Ideal ist ein (t-endliches) t-Ideal. Da umgekehrt jedes t-Ideal $\mathfrak{p}$ wegen $\mathfrak{p}_t = \mathfrak{p} \subseteq \mathfrak{p}_* \subseteq \mathfrak{p}_t$ ein $*$-Ideal ist, folgt die Behauptung.

(2) $\Rightarrow$ (3) Es sei $\mathfrak{p} = \mathfrak{p}_t$ t-prim. Wegen $\mathfrak{p} = (p_1, \ldots, p_r)_t$ mit $p_i \in \mathfrak{p}$ reicht es, für alle $a \in D \setminus \mathfrak{p}_t$ die Gleichheit $(p_1, \ldots, p_r, a)_t = D$ zu zeigen. Bedenkt man, daß sich mit Lemma 1.8 für die t-invertierbaren t-Ideale von D jede Inklusionsbeziehung in eine Teilbarkeitsbeziehung übersetzt, und berücksichtigt außerdem, daß damit das Primideal $\mathfrak{p}_t$ zu einem bzgl. der t-Multiplikation irreduziblen t-Ideal wird, so erhält man für ein beliebiges $\mu \in K^*$

$$\begin{aligned}(p_1, \ldots, p_r, a) \subseteq \mu D \quad &\Leftrightarrow \quad (p_1, \ldots, p_r)_t \subseteq \mu D \quad \text{und} \quad aD \subseteq \mu D \\ &\Leftrightarrow \quad \mu D \mid \mathfrak{p}_t \quad \text{und} \quad \mu \mid a \\ &\Leftrightarrow \quad \mu D = \mathfrak{p}_t \text{ und } \mathfrak{p}_t \mid aD \quad \text{oder} \quad \mu D = D \text{ und } a \in D.\end{aligned}$$

Nach Voraussetzung gilt $a \notin \mathfrak{p}_t$, also $\mathfrak{p}_t \nmid aD$, weshalb die erste der beiden Möglichkeiten ausscheidet. Also ist

$$(p_1, \ldots, p_r, a)_t = \bigcap_{\substack{\mu \in K^* \\ (p_1, \ldots, p_r, a) \subseteq \mu D}} \mu D = D.$$

(2) $\Rightarrow$ (4) Es sei $\mathfrak{p} = \mathfrak{p}_t$ t-prim. Wegen $\mathfrak{p}\mathfrak{p}^{-1} \not\subseteq \mathfrak{p}$ existieren $a \in \mathfrak{p}$ und $b \in \mathfrak{p}^{-1}$ mit $ab \notin \mathfrak{p}$. Ist $\mathfrak{q}$ ein D-Primideal mit $aD \subseteq \mathfrak{q} \subseteq \mathfrak{p}$, so sind alle $\mu \in D$ mit $\mu ab \in \mathfrak{q}$ wegen $ab \notin \mathfrak{q}$ bereits in $\mathfrak{q}$ enthalten. Aufgrund von $\mathfrak{p} \cdot b \subseteq D$ erhält man demnach

$$\mathfrak{p} \subseteq \{\mu \in D : \mu b \in D\} = \{\mu \in D : \mu ab \in aD\} \subseteq \{\mu \in D : \mu ab \in \mathfrak{q}\} = \mathfrak{q},$$

woraus $\mathfrak{q} = \mathfrak{p}$ und damit die Minimalität von $\mathfrak{p}$ über dem Hauptideal $(a) \neq \{0\}$ folgt. □

Insbesondere stimmen t-prime und t-maximale D-Ideale überein, wenn die $*$-Ideale von D bzgl. der $*$-Multiplikation eine Gruppe bilden. Wir wollen diese Situation genauer untersuchen. Durch Verallgemeinerung der klassischen Begriffsbildung erhält man

Definition 1.16. *Ein Integritätsbereich D mit der Idealoperation $(\cdot)_*$ heißt **$*$-noethersch**, wenn jede aufsteigende Kette von ganzen $*$-Idealen $\mathfrak{a}_*^{(0)} \subseteq \mathfrak{a}_*^{(1)} \subseteq \ldots \subseteq \mathfrak{a}_*^{(n)} \subseteq \ldots$ stationär wird.*[28]

Lemma 1.17. *Folgende Aussagen über einen Integritätsbereich D mit der Idealoperation $(\cdot)_*$ und der zugehörigen endlichartigen Idealoperation $(\cdot)_{*_s}$ sind äquivalent:*
(1) D *ist $*$-noethersch.*
(2) D *ist $*_s$-noethersch.*
(3) *Jedes ganze $*_s$-Ideal ist $*_s$-endlich.*
(4) *Jede nichtleere Menge von $*_s$-Idealen besitzt ein (bzgl. Inklusion) maximales Element.*

[27] Siehe *Jaffard 1960*, S. 30f., Corollaire 1 und Corollaire 3 zu Théorème 9.
[28] Vgl. *Jaffard 1960*, S. 31.

Der Beweis ergibt sich aufgrund der Endlichartigkeit der Idealoperation $(\cdot)_{*_s}$ unmittelbar aus dem entsprechenden Beweis für d-Ideale.[29] Man beachte, daß im Falle einer nicht-endlichartigen Idealoperation $(\cdot)_*$ die $*$-Endlichkeit jedes $*$-Ideals zwar notwendig, i. a. jedoch *nicht* hinreichend für die $*$-noethersche Eigenschaft ist.[30]

Für den Fall, daß die $*$-Ideale bzgl. der $*$-Multiplikation eine Gruppe bilden, läßt sich die Analogie noch weiter fortschreiben. Bekanntlich lassen sich *Dedekindbereiche*, also Integritätsbereiche, in denen die d-Ideale bzgl. der d-Multiplikation eine Gruppe bilden, auch charakterisieren als ganzabgeschlossene, noethersche Integritätsbereiche, in denen jedes Primideal $\neq \{0\}$ maximal ist, bzw. als Ringe, in denen jedes ganze d-Ideal als d-Produkt von d-primen Idealen darstellbar ist.[31] Allgemein gilt

Satz 1.18. *Für einen Integritätsbereich D mit einer endlichartigen Idealoperation $(\cdot)_*$ sind folgende Aussagen äquivalent:*
(1) *Die gebrochenen $*$-Ideale von D bilden eine Gruppe bzgl. der $*$-Multiplikation.*
(2) *Jedes ganze $*$-Ideal ist als $*$-Produkt von endlich vielen $*$-primen $*$-Idealen darstellbar.*
(3) *D ist $*$-abgeschlossen*[32]*, $*$-noethersch und jedes $*$-prime D-Ideal $\neq \{0\}$ ist $*$-maximal.*

Beweis: Für den Beweis der Äquivalenz (1) $\Leftrightarrow$ (3) sei auf Jaffard verwiesen.[33]

(1) $\Rightarrow$ (2) Bilden die $*$-Ideale von D bzgl. der $*$-Multiplikation eine Gruppe, so ist jedes $*$-Ideal $*$-endlich und daher D aufgrund von Lemma 1.17.(3) $*$-noethersch. Angenommen, es gebe ganze $*$-Ideale, die sich nicht als $*$-Produkt von $*$-primen Idealen darstellen lassen. Die Menge all dieser $*$-Ideale besitzt nach Lemma 1.17.(4) ein maximales Element $\mathfrak{m}_*$. $\mathfrak{m}_*$ ist nicht $*$-prim und somit auch nicht $*$-maximal. Es muß jedoch in einem $*$-maximalen, also $*$-primen D-Ideal $\mathfrak{p}_*$ enthalten sein.[34] Aus $\mathfrak{m}_* \subsetneqq \mathfrak{p}_*$ und $D \subsetneqq \mathfrak{p}_*^{-1}$ folgt aber $\mathfrak{m}_* \subsetneqq \mathfrak{m}_* \times \mathfrak{p}_*^{-1} \subsetneqq D$. Aufgrund der Maximalitätseigenschaft von $\mathfrak{m}_*$ muß das ganze $*$-Ideal $\mathfrak{m}_* \times \mathfrak{p}_*^{-1}$ als $*$-Produkt von endlich vielen $*$-primen $*$-Idealen $\mathfrak{p}_*^{(1)}, \ldots, \mathfrak{p}_*^{(r)}$ darstellbar sein. Daraus folgt jedoch $\mathfrak{m}_* = \mathfrak{p}_* \times \mathfrak{p}_*^{(1)} \times \ldots \times \mathfrak{p}_*^{(r)}$, was im Widerspruch zur Wahl von $\mathfrak{m}_*$ steht.

(2) $\Rightarrow$ (1) Es reicht zu zeigen, daß jedes $*$-prime $*$-Ideal $\mathfrak{p}_* \neq \{0\}$ $*$-invertierbar ist. Dazu sei $p \in \mathfrak{p}_*$, $p \neq 0$. Das von p erzeugte Hauptideal pD ist als $*$-Produkt von endlich vielen $*$-primen D-Idealen $\mathfrak{p}_*^{(1)}, \ldots, \mathfrak{p}_*^{(r)}$ darstellbar. Da pD $*$-invertierbar ist, muß auch jedes $*$-prime $\mathfrak{p}_*^{(i)}$ $*$-invertierbar und somit aufgrund von Satz 1.15 $*$-maximal sein. Die $*$-Primeigenschaft von $\mathfrak{p}_*$ impliziert $\mathfrak{p}_*^{(i)} \subseteq \mathfrak{p}_*$ für ein $\mathfrak{p}_*^{(i)}$. Wegen der $*$-Maximalität von $\mathfrak{p}_*^{(i)}$ folgt daraus jedoch $\mathfrak{p}_*^{(i)} = \mathfrak{p}_*$, womit $\mathfrak{p}_*$ als $*$-invertierbar nachgewiesen ist. □

Korollar 1.19. *Ist eine der gleichwertigen Bedingungen von Satz 1.18 erfüllt, so sind folgende Aussagen über ein D-Ideal $\mathfrak{p} \neq \{0\}$ äquivalent:*
(1) *$\mathfrak{p}$ ist $*$-prim.*
(2) *$\mathfrak{p}$ ist ein minimales D-Primideal, also ein primes D-Ideal der Höhe 1.*
(3) *Die Lokalisierung $D_\mathfrak{p}$ von D bei $\mathfrak{p}$ ist ein diskreter Bewertungsring, also ein Hauptidealring mit genau einem Primideal.*

---

[29] Vgl. *Zariski et al. 1958*, S. 199, sowie S. 156, Theorem 15 und Theorem 17. Siehe auch *Jaffard 1960*, S. 31f., Proposition 7 zusammen mit dem zugehörigen Corollaire, sowie *Anderson et al. 1988*, S. 28, Theorem 1.1.

[30] Siehe hierzu *Gilmer 1992*, S. 431, Exercise 14, sowie S. 545. Dort wird das Beispiel eines Integritätsbereiches gegeben, in dem jedes v-Ideal sogar Hauptideal ist, ohne daß der Ring deshalb bereits die v-noethersche Eigenschaft besäße.

[31] Vgl. *Zariski et al. 1958*, S. 270, Definition 1, sowie S. 275, Theorem 12 und Theorem 13.

[32] D heißt nach *Lorenzen 1939*, S. 537 (bzw. S. 541) *$*$-abgeschlossen* (bzw. *vollständig $*$-abgeschlossen*), wenn für jedes endlich erzeugte D-Ideal (bzw. jedes D-Ideal) $\mathfrak{a}$ stets $(\mathfrak{a}_* : \mathfrak{a}_*) = D$ gilt.

[33] Siehe *Jaffard 1960*, S. 33, Théorème 11.

[34] Siehe *Jaffard 1960*, S. 31, Corollaire 2 zu Théorème 9.

Beweis: (2) $\Rightarrow$ (1) Jedes D-Primideal der Höhe 1 ist trivialerweise minimal über einem Hauptideal, also nach Satz 1.15 $*$-prim.

(1) $\Rightarrow$ (2) Sei $\mathfrak{p} = \mathfrak{p}_*$ irgendein $*$-primes Ideal von D. Angenommen, die Höhe von $\mathfrak{p}_*$ sei > 1. Dann existiert ein Primideal $\mathfrak{q}$ von D mit $\{0\} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}_*$. Sei $q \in \mathfrak{q}$ mit $q \neq 0$. Dann ist das von q erzeugte Hauptideal darstellbar als $*$-Produkt von endlich vielen $*$-primen D-Idealen $\mathfrak{q}_*^{(1)}, \ldots, \mathfrak{q}_*^{(r)}$, also $\mathfrak{q}_*^{(1)} \cdot \ldots \cdot \mathfrak{q}_*^{(r)} \subseteq \mathfrak{q}_*^{(1)} \times \ldots \times \mathfrak{q}_*^{(r)} = qD \subseteq \mathfrak{q} \subsetneqq \mathfrak{p}_*$. Aufgrund der Primeigenschaft von $\mathfrak{q}$ ist eines der primen $*$-Ideale $\mathfrak{q}_*^{(i)}$ in $\mathfrak{q}$ enthalten. Die daraus resultierende echte Inklusion $\mathfrak{q}_*^{(i)} \subsetneqq \mathfrak{p}_*$ für ein $i \in \{1, \ldots, r\}$ steht jedoch im Widerspruch zur $*$-Maximalität von $\mathfrak{q}_*^{(i)}$, weshalb $\mathfrak{p}_*$ doch ein Primideal der Höhe 1 gewesen sein muß.

(2) $\Leftrightarrow$ (3) Da die Primideale der Lokalisierung $D_\mathfrak{p}$ umkehrbar eindeutig jenen Primidealen von D entsprechen, die in $\mathfrak{p}$ enthalten sind, ist klar, daß $D_\mathfrak{p}$ genau dann nur ein einziges Primideal (nämlich das maximale Ideal $\mathfrak{p}D_\mathfrak{p}$) enthält, wenn $\mathfrak{p}$ ein minimales D-Primideal ist. Daß $D_\mathfrak{p}$ in diesem Fall ein Hauptidealring ist, wird an anderer Stelle gezeigt. [35] □

Kapitel 2

Ringe mit ggT-Theorie

2.1. Ringe mit ggT

Ist G^+ irgendein multiplikativer abelscher Monoid, also eine kommutative Halbgruppe mit Kürzungsregel, so stellt sich die Frage nach der Exsitenz eines größten gemeinsamen Teilers in G^+: Gibt es zu je zwei Elementen $\alpha, \beta \in G^+$ stets ein $\gamma \in G^+$ mit

1.) $\gamma \mid \alpha$, $\gamma \mid \beta$ und

2.) $\delta \mid \gamma$ für alle $\delta \in G^+$ mit $\delta \mid \alpha$, $\delta \mid \beta$?

Falls dies der Fall ist, so heißt G^+ *Monoid mit ggT*. Größte gemeinsame Teiler sind stets nur bis auf Assoziiertheit eindeutig bestimmt. Ist die Einheitengruppe von G^+ trivial und somit jeder größte gemeinsame Teiler unzweideutig festgelegt, so heißt G^+ auch *ggT-Monoid*.[36]

Definition 2.1. *Ist die multiplikative Halbgruppe D^* eines Integritätsbereiches D ein Monoid mit ggT, so heißt D auch* ***ggT-Bereich****. Läßt sich ein größter gemeinsamer Teiler zweier beliebiger Ringelemente $\alpha, \beta \in D$ als D-Linearkombination von α und β darstellen, so spricht man von einem* ***Bezoutbereich*** *D.*

Die ggT-Bereichseigenschaft und die Bezout-Eigenschaft eines Integritätsbereiches D lassen sich idealtheoretisch charakterisieren.

Satz 2.2. *Der Integritätsbereich D ist genau dann ein ggT-Bereich (Bezoutbereich), wenn jedes t-endliche t-Ideal (jedes d-endliche d-Ideal) ein Hauptideal ist. Für $\alpha, \beta, \gamma \in D$ ist dann $\gamma \sim \mathrm{ggT}(\alpha, \beta)$ äquivalent zu $\gamma D = (\alpha, \beta)_t$.*[37]

In diesem Satz zeigt sich bereits die Bedeutung, die das Idealsystem der t-Ideale bzw. v-Ideale für die Untersuchung der arithmetischen Eigenschaften von Integritätsbereichen hat. Bedenkt man

[35] Siehe unten, S. 36, Satz 3.9.(2).

[36] Der ggT-Monoid (Monoid mit ggT) G^+ kann vermöge $\alpha \geqslant \beta \;:\Leftrightarrow\; \beta \mid \alpha$ als (teilweise) geordnete Halbgruppe charakterisiert werden, in der je endlich viele Elemente ein Infimum besitzen. Solche Halbgruppen werden im modernen Sprachgebrauch auch als (*teilweise*) *verbandsgeordnet* („*lattice ordered*“, „*réticulé*“) bezeichnet.

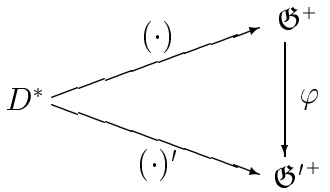
[37] *Gilmer 1992*, S. 175, Theroem 16.2, und S. 79, Exercise 12. Ein Bezoutbereich ist also ein ggT-Bereich, in dem das Idealsystem der t-endlichen t-Ideale mit dem Idealsystem der d-endlichen d-Ideale übereinstimmt.

ferner, daß jeder faktorielle Ring ein ggT-Bereich und jeder Hauptidealring ein Bezoutbereich ist, so liegt die Vermutung nahe, daß faktorielle Ringe im Gegensatz zu ggT-Bereichen dadurch charakterisiert sind, daß *alle* ihre t-Ideale (also nicht nur die t-endlichen t-Ideale) Hauptideale sind. Diese Vermutung ist tatsächlich richtig. Es wird sich sogar zeigen, daß dahinter gewissermaßen ein allgemeineres Prinzip steht, welches auch zu beobachten ist, wenn man von der ggT-Eigenschaft bzw. Primzerlegungseigenschaft abstrahiert und zu den sogenannten Ringen mit ggT-Theorie bzw. Divisorentheorie übergeht.

2.2. Der Begriff des Ringes mit ggT-Theorie

Um alle weiteren Überlegungen auf eine sichere begriffliche Grundlage zu stellen, wollen wir in diesem Abschnitt noch einmal exakt definieren, was es heißen soll, daß ein Ring eine ggT-Theorie, d. h. so etwas wie einen größten gemeinsamen Teiler, besitzt. Dazu bezeichne im folgenden $\mathfrak{G}^+$ stets einen ggT-Monoiden, d. h. eine abelsche Halbgruppe mit Kürzungsregel, in der je zwei Elemente einen größten gemeinsamen Teiler besitzen, und $\mathfrak{G}$ die Quotientengruppe von $\mathfrak{G}^+$.

Definition 2.3. *Ein Integritätsbereich D heißt **Ring mit ggT-Theorie**,*[38] *wenn es einen ggT-Monoiden $\mathfrak{G}^+$ sowie einen Halbgruppenhomomorphismus $(\cdot) : D^* \to \mathfrak{G}^+$, $\alpha \mapsto (\alpha)$, mit folgenden Eigenschaften gibt:*
(G 1) *Für $\alpha, \beta \in D^*$ gilt: $(\alpha) \mid (\beta)$ in $\mathfrak{G}^+ \Leftrightarrow \alpha \mid \beta$ in D.*
(G 2) *Für $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}^+$ mit $\overline{\mathfrak{a}} := \{\mu \in D^* : \mathfrak{a} \mid (\mu)\} \cup \{0\}$ gilt: $\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \Leftrightarrow \mathfrak{a} = \mathfrak{b}$.*
*Der ggT-Monoid $\mathfrak{G}^+$ heißt **Divisorenhalbgruppe**, die Quotientengruppe $\mathfrak{G}$ **Divisorengruppe** der ggT-Theorie. Die Elemente von $\mathfrak{G}^+$ bzw. $\mathfrak{G}$ werden entsprechend als ganze bzw. gebrochene **Divisoren**, Elemente der Gestalt (α), $\alpha \in D^*$, auch als **Hauptdivisoren** bezeichnet. Zwei ggT-Theorien $(\cdot) : D^* \to \mathfrak{G}^+$ und $(\cdot)' : D^* \to \mathfrak{G}'^+$ für einen Integritätsbereich D heißen zueinander **isomorph**, wenn zwischen den zugehörigen Divisorenhalbgruppen $\mathfrak{G}^+$ und $\mathfrak{G}'^+$ ein Isomorphismus φ besteht, der das folgende Diagramm kommutativ macht:*



Axiom (G 1) besagt, daß die Teilbarkeitseigenschaften von D in der Divisorenhalbgruppe $\mathfrak{G}^+$ treu wiedergegeben werden.

Axiom (G 2) besagt, daß zwei Divisoren, die dieselben Vielfachen in D besitzen, miteinander übereinstimmen sollen. Inwieweit dadurch bereits sichergestellt ist, daß die Divisorenhalbgruppe tatsächlich keine überflüssigen Divisoren enthält, wird noch genauer zu untersuchen sein. Für den Fall, daß die Divisorenhalbgruppe $\mathfrak{G}^+$ faktoriell und somit D ein Ring mit Divisorentheorie im Borewicz-Šafarevičschen Sinne ist, weiß man jedenfalls, daß $\mathfrak{G}^+$ bzgl. der Eigenschaft (G 1) in gewisser Weise minimal gewählt ist.

[38] Die Begriffsbildung geht in dieser Form auf E. Maus zurück. Vgl. auch Anmerkung 61, S. 32. Gegenüber der Borewicz-Šafarevičschen Definition für Ringe mit Divisorentheorie (vgl. Einleitung, S. 2) ergeben sich zwei wesentliche Unterschiede:
(1) Für die Divisorenhalbgruppe $\mathfrak{G}^+$ wird lediglich die Existenz eines (eindeutig bestimmten) größten gemeinsamen Teilers, nicht aber die Faktorialität gefordert.
(2) Auf das zweite Axiom wurde ganz verzichtet, da es in den Bedingungen (G 1) und (G 2), wie wir in Satz 2.7, S. 19, zeigen werden, bereits enthalten ist.

Die in Axiom (G 2) auftretende Menge $\overline{\mathfrak{a}}$, $\mathfrak{a} \in \mathfrak{G}^+$, enthält in jedem Fall ein Ringelement $\neq 0$. Denn aus $\overline{\mathfrak{a}} = \{0\}$ würde $\overline{\mathfrak{a}^2} = \{0\}$, also $\overline{\mathfrak{a}} = \overline{\mathfrak{a}^2}$ folgen, woraus sich mit Axiom (G 2) die Gleichheit $\mathfrak{a} = \mathfrak{a}^2$ ergäbe. Da Divisoren nach Voraussetzung kürzbar sind, erhielte man $(1) = \mathfrak{a}$, also $1 \in \overline{\mathfrak{a}}$, was wegen $0 \neq 1$ im Widerspruch zur Annahme $\overline{\mathfrak{a}} = \{0\}$ stünde. Als Folgerung halten wir fest:

Bemerkung 2.4. Die Fortsetzung einer ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ von D zu einem Gruppenhomomorphismus $(\cdot)' : K^* \to \mathfrak{G}$ hat folgende Eigenschaften:
(1) Für $\alpha, \beta \in K^*$ gilt: $(\alpha)' \mid (\beta)'$ bzgl. $\mathfrak{G}^+ \Leftrightarrow \alpha \mid \beta$ bzgl. D.
(2) Für $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}$ mit $\overline{\mathfrak{a}} := \{\mu \in K^* : \mathfrak{a} \mid (\mu)'\} \cup \{0\}$ gilt: $\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \Leftrightarrow \mathfrak{a} = \mathfrak{b}$.

Beweis: (1) ist eine unmittelbare Folgerung aus Axiom (G 1). Für (2) überlege man sich, daß jeder gebrochene Divisor $\mathfrak{a} \in \mathfrak{G}$ als Quotient $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{-1}$, $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathfrak{G}^+$, darstellbar ist. Wegen $\overline{\mathfrak{a}_2} \neq \{0\}$ existiert ein $\alpha \in D^*$ mit $(\alpha)\mathfrak{a}_2^{-1} \in \mathfrak{G}^+$, also $(\alpha)\mathfrak{a} \in \mathfrak{G}^+$. Zu je zwei gebrochenen Divisoren $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}$ existiert also stets ein $\gamma \in D^*$ mit $(\gamma)\mathfrak{a}, (\gamma)\mathfrak{b} \in \mathfrak{G}^+$. Es gelte $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. Wenn $\mathfrak{a}$ und $\mathfrak{b}$ dieselben Hauptdivisoren bzgl. $\mathfrak{G}^+$ teilen, dann auch $(\gamma)\mathfrak{a}$ und $(\gamma)\mathfrak{b}$. Aus $\overline{(\gamma)\mathfrak{a}} = \overline{(\gamma)\mathfrak{b}}$ folgt jedoch nach Axiom (G 2) $(\gamma)\mathfrak{a} = (\gamma)\mathfrak{b}$, also $\mathfrak{a} = \mathfrak{b}$. □

Im folgenden werden wir zwischen einer ggT-Theorie $(\cdot)$ für D und ihrer Fortsetzung $(\cdot)'$ nach K nicht mehr unterscheiden und, sofern nichts anderes bestimmt ist, unter einem Divisor grundsätzlich einen gebrochenen Divisor verstehen. Entsprechend bezeichne $\overline{\mathfrak{a}}$ stets die Menge $\{\mu \in K^* : \mathfrak{a} \mid (\mu)\} \cup \{0\}$. Außerdem verzichten wir bei Hauptdivisoren auf die Notation in Klammern, wenn Mißverständnisse auszuschließen sind.

Die rein axiomatische Definition eines Ringes mit ggT-Theorie ist zwar durchaus suggestiv, erweist sich in der Praxis jedoch als unhandlich. Sie verlangt geradezu nach weiteren äquivalenten Charakterisierungen, insbesondere solchen, die etwas über die konkrete Gestalt der Divisorenhalbgruppe $\mathfrak{G}^+$ aussagen.

Eine weitere Frage, die uns beschäftigen wird, ist die nach der Eindeutigkeit einer ggT-Theorie: Ist es denkbar, daß ein Ring mit ggT-Theorie mehrere nicht-isomorphe ggT-Theorien besitzt?

Schließlich interessiert man sich für das Verhalten von Ringen mit ggT-Theorie beim Übergang zu Polynomringen, allgemeinen Quotientenringen oder ganzen Abschließungen in algebraischen Körpererweiterungen.

In der Einleitung wurde bereits angedeutet, daß der Schlüssel zur Lösung all dieser Probleme in einem genauen Verständnis der definitorischen Eigenschaften eines Ringes mit ggT-Theorie, insbesondere in dem genauen Verständnis des Axioms (G 2), liegt. Wir wollen daher zunächst zwei äquivalente Fassungen dieses Axioms angeben.

Lemma 2.5. *Für einen Ring D mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ sind folgende Fassungen des Axioms (G 2) äquivalent:*
(1) $\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{b}} \Leftrightarrow \mathfrak{b} \mid \mathfrak{a}$.
(2) $\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \Leftrightarrow \mathfrak{a} = \mathfrak{b}$.
(3) $\mathfrak{a} = \mathrm{ggT}(\{\alpha\}_{\mathfrak{a}\mid\alpha})$.

Beweis: Die Implikation (1) ⇒ (2) ist klar. Es gelte also $\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \Leftrightarrow \mathfrak{a} = \mathfrak{b}$. Wir betrachten die Familie $\{\alpha\mathfrak{a}^{-1}\}_{\mathfrak{a}\mid\alpha}$ ganzer Divisoren aus $\mathfrak{G}$. Diese ist wegen $\overline{\mathfrak{a}} \setminus \{0\} \neq \emptyset$ nichtleer. Gäbe es einen gemeinsamen Teiler $\mathfrak{g} \neq (1)$ aller $\alpha\mathfrak{a}^{-1}$, $\alpha \in \overline{\mathfrak{a}} \setminus \{0\}$, so wäre der Divisor $\mathfrak{a}\mathfrak{g} \neq \mathfrak{a}$ ein gemeinsamer Teiler aller Hauptdivisoren (α). Da nach Voraussetzung $\overline{\mathfrak{a}\mathfrak{g}} \neq \overline{\mathfrak{a}}$ gilt, folgt also $\overline{\mathfrak{a}} \subsetneq \overline{\mathfrak{a}\mathfrak{g}}$. Dies steht jedoch im Widerspruch zu $\mathfrak{a} \mid \mathfrak{a}\mathfrak{g}$, also $\overline{\mathfrak{a}\mathfrak{g}} \subseteq \overline{\mathfrak{a}}$. Demnach ist $\{\alpha\mathfrak{a}^{-1}\}_{\mathfrak{a}\mid\alpha}$ eine teilerfremde Familie

ganzer Divisoren, woraus wegen $\mathfrak{a} = \mathfrak{a} \cdot \mathrm{ggT}(\{\alpha\mathfrak{a}^{-1}\}_{\mathfrak{a}|\alpha}) = \mathrm{ggT}(\{\alpha\}_{\mathfrak{a}|\alpha})$ Aussage (3) folgt.[39] Für die Implikation (3) $\Rightarrow$ (1) überlege man sich, daß aus $\overline{\mathfrak{a}} \subseteq \overline{\mathfrak{b}}$ sofort $\mathfrak{b} \mid \alpha$ für alle $\alpha \in \overline{\mathfrak{a}} \setminus \{0\}$ und somit $\mathfrak{b} \mid \mathfrak{a}$ folgt. □

Mit Hilfe von Lemma 2.5 soll im folgenden Abschnitt nunmehr untersucht werden, inwieweit bereits die definitorischen Eigenschaften, insbesondere Axiom (G 2) und seine äquivalenten Fassungen, Aussagen über die Idealstruktur eines Ringes mit ggT-Theorie zulassen.

2.3. Die Idealstruktur von Ringen mit ggT-Theorie

Als erstes beweisen wir einen Satz, der uns genauen Aufschluß über die Struktur der Menge $\overline{\mathfrak{a}}$, also der Menge aller Vielfachen eines Divisors $\mathfrak{a} \in \mathfrak{G}$ in K, gibt. Seine zentrale Bedeutung liegt darin, daß er die Verbindung zur Idealtheorie herstellt und dadurch eine idealtheoretische Charakterisierung der Ringe mit ggT-Theorie möglich macht.

Satz 2.6. *Es seien D ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$, $\mathfrak{a}$ ein beliebiger Divisor und $\{(\alpha)_i\}_{i\in I}$ eine Familie von Hauptdivisoren mit $\mathfrak{a} = \mathrm{ggT}(\{\alpha_i\}_{i\in I})$. Dann gilt $\overline{\mathfrak{a}} = (\{\alpha_i\}_{i\in I})_v = (\overline{\mathfrak{a}})_v$, wobei $(\overline{\mathfrak{a}})_v$ das von den Elementen aus $\overline{\mathfrak{a}}$ erzeugte v-Ideal bezeichne.*

Beweis: Wir beweisen den Satz zunächst für die Hauptdivisorenfamilie $\{(\alpha)\}_{\alpha\in\overline{\mathfrak{a}}\setminus\{0\}}$, die aufgrund von Lemma 2.5.(3) als größten gemeinsamen Teiler den Divisor $\mathfrak{a}$ besitzt. Die Inklusion $\overline{\mathfrak{a}} \subseteq (\overline{\mathfrak{a}})_v$ ist klar. Für die Inklusion „$\supseteq$“ sei $\gamma \in (\overline{\mathfrak{a}})_v$, wobei wir o. E. d. A. $\gamma \neq 0$ annehmen. Dann gilt wegen Lemma 2.5.(1)

$$\gamma \in \bigcap_{\substack{\mu\in K\\ \overline{\mathfrak{a}}\subseteq\mu D}} \mu D = \bigcap_{\substack{\mu\in K\\ \overline{\mathfrak{a}}\subseteq\overline{(\mu)}}} \mu D = \bigcap_{\substack{\mu\in K\\ (\mu)\mid\mathfrak{a}}} \mu D.$$

D. h. $\mu \mid \gamma$ für alle $\mu \in K$ mit $(\mu) \mid \mathfrak{a}$, oder anders ausgedrückt: Für $\mu \in K$ ist $(\mu) \mid \mathfrak{a}$ äquivalent zu $(\mu) \mid \mathrm{ggT}(\gamma, \mathfrak{a})$. Setzt man $\mathfrak{g} = \mathrm{ggT}(\gamma, \mathfrak{a})$, so ergibt sich mit Axiom (G 2) folgende Kette von Implikationen:

$$\begin{aligned}
(\mu) \mid \mathfrak{a} &\Leftrightarrow (\mu) \mid \mathfrak{g}\\
\mathfrak{a}^{-1} \mid (\mu^{-1}) &\Leftrightarrow \mathfrak{g}^{-1} \mid (\mu^{-1})\\
\{\mu \in K : \mathfrak{a}^{-1} \mid (\mu^{-1})\} &= \{\mu \in K : \mathfrak{g}^{-1} \mid (\mu^{-1})\}\\
\{\mu \in K : \mathfrak{a}^{-1} \mid (\mu)\} &= \{\mu \in K : \mathfrak{g}^{-1} \mid (\mu)\}\\
\overline{\mathfrak{a}^{-1}} &= \overline{\mathfrak{g}^{-1}}\\
\mathfrak{a}^{-1} &= \mathfrak{g}^{-1}\\
\mathfrak{a} &= \mathfrak{g} = \mathrm{ggT}(\gamma, \mathfrak{a}).
\end{aligned}$$

Also gilt $\mathfrak{a} \mid (\gamma)$, woraus schließlich $\gamma \in \overline{\mathfrak{a}}$ folgt. Sei nun allgemein $\mathfrak{a} = \mathrm{ggT}(\{\alpha_i\}_{i\in I})$. Aufgrund des gerade eben Bewiesenen und wegen $\alpha_i \in \overline{\mathfrak{a}}$ gilt $(\{\alpha_i\}_{i\in I})_v \subseteq (\overline{\mathfrak{a}})_v = \overline{\mathfrak{a}}$. Bleibt die umgekehrte Inklusion zu zeigen. Dazu sei $\gamma \in \overline{\mathfrak{a}}$, also $\mathfrak{a} \mid (\gamma)$. Es folgt $\mu \mid \gamma$ für alle $\mu \in K$ mit $(\mu) \mid \mathfrak{a}$. Wegen $\mathfrak{a} = \mathrm{ggT}(\{\alpha_i\}_{i\in I}) = \mathrm{ggT}(\{\alpha\}_{\alpha\in\overline{\mathfrak{a}}\setminus\{0\}})$ gilt für ein $\mu \in K^*$ jedoch $(\mu) \mid \mathfrak{a}$ genau dann, wenn $\mu \mid \alpha_i$ für alle $i \in I$. Daraus erhält man

$$\gamma \in \bigcap_{\substack{\mu\in K\\ (\mu)\mid\mathfrak{a}}} \mu D = \bigcap_{\substack{\mu\in K\\ \mu\mid\alpha_i}} \mu D = \bigcap_{\substack{\mu\in K\\ \{\alpha_i\}_{i\in I}\subseteq\mu D}} \mu D = (\{\alpha_i\}_{i\in I})_v.$$ □

[39] Besitzen zwei Familien $\{\alpha_i\}_{i\in I}$ und $\{\beta_j\}_{j\in J}$ von Elementen aus dem multiplikativen Monoiden G^+ einen größten gemeinsamen Teiler mit $\alpha \sim \mathrm{ggT}(\{\alpha_i\}_{i\in I})$ und $\beta \sim \mathrm{ggT}(\{\beta_j\}_{j\in J})$, so gilt, wie man ohne Probleme beweist:
(1) $\delta\alpha \sim \mathrm{ggT}(\{\delta\alpha_i\}_{i\in I})$ für alle $\delta \in G$. Für spätere Anwendungen notieren wir außerdem
(2) $\mathrm{ggT}(\{\alpha_i\}_{i\in I}) \cdot \mathrm{ggT}(\{\beta_j\}_{j\in J}) \sim \mathrm{ggT}(\{\alpha_i\beta_j\}_{i\in I, j\in J})$.

Aus diesem Satz ergeben sich eine ganze Reihe von Folgerungen. Als erstes halten wir fest, daß das zweite Axiom der Borewicz-Šafarevičschen Definition für Ringe mit Divisorentheorie für Ringe mit ggT-Theorie (folglich auch für Ringe mit Divisorentheorie) überflüssig ist.[40]

Korollar 2.7. *Es seien D ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$, $\alpha, \beta \in D^*$ mit $\alpha \pm \beta \neq 0$ und $\mathfrak{g} \in \mathfrak{G}^+$. Dann folgt aus $\mathfrak{g} \mid (\alpha)$ und $\mathfrak{g} \mid (\beta)$ stets $\mathfrak{g} \mid (\alpha \pm \beta)$.*

Beweis: Da $\overline{\mathfrak{g}}$ nach Satz 2.6 ein Ideal ist, folgt aus $\mathfrak{g} \mid (\alpha)$, $\mathfrak{g} \mid (\beta)$, also $\alpha, \beta \in \overline{\mathfrak{g}}$, sofort $\alpha \pm \beta \in \overline{\mathfrak{g}}$, also $\mathfrak{g} \mid (\alpha \pm \beta)$. □

Satz 2.6 deutet darauf hin, daß die Divisoren eines Ringes mit ggT-Theorie in enger Beziehung zu den v-Idealen des Ringes stehen. Die drei folgenden Korollare gewähren einen noch tieferen Einblick in die genauen Zusammenhänge. Für den Rest dieses Abschnittes sei D stets ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$.

Korollar 2.8. *Seien $\alpha_1, \ldots, \alpha_m \in K$. Dann gilt für einen Divisor $\mathfrak{a} \in \mathfrak{G}$*

$$\mathfrak{a} = \mathrm{ggT}(\alpha_1, \ldots, \alpha_m) \quad \Leftrightarrow \quad \overline{\mathfrak{a}} = (\alpha_1, \ldots, \alpha_m)_v = (\alpha_1, \ldots, \alpha_m)_t.$$

Beweis: Die Implikation „⇒“ ergibt sich aus Satz 2.6, wenn man die endliche Familie von Hauptdivisoren $\{(\alpha_i)\}_{1 \leqslant i \leqslant m}$ betrachtet. Für die Umkehrung sei $\mathfrak{g} = \mathrm{ggT}(\alpha_1, \ldots, \alpha_m)$. Dann gilt nach Satz 2.6 $\overline{\mathfrak{g}} = (\alpha_1, \ldots, \alpha_m)_v = \overline{\mathfrak{a}}$, woraus mit Axiom (G 2) die Gleichheit der Divisoren $\mathfrak{g}$ und $\mathfrak{a}$ folgt. □

Korollar 2.9. *Seien $\mathfrak{a}$ und $\mathfrak{b}$ beliebige Divisoren in $\mathfrak{G}$. Dann ist $\overline{\mathfrak{ab}} = (\overline{\mathfrak{a}})_v \times (\overline{\mathfrak{b}})_v$. Insbesondere gilt $\overline{\mathfrak{a}}^{-1} = \overline{\mathfrak{a}^{-1}}$.*

Beweis: Aufgrund von Lemma 2.5.(3) gilt $\mathfrak{a} = \mathrm{ggT}(\{\alpha\}_{\mathfrak{a}|\alpha})$ und $\mathfrak{b} = \mathrm{ggT}(\{\beta\}_{\mathfrak{b}|\beta})$, woraus $\mathfrak{ab} = \mathrm{ggT}(\{\alpha\beta\}_{\mathfrak{a}|\alpha,\, \mathfrak{b}|\beta})$ folgt.[41] Mit Satz 2.6 ergibt sich

$$\overline{\mathfrak{ab}} = (\{\alpha\beta\}_{\mathfrak{a}|\alpha,\, \mathfrak{b}|\beta})_v = (\{\alpha\}_{\mathfrak{a}|\alpha})_v \times (\{\beta\}_{\mathfrak{b}|\beta})_v = (\overline{\mathfrak{a}})_v \times (\overline{\mathfrak{b}})_v,$$

womit die erste Behauptung bewiesen ist. Die zweite Behauptung folgt dann unmittelbar. Denn wegen $D = \overline{(1)} = \overline{\mathfrak{a}\mathfrak{a}^{-1}} = (\overline{\mathfrak{a}})_v \times (\overline{\mathfrak{a}^{-1}})_v$ gilt $\overline{\mathfrak{a}}^{-1} = \overline{\mathfrak{a}^{-1}}$ nach Lemma 1.10, S. 11. □

Korollar 2.10. *In jedem Ring mit ggT-Theorie sind die v-endlichen v-Ideale v-invertierbar.*[42]

Beweis: Sei $(\alpha_1, \ldots, \alpha_m)_v$ ein v-endliches v-Ideal von D. Ist $\mathfrak{a} = \mathrm{ggT}(\alpha_1, \ldots, \alpha_m) \in \mathfrak{G}$, so gilt aufgrund von Satz 2.6 $\overline{\mathfrak{a}} = (\alpha_1, \ldots, \alpha_m)_v$. Mit Korollar 2.9 folgt die Behautpung. □

Integritätsbereiche, in denen die v-endlichen v-Ideale v-invertierbar sind, heißen *v-Bereiche*.[43] Jeder Ring mit ggT-Theorie ist also ein v-Bereich. Tatsächlich sind Ringe mit ggT-Theorie durch

[40] *Skula 1970* konnte als erster die Entbehrlichkeit des zweiten Borewicz-Šafarevičschen Axioms für Ringe mit Divisorentheorie zeigen. Sein Beweis gründet sich allerdings wesentlich auf die Faktorialität der Divisorenhalbgruppe $\mathfrak{G}^+$ (in Skulas Notation $\mathfrak{D}$) und ist somit auf die hier vorliegende Situation nicht ohne weiteres übertragbar. Außerdem ist Skulas Ansatz im wesentlichen ein multiplikativer, d. h. es werden zunächst rein multiplikative Strukturen untersucht und die Ergebnisse anschließend auf Ringe übertragen.

[41] Vgl. Anmerkung 39, Aussage (2).

[42] Zum Begriff des v-Bereichs vgl. *Gilmer 1992*, S. 418 sowie S. 422, Theorem 34.6. *Bourbaki 1989*, VII, § 1, Exercise 30, spricht von „*regularly closed domains*“, eine Bezeichnung, die sich nicht durchgesetzt hat. Man beachte, daß die v-Idealoperation i. a. *nicht* endlichartig ist. Man kann deshalb (vgl. Satz 1.9, S. 10) *nicht* davon ausgehen, daß in einem v-Bereich die v-Inversen eines v-endlichen Ideals wieder v-endlich sind.

[43] Zum Begriff des v-Bereichs vgl. *Gilmer 1992*, S. 418 sowie S. 422, Theorem 34.6. *Bourbaki 1989*, VII, § 1, Exercise 30, spricht von „*regularly closed domains*“, eine Bezeichnung, die sich nicht durchgesetzt hat. Man beachte, daß die v-Idealoperation i. a. *nicht* endlichartig ist. Man kann deshalb *nicht* davon ausgehen, daß in einem v-Bereich die v-Inversen eines v-endlichen Ideals wieder v-endlich sind.

die v-Bereichseigenschaft bereits hinreichend charakterisiert. Dieses tieferliegende Ergebnis werden wir in Abschnitt 2.6, Satz 2.23, beweisen.

Zuvor jedoch wollen wir unsere Aufmerksamkeit auf eine weitere wichtige Eigenschaft von Ringen mit ggT-Theorie richten: die Ganzabgeschlossenheit.

2.4. Ganzabgeschlossenheit und Multiplikativität des Inhalts

Satz 2.11. *Jeder Ring mit ggT-Theorie ist ganzabgeschlossen.*

Beweis: Der Satz folgt bereits aus der Ganzabgeschlossenheit von v-Bereichen.[44] Wir wollen hier jedoch einen Beweis vorstellen, der allein die definitorischen Eigenschaften eines Ringes mit ggT-Theorie benutzt. Es ist zu zeigen: Jedes $\alpha = \frac{a}{b} \in K^*$ mit $a, b \in D$, das ganz über D ist, ist bereits in D enthalten. Dabei kann der Beweis als erbracht gelten, wenn wir zeigen, daß b ein Teiler von a ist. Als über D ganzes Element genügt $\alpha = \frac{a}{b}$ einer Gleichung

$$a^n = -a_1 a^{n-1} b - a_2 a^{n-2} b^2 - \ldots - a_{n-1} a b^{n-1} - a_n b^n \quad \text{mit } a_i \in D. \tag{2.12}$$

Es seien $\mathfrak{g} := \mathrm{ggT}(a, b)$ und $(a) = \mathfrak{a}_1 \mathfrak{g}$, $(b) = \mathfrak{b}_1 \mathfrak{g}$ mit $\mathfrak{a}_1, \mathfrak{b}_1 \in \mathfrak{G}^+$. Mit Korollar 2.7 folgt

$$\begin{aligned} \mathfrak{g}\mathfrak{b}_1 \mid (b) \quad \text{und} \quad \mathfrak{g} \mid (a) \quad &\Rightarrow \quad \mathfrak{g}^n \mathfrak{b}_1 \quad \text{teilt die rechte Seite von Gleichung (2.12)} \\ &\Rightarrow \quad \mathfrak{g}^n \mathfrak{b}_1 \mid (a)^n = \mathfrak{g}^n \mathfrak{a}_1^n \\ &\Rightarrow \quad \mathfrak{b}_1 \mid \mathfrak{a}_1^n. \end{aligned}$$

Wegen $1 = \mathrm{ggT}\big(\mathfrak{a}_1, \mathfrak{b}_1\big) = \ldots = \mathrm{ggT}\big(\mathfrak{a}_1^n, \mathfrak{b}_1\big) = \mathfrak{b}_1$ folgt daraus $\mathfrak{g} = (b)$. Das bedeutet aber $(b) \mid (a)$, was aufgrund von Axiom (G 1) äquivalent zu $b \mid a$ ist. Also gilt $\frac{a}{b} \in D$. □

Der Beweis macht deutlich, daß man lediglich einige elementare Eigenschaften des größten gemeinsamen Teilers sowie Axiom (G 1) benötigt, um die Ganzabgeschlossenheit eines Ringes mit ggT-Theorie zu zeigen.[45] Nicht einmal das Axiom (G 2) wird gebraucht. Prüfer konnte immerhin zeigen, daß die Ganzabgeschlossenheit eines Ringes auch hinreichend ist, um einen Homomorphismus von D in einen ggT-Monoiden $\mathfrak{G}^+$ zu konstruieren, die zumindest noch Axiom (G 1) erfüllt.[46] I. a. wird die Ganzabgeschlossenheit jedoch keine hinreichende Bedingung für die Existenz einer ggT-Theorie im hier verstandenen Sinne sein. Denn dann wäre das zweite Axiom ja genau genommen überflüssig, was mit Sicherheit nicht der Fall ist. Eine hinreichende Bedingung für die Existenz einer ggT-Theorie muß also stärker als die Ganzabgeschlossenheit sein.

Da offenbar, wie der vorangegangene Abschnitt gezeigt hat, die v-Ideale in Ringen mit ggT-Theorie eine ausgezeichnete Rolle spielen, stellt sich die Frage, ob die Ganzabgeschlossenheit eines Ringes mit ggT-Theorie auch Auswirkungen auf seine v-Idealstruktur hat. Eine Antwort gibt der folgende, in dieser Form wohl erstmalig von Prüfer[47] bewiesene Satz, der eine Verallgemeinerung des berühmten Lemmas von Gauß darstellt.

Satz 2.13. (Dedekind-Prüfer) *Sei D ein Integritätsbereich mit Quotientenkörper K. Seien ferner $f(X) = a_0 + a_1 X + \ldots + a_m X^m$ und $g(X) = b_0 + b_1 X + \ldots + b_n X^n$ Polynome in der*

[44] Vgl. *Gilmer 1992*, S. 400, Corollary 32.8. Gilmer beweist allgemein, daß ein Integritätsbereich ganzabgeschlossen ist, wenn es ein Idealsystem von $*$-Idealen gibt, in dem die $*$-endlichen $*$-Ideale bzgl. der $*$-Multiplikation kürzbar sind. Solche Idealsysteme heißen nach Krull auch *endlich arithmetisch brauchbar*. Da in v-Bereichen die v-Ideale v-invertierbar und damit bzgl. der v-Multiplikation kürzbar sind, sind v-Bereiche also insbesondere ganzabgeschlossen.

[45] Die bekannten Beweise der Ganzabgeschlossenheit von Ringen mit Divisorentheorie machen durchweg von der Existenz einer eindeutigen Primdivisorzerlegung in der Divisorenhalbgruppe $\mathfrak{G}^+$ Gebrauch (siehe z. B. *Borewicz et al. 1966*, S. 192, Satz 3). Der hier vorgestellte Beweis zeigt, daß man bereits mit schwächeren Voraussetzungen, nämlich der Existenz eines größten gemeinsamen Teilers in $\mathfrak{G}^+$, auskommt.

[46] Vgl. *Prüfer 1932*, S. 34ff. Die Konstruktion erfolgt mit Hilfe der weiter unten behandelten Kroneckerschen Funktionalringe von D.

[47] Vgl. *Prüfer 1932*, S. 25, Satz (2) und (2)*.

Unbestimmten X mit $a_j, b_j \in K$ und $f(X) \cdot g(X) = c_0 + c_1X + \ldots + c_{mn}X^{mn}$. Dann sind folgende Aussagen äquivalent:
(1) *D ist ganzabgeschlossen.*
(2) *$c_k \in D$ für $0 \leqslant k \leqslant mn \quad \Leftrightarrow \quad a_ib_j \in D$ für $0 \leqslant i \leqslant m$ und $0 \leqslant j \leqslant n$.*
(3) $(a_0, a_1, \ldots, a_m)_v \times (b_0, b_1, \ldots, b_n)_v = (c_0, c_1, \ldots, c_{mn})_v$.

Beweis: (1) $\Rightarrow$ (2) Hierbei handelt es sich um eine Verallgemeinerung des Prager Satzes von Dedekind.[48] Wir übertragen den ersten von Dedekinds zwei Beweisen auf die vorliegende Situation. Dazu folgende Vorüberlegung: Es seien $h(X) = c_0 + c_1X + \ldots + c_rX^r$ ein Polynom mit Koeffizienten aus D und γ eine Nullstelle von h. Dann läßt sich über dem algebraischen Abschluß $\overline{K}$ von K der Linearfaktor $(X - \gamma)$ abspalten, und man erhält

$$h(X) = (X - \gamma)(c'_0 + c'_1X + \ldots + c'_{r-1}X^{r-1}) \quad \text{mit } c'_k \in \overline{K}.$$

Man überlegt sich leicht, daß wegen $c_0 + c_1\gamma + \ldots + c_r\gamma^r = 0$ und $c'_k = c_{k+1} + c_{k+2}\gamma + \ldots + c_r\gamma^{r-k-1}$ die Produkte $c'_k \cdot 1, c'_k \cdot \gamma, \ldots, c'_k \cdot \gamma^{r-1}$ für alle $k = 0, 1, \ldots, r-1$ als D-Linearkombination von $1, \gamma, \ldots, \gamma^{r-1}$ darstellbar sein müssen. Damit ist aber das charakteristische Polynom eines jeden c'_k ein Polynom mit Koeffizienten aus D, d. h. die c'_k genügen einer Ganzheitsgleichung über D und sind somit in dem ganzen Abschluß $\overline{D}$ von D enthalten. Seien nunmehr f und g zwei Polynome mit Koeffizienten aus dem Körper K, deren Produktpolynom $h = fg$ in $T[X]$ enthalten ist. Über dem algebraischen Abschluß $\overline{K}$ von K mögen beide Polynome wie folgt zerfallen:

$$f(t) = a_m(t - \alpha_1) \cdot \ldots \cdot (t - \alpha_m) \qquad \text{und} \qquad g(t) = b_n(t - \beta_1) \cdot \ldots \cdot (t - \beta_n)$$

mit $a, b \in K$, $\alpha_i, \beta_j \in \overline{K}$. Die Vorüberlegung zeigt, daß $h = fg$ in $\overline{K}[X]$ durch jedes aus gewissen Linearfaktoren $(X - \alpha_i)$ und $(X - \beta_j)$ gebildete Produktpolynom p teilbar ist und man nach Division durch p ein Polynom h_p mit ganzalgebraischen Koeffizienten, also ein Polynom aus $\overline{D}[X]$ erhält. Das absolute Glied dieses Polynoms h_p ist ein Produkt von $a_m \cdot b_n$ sowie, je nach Wahl von p, gewissen α_i und β_j. Genauer gesagt, erhält man als mögliche absolute Glieder von h_p sämtliche Produkte der Form $a_m\alpha \cdot b_n\beta$, wobei α alle denkbaren Produktkombinationen der α_i und β alle denkbaren Produktkombinationen der β_j durchläuft. Nun sind aber die Koeffizienten a_i von f bzw. b_j von g ihrerseits Summen von Produkten der Gestalt $a_m\alpha$ bzw. $b_n\beta$, d. h. jedes Produkt a_ib_j läßt sich als Summe von Produkten der Gestalt $a_m\alpha \cdot b_n\beta$ darstellen. Nach dem eben Gesagten sind die Produkte a_ib_j demzufolge Summen von über D ganzen Zahlen und somit selbst wieder ganz über D. Als Elemente von K sind sie daher in $\overline{D} \cap K$, also — aufgrund der Ganzabgeschlossenheit von D — bereits in D enthalten.

(2) $\Rightarrow$ (3) Es sei $\mu \in K^*$. Nach Voraussetzung sind die Koeffizienten $\frac{1}{\mu}c_k$ des Produktpolynoms $\frac{1}{\mu}f \cdot g$ genau dann ganz, wenn sämtliche Produkte $\frac{1}{\mu}a_i \cdot b_j$ ganz sind. Also ist $c_kD \subseteq \mu D$ äquivalent zu $a_ib_jD \subseteq \mu D$. Aus der Definition für v-Ideale folgt damit sofort $(\ldots, a_ib_j, \ldots)_v = (\ldots, c_k, \ldots)_v$.

(3) $\Rightarrow$ (1) Es sei $\alpha \in K$ ganz über D und $f(X) \in D[X]$ ein normiertes Polynom, das α zur Nullstelle hat. Über K läßt sich von f der Linearfaktor $(X - \alpha)$ abspalten, so daß man eine Polynomgleichung der Gestalt $f(X) = (X - \alpha)\big(b_0 + b_1X + \ldots + b_{n-2}X^{n-2} + X^{n-1}\big)$ mit $b_i \in K$ erhält. Wegen $f(X) \in D[X]$ liegt das von den Koeffizienten von f erzeugte v-Ideal in D, woraus nach Voraussetzung $\alpha \cdot 1 \in D$, also die Ganzabgeschlossenheit von K folgt. □

[48] Der Prager Satz von Dedekind ist eine Verallgemeinerung des Lemmas von Gauß, wonach zwei normierte Polynome über $\mathbb{Q}$ genau dann ganzrationale Koeffizienten besitzen, wenn die Koeffizienten ihres Produktpolynoms ganzrational sind. Er lautet (siehe *Dedekind 1892*, S. 32, § 5, Satz V):

„Wenn das Produkt aus zwei Funktionen A, B [= Polynome aus dem Polynomring $K[X]$] lauter ganze Koeffizienten besitzt, so ist jedes aus einem Koeffizienten von A und einem Koeffizienten von B gebildete Produkt eine ganze Zahl."

Dedekind stellte zwei methodisch grundlegend verschiedene Beweise für seinen Satz vor.

Auch wenn es auf den ersten Blick nicht so scheinen mag: Satz 2.13, insbesondere die unter (3) formulierte Eigenschaft über das v-Produkt v-endlicher v-Ideale, ist für die weitere Untersuchung der Ringe mit ggT-Theorie grundlegend. Er liefert gewissermaßen das Fundament für die im folgenden zu entwickelnde Theorie der sogenannten *Kroneckerschen Funktionalringe* und damit das Fundament für eine allgemeine Theorie des größten gemeinsamen Teilers. Es lohnt sich daher, die Situation noch einmal eingehend zu studieren. Dazu folgende

Definition 2.14. *Es seien D ein beliebiger Integritätsbereich mit Quotientenkörper K und $K[X]$ der Polynomring über K in der Unbestimmten X. Bezeichnet $(\cdot)_*$ eine beliebige $*$-Idealoperation von D und $f(X) = a_0 + a_1X + \ldots + a_mX^m \neq 0$ irgendein Polynom über K, so heißt das von den Koeffizienten $a_i \in K$ erzeugte $*$-Ideal*

$$\mathrm{c}(f)_* := (a_0, a_1, \ldots, a_m)_*$$

*der **$*$-Inhalt** des Polynoms f.*[49] *Ist $\mathrm{c}(f)_* = D$, so wird f auch als **$*$-primitives Polynom** bezeichnet. Besitzt D eine ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$, so heißt der Divisor*

$$\mathrm{c}(f)_D := \mathrm{ggT}(a_0, a_1, \ldots, a_m)$$

*der **D-Inhalt** von f, wobei im Falle $m = 0$ unter $\mathrm{c}(f)_D = \mathrm{c}(a_0)_D$ der Hauptdivsor $(a_0) \in \mathfrak{G}$ zu verstehen ist. Falls $\mathrm{c}(f)_D$ gleich dem Einheitsdivisor ist, so heißt f auch **D-primitiv**.*

Satz 2.13 nimmt in dieser Terminologie folgende Gestalt an: Ein Integritätsbereich D ist ganzabgeschlossen genau dann, wenn die Inhaltsfunktion $\mathrm{c}(\cdot)_v : K[X]^* \to \mathfrak{f}_v(D)$ mit $\mathrm{c}(a_0 + a_1X + \ldots + a_mX^m)_v = (a_0, a_1, \ldots, a_m)_v$ ein Halbgruppenhomomorphismus ist, d. h. wenn für alle $f, g \in K[X]$ stets $\mathrm{c}(f)_v \times \mathrm{c}(g)_v = \mathrm{c}(fg)_v$ gilt. Wir sagen dann auch, der v-Inhalt von Polynomen sei *multiplikativ*. Für Ringe mit ggT-Theorie notieren wir

Korollar 2.15. *Sei D ein Ring mit ggT-Theorie. Dann ist*
(1) *der D-Inhalt multiplikativ mit $\mathrm{c}(f)_D \cdot \mathrm{c}(g)_D = \mathrm{c}(fg)_D$ für alle $f, g \in K[X]$.*
(2) *der v-Inhalt multiplikativ mit $\mathrm{c}(f)_v \times \mathrm{c}(g)_v = \mathrm{c}(fg)_v$ für alle $f, g \in K[X]$.*

Beweis: Nach Korollar 2.8 gilt $\overline{\mathrm{c}(f)_D} = \overline{\mathrm{ggT}(a_0, a_1, \ldots, a_m)} = (a_0, a_1, \ldots, a_m)_v = \mathrm{c}(f)_v$. Unter Verwendung von Korollar 2.9 und Axiom (G 2) ergibt sich hieraus

$$\begin{aligned} \mathrm{c}(f)_v \times \mathrm{c}(g)_v = \mathrm{c}(fg)_v \quad &\Leftrightarrow \quad \overline{\mathrm{c}(f)_D} \times \overline{\mathrm{c}(g)_D} = \overline{\mathrm{c}(f)_D \cdot \mathrm{c}(g)_D} = \overline{\mathrm{c}(fg)_D} \\ &\Leftrightarrow \quad \mathrm{c}(f)_D \cdot \mathrm{c}(g)_D = \mathrm{c}(fg)_D. \end{aligned}$$

Da D nach Satz 2.11 jedoch ganzabgeschlossen und der v-Inhalt bzgl. D somit multiplikativ ist, folgt daraus insgesamt die Behauptung. □

Ist D ein Ring mit ggT-Theorie, so werden also beide Inhaltsfunktionen $\mathrm{c}(\cdot)_D : K[X]^* \to \mathfrak{G}$ und $\mathrm{c}(\cdot)_v : K[X]^* \to \mathfrak{F}_v(D)$ zu Halbgruppenhomomorphismen. Diese wiederum lassen sich in kanonischer Weise zu wohldefinierten Homomorphismen auf den Quotientenkörper von $K[X]$, also auf den rationalen Funktionenkörper $K(X)$ über K in der Unbestimmten X, fortsetzen. Wir können dementsprechend die Inhaltsdefinition auf rationale Funktionen über K ausdehnen.

Definition 2.16. *Sei D ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$. Dann heißen die wohldefinierten Homomorphismen $\mathrm{c}(\cdot)_v : K(X)^* \to \mathfrak{F}_v(D)$ bzw. $\mathrm{c}(\cdot)_D : K(X)^* \to \mathfrak{G}$ mit*

$$\mathrm{c}(f)_v := \mathrm{c}(f_1)_v \times \mathrm{c}(f_2)_v^{-1} \quad \textit{bzw.} \quad \mathrm{c}(f)_D := \mathrm{c}(f_1)_D \cdot \mathrm{c}(f_2)_D^{-1} \quad \textit{für alle } f = \frac{f_1}{f_2} \in K(X),$$

*$f_1, f_2 \in K[X]$, v- bzw. D-**Inhaltsfunktion** der ggT-Theorie $(\cdot)$. Das v-Ideal $\mathrm{c}(f)_v$ (bzw. der Divisor $\mathrm{c}(f)_D$) heißt **v-Inhalt** (bzw. D-Inhalt) der rationalen Funktion f. Ist $\mathrm{c}(f)_v = D$ (bzw. $\mathrm{c}(f)_D = (1)$), so heißt f **v-primitiv** (bzw. D-primitiv).*

[49] „$\mathrm{c}(f)$“ steht für „content of f“.

2.5. Die Konstruktion einer ggT-Theorie nach Kronecker

Man mag sich fragen, worin der Vorteil liegt, anstelle der Elemente aus K Polynome (bzw. rationale Funktionen) über K zu betrachten. In der Tat erscheint dieser Gedanke nicht gerade naheliegend, und dennoch erweist er sich als überaus hilfreich, wenn es darum geht, eine ggT-Theorie für D in Abhängigkeit von D explizit zu beschreiben.

Es war — so jedenfalls stellt es sich dem heutigen Betrachter dar — Kroneckers Idee, in dem Funktionenkörper $K(X)$ in bestimmter Weise ganze Elemente auszuzeichnen. Prüfer gelang es, Kroneckers Verfahren zur Konstruktion dieser ganzen Elemente transparent zu machen und den Nachweis zu führen, daß die ganzen Elemente einen Ring, genau genommen, einen Bezoutbereich bilden, der aus dem Grundkörper K nur die ganzen Elemente, also die Elemente aus D, enthält. Krull schließlich führte für Integritätsbereiche dieser Gestalt die Bezeichnung *Kroneckerscher Funktionalring* ein.

Der Kroneckersche Funktionalring liefert als ggT-Bereich insbesondere einen größten gemeinsamen Teiler für die Elemente des Grundrings D. Die in ihm enthaltenen rationalen Funktionen werden so zu Divisoren, sogenannten *Kronecker-Divisoren*, für die Elemente aus D.

Wir wollen diese Vorgehensweise eingehender studieren. Dazu sei D ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$. Durch die zugehörige Inhaltsfunktion $\mathrm{c}(\cdot)_D : K(X)^* \to \mathfrak{G}$ erscheint folgende Möglichkeit, gewisse Elemente in dem rationalen Funktionenkörper $K(X)$ als *ganz* auszuzeichnen, besonders naheliegend: $f \in K(X)$ heiße *ganz* in $K(X)$ genau dann, wenn $\mathrm{c}(f)_D$ ein ganzer Divisor in $\mathfrak{G}$ ist. Über die in diesem Sinne ganzen Elemente eines rationalen Funktionenkörpers $K(X)$ gilt der folgende zentrale Satz.

Satz und Definition 2.17. *Es seien D ein Ring mit ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ und $K(X)$ der Körper der rationalen Funktionen über dem Quotientenkörper K von D in der Unbestimmten X. Es bezeichne $D^{\mathfrak{G}} = \{f \in K(X) : \mathrm{c}(f)_D \in \mathfrak{G}^+\}$ die Menge aller ganzen Elemente in $K(X)$ bzgl. D. Dann gilt:*

(1) *$D^{\mathfrak{G}}$ ist ein Integritätsbereich mit Quotientenkörper $K(X)$, der sogenannte **Kroneckersche Funktionalring** von D bzgl. der ggT-Theorie $D^* \to \mathfrak{G}^+$. Die Einheitengruppe von $D^{\mathfrak{G}}$ ist gegeben durch $D^{\mathfrak{G}\times} = \{f \in K(X) : \mathrm{c}(f)_D = (1)\}$.*

(2) *$D^{\mathfrak{G}} \cap K = D$.*

(3) *Das von $\frac{f_1}{g}, \ldots, \frac{f_m}{g} \in K(X)$, $f_i, g \in D[X]$, erzeugte $D^{\mathfrak{G}}$-Ideal ist gleich dem Hauptideal $\frac{f}{g}D^{\mathfrak{G}}$ mit $f(X) = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$ und geeignet gewählten Exponenten r_i, beispielsweise mit $r_1 = 0$ und $r_{i+1} = i \cdot \big(1 + \max\limits_{1 \leqslant j \leqslant m} \{\mathrm{grad} f_j\}\big)$ für $i = 1, \ldots, m-1$.*

(4) *$D^{\mathfrak{G}}$ ist ein Bezoutbereich.*

Beweis: Ad (1) Da $K(X)$ Quotientenkörper des Polynomringes $D[X]$ und $D^{\mathfrak{G}}$ eine Teilmenge von $K(X)$ ist, läßt sich jedes Element aus $D^{\mathfrak{G}}$ als Quotient zweier Elemente aus $D[X]$ darstellen. Aufgrund der Wohldefiniertheit der Inhaltsfunktion ist der D-Inhalt einer ganzen rationalen Funktion aus $D^{\mathfrak{G}}$ von dieser Darstellung unabhängig, d. h. wir können $D^{\mathfrak{G}}$ auch schreiben als

$$D^{\mathfrak{G}} = \Big\{ \frac{f}{g} \in K(X) : f, g \in D[X] \text{ mit } \mathrm{c}(g)_D \mid \mathrm{c}(f)_D \text{ in } \mathfrak{G} \Big\}.$$

Mit der auf $K(X)$ definierten Addition und Multiplikation sowie mit dem Null– und dem Einselement aus $K(X)$ wird diese Menge zu einem Integritätsbereich. Dazu seien $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in D^{\mathfrak{G}}$ mit $f_i, g_i \in D[X]$. Aus $\mathrm{c}(f_i)_D \mid \mathrm{c}(g_i)_D$ folgt dann aufgrund der Multiplikativität des D-Inhalts (vgl. Satz 2.15)

$$\mathrm{c}(f_1 f_2)_D = \mathrm{c}(f_1)_D \cdot \mathrm{c}(f_2)_D \mid \mathrm{c}(g_1)_D \cdot \mathrm{c}(g_2)_D = \mathrm{c}(g_1 g_2)_D,$$

also

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2} \in D^{\mathfrak{G}}.$$

Damit ist gezeigt, daß $D^{\mathfrak{G}}$ eine bzgl. der Multiplikation abgeschlossene Teilmenge von $K(X)$ ist. Da in der Divisorengruppe $\mathfrak{G}$ die Kürzungsregel gilt, kann man in $D^{\mathfrak{G}}$ darüber hinaus in gewohnter Weise erweitern und kürzen. Wir können also davon ausgehen, daß zwei Elemente aus $D^{\mathfrak{G}}$, gegebenenfalls nach entsprechender Erweiterung, stets denselben Nenner besitzen. Aufgrund von Satz 2.7 gilt daher

$$\mathrm{c}(g)_D \mid \mathrm{c}(f_1)_D, \quad \mathrm{c}(g)_D \mid \mathrm{c}(f_2)_D \quad \Rightarrow \quad \mathrm{c}(g)_D \mid \mathrm{c}(f_1 + f_2)_D,$$

also

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \in D^{\mathfrak{G}},$$

womit auch die Abgeschlossenheit der Addition in $D^{\mathfrak{G}}$ gezeigt ist. Insgesamt ist damit $D^{\mathfrak{G}}$ als Integritätsbereich mit Quotientenkörper $K(X)$ nachgewiesen. Die Aussage über die Gestalt der Einheitengruppe von $D^{\mathfrak{G}}$ ergibt sich aus folgender einfacher Überlegung: Ein Element $\frac{f}{g} \in K(X)$ ist genau dann eine Einheit, wenn mit $\frac{f}{g}$ auch $\frac{g}{f}$ in $D^{\mathfrak{G}}$ liegt. Dies ist jedoch gleichbedeutend mit $\mathrm{c}(f)_D \mid \mathrm{c}(g)_D$ und $\mathrm{c}(g)_D \mid \mathrm{c}(f)_D$, also $\mathrm{c}(f)_D = \mathrm{c}(g)_D$ bzw. $\mathrm{c}(\frac{f}{g})_D = (1)$.

Ad (2) Die Inklusion „$\supseteq$“ ist trivial. Sei also $\frac{f}{g} \in D^{\mathfrak{G}} \cap K$ mit $f, g \in D[X]$. Wegen $\frac{f}{g} \in K$ existieren $a, b \in D$ und ein $h \in K[X]$ mit $f = ah$, $g = bh$ und $\frac{f}{g} = \frac{ah}{bh} = \frac{a}{b}$. Aus $\mathrm{c}(f)_D = \mathrm{c}(ah)_D = a \cdot \mathrm{c}(h)_D$ und $\mathrm{c}(g)_D = \mathrm{c}(bh)_D = b \cdot \mathrm{c}(h)_D$ folgt wegen $\mathrm{c}(g)_D \mid \mathrm{c}(f)_D$ nun aber $b \mid a$, womit $\frac{f}{g} = \frac{a}{b} \in D$ gezeigt ist.

Ad (3) Es reicht zu zeigen, daß das Polynom $f = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$ bzgl. $D^{\mathfrak{G}}$ ein größter gemeinsamer Teiler von $f_1, \ldots, f_m$ ist. Da die Exponenten r_i gerade so gewählt sind, daß in f keine Monome gleichen Grades auftreten, gilt $\mathrm{c}(f)_D \mid \mathrm{c}(f_i)_D$ bzgl. $\mathfrak{G}^+$, und man erhält

$$\frac{f_i}{f} \in D^{\mathfrak{G}}, \quad \text{also} \quad f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m} \mid f_i \quad \text{bzgl. } D^{\mathfrak{G}}.$$

Für jeden weiteren Teiler $\frac{p}{q} \in D^{\mathfrak{G}*}$ von f_i gilt wegen $\mathrm{c}(p)_D \mid \mathrm{c}(f_i q)_D$

$$\frac{f \cdot q}{p} \in D^{\mathfrak{G}}, \quad \text{also} \quad \frac{p}{q} \mid f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m} \quad \text{bzgl. } D^{\mathfrak{G}}.$$

Damit ist $f = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$ als größter gemeinsamer Teiler von $f_1, \ldots, f_m$ nachgeweisen.

Ad (4) Nach Aussage (3) ist $D^{\mathfrak{G}}$ ein ggT-Bereich, in dem sich jeder größte gemeinsame Teiler von jeweils endlich vielen Elementen aus $D^{\mathfrak{G}}$ als $D^{\mathfrak{G}}$-Linearkombination eben dieser Elemente darstellen läßt. Daher ist $D^{\mathfrak{G}}$ insbesondere ein Bezoutbereich. □

Aufgrund von Satz 2.17.(4) handelt es sich bei dem Kroneckerschen Funktionalring $D^{\mathfrak{G}}$ von D um einen ggT-Bereich. Insbesondere ist seine Teilbarkeitshalbgruppe $D^{\mathfrak{G}*}/D^{\mathfrak{G}\times}$ ein ggT-Monoid, der den Homomorphismus

$$[\,\cdot\,] : D^* \longrightarrow D^{\mathfrak{G}*}/D^{\mathfrak{G}\times} \tag{2.18}$$

zu einer weiteren ggT-Theorie für D macht. Denn tatsächlich sind die beiden Axiome (G 1) und (G 2) erfüllt. So gilt wegen Satz 2.17.(2) für $\alpha, \beta \in D^*$

$$\alpha \mid \beta \text{ in } D \quad \Leftrightarrow \quad \frac{\beta}{\alpha} \in D = D^{\mathfrak{G}} \cap K \quad \Leftrightarrow \quad \alpha \mid \beta \text{ in } D^{\mathfrak{G}},$$

womit Axiom (G 1) nachgewiesen ist. Aus der Definition der D-Inhaltsfunktion erhält man für beliebige rationale Funktionen $f, g \in D^{\mathfrak{G}} \subseteq K(X)$

$$\overline{[\,f\,]} = \{\mu \in K : f \mid \mu \text{ in } D^{\mathfrak{G}}\} = \{\mu \in K : \mathrm{c}(f)_D \mid (\mu) \text{ in } \mathfrak{G}^+\} = \overline{\mathrm{c}(f)_D}.$$

Aufgrund der Gültigkeit von Axiom (G 2) für die ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ folgt hieraus

$$\overline{[\,f\,]} = \overline{[\,g\,]} \quad \Leftrightarrow \quad \overline{\mathrm{c}(f)_D} = \overline{\mathrm{c}(g)_D} \quad \Leftrightarrow \quad \mathrm{c}(f)_D = \mathrm{c}(g)_D.$$

Damit sind jedoch f und g bzgl. $D^{\mathfrak{G}}$ zueinander assoziiert, und es folgt $[\,f\,] = [\,g\,]$, womit auch Axiom (G 2) gezeigt ist.

Die ggT-Theorie (2.18) ist unter allen ggT-Theorien für D ausgezeichnet. Dazu überlege man sich, daß aufgrund der Äquivalenz der Bedingungen $\mathrm{c}(f)_D \in \mathfrak{G}^+$ und $\mathrm{c}(f)_v \subseteq D$ jeder Kroneckersche Funktionalring $D^{\mathfrak{G}}$ auch geschrieben werden kann als

$$D^{\mathfrak{G}} = \{f \in K(X) : \mathrm{c}(f)_v \subseteq D\}.$$

Diese Darstellung ist jedoch völlig unabhängig von etwaigen speziellen Eigenschaften der $D^{\mathfrak{G}}$ zugrundeliegenden ggT-Theorie. Sie hängt allein von der v-Idealoperation auf D ab. Zu jedem Ring K mit ggT-Theorie gibt es somit nur einen einzigen Kroneckerschen Funktionalring und damit auch nur eine einzige ggT-Theorie der Gestalt (2.18). Um diesen Sachverhalt auch in der Notation zum Ausdruck zu bringen, werden wir im folgenden *den* Kroneckerschen Funktionalring von D mit

$$D^v = \left\{\frac{f}{g} \in K(X) : f, g \in D[X] \text{ mit } \mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v\right\} \tag{2.19}$$

bezeichnen, eine Schreibweise, die auch in der Literatur verbreitet ist.[50] Außerdem führen wir folgende Bezeichnungsweise ein:

Definition 2.20. *Es sei D ein Ring mit ggT-Theorie. Dann heißt der Halbgruppenhomomorphismus $[\,\cdot\,] : D^* \to D^{v*}/D^{v\times}$ **Kroneckersche ggT-Theorie** von D. Die Elemente von D^v bzw. von $D^{v*}/D^{v\times}$ werden als **ganze**, die Elemente von $K(X)$ bzw. von $K(X)^*/D^{v\times}$ entsprechend als **gebrochene Kronecker-Divisoren** bezeichnet.*

Die Kroneckersche ggT-Theorie $[\,\cdot\,] : D^* \to D^{v*}/D^{v\times}$ ist die „kleinste" aller ggT-Theorien für D, und zwar in dem Sinne, daß die Divisorenhalbgruppe $D^{v*}/D^{v\times}$ keine überflüssigen Divisoren enthält. Formal ausgedrückt: Wenn $(\cdot) : D^* \to \mathfrak{G}^+$ eine weitere ggT-Theorie von D ist, so ist die Kroneckersche Divisorenhalbgruppe $D^{v*}/D^{v\times}$ zu einem Untermonoiden von $\mathfrak{G}^+$ isomorph dergestalt, daß für alle $\alpha \in D^*$ der Hauptdivisor $[\,\alpha\,]$ auf den Hauptdivisor (α) abgebildet wird. Dazu weist man nach, daß die Abbildung

$$\begin{aligned} \varphi : D^{v*}/D^{v\times} &\longrightarrow \mathfrak{G}^+ \\ [\,f\,] &\longmapsto \mathrm{c}(f)_D \end{aligned}$$

ein wohldefinierter Monomorphismus ist. Wohldefiniertheit und Injektivität der Abbildung φ ergeben sich aus folgenden Äquivalenzen:

$$[\,f\,] = [\,g\,] \quad \Leftrightarrow \quad \mathrm{c}(f)_v = \mathrm{c}(g)_v \quad \Leftrightarrow \quad \overline{\mathrm{c}(f)_D} = \overline{\mathrm{c}(g)_D} \quad \Leftrightarrow \quad \mathrm{c}(f)_D = \mathrm{c}(g)_D.$$

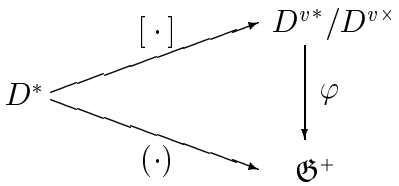
Die Homomorphie ist wegen $[\,f\,] \cdot [\,g\,] = [\,fg\,]$ und $\mathrm{c}(f)_D \cdot \mathrm{c}(g)_D = \mathrm{c}(fg)_D$ ebenfalls klar. Da der D-Inhalt einer konstanten rationalen Funktion $\alpha \in D^*$ dem Hauptdivisor (α) entspricht, ergibt sich ferner, daß durch den Monomorphismus φ der Hauptdivisor $[\,\alpha\,] \in D^{v*}/D^{v\times}$ auf den Hauptdivisor $(\alpha) \in \mathfrak{G}^+$ abgebildet wird. Zusammenfassend halten wir fest:

Satz 2.21. *Jede ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ für D faktorisiert über der Kroneckerschen ggT-Theorie $[\,\cdot\,] : D^* \to D^{v*}/D^{v\times}$, d. h. es gibt einen injektiven Homomorphismus $\varphi : D^{v*}/D^{v\times} \to \mathfrak{G}^+$, der das folgende Diagramm kommutativ macht:*

[50] *Prüfer 1932*, S. 34, definiert Kroneckersche Funktionalringe allgemein für ganzabgeschlossene Integritätsbereiche, und zwar bzgl. eines endlich arithmetisch brauchbaren $*$-Idealsystems (vgl. Anmerkung 44, S. 20). Die Definition hat dann folgende Gestalt:

$$D^{(*)} = \left\{\frac{f}{g} \in K(X) : f, g \in D[X] \text{ mit } \mathrm{c}(f)_* \subseteq \mathrm{c}(g)_*\right\}.$$

Für den Kroneckerschen Funktionalring D^d bzgl. der d-Idealoperation schreibt man häufig auch D^κ.



Der größte gemeinsame Teiler von $\alpha_1, \ldots, \alpha_m \in K^*$ ist in der Kroneckerschen ggT-Theorie durch $\mathrm{ggT}(\alpha_1, \ldots, \alpha_m) = [\,\alpha_0 + \alpha_1 X + \ldots + \alpha_m X^m\,]$ *gegeben.*

Im Hinblick auf die Frage nach der Eindeutigkeit einer ggT-Theorie ergibt sich hieraus

Korollar 2.22. *Ein Ring mit ggT-Theorie besitzt genau dann (bis auf Isomorphie) nur eine einzige ggT-Theorie, wenn für jede Divisorenhalbgruppe $\mathfrak{G}^+$ der Homomorphismus φ aus Satz 2.21 stets surjektiv, also insgesamt ein Isomorphismus ist.*

Der Eindeutigkeitssatz gilt für ggT-Theorien demzufolge nur dann, wenn zu jedem ganzen Divisor $\mathfrak{a} \in \mathfrak{G}^+$ eine rationale Funktion $\frac{f}{g} \in D^v$, $f, g \in D[X]$, mit $\mathrm{c}(\frac{f}{g})_D = \mathrm{c}(f)_D \cdot \mathrm{c}(g)_D^{-1} = \mathfrak{a}$ existiert. Also genau dann, wenn jeder Divisor $\mathfrak{a} \in \mathfrak{G}^+$ die Gestalt

$$\mathfrak{a} = \frac{\mathrm{ggT}(\alpha_1, \ldots, \alpha_m)}{\mathrm{ggT}(\beta_1, \ldots, \beta_n)} \quad \text{mit } \alpha_i, \beta_i \in D^*$$

hat. Die Frage, ob Axiom (G 2) die Elemente der Divisorenhalbgruppe $\mathfrak{G}^+$ in dieser Weise determiniert, muß hier leider offen bleiben.

2.6. Verschiedene Charakterisierungen für Ringe mit ggT-Theorie

Satz 2.23. *Es seien D ein Integritätsbereich mit Quotientenkörper K und D^v die in* (2.19) *beschriebene Menge rationaler Funktionen von $K(X)$. Dann sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit ggT-Theorie.*
(2) *D ist ein v-Bereich.*
(3) *D^v ist ein Bezoutbereich mit Quotientenkörper $K(X)$.*
(4) *D^v ist ein Prüferbereich mit Quotientenkörper $K(X)$.*
(5) *D^v ist ein ggT-Bereich mit Quotientenkörper $K(X)$.*
(6) *D^v ist ein Ring mit ggT-Theorie und Quotientenkörper $K(X)$.*
(7) *D^v ist ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper $K(X)$.*

Beweis: (1) $\Rightarrow$ (2) ist klar, da jeder Ring mit ggT-Theorie nach Korollar 2.10 ein v-Bereich ist. (3) $\Rightarrow$ (4) $\Rightarrow$ (6) sowie (3) $\Rightarrow$ (5) $\Rightarrow$ (6) sind trivial. Die Implikation (6) $\Rightarrow$ (7) ergibt sich unmittelbar aus Satz 2.11. Bleiben also (2) $\Rightarrow$ (3) und (7) $\Rightarrow$ (1) zu zeigen.

(2) $\Rightarrow$ (3) Sei D ein v-Bereich. Dann ist D ganzabgeschlossen,[51] der v-Inhalt also multiplikativ. Man kann daher im Beweis von Satz 2.17.(3) statt der D-Inhalte die entsprechenden v-Inhalte betrachten sowie die Teilbarkeits– durch die zugehörigen Inklusionsbeziehungen ersetzen und erhält völlig analog, daß D^v ein Bezoutbereich mit Quotientenkörper $K(X)$ ist.[52]

(7) $\Rightarrow$ (1) Die Menge D^v sei, versehen mit der Addition und Multiplikation aus $K(X)$, ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper $K(X)$. Wir zeigen zunächst, daß dann der Integritätsbereich D ganzabgeschlossen ist. Sei $\frac{a}{b} \in K^*$ mit $a, b \in D^*$. Dann gilt $\frac{a}{b} \in D^v$

[51] Vgl. Anmerkung 44.

[52] Der Beweis behält selbst dann seine Gültigkeit, wenn man statt der v-Idealoperation eine beliebige endlich arithmetisch brauchbare $*$-Idealoperation betrachtet. Denn dann ist der $*$-Inhalt, wie *Prüfer 1932*, S. 24, Satz 1, gezeigt hat, multiplikativ, und alle Beweisschritte übertragen sich entsprechend. Man erhält schließlich einen Bezoutbereich der Gestalt $\{f \in K(X) : \mathrm{c}(f)_* \subseteq D\}$ mit Quotientenkörper $K(X)$, den sogenannten Kroneckerschen Funktionalring $D^{(*)}$ von K bzgl. der $*$-Idealoperation (vgl. Anmerkung 50 sowie *Gilmer 1992*, S. 398, Theorem 32.7).

genau dann, wenn $aD = \mathrm{c}(a)_v \subseteq \mathrm{c}(b)_v = bD$, also $\frac{a}{b} \in D$. Daher ist $D^v \cap K = D$. Wenn nun ein $\alpha \in K^*$ ganz über D ist, so ist es als Element von $K(X)$ insbesondere ganz über D^v, liegt also aufgrund der Ganzabgeschlossenheit von D^v in $D^v \cap K = D$. Also ist auch D ganzabgeschlossen. Mit Satz 2.13 ergibt sich daraus, daß der v-Inhalt über K bzgl. D multiplikativ ist, daß also $\mathrm{c}(f)_v \times \mathrm{c}(g)_v = \mathrm{c}(fg)_v$ für alle $f, g \in K[X]$ gilt. Wir zeigen, daß dies bereits die v-Kürzbarkeit der v-endlichen v-Ideale in $\mathfrak{f}_v(D)$ impliziert. Dazu sei $\frac{f}{g} \in D^v$ mit $f, g \in D[X]$. Da D^v ein Integritätsbereich mit Quotientenkörper $K(X)$ ist, kann man in D^v in gewohnter Weise erweitern und kürzen. Es gilt also $\frac{f}{g} = \frac{fh}{gh} \in D^v$ für alle Polynome $h \in D[X]$, woraus aufgrund der v-Multiplikativität

$$\mathrm{c}(f)_v \times \mathrm{c}(h)_v \subseteq \mathrm{c}(g)_v \times \mathrm{c}(h)_v \quad \Leftrightarrow \quad \mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v \quad \text{für alle } h \in D[X]$$

folgt. Die v-endlichen v-Ideale sind also in $\mathfrak{f}_v(D)$ v-kürzbar, ja sogar v-invertierbar. Dazu überlege man sich, daß für ein v-endliches v-kürzbares v-Ideal $\mathfrak{a}$ und ein Element $\mu \in K^*$ stets

$$\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mu D \quad \Leftrightarrow \quad (\mu^{-1}\mathfrak{a})\mathfrak{a}^{-1} \subseteq D \quad \Leftrightarrow \quad \mu^{-1}\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1} = \mathfrak{a}_v = \mathfrak{a} \quad \Leftrightarrow \quad \mu^{-1}D \subseteq D$$

gilt. Daraus folgt jedoch mit der Definition für v-Ideale $(\mathfrak{a}\mathfrak{a}^{-1})_v = D$, womit $\mathfrak{a}$ als v-invertierbar nachgewiesen ist.[53] D ist demzufolge ein v-Bereich. Aufgrund von (2) $\Rightarrow$ (3) ist D^v insbesondere ein Bezoutbereich und damit $D^{v*}/D^{v\times}$ ein ggT-Monoid. Der Halbgruppenhomomorphismus $[\,\cdot\,] : D^* \to D^{v*}/D^{v\times}$ liefert nunmehr eine ggT-Theorie für D. Denn wegen $D^v \cap K = D$ ist, wie man leicht sieht, Axiom (G 1) erfüllt. Axiom (G 2) folgt aus der Tatsache, daß für jedes $f \in D^v$ aufgrund der v-Inhaltsdefinition 2.16 stets $\overline{[\,f\,]} = \{\mu \in K : f \mid \mu \text{ bzgl. } D^v\} = \mathrm{c}(f)_v$ gilt, also

$$\overline{[\,f\,]} = \overline{[\,g\,]} \quad \Leftrightarrow \quad \mathrm{c}(f)_v = \mathrm{c}(g)_v \qquad \text{für alle } f, g \in D^v.$$

Daraus ergibt sich, daß f und g bzgl. D^v assoziiert sind und somit $[\,f\,] = [\,g\,]$ gilt. □

Korollar 2.24. *Es sei D ein Integritätsbereich mit Quotientenkörper K. Ist $\mathfrak{g}_v(D) := \{\mathfrak{a}_v \times \mathfrak{b}_v^{-1} : \mathfrak{a}, \mathfrak{b}$ ganze, endlich erzeugte D-Ideale$\}$ und bezeichnet $\mathfrak{g}_v^+(D)$ die Menge der in $\mathfrak{g}_v(D)$ ganzen v-Ideale, so sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit ggT-Theorie.*
(2) *Die Menge $\mathfrak{g}_v(D)$ ist eine Gruppe bzgl. der v-Multiplikation.*
Ist eine der äquivalenten Bedingungen erfüllt, so ist $\mathfrak{g}_v^+(D)$ insbesondere ein ggT-Monoid, und der Homomorphismus $(\cdot)_v : D^* \to \mathfrak{g}_v^+(D)$ mit $\alpha \mapsto (\alpha)_v = \alpha D$ liefert eine zur Kroneckerschen ggT-Theorie isomorphe ggT-Theorie für D. Der größte gemeinsame Teiler von endlich vielen Hauptdivisoren $(\alpha_1)_v, \ldots, (\alpha_m)_v$, $\alpha_i \in K^*$, ist in dieser ggT-Theorie gegeben durch $\mathrm{ggT}(\alpha_1, \ldots, \alpha_m) = (\alpha_1, \ldots, \alpha_m)_v$.

Beweis: Die Äquivalenz der Aussagen (1) und (2) ergibt sich unmittelbar aus Satz 2.23. Denn ist D ein Ring mit ggT-Theorie, so ist D ein v-Bereich, d. h. alle v-endlichen v-Ideale und demzufolge auch alle v-Ideale aus $\mathfrak{g}_v(D)$ sind v-invertierbar. Damit wird aber die Menge $\mathfrak{g}_v(D)$ bzgl. der v-Multiplikation zu einer Untergruppe aller v-invertierbaren v-Ideale von D. Ist umgekehrt $\mathfrak{g}_v(D)$ eine Gruppe bzgl. der v-Multiplikation, so ist wegen $\mathfrak{f}_v(D) \subseteq \mathfrak{g}_v(D)$ D ein v-Bereich, also ein Ring mit ggT-Theorie.

Für den zweiten Teil der Aussage sei eine der beiden äquivalenten Bedingungen erfüllt. Dann ist $\mathfrak{g}_v^+(D)$ bzgl. der v-Multiplikation ein abelscher Monoid mit Quotientengruppe $\mathfrak{g}_v(D)$. Es reicht somit zu zeigen, daß die Abbildung $D^{v*}/D^{v\times} \to \mathfrak{g}_v^+(D)$ mit $[\,f\,] \mapsto \mathrm{c}(f)_v$, $f \in D^v$, ein wohldefinierter Isomorphismus ist, bei dem Elemente der Gestalt $[\,\alpha\,]$, $\alpha \in D^*$, auf $(\alpha)_v = \alpha D$ abgebildet werden. Denn dann ist $\mathfrak{g}_v^+(D)$ als ggT-Monoid nachgewiesen und zugleich der Beweis erbracht,

[53] Wir haben eben demnach die Äquivalenz folgender drei Aussagen bewiesen: (1) D ist ein v-Bereich. (2) $\mathfrak{a}_v \times \mathfrak{b}_v = \mathfrak{a}_v \times \mathfrak{c}_v \Rightarrow \mathfrak{b}_v = \mathfrak{c}_v$ für alle $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathfrak{f}(D)$. (3) $(\mathfrak{a}_v : \mathfrak{a}_v) = D$ für alle $\mathfrak{a} \in \mathfrak{f}(D)$. Vgl. hierzu auch *Gilmer 1992*, S. 420, Proposition 34.2.(3).

daß die angegebene Abbildung $(\cdot)_v : D^* \to \mathfrak{g}_v^+(D)$ eine zur Kroneckerschen ggT-Theorie isomorphe ggT-Theorie für D ist. Daß es sich bei der Abbildung $[\, f \,] \mapsto \mathrm{c}(f)_v$ um einen wohldefinierten Monomorphismus handelt, ist unmittelbar klar. Die Surjektivität folgt aus der Tatsache, daß es zu jedem ganzen v-endlichen v-Ideal $\mathfrak{a}_v$ ein Polynom $f \in D[X]$ mit genau diesem v-Inhalt gibt. Daher läßt sich jedes v-Ideal $\mathfrak{a}_v \times \mathfrak{b}_v^{-1} \in \mathfrak{g}_v^+(D)$ schreiben als $\mathrm{c}(f)_v \times \mathrm{c}(g)_v^{-1}$, $f, g \in D[X]$, d. h. als ein v-Ideal, das den Kronecker-Divisor $[\, \frac{f}{g} \,]$ als Urbild hat. □

Definition 2.25. *Es sei D ein Ring mit ggT-Theorie. Dann heißt die ggT-Theorie $(\cdot)_v : D^* \to \mathfrak{g}_v^+(D)$ aus Korollar 2.24* ***Prüfersche ggT-Theorie****.*

In Anknüpfung an den vorangegangenen Abschnitt ist eine ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ für D demzufolge genau dann (bis auf Isomorphie) eindeutig bestimmt, wenn für alle Divisoren $\mathfrak{a} \in \mathfrak{G}^+$ stets $\overline{\mathfrak{a}} \in \mathfrak{g}_v^+(D)$ gilt. Oder äquivalent: wenn $\mathfrak{g}_v^+(D)$ innerhalb der Gruppe aller v-invertierbaren v-Ideale von D der einzige ggT-Untermonoid ist, in dem die ganzen v-endlichen v-Ideale von D enthalten sind.

Mit Satz 2.23 werden alle Ergebnisse der kommutativen Algebra über v-Bereiche für Ringe mit ggT-Theorie erschlossen und nutzbar gemacht. Insbesondere gibt es eine Vielzahl idealtheoretischer, sowohl notwendiger als auch hinreichender Kriterien für v-Bereiche, die weitere Charakterisierungen für Ringe mit ggT-Theorie liefern.[54]

2.7. Der ganze Abschluß von Ringen mit ggT-Theorie

Ist D ein Ring mit Divisorentheorie, so besitzt der ganze Abschluß T von D in einer *endlichen* Körpererweiterung L/K ebenfalls eine Divisorentheorie.[55] Für Ringe mit ggT-Theorie gilt sogar

Satz 2.26. *Es seien D ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper K und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Genau dann ist T ein Ring mit ggT-Theorie/v-Bereich, wenn D ein Ring mit ggT-Theorie/v-Bereich ist.*[56]

Für den Beweis dieses Satzes benötigen wir eine Aussage, die in dieser Form erstmalig von Krull bewiesen wurde und die insofern allgemeine Gültigkeit besitzt, als sie nicht nur für Ringe mit ggT-Theorie, sondern für beliebige ganzabgeschlossene Integritätsbereiche gilt.

Um in diesem Zusammenhang die v-Idealoperation bzgl. D von der v-Idealoperation bzgl. T besser unterscheiden zu können, fügen wir jeweils einen entsprechenden Indexbuchstaben hinzu: Für die v-Idealoperation auf D schreiben wir dann $(\cdot)_{v_D}$ im Unterschied zur v-Idealoperation $(\cdot)_{v_T}$ auf T. Krull bewies folgenden Zusammenhang zwischen v_D- und v_T-Idealen:

Lemma 2.27. (Krull) *Sei D ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper K und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Dann gilt $\mathfrak{a}_{v_D} = \mathfrak{a}_{v_T} \cap K$ für alle D-Ideale $\mathfrak{a}$.*[57]

---

[54] Zu nennen sind in diesem Zusammenhang vor allem zwei Arbeiten von Anderson, Mott, Zafrullah u. a. aus dem Jahre 1989. In *Anderson et al. 1989a* sowie *Anderson et al. 1989b*, S. 465, Theorem 4.1, werden über 25 verschiedene Charakterisierungen für v-Bereiche bewiesen.

[55] *Borewicz et al. 1966*, S. 212, Satz 1. Siehe auch Abschnitt 3.4, insbesondere Satz 3.16, S. 41.

[56] Bei *Becker 1992* wird gezeigt, daß der ganze Abschluß eines ggT-Bereiches in einer beliebigen algebraischen Körpererweiterung L/K ein Ring mit ggT-Theorie ist. Die hier vorgestellte allgemeine Aussage wurde m. E. bislang noch nicht bewiesen.

[57] *Krull 1936b*, S. 675, Satz 9, oder *Jaffard 1960*, S. 109f., Théorème 5. Für endlich erzeugte D-Ideale $\mathfrak{a}$ findet sich die Aussage bereits bei *Prüfer 1932*, S. 31, § 11.1. In der Sprache der Spurideale besagt dieses Lemma, daß die v-Spurideale von D bzgl. $\mathfrak{f}_v(T)$ mit den v-Idealen von D übereinstimmen.

Beweis von Satz 2.26: Wir beweisen die Aussage des Satzes für v-Bereiche. Es seien also D ein v-Bereich und $\mathfrak{a}$ irgendein ganzes endlich erzeugtes T-Ideal. Um $\mathfrak{a}$ als v_T-invertierbar nachzuweisen, betrachten wir ein Polynom $f \in T[X]$ mit $\mathrm{c}(f)_{v_T} = \mathfrak{a}_{v_T}$ sowie jenen Unterkörper K' von L, der aus K durch Adjunktion der Koeffizienten von f entsteht. Dann ist die Norm von f bzgl. der endlichen Körpererweiterung $K'(X)/K(X)$ — wir schreiben dafür $N_{K'/K}(f)$[58] — ein Polynom über D. Außerdem ist f ein Teiler von $N_{K'/K}(f)$ in $T[X]$, d. h. $f' := \frac{1}{f} N_{K'/K}(f) \in T[X]$. ff' ist also ein Polynom über dem v-Bereich D. Bezeichnet $\mathfrak{b}$ das von den Koeffizienten von ff' erzeugte D-Ideal, so gilt demnach $\mathfrak{b}_{v_D} \times \mathfrak{b}_{v_D}^{-1} = D$. Geht man über zur v_T-Idealoperation auf T, so erhält man mit Lemma 2.27 und wegen $\mathfrak{b}^{-1}T \subseteq (\mathfrak{b}T)^{-1}$ die Inklusionen

$$T = (\mathfrak{b}\mathfrak{b}^{-1})_{v_D} \cdot T \subseteq (\mathfrak{b}\mathfrak{b}^{-1})_{v_T} = (\mathfrak{b}T \cdot \mathfrak{b}^{-1}T)_{v_T} \subseteq (\mathfrak{b}T \cdot (\mathfrak{b}T)^{-1})_{v_T} = \mathfrak{b}_{v_T} \times \mathfrak{b}_{v_T}^{-1} \subseteq T.$$

Wegen $\mathfrak{b}_{v_T} = \mathrm{c}(ff')_{v_T}$ und aufgrund der Multiplikativität des v-Inhalts in ganzabgeschlossenen Integritätsbereichen folgt hieraus $T = \mathfrak{b}_{v_T} \times \mathfrak{b}_{v_T}^{-1} = \mathrm{c}(f)_{v_T} \times \big(\mathrm{c}(f')_{v_T} \times \mathfrak{b}_{v_T}^{-1}\big)$, womit $\mathfrak{a}_{v_T} = \mathrm{c}(f)_{v_T}$ als v_T-invertierbar nachgewiesen ist. T ist demnach ein v-Bereich.

Es werde nunmehr T als v-Bereich vorausgesetzt. Wir betrachten die D-Ideale $\mathfrak{a} \in \mathfrak{f}(D)$ und $\mathfrak{b}, \mathfrak{c} \in \mathfrak{F}(D)$ mit $\mathfrak{a}_{v_D} \times \mathfrak{b}_{v_D} = \mathfrak{a}_{v_D} \times \mathfrak{c}_{v_D}$. Aufgrund des Krullschen Lemmas 2.27 gilt $\mathfrak{d}_{v_T} \subseteq (\mathfrak{d}_{v_D}T)_{v_T} \subseteq (\mathfrak{d}_{v_T}T)_{v_T} = \mathfrak{d}_{v_T}$, also $(\mathfrak{d}_{v_D}T)_{v_T} = \mathfrak{d}_{v_T}$, für alle $\mathfrak{d} \in \mathfrak{F}(D)$, woraus im vorliegenden Fall $\mathfrak{a}_{v_T} \times \mathfrak{b}_{v_T} = \mathfrak{a}_{v_T} \times \mathfrak{c}_{v_T}$ folgt. Da $\mathfrak{a}_{v_T}$ v_T-invertierbar ist, ergibt sich $\mathfrak{b}_{v_T} = \mathfrak{c}_{v_T}$, also $\mathfrak{b}_{v_D} = \mathfrak{b}_{v_T} \cap D = \mathfrak{c}_{v_T} \cap D = \mathfrak{c}_{v_D}$. Damit sind die v_D-endlichen v_D-Ideale als v_D-kürzbar nachgewiesen. Der Beweis der Implikation (7) $\Rightarrow$ (1) von Satz 2.23 zeigt jedoch, daß dies bereits die v_D-Invertierbarkeit der v_D-endlichen v_D-Ideale zur Folge hat. D ist demnach ein v-Bereich. □

Aus Satz 2.26 folgt zusammen mit Satz 2.21, daß der Kroneckersche Funktionalring T^v von T vermöge $[\,\cdot\,] : T^* \to T^{v*}/T^{v\times}$ eine ggT-Theorie für den ganzen Abschluß T liefert. Es liegt die Vermutung nahe, daß T^v mit dem ganzen Abschluß $\overline{D^v}$ des Kroneckerschen Funktionalringes D^v von D in der algebraischen Körpererweiterung $L(X)/K(X)$ übereinstimmt. Dies ist tatsächlich der Fall.

Satz 2.28. *Es seien D ein Ring mit ggT-Theorie und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Dann ist der ganze Abschluß des Kroneckerschen Funktionalringes D^v von D in $L(X)/K(X)$ gleich dem Kroneckerschen Funktionalring T^v von T, also $\overline{D^v} = T^v$.*

Für den Beweis dieses Satzes zeigen wir zunächst

Lemma 2.29. *Es seien $\frac{f}{g} \in T^v$ mit $f, g \in T[X]$ und K' jener Körper, der aus K durch Adjunktion der Koeffizienten von f und g entsteht. Dann gilt $N_{K'/K}\big(\frac{f}{g}\big) \in D^v$.*

Beweis: Es sei $D' \subseteq T$ der ganze Abschluß von D in K'. Dann gilt wegen $\mathrm{c}(f)_{v_T} \subseteq \mathrm{c}(g)_{v_T}$ und aufgrund des Krullschen Lemmas 2.27 $\mathrm{c}(f)_{v_{D'}} = \mathrm{c}(f)_{v_T} \cap K' \subseteq \mathrm{c}(g)_{v_T} \cap K' = \mathrm{c}(g)_{v_{D'}}$. Geht man über zur normalen Hülle $\widetilde{K'}$ von K' über K, so erhält man hieraus, wiederum mit Hilfe von Lemma 2.27, $\mathrm{c}(f)_{v_{\widetilde{D'}}} = \big(\mathrm{c}(f)_{v_{D'}}\big)_{v_{\widetilde{D'}}} \subseteq \big(\mathrm{c}(g)_{v_{D'}}\big)_{v_{\widetilde{D'}}} = \mathrm{c}(g)_{v_{\widetilde{D'}}}$, also $\frac{f}{g} \in \widetilde{D'^v}$. Wir können daher o. E. d. A. annehmen, daß die Körpererweiterung K'/K normal ist. Bezeichnen s den Grad der Körpererweiterung K'/K, s' den Separabilitätsgrad und s'' den Inseparabilitätsgrad, so gibt es

[58] Korrekterweise müßte es $N_{K'(X)/K(X)}(f)$ heißen. Diese Schreibweise ist jedoch mitunter etwas schwerfällig. Daher wird im folgenden mit der Angabe der Körpererweiterung im Index des Normsymbols immer nur auf die *Koeffizienten* des entsprechenden Polynomausdruckes, *nicht* aber auf seine *Unbestimmten* Bezug genommen. Mißverständnisse können dabei nicht auftreten.

genau s' K-Konjugationsautomorphismen $\sigma_i : K' \to K'$, und es gilt

$$N_{K'/K}(f) = \prod_{i=1}^{s'} \sigma_i(f)^{s''} \quad \text{für alle } f \in K'[X].^{59} \tag{2.30}$$

Durchläuft α_j die Koeffizienten von f, so gilt, da der ganze Abschluß D' von D in K' unter Konjugation invariant ist, für jedes σ_i darüber hinaus

$$\mathrm{c}(f)_{v_{D'}} = \bigcap_{\substack{\mu\in K'\\ \alpha_j\in\mu D'}} \mu D' = \bigcap_{\substack{\mu\in K'\\ \sigma_i(\alpha_j)\in\sigma_i(\mu)D'}} \mu D' = \bigcap_{\substack{\mu\in K'\\ \sigma_i(\alpha_j)\subseteq\mu D'}} \sigma_i^{-1}(\mu)D' = \sigma_i^{-1}\Big(\mathrm{c}\big(\sigma_i(f)\big)_{v_{D'}}\Big).$$

Insgesamt folgt also $\sigma_i\big(\mathrm{c}(f)_{v_{D'}}\big) = \mathrm{c}\big(\sigma_i(f)\big)_{v_{D'}}$, und man erhält folgende Äquivalenzen:

$$\mathrm{c}(f)_{v_{D'}} \subseteq \mathrm{c}(g)_{v_{D'}} \quad \Leftrightarrow \quad \sigma_i\big(\mathrm{c}(f)_{v_{D'}}\big) \subseteq \sigma_i\big(\mathrm{c}(g)_{v_{D'}}\big) \quad \Leftrightarrow \quad \mathrm{c}\big(\sigma_i(f)\big)_{v_{D'}} \subseteq \mathrm{c}\big(\sigma_i(g)\big)_{v_{D'}}.$$

Bedenkt man, daß D' ganzabgeschlossen und der $v_{D'}$-Inhalt demnach multiplikativ ist, so ergibt sich hieraus zusammen mit (2.30)

$$\mathrm{c}\big(N_{K'/K}(f)\big)_{v_{D'}} = \Big(\prod_{i=1}^{s'} \mathrm{c}\big(\sigma_i(f)\big)_{v_{D'}}^{s''}\Big)_{v_{D'}} \subseteq \Big(\prod_{i=1}^{s'} \mathrm{c}\big(\sigma_i(g)\big)_{v_{D'}}^{s''}\Big)_{v_{D'}} = \mathrm{c}\big(N_{K'/K}(g)\big)_{v_{D'}}.$$

Mit dem Krullschen Lemma 2.27 folgt schließlich $\mathrm{c}\big(N_{K'/K}(f)\big)_{v_D} \subseteq \mathrm{c}\big(N_{K'/K}(g)\big)_{v_D}$, was die Behauptung $N_{K'/K}\big(\frac{f}{g}\big) \in D^v$ impliziert. □

In Analogie zu Satz 2.17 beweisen wir

Satz 2.31. *Für den ganzen Abschluß $\overline{D^v}$ des Kroneckerschen Funktionalringes D^v in der algebraischen Körpererweiterung $L(X)/K(X)$ gilt:*

(1) $\overline{D^v} \cap L = T$.

(2) *Das von $\frac{f_1}{g}, \ldots, \frac{f_m}{g} \in L(X)$, $f_k, g \in T[X]$, erzeugte $\overline{D^v}$-Ideal ist gleich dem Hauptideal $\frac{f}{g}\overline{D^v}$ mit $f(X) = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$ und geeignet gewählten Exponenten r_i, beispielsweise mit $r_1 = 0$ und $r_{i+1} = i \cdot \big(1 + \max\limits_{1\leqslant j\leqslant m}\{\mathrm{grad} f_j\}\big)$ für $i = 1, \ldots, m-1$.*

(3) *$\overline{D^v}$ ist ein Bezout-Bereich.*

Beweis: Die Bezout-Eigenschaft von $\overline{D^v}$ ergibt sich unmittelbar aus Aussage (2). Bleiben also (1) und (2) zu zeigen.

Ad (1) Die Inklusion „$\supseteq$“ ist trivial. Sei also $\frac{f}{g} \in \overline{D^v} \cap L$ mit $f, g \in T[X]$. Wegen $\frac{f}{g} \in L$ existieren $a, b \in T$ mit $\frac{f}{g} = \frac{a}{b}$. Bezeichnet K' jenen Körper, der aus K durch Adjunktion der Koeffizienten von K entsteht, so gilt für das charakteristische Polynom der über D^v ganzen algebraischen Funktion $\frac{f}{g}$ bzgl. der Körpererweiterung K'/K

$$\chi_{f/g}(Y) = N_{K'/K}\Big(Y - \frac{f}{g}\Big) = N_{K'/K}\Big(Y - \frac{a}{b}\Big) \in D^v[Y] \cap K[Y].$$

Die Koeffizienten von $\chi_{f/g}$ liegen demnach in $D^v \cap K$, also nach Satz 2.17.(2), S. 23, in D. Es folgt, daß $\frac{f}{g} = \frac{a}{b}$ ganz über D und somit in T enthalten ist.

Ad (2) Das Hauptideal $\frac{f}{g}\overline{D^v}$ mit $f(X) = f_1 \cdot X^{r_1} + \ldots + f_m \cdot X^{r_m}$, $r_i \in \mathbb{N}$, ist in dem von $\frac{f_1}{g}, \ldots, \frac{f_m}{g}$ erzeugten $\overline{D^v}$-Ideal enthalten. Bleibt die umgekehrte Inklusion zu zeigen. Dazu seien K' jener Körper, der aus K durch Adjunktion der Koeffizienten von $f_1, \ldots, f_m$ entsteht, und χ_k das charakteristische Polynom von $\frac{f_k}{f}$ bzgl. der Körpererweiterung $K'(X)/K(X)$. Dann gilt für $k = 1, \ldots, m$

$$\frac{f_k}{g} \in \frac{f}{g}\overline{D^v} \quad \Leftrightarrow \quad \frac{f_k}{f} \in \overline{D^v} \quad \Leftrightarrow \quad \frac{f_k}{f} \text{ ganz über } D^v \quad \Leftrightarrow \quad \chi_k(Y) = N_{K'/K}\Big(Y - \frac{f_k}{f}\Big) \in D^v[Y].$$

[58] Vgl. *Zariski et al. 1958*, S. 77, Theorem 16, S. 91, Formel (19), sowie S. 115, Corollary 1.

Wählt man in dem Polynom f die Exponenten r_i so, wie im Satz angegeben, dann gilt $\mathrm{c}(f_k)_{v_T} \subseteq \mathrm{c}(f)_{v_T}$, woraus $\mathrm{c}(f \cdot X^r - f_k)_{v_T} \subseteq \mathrm{c}(f)_{v_T}$ für alle $r \geqslant 1 + \max_{1 \leqslant j \leqslant m}\{\mathrm{grad} f_j\}$ folgt. Mit Lemma 2.29 erhält man hieraus

$$N_{K'/K}\Big(\frac{f \cdot X^r - f_k}{f}\Big) \in D^v, \quad \text{also} \quad \big(N_{K'/K}(f \cdot X^r - f_k)\big)_{v_D} \subseteq \big(N_{K'/K}(f)\big)_{v_D}$$

für alle $r \geqslant 1 + \max_{1 \leqslant j \leqslant m}\{\mathrm{grad} f_j\}$. Wählt man die Potenz X^r hinreichend groß, so haben die Polynome $N_{K'/K}(f \cdot Y - f_k)$ und $N_{K'/K}(f \cdot X^r - f_k)$ über D dieselben Koeffizienten. Damit ist aber insbesondere der v_D-Inhalt jedes Koeffizienten von $N_{K'/K}(f \cdot Y - f_k)$, aufgefaßt als Polynom über $D[X]$, in $\mathrm{c}(N_{K'/K}(f \cdot X^r - f_k))_{v_D}$, also in $\mathrm{c}(N_{K'/K}(f))_{v_D}$ enthalten. Insgesamt ist daher jeder Koeffizient von $N_{K'/K}(f \cdot Y - f_k)$ bzgl. D^v durch $N_{K'/K}(f)$ teilbar, und man erhält $N_{K'/K}\big(Y - \frac{f_k}{f}\big) \in D^v[Y]$, was zu beweisen war. □

Beweis von Satz 2.28: „$\subseteq$“ Aus $\frac{f}{g} \in \overline{D^v}$ mit $f, g \in T[X]$ folgt $f\overline{D^v} \subseteq g\overline{D^v}$. Nach Satz 2.31.(2) stimmt das Hauptideal $f\overline{D^v}$ mit jenem $\overline{D^v}$-Ideal überein, das von den Koeffizienten von f erzeugt wird. Wegen $\overline{D^v} \cap L = T$ ist das Verengungsideal $f\overline{D^v} \cap L$ demzufolge ein T-Ideal, das einerseits die Koeffizienten von f enthält, andererseits (als d-Spurideal bzgl. $\mathfrak{f}_d(\overline{D^v})$) in dem v-Ideal $\mathrm{c}(f)_{v_T}$ enthalten ist. Insgesamt folgt also

$$\mathrm{c}(f)_{v_T} = (f\overline{D^v} \cap T)_{v_T} \subseteq (g\overline{D^v} \cap T)_{v_T} = \mathrm{c}(g)_{v_T},$$

was wiederum äquivalent zu $\frac{f}{g} \in T^v$ ist.

„$\supseteq$“ Es sei $\frac{f}{g} \in T^v$ mit $f, g \in T[X]$, d. h. es gelte $\mathrm{c}(f)_{v_T} \subseteq \mathrm{c}(g)_{v_T}$. Mit Satz 2.31.(2) erhält man hieraus $f\overline{D^v} \subseteq \mathrm{c}(f)_{v_T}\overline{D^v} \subseteq \mathrm{c}(g)_{v_T}\overline{D^v}$, also $\frac{f}{g}\overline{D^v} \subseteq \frac{1}{g}\mathrm{c}(g)_{v_T}\overline{D^v}$. Tatsächlich ist $\frac{1}{g}\mathrm{c}(g)_{v_T}\overline{D^v}$ ein ganzes $\overline{D^v}$-Ideal. Dazu weisen wir nach, daß die algebraische Funktion $\frac{\beta}{g} \in L(X)$ für alle $\beta \in \mathrm{c}(g)_{v_T}$ ganz über D^v ist. Es sei $\chi_\beta := N_{K'/K}\big(Y - \frac{\beta}{g}\big)$ das charakteristische Polynom von $\frac{\beta}{g}$ bzgl. der Körpererweiterung K'/K, wobei K', wie üblich, jenen Körper bezeichne, der aus K durch Adjunktion des Elements β sowie der Koeffizienten von g entsteht. Nach Voraussetzung gilt $\mathrm{c}(g \cdot X^r - \beta)_{v_T} \subseteq \mathrm{c}(g)_{v_T}$, also $X^r - \frac{\beta}{g} \in T^v$ für alle $r \geqslant 1$. Mit der gleichen Argumentation wie im Beweis von Satz 2.31.(2) ergibt sich hieraus, daß jeder Koeffizient von $N_{K'/K}(g \cdot Y - \beta)$, aufgefaßt als Polynom über $D[X]$, bzgl. D^v durch $N_{K'/K}(g)$ teilbar ist, d. h. $N_{K'/K}\big(Y - \frac{\beta}{g}\big) \in D^v[Y]$. Demnach gilt $\frac{\beta}{g} \in \overline{D^v}$ für alle $\beta \in \mathrm{c}(g)_{v_T}$, woraus insgesamt $\frac{f}{g}\overline{D^v} \subseteq \frac{1}{g}\mathrm{c}(g)_{v_T}\overline{D^v} \subseteq \overline{D^v}$, also $\frac{f}{g} \in \overline{D^v}$ folgt. □

Kapitel 3

Ringe mit ggT-Theorie endlichen Typs

Ist D ein Ring mit Divisorentheorie, so kann aus der Faktorialität der Divisorenhalbgruppe gefolgert werden, daß jeder Divisor größter gemeinsamer Teiler von endlich vielen, genau genommen sogar nur zwei Hauptdivisoren ist. In diesem Abschnitt werden wir u. a. zeigen, daß eine entsprechende Aussage für Ringe mit ggT-Theorie i. a. *nicht* gilt, sondern eine echte Verschärfung darstellt. Durch eine entsprechende Modifikation unserer Definition für Ringe mit ggT-Theorie werden wir auf den Begriff der *ggT-Theorie endlichen Typs* geführt. Die arithmetische Situation wird dadurch insgesamt einfacher und übersichtlicher. Insbesondere wird sich zeigen, daß ein Ring mit ggT-Theorie endlichen Typs bis auf Isomorphie nur eine einzige ggT-Theorie besitzt. Darüber hinaus werden wir in diesem Zusammenhang auch auf den Spezialfall der Ringe mit Divisorentheorie näher eingehen.

3.1. Das Axiom (G 2) und der Begriff des Ringes mit ggT-Theorie e. T.

Skula hat für das Axiom (G 2), das dem dritten Borewicz-Šafarevičschen Axiom für Ringe mit Divisorentheorie entspricht, mehrere äquivalente Fassungen bewiesen.[60] Wir wollen seine verschiedenen Versionen des Axioms (G 2) unter der Voraussetzung untersuchen, daß die Divisorenhalbgruppe nicht mehr faktoriell, sondern ein ggT-Monoid ist.

Satz 3.1. *Es seien D ein Integritätsbereich und $(\cdot)$ ein Halbgruppenhomomorphimus von D^* in einen ggT-Monoiden $\mathfrak{G}^+$, der das Axiom (G 1) für Ringe mit ggT-Theorie erfüllt. Es gelte außerdem eine der folgenden vier Bedingungen:*

(G 2.1) $\mathfrak{a} = \mathrm{ggT}(\{\alpha\}_{\mathfrak{a}\mid(\alpha)})$ *für alle* $\mathfrak{a} \in \mathfrak{G}^+$.

(G 2.2) *Zu jedem Divisor* $\mathfrak{a} \in \mathfrak{G}^+$ *existieren* $\alpha_1, \ldots, \alpha_m \in D^*$ *mit* $\mathfrak{a} = \mathrm{ggT}(\alpha_1, \ldots, \alpha_m)$.

(G 2.3) *Zu jedem Divisor* $\mathfrak{a} \in \mathfrak{G}^+$ *existieren* $\alpha, \beta \in D^*$ *mit* $\mathfrak{a} = \mathrm{ggT}(\alpha, \beta)$.

(G 2.4) *Zu je zwei Divisoren* $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}^+$ *existiert ein* $\mathfrak{c} \in \mathfrak{G}^+$ *mit* $\mathrm{ggT}(\mathfrak{b}, \mathfrak{c}) = (1)$, *so daß* $\mathfrak{ac}$ *ein ganzer Hauptdivisor ist.*

Dann ist jede Bedingung hinreichend für die Gültigkeit der vorangehenden. Insbesondere ist D in jedem Fall ein Ring mit ggT-Theorie. Ist $\mathfrak{G}^+$ ein faktorieller Monoid, so sind alle vier Bedingungen äquivalente Fassungen des Axioms (G 2), und die ggT-Theorie $(\cdot) : D^* \to \mathfrak{G}^+$ liefert eine Divisorentheorie für D.

Beweis: Wir zeigen zunächst die Implikationen (G 2.4) ⇒ (G 2.3) ⇒ (G 2.2) ⇒ (G 2.1) unter der Annahme, daß $\mathfrak{G}^+$ ein ggT-Monoid ist. Die Implikation (G 2.3) ⇒ (G 2.2) ist trivial. Bleiben also (G 2.4) ⇒ (G 2.3) und (G 2.2) ⇒ (G 2.1) zu zeigen.

(G 2.4) ⇒ (G 2.3) Es sei $\mathfrak{a} \in \mathfrak{G}^+$. Nach Voraussetzung existiert ein $\mathfrak{b} \in \mathfrak{G}^+$ mit $\mathfrak{ab} = (\alpha)$, $\alpha \in D^*$. Zu $\mathfrak{b}$ wiederum existiert ein $\mathfrak{c} \in \mathfrak{G}^+$ mit $\mathrm{ggT}(\mathfrak{b}, \mathfrak{c}) = (1)$ und $\mathfrak{ac} = (\beta)$, $\beta \in D^*$. Es folgt $\mathfrak{a} = \mathfrak{a} \cdot \mathrm{ggT}(\mathfrak{b}, \mathfrak{c}) = \mathrm{ggT}(\alpha, \beta)$.

(G 2.2) ⇒ (G 2.1) Es seien $\mathfrak{a} = \mathrm{ggT}(\alpha_1, \ldots, \alpha_m)$ und $\mathfrak{b} = \mathrm{ggT}(\beta_1, \ldots, \beta_n)$ ganze Divisoren mit $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. Dann folgt wegen $\alpha_i \in \overline{\mathfrak{b}}$ und $\beta_i \in \overline{\mathfrak{a}}$ sofort $\mathfrak{a} \mid (\beta_i)$, also $\mathfrak{a} \mid \mathrm{ggT}(\beta_1, \ldots, \beta_n)$, und entsprechend $\mathfrak{b} \mid \mathrm{ggT}(\alpha_1, \ldots, \alpha_m)$. Daher sind $\mathfrak{a}$ und $\mathfrak{b}$ assoziiert in $\mathfrak{G}^+$. Da Assoziiertheits- und Gleichheitsrelation in ggT-Monoiden übereinstimmen, folgt $\mathfrak{a} = \mathfrak{b}$, womit die Gültigkeit von Axiom (G 2), also auch die nach Lemma 2.5, S. 17, hierzu äquivalente Bedingung (G 2.1) nachgewiesen ist.

Aufgrund der eben gezeigten Implikationen ist D in jedem Fall ein Ring mit ggT-Theorie. Unter der Annahme, daß die Divisorenhalbgruppe $\mathfrak{G}^+$ faktoriell ist, folgt auch die Implikation (G 2.1) ⇒ (G 2.4) und damit die Äquivalenz aller vier Bedingungen für Ringe mit Divisorentheorie. Dazu seien $\mathfrak{a}, \mathfrak{b} \in \mathfrak{G}^+$ mit $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_n^{r_n}$, $r_i \in \mathbb{N}$. Seien ferner $\mathfrak{q} := \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ und $\mathfrak{q}_i := \mathfrak{q}\mathfrak{p}_i^{-1}$. Dann ist der Divisor $\mathfrak{aq}_i$ für jedes $i = 1, \ldots, n$ ein echter Teiler von $\mathfrak{aq}$, woraus wegen Axiom (G 2) sofort $\overline{\mathfrak{aq}} \subsetneqq \overline{\mathfrak{aq}_i}$ folgt. Es existiert also zu jedem $i = 1, \ldots, n$ ein $\alpha_i \in D^*$ mit $\mathfrak{aq}_i \mid \alpha_i$ und $\mathfrak{aq} \nmid \alpha_i$. Setze $\alpha := \alpha_1 + \ldots + \alpha_n$. Dann gilt $\mathfrak{a} \mid \alpha$, aber $\mathfrak{ap}_i \nmid \alpha$. Andernfalls würde aus $\mathfrak{ap}_i \mid \alpha_j$ für alle $i \neq j$ $\mathfrak{ap}_i \mid (\alpha_i)$, also $\mathfrak{aq}_i\mathfrak{p}_i = \mathfrak{aq} \mid \alpha_i$ folgen, was nicht sein kann. Mit $\mathfrak{c} := \alpha\mathfrak{a}^{-1} \in \mathfrak{G}^+$ ergibt sich nun die Behauptung, denn wegen $\mathfrak{p}_i \nmid \mathfrak{c}$ ist $\mathrm{ggT}(\mathfrak{b}, \mathfrak{c}) = 1$ und $\mathfrak{ac} = (\alpha)$. □

Definition 3.2. *Ist D ein Ring mit ggT-Theorie, in dem statt des Axioms (G 2) das Axiom (G 2.2) erfüllt ist, so heißt D* ***Ring mit ggT-Theorie endlichen Typs*** *(e. T.).*[61]

[60] Vgl. *Skula 1970*, S. 114, 2.1, und S. 119, 4.7.

[61] Für den allgemeineren Fall, daß statt Ringen und deren Quotientenkörpern Monoide und deren Quotientengruppen betrachtet werden, findet sich in der Literatur auch der Begriff der *Quasi-Divisorentheorie* („*theory of quasi-divisors*"), der auf *Aubert 1983*, S. 339, zurückgeht (vgl. auch Anmerkung 21). Aubert nimmt allerdings an, daß die Axiome (G 2) und (G 2.2) für verbandsgeordnete Divisorengruppen $\mathfrak{G}$ gleichbedeutend seien. Wie wir weiter unten sehen werden, ist diese Annahme i. a. jedoch falsch. Demselben Irrtum erliegt auch Močkoř, der sich auf Aubert beruft

Für Ringe mit ggT-Theorie e. T. gilt in Analogie zu Korollar 2.24

Korollar 3.3. *Für einen Integritätsbereich D sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit ggT-Theorie e. T.*
(2) *Die Menge $\mathfrak{f}_v(D)$ der gebrochenen v-endlichen v-Ideale von D ist eine Gruppe bzgl. der v-Multiplikation.*

Ist eine der äquivalenten Bedingungen erfüllt, so ist die Halbgruppe $\mathfrak{f}_v^+(D)$ der ganzen v-endlichen v-Ideale ein ggT-Monoid, und der Homomorphismus $(\cdot)_v : D^* \to \mathfrak{f}_v^+(D)$ mit $\alpha \mapsto (\alpha)_v = \alpha D$ liefert eine ggT-Theorie endlichen Typs, die mit der Prüferschen ggT-Theorie übereinstimmt.

Beweis: (1) $\Rightarrow$ (2) Jeder Ring mit ggT-Theorie e. T. ist ein Ring mit ggT-Theorie und somit ein v-Bereich. Bleibt zu zeigen, daß das v-Inverse eines v-endlichen v-Ideals wieder v-endlich ist. Dazu sei $\mathfrak{a}_v = (\alpha_1, \ldots, \alpha_m)_v$ irgendein v-endliches v-Ideal. Mit Korollar 2.9 gilt dann $\mathfrak{a}_v^{-1} = \operatorname{ggT}(\alpha_1, \ldots, \alpha_m)^{-1}$. Nach Voraussetzung ist der echt gebrochene Divisor $\operatorname{ggT}(\alpha_1, \ldots, \alpha_m)^{-1}$ größter gemeinsamer Teiler von endlich vielen gebrochenen Hauptdivisoren, d. h. es existieren $\beta_1, \ldots, \beta_n \in K^*$ mit $\operatorname{ggT}(\alpha_1, \ldots, \alpha_m)^{-1} = \operatorname{ggT}(\beta_1, \ldots, \beta_n)$. Daraus folgt $\mathfrak{a}_v^{-1} = (\beta_1, \ldots, \beta_n)_v$, womit $\mathfrak{a}_v^{-1}$ als v-endlich nachgewiesen ist.

(2) $\Rightarrow$ (1) Setzen wir $\mathfrak{f}_v(D)$ als Gruppe voraus, ist also insbesondere das v-Inverse eines v-endlichen v-Ideals wieder v-endlich, so gilt

$$\mathfrak{f}_v^+(D) = \{\mathfrak{a}_v \text{ ganz} : \mathfrak{a} \in \mathfrak{f}(D)\} = \{\mathfrak{a}_v \times \mathfrak{b}_v^{-1} \text{ ganz} : \mathfrak{a}, \mathfrak{b} \in \mathfrak{f}(D) \text{ ganz}\} = \mathfrak{g}_v^+(D).$$

Aufgrund von Korollar 2.24, S. 27, ist daher D ein Ring mit ggT-Theorie, dessen Prüfersche ggT-Theorie durch $(\cdot)_v : D^* \to \mathfrak{f}_v^+(D)$ gegeben ist. Daß diese ggT-Theorie eine ggT-Theorie endlichen Typs liefert, folgt aus der Tatsache, daß jedes v-Ideal $\mathfrak{a}_v \in \mathfrak{f}_v^+(D)$ die Gestalt $\mathfrak{a}_v = (\alpha_1, \ldots, \alpha_m)_v$ mit $\alpha_i \in D^*$ hat. □

Integritätsbereiche, in denen die v-endlichen v-Ideale bzgl. der v-Multiplikation eine Gruppe bilden, heißen nach Krull auch *Prüfer-v-Multiplikationsbereiche*.[62] Wir haben somit bewiesen:

Satz 3.4. *Ein Integritätsbereich D ist ein Ring mit ggT-Theorie e. T. genau dann, wenn D ein Prüfer-v-Multiplikationsbereich ist.*[63]

Im Hinblick auf die Frage nach der Eindeutigkeit einer ggT-Theorie endlichen Typs ergibt sich

(vgl. *Močkoř 1983*, S. 126, Theorem 10.7). Inzwischen scheint stillschweigend Übereinkommen darüber zu bestehen, daß Ringe (bzw. Gruppen) mit *Quasi-Divisorentheorie* allein durch die Gültigkeit von Axiom (G 2.2) (bzw. einem entsprechendem Axiom) charakterisiert sind (vgl. *Geroldinger et al. 1995* und *Močkoř et al. 1993a*).

[62] In der englischsprachigen Literatur ist die Abkürzung *PVMD* für „*Prüfer-v-multiplication domain*“ verbreitet. Nach Bourbaki wird bisweilen auch von *Pseudo-Prüferbereichen* („*anneaux pseudo-prüférien*“) gesprochen.

[63] Dieser Satz wurde erstmals von Jaffard im Jahre 1960 bewiesen (siehe *Jaffard 1960*, S. 55, Corollaire zu Théorème 3), und zwar, entsprechend dem Anliegen Jaffards, in der Sprache einer rein multiplikativ begründeten Idealtheorie (vgl. Anmerkung 21, S. 9). *Griffin 1967*, S. 717, formulierte die Aussage erstmals für Integritätsbereiche. Der Jaffardsche Beweis für die Aussage, daß jeder Ring D mit ggT-Theorie e. T. ein Prüfer v-Multiplikationsbereich ist (bei Jaffard: die Eigenschaft „$v - \beta$ finie“ hat), beruht auf der Tatsache, daß die endlich erzeugten Ideale des zugehörigen Kroneckerschen Funktionalringes D^v eine Gruppe bzgl. der gewöhnlichen Idealmultiplikation (bei Jaffard: „v-groupe de Lorenzen“) bilden, sowie dem Nachweis, daß das Spursystem dieses Idealsystems, also das d_p-System der d_p-endlichen Ideale von D, ebenfalls wieder eine Gruppe ist. Es folgt dann (vgl. Korollar 1.11, S. 11), daß die t-endlichen t-Ideale bzgl. der t-Multiplikation oder, was dasselbe ist, daß die v-endlichen v-Ideale bzgl. der v-Multiplikation eine Gruppe bilden. Zu der gleichen Aussage wie Jaffard kommt auch Aubert in seiner Arbeit „Divisors of finite character“ aus dem Jahre 1983 (siehe *Aubert 1983*, S. 339, Theorem 4). Aubert bedient sich ebenfalls der Theorie der Spurideale, so daß sein Beweis methodisch wie inhaltlich im Grunde nichts Neues bietet. Es ist insofern nicht ganz einsichtig, warum Aubert als Quelle für den Satz nicht Jaffard, sondern die Dissertation des Norwegers K. Gudlaugsson zitiert, bei dem es sich vermutlich um einen Schüler Auberts handelt.

Satz 3.5. *Jeder Ring mit ggT-Theorie e. T. besitzt bis auf Isomorphie nur eine einzige ggT-Theorie.*[64]

Beweis: Ist $\mathfrak{G}^+$ die Divisorenhalbgruppe irgendeiner ggT-Theorie e. T. für D, so liefert die Abbildung $\mathfrak{G}^+ \to \mathfrak{g}_v^+(D)$, $\mathfrak{a} \mapsto \overline{\mathfrak{a}}$, einen Isomorphismus, bei dem die Hauptdivisoren (α) genau auf die Hauptideale $(\alpha)_v = \alpha D$ abgebildet werden. Injektivität und Homorphie der Abbildung sind klar, die Surjektivität ergibt sich aus der Tatsache, daß der ggT-Monoid $\mathfrak{g}_v^+(D)$ mit der Halbgruppe $\mathfrak{f}_v^+(D)$ der ganzen v-endlichen v-Ideale von D übereinstimmt. Jede ggT-Theorie e. T. für D ist daher zur Prüferschen ggT-Theorie isomorph. □

Es gibt Beispiele von v-Bereichen, in denen die v-endlichen v-Ideale bzgl. der v-Multiplikation *keine* Gruppe bilden.[65] Im Gegensatz zur Situation der Ringe mit Divisorentheorie stellt somit der Übergang von Axiom (G 2) bzw. (G 2.1) zu Axiom (G 2.2) eine echte Verschärfung dar. In der Literatur schien man bislang dagegen von der Äquivalenz dieser Axiome auszugehen.[66]

Ringe mit ggT-Theorie e. T., die dem Axiom (G 2.3) genügen, sind offenbar genau jene Prüfer-v-Multiplikationsbereiche, in denen jedes v-endliche v-Ideal höchstens zwei v-Erzeuger hat. Es kann gezeigt werden, daß es Prüferbereiche und damit Prüfer-v-Multiplikationsbereiche gibt, in denen jedes Ideal genau $m \geqslant 1$ Erzeuger hat.[67] Also stellt auch der Übergang von Axiom (G 2.2) zu Axiom (G 2.3) eine echte Verschärfung dar.

Axiom (G 2.4) schließlich übersetzt sich idealtheoretisch dahingehend, daß es in einem Prüfer-v-Multiplikationsbereich zu je zwei ganzen v-endlichen v-Idealen $\mathfrak{a}_v$ und $\mathfrak{b}_v$ stets eine weiteres v-endliches v-Ideal $\mathfrak{c}_v$ mit $(\mathfrak{b}_v, \mathfrak{c}_v)_v = D$ gibt, so daß $\mathfrak{a}_v \times \mathfrak{c}_v$ ein Hauptideal ist.[68] Mir ist kein Beispiel eines Prüfer-v-Multiplikationsbereiches geläufig, in denen jedes v-endliche v-Ideal höchstens zwei v-Erzeuger hat, in denen aber die oben genannte Bedingung nicht erfüllt ist.

3.2. Idealtheoretische Charakterisierung von Ringen mit ggT-Theorie e. T.

Aus der v-Gruppeneigenschaft der v-endlichen v-Ideale von D erhält man ohne Schwierigkeiten weitere idealtheoretische Charakterisierungen für Ringe mit ggT-Theorie e. T.

Satz 3.6. *Für einen Integritätsbereich D mit Quotientenkörper K sind folgende Aussagen äquivalent:*

(1) *D ist ein Ring mit ggT-Theorie e. T./Prüfer-v-Multiplikationsbereich.*
(2) *Die Menge $\mathfrak{f}_t(D)$ der t-endlichen t-Ideale bildet eine Gruppe bzgl. der t-Multiplikation.*
(3) *Zu jedem $f \in K[X]$ existiert ein $g \in K[X]$ mit $\mathrm{c}(f)_v \times \mathrm{c}(g)_v = D$.*[69]
(4) *D ist ganzabgeschlossen, und zu jedem $f \in K[X]$ gibt es ein $g \in K[X]$ mit $\mathrm{c}(fg)_v = D$.*
(5) *D ist ganzabgeschlossen, und zu allen $f, g \in D[X]$ mit $\mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v$ existiert ein $h \in K[X]$ mit $\mathrm{c}(fh)_v \subseteq \mathrm{c}(gh)_v = D$.*[70]

[64] Aus diesem Satz folgt unmittelbar, daß die entsprechende Eindeutigkeitsaussage für Ringe mit Divisorentheorie nicht auf der eindeutigen Primdivisorzerlegung, sondern im wesentlichen auf der Existenz eines größten gemeinsamen Teilers beruht. Vgl. hierzu auch *Borewicz et al. 1966*, S. 190.

[65] *Mott et al. 1981* geben das Beispiel eines sogenannten „*P-domain*“ D, dessen v-endliche v-Ideale keine Gruppe bilden (S. 5ff., Example 2.1). Es wird bewiesen, daß D ein *wesentlicher Integritätsbereich* (S. 3f., Proposition 1.1) und als solcher ein v-Bereich ist (vgl. hierzu *Gilmer 1992*, S. 553, Theorem 44.13, und S. 396, Theorem 32.5). Siehe auch *Bourbaki 1989*, S. 561, VII, § 2, Exercise 19.(b), oder *Gilmer 1992*, S. 429, Exercises 3–5.

[66] Vgl. Anmerkung 61.

[67] Vgl. *Swan 1984*.

[68] In dem Fall, daß Axiom (G 2.2) durch Axiom (G 2.4) ersetzt wird, sprechen *Močkoř et al. 1993a* auch von einer „*strong theory of quasi-divisors*“.

[69] *Zafrullah 1984*, S. 232, Lemma 1.

[70] *Zafrullah 1984*, S. 232, Proposition 3.

Beweis: Da das System der v-endlichen v-Ideale mit dem System der t-endlichen t-Ideale übereinstimmt, ist die Äquivalenz (1) $\Leftrightarrow$ (2) offensichtlich, ebenso (1) $\Leftrightarrow$ (3). Die Äquivalenz (1) $\Leftrightarrow$ (4) folgt aus Satz 2.11, S. 20, zusammen mit Satz 2.13, S. 20; das gleiche gilt für (4) $\Leftrightarrow$ (5). $\square$

Bereits bei oberflächlicher Durchsicht der einschlägigen Literatur stößt man auf zahlreiche weitere Charakterisierungen von Prüfer-v-Multiplikationsbereichen. Die genaue Zahl ist schwer zu schätzen. Eigene Recherchen ergaben allein weit über 60 notwendige und hinreichende Kriterien, wobei äquivalente Charakterisierungen für die Ganzabgeschlossenheit oder die v-Bereichseigenschaft noch nicht einmal mitgezählt sind.

Bevor wir im nächsten Abschnitt zeigen, wie sich Ringe mit ggT-Theorie e. T. bzw. Prüfer-v-Multiplikationsbereiche anhand ihres zugehörigen Kroneckerschen Funktionalringes charakterisieren lassen, wollen wir noch einen Blick auf die Idealstruktur von Ringen mit Divisorentheorie werfen. Dazu sei D ein Ring mit Divisorentheorie $(\cdot) : D^* \to \mathfrak{G}^+$. Aufgrund von Satz 3.1 ist diese Divisorentheorie nicht nur eine ggT-Theorie, sondern eine ggT-Theorie e. T. Damit ist D insbesondere ein Prüfer-v-Multiplikationsbereich , und die t-endlichen t-Ideale von D bilden bzgl. der t-Multiplikation eine Gruppe. Es stellt sich die Frage, welche idealtheroetischen Auswirkungen die Faktorialität der Divisorenhalbgruppe $\mathfrak{G}^+$ darüber hinaus nach sich zieht.

Wir wissen: In einem Ring mit Divisorentheorie ist jedes t-endliche t-Ideal t-invertierbar. Wie sieht es jedoch mit jenen t-Idealen aus, die *nicht* t-endlich sind? Dazu betrachte man ein ganzes D-Ideal $\mathfrak{a}$. Wir nehmen an, das zugehörige t-Ideal $\mathfrak{a}_t$ sei nicht t-endlich. Dann gibt es eine unendliche Familie $\{\alpha_i\}_{i\in\mathbb{N}}$ paarweise verschiedener Elemente aus $\mathfrak{a}$ mit

$$(\alpha_1)_t \subsetneqq (\alpha_1, \alpha_2)_t \subsetneqq (\alpha_1, \alpha_2, \alpha_3)_t \subsetneqq \dots$$

Aufgrund von Korollar 2.8, S. 19, und Lemma 2.5.(1), S. 17, entspricht dieser echt aufsteigenden unendlichen Kette von t-endlichen t-Idealen umkehrbar eindeutig die echt absteigende unendliche Teilerkette von Divisoren

$$\dots, \quad \mathrm{ggT}(\alpha_1, \alpha_2, \alpha_3) \mid \mathrm{ggT}(\alpha_1, \alpha_2), \quad \mathrm{ggT}(\alpha_1, \alpha_2) \mid (\alpha_1).$$

Dies steht jedoch im Widerspruch dazu, daß der Hauptdivisor (α_1) nur endlich viele echte Teiler in der faktoriellen Divisorengruppe $\mathfrak{G}$ besitzt. Also muß die obige Kette von t-Idealen nach endlich vielen Schritten abbrechen und das t-Ideal $\mathfrak{a}_t$ t-endlich sein. Unter Berücksichtigung von Lemma 1.17, S. 13, haben wir somit bewiesen: Ein Ring mit Divisorentheorie ist ein v-noetherscher Prüfer-v-Multiplikationsbereich. Oder einfacher ausgedrückt: Ein Ring mit Divisorentheorie ist ein Integritätsbereich, in dem die t-Ideale bzgl. der t-Multiplikation eine Gruppe bilden.

Auch die Umkehrung ist richtig, denn die Gruppe der t-Ideale ist nach Satz 1.18, S. 14, stets faktoriell, womit die Prüfersche ggT-Theorie in diesem Fall zu einer Divisorentheorie für D wird. Als Hauptergebnis halten wir fest:

Satz 3.7. *Ein Integritätsbereich D ist genau dann ein Ring mit Divisorentheorie, wenn die Menge $\mathsf{F}_t(D)$ der gebrochenen t-Ideale von D bzgl. der t-Multiplikation eine Gruppe bildet.*[71]

In dieser Charakterisierung tritt der Unterschied zwischen Ringen mit ggT-Theorie und Ringen mit Divisorentheorie besonders deutlich hervor. Ringe mit einer ggT-Theorie, die nicht zugleich auch eine Divisorentheorie ist, müssen t-Ideale enthalten, die *nicht* t-endlich sind, d. h.: Ringe mit einer „echten“ ggT-Theorie sind im Gegensatz zu Ringen mit einer Divisorentheorie *nicht* v-noethersch. Oder anders ausgedrückt: In Ringen mit einer „echten“ ggT-Theorie muß es Elemente geben, die durch beliebig viele Divisoren teilbar sind.

Wir notieren noch einige idealtheoretische Charakterisierungen für einen Ring mit Divisorentheorie. Die meisten davon ergeben sich ohne Schwierigkeiten aus dem bisher Gesagten.

[71] Vgl. *Jaffard 1960*, S. 82, Théorème 5, oder *Anderson et al. 1989b*, S. 463, Theorem 3.9.(5).

Satz 3.8. *Für einen Integritätsbereich D sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit Divisorentheorie.*
(2) *Die Menge $\mathsf{F}_t(D)$ der gebrochenen t-Ideale D bildet eine Gruppe bzgl. der t-Multiplikation.*
(3) *Jedes ganze t-Ideal von D ist das t-Produkt von endlich vielen t-primen t-Idealen.*[72]
(4) *D ist vollständig ganzabgeschlossen und v-noethersch.*[73]
(5) *D ist ein v-noetherscher v-Bereich.*
(6) *D ist ein v-noetherscher Prüfer-v-Multiplikationsbereich.*

Beweis: Die Äquivalenzen (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (6) sind klar. (2) $\Leftrightarrow$ (3) ist genau die Aussage von Satz 1.18, S. 14, für t-Ideale. Wir beweisen die Implikationen (2) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6).

(2) $\Rightarrow$ (4) Bilden die gebrochen t-Ideale bzgl. der t-Multiplikation eine Gruppe, so stimmen t- und v-Idealsystem überein. Insbesondere ist also jedes v-Ideal v-invertierbar, woraus die vollständige Ganzabgeschlossenheit von D folgt. Da in D jedes t-Ideal t-invertierbar und somit t-endlich ist, besitzt D nach Lemma 1.17, S. 13, darüber hinaus die v-noethersche Eigenschaft.

(4) $\Rightarrow$ (5) In einem vollständig ganzabgeschlossenen Ring sind alle v-Ideale, insbesondere alle v-endlichen v-Ideale v-invertierbar.

(5) $\Rightarrow$ (6) In einem v-noetherschen v-Bereich ist das v-Inverse eines v-endlichen v-Ideals stets ein v-endliches v-Ideal. Insgesamt bilden die v-endlichen v-Ideale demnach eine Gruppe bzgl. der v-Multiplikation. □

Zum Abschluß dieses Abschnitts werfen wir noch ein Blick auf die Quotientenringe von Ringen mit ggT-Theorie e. T. und Ringen mit Divisorentheorie.

Satz 3.9. *Es seien D ein Integritätsbereich, N eine multiplikativ abgeschlossene Teilmenge von D und D_N der zugehörige Quotientenring. Dann gilt:*
(1) *Ist D ein Ring mit ggT-Theorie e. T., so auch D_N.*[74]
(2) *Ist D ein Ring mit Divisorentheorie, so auch D_N. Ist N das Komplement eines t-primen D-Ideals $\mathfrak{p}$, so ist die Lokalisierung $D_N = D_\mathfrak{p}$ von D bei $\mathfrak{p}$ insbesondere ein lokaler Hauptidealring.*

Beweis: Für jedes endlich erzeugte D-Ideal $\mathfrak{a}$ gilt aufgrund von Lemma 1.13.(2), S. 11,

$$(\mathfrak{a}_v D_N)^{-1} \subseteq (\mathfrak{a} D_N)^{-1} = \mathfrak{a}^{-1} D_N = \mathfrak{a}_v^{-1} D_N \subseteq (\mathfrak{a}_v D_N)^{-1}, \quad \text{d. h.} \quad (\mathfrak{a} D_N)_v = (\mathfrak{a}_v D_N)_v.$$

Ad (1) Sei D ein Ring mit ggT-Theorie e. T. Bedenkt man, daß dann mit $\mathfrak{a}_v$ auch das v-Ideal $\mathfrak{a}_v^{-1} = \mathfrak{a}^{-1}$ v-endlich ist, beispielsweise mit $\mathfrak{a}^{-1} = \mathfrak{b}_v$, $\mathfrak{b} \in \mathsf{f}(D)$, so erhält man $D_N = ((\mathfrak{a}\mathfrak{a}^{-1})_v D_N)_v = ((\mathfrak{a}\mathfrak{b})_v D_N)_v = (\mathfrak{a}\mathfrak{b} D_N)_v = (\mathfrak{a} D_N)_v \times (\mathfrak{b} D_N)_v$. Da jedes endlich erzeugte D_N-

[72] Bereits *Lorenzen 1939*, S. 542, bemerkt, daß „der totale Gruppensatz gleichwertig mit dem sogenannten Z. P. I." sei, also jenem Satz, daß sich „jedes ganze Ideal [...] eindeutig als Produkt von Primidealen darstellen" läßt.

[73] Ein Integritätsbereich D heißt *vollständig ganzabgeschlossen*, wenn jedes über D *fast ganze* Element aus K bereits in D enthalten ist. Dabei wird ein Element $\alpha \in K^*$ *fast ganz* über D genannt, wenn ein $a \neq 0$ mit $a\alpha^i \in D$ für alle $i \in \mathbb{N}$ existiert. Man überlegt sich leicht, daß über D ganze Elemente immer auch fast ganz über D sind. Falls D noethersch ist, so ist auch die Umkehrung dieser Aussage richtig, d. h. Ganzheits- und Fast-Ganzheitsbegriff stimmen überein. Andernfalls besteht die Möglichkeit, daß es über D fast ganze Elemente gibt, die keiner Ganzheitsbedingung im üblichen Sinne genügen. Die Begriffsbildung geht auf *Krull 1932* zurück und wurde angeregt durch seine Entdeckung, daß der von *van der Waerden 1967*, § 135, benutzte Ganzheitsbegriff für allgemeine Integritätsbereiche zu schwach ist. *Lorenzen 1939* konnte zeigen, daß sich Krulls vollständige Ganzabgeschlossenenheit idealtheoretisch als sogenannte „vollständige v-Abgeschlossenheit" charakterisieren läßt. Dabei heißt D *vollständig v-abgeschlossen*, wenn für jedes D-Ideal $\mathfrak{a}$ $(\mathfrak{a}_v : \mathfrak{a}_v) = D$ gilt (vgl. Anmerkung 32, S. 14). *van der Waerden 1967*, S. 195, schließlich führte den Beweis, daß D genau dann vollständig ganzabgeschlossen ist, wenn die v-Ideale bzgl. der v-Multiplikation eine Gruppe bilden. Insgesamt vgl. hierzu auch *Krull 1936b*. Daß Ringe mit Divisorentheorie durch die vollständige Ganzabgeschlossenheit sowie die v-noethersche Eigenschaft vollständig charakterisiert sind, wurde erstmals von *Lorenzen 1939*, S. 542, Satz 7, bewiesen. Vgl. auch *Anderson et al. 1988*, S. 28, Theorem 1.1.

[74] *Zafrullah 1978*, S. 8, Corollary 11.

Ideal ein D-Erweiterungsideal der Gestalt $\mathfrak{a}D_N$ mit $\mathfrak{a} \in \mathfrak{f}(D)$ ist, folgt hieraus die v-Gruppeneigenschaft der v-endlichen v-Ideale von D_N.

Ad (2) Sei D ein Ring mit Divisorentheorie. Dann ist D_N nach (1) ein Prüfer-v-Multiplikationsbereich. Um D_N als Ring mit Divisorentheorie nachzuweisen, reicht es zu zeigen, daß D_N v-noethersch ist (vgl. Satz 3.8.(6)). Dazu betrachten wir ein beliebiges ganzes t-Ideal des Quotientenringes D_N, und zwar in der Darstellung $(\mathfrak{a}D_N)_t$ mit $\mathfrak{a} \in \mathfrak{F}(D)$, sowie die aufsteigende Kette von ganzen D_N-Idealen

$$(\alpha_1 D_N)_t \subseteq ((\alpha_1, \alpha_2)D_N)_t \subseteq ((\alpha_1, \alpha_2, \alpha_3)D_N)_t \subseteq \ldots \qquad \text{mit } \alpha_i \in \mathfrak{a}. \tag{3.10}$$

Wegen $(\mathfrak{b}D_N)_v = (\mathfrak{b}D_N)_t \subseteq (\mathfrak{b}_t D_N)_t \subseteq (\mathfrak{b}_v D_N)_v = (\mathfrak{b}D_N)_v$ für alle $\mathfrak{b} \in \mathfrak{f}(D)$ lassen sich sämtliche in (3.10) auftretenden D_N-Ideale auch in der Form $((\alpha_1, \ldots, \alpha_n)_t D_N)_t$ schreiben. Die aufsteigende Kette von ganzen D-Idealen $(\alpha_1)_t \subseteq (\alpha_1, \alpha_2)_t \subseteq (\alpha_1, \alpha_2, \alpha_3)_t \subseteq \ldots$ muß jedoch abbrechen, da D als Ring mit Divisorentheorie v-noethersch ist. Dann wird jedoch auch die Kette (3.10) stationär, womit $(\mathfrak{a}D_N)_t$ als t-endlich und D_N insgesamt als v-noethersch nachgewiesen ist. Für den zweiten Teil der Aussage sei $\mathfrak{p} = \mathfrak{p}_t$ ein t-primes, nach Korollar 1.19.(2), S. 14, minimales D-Ideal. Aufgrund des eben Bewiesenen ist die Lokalisierung $D_\mathfrak{p}$ von D bei $\mathfrak{p}$ ein Ring mit Divisorentheorie. Da $D_\mathfrak{p}$ jedoch nur das eine (maximale, daher t-prime) Primideal $\mathfrak{m}_t = \mathfrak{p}D_\mathfrak{p}$ besitzt, ist jedes t-Ideal von $D_\mathfrak{p}$ eine t-Potenz von $\mathfrak{m}_t$. Wegen $\mathfrak{m}_t \times \mathfrak{m}_t \subsetneqq \mathfrak{m}_t$ existiert ein $\pi \in \mathfrak{m}_t$, das nicht in $\mathfrak{m}_t \times \mathfrak{m}_t$ enthalten ist, also ein π mit $\mathfrak{m}_t \mid \pi D_\mathfrak{p}$, aber $\mathfrak{m}_t \times \mathfrak{m}_t \nmid \pi D_\mathfrak{p}$. Daraus folgt aufgrund der Irreduzibilität von $\mathfrak{m}_t$ jedoch $\mathfrak{m}_t = \pi D_\mathfrak{p}$. Daher ist jedes $D_\mathfrak{p}$-Ideal ein Hauptideal. □

3.3. Divisorentheoretische Charakterisierung von Ringen mit ggT-Theorie e. T.

Aus der Tatsache, daß in einem Ring mit ggT-Theorie e. T. die gebrochenen v-endlichen v-Ideale eine Gruppe bilden, ergibt sich für die Kroneckersche ggT-Theorie $[\,\cdot\,] : D^* \to D^{v*}/D^{v\times}$ eine erhebliche Vereinfachung. Dazu überlege man sich, daß zu jedem $\frac{f}{g} \in D^v$ mit $\mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v$ ein $h \in K[X]$ existiert, so daß

$$\mathrm{c}(fh)_v = \mathrm{c}(f)_v \times \mathrm{c}(h)_v \subseteq \mathrm{c}(g)_v \times \mathrm{c}(h)_v = \mathrm{c}(gh)_v = D$$

gilt. Man kann also durch Erweitern mit einem geeigneten Polynom $h \in K[X]$ erreichen, daß im Nenner eines Elementes aus D^v stets ein v-primitives Polynom steht. Da die v-primitiven Polynome Einheiten in D^v sind, folgt daraus mit Satz 2.21, S. 25, daß jeder Kronecker-Divisor von D die Gestalt $[\,\alpha_0 + \alpha_1 X + \ldots + \alpha_m X^m\,]$ mit $\alpha_i \in K^*$ hat. Darüber hinaus ergibt sich, daß der Kroneckersche Funktionalring D^v folgende Gestalt annimmt:

$$D^v = \left\{ \frac{f}{g} : f, g \in D[X] \text{ mit } \mathrm{c}(g)_v = D \right\}.$$

Definition 3.11. *Es seien D ein Integritätsbereich, $D[X]$ der Polynomring über D in der Unbestimmten X und $(\cdot)_*$ eine $*$-Idealoperation auf D. Dann heißt der Quotientenring von $D[X]$ nach der multiplikativ abgeschlossenen Menge aller $*$-primitiven Polynome von D,*[75] *also der Quotientenring*

$$D[X]_{N_*(D)} \quad \textit{mit} \quad N_*(D) := \{g \in D[X] : \mathrm{c}(g)_* = D\},$$

*der **Nagatabereich** von D bzgl. der $*$-Idealoperation $(\cdot)_*$. Wir schreiben dafür auch $D_*(X)$.*[76]

[75] Die Menge der $*$-primitiven Polynome ist für jede Idealoperation $(\cdot)_*$ multiplikativ abgeschlossen. Vgl. hierzu auch *Kang 1989*, S. 153, Proposition 2.1.(1).

[76] Quotientenringe der Gestalt $D[X]_{N_d(D)}$ mit $N_d(D) = \{f \in D[X] : \mathrm{c}(f)_d = D\}$ kommen schon bei *Krull 1942* vor. *Huckaba 1988*, S. 140, zufolge wurden sie jedoch erstmals von Nagata in seinem Buch „Local rings“ aus dem Jahre 1962 in der heute üblichen Notation $D(X)$ systematisch untersucht. Bei *Querre 1980*, S. 270, findet sich für diese Ringe die Bezeichnung *Nagata-Ring* („*anneau de Nagata*“).

Wir haben demnach soeben gezeigt, daß für einen Ring mit ggT-Theorie e. T. der zugehörige Kroneckersche Funktionalring D^v mit dem zugehörigen Nagatabereich $D_v(X)$ übereinstimmt. Der folgende Satz, der das Analogon zu Satz 2.23, S. 26, darstellt, zeigt u. a., daß für ganzabgeschlossene Integritätsbereiche auch die Umkehrung dieser Aussage richtig ist.

Satz 3.12. *Für einen Integritätsbereich D sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit ggT-Theorie e. T.*
(2) *D ist ganzabgeschlossen und $D_v(X) = D^v$.*[77]
(3) *$D_v(X)$ ist ganzabgeschlossen und $D_v(X) = D^v$.*
(4) *D ist ein v-Bereich mit $D_v(X) = D^v$.*[78]
(5) *$D_v(X)$ ist ein Bezoutbereich mit $D_v(X) = D^v$.*
(6) *$D_v(X)$ ist ein Bezoutbereich.*[79]
(7) *$D_v(X)$ ist ein Prüferbereich.*[80]
(8) *$D_v(X)$ ist ein ggT-Bereich.*[81]
(9) *$D_v(X)$ ist ein Ring mit ggT-Theorie e. T.*[82]
(10) *$D[X]$ ist ein Ring mit ggT-Theorie e. T.*[83]

Beweis: (1) $\Rightarrow$ (2) ergibt sich aus dem oben Gesagten. (2) $\Rightarrow$ (3) folgt aus der Tatsache, daß jeder Polynomring sowie jeder Quotientenring eines ganzabgeschlossenen Ringes wieder ganzabgeschlossen ist. Die Implikationen (3) $\Rightarrow$ (4) $\Rightarrow$ (5) ergeben sich unmittelbar aus Satz 2.23, S. 26, die Implikationen (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (9) sind trivial, ebenso (6) $\Rightarrow$ (8) $\Rightarrow$ (9). Zu (9) $\Rightarrow$ (1) überlege man sich, daß $D[X]$ ein freier D-Modul ist und für den Quotientenring $D_v(X) = D[X]_{N_v(D)}$ stets $D_v(X) \cap K = D$ gilt. Damit sind jedoch die Voraussetzungen von Satz 1.12, S. 11, erfüllt, und es folgt, daß D ein Prüfer-v-Multiplikationsbereich, also ein Ring mit ggT-Theorie e. T. ist. Mit demselben Argument ergibt sich (für $N = \{1\}$) die Implikation (10) $\Rightarrow$ (1). Für den Beweis von (1) $\Rightarrow$ (10), der etwas komplizierter ist, verweisen wir auf die Literatur.[84] □

Die Aussagen von Satz 3.12 sind im wesentlichen bekannt. Der hier vorgestellte Beweis unterscheidet sich von den bereits vorhandenen vor allem in methodischer Hinsicht.[85]

Wenden wir uns nunmehr wieder dem Fall zu, daß die Divisorengruppe $\mathfrak{G}$ faktoriell ist, also mit der ggT-Theorie e. T. $(\cdot) : D^* \to \mathfrak{G}^+$ eine Divisorentheorie für den Integritätsbereich D vorliegt. Wir wissen, daß D ein Prüfer-v-Multiplikationsbereich ist, in dem sämtliche t-Ideale t-endlich sind. Insbesondere ist der Kroneckersche Funktionalring D^v von D ein Bezoutbereich mit $D^v = D_v(X)$. Da die Divisorentheorie für D aufgrund des Eindeutigkeitssatzes 3.5 zur Kroneckerschen ggT-Theorie isomorph ist, erhält man darüber hinaus $\mathfrak{G}^+ \cong D_v(X)^*/D_v(X)^\times$. Daraus folgt schließlich, daß der Bezoutbereich $D_v(X)$ ein faktorieller Ring, insbesondere also ein Ring mit Divisorentheorie und somit v-noethersch ist. Zu jedem $D_v(X)$-Ideal $\mathfrak{a}$ existieren daher endlich viele rationale Funktionen $f_1, \ldots, f_n \in \mathfrak{a}$ mit $\mathfrak{a}_t = (f_1, \ldots, f_n)_t$. Aufgrund der Bezouteigenschaft ist jedoch bereits das von $f_1, \ldots, f_n$ erzeugte d-Ideal, also erst recht des zugehörige t-Ideal ein Hauptideal. Es gibt also ein $f \in \mathfrak{a}$ mit $\mathfrak{a} \subseteq \mathfrak{a}_t = fD_v(X) \subseteq \mathfrak{a}$, womit $\mathfrak{a}$ als $D_v(X)$-Hauptideal

[77] *Querre 1980*, S. 279, Corollaire 4.2.
[78] *Arnold et al. 1971*, S. 484, Theorem 3.(2), oder *Gilmer 1970*, S. 586, Theorem 2.5.
[79] *Zafrullah 1984*, S. 236, Corollary 13.(3), oder *Kang 1989*, S. 160, Theorem 3.7.(5).
[80] *Zafrullah 1984*, S. 235, Theorem 11, oder *Kang 1989*, S. 160, Theorem 3.7.(4).
[81] *Querre 1980*, S. 278, Corollaire 1.(2).
[82] *Kang 1989*, S. 160, Theorem 3.7.(3).
[83] *Houston et al. 1984*, S. 51, Proposition 2.3, oder *Kang 1989*, S. 160, Theorem 3.7.(2).
[84] *Querre 1980*, S. 275, Théorème 4.
[85] Den besten Eindruck von der üblichen Vorgehensweise und einen guten Überblick über die wichtigsten Ergebnisse verschafft m. E. die Darstellung von *Kang 1989*.

nachgewiesen ist. Ist also D ein Ring mit Divisorentheorie, so ist der zugehörige Nagatabereich $D_v(X) = D^v$ ein Hauptidealbereich.

Auch die Umkehrung dieser Aussage ist richtig. Dazu charakterisieren wir die Ringe mit Divisorentheorie allgemein durch ihren zugehörigen Nagatabereich $D_v(X)$ bzgl. der v-Idealoperation. In vollkommener Analogie zu Satz 3.12 beweist man

Satz 3.13. *Für einen Integritätsbereich D sind folgende Aussagen äquivalent:*
(1) *D ist ein Ring mit Divisorentheorie.*
(2) *$D_v(X)$ ist ein Hauptidealbereich.*[86]
(3) *$D_v(X)$ ist ein Dedekindbereich.*
(4) *$D_v(X)$ ist eine faktorieller Integritätsbereich.*
(5) *$D_v(X)$ ist ein Ring mit Divisorentheorie.*[87]

Beweis: Die Implikationen (1) $\Rightarrow$ (2) $\Rightarrow$ (4) $\Rightarrow$ (5) sowie (2) $\Rightarrow$ (3) sind aufgrund des oben Gesagten klar.

(3) $\Rightarrow$ (5) Da das d-Idealsystem endlichartig ist, stimmt im Falle eines Dedekindbereiches die Gruppe der d-Ideale mit der Gruppe der t-Ideale überein. Daher ist jeder Dedekindbereich ein Ring mit Divisorentheorie.

(5) $\Rightarrow$ (1) Sei $D_v(X)$ ein Ring mit Divisorentheorie. Dann ist D ein Prüfer-v-Multiplikationsbereich, und nach Satz 3.7.(3) reicht es zu zeigen, daß D v-noethersch ist. Dazu sei $\mathfrak{a}$ ein beliebiges gebrochenes D-Ideal. Da $D_v(X)$ v-noethersch und somit jedes t-Ideal t-endlich ist, ist auch das von $\mathfrak{a}$ in $D_v(X)$ erzeugte t-Ideal $(\mathfrak{a}D_v(X))_t$ t-endlich. Insbesondere besitzt $(\mathfrak{a}D_v(X))_t$ ein endliches t-Erzeugendensystem aus Elementen von $\mathfrak{a}$. Denn die aufsteigende Kette von $D_v(X)$-Idealen

$$(\alpha_1)_t \subsetneqq (\alpha_1, \alpha_2)_t \subsetneqq (\alpha_1, \alpha_2, \alpha_3)_t \subsetneqq \dots \quad \text{mit } \alpha_i \in \mathfrak{a}$$

muß nach endlich vielen Schritten abbrechen. Es existieren also $\alpha_1, \dots, \alpha_m \in \mathfrak{a}$ mit $(\mathfrak{a}D_v(X))_t = ((\alpha_1, \dots, \alpha_m)D_v(X))_t$. Das t-Spurideal von $\mathfrak{a}$ in D ist demnach gegeben durch

$$\mathfrak{a}_{t_p} = (\mathfrak{a}D_v(X))_t \cap K = ((\alpha_1, \dots, \alpha_m)D_v(X))_t \cap K = (\alpha_1, \dots, \alpha_m)_{t_p},$$

d. h. jedes t_p-Ideal von D ist t_p-endlich. Da jedes t-Ideal von D ein t_p-Ideal ist, ergibt sich

$$\mathfrak{a}_t = (\mathfrak{a}_t)_{t_p} = (\alpha_1, \dots, \alpha_m)_{t_p} \subseteq (\alpha_1, \dots, \alpha_m)_t \subseteq (\mathfrak{a}_t)_t = \mathfrak{a}_t \qquad \text{mit } \alpha_i \in \mathfrak{a}_t.$$

Jedes t-Ideal von D ist daher t-endlich, womit D insgesamt als v-noethersch nachgewiesen ist. □

Beschreiben wir die Divisorentheorie für D als Kroneckersche Divisorentheorie $(\cdot) : D^* \to D_v(X)^*/D_v(X)^\times$, so nehmen die Primdivisoren aufgrund von Satz 3.13 eine besonders einfache Gestalt an: Es handelt sich nämlich (bis auf Assoziiertheit) genau um die Primelemente von $D_v(X)$. Die Primdivisorzerlegung eines Elementes $\alpha \in D^*$ zu bestimmen, läuft also darauf hinaus, α als Element von $D_v(X)$ aufzufassen und seine Primfaktorzerlegung in dem Hauptidealring $D_v(X)$ zu bestimmen.

3.4. Der ganze Abschluß von Ringen mit ggT-Theorie e. T.

In Abschnitt 2.7 wurde gezeigt, daß der ganze Abschluß T eines Ringes D mit ggT-Theorie in einer beliebigen algebraischen Körpererweiterung L/K wieder ein Ring mit ggT-Theorie ist. Für Ringe mit ggT-Theorie e. T. gilt eine entsprechende Aussage.

[86] *Gilmer 1992*, S. 552, Corollary 44.12.

[87] Obwohl Ringe mit Divisorentheorie (unter der Bezeichnung Krullbereich; vgl. Abschnitt 3.5) besser erforscht sind als Ringe mit ggT-Theorie e. T. (unter der Bezeichnung Prüfer-v-Multiplikationsbereich) und obwohl die entsprechenden Aussagen für Prüfer-v-Multiplikationsbereiche (also die äquivalenten Bedingungen von Satz 3.12) in der Literatur bewiesen werden, habe ich bis auf die Äquivalenz (1) $\Leftrightarrow$ (2) keinen Nachweis für die aufgeführten Charakterisierungen eines Ringes mit Divisorentheorie/Krullbereiches finden können.

Satz 3.14. *Es seien D ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper K und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Genau dann ist T ein Ring mit ggT-Theorie e. T./Prüfer-v-Multiplikationsbereich, wenn D ein Ring mit ggT-Theorie e. T./Prüfer-v-Multiplikationsbereich ist.*[88]

Beweis: Wir beweisen die Aussage des Satzes für Prüfer-v-Multiplikationsbereiche. Es seien also D ein Prüfer-v-Multiplikationsbereich und $\mathfrak{a}$ irgendein ganzes endlich erzeugtes T-Ideal. Dieselben Überlegungen wie im Beweis von Satz 2.26 zeigen, daß dann ein endlich erzeugtes ganzes T-Ideal $\mathfrak{a}'$ sowie ein endlich erzeugtes ganzes D-Ideal $\mathfrak{b}$ mit $\mathfrak{a}_{v_T} \times \mathfrak{a}'_{v_T} \times \mathfrak{b}_{v_T}^{-1} = T$ existieren. Nach Voraussetzung gibt es zu $\mathfrak{b}$ ein endlich erzeugtes gebrochenes D-Ideal $\mathfrak{b}'$ mit $D = (\mathfrak{b}\mathfrak{b}')_{v_D}$. Aufgrund des Krullschen Lemmas 2.27 folgt hieraus jedoch $T = (\mathfrak{b}\mathfrak{b}')_{v_T} = \mathfrak{b}_{v_T} \times \mathfrak{b}'_{v_T}$, und man erhält $\mathfrak{b}_{v_T}^{-1} = \mathfrak{b}'_{v_T}$. Also besitzt das endlich erzeugte T-Ideal $\mathfrak{a}$ in dem v_T-Ideal $\mathfrak{a}'_{v_T} \times \mathfrak{b}'_{v_T}$ ein v_T-endliches v_T-Inverses, womit T als Prüfer-v-Multiplikationsbereich nachgewiesen ist.

Es werde nunmehr T als Prüfer-v-Multiplikationsbereich vorausgesetzt. Wegen Satz 3.12.(2) reicht es, die Gleichheit $D^v = D_v(X)$ zu zeigen. Dazu überlege man sich, daß D Satz 2.26 zufolge zumindest ein Ring mit ggT-Theorie ist und somit durch $T^v = T_v(X) = T[X]_{N_v(T)}$ der ganze Abschluß von D^v in der algebraischen Körpererweiterung $L(X)/K(X)$ gegeben ist (vgl. Satz 2.28). Wir zeigen, daß der Quotientenring $T[X]_{N_v(D)}$, also der ganze Abschluß von $D[X]_{N_v(D)} = D_v(X)$ in $L(X)/K(X)$, mit dem Nagatabereich $T_v(X)$ übereinstimmt. Wegen

$$D^v = T^v \cap K(X) = T_v(X) \cap K(X) = T[X]_{N_v(D)} \cap K(X) = D[X]_{N_v(D)} = D_v(X)$$

folgt daraus dann die Behauptung. Die Inklusion $T[X]_{N_v(D)} \subseteq T[X]_{N_v(T)}$ ergibt sich aus $N_v(D) \subseteq N_v(T)$, einer unmittelbaren Folgerung aus dem Krullschen Lemma 2.27. Für die umgekehrte Inklusion sei $p \in N_v(T)$, also $p \in T[X]$ mit $\mathrm{c}(p)_{v_T} = T$. Dann ist p wegen $p, \frac{1}{p} \in T^v$ eine Einheit in T^v. Bezeichnet K' jenen Körper, der aus K durch Adjunktion der Koeffizienten von p entsteht, so ist $N_{K'/K}(p) \in D[X]$ eine Einheit in D^v, also $N_{K'/K}(p)^{-1} \in D^v$. Daraus folgt aber $D \subseteq \mathrm{c}(N_{K'/K}(p))_{v_D} \subseteq D$, also $N_{K'/K}(p) \in N_v(D)$. $N_{K'/K}(p)$ wiederum ist bzgl. $T[X]$ durch p teilbar, d. h. es existiert ein $g \in T[X]$ mit $N_{K'/K}(p) = p \cdot g$. Für jedes $\frac{f}{p} \in T_v(X)$ mit $f \in T[X]$, $p \in N_v(T)$, gilt daher

$$\frac{f}{p} = \frac{fg}{pg} = \frac{fg}{N_{K'/K}(p)} \in T[X]_{N_v(D)},$$

woraus $T[X]_{N_v(T)} \subseteq T[X]_{N_v(D)}$ folgt. □

Satz 3.15. *Es seien D ein Ring mit ggT-Theorie e. T./Prüfer-v-Multiplikationsbereich mit Quotientenkörper K und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Dann ist der ganze Abschluß des Nagatabereichs $D_v(X)$ von D in der algebraischen Körpererweiterung $L(X)/K(X)$ gleich dem Nagatabereich $T_v(X)$ von T.*

Beweis: In einem Ring mit ggT-Theorie e. T. stimmen Kroneckerscher Funktionalring und Nagatabereich bzgl. der v-Idealoperation überein. Aufgrund von Satz 3.14 ist daher $D^v = D_v(X)$ und $T^v = T_v(X)$. Mit Satz 2.28, S. 29, folgt hieraus die Behauptung. □

Es sei an dieser Stelle kurz bemerkt, daß Satz 3.14 über den ganzen Abschluß eines Ringes mit ggT-Theorie e. T. sowie Satz 3.15 über den ganzen Abschluß des zugehörigen Nagatabereichs auch ohne Rückgriff auf das zentrale Krullsche Lemma 2.27 bewiesen werden können, und zwar durch

[88] Daß der ganze Abschluß eines Prüfer-v-Multiplikationsbereiches in einer algebraischen Körpererweiterung wieder ein Prüfer-v-Multiplikationsbereich ist, wurde erstmals von *Prüfer 1932*, S. 31, § 11, bewiesen. *Jaffard 1960*, S. 108, Théorème 9, zeigt eine entsprechende Aussage für Prüferbereiche und bemerkt, daß sich sein Beweis auf Prüfer-v-Multiplikationsbereiche übertragen lasse. Die Umkehrung dieser Aussage wurde meines Wissens bislang noch nicht bewiesen.

Adaption eines entsprechenden Beweises für Ringe mit Divisorentheorie, wie er beispielsweise bei *Koch 1992* zu finden ist.[89] Wir wollen darauf jedoch hier nicht weiter eingehen.

Es sei nunmehr D wieder ein Ring mit Divisorentheorie. Nach den bisherigen Ergebnissen ist der ganze Abschluß T von D in einer beliebigen algebraischen Körpererweiterung L/K zumindest ein Ring mit ggT-Theorie e. T. Tatsächlich gilt

Satz 3.16. *Es seien D ein ganzabgeschlossener Integritätsbereich mit Quotientenkörper K und T der ganze Abschluß von D in der algebraischen Körpererweiterung L/K. Dann gilt*
(1) *Ist $[L:K] < \infty$ und D ein Ring mit Divisorentheorie, so besitzt auch T eine Divisorentheorie.*
(2) *Ist T ein Ring mit Divisorentheorie, so besitzt auch D eine Divisorentheorie.*

Beweis: Ad (1) Ist D ein Ring mit Divisorentheorie, so ist der ganze Abschluß T auf jeden Fall ein Ring mit ggT-Theorie e. T., und es gilt $T_v(X) = T^v$. Aufgrund von Satz 3.13.(2) reicht es zu zeigen, daß in dem Bezoutbereich $T_v(X)$ *jedes* Ideal endlich erzeugt und somit Hauptideal ist. Dazu betrachte man ein beliebiges ganzes $T_v(X)$-Ideal $\mathfrak{a}$ und die aufsteigende Kette von ganzen endlich erzeugten $T_v(X)$-Idealen

$$(\alpha_1)_d \subsetneqq (\alpha_1,\alpha_2)_d \subsetneqq (\alpha_1,\alpha_2,\alpha_3)_d \subsetneqq \dots \quad \text{mit } \alpha_i \in \mathfrak{a}. \tag{3.17}$$

Sämtliche in dieser Kette auftretenden Ideale sind aufgrund der Bezout-Eigenschaft von $T_v(X)$ Hauptideale, sagen wir $\gamma_i T_v(X) := (\alpha_1,\dots,\alpha_i)_d$ mit $\gamma_i \in T_v(X)$ für $i = 1,2,\dots$. Damit übersetzen sich die Inklusionsbeziehungen jedoch in Teilbarkeitsbeziehungen, und man erhält eine echt absteigende Teilerkette

$$\dots, \quad \gamma_4 \mid \gamma_3, \quad \gamma_3 \mid \gamma_2, \quad \gamma_2 \mid \gamma_1.$$

Dann gilt entsprechendes aber auch für die Normen dieser Elemente bzgl. der Körpererweiterung $L(X)/K(X)$.[90] Da jedoch $N_{L/K}(\gamma_1)$ als Element von $K(X)$ bzgl. des Hauptidealringes $D_v(X)$ nur endlich viele Teiler besitzt, muß die Teilerkette der Normen und damit auch die Idealkette (3.17) nach endlich vielen Schritten abbrechen. Es folgt $\mathfrak{a} = (\alpha_1,\dots,\alpha_m)_d = \gamma_m T_v(X)$ für ein $m \in \mathbb{N}$, womit $T_v(X)$ als Hauptidealring nachgewiesen ist.

Ad (2) Besitzt T eine Divisorentheorie, so ist D zumindest noch ein Ring mit ggT-Theorie, und es reicht gemäß Satz 3.7.(2) zu zeigen, daß D die v-noethersche Eigenschaft besitzt. Dazu sei $\mathfrak{a}$ ein ganzes D-Ideal. Für das Erweiterungsideal $\mathfrak{a}T$ muß die aufsteigende Kette von v_T-Idealen

$$(\alpha_1)_{v_T} \subseteq (\alpha_1,\alpha_1)_{v_T} \subseteq (\alpha_1,\alpha_2,\alpha_3)_{v_T} \subseteq \dots \qquad \text{mit } \alpha_i \in \mathfrak{a}$$

nach endlich vielen Schritten abbrechen, da T als Ring mit Divisorentheorie v-noethersch ist. Es existieren also $\alpha_1,\dots,\alpha_m \in \mathfrak{a}$ mit $\mathfrak{a}_{v_T} = (\alpha_1,\dots,\alpha_m)_{v_T}$. Da v- und t-Idealoperation von T übereinstimmen, die v_T-Idealoperation also insbesondere endlichartig ist, muß auch die Spuroperation von D bzgl. $\mathsf{F}_v(T) = \mathsf{F}_t(T)$ endlichartig sein. Die Spuroperation ist jedoch nach Aussage des Krullschen Lemmas 2.27 genau die v-Idealoperation von D, die demzufolge mit ihrer zugehörigen endlichartigen Idealoperation, der t-Operation, übereinstimmt. Es folgt $\mathfrak{a}_t = \mathfrak{a}_{v_D} = (\alpha_1,\dots,\alpha_m)_{v_D}$, womit $\mathfrak{a}_t$ als t-endlich und D insgesamt als v-noethersch nachgewiesen ist. □

3.5. Der bewertungstheoretische Zugang

Es entspricht durchaus nicht dem üblichen Vorgehen, Ringe mit Divisorentheorie, wie in vorangegangenen Abschnitten geschehen, in der Sprache der v-Ideale bzw. der Kronecker-Divisoren

[89] *Koch 1992*, S. 26, Lemma 1.31, oder *Koch 1966*, S. 187f., Abschnitt 2.

[90] An dieser Stelle benötigt man die Endlichkeit der algebraischen Erweiterung L/K. Denn man kann i. a. nicht davon ausgehen, daß sich die Erzeugenden aller $T_v(X)$-Ideale $\mathfrak{a}$ in einer endlichen Körpererweiterung K'/K einfangen lassen, falls $[L:K] = \infty$ ist.

zu beschreiben und zu charakterisieren. In der Regel werden Ringe mit Divisorentheorie im Rahmen der allgemeinen Bewertungstheorie untersucht, so z. B. auch in der klassischen Darstellung von Borewicz-Šafarevič. Selbst Bourbaki, dessen Abschnitt über Ringe mit Divisorentheorie mit der Einführung der v-Ideale („*divisorial ideals*“) beginnt und im weiteren Verlauf auch eine idealtheoretische Charakterisierung für Ringe mit Divisorentheorie bringt (vgl. Satz 3.8.(4) in dieser Arbeit), arbeitet fast ausschließlich mit bewertungstheoretischen Methoden.[91] Und auch das bereits mehrfach zitierte Werk „Multiplicative Ideal Theory“ von Gilmer macht in dieser Beziehung im Grunde keine Ausnahme. Zwar geht Gilmer ausführlich auf die Idealstruktur von Ringen mit Divisorentheorie ein, argumentiert aber bei den Beweisen häufig bewertungstheoretisch.[92]

Das Übergewicht der bewertungstheoretischen Methode ist nicht allein aus ihrer großen Bedeutung für die moderne algebraische Zahlentheorie und kommutative Algebra zu erklären; sie hat m. E. auch historische Gründe. Die Grundlagen der allgemeinen Bewertungstheorie, d. h. jener Theorie, die die Bewertungen eines beliebigen Körpers sowohl mit archimedischer wie auch nichtarchimedischer Wertgruppe zum Gegenstand hat,[93] wurden zu Beginn der 30-er Jahre von Krull gelegt. In seiner 1932 erschienenen Abhandlung „Allgemeine Bewertungstheorie“ entwickelte Krull den noch heute gültigen Begriffsapparat (u. a. den Begriff der allgemeinen *Bewertung* und des *Bewertungsringes*[94]). Die Untersuchungen zeigen, daß sich viele algebraische Eigenschaften von Integritätsbereichen und deren Quotientenkörpern bewertungstheoretisch beschreiben lassen. So konnte Krull z. B. beweisen: Ein Integritätsbereich ist ganzabgeschlossen genau dann, wenn er als Durchschnitt von Bewertungsoberringen darstellbar ist. Gibt es eine Darstellung, in der ausschließlich Bewertungsringe von reellwertigen Bewertungen (sogenannte „spezielle Bewertungsringe“ in Krullscher Terminologie) vorkommen, so ist der Integritätsbereich darüber hinaus vollständig ganzabgeschlossen.[95]

Es liegt auf der Hand, daß durch weitere Bedingungen an die Durchschnittsdarstellung eines ganzabgeschlossenen Integritätsbereiches Ringe mit neuen charakteristischen Eigenschaften entstehen. Besonderes Augenmerk richtete Krull auf vollständig ganzabgeschlossene Integritätsbereiche der Gestalt

$$D = \bigcap_{i \in I} D_i, \quad \{D_i\}_{i \in I} \text{ Familie diskreter Bewertungsoberringe von } D,$$

mit der zusätzlichen Eigenschaft, daß jedes $\alpha \in D^*$ in fast allen D_i eine Einheit ist.[96] Krull wählte für diese Ringe den Namen „*endliche diskrete Hauptordnung*“, eine Bezeichnung, die sich nicht durchgesetzt hat. Heute spricht man stattdessen von sogenannten *Krullbereichen*, und diese wiederum sind nichts anderes als die hier behandelten Ringe mit Divisorentheorie. Diese

[91] Vgl. *Bourbaki 1989*, VII.

[92] Vgl. *Gilmer 1992*, § 44.

[93] Bezeichnet Γ eine linear geordnete additive Gruppe, so heißt eine Abbildung $v : K \to \Gamma \cup \{\infty\}$ *Bewertung* von K, wenn sie den folgenden drei Axiomen genügt: (1) $v(K^*) = \Gamma$, $v(0) = \infty$, (2) $v(\alpha\beta) = v(\alpha) + v(\beta)$ für alle $\alpha, \beta \in K$, (3) $v(\alpha + \beta) \geqslant \min\{v(\alpha), v(\beta)\}$ für alle $\alpha, \beta \in K$. Genau dann, wenn die *Wertgruppe* Γ das archimedische Axiom erfüllt, ist Γ zu einer additiven Untergruppe der reellen Zahlen isomorph, und man nennt in diesem Fall die Bewertung auch *reellwertig*. Eine reellwertige Bewertung heißt *diskret*, wenn die Wertgruppe zur additiven Gruppe der ganzrationalen Zahlen $\mathbb{Z}$ isomorph ist.

[94] Ein Integritätsbereich D heißt danach *Bewertungsring*, wenn für alle $\alpha, \beta \in D$ entweder $\alpha \mid \beta$ oder $\beta \mid \alpha$ gilt. Man zeigt, daß es zu jedem Bewertungsring D mit Quotientenkörper K eine Bewertung $v : K \to \Gamma \cup \{\infty\}$ mit archimedischer oder nichtarchimedischer Wertgruppe gibt, so daß $D = D_v := \{\alpha \in K : v(\alpha) \geqslant 0\}$ gilt. Ist die Bewertung v diskret, so spricht man auch von einem *diskreten Bewertungsring*. Ein lokaler Ring ist genau dann ein Bewertungsring (diskreter Bewertungsring), wenn er ein Bezoutbereich (Hauptidealbereich) ist.

[95] Vgl. Anmerkung 73.

[96] Ringe, die sich als Durchschnitt von beliebigen (nicht notwendig diskreten) Bewertungsoberringen darstellen lassen und darüber hinaus dieser zusätzlichen Bedingung genügen, heißen in der englischsprachigen Literatur „*rings of finite character*“, bei *Krull 1935*, S. 104, Abschnitt 37, auch „*endliche Hauptordnungen*“.

Übereinstimmung ist mit Sicherheit nicht zufällig. Es liegt vielmehr die Vermutung nahe, daß Borewicz-Šafarevič in den endlichen diskreten Hauptordnungen von Krull die allgemeinsten Ringe mit Primdivisorzerlegung erkannten und diese bezeichnende arithmetische Eigenschaft auch in der Definition zum Ausdruck bringen wollten. Mit anderen Worten: Der Begriff eines Ringes mit Divisorentheorie ist zunächst nichts anderes als der Versuch, der abstrakten Krullschen Defintion eine plastische, anschauliche Gestalt zu geben. Das zeigt sich auch deutlich in der Darstellung von Borewicz-Šafarevič. Sobald die Ringe mit Divisorentheorie erst einmal im Krullschen Sinne als endliche diskrete Hauptordnungen charakterisiert sind,[97] tritt die axiomatische Definition vollkommen in den Hintergrund, und die weitere Argumentation verläuft im wesentlichen bewertungstheoretisch.

Aus Korollar 1.19, S. 14, Satz 3.8.(2), S. 36, und Satz 3.9.(2), S. 36, folgt, daß die Lokalisierung $D_{\mathfrak{p}}$ eines Ringes D mit Divisorentheorie bei einem Primideal $\mathfrak{p}$ genau dann ein diskreter Bewertungsring ist, wenn $\mathfrak{p}$ t-prim ist. Also sind durch die Familie $\{D_{\mathfrak{p}}\}_{\mathfrak{p}\ t\text{-prim}}$ sämtliche diskreten Bewertungsoberringe von D gegeben, die sich als Lokalisierungen von D darstellen lassen. Da jedes Element $\alpha \in D^*$ nur in endlich vielen t-Primidealen enthalten ist bzw. das von ihm erzeugte Hauptideal nur von endlich vielen t-Primidealen geteilt wird, ist unmittelbar einsichtig, daß α nur in endlich vielen diskreten Bewertungsoberringen $D_{\mathfrak{p}}$ eine Nichteinheit ist. Da außerdem die Einheiten von D genau jene Elemente sind, die in keinem t-Primideal eingefangen werden, gilt darüber hinaus $\alpha \in D_{\mathfrak{p}}$ für alle t-Primideale $\mathfrak{p}$ genau dann, wenn α eine Einheit in D ist. Daraus folgt schließlich für Ringe mit Divisorentheorie die Krullsche Darstellung

$$D = \bigcap_{\mathfrak{p}\ t\text{-prim}} D_{\mathfrak{p}}.$$

Es stellt sich die Frage, inwieweit auch Ringe mit ggT-Theorie e. T. eine solche bewertungstheoretische Beschreibung zulassen. Man beweist die Äquivalenz folgender Aussagen:
(1) D ist ein Ring mit ggT-Theorie e. T.
(2) Die Lokalisierung $D_{\mathfrak{p}}$ ist für alle t-primen t-Ideale $\mathfrak{p}$ ein Bewertungsring.[98]
(3) Die Lokalisierung $D_{\mathfrak{m}}$ ist für alle t-maximalen t-Ideale $\mathfrak{m}$ ein Bewertungsring.[99]
Verglichen mit der bewertungstheoretischen Charakterisierung von Ringen mit Divisorentheorie sind diese Kriterien verhältnismäßig schwach. Zwar läßt sich jeder Ring D mit ggT-Theorie e. T. ebenfalls als Durchschnitt von Bewertungsoberringen darstellen, nämlich als

$$D = \bigcap_{\mathfrak{m}\ t\text{-maximal}} D_{\mathfrak{m}} \qquad \text{bzw.} \qquad D = \bigcap_{\mathfrak{p}\ t\text{-prim}} D_{\mathfrak{p}};$$

die Bewertungsoberringe $D_{\mathfrak{m}}$ bzw. $D_{\mathfrak{p}}$ werden i. a. jedoch nicht diskret sein, und auch die entscheidende Endlichkeitsvoraussetzung, daß jedes $\alpha \in D$ in fast allen $D_{\mathfrak{m}}$ bzw. $D_{\mathfrak{p}}$ eine Einheit ist, braucht nicht erfüllt zu sein.

Im Hinblick auf allgemeine arithmetische Überlegungen, wie sie in der vorliegenden Arbeit angestellt wurden, trägt der bewertungstheoretische Ansatz daher nicht so weit, wie man es von seiner Bedeutung für die Behandlung der Ringe mit Divisorentheorie vielleicht erwarten würde. Die neuesten Arbeiten über Ringe mit ggT-Theorie e. T. („*rings with quasi-divisors theory*“) zeigen jedoch, daß bei anderen Fragestellungen, z. B. bei der Formulierung von Appproximationssätzen, die Bewertungstheorie durchaus gewinnbringend eingesetzt werden kann.[100]

[97] *Borewicz et al. 1966*, S. 196, Satz 4.
[98] *Mott et al. 1981*, S. 12, Corollary 4.3.(2).
[99] *Griffin 1967*, S. 715, Theorem 5.2.
[100] Vgl. hierzu die Arbeiten von Močkoř, insbesondere *Močkoř et al. 1993a*, *Močkoř et al. 1993b* sowie *Geroldinger et al. 1995*.

Kapitel 4

Der Begriff des „algebraischen Divisors“ bei Kronecker

Bereits im Jahre 1859 hatte Kummer angekündigt, daß Kronecker „nächstens“ eine vollständige Theorie der Idealzerlegung in beliebigen algebraischen Zahlkörpern veröffentlichen werde. Aus heute nicht mehr nachvollziehbaren Gründen vergingen jedoch noch mehr als 20 Jahre, bis Kronecker mit der sogenannten Kummer-Festschrift seine „Grundzüge einer arithmetischen Theorie der algebraischen Grössen“ publizierte. In der Zwischenzeit hatte Dedekind die Grundlagen der Idealtheorie entwickelt und mit ihrer Hilfe die arithmetische Situation in algebraischen Zahlkörpern analysiert und umfassend beschrieben. Nach Erscheinen der Kummer-Festschrift im Jahre 1882 wurde jedoch deutlich, daß Kronecker offenbar einen sehr viel allgemeineren Ansatz als Dedekind verfolgte: Ihm ging es nicht allein um eine Theorie der ganzen algebraischen Zahlen in algebraischen Zahlkörpern, sondern vielmehr um eine großangelegte Theorie der algebraischen Funktionenkörper, in denen die algebraischen Zahlkörper als Spezialfall vorkamen. Abgesehen davon, daß Dedekinds Idealbegriff diesbezüglich nicht verallgemeinerungsfähig schien, hatte Kronecker auch Grundsätzliches an der Arbeit Dedekinds auszusetzen: Zum einen hielt er Ideale als Mengen von unendlich vielen Elementen für allzu abstrakte und künstliche Gebilde, zum anderen konnte er sich mit der Dedekindschen Terminologie nicht anfreunden. Beide Kritikpunkte erscheinen aus heutiger Sicht unverständlich, sind doch die Dedekindschen Ideale inzwischen aus der modernen Algebra ebenso wenig wegzudenken wie viele der mittlerweile Standard gewordenen Dedekindschen Begriffsbestimmungen, beispielsweise des *Körpers* oder der *Ordnung*.[101]

Man könnte die Kummer-Festschrift sicherlich mit einigem Recht als Gegenentwurf zur Idealtheorie Dedekinds charakterisieren, und zwar in inhaltlich-methodischer wie in sprachlich-formaler Hinsicht. Was die Verständlichkeit der Sprache, die Wahl der Begriffe, die Übersichtlichkeit der Gedankenführung und die Klarheit der Beweise angeht, liegen Welten zwischen den Ausführungen Kroneckers und Dedekinds. Darauf soll an dieser Stelle nicht weiter eingegangen werden. Uns geht es hier vor allem um einen zentralen Begriff der Kroneckerschen Arbeit, den Begriff des „algebraischen Divisors“.

Kronecker verfolgte das Ziel, den Kummerschen Begriff der „idealen Zahl“ „aus der Sphäre blosser Abstraction in die Wirklichkeit algebraischer Gebilde zu versetzen“. Dedekinds Ansatz, eine „ideale Zahl“ mittelbar als Menge der von ihr geteilten wirklichen algebraischen Zahlen zu begreifen, modern ausgedrückt: eine „ideale Zahl“ $\mathfrak{a}$ mit der Menge $\overline{\mathfrak{a}} = \{\mu \text{ algebraische Zahl} : \mathfrak{a} \mid \mu\}$ gleichzusetzen, erschien Kronecker offenbar nicht konkret genug. Seine Idee bestand darin, eine „ideale Zahl“ als größten gemeinsamen Teiler von endlich vielen ganzalgebraischen Zahlen (bzw. ganzalgebraischen Funktionen) aufzufassen und für diesen größten gemeinsamen Teiler einen expliziten algebraischen Ausdruck zu finden. Dazu bediente er sich des Prinzips der „Association neuer Grössengebilde“, welches darauf hinauslief,

> [...] das Gebiet der algebraischen Grössen, welche den Ausgangspunkt bilden, genügend [*zu erweitern* ...], um den bei den ganzen Zahlen und bei den ganzen rationalen Funktionen von Variabeln[102] geltenden einfachen Gesetzen der Theilbarkeit, welche beim Uebergang zu den ganzen algebraischen Grössen modificirt werden, wiederum Raum zur vollen Wirksamkeit zu schaffen.[103]

Modern ausgedrückt: Kronecker bettete den zu untersuchenden algebraischen Erweiterungskörper durch Hinzunahme „neuer Grössengebilde“ in einen Oberkörper ein, in dem die „ganzen algebraischen Grössen“ bei geeigneter Definition eines Teilbarkeits- bzw. Ganzheitsbegriffes über einen

[101] Beide Begriffe werden von Kronecker als unpassend kritisiert. Vgl. *Kronecker 1882*, S. 250 (§ 1) und S. 255 (§ 3).
[102] Gemeint sind die ganzrationalen Zahlen $\mathbb{Z}$ sowie Polynome über $\mathbb{Z}$ in mehreren Unbestimmten.
[103] *Kronecker 1882*, S. 300 (§ 14).

größten gemeinsamen Teiler verfügten. Dabei sind die „neuen Grössengebilde“ genau so gewählt, daß sie in dem Oberkörper zu größten gemeinsamen Teilern gewisser „algebraischer Grössen“ oder — in Kroneckerscher Terminologie — zu „algebraischen Divisoren“ werden. Kroneckers „algebraische Divisoren“ sind ihrem Selbstverständnis zufolge also nichts anderes als unmittelbare Verkörperungen der Kummerschen „idealen Zahlen“.

Der Begriff des „algebraischen Divisors“ wird in den §§ 14 – 17 der Kummer-Festschrift eingeführt. Es ist nicht einfach, Ordnung in die Kroneckersche Gedankenführung zu bringen. Allzu schnell läuft man Gefahr, die Distanz und den Blick für das Ganze zu verlieren und sich von der Kroneckerschen Diktion gefangen nehmen zu lassen. Gerade an diesem Punkt kranken m. E. die meisten Darstellungen über Kroneckers Divisorentheorie. Dieser Problematik eingedenk, soll hier der Versuch unternommen werden, Kroneckers Vorgehen einerseits mit präzisen Begriffen zu beschreiben und nachvollziehbar zu machen, andererseits durch Einordnung in einen größeren Kontext die Kernidee der Kroneckerschen Divisorentheorie herauszuarbeiten. Was den letztgenannten Punkt angeht, wurden in den vorangegangenen Kapiteln bereits die entscheidenden Vorarbeiten geleistet.

Es ist nicht zu vermeiden, daß dabei Überschneidungen mit in der Literatur bereits vorhandenen Darstellungen der Kroneckerschen Divisorentheorie auftreten, insbesondere mit der Abhandlung „The Genesis of Ideal Theory“ von Edwards aus dem Jahre 1980. Dennoch lassen m. E. die zusätzlich gewonnenen Erkenntnisse eine erneute Darstellung rechtfertigen.

4.1. Zur algebraischen Ausgangssituation bei Kronecker

Entsprechend seinem Anliegen, eine Theorie der algebraischen Funktionenkörper zu entwikkeln, wählt Kronecker als Grundring D für seine Untersuchungen nicht, wie Dedekind, den Ring der ganzrationalen Zahlen $\mathbb{Z}$, sondern allgemeiner den Polynomring $\mathbb{Z}[Y]$, wobei $Y = \{Y_i\}_{i\in\mathbb{N}}$ eine beliebige Familie von Unbestimmten bezeichnet. Der Quotientenkörper von D, also der rationale Funktionenkörper $K = \mathbb{Q}(Y)$, heißt „natürlicher Rationalitätsbereich“[104], für den Fall, daß es sich bei $\{Y_i\}_{i\in\mathbb{N}}$ um die leere Familie handelt, also der natürliche Rationalitätsbereich gleich dem Körper $\mathbb{Q}$ der rationalen Zahlen ist, auch „absoluter Rationalitätsbereich“[105]. Über diesem Körper K betrachtet Kronecker nunmehr beliebige algebraische Körpererweiterungen L/K. Ist L/K endlich, so spricht Kronecker auch von einem sogenannten „(natürlichen) Gattungsbereich“ L. Insgesamt fällt dem Körper K für alle weiteren Überlegungen die Rolle des Grundkörpers oder auch „Stammbereiches“ zu.[106]

An vielen Stellen der Festschrift werden „algebraische Grössen“ einer bestimmten „Gattung“ untersucht. Dabei handelt es sich um die Menge all jener Elemente eines „Gattungsbereichs“ L mit $[L : K] = s$, deren Minimalpolynom denselben Grad s hat, also die Menge aller primitiven Elemente $\alpha \in L$ mit $L = K(\alpha)$. Warum diese Elemente gegenüber den anderen Körperelementen ausgezeichnet werden, ist zunächst nicht ganz einsichtig, und Dedekind bemerkt in seinen „Bunten Bemerkungen“ treffend, daß der Begriff der „Gattung“ von „weit geringerer Wichtigkeit und Brauchbarkeit als der des Gattungsbereiches“ sei.[107] Die Forderung, bestimmte ganze algebraische Größen $\alpha_1, \ldots, \alpha_m$ müßten derselben „Gattung“ angehören, steht m. E. in engem Zusammenhang mit Kroneckers Normbegriff sowie seinem Bemühen, sich nicht von vornherein auf eine bestimmte Körpererweiterung L/K festzulegen.

[104] *Kronecker 1882*, S. 255 (§ 3).
[105] *Kronecker 1882*, S. 254 (§ 3).
[106] *Kronecker 1882*, S. 252 (§ 2).
[107] *Edwards et al. 1982*, S. 55, Bemerkung Dedekinds Nr. 3.

Da die Körpererweiterung L/K unter den Kroneckerschen Voraussetzungen stets separabel ist, läßt sich im Falle $[L : K] = s < \infty$ die Norm eines $\alpha \in L$ bzgl. L/K auch schreiben als $N_{L/K}(\alpha) = \sigma_1(\alpha) \cdot \ldots \cdot \sigma_s(\alpha)$, wobei σ_i sämtliche K-Konjugationshomomorphismen von L in den algebraischen Abschluß von K durchläuft. Einige der $\sigma_i(\alpha)$ werden i. a. übereinstimmen, also dieselben Konjugierten von α bezeichnen. Nun möchte Kronecker die Norm eines Elementes $\alpha \in L$ in besonders einfacher Weise als das Produkt seiner Konjugierten definieren. Diese Defintion ist jedoch nur dann richtig, wenn unter der Norm die Relativnorm bzgl. der endlichen Körpererweiterung $K(\alpha)/K$ verstanden wird. Kronecker muß also sicherstellen, daß jedesmal dann, wenn er die Normen verschiedener Elemente betrachtet, diese Normen miteinander kompatibel sind, also in dem oben beschriebenen Sinne dieselben Relativnormen bezeichnen. Für die Norm der Elemente $\alpha_1, \ldots, \alpha_m \in L$ wird dies durch die Forderung nach Zugehörigkeit zu derselben Gattung erreicht, denn dann gilt offensichtlich $K(\alpha_1) = \ldots = K(\alpha_m)$.

Aus heutiger Sicht empfiehlt es sich, auf diese zusätzliche Bedingung zu verzichten und stattdessen $\alpha_1, \ldots, \alpha_m \in L$ — wie auch immer der Grad der Körpererweiterung L/K ausfallen mag — als Elemente der endlichen Erweiterung $K(\alpha_1, \ldots, \alpha_m)/K$ aufzufassen und unter der Norm von α_i stets die Relativnorm bzgl. dieser Körpererweiterung zu verstehen. Jedenfalls behalten bei dieser Lesart die Kroneckerschen Überlegungen in vollem Umfang ihre Gültigkeit, und man vermeidet, sich frühzeitig auf eine bestimmte endliche Körpererweiterung L/K festlegen zu müssen.[108]

Bezeichnet L irgendeinen algebraischen Erweiterungskörper, so erhalten die Elemente von L das Attribut „algebraisch“, wohingegen die Elemente des Grundkörpers K als „rational“ gekennzeichnet werden.[109] Eine „rationale Grösse“, also ein Element des Grundkörpers („Stammbereichs“) $K = \mathbb{Q}(Y)$, heißt „ganz“, wenn es sich um ein Element des Grundringes D handelt. Eine „algebraische Grösse“, also ein Element aus dem Erweiterungskörper L, heißt „ganz“, wenn es einem normierten Polynom mit ganzen rationalen Koeffizienten, also Koeffizienten aus D genügt.[110]

Einen Ring, der aus dem Grundring D durch Adjunktion endlich vieler algebraischer Größen entsteht, also eine Ordnung im Dedekindschen Sinne, nennt Kronecker „Art-Bereich“, den Ring aller ganzen algebraischen Größen in einem „Gattungsbereich“ L, also den ganzen Abschluß von D in einer endlichen Körpererweiterung L/K, auch „Haupt-Art-Bereich“.[111]

Damit wäre die algebraische Ausgangssituation bei Kronecker in ihren wesentlichen Punkten umrissen. Daß der Körper der rationalen Funktionen über $\mathbb{Q}$ als *natürlich* charakterisiert wird, erklärt sich daraus, daß die ganzen rationalen Größen dieses Körpers, also die Polynome aus $\mathbb{Z}[Y]$, weitgehend denselben arithmetischen Eigenschaften genügen wie die ganzrationalen Zahlen $\mathbb{Z}$. Dabei mag man zuallererst an die Existenz einer eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ sowie $\mathbb{Z}[Y]$ denken, und in der Tat lassen sich die Kroneckerschen Ausführungen für den Fall eines faktoriellen Grundringes D mühelos verallgemeinern. Dennoch arbeitet Kronecker ganz bewußt über Grundringen der Gestalt $\mathbb{Z}[Y]$, denn die bloße *formale* Existenz eine Primzerlegung war für ihn ohne jeglichen Wert. Entscheidend ist das Vorhandensein eines Zerlegungsalgorithmus'.

---

[108] Zum Problem des Normbegriffs bei Kronecker vgl. auch *Edwards et al. 1982*, S. 60, Bemerkung Dedekinds Nr. 22, sowie S. 70, Kommentar Nr. 22 (falsche Zählung).

[109] Vgl. *Kronecker 1882*, S. 254f. (§ 3). Entsprechend ist in der Kummer-Festschrift von „rationalen/algebraischen Grössen“ oder auch „rationalen/algebraischen Functionen“, im Falle algebraischer Zahlkörper (also $D = \mathbb{Z}$ und $K = \mathbb{Q}$) von „rationalen/algebraischen Zahlen“ die Rede.

[110] *Kronecker 1882*, S. 260f. (§ 5). Dieser Ganzheitsbegriff entspricht dem Dedekindschen und damit dem heute üblichen.

[111] *Kronecker 1882*, S. 262 (§ 5). Kronecker bezeichnet die Menge derjenigen Elemente eines Art-Bereiches, die derselben Gattung angehören, deren Minimalpolynom also denselben Grad hat, als „Art“ oder „Species“. Für die „Art“ bzw. „Species“ gilt das über den Begriff der Gattung Gesagte in gleicher Weise.

> Die [...] Definition der Irreductibilität entbehrt so lange einer sicheren Grundlage, als nicht eine Methode angegeben ist, mittels deren bei einer bestimmten, vorgelegten Function entschieden werden kann, ob dieselbe der aufgestellten Definition gemäß irreductibel ist oder nicht.[112]

Kronecker wies nach, daß eine solche „Methode“ für Polynomringe der Gestalt $\mathbb{Z}[Y]$ tatsächlich existiert, und zeigte, wie diese „Methode“ auch für die Zerlegung in Polynomringen über endlichen Erweiterungskörpern von $K = \mathbb{Q}(Y)$ angewendet werden kann.[113] Man darf davon ausgehen, daß Kronecker vor allem in diesem Sinne die oben geschilderte algebraische Situation als eine *natürliche* empfand.[114]

4.2. Kroneckers Divisor- und Teilbarkeitsbegriff

Seien $\alpha_1, \ldots, \alpha_m$ Elemente aus dem ganzen Abschluß T igendeiner nicht näher fixierten algebraischen Körpererweiterung L/K, also algebraische Größen, die einer Ganzheitsgleichung über dem Grundring $D = \mathbb{Z}[Y]$ genügen. Für diese ganzen Größen definiert Kronecker nunmehr einen zugehörigen „algebraischen Modul oder Divisor“.[115] Dazu seien $X = \{X_i\}_{i\in\mathbb{N}}$ eine abzählbar unendliche Familie von Unbestimmten und f ein Polynom mit den Koeffizienten $\alpha_1, \ldots, \alpha_m \in D$ in den Unbestimmten $X_{i_1}, \ldots, X_{i_s}$.[116] Ferner bezeichne K_f jenen Körper, der aus dem Grundkörper K durch Adjunktion der Koeffizienten von f entsteht, also den Körper $K(\alpha_1, \ldots, \alpha_m)$. Die Norm von f bzgl. der endlichen Körpererweiterung $K_f(X)/K(X)$ ist ein Polynom über D in den Unbestimmten $X_{i_1}, \ldots, X_{i_s}$.[117] Da D ein faktorieller Ring, also insbesondere ein ggT-Bereich ist, kann man dieses Polynom durch einen größten gemeinsamen Teiler $\gamma \in D$ seiner Koeffizienten dividieren und erhält dann ein Polynom mit teilerfremden Koeffizienten, eine sogenannte zu f gehörige *primitive Form*, geschrieben $F_{K_f/K}(f)$.[118] Bildet man in dem Körper der rationalen Funktionen $L(X)$ den Quotienten von f mit einer zu f gehörigen primitven Form $F_{K_f/K}(f)$, so erhält man schließlich das, was Kronecker einen zu $\alpha_1, \ldots, \alpha_m$ gehörigen „algebraischen Divisor“ nennt.

Definition 4.1. *Es seien $\alpha_1, \ldots, \alpha_m$ Elemente aus dem ganzen Abschluß T von D in der algebraischen Körpererweiterung L/K, $X^{(1)}, \ldots, X^{(m)}$ paarweise verschiedene Potenzprodukte von Unbestimmten aus $X = \{X_i\}_{i\in\mathbb{N}}$ und f das aus ihnen gebildete Polynom $\alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)} \in T[X]$. Ferner bezeichne K_f den Körper $K(\alpha_1, \ldots, \alpha_m) \subseteq L$. Dann heißt bei Kronecker ein gebrochen rationaler Ausdruck der Gestalt*

$$\operatorname{div}[f] := \frac{\alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)}}{F_{K_f/K}\left(\alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)}\right)} \tag{4.2}$$

[112] *Kronecker 1882*, S. 256f. (§ 4).

[113] Vgl. *Kronecker 1882*, S. 256ff. (§ 4). Eine moderne, gut verständliche Darstellung der Kroneckerschen Zerlegungsalgorithmen findet sich bei *Edwards 1984*, §§ 55–61.

[114] Vgl. hierzu auch *Edwards 1990*, § 1.2. Edwards versucht, die Kroneckersche Ausgangssituation dahingehend zu verallgemeinern, daß er als Grundringe D sogenannte *natürliche Integritätsbereiche* („*natural rings*“) betrachtet. Diese sind nichts anderes als faktorielle Integritätsbereiche, in denen es einen Algorithmus gibt, mit dessen Hilfe für jedes Polynom in endlich vielen Schritten eine Zerlegung in irreduzible Faktoren bestimmt werden kann. Es handelt sich demnach um die allgemeinsten Ringe, die noch den Kroneckerschen Konstruierbarkeitsanforderungen genügen.

[115] *Kronecker 1882*, S. 302 (§ 15), Definition IV.

[116] Bei *Kronecker 1882*, S. 302 (§ 15), Definition I: „ganze algebraische Form“.

[117] Bei *Kronecker 1882*, S. 302 (§ 15), Definition I: „ganze rationale Form“.

[118] Bei *Kronecker 1882*, S. 303 (§ 15), Definition IV: „primitive Form, deren abgeleitete die Norm der algebraischen Form“ f ist. Kronecker verzichtet auf die Angabe der Körpererweiterung im Index. Für die hier gewählte Schreibweise gilt das in Anmerkung 58, S. 29, über die Norm Gesagte in gleicher Weise.

ein zu $\alpha_1, \ldots, \alpha_m$ bzw. f gehöriger ***„algebraischer Divisor“***.[119] *Ist $f = \alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)}$ ein lineares Polynom, sind also $X^{(1)}, \ldots, X^{(m)}$ einfache Unbestimmte (und keine Potenzprodukte von Unbestimmten), so spricht Kronecker von einem aus einer „Linearform gebildeten Divisor“, im folgenden auch* ***linearer algebraischer Divisor*** *genannt.*

Seinen eigentlichen Sinn erhält der Begriff des algebraischen Divisors erst mit der Definition einer Teilbarkeitsrelation. Denn dann wird ein algebraischer Divisor zu dem, was sein Name verheißt: zu einem *Teiler*. Es wird sich zeigen, daß algebraische Divisoren nichts anderes als Vertreter von bestimmten Teilbarkeitsklassen sind und Divisoren, die aus denselben Elementen $\alpha_1, \ldots, \alpha_m$ gebildet werden, dieselbe Teilbarkeitsklasse repräsentieren.[120] Im Grunde ist der Teilbarkeitsbegriff das eigentliche Herzstück der Kroneckerschen Divisorentheorie, und erst ein richtiges Verständnis dessen, was die Teilbarkeit von Divisoren bedeutet, ermöglicht ein tieferes Verständnis des kunstvollen Kroneckerschen Divisorbegriffs. Gerade in diesem Punkt läßt jedoch die Kroneckersche Darstellung die nötige Klarheit vermissen.

Im folgenden bezeichne T stets den ganzen Abschluß von D in L/K und K_f, wie gehabt, jenen Unterkörper von L, der aus dem Grundkörper K durch Adjunktion der Koeffizienten eines Polynoms $f \in T[X]$ entsteht. Durch einen algebraischen Divisor $\mathrm{div}[f]$ der Gestalt (4.2) zu teilen, heißt bei Kronecker grundsätzlich, eine entsprechende Division in dem Körper der rationalen Funktionen $L(X)$ auszuführen. Den algebraischen Divisor $\mathrm{div}[f]$ durch den algebraischen Divisor $\mathrm{div}[g]$ zu teilen, hieße demzufolge, in $L(X)$ den Quotienten

$$\frac{\mathrm{div}[f]}{\mathrm{div}[g]} = \frac{f \cdot F_{K_g/K}(g)}{F_{K_f/K}(f) \cdot g} \in L(X) \tag{4.3}$$

zu bilden. Ausgehend von einen natürlichen Teilbarkeitsverständnis, müßte man $\mathrm{div}[g]$ durch den Divisor $\mathrm{div}[f]$ teilbar nennen, wenn der gebildete Quotient *ganz* ist. Doch was soll *Ganzheit* in diesem Fall bedeuten? Etwa, daß die rationale Funktion (4.3) ein Polynom mit ganzalgebraischen Koeffizienten ist? Ein solcher naiver Ganzheitsbegriff würde den grundlegenden Charakter der Kroneckerschen Divisoren, insbesondere die entscheidende Rolle der primitiven Formen verkennen, und das ganze kunstvolle Gebäude der Kroneckerschen Theorie, auch wenn es auf den ersten Blick nicht den Anschein hat, wie ein Kartenhaus zum Einsturz bringen. Schon besser und der Begriffsbildung angemessener wäre folgender Vorschlag: Der Quotient (4.3) heiße *ganz*, wenn er wieder die Gestalt eines algebraischen Divisors im Sinne von Definition 4.1 hat. Es stellt sich jedoch heraus, daß auch dieser Ganzheitsbegriff den Kroneckerschen Divisoren nicht gerecht wird.

Definition 4.4. *Für die aus $f, g \in T[X]$ gebildeten algebraischen Divisoren* $\mathrm{div}[f]$ *und* $\mathrm{div}[g]$ *wird die Teilbarkeit in folgender Weise erklärt:*[121]

$$\mathrm{div}[g] \mid \mathrm{div}[f] \quad :\Leftrightarrow \quad f \cdot \frac{F_{K_g/K}(g)}{g} \in T[X].$$

Ist $\mathrm{div}[f]$ *durch* $\mathrm{div}[g]$ *und* $\mathrm{div}[g]$ *durch* $\mathrm{div}[f]$ *in diesem Sinne teilbar, können also die algebraischen Divisoren* $\mathrm{div}[f]$ *und* $\mathrm{div}[g]$ *hinsichtlich ihrer Teilbarkeitseigenschaften als im wesentlichen gleich angesehen werden, so heißen sie nach Kronecker* ***„absolut äquivalent“****, in Zeichen* $\mathrm{div}[f] \sim \mathrm{div}[g]$.[122]

[119] Man sieht, daß in dieser Definition den Elementen $\alpha_1, \ldots, \alpha_m$ zunächst unendlich viele algebraische Divisoren zugeordnet sind, da die Wahl der Potenzprodukte $X^{(1)}, \ldots, X^{(m)}$ keinerlei Beschränkungen unterliegt. Gleiches gilt auch für einen algebraischen Divisor, der dem Polynom f zugeordnet ist, und zwar insofern, als die primitive Form $F_{K_f/K}(f)$ nur bis auf Multiplikation mit Einheiten aus D eindeutig bestimmt ist.

[120] Kronecker deutet dies an, indem er sagt, der Quotient (4.2) „repräsentiere“ einen algebraischen Divisor (*Kronecker 1882*, S. 303 (§ 15), Definition IV).

[121] *Kronecker 1882*, S. 304 (§ 15), Definition VII.

[122] *Kronecker 1882*, S. 304 (§ 15), Definition VIII.

Dieser Teilbarkeitsbegriff erscheint auf den ersten Blick wenig plausibel. Wieso beispielsweise läßt Kronecker das primitive Nennerpolynom $F_{K_f/K}(f)$ von $\operatorname{div}[f]$ bei der Quotientenbildung einfach unter den Tisch fallen? Man ahnt, daß gerade darin der besondere Clou der Kroneckerschen Teilbarkeitstheorie liegt, den primitiven Polynomen also offenbar eine ganz besondere Rolle zukommt. Im Zusammenhang mit dem folgenden Satz, den Kronecker auch als „Fundamentaltheorem" bezeichnet, erschließt sich die eigentliche Bedeutung des Kroneckerschen Teilbarkeitsbegriffes.[123] Bevor wir ihn formulieren, dehnen wir jedoch den Begriff der Primitivität auf Polynome mit Koeffizienten aus T aus.

Definition 4.5. *Seien $q \in T[X]$ und K_q jener Unterkörper von L, der aus dem Grundkörper K durch Adjunktion der Koeffizienten von q entsteht. Dann heißt das Polynom q* ***im Kroneckerschen Sinne primitiv****, wenn die Norm $N_{K_q/K}(q)$ ein Polynom mit in D teilerfremden Koeffizienten ist.*[124] *Für die Menge aller im Kroneckerschen Sinne primitiven Polynome aus $T[X]$ schreiben wir im folgenden auch $N(T)$.*

Satz 4.6. *(„1. Fundamentaltheorem") Sind $f, g \in T[X]$ zwei beliebige Polynome mit ganzalgebraischen Koeffizienten und $q \in T[X]$ ein im Kroneckerschen Sinne primitives Polynom, so gilt*

$$\operatorname{div}[g] \mid \operatorname{div}[f] \quad \Leftrightarrow \quad \operatorname{div}[g] \mid \operatorname{div}[fq].$$

Beweis: Bezeichnet K_g jenen Körper, der aus K durch Adjunktion der Koeffizienten von g entsteht, so lautet die Aussage des Satzes in äquivalenter Formulierung

$$f \cdot \frac{F_{K_g/K}(g)}{g} \in T[X] \quad \Leftrightarrow \quad fq \cdot \frac{F_{K_g/K}(g)}{g} \in T[X].$$

Die Implikation „$\Rightarrow$" ist klar (und wird bei Kronecker auch gar nicht erwähnt). Für den Beweis der Richtung „$\Leftarrow$" unterscheidet Kronecker zwei Fälle.

1. Fall: $g \in T$. Dann ist jede zu g gehörige primitive Form bzgl. der Erweiterung $K_g(X)/K(X)$ assoziiert zu 1. Man kann o. E. d. A. also $F_{K_g/K}(g) = 1$ annehmen. Es sei $h := fq \cdot \frac{1}{g} \in T[X]$, also $fq = hg$. Ist Z eine weitere (von allen bisherigen Unbestimmten $X_i \in X$, $Y_j \in Y$ unabhängige) Unbestimmte, so erhält man

$$gq \cdot Z - fq = gq \cdot Z - hg, \quad \text{also} \quad q(g \cdot Z - f) = g(q \cdot Z - h).$$

Bezeichnet man mit K' jenen Körper, der aus K durch Adjunktion der Koeffizienten von f, g und q entsteht, und geht auf beiden Seiten der Gleichung zur Norm bzgl. der Körpererweiterung $K'(X, Z)/K(X, Z)$ über, dann folgt hieraus

$$N_{K'/K}(g) \mid N_{K'/K}(q) \cdot N_{K'/K}(g \cdot Z - f) \quad \text{in } D[X].$$

$N_{K'/K}(q)$ ist nach Voraussetzung ein primitives Polynom von $D[X]$. Also ist auch jedes irreduzible Polynom, das in der Zerlegung von $N_{K'/K}(q)$ auftritt, primitiv, so daß $N_{K'/K}(g) \in D$ in $D[X]$ kein echter Teiler von $N_{K'/K}(q)$ sein kann. Also ist $N_{K'/K}(g \cdot Z - f)$ in $D[X]$ durch $N_{K'/K}(g)$ teilbar, d. h.

$$\frac{N_{K'/K}(g \cdot Z - f)}{N_{K'/K}(g)} = N_{K'/K}\Big(Z - \frac{f}{g}\Big) \in D[X, Z].$$

[123] *Kronecker 1882*, S. 305 (§ 15), Satz IX.

[124] Bezeichnet K' irgendeine endliche Erweiterung von K, die sämtliche Koeffizienten von q enthält, d. h. eine endliche Erweiterung von K mit $K_q \subseteq K' \subseteq L$, so gilt aufgrund der Normschachtelungsformel $N_{K'/K}(q) = N_{K_q/K}(q)^{[K':K_q]}$. Bedenkt man, daß das Produkt von Polynomen aus $D[X]$ genau dann teilerfremde Koeffizienten in D hat, wenn dasselbe für jeden Polynomfaktor gilt (Folgerung aus Satz 2.13, S. 20), so ist demzufolge ein Polynom $q \in T[X]$ genau dann im Kroneckerschen Sinne primitiv, wenn das Polynom $N_{K'/K}(q) \in D[X]$ teilerfremde Koeffizienten besitzt. Es spielt also keine Rolle, bzgl. welcher Norm die Primitivität eines Polynoms $q \in T[X]$ festgestellt wird. Außerdem zeigt sich, daß jedes in $D[X]$ primitive Polynom, aufgefaßt als Polynom von $T[X]$, auch primitiv im erweiterten Kroneckerschen Sinne ist, also der neue Primitivitätsbegriff mit dem bisherigen verträglich ist.

$\frac{f}{g}$ ist daher Nullstelle eines normierten Polynoms mit Koeffizienten aus $D[X]$, also ganz über $D[X]$. An dieser Stelle folgert Kronecker nun richtigerweise $\frac{f}{g} \in T[X]$, d. h. er benutzt den Satz, daß $T[X]$ der ganze Abschluß von $D[X]$ in $L(X)$ ist. Diese, auch für andere Beweise Kroneckers unverzichtbare Aussage wird allerdings an keiner Stelle der Arbeit explizit bewiesen.[125]

2. Fall: $g \in T[X]$. Dieser Fall wird auf den ersten zurückgeführt. Sei $h := fq \cdot \frac{1}{g} F_{K_g/K}(g)$, also

$$\left(f \cdot \frac{N_{K_g/K}(g)}{g}\right) \cdot q = h \cdot \frac{N_{K_g/K}(g)}{F_{K_g/K}(g)}.$$

Wegen $f \cdot \frac{1}{g} N_{K_g/K}(g) \in T[X]$ und wegen $N_{K_g/K}(g) \cdot F_{K_g/K}(g)^{-1} \in D \subseteq T$ folgt daraus mit Fall 1

$$f \cdot \frac{N_{K_g/K}(g)}{g} \cdot \frac{F_{K_g/K}(g)}{N_{K_g/K}(g)} = f \cdot \frac{F_{K_g/K}(g)}{g} \in T[X], \quad \text{also} \quad \text{div}[g] \mid \text{div}[f]. \qquad \square$$

Mit Hilfe von Satz 4.6 ist es nunmehr möglich, der Teilbarkeitsdefinition 4.4 eine etwas plastischere Gestalt zu geben. Als erstes halten wir fest

Lemma 4.7. *Die Menge der im Kroneckerschen Sinne primitiven Polynome von $T[X]$, also $N(T) = \{f \in T[X] : N_{K_f/K}(f)$ hat teilerfremde Koeffizienten in $D\}$, ist multiplikativ abgeschlossen.*

Beweis: Seien $f, g \in N(T)$, und es bezeichne K' einen endlichen Erweiterungskörper von K, der die Koeffizienten von f und g enthält. Aufgrund der Normschachtelungsformel sind mit $N_{K_f/K}(f)$ und $N_{K_g/K}(g)$ auch $N_{K'/K}(f)$ und $N_{K'/K}(g)$ Polynome mit teilerfremden Koeffizienten in D (vgl. Anmerkung 124). Die Multiplikativität der Norm ergibt $N_{K'/K}(f) \cdot N_{K'/K}(g) = N_{K'/K}(fg)$, also ein Polynom in $D[X]$, dessen Koeffizienten ebenfalls teilerfremd sein müssen. Dann ist aber auch $N_{K_{fg}/K}(fg)$ ein primitives Polynom in $D[X]$, woraus schließlich $fg \in N(T)$ folgt. $\square$

Lemma 4.7 erlaubt es, den Quotientenring $T[X]_{N(T)}$ von $T[X]$ nach den primitiven Polynomen $N(T)$ zu bilden. Sind $\text{div}[f]$ und $\text{div}[g]$ zwei algebraische Divisoren im Sinne von Definition 4.1, so gilt einerseits

$$\text{div}[g] \mid \text{div}[f] \quad \Rightarrow \quad \frac{f}{g} F_{K_g/K}(g) \in T[X] \quad \Rightarrow \quad \frac{f}{g} \in T[X]_{N(T)}.$$

Andererseits erhält man

$$\begin{aligned} \frac{f}{g} \in T[X]_{N(T)} \quad &\Rightarrow \quad \frac{f}{g} = \frac{h}{q} \quad \text{mit } h \in T[X] \text{ und } q \in N(T) \\ &\Rightarrow \quad fq \cdot \frac{F_{K_g/K}(g)}{g} = h \cdot F_{K_g/K}(g) \in T[X], \end{aligned}$$

also $\text{div}[g] \mid \text{div}[f \cdot q]$, woraus mit dem Kroneckerschen „Fundamentaltheorem“ $\text{div}[g] \mid \text{div}[f]$ folgt. Damit können wir Kroneckers Teilbarkeitsbegriff folgende alternative Fassung geben.

Satz 4.8. *Bezeichnen f und g zwei beliebige Polynome aus $T[X]$, so gilt*

$$\text{div}[f] \mid \text{div}[g] \quad \Leftrightarrow \quad \frac{f}{g} \in T[X]_{N(T)} \quad \Leftrightarrow \quad \frac{\text{div}[f]}{\text{div}[g]} \in T[X]_{N(T)}.$$

Formuliert man die Teilbarkeit von Divisoren in dieser Form, so ist unmittelbar ersichtlich, wann der Quotient zweier algebraischer Divisoren sinnvollerweise *ganz* heißt, nämlich dann, wenn er sich als Quotient eines Polynoms aus $T[X]$ und eines primitiven Polynoms aus $D[X]$ schreiben läßt. Darüber hinaus sind zwei algebraische Divisoren $\text{div}[f]$ und $\text{div}[g]$ genau dann im Kroneckerschen Sinne „absolut äquivalent“, also bzgl. ihrer Teilbarkeitseigenschaften als im wesentlichen

[125] Vgl. hierzu Anmerkung 132, S. 54, im folgenden Abschnitt.

gleich anzusehen, wenn sowohl der Quotient $\frac{\text{div}[g]}{\text{div}[f]}$ als auch der Quotient $\frac{\text{div}[f]}{\text{div}[g]}$ in $T[X]_{N(T)}$ enthalten sind. Dies wiederum bedeutet nichts anderes, als daß die Polynome f und g in $T[X]_{N(T)}$ zueinander assoziiert sind, sich also lediglich um eine Einheit aus $T[X]_{N(T)}$ unterscheiden. Und schließlich ist ein algebraischer Divisor genau dann *irreduzibel*, wenn er als Element des Quotientenringes $T[X]_{N(T)}$ irreduzibel im üblichen Sinne ist.

Auch die Kroneckersche Bemerkung, daß das „Fundamentaltheorem“ 4.6 den „Einheitscharakter der primitiven Formen“ beweise,[126] erscheint nunmehr in klarerem Licht. Denn offensichtlich ist jeder aus einem im Kroneckerschen Sinne primitiven Polynom $q \in T[X]$ gebildete algebraische Divisor $\text{div}[q]$ eine Einheit in $T[X]_{N(T)}$, d. h. bei den aus primitiven Polynomen gebildeten Divisoren handelt es sich genau um jene algebraischen Divisoren, die absolut äquivalent zur 1 (genauer: zu $\text{div}[1]$) sind. Mit anderen Worten: Die Divisoren $\text{div}[f]$ und $\text{div}[fq]$ sind für alle primitiven $q \in T[X]$ absolut äquivalent, also im Hinblick auf ihre Teilbarkeitseigenschaften im wesentlichen gleich.

Aus all diesen Überlegungen ergibt sich schließlich, daß der Begriff der „absoluten Äquivalenz“ auf der Menge aller algebraischen Divisoren eine Äquivalenzrelation liefert.[127] Reflexivität und Symmetrie der Relation „$\sim$“ sind klar. Für die Transitivität betrachte man die drei algebraischen Divisoren $\text{div}[f]$, $\text{div}[g]$ und $\text{div}[h]$. Dann gilt aufgrund von Satz 4.8

$$\begin{aligned} & \text{div}[f] \sim \text{div}[g] \quad \text{und} \quad \text{div}[g] \sim \text{div}[h] \\ \Rightarrow \quad & \frac{f}{g}, \frac{g}{f} \quad \text{und} \quad \frac{g}{h}, \frac{h}{g} \in T[X]_{N(T)} \\ \Rightarrow \quad & \frac{f}{h} = \frac{f}{g} \cdot \frac{g}{h} \quad \text{und} \quad \frac{h}{f} = \frac{h}{g} \cdot \frac{g}{f} \in T_{N(T)} \\ \Rightarrow \quad & \text{div}[f] \sim \text{div}[h]. \end{aligned}$$

Auf der Menge der absoluten Äquivalenzklassen ist nun in natürlicher Weise, nämlich vermöge

$$\text{div}[f] \cdot \text{div}[g] \sim \text{div}[f \cdot g] \quad \text{für alle } f, g \in T[X]$$

eine Multiplikation definiert. Bzgl. dieser Multiplikation bilden die Klassen absolut äquivalenter algebraischer Divisoren eine abelsche Halbgruppe, deren Einselement durch die Klasse der im Kroneckerschen Sinne primitiven Divisoren gegeben ist. Übersetzt man jede Teilbarkeitsrelation zwischen algebraischen Divisoren, also gewissen Elementen aus dem Funktionenkörper $L(X)$, in eine entsprechende Teilbarkeitsrelation der zugehörigen absoluten Äquivalenzklassen, so werden viele der Kroneckerschen Überlegungen transparenter.

Durch eine leichte Modifizierung des Kroneckerschen Divisorbegriffs läßt sich die Situation allerdings noch stärker vereinfachen. Die Kroneckersche Definition eines algebraischen Divisors hat aus heutiger Sicht den Nachteil, daß sie zwar auf der Menge der absoluten Äquivalenzklassen, nicht jedoch auf der Divisorenmenge selbst die Einführung einer algebraischen Struktur, sprich: Multiplikation, erlaubt. Die Schwierigkeiten beginnen bereits bei der Produktbildung. Sind f und g zwei Polynome aus $T[X]$, so werden die zugehörigen Unterkörper K_f und K_g von L i. a. verschieden sein. Damit ist jedoch die zu fg gehörige primitive Form $F_{K_{fg}/K}(fg)$ i. a. auch nicht das Produkt der zu f und g gehörigen primitiven Formen $F_{K_f/K}(f)$ und $F_{K_g/K}(g)$, d. h.

$$\text{div}[f] \cdot \text{div}[g] = \frac{f}{F_{K_f/K}(f)} \cdot \frac{g}{F_{K_g/K}(g)} \overset{\text{i. a.}}{\neq} \frac{fg}{F_{K_{fg}/K}(fg)} = \text{div}[fg].$$

Immerhin ließe sich dieses Problem vermeiden, wenn man die Wahl von f und g entsprechend der Kroneckerschen Grundannahme auf jene Polynome aus $T[X]$ einschränkt, deren Koeffizienten

[126] *Kronecker 1882*, S. 304 (§ 15).

[127] Dedekind moniert in seinen „Bunten Bemerkungen“, daß Kronecker die Transitivität der absoluten Äquivalenz nicht bewiesen habe (*Edwards et al. 1982*, S. 60f., Bemerkungen Dedekinds Nr. 24 und Nr. 26).

derselben „Gattung“ angehören, deren Koeffizienten über K also alle denselben Körper K' erzeugen. Aber selbst dann bleibt das Problem, daß der Quotient zweier algebraischer Divisoren, von denen der eine durch den anderen teilbar ist, i. a. *kein* algebraischer Divisor im Kroneckerschen Sinne mehr ist, d. h. nicht mehr die verlangte Gestalt (4.2) hat.

Dieser Nachteil des Kroneckerschen Divisor– und Teilbarkeitsbegriffes wird zwar durch den Übergang zu den absoluten Äquivalenzklassen einigermaßen behoben. Die Kroneckersche Theorie erscheint dadurch jedoch aus heutiger Sicht insgesamt unübersichtlich und umständlich. Es empfiehlt sich, eine leichte, aber entscheidende Modifizierung der Begriffe vorzunehmen, und zwar in jener Weise, wie sie durch Satz 4.8 sowie die anschließenden Bemerkungen nahegelegt wird. Dazu folgende Überlegung:

Wir hatten gesehen, daß zwei algebraische Divisoren genau dann im Kroneckerschen Sinne absolut äquivalent sind, wenn sie derselben Assoziiertheitsklasse von $T[X]_{N(T)}$ angehören. Kroneckers Teilbarkeitsbegriff macht somit algebraische Divisoren zu bestimmten Repräsentanten von Assoziiertheitsklassen.

Die Modifizierung des Kroneckerschen Divisorbegriffs besteht nun darin, den algebraischen Divisor $\mathrm{div}[f]$ hinsichtlich seiner Teilbarkeitseigenschaften nicht nur den absolut äquivalenten Divisoren, sondern *allen* Elementen seiner Assoziiertheitsklasse aus $T[X]_{N(T)}$ gleichzustellen. Mit anderen Worten: Wir fassen auch jene Elemente von $T[X]_{N(T)}$ als „algebraische Divisoren“ auf, die nicht die von Kronecker verlangte Gestalt (4.2) haben. Dies hat den entscheidenden Vorteil, daß die Menge aller algebraischen Divisoren mit dem Quotientenring $T[X]_{N(T)}$ übereinstimmt und somit in natürlicher Weise ein Teilbarkeits– bzw. Ganzheitsbegriff gegeben ist. Man sieht sofort, daß dann die Halbgruppe der Assoziiertheitsklassen von $T[X]_{N(T)}$ zu der Halbgruppe der Klassen absolut äquivalenter Divisoren isomorph ist; denn jeder Divisor im modifizierten Sinne ist natürlich assoziiert zu einem algebraischen Divisor im herkömmlichen, d. h. Kroneckerschen Sinne.

Man darf also jede Teilbarkeitsrelation zwischen algebraischen Divisoren, die bei Kronecker auftritt, ruhigen Gewissens als Teilbarkeitsrelation in dem Ring $T[X]_{N(T)}$ auffassen. Genau diese Lesart des Kroneckerschen Teilbarkeits– und Divisorbegriffs werden wir jedenfalls in den folgenden Abschnitten dieses Kapitels zugrunde legen. Dementsprechend bezeichne „$\sim$“ im folgenden stets die Assoziiertheitsrelation und „ $\mid$ “ stets die Teilbarkeitsrelation in dem Quotientenring $T[X]_{N(T)}$. Sprechen wir von Polynomen aus $T[X]$, so sollen diese stets als Elemente des Quotientenrings $T[X]_{N(T)}$ aufgefaßt werden.

4.3. „Algebraische Divisoren“ als größte gemeinsame Teiler von „algebraischen Grössen“

Vor dem Hintergrund der Ergebnisse des vorangegangenen Abschnitts erscheinen die §§ 14 – 17 der Kummer-Festschrift insgesamt in einem völlig neuen Licht. Denn hinter den Ausführungen Kroneckers verbirgt sich im Grunde nicht mehr und nicht weniger als der Beweis des folgenden grundlegenden Satzes.

Hauptsatz 4.9. *Der Quotientenring $T[X]_{N(T)}$ von $T[X]$ nach den im Kroneckerschen Sinne primitiven Polynomen $N(T)$ ist ein Bezout-Bereich.*[128] *Bezeichnen $\frac{f_1}{q_1}, \ldots, \frac{f_m}{q_m}$ Elemente aus $T[X]_{N(T)}$, $f_i \in T[X]$, $q_i \in N(T)$, und $X_{i_1}, \ldots, X_{i_m}$ Unbestimmte aus $X = \{X_i\}_{i\in\mathbb{N}}$, die in den Polynomen f_i und q_i nicht auftreten, so gilt*

$$\mathrm{ggT}\Big(\frac{f_1}{q_1}, \ldots, \frac{f_m}{q_m}\Big) \sim f_1 X_{i_1} + \ldots + f_m X_{i_m}.$$

[128] In dieser Deutlichkeit wurde die Aussage wohl erstmals von J. König formuliert (vgl. *König 1903*, S. 478ff., IX, § 7), dessen „Einleitung in die allgemeine Theorie der algebraischen Grösen“ aus dem Jahre 1903 sich durch ein für die damalige Zeit bemerkenswertes Verständnis der Kroneckerschen Theorie auszeichnet.

In dieser Formulierung wird man die Aussage bei Kronecker freilich vergeblich suchen.[129] Kronecker beweist jedoch zwei entscheidende Sätze, aus denen sich die Bezout-Eigenschaft des Quotientenringes $T[X]_{N(T)}$ unmittelbar ergibt. Sie lauten, modern formuliert:

Satz 4.10. *Sind $\alpha_1, \ldots, \alpha_m$ Elemente aus dem ganzen Abschluß T von D in L/K und bezeichnen $X_{i_1}, \ldots, X_{i_m}$ sowie $X_{j_1}, \ldots, X_{j_m}$ irgendwelche Unbestimmte aus $X = \{X_i\}_{i\in\mathbb{N}}$, so gilt $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m} \sim \alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}$.*[130] *Insbesondere ist jedes lineare Polynom bzgl. $T[X]_{N(T)}$ ein größter gemeinsamer Teiler seiner Koeffizienten, d. h.* $\mathrm{ggT}(\alpha_1, \ldots, \alpha_m) \sim \alpha_1 X_1 + \ldots + \alpha_m X_m$.

Satz 4.11. (*„2. Fundamentaltheorem“*) *Sind f und g zwei Polynome aus $T[X]$ mit denselben Koeffizienten, so gilt $f \sim g$ bzgl. $T[X]_{N(T)}$.*[131]

Aus diesen beiden Sätzen leitet man numehr ohne Probleme die Aussage des Hauptsatzes 4.9 her. Dazu seien $\frac{f_1}{q_1}, \ldots, \frac{f_m}{q_m} \in T[X]_{N(T)}$ gegeben. Existiert in $T[X]_{N(T)}$ ein größter gemeinsamer Teiler dieser Elemente, so ist dieser auf jeden Fall auch ein größter gemeinsamer Teiler der zu $\frac{f_1}{q_1}, \ldots, \frac{f_m}{q_m}$ in $T[X]_{N(T)}$ assoziierten Polynome $f_1, \ldots, f_m \in T[X]$. Es reicht also,

$$\mathrm{ggT}(f_1, \ldots, f_m) \sim f_1 X_{i_1} + \ldots f_m X_{i_m}$$

zu zeigen. Es bezeichnen $\alpha_{i1}, \ldots, \alpha_{in_i}$ für $i = 1, \ldots, m$ die Koeffizienten des Polynoms f_i. Nach Voraussetzung über die Unbestimmten $X_{i_1}, \ldots, X_{i_m}$ ist dann $f_1 X_{i_1} + \ldots + f_m X_{i_m}$ ein Polynom von $T[X]$ mit den Koeffizienten α_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n_i$. Dieses ist nach Satz 4.11 assoziiert zu einem *linearen* Polynom mit denselben Koeffizienten. Jedes lineare Polynom ist aber aufgrund von Satz 4.10 ein größter gemeinsamer Teiler all seiner Koeffizienten, so daß man schließlich folgende Kette von Assoziiertheitsrelationen erhält:

$$\begin{aligned} f_1 X_{i_1} + \ldots + f_m X_{i_m} &\sim \mathrm{ggT}(\ldots, \alpha_{i1}, \ldots, \alpha_{in_i}, \ldots)_{0\leqslant i\leqslant m} \\ &\sim \mathrm{ggT}(\ldots, \mathrm{ggT}(\alpha_{i1}, \ldots, \alpha_{in_i}), \ldots)_{0\leqslant i\leqslant m} \\ &\sim \mathrm{ggT}(\ldots, f_i, \ldots)_{0\leqslant i\leqslant m} \\ &\sim \mathrm{ggT}\Big(\frac{f_1}{q_1}, \ldots, \frac{f_m}{q_m}\Big). \end{aligned}$$

Wenden wir uns nunmehr den Kroneckerschen Beweisen für die Sätze 4.10 und 4.11 zu.

Beweis von Satz 4.10: Die Aussage, daß zwei lineare Polynome, deren Koeffizienten übereinstimmen, assoziiert in $T[X]_{N(T)}$ sind, wird erst in § 16 der Kummer-Festschrift formuliert. Der Beweis erfolgt jedoch bereits in § 14, also noch *vor* der eigentlichen Begriffsbildung. Entsprechend schwierig sind die Ausführungen Kroneckers nachzuvollziehen.

In § 14 zeigt Kronecker, daß der gebrochen rationale Ausdruck

$$\frac{\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}}{\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}} \cdot F_{K'/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}) \tag{4.12}$$

— K' bezeichne den Körper $K(\alpha_1, \ldots, \alpha_m) \subseteq L$ — ein Polynom aus $T[X]$ ist. Dies besagt jedoch nach den Ergebnissen des vorangegangenen Abschnitts nichts anderes, als daß $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}$

[129] In § 22, S. 350, der Kummer-Festschrift schreibt Kronecker, daß

> [...] der grösste gemeinsame Teiler zweier Grössen, also wenn sie gegeneinander relativ prim sind, die Zahl Eins[,] als lineare homogene Function derselben dargestellt werden kann und zwar mit Coefficienten, welche ebenfalls dem festgesetzten Grössenbereich entnommen sind.

Versteht man unter dem „festgesetzten Grössenbereich“ nach Kronecker jenen „Grössenbereich“, der entsteht, wenn man den „Gattungsbereich“ L „durch die Gesammtheit der ganzen algebraischen Formen des Gattungs-Bereichs“ erweitert und anschließend zu den Klassen absoluter Äquivalenz übergeht, betrachet man also im Prinzip den Quotientenkörper $T[X]_{N(T)}$, so scheint aus alledem hervorzugehen, daß Kronecker durchaus eine Vorstellung von der Bezout-Eigenschaft seiner algebraischen Divisoren besaß.

[130] *Kronecker 1882*, S. 307 (§ 16), Satz I.

[131] *Kronecker 1882*, S. 310 (§ 17), Satz II.

durch $\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}$ und aus Symmetriegründen demnach auch $\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}$ durch $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}$ teilbar ist, woraus schließlich die Behauptung folgt. Kroneckers Beweis besteht darin zu zeigen, daß der Ausdruck (4.12) einer Ganzheitsgleichung über dem Grundring D genügt. Und zwar betrachtet er das charakteristische Polynom dieses gebrochen rationalen Ausdrucks in der Unbestimmten Z. Setzt man $Z_k := X_{i_k} Z - X_{j_k} F_{K'/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m})$, so ist das charakteristische Polynom gegeben durch

$$N_{K'/K}\Big(Z - (\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}) \frac{F_{K'/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m})}{\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}}\Big) = \frac{N_{K'/K}(\alpha_1 Z_1 + \ldots + \alpha_m Z_m)}{N_{K'/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m})}.$$

Da $F_{K'/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m})$ ein Polynom mit Koeffizienten aus D ist, sind die Z_k ebenso wie die Unbestimmten X_{i_k} unter Konjugation invariant. Da im vorliegenden Fall ferner die Norm eines Polynoms das Produkt seiner Konjugierten ist, müssen die Koeffizienten von Zähler– und Nennerpolynom in D denselben größten gemeinsamen Teiler besitzen. Es folgt also

$$\frac{N_{K'/K}(\alpha_1 Z_1 + \ldots + \alpha_m Z_m)}{N_{K'/K}(\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m})} = \frac{F_{K'/K}(\alpha_1 Z_1 + \ldots + \alpha_m Z_m)}{F_{K'/K}(\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m})}.$$

Etwas knapp schreibt Kronecker, es werde „hiermit evident“, daß dieser Ausdruck ein bzgl. Z normiertes Polynom über D sei. Um diese lapidare Feststellung einzusehen, mache man sich klar, daß in jedem Koeffizienten des Zählerpolynoms, wenn man die Z_k wieder entsprechend aufschlüsselt, der Faktor $F_{K'/K}(\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m})$ enthalten ist und sich somit aus dem Quotienten herauskürzt.[132] Damit hat Kronecker den gebrochen rationalen Ausdruck (4.12) in der Tat als ganz über $D[X]$ nachgewiesen. Hieraus folgert er jedoch, daß dieser Ausdruck demnach ein Polynom mit Koeffizienten aus T sein müsse. Dies ist natürlich richtig, jedoch insofern ein unzulässiger Schluß, als Kronecker an keiner Stelle den Beweis erbringt, daß der Polynomring $T[X]$ der ganze Abschluß von $D[X]$ in $L(X)$ ist. Hier liegt eine der großen, allerdings schließbaren Lücken in Kroneckers Beweisführung.[133]

Die zweite Aussage von Satz 4.10 ist eine unmittelbare Folgerung aus dem eben Bewiesenen. Faßt man den Ausdruck (4.12) als Polynom über $T[X_{j_1}, \ldots, X_{j_m}]$ in den Unbestimmten $X_{i_1}, \ldots, X_{i_m}$ auf und ordnet die Koeffizienten entsprechend, so folgt

$$\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m} \mid \alpha_k \quad \text{für } k = 1, \ldots, m.$$

Jeder weitere gemeinsame Teiler der α_k teilt jedoch auch $\alpha_k X_{i_k}$ und schließlich $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}$, womit $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}$ als größter gemeinsamer Teiler von $\alpha_1, \ldots, \alpha_m$ nachgewiesen ist. Diese Argumentation ist m. E. der Kroneckerschen vorzuziehen. In der Festschrift wird nämlich stattdessen gezeigt:[134]

$$\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n} \mid \frac{\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}}{\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}} \quad \Leftrightarrow \quad \beta_1 X_{l_1} + \ldots + \beta_n X_{l_n} \sim 1.$$

Dabei seien $\beta_1, \ldots, \beta_n$ irgendwelche ganzen algebraischen Größen aus T und $X_{l_1}, \ldots, X_{l_s}$ von X_{i_k}, X_{j_k} unabhängige Unbestimmte aus $X = \{X_i\}_{i \in \mathbb{N}}$.

[132] Dedekind bemängelt in seinen „Bunten Bemerkungen“ die Kürze der Kroneckerschen Argumentation an dieser Stelle (vgl. *Edwards et al. 1982*, S. 57, Bemerkung Dedekinds Nr. 20). Seine diesbezüglichen Ausführungen entsprechen im wesentlichen den hier vorgestellten.

[133] Dedekind hat diese Lücke offenbar besonders gestört (vgl. *Edwards et al. 1982*, S. 57f., Bemerkung Dedekinds Nr. 20). *Edwards et al. 1982*, S. 68, Kommentar Nr. 20, zufolge stieß er bei dem Versuch, einen einfachen Beweis zu finden, auf einen sehr viel umfassenderen Satz, nämlich seinen sogenannten Prager Satz (vgl. Anmerkung 48, S. 21), der die zu beweisende Aussage als Korollar enthielt. Siehe hierzu auch den folgenden Abschnitt 4.4, insbesondere Satz 4.15, S. 59.

[134] *Kronecker 1882*, S. 299 (§ 14).

Für den Beweis betrachtet Kronecker $N_{K''/K}(\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n})$, wobei K'' jenen Körper bezeichne, der aus K durch Adjunktion von $\alpha_1, \ldots, \alpha_m$ und $\beta_1, \ldots, \beta_n$ entsteht. Ist γ ein größter gemeinsamer Teiler der Koeffizienten dieses Normpolynoms in D, so gilt

$$N_{K''/K}\left((\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m})\,\frac{F_{K''/K}(\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m})}{\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}} \cdot \frac{F_{K''/K}(\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n})}{\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n}}\right)$$
$$= \frac{1}{\gamma} F_{K''/K}(\beta_1 X_{l_1} + \ldots)^{[K'':K]-1} \cdot F_{K''/K}(\alpha_1 X_{i_1} + \ldots) \cdot F_{K''/K}(\alpha_1 X_{j_1} + \ldots)^{[K'':K]-1}.$$

Soll der Quotient $\frac{\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}}{\alpha_1 X_{j_1} + \ldots + \alpha_m X_{j_m}}$ durch das lineare Polynom $\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n}$ teilbar sein, so muß dieses Produkt notwendig ein Polynom in $D[X]$ sein. Dies ist jedoch nur dann der Fall, wenn das Element γ eine Einheit in D, also das lineare Polynom $\beta_1 X_{l_1} + \ldots + \beta_n X_{l_n}$ im Kroneckerschen Sinne primitiv und somit eine Einheit in $T[X]_{N(T)}$ ist.

An dieser Stelle bricht die Kroneckersche Argumentation ab. Zwar weiß man nun — man fasse den Normausdruck, wie oben, als Polynom in den Unbestimmten $X_{i_1}, \ldots, X_{i_m}$ auf —, daß $\alpha_1 X_{i_1} + \ldots + \alpha_m X_{i_m}$ ein größter gemeinsamer Teiler von $\alpha_1, \ldots, \alpha_m$ ist, sofern man ausschließlich lineare Divisoren als Teiler zuläßt. Der Beweis der generellen ggT-Eigenschaft kann jedoch m. E. erst dann als vollständig erbracht gelten, wenn bewiesen ist, daß — mit Kronecker gesprochen — jeder „algebraische Divisor“ zu einem linearen algebraischen Divisor „absolut äquivalent“, also in $T[X]_{N(T)}$ assoziiert ist. □

Kommen wir nun zum Beweis des zweiten der Kroneckerschen Hauptsätze. Die Aussage des Satzes sowie seinen Beweis formuliert Kronecker in § 17 der Festschrift. Dedekind merkt hierzu an: „Der Beweis ist so kurz und dunkel, daß ich über seine *Vollständigkeit* nicht zu urtheilen wage.“[135] Die Dedekindsche Kritik ist durchaus berechtigt. Dennoch sei der Versuch unternommen, Kroneckers Argumentation im einzelnen nachzuvollziehen, schon allein, um aufzuzeigen, an welchen Stellen sie lücken– oder gar fehlerhaft ist.

Beweis von Satz 4.11: Aufgrund der Transitivität der Assoziiertheitsrelation reicht es zu zeigen: Jedes Polynom $f \in T[X]$ ist in $T[X]_{N(T)}$ assoziiert zu einem aus seinen Koeffizienten gebildeten linearen Polynom, also $\alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)} \sim \alpha_1 X_1 + \ldots + \alpha_m X_m$, wobei $X^{(1)}, \ldots, X^{(m)}$ verschiedene Potenzprodukte von Unbestimmten aus $X = \{X_i\}_{i \in \mathbb{N}}$ bezeichnen. Daß das lineare Polynom auf der rechten Seite das Polynom auf der linken in dem Quotientenring $T[X]_{N(T)}$ teilt, ist aufgrund von Satz 4.10 klar. Bleibt also zu beweisen, daß ein lineares Polynom durch jedes Polynom mit denselben Koeffizienten teilbar ist.

Kroneckers Beweis untergliedert sich in mehrere Schritte. Der eigentliche Hauptbeweis wird im wesentlichen auf zwei Hilfsaussagen über lineare Divisoren zurückgeführt und läuft, modern gesprochen, darauf hinaus zu zeigen, daß der Quotientenring $T[X]_{N(T)}$ faktoriell ist.

Lemma 4.13. *Es seien f und g lineare Polynome aus $T[X]$ mit den Koeffizienten $\alpha_1, \ldots, \alpha_m$ und $\beta_1, \ldots, \beta_n$ und h ein lineares Polynom aus $T[X]$ mit den Koeffizienten $\alpha_i \beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$. Dann gilt $f \cdot g \sim h$.*[136]

Beweis: Aufgrund von Satz 4.10 gilt $f \mid \alpha_i$ und $g \mid \beta_j$, also $fg \mid \alpha_i \beta_j$, woraus schließlich $fg \mid h$ folgt. Umgekehrt gilt $h \mid \alpha_i \beta_j$, woraus sich $h \mid \sum_{i+j=k} \alpha_i \beta_j$, also $h \mid fg$, ergibt. □

[135] *Edwards et al. 1982*, S. 61, Bemerkung Dedekinds Nr. 27.
[136] *Kronecker 1882*, S. 308 (§ 16), Satz IV.

Mit der zweiten Hilfsaussage bringt Kronecker die algebraischen Primdivisoren ins Spiel. Dabei heißt ein algebraischer Divisor *prim*, wenn er, aufgefaßt als Element des Quotientenringes $T[X]_{N(T)}$, die Primeigenschaft besitzt.[137]

Lemma 4.14. *Jedes Polynom $f \in T[X]$ ist durch ein in $T[X]_{N(T)}$ primes lineares Polynom $p = \pi_1 X_{i_1} + \ldots + \pi_r X_{i_r} \in T[X]$ teilbar.*[138]

Über den Beweis dieser Aussage verliert Kronecker kein einziges Wort. Edwards bemerkt hierzu treffend:

> He [=Kronecker] seems to take it as obvious, that a given form is divisible by a *linear* prime divisor. I do not see the justification for this assertion [...].[139]

Nimmt man Lemma 4.14 trotz aller Vorbehalte als gegeben an, so verläuft Kroneckers weitere Argumentation wie folgt: Sei f irgendein Polynom aus $T[X]$.

1. Fall: f im Kroneckerschen Sinne primitiv. Ist f im Kroneckerschen Sinne primitiv, also $f \in N(T)$, so ist f eine Einheit in $T[X]_{N(T)}$, also $f \sim 1$. Jeder Teiler von f in $T[X]_{N(T)}$, insbesondere jedes aus den Koeffizienten von f gebildete lineare Polynom, ist damit ebenfalls eine Einheit und folglich assoziiert zu f.[140]

2. Fall: f *nicht* im Kroneckerschen Sinne primitiv. Kronecker geht in diesem Fall davon aus, daß sämtliche Konjugierten von f wiederum Polynome in $T[X]$ sind, die Körpererweiterung L/K also normal ist.[141] Eigentlich müßte er sogar die Endlichkeit der Körpererweiterung L/K verlangen, damit seine nachfolgende Argumentation durchführbar bleibt. Beide Einschränkungen passen jedoch nicht so recht zu dem unausgesprochenen Bestreben Kroneckers, seine Divisorentheorie

[137] Vgl. *Kronecker 1882*, S. 310 (§ 17), Definition I. Kronecker definiert zunächst nur den Begriff des „irreductiblen“ algebraischen Divisors, verwendet dafür allerdings auch die Bezeichnung „Primdivisor“. Dies ist insofern berechtigt, als sich beide Begriffe letztendlich als äquivalent erweisen. Der Beweis, den Kronecker angibt, ist allerdings unvollständig. Er behauptet: Ist $p = \pi_1 X_{i_1} + \ldots + \pi_r X_{i_r} \in T[X]$ ein lineares, in $T[X]_{N(T)}$ irreduzibles Polynom, so folgt aus $p \mid fg$, $f, g \in T[X]$, stets $p \mid f$ oder $p \mid g$ (vgl. *Kronecker 1882*, S. 311 (§ 17)). Diese Aussage versucht Kronecker durch vollständige Induktion nach der Anzahl s der in f und g insgesamt auftretenden verschiedenen Unbestimmten $X_j \in X = \{X_i\}_{i \in \mathbb{N}}$ zu beweisen. Den Fall $s = 0$ führt er auf eine Aussage zurück, die sich aus Satz 4.10 ergibt: Sind $f, g, h \in T[X]$ lineare Polynome in paarweise verschiedenen Unbestimmten mit $h \mid fg$ und $\mathrm{ggT}(h, g) \sim 1$, dann gilt $h \mid f$ (vgl. *Kronecker 1882*, S. 309 (§ 16), Satz V). Denn nach Satz 4.10 ist $\mathrm{ggT}(h, g) \sim h + g$, also $f \sim fh + fg$, woraus wegen $h \mid fg$ sofort $h \mid f$ folgt. Wählt man f und g als konstante Polynome und h als irreduzibles lineares Polynom p, so ist demnach der Induktionsanfang erbracht. Die Behauptung sei nunmehr bewiesen für $s - 1$ Unbestimmte, und es seien f, g Polynome aus $T[X]$ in den s Unbestimmten $X_1, \ldots, X_s \in X = \{X_i\}_{i \in N}$. Faßt man f und g als Polynome über $T[X_1, \ldots, X_{s-1}]$ in der Unbestimmten X_s auf, so zeigt ein einfacher Schluß, daß im Falle $p \nmid f$ und $p \nmid g$ nach Induktionsvoraussetzung mindestens ein Koeffizient von fg, ebenfalls aufgefaßt als Polynom in der Unbestimmten X_s, nicht durch p teilbar ist. An dieser Stelle bricht die Argumentation ab, und Kronecker bleibt somit eine einfache Erklärung schuldig, warum hieraus bereits $p \nmid fg$ folgt.

[138] *Kronecker 1882*, S. 311 (§ 17).

[139] *Edwards 1980*, S. 362, Anmerkung $\star$. Die Aussage des Lemmas ist in der Tat äußerst problematisch. Denn um die Existenz eines irreduziblen linearen Polynoms p mit der genannten Eigenschaft rechtfertigen zu können, benötigt man eigentlich genauere Kenntnisse über die Irreduzibilitätsverhältnisse in $T[X]_{N(T)}$. Diese ergeben sich jedoch erst an späterer Stelle, nämlich im nachfolgenden § 18 der Kummer-Festschrift, wo in groben Zügen ein Verfahren zur Primdivisorzerlegung in $T[X]_{N(T)}$ angedeutet wird. Selbst dann bleibt aber noch unklar, warum der besagte Primfaktor als *lineares* Polynom gewählt werden kann. Alles in allem liegt hierin eine große Lücke in der Kroneckerschen Argumentation. Um diese zumindest notdürftig zu schließen, beweist Edwards auf der Grundlage des § 18 der Festschrift für den Fall $D = \mathbb{Z}$ und L/K galoissch ein Lemma, wonach jede ganzrationale Primzahl in dem Quotientenring $T[X]_{N(T)}$ durch ein irreduzibles lineares Polynom aus $T[X]$ teilbar ist (vgl. *Edwards 1980*, S. 362). Leider läßt sich Edwards' Beweis nicht ohne weiteres auf den Fall $D = \mathbb{Z}[Y]$ übertragen.

[140] Kronecker schenkt dem Fall, daß f primitiv ist, keinerlei Beachtung. Zu einer vollständigen Beweisführung gehört er jedoch dazu.

[141] Dedekind moniert in seinen „Bunten Bemerkungen“, daß „das Heranziehen einer „Galoisschen Gattung [= *galoisschen Körpererweiterung* ...] sehr *künstlich*“ erscheine (*Edwards et al. 1982*, S. 61, Bemerkung Dedekinds Nr. 27).

für beliebige Körpererweiterungen L/K zu formulieren. Wir werden sehen, daß es ausreicht, die Kroneckerschen Beweisschritte zunächst in der normalen Hülle $\widetilde{K}_f$ von K_f/K durchzuführen. Ist gezeigt, daß das Polynom f in dem Quotientenring $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ — $\widetilde{T}_f$ bezeichne den ganzen Abschluß von D in $\widetilde{K}_f$ — jedes aus seinen Koeffizienten gebildete lineare Polynom teilt, folgt mit einer einfachen Überlegung, daß diese Teilbarkeitsrelation auch in $T[X]_{N(T)}$ erhalten bleibt.

Da f als nicht primitiv vorausgesetzt wird, ist $N_{\widetilde{K}_f/K}(f)$ ein Polynom in $D[X]$, dessen Koeffizienten in D einen *echten* größten gemeinsamen Teiler besitzen. Aufgrund von Lemma 4.14 existiert ein in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ primes lineares Polynom $p \in \widetilde{T}_f[X]$, welches $N_{\widetilde{K}_f/K}(f)$ (vermutlich denkt Kronecker an den größten gemeinsamen Teiler der Koeffizienten dieses Polynoms) in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ teilt und zudem mit dem Polynom f keine Unbestimmten gemein hat. Bezeichnen $\sigma_1, \ldots, \sigma_s$ die K-Automorphismen von $\widetilde{K}_f$, so läßt sich das Normpolynom von f auch schreiben als $N_{\widetilde{K}_f/K}(f) = \sigma_1(f) \cdot \ldots \cdot \sigma_s(f)$. Nach Voraussetzung sind alle Faktoren $\sigma_i(f)$ in dem Polynomring $\widetilde{T}_f[X]$ enthalten. Als Primelement teilt daher p in dem Quotientenring $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ einen Faktor $\sigma_i(f)$. Insbesondere gilt $\sigma_j(p) \mid f$ für ein $j \in \{1, \ldots, s\}$. Bei diesem $\sigma_j(p)$ handelt es sich wiederum um ein lineares, in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ primes Polynom aus $\widetilde{T}_f[X]$. Setzen wir $p_1 := \sigma_j(p)$, so existiert mit dem Polynom $f_1 := f \cdot \frac{1}{p_1} F_{\widetilde{K}_f/K}(p_1)$ ein Element aus $\widetilde{T}_f[X]$ dergestalt, daß f in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ assoziiert zu $p_1 f_1$ ist. Wendet man nun auf das Polynom f_1 dieselbe Überlegung wie für f an, so erhält man eine Assoziiertheitsrelation $f \sim p_1 p_2 f_2$ in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ mit $p_1, p_2, f_1 \in \widetilde{T}_f[X]$, p_1, p_2 linear und prim. Bedenkt man, daß $N_{\widetilde{K}_f/K}(f)$ in $D[X]$ eine Primzerlegung besitzt, so folgt, daß das Verfahren nach endlich vielen Schritten abbrechen muß, da das resultierende Polynom $f_i \in \widetilde{T}_f[X]$ irgendwann primitiv im Kroneckerschen Sinne, also eine Einheit in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ wird.[142] Man erhält also schließlich eine Assoziiertheitsrelation

$$f \sim p_1 \cdot \ldots \cdot p_n \cdot f_n \quad \text{mit } p_1, \ldots, p_n, f_n \in \widetilde{T}_f[X],\ p_i \text{ linear und prim},\ f_n \text{ primitiv}.$$

Diese Relation besagt in Kroneckerscher Terminologie nichts anderes, als daß jeder algebraische Divisor eindeutig als das Produkt von endlich vielen Primdivisoren darstellbar ist. Mit anderen Worten: Der Quotientenring $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ ist faktoriell. Darauf kommt es Kronecker an dieser Stelle jedoch überhaupt nicht an. Vielmehr führt er die Argumentation folgendermaßen fort. Das Produkt der linearen Polynome $p_1, \ldots, p_n$ läßt sich aufgrund von Lemma 4.13 zu einem einzigen assoziierten linearen Polynom $g \in \widetilde{T}_f[X]$ zusammenfassen, das mit dem Ausgangspolynom f keine Unbestimmten in $X = \{X_i\}_{i \in \mathbb{N}}$ gemein hat. Bezeichnen X' und X'' die disjunkten Teilmengen der in f und g auftretenden Unbestimmten, so gilt also $f(X') \sim g(X'') \cdot f_n(X', X'') \sim g(X'')$. Das Polynom $q(X', X'') := f(X') \cdot \frac{1}{g(X'')} F_{K_g/K}\big(g(X'')\big) \in \widetilde{T}_f[X]$ ist daher eine Einheit in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$, also insbesondere im Kroneckerschen Sinne primitiv, und man erhält die Gleichung

$$f(X') = q(X', X'') \cdot \frac{g(X'')}{F_{K_g/K}\big(g(X'')\big)}.$$

Faßt man die rechte Seite als Polynom in den Unbestimmten X' auf, so folgt durch Koeffizientenvergleich, daß die Koeffizienten $\alpha_1, \ldots, \alpha_m$ von f in dem Quotientenring $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$ durch g, wegen $f \sim g$ also insbesondere durch f teilbar sein müssen. Insgesamt folgt daher $f \mid \alpha_1 X_1 + \ldots + \alpha_m X_m$. Zwar handelt es sich hierbei um eine Teilbarkeitsbeziehung in $\widetilde{T}_f[X]_{N(\tilde{T}_f)}$. Wegen

$$(\alpha_1 X_1 + \ldots + \alpha_m X_m) \cdot \frac{F_{\widetilde{K}_f/K}(f)}{f} \ \in \widetilde{T}_f[X] \cap L[X] \subseteq T[X]$$

folgt jedoch unmittelbar mit Satz 4.8 auch die Teilbarkeit in $T[X]_{N(T)}$. □

[142] Vgl. hierzu *Edwards et al. 1982*, S. 61, Bemerkung Dedekinds Nr. 27, sowie S. 71, Kommentar Nr. 27.

4.4. Zu einem zeitgemäßen Verständnis des Kroneckerschen Divisorbegriffs

In den vorangegangenen beiden Abschnitten wurde herausgearbeitet, daß ein zeitgemäßes Verständis der Kroneckerschen Divisorentheorie m. E. darauf hinausläuft,

1.) Kroneckers algebraische Divisoren als Elemente des Quotientenringes $T[X]_{N(T)}$, genauer gesagt: als Repräsentanten seiner Assoziiertheitsklassen aufzufassen und
2.) die §§ 14 – 17 der Kummer-Festschrift als Beweis für die Bezout-Eigenschaft eben dieses Quotientenringes $T[X]_{N(T)}$ zu lesen.

Was den zweiten Punkt betrifft, ergeben sich jedoch insofern Schwierigkeiten, als Kroneckers Argumentation, wie wir sahen, an einigen Stellen lückenhaft und dunkel ist. Da ist zum einen die unbewiesene Behauptung, daß der Polynomring $T[X]$ der ganze Abschluß von $D[X]$ in $L(X)$ ist. Diese Lücke kann mit vertretbarem Aufwand geschlossen werden, ohne die Kroneckersche Beweisführung ändern zu müssen.[143] Weitaus schwieriger gestaltet sich jedoch ein adäquater Beweis des „2. Fundamentaltheorems“, also jenes Satzes, daß zwei Polynome aus $T[X]$ in $T[X]_{N(T)}$ assoziiert zueinander sind, wenn sie dieselben Koeffizienten besitzen. Der von Kronecker in der Festschrift vorgezeichnete Weg ist offensichtlich nur gangbar, wenn man einige Ungereimtheiten in Kauf nimmt. Mir ist keine Darstellung bekannt, die sich in dieser Beziehung konsequent an das Kroneckersche Vorbild hält.

Einen Schlüssel zur Vervollständigung bzw. Vereinfachung der Kroneckerschen Beweisführung, dessen sich mittlerweile nahezu alle Darstellungen der Kroneckerschen Divisorentheorie mehr oder weniger offen bedienen, stellt der Prager Satz von Dedekind dar. Danach besitzt das Produkt zweier Polynome $f = \alpha_1 X^{(1)} + \ldots + \alpha_m X^{(m)}$ und $g = \beta_1 X^{(1)'} + \ldots + \beta_n X^{(n)'}$ aus $L[X]$ — $X^{(i)}, X^{(i)'}$ bezeichnen, wie bisher, beliebige Potenzprodukte von Unbestimmten aus $X = \{X_i\}_{i\in\mathbb{N}}$ —, genau dann ausschließlich Koeffizienten in T, wenn $\alpha_i\beta_j$ für alle $i = 1, \ldots, m$ und $j = 1, \ldots, n$ bereits ganz über D, d. h. in T enthalten ist.[144] Es ist bezeichnend, daß Dedekind offenbar gerade in Auseinandersetzung mit der Kummer-Festschrift auf diesen wichtigen Satz stieß.[145] Interessanterweise schrieb Hurwitz die Autorenschaft an der im Prager Satz formulierten Aussage nicht Dedekind, sondern Kronecker zu.[146] Dies ist allerdings wohl nur insofern gerechtfertigt, als sich der Satz auch aus Gedankengängen ergibt, die Kronecker in seiner Abhandlung „Zur Theorie der Formen höherer Stufen“ aus dem Jahre 1883 darlegte. Eine dem Prager Satz vergleichbare Aussage wird man bei Kronecker vergebens suchen.[147]

Wie dem auch sei — fest steht, daß die Kroneckersche Theorie durch den Prager Satz in der Tat „eine nicht unerhebliche Vereinfachung“ erfährt.[148] Man kann m. E. sogar noch einen Schritt weiter gehen und sagen, daß das Gebäude der Kroneckerschen Divisorentheorie erst durch den Prager Satz ein solides, wirklich tragfähiges Fundament erhält. Dies soll im folgenden näher ausgeführt und begründet werden.

---

[143] Der erste einfache Beweis stammt von Hurwitz (siehe *Hurwitz 1895*, S. 231) und wurde im Jahre 1895 veröffentlicht, nachdem Dedekind auf die Lücke in der Kroneckerschen Beweisführung aufmerksam gemacht hatte (vgl. *Edwards et al. 1982*, S. 68, Kommentar Nr. 20).

[144] Dedekind formulierte den Satz zunächst nur für den Fall algebraischer Zahlkörper, d. h. für den Fall $D = \mathbb{Z}$, $K = \mathbb{Q}$ und L/K endlich (für den genauen Wortlaut siehe Anmerkung 48). Für den Beweis des allgemeinen Falles siehe Satz 2.13, S. 20.

[145] Vgl. Anmerkung 133.

[146] Siehe *Hurwitz 1895*, S. 230f.,

[147] Vgl. hierzu *Edwards 1980*, S. 367f., sowie *Edwards et al. 1982*, S. 69, Kommentar Nr. 20. Dort ist auch ausgeführt, in welcher Weise von Kroneckers Überlegungen auf die Aussage des Prager Satzes geschlossen werden kann. Nachfolgende Mathematiker schlossen sich allerdings dem Urteil Hurwitz' an. So spricht Krull vom „Kroneckerschen Satze“ (*Krull 1935*, S. 124, § 45), Prüfer immerhin noch vom „Gauß-Kronecker-Dedekindschen Satz“ (*Prüfer 1932*, S. 23, § 9).

[148] So Dedekind in einem Brief an H. Weber vom 20. Februar 1887. Zitiert nach *Edwards et al. 1982*, S. 77.

Als erste Folgerung aus dem Prager Satz ergibt sich unmittelbar

Satz 4.15. *Bezeichnet T den ganzen Abschluß von D in der algebraischen Körpererweiterung L/K, so ist der Polynomring $T[X]$ der ganze Abschluß von $D[X]$ in $L(X)/K(X)$.*

Beweis: Die rationale Funktion $f \in L(X)$ genüge einer Ganzheitsgleichung über $D[X]$, d. h. es gebe ein normiertes Polynom d in der Unbestimmten Z mit Koeffizienten aus $D[X]$, das f zur Nullstelle hat. Da die Norm von f bzgl. der Körpererweiterung $K_f(X)/K(X)$ ein Polynom mit Koeffizienten aus D ist, muß f ebenfalls ein Polynom sein. Über dem Polynomring $L[X]$ läßt sich demzufolge von d der Linearfaktor $(Z - f)$ abspalten, d. h. es existieren $d_1, \ldots, d_{n-1} \in L[X]$, $n = \text{grad}\, d(Z)$, mit

$$d(Z) = (Z - f)(Z^{n-1} + d_1 Z^{n-1} + \ldots + d_{n-2}Z + d_{n-1}).$$

Faßt man nunmehr d als Polynom über L in den Unbestimmten Z und $X_i \in X = \{X_i\}_{i\in\mathbb{N}}$ auf, so folgt aus dem Prager Satz, daß jeder Koeffizient von f, multipliziert mit einem beliebigen Koeffizienten von $Z^{n-1} + d_1 Z^{n-1} + \ldots + d_{n-2}Z + d_{n-1} \in L[X, Z]$, also insbesondere multipliziert mit dem Leitkoeffizienten 1, ein Element aus T ergibt. Also ist f ein Polynom aus $T[X]$. □

Damit schließt der Prager Satz eine der großen Lücken in Kroneckers Divisorentheorie. Sein eigentlicher Wert liegt allerdings darin, daß er den undurchsichtigen Kroneckerschen Beweis für das „2. Fundamentaltheorem“ vollkommen zu ersetzen vermag.

Satz 4.16. *Sei f ein Polynom aus $T[X]$ mit den Koeffizienten $\alpha_1, \ldots, \alpha_m$. Dann gilt $f \mid \alpha_i$ in $T[X]_{N(T)}$. Insbesondere ist f in $T[X]_{N(T)}$ zu jedem linearen Polynom mit den Koeffizienten $\alpha_1, \ldots, \alpha_m$ assoziiert.*

Beweis: Es seien $\gamma \in D$ ein größter gemeinsamer Teiler der Koeffizienten von $N_{K_f/K}(f) \in D[X]$ und $h \in T[X]$ der Komplementärteiler von f in $N_{K_f/K}(f)$, d. h. es gelte $N_{K_f/K}(f) = fh$. Wegen

$$\gamma \cdot \frac{F_{K_f/K}(f)}{f} = \frac{N_{K_f/K}(f)}{f} = h \in T[X]$$

ist γ in $T[X]_{N(T)}$ durch f teilbar. Aus $F_{K_f/K}(f) = \frac{1}{\gamma}h \cdot f \in T[X]$ und $\frac{1}{\gamma}h \in L[X]$ folgt mit dem Prager Satz nunmehr, daß jeder Koeffizient α_i von f, multipliziert mit einem Koeffizienten des Polynoms $\frac{1}{\gamma}h$, in T liegt. Es gilt also $\alpha_i \cdot \frac{1}{\gamma}h \in T[X]$ für $i = 1, \ldots, m$. Daraus erhält man schließlich

$$\alpha_i \cdot F_{K_f/K}(f) = f \cdot \alpha_i \frac{h}{\gamma}, \quad \text{also} \quad \alpha_i = f \cdot \frac{\alpha_i \cdot \frac{h}{\gamma}}{F_{K_f/K}(f)},$$

was gerade besagt, daß α_i in $T[X]_{N(T)}$ durch f teilbar ist. □

Dieser Beweis ist dem Kroneckerschen nicht nur in puncto Klarheit und Einfachheit, sondern auch in methodischer Hinsicht deutlich überlegen. Denn Kronecker setzt, wie wir sahen, beim Beweis seines Fundamentaltheorems Argumente ein, die die Faktorialität des Grundringes $D = \mathbb{Z}[Y]$ ausnutzen.[149] Nunmehr tritt jedoch offen zutage, daß man für den Begriff des algebraischen Divisors und den Beweis der Bezout-Eigenschaft des Quotientenringes $T[X]_{N(T)}$ lediglich die Existenz eines größten gemeinsamen Teilers in D, nicht aber die Existenz einer eindeutigen Primfaktorzerlegung benötigt. Mit anderen Worten: Kroneckers Divisorentheorie ist zunächst vor allem eine Theorie des größten gemeinsamen Teilers, in der Irreduzibilitäts– bzw. Primeigenschaft bei der Begriffsbildung überhaupt keine Rolle spielen.

[149] Vgl. Anmerkung 139.

Dies ist m. E. die richtige Stelle, um Kroneckers Ausführungen im Kontext mit dem eigentlichen Untersuchungsgegenstand dieser Arbeit, nämlich den Ringen mit ggT-Theorie, ausführlich zu beleuchten.

Beginnen möchte ich mit einigen Bemerkungen über die Familie $X = \{X_i\}_{i\in\mathbb{N}}$ von Unbestimmten. Die Möglichkeit, aus einem unerschöpflichen Reservoir von paarweise unabhängigen Unbestimmten verfügen zu können, scheint für Kroneckers Theorie grundlegend und unentbehrlich zu sein. So schreibt Edwards: „[...] it is important that one be able to add new indeterminates at will.“[150] Diese Notwendigkeit besteht jedoch nicht. Kronecker selbst hat ein Verfahren beschrieben, das die Übertragung sämtlicher Überlegungen auf den Fall einer einzigen Unbestimmten erlaubt. Dazu seien f und g zwei Polynome aus $T[X]$ in den Unbestimmten $X_1, \ldots, X_s \in X = \{X_i\}_{i\in\mathbb{N}}$. Man könnte natürlich ohne weiteres f und g jeweils irgendein Polynom in der Unbestimmten Z zuordnen, das dieselben Koeffizienten hat. Aber dann würden sich die Koeffizienten bei der Produktbildung von f und g i. a. anders zusammenfassen als bei der Produktbildung der entsprechenden Polynome in *einer* Unbestimmten, und genau das gilt es zu verhindern. Kronecker löst dieses Problem, indem er für eine zunächst nicht näher spezifizierte natürliche Zahl d folgenden Ringhomomorphismus betrachtet:[151]

$$\begin{aligned}\varphi_d : \qquad & T[X_1, \ldots, X_s] \longrightarrow T[Z] \\ & \alpha_{i_0\ldots i_s} X_1^{i_0} \cdot \ldots \cdot X_s^{i_s} \longmapsto \alpha_{i_0\ldots i_s} Z^{i_0+i_1 d+\ldots+i_s d^m}.\end{aligned}$$

Offenbar handelt es sich bei dem rechts auftretenden Exponenten um die d-adische Darstellung einer natürlichen Zahl. Durch geeignete Wahl von d kann somit erreicht werden, daß die Koeffizienten von f, g und fg mit den Koeffizienten der Bildpolynome $\varphi_d(f)$, $\varphi_d(g)$ und $\varphi_d(fg)$ aus $T[Z]$ übereinstimmen. Man hat dazu lediglich d größer als den größten im Produkt fg auftretenden Exponenten i_k der X_k, $k = 1, \ldots, s$, zu wählen. Eine entsprechende Überlegung läßt sich natürlich auch für mehr als zwei Polynome, genauer gesagt: stets für endlich viele Polynome $f_1, \ldots, f_m$ anstellen. Das heißt konkret, daß man die Kroneckerschen Beweise zunächst ohne Beschränkung an die Menge der zur Verfügung stehenden Unbestimmten durchführt, dann aus sämtlichen auftretenden Polynomen bzw. Potenzprodukten in der angegebenen Weise die Basiszahl d bestimmt und schließlich vermöge der Abbildung φ_d den Reduktionsprozeß auf eine einzige Unbestimmte durchführt. Die Beschränkung, die man sich im Falle einer einzigen Unbestimmten auferlegt, wird also durch die Möglichkeit, in den Potenzen beliebig hoch gehen zu können, wieder ausgeglichen.

Es ist letztendlich vor allem eine Geschmacksfrage, welche Variante bei der Darstellung der Kroneckerschen Divisorentheorie vorzuziehen ist. Allerdings hat Koch m. E. recht, wenn er zu bedenken gibt:

> [...] a function field in one variable appears to the mathematician of our days as a nicer object and it is a simpler object than a function field in infinitely many variables.[152]

Wie in den vorangegangenen Kapiteln dieser Arbeit auch, soll daher X ab jetzt wieder als Unbestimmte (und nicht als Familie von Unbestimmten) aufgefaßt werden.

Wir wollen nun zeigen, daß Kroneckers algebraische Divisoren, also die Elemente (bzw. die Repräsentanten von Assoziiertheitsklassen) des Quotientenringes $T[X]_{N(T)}$, damit zu dem werden, was in den vorangegangenen Kapiteln dieser Arbeit als *Kronecker-Divisor* bezeichnet wurde.[153] Dazu folgende Überlegung.

Kronecker arbeitet über faktoriellen Grundringen D der Gestalt $\mathbb{Z}[Y]$, wobei $Y = \{Y_i\}_{i\in\mathbb{N}}$ eine Familie von paarweise unabhängigen Unbestimmten bezeichnet. Bei der Begründung des

[150] *Edwards 1980*, S. 355.
[151] *Kronecker 1882*, S. 257f. (§ 4).
[152] *Koch 1992*, S. 27, Remark.
[153] Vgl. Defintion 2.20, S. 25.

Kroneckerschen Divisorbegriffs tritt die Faktorialität von D allerdings vollkommen in den Hintergrund; entscheidend ist vielmehr die Existenz eines größten gemeinsamen Teilers in D. Als ggT-Bereich ist D und damit auch sein ganzer Abschluß T in jeder beliebigen algebraischen Körpererweiterung L/K insbesondere ein Ring mit ggT-Theorie e. T.[154] Wir hatten gesehen, daß in diesem Fall jede ggT-Theorie für T isomorph zur *Kroneckerschen ggT-Theorie*

$$(\cdot) : T^* \to T^{v*}/T^{v\times} \quad \text{mit} \quad T^v = \left\{ \frac{f}{g} : f, g \in T[X] \text{ mit } \mathrm{c}(f)_v \subseteq \mathrm{c}(g)_v \right\}$$

ist und der *Kroneckersche Funktionalring* T^v von T bzgl. der v-Idealoperation mit dem Quotientenring von $T[X]$ nach den v-primitiven Polynomen $N_v(T)$, also dem *Nagatabereich* $T_v(X)$ bzgl. der v-Idealoperation, übereinstimmt.[155]

Andererseits liefert aufgrund des Kroneckerschen Hauptsatzes 4.9 auch der Ring $T[X]_{N(T)}$, also der Quotientenring von $T[X]$ nach den im Kroneckerschen Sinne primitiven Polynomen $N(T)$, eine ggT-Theorie für T vermöge

$$\begin{array}{rcl} [\,\cdot\,] : \; T^* & \longrightarrow & T[X]^*_{N(T)}/T[X]^\times_{N(T)} \\ \alpha & \longmapsto & [\,\alpha\,] \end{array} .$$

Denn als Bezoutbereich ist $T[X]_{N(T)}$ insbesondere ein ggT-Bereich und somit die Halbgruppe der Assoziiertheitsklassen ein ggT-Monoid. Darüber hinaus gilt aufgrund von Satz 4.8 für zwei Elemente $\alpha, \beta \in T$

$$\beta \mid \alpha \quad \text{bzgl. } T \quad \Leftrightarrow \quad \beta \mid \alpha \quad \text{bzgl. } T[X]_{N(T)},$$

womit Axiom (G 1) nachgewiesen ist.[156] Axiom (G 2.2) ist ebenfalls erfüllt, da jedes Element aus $T[X]_{N(T)}$ zu einem Polynom aus $T[X]$ assoziiert und jedes Polynom in $T[X]_{N(T)}$ aufgrund des Hauptsatzes 4.9 in $T[X]_{N(T)}$ ein größter gemeinsamer Teiler seiner Koeffizienten ist.

Nun wird die ggT-Theorie $(\cdot) : T^* \to T^{v*}/T^{v\times}$ nicht ohne Grund nach Kronecker benannt. Denn es zeigt sich, daß der Quotientenring $T[X]_{N(T)}$ mit dem Quotientenring $T[X]_{N_v(T)} = T_v(X)$ nicht nur eine große Ähnlichkeit hat, sondern tatsächlich mit ihm übereinstimmt. Dies wiederum hat zur Folge, daß wegen $T[X]_{N_v(T)} = T^v$ beide zugehörigen ggT-Theorien nicht nur isomorph, sondern sogar identisch sind. Um dies einzusehen, werfen wir einen genauen Blick auf den Kroneckerschen Primitivitätsbegriff.

Der ggT-Bereich $D = \mathbb{Z}[Y]$, von dem Kronecker ausgeht, läßt sich nach Satz 2.2, S. 15, idealtheoretisch als ein Integritätsbereich charakterisieren, in dem jedes v-endliche v-Ideal ein Hauptideal ist. Ist also $f \in D[X]$ ein Polynom mit den Koeffizienten $\alpha_1, \ldots, \alpha_m \in D$, so gilt

$$\mathrm{ggT}(\alpha_1, \ldots, \alpha_m) \sim \gamma \quad \Leftrightarrow \quad (\alpha_1, \ldots, \alpha_m)_v = \gamma D.$$

Kronecker nennt nun das Polynom f „primitiv“, wenn seine Koeffizienten $\alpha_1, \ldots, \alpha_m$ teilerfremd sind. Kroneckers Primitivitätsbegriff für Polynome mit Koeffizienten aus dem Grundring D entspricht damit genau dem in dieser Arbeit benutzten Begriff der v-Primitivität bzw., sofern man den ggT-Bereich D als Ring mit ggT-Theorie e. T. auffaßt, dem Begriff der D-Primitivität.[157]

---

[154] Vgl. Abschnitt 3.4, insbesondere Satz 3.14, S. 40.

[155] Vgl. Satz 2.28, S. 29, und 3.15, S. 40.

[156] Man beachte, daß wegen $F_{K(\alpha)/K}(\alpha) \sim 1$ (Assoziiertheit in $D[X]$) der gemäß Definition 4.1 zu α gehörige algebraische Divisor $\mathrm{div}[\alpha]$ im Prinzip mit dem Element α identisch ist und sich daher die Teilbarkeitsrelation $\mathrm{div}[\beta] \mid \mathrm{div}[\alpha]$ im Sinne von Definition 4.4 übersetzt zu $\frac{\alpha}{\beta} \in T$.

[157] Vgl. Definition 2.14, S. 22. Man beachte, daß Kroneckers Grundring $D = \mathbb{Z}[Y]$ *kein* Bezoutbereich ist und somit das von $\alpha_1, \ldots, \alpha_m$ erzeugte D-Ideal i. a. nicht mit seinem zugehörigen v-Ideal übereinstimmen wird. Mit anderen Worten: Ist das von den Koeffizienten eines Polynoms $f \in D[X]$ erzeugte gewöhnliche D-Ideal ungleich D, so kann f dennoch im Kroneckerschen Sinne primitiv sein. Erst für den Fall $D = \mathbb{Z}$ ergibt sich diesbezüglich eine völlige Identität, denn dann stimmt das Idealsystem der v-Ideale trivialerweise mit dem Idealsystem der gewöhnlichen D-Ideale (= d-Ideale) überein, und ein Polynom $f \in D[X]$ ist primitiv genau dann, wenn das von seinen Koeffizienten erzeugte D-Ideal gleich D ist.

Nun weitet jedoch Kronecker beim Übergang von D zum ganzen Abschluß T in einer beliebigen algebraischen Körpererweiterung L/K seinen Primitivitätsbegriff aus, und zwar in der in Definition 4.5 beschriebenen Weise. Bezeichnet $N(D)$ die Menge der primitiven Polynome von $D[X]$ und $N(T)$, wie gehabt, die Menge der im erweiterten Kroneckerschen Sinne primitiven Polynome von $T[X]$, so stellt man fest, daß der Quotientenring $T[X]_{N(D)}$ mit dem Quotientenring $T[X]_{N(T)}$ übereinstimmt. Denn nach dem oben Gesagten gilt

$$N_v(D) = \{f \in D[X] : \mathrm{c}(f)_v = D\} = N(D) \subseteq N(T),$$

woraus $T[X]_{N(D)} \subseteq T[X]_{N(T)}$ folgt. Für die umgekehrte Inklusion betrachte man ein $\frac{f}{q} \in T[X]_{N(T)}$ mit $f \in T[X]$, $q \in N(T)$. Wegen $N_{K_q/K}(q) \in N(D)$ und $q \mid N_{K_q/K}(q)$ in $T[X]$ gilt

$$\frac{f}{q} = \frac{f \cdot \frac{N_{K_q/K}(q)}{q}}{N_{K_q/K}(q)} \in T[X]_{N(D)},$$

womit auch $T[X]_{N(T)} \subseteq T[X]_{N(D)}$ bewiesen ist. Bedenkt man, daß der Quotientenring $T[X]_{N_v(D)}$ der ganze Abschluß des Nagatabereiches $D[X]_{N_v(D)} = D_v(X)$ in der algebraischen Körpererweiterung $L(X)/K(X)$ ist, so ergeben sich aufgrund von Satz 2.28, S. 29, sowie Satz 3.15, S. 40, insgesamt die Gleichheitsrelationen

$$T[X]_{N(T)} = T[X]_{N(D)} = T[X]_{N_v(D)} = T[X]_{N_v(T)} = T_v(X) = T^v,$$

was beweist, daß die oben untersuchten ggT-Theorien tatsächlich identisch sind. Es folgt jedoch noch mehr.

Aufgrund der Gleichheit der Quotientenringe $T[X]_{N_v(T)}$ und $T[X]_{N(T)}$ liegt die Vermutung nahe, daß die Menge $N(T)$ der im Kroneckerschen Sinne primitiven Polynome mit der Menge $N_v(T)$ der v-primitiven Polynome von $T[X]$ übereinstimmt. Dies ist tatsächlich der Fall. Denn für zwei Polynome $f, g \in T[X]$ gilt

$$f \sim g \quad \text{in } T[X]_{N(T)} \quad \Leftrightarrow \quad \frac{f}{g}, \frac{g}{f} \in T[X]_{N(T)} = T^v \quad \Leftrightarrow \quad \mathrm{c}(f)_v = \mathrm{c}(g)_v.$$

Daraus erhält man

$$\begin{aligned} f \in N(T) \quad &\Leftrightarrow \quad N_{K_f/K}(f) \in N(D) \quad \Leftrightarrow \quad N_{K_f/K}(f) \quad \text{Einheit in } D[X]_{N(D)} \\ &\Leftrightarrow \quad f \quad \text{Einheit in } T[X]_{N(D)} = T_v(X) \quad \Leftrightarrow \quad \mathrm{c}(f)_v = T \\ &\Leftrightarrow \quad f \in N_v(T), \end{aligned}$$

d. h. ein Polynom $f \in T[X]$ ist genau dann primitiv im Kroneckerschen Sinne, wenn es v-primitiv ist. Man kann demnach den Kroneckerschen Primitivitätsbegriff vollkommen durch den Begriff der v-Primitivität ersetzen, unabhängig davon, ob man Polynome mit Koeffizienten aus dem Grundring D oder dem ganzen Abschluß T betrachtet.

Für den Fall $D = \mathbb{Z}$, $K = \mathbb{Q}$ und L/K endlich, für den Fall also, daß die klassische Ausgangssituation der algebraischen Zahlentheorie mit L als algebraischem Zahlkörper und T als Ring der ganzen Zahlen vorliegt, deckt sich der Kroneckersche Primitivitätsbegriff mit dem Begriff der d-Primitivität. Denn dann sind bekanntlich D und T Dedekindringe, in denen die d-Ideale (= gewöhnliche gebrochene D- bzw. T-Ideale) bzgl. der d-Multiplikation (= gewöhnliche Idealmultiplikation) eine Gruppe bilden. Daraus wiederum folgt mit Korollar 1.11, S. 11, die Gleichheit von d- und t-Idealsystem, also schließlich, da t-endliche t-Ideale und v-endliche v-Ideale dasselbe sind, die Gleichheit von d-Inhalt und v-Inhalt bzw. d-Primitivität und v-Primitivität.[158]

Bezieht man schließlich die Faktorialität des Kroneckerschen Grundringes $D = \mathbb{Z}[Y]$ in die Betrachtungen ein, weil man auf eine Übertragung der eindeutigen Primfaktorzerlegung in den

[158] Vgl. hierzu auch § 6 des Hilbertschen „Zahlberichtes“. Hilberts „Einheitsformen“ entsprechen genau den d-primitiven Polynomen von $T[X]$, sein Inhaltsbegriff deckt sich mit dem des d-Inhalts. Man erkennt daraus, daß Hilberts Ausführungen nur für den Fall $D = \mathbb{Z}$ richtig sind, jedoch für den allgemeinen Kroneckerschen Fall $D = \mathbb{Z}[Y]$ ihre Gültigkeit verlieren, sofern man die Begriffe nicht in der entsprechenden Weise modifiziert.

ganzen Abschluß T abzielt, und setzt zudem die Körpererweiterung L/K als endlich voraus, so wird die Kroneckersche ggT-Theorie $[\,\cdot\,] : T^* \to T^{v*}/T^{v\times}$ des ganzen Abschlusses T aufgrund von Satz 3.16, S. 41, genau genommen zu einer Divisorentheorie für T. Insbesondere ist der zugehörige Kroneckersche Funktionalring $T^v = T_v(X) = T[X]_{N(T)}$ nach Satz 3.13, S. 39, ein Hauptidealbereich, dessen Primelemente genau den Kroneckerschen Primdivisoren und damit den primen t-Idealen von T entsprechen.

Insgesamt zeigt sich, daß der methodische Ansatz Kroneckers, seine Theorie ganz auf dem Begriff des größten gemeinsamen Teilers aufzubauen, zunächst ohne Irreduzibilitäts-bzw. Primbegriff (damit auch ohne Fixierung auf eine bestimmte endliche Körpererweiterung L/K) auskommt. Der Übergang zur eindeutigen Primzerlegung (damit die Festlegung auf eine bestimmte endliche Körpererweiterung L/K) braucht erst in einem letzten gedanklichen Schritt vollzogen zu werden und ergibt sich dann auf überaus elegante Weise. Kroneckers Theorie der algebraischen Divisoren ist also zunächst vor allem eine Theorie des größten gemeinsamen Teilers, die dann das Fundament für eine Theorie der Primfaktorzerlegung bildet. Es ist Edwards zuzustimmen, wenn er schreibt:

> [. . .] one of Kronecker's most valuable ideas [*is* . . .] the idea that the objective of the theory is to define greatest common divisors, *not* to achieve factorization into primes.[159]

Bemerkenswert ist, daß es in J. König bereits zu Anfang dieses Jahrhunderts einen Mathematiker gab, der die Kroneckersche Theorie offenbar genau in diesem Sinne verstand.[160]

In der Regel wurde (und wird) die Kroneckersche Divisorentheorie, wenn man von Mathmatikern wie König, Prüfer oder Edwards einmal absieht, als Theorie der eindeutigen Primfaktorzerlegung verstanden. Dies gilt insbesondere auch für die „Einführung in die Theorie der algebraischen Zahlen" von M. Eichler, wo es im Vorwort heißt:[161]

> [. . .] die weitaus eleganteste Begründung der Teilbarkeitslehre [ist] die älteste, nämlich die von Kronecker [. . .], denn sie führt direkt zu einem Hauptidealring, dessen Divisoren den Idealen entsprechen.

Eichler liest die §§ 14 – 18 der Kummer-Festschrift also nicht als Beweis für die Bezout-Eigenschaft, sondern als Beweis für die Hauptideal-Eigenschaft des Kroneckerschen Quotientenringes $T[X]_{N(T)}$. In seiner Darstellung der Kroneckerschen Theorie setzt er den Grundring D zunächst als Hauptidealbereich voraus, um zu zeigen, daß in diesem Fall die Quotientenringe $D[X]_{N(D)}$ sowie $T[X]_{N(T)}$ ebenfalls Hauptidealbereiche sind.[162] Erst im Anschluß daran beweist er die Gültigkeit einer entsprechenden Aussage unter der schwächeren Voraussetzung, daß der Grundring D, wie in der Kroneckerschen Ausgangssituation, faktoriell ist.[163]

---

[159] *Edwards 1990*, S. v.

[160] Vgl. *König 1903*, S. 477, XI, § 7, wo Kroneckers Vorgehen als Einbettung des ganzen Abschlusses T in einen geeigneten ggT-Bereich („vollständigen holoiden Bereich") beschrieben wird. König führt anschließend den Beweis, daß der Kroneckersche Quotientenring $T[X]_{N(T)}$ zu einem Bezout-Bereich wird, wenn der Ausgangsring D ein ggT-Bereich ist (vgl. *König 1903*, S. 478ff., IX, § 7), und zeigt, daß dieser Bezout-Bereich faktoriell (insgesamt also Hauptidealbereich) wird, wenn auch D faktoriell ist (vgl. *König 1903*, S. 485f., IX, § 9). Siehe auch Anmerkung 128 in dieser Arbeit.

[161] *Eichler 1963*, S. 8.

[162] Siehe *Eichler 1963*, S. 70, § 3.

[163] Siehe *Eichler 1963*, S. 75f., § 6. Eichler behauptet sogar, mit der Theorie der *quasigleichen Ideale* (vgl. Anmerkung 19, S. 8) könne „leicht" gezeigt werden, daß es ausreicht, den Grundring D als Krullbereich („Integritätsring, in dem die Theorie der quasigleichen Ideale gilt") vorauszusetzen. Den expliziten Beweis führte wohl erstmalig H. Koch im Rahmen seines Habilitationsvortrages (siehe *Koch 1966*). Bereits im Jahre 1960, also drei Jahre *vor* dem Erscheinen der Eichlerschen Darstellung, gelang H. Flanders der Nachweis, daß die Kroneckerschen Quotientenringe $D[X]_{N(D)}$ und $T[X]_{N(T)}$ Hauptidealbereiche sind, wenn D ein Dedekindbereich ist (*Flanders 1960*, S. 95, Theorem A), womit sich der Fall „D faktoriell" von selbst erledigt. Flanders' Ausführungen zeigen, daß er in seinem strukturellen Verständnis der Kroneckerschen Theorie seiner Zeit deutlich voraus war. Vgl. hierzu auch den folgenden Abschnitt.

4.5. Dedekinds Ideale und Kroneckers Divisoren im Vergleich

Die Ergebnisse des vorangegangenen Abschnitts machen deutlich, daß Kroneckers Theorie der algebraischen Divisoren zunächst vor allem eine Theorie des größten gemeinsamen Teilers ist. In diesem Punkt unterscheidet sich Kroneckers Divisorentheorie sicherlich grundlegend von der Idealtheorie Dedekinds, die in erster Line auf die eindeutige Primzerlegung abzielt. Wie kommt es aber, daß beide Ansätze in dieser Hinsicht auf den ersten Blick so grundverschieden aussehen, wo sie doch letztendlich im Kummerschen Begriff der „idealen Zahl“ ihre gemeinsame Wurzel haben und beide für sich in Anspruch nehmen, den abstrakten Begriff der „idealen Zahl“ „aus der Sphäre blosser Abstraction in die Wirklichkeit algebraischer Gebilde zu versetzen“?

Kummers „ideale Zahlen“ sind aus heutiger Sicht reichlich abstrakte Gedankengebilde, deren Existenz lediglich mittelbar gegeben ist, und zwar durch die Definition gewisser Teilbarkeitsrelationen mit realen algebraischen Zahlen. Eine „ideale Zahl“ gewinnt also erst dadurch Gestalt, daß man sagt, welche algebraischen Zahlen durch sie teilbar sein sollen. In diesem Sinne sind zwei ideale Zahlen, sagen wir $\mathfrak{a}$ und $\mathfrak{b}$, als gleich anzusehen, wenn sie im Hinblick auf die realen algebraischen Zahlen, d. h. die Elemente aus dem Ring der ganzen Zahlen T des algebraischen Zahlkörpers L, dieselben Teilbarkeitseigenschaften haben. Formal ausgedrückt:

$$\mathfrak{a} = \mathfrak{b} \quad \Leftrightarrow \quad \overline{\mathfrak{a}} := \{\mu \in T : \mathfrak{a} \mid \mu\} \cup \{0\} = \{\mu \in T : \mathfrak{b} \mid \mu\} \cup \{0\} = \overline{\mathfrak{b}}. \tag{4.17}$$

Dedekinds Ansatz besteht nun darin, die „idealen Zahlen“ $\mathfrak{a}$ und $\mathfrak{b}$ dadurch zu konkret faßbaren algebraischen Gebilden zu machen, daß er statt $\mathfrak{a}$ die zugehörige Menge $\overline{\mathfrak{a}}$ betrachtet.[164] Genau hier liegt der Ursprung des Dedekindschen Idealbegriffs, der sich ergibt, wenn man von den Eigenschaften der Menge $\overline{\mathfrak{a}}$ in geeigneter Weise abstrahiert. Es stellt sich heraus, daß die so definierten Dedekindschen Ideale in einer umkehrbar eindeutigen Beziehung zu den Kummerschen „idealen Zahlen“ stehen und sich jedes Ideal, zumindest im Fall algebraischer Zahlkörper, als $\overline{\mathfrak{a}}$ schreiben läßt. Mehr noch: Definiert man für Ideale eine Multiplikation im Dedekindschen Sinne, so bilden die Ideale eine faktorielle Gruppe, und die bijektive Zuordnung zwischen Idealen und „idealen Zahlen“ wird in Wahrheit zu einem Isomorphismus.[165] Diese Lösung scheint aus heutiger Sicht vollkommen befriedigend, hat man sich doch inzwischen daran gewöhnt, zwischen isomorphen algebraischen Strukturen nicht mehr zu unterscheiden.

Kronecker jedoch war Dedekinds Zugang noch nicht konkret genug. Denn bei den Dedekindschen Idealen handelt es sich um algebraische Objekte, die lediglich die gleichen Teilbarkeitseigenschaften wie Kummers „ideale Zahlen“ haben. Sie sind mit ihnen jedoch nicht identisch und beschreiben insofern den Begriff der „idealen Zahl“ nur *mittelbar*. Kronecker schwebte offenbar ein expliziter algebraischer Ausdruck für die „ideale Zahl“ $\mathfrak{a}$ vor, mit dem sich in gewohnter Weise konkret rechnen ließ. Damit mußte jedoch Kroneckers Vorgehensweise notwendig eine andere sein als diejenige Dedekinds. Welche Schritte Kronecker gedanklich vollzog, bis er vom Begriff der „idealen Zahl“ zu seinem Begriff des algebraischen Divisors gelangte, ist heute leider nicht mehr nachvollziehbar. Einige der folgenden Überlegungen dürften jedoch mit ziemlicher Sicherheit eine Rolle gespielt haben.

Zunächst stellt man fest, daß die „ideale Zahl“ $\mathfrak{a}$ als ein größter gemeinsamer Teiler aller wirklichen algebraischen Zahlen aufgefaßt werden kann, die von $\mathfrak{a}$ geteilt werden. Dies folgt aus (4.17) — man beachte die Übereinstimmung mit dem Axiom (G 2) für Ringe mit ggT-Theorie —, und zwar wortwörtlich wie im Beweis von Lemma 2.5, S. 17. Bedenkt man ferner, daß die „ideale Zahl“ $\mathfrak{a}$ das Produkt von idealen Primfaktoren ist, so ergibt sich mit denselben Argumenten wie im Beweis von Satz 3.1, S. 32, daß jede „ideale Zahl“ der größte gemeinsame Teiler von nur

[164] Vgl. hierzu *Dedekind 1894*, S. 143, § 181.
[165] Vgl. hierzu auch *Edwards 1980*, Abschnitt 7, S. 342–346.

endlich vielen (genau genommen zwei) wirklichen algebraischen Zahlen ist. Es existieren zu jeder „idealen Zahl“ $\mathfrak{a}$ also ganze algebraische Zahlen $\alpha_1, \ldots, \alpha_m \in T$ mit $\mathfrak{a} = \text{ggT}(\alpha_1, \ldots, \alpha_m)$. Damit läuft die Suche nach einem expliziten algebraischen Ausdruck für die „ideale Zahl“ $\mathfrak{a}$ auf die Suche nach einem größten gemeinsamen Teiler je endlich vieler ganzalgebraischer Zahlen hinaus. Oder anders ausgedrückt: Gelingt es, den Ring der ganzen Zahlen T in einen ggT-Bereich einzubetten dergestalt, daß jedes Element dieses ggT-Bereiches als größter gemeinsamer Teiler von Elementen aus T geschrieben werden kann, so entspricht jedes Element des ggT-Bereiches (bis auf Assoziiertheit) umkehrbar eindeutig einer „idealen Zahl“.[166]

Wie in den vorangegangenen Abschnitten ausgeführt, besteht Kroneckers einmalige Leistung darin, mit dem Quotientenring $T[X]_{N(T)}$ genau diesen ggT-Bereich gefunden, zumindest seine Assoziiertheitsklassen beschrieben zu haben. Es wird nunmehr auch deutlich, inwiefern Kronecker seine algebraischen Divisoren zurecht als „concrete algebraische Gebilde“ in „einfacher, übersichtlicher, naturgemässer Gestalt“ charakterisiert, die der „abstracten Eigenschaften“ der Kummerschen *idealen Zahlen* oder der Dedekindschen *Ideale* entbehren[167]. Denn Kroneckers algebraische Divisoren können, ebenso wie die ganzalgebraischen Zahlen aus T, in natürlicher Weise als Elemente des Quotientenringes $T[X]_{N(T)}$ aufgefaßt werden, so daß sich Teilbarkeitsbeziehungen zwischen ganzalgebraischen Zahlen und „idealen Zahlen“, sprich: algebraischen Divisoren, zu Teilbarkeitsbeziehungen der entsprechenden Elemente in $T[X]_{N(T)}$ konkretisieren.

Ein weiterer Punkt kommt hinzu. In seinem Buch „Divisor Theory“ schreibt Edwards:[168]

> The reason Kronecker gave greatest common divisors the primary role is simple: they are independent of the ambient field while factorization into primes is not. The very notion of primality depends on the field under consideration — a prime in one field may factor in a larger field — so if the theory is founded on factorization into primes, extension of the field entails a completely new theory. Greatest common divisors, on the other hand, can be defined in a manner that does not change at all when the field is extended [...]

Hierin liegt in der Tat ein entscheidender Vorzug der Kroneckerschen Divisoren gegebenüber den Dedekindschen Idealen, jedenfalls so lange, wie man sich nach dem Vorbild Kroneckers auf Grundringe D beschränkt, in denen es ein explizites Verfahren zur Bestimmung eines größten gemeinsamen Teilers von je endlich vielen Elementen und somit ein Verfahren zur Konstruktion primitiver Polynome gibt.[169] Wir wollen diesen Punkt genauer ausführen. Dazu seien $L_1 \subseteq L_2$ zwei algebraische Erweiterungskörper über dem Quotientenkörper K von D mit den ganzen Abschlüssen $T_1 \subseteq T_2$. Nach den Ergebnissen des vorangegangenen Abschnittes sind für T_1 und T_2

[166] Möglicherweise war sich auch Dedekind dessen bewußt. In seiner „Theorie der ganzen algebraischen Zahlen“, dem berühmten XI. Supplement zu Dirichlets Vorlesungen über Zahlentheorie, beweist er mit Hilfe idealtheoretischer Überlegungen, daß jede „ideale Zahl“ als größter gemeinsamer Teiler von zwei ganzen algebraischen Zahlen darstellbar ist und umgekehrt je zwei ganze algebraische Zahlen stets eine „ideale Zahl“ als größten gemeinsamen Teiler haben (siehe *Dedekind 1894*, S. 125, § 176, Satz XII, sowie S. 143f., § 181, Satz III). Demnach, so Dedekind, könne „unter einer *idealen Zahl* [...] auch jede Zahl δ_0 verstanden werden, welche der größte gemeinschaftliche Teiler von zwei *wirklichen* [*ganzalgebraischen* ...] Zahlen α, β ist.“ (S. 144, § 181). Wie er im Vorwort zur 4. Auflage von Dirichlets Vorlesungen über Zahlentheorie schreibt, sah Dedekind hierin offenbar eine Möglichkeit, seine Idealtheorie auf „noch einfachere Grundlagen, als die bisher bekannten“ zu stellen (*Dedekind 1894*, S. 427). Es gelang ihm nach eigenem Bekunden jedoch nicht, einen unmittelbaren Beweis für die oben beschriebene ggT-Eigenschaft der „idealen Zahlen“ zu finden, der ganz ohne ideal- bzw. modultheoretische Hilfsmittel auskam.

[167] *Kronecker 1882*, S. 300 (§ 14).

[168] *Edwards 1990*, S. v.

[169] Diese Konstruierbarkeitsforderung bedeutet noch eine Abschwächung gegenüber der Forderung von *Edwards 1990*, als Grundringe nur *natürliche Integritätsbereiche* („*natural rings*“; vgl. Anmerkung 114 in dieser Arbeit) zuzulassen. Benutzt man die Kronecker-Divisoren nur zur Darstellung größter gemeinsamer Teiler, so reicht die Forderung nach Konstruierbarkeit eines größten gemeinsamen Teilers in D aus. Hat man es hingegen auf die eindeutige Primzerlegung abgesehen, so muß man — immer unter der Voraussetzung, daß die Theorie im Kroneckerschen Sinne *konstruktiv* bleiben soll — als Grundring D einen *natürlichen Integritätsbereich* zugrundelegen.

jeweils ggT-Theorien e. T. gegeben vermöge

$$[\,\cdot\,]_1 : T_1^* \longrightarrow T_1[X]^*_{N(T_1)}/T_1[X]^\times_{N(T_1)} \quad \text{und} \quad [\,\cdot\,]_2 : T_2^* \longrightarrow T_2[X]^*_{N(T_2)}/T_2[X]^\times_{N(T_2)}.$$

Bezeichnen $\alpha_1, \ldots, \alpha_m$ irgendwelche Elemente aus T_1, so wird ihr größter gemeinsamer Teiler in T_1 (bis auf Assoziiertheit) durch das Polynom $\alpha_0 + \alpha_1 X + \ldots + \alpha_m X^m$, aufgefaßt als Kronecker-Divisor, sprich: als Element des Quotientenringes $T_1[X]_{N(T_1)}$, dargestellt. Geht man zum Ring T_2 über, so bleibt $\alpha_0 + \alpha_1 X + \ldots + \alpha_m X^m$, nunmehr aufgefaßt als Element des Quotientenringes $T_2[X]_{N(T_2)}$, ein größter gemeinsamer Teiler von $\alpha_1, \ldots, \alpha_m$. Salopp formuliert: „ggT in T_1 bleibt ggT in T_2“.[170] Oder formal ausgedrückt: Die Abbildung

$$\begin{array}{c} T_1[X]^*_{N(T_1)}/T_1[X]^\times_{N(T_1)} \longrightarrow T_2[X]^*_{N(T_2)}/T_2[X]^\times_{N(T_2)} \\ [\,f\,]_1 \longmapsto [\,f\,]_2 \end{array}$$

ist ein wohldefinierter injektiver Homomorphismus. Wohldefiniertheit und Injektivität drücken sich dabei in der Beziehung

$$[\,f\,]_1 = [\,g\,]_1 \quad \Leftrightarrow \quad [\,f\,]_2 = [\,g\,]_2, \quad f, g \in T_1[X]^*_{N(T_1)},$$

aus, eine Äquivalenz, die unmittelbar aus der Gleichheit $T_2[X]^\times_{N(D)} \cap L_1(X) = T_1[X]^\times_{N(D)}$ folgt.

Im Gegensatz zum Dedekindschen Ideal ändert also ein Kronecker-Divisor beim Übergang von einer algebraischen Körpererweiterung zu einer anderen seine konkrete äußere Gestalt nicht. Was sich allein ändert, ist die Menge der zu ihm assoziierten Elemente. Ferner bleiben seine Teilbarkeitseigenschaften insofern erhalten, als derselbe Kronecker-Divisor in unterschiedlichen algebraischen Erweiterungen stets denselben größten gemeinsamen Teiler repräsentiert.

Aus alledem eine prinzipielle Überlegenheit der Kroneckerschen Divisorentheorie gegenüber der Idealtheorie abzuleiten, erscheint mir allerdings nicht gerechtfertigt. Es ist sicherlich richtig, daß Kroneckers Divisorentheorie aufgrund ihrer allgemeineren Ausgangsituation ($D = \mathbb{Z}[Y]$ statt $D = \mathbb{Z}$) der Idealtheorie von Dedekind zunächst überlegen ist. Die vorangegangenen Kapitel dieser Arbeit haben jedoch gezeigt, daß die Idealtheorie durch eine Erweiterung bzw. Modifizierung des Dedekindschen Idealbegriffes im Prüferschen Sinne, insbesondere durch Einführung der v-Ideale, der Kroneckerschen Divisorentheorie wieder weitgehend ebenbürtig wird. Wir haben gesehen, daß die Gruppe der gebrochenen v-endlichen v-Ideale isomorph zur Gruppe der Assoziiertheitsklassen von $T[X]_{N(T)}$ ist und somit v-endliche v-Ideale und Kronecker-Divisoren im Grunde miteinander austauschbare algebraische Objekte darstellen. Teilbarkeitsbeziehungen zwischen Divisoren übersetzen sich zu Inklusionsbeziehungen zwischen den zugehörigen v-Idealen, der Multiplikation von Divisoren entspricht die v-Multiplikation der zugehörigen v-Ideale und umgekehrt. Damit ergibt sich insgesamt zumindest eine theoretische Ebenbürtigkeit von Idealtheorie und Kroneckerscher Divisorentheorie.

In ihrer äußeren Gestalt und Handhabung unterscheiden sich divisorentheoretischer und idealtheoretischer Ansatz jedoch erheblich. So schreibt Eichler:[171]

> [...] beide Erweiterungen der Teilbarkeitslehre [laufen] faktisch auf das Gleiche hinaus. Zweifellos sind die Kroneckerschen Divisoren bei konkreten Problemen leichter zu handhaben als die Klassen quasigleicher Ideale [d. h. v-Ideale].

In der Tat liegen m. E. gerade darin die Stärken der Kronecker-Divisoren: So gestalten sich viele neue Begriffsbildungen in der Sprache der Kronecker-Divisoren wesentlich einfacher. Was unter der Norm, der Diskriminante oder der Differente eines Kronecker-Divisors $f \in L(X)$ zu verstehen ist, ergibt sich in natürlicher Weise aus den allgemeinen Definitionen. Die entsprechenden Begriffbildungen für Ideale sind ungleich komplizierter. Auch die Handhabung der Kronecker-Divisoren ist bequemer. Bildet man beispielsweise das Produkt zweier Divisoren, also im Grunde

[170] Zu der gleichen Einsicht gelangt bereits König; vgl. *König 1903*, S. 484ff., XI, § 9.
[171] *Eichler 1963*, S. 76f.

das Produkt zweier Polynome vom Grad m und n, so erhält man ein Polynom mit $1 + m + n$ Koeffizienten; das Produkt der entsprechenden v-Ideale ergäbe hingegen ein v-Ideal mit $m \cdot n$ v-Erzeugern (dem wiederum ein Polynom mit genauso vielen Koeffizienten entspricht). Auch die Inversenbildung gestaltet sich wesentlich einfacher, zumal wenn die Wahl des Grundringes in der oben angegebenen Weise eingeschränkt wird. Denn dann ist es möglich, zu einem Polynom f eine zugehörige primitive Form $F_{K_f/K}(f)$ zu konstruieren, und man erhält in $\frac{1}{f} \cdot F_{K_f/K}(f)$ den Repräsentanten eines zu f inversen Kronecker-Divisors. Man versuche einmal, auf ähnlich elegante Weise ein v-Erzeugendensystem für das entsprechende v-Ideal $\mathrm{c}(f)_v^{-1}$ zu finden. Bei Fragen, die im Zusammenhang mit der eindeutigen Primfaktorzerlegung stehen, kommt schließlich ein weiterer Vorzug der Kroneckerschen Divisorentheorie zum Tragen, auf den Flanders bereits im Jahre 1960 aufmerksam gemacht hat: [172]

> In many situtations it is extremely convenient, indeed almost imperative, to have a principal ideal ring instead of a Dedekind ring. The usual modern device for passing to this technically vastly simpler situation ist to localize either by passing to p-adic completions or by forming the quotient ring with respect to the complement of a finite set of prime ideals. [*Kroneckers* ...] form theory has not generally been looked upon as a tool for accomplishing this reduction to principal ideals, [...]. In a certain sense it accomplishes the task much better than does localization because with localization the bulk of the structure of the ideal group is lost, whereas with forms this structure is preserved down to the finest detail.[173]

Damit stellen die Kronecker-Divisoren m. E. eine echte, durchaus vorteilhafte methodische Alternative zur Idealtheorie dar.

[172] *Flanders 1960*, S. 92.

[173] In der Abhandlung von Flanders, die überaus aufschlußreich und m. E. zu Unrecht in Vergessenheit geraten ist, wird die Idealtheorie eines Dedekindbereiches D mit der Idealtheorie des zugehörigen Quotientenringes nach den d-primitiven Polynomen, d. h. des Nagatabereiches $D_v(X) = D_d(X)$, verglichen und zu ihr in Beziehung gesetzt. Flanders untersucht die Situtation bei Körpererweiterungen und geht in diesem Zusammenhang auch auf die Begriffe der Norm, der Diskriminante und der Differente für Ideale bzw. für Kronecker-Divisoren ein.

Literaturverzeichnis

Anderson et al. 1979. D. D. Anderson/D. F. Anderson: Generalized GCD domains. — Commentarii Mathematici Universitatis Sancti Pauli 28 (1979), S. 215–221.

Anderson et al. 1988. D. D. Anderson/David F. Anderson: Some remarks on star operations and the class group. — Journal of Pure and Applied Mathematics 51 (1988), S. 27–33.

Anderson 1988. D. D. Anderson: Star-operations induced by overrings. — Communications in Algebra 16 (1988), S. 2535–2553.

Anderson et al. 1989a. D. D. Anderson/D. F. Anderson/D. L. Costa/D. E. Dobbs/J. L. Mott/M. Zafrullah: Some characterizations of v-domains and related topics. — Colloquium Mathematicum 58 (1989), S. 1–9.

Anderson et al. 1989b. D. D. Anderson/J. Mott/M. Zafrullah: Some Quotient Based Statements in Multiplicative Ideal Theory. — Bolletino Della Unione Matematica Italiana. Serie VII. B. 3 (1989), S. 456–476.

Anderson 1993. D. D. Anderson: On t-invertibility III. — Communications in Algebra 21 (1993), S. 1189–1201.

Arnold et al. 1971. J. T. Arnold/J. W. Brewer: Kronecker function rings and flat $D[x]$-modules. — Proceedings of the American Mathematical Society 27 (1971), S. 483–485.

Aubert 1983. Karl Egil Aubert: Divisors of finite character. — Annali Die Matematica Pura et Applicata 38 (1983), S. 327–360.

Becker 1992. Ulrich Becker: Kronecker-Divisoren und ggT-Theorie. Unveröffentlichte Diplomarbeit. Mathematisches Institut der Georg-August-Universität Göttingen 1992.

Borewicz et al. 1966. Senon I. Borewicz/Igor R. Šafarevič: Zahlentheorie. — Basel/Stuttgart: Birkhäuser 1966.

Bourbaki 1989. Nicolas Bourbaki: Commutative Algebra. Chapters 1–7. — Berlin u. a.: Springer 1989.

Brewer et al. 1974. J. W Brewer/W. J Heinzer: Associated primes of principal ideals. — Duke Mathematical Journal 41 (1974), S. 1–7.

Dedekind 1892. Richard Dedekind: Über einen arithmetischen Satz von Gauß. — Mitteilungen der Deutschen Mathematischen Gesellschaft in Prag (1892), S. 1–11. Zitiert nach *Dedekind 1931*, S. 28–39.

Dedekind 1894. Richard Dedekind: Über die Theorie der ganzen algebraischen Zahlen. Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl., S. 434–657. — Braunschweig: Vieweg 1894. Zitiert nach *Dedekind 1932*, S. 1–222.

Dedekind 1931. Richard Dedekind: Gesammelte mathematische Werke, Bd. 2. — Braunschweig: Vieweg 1931.

Dedekind 1932. Richard Dedekind: Gesammelte mathematische Werke, Bd. 3. — Braunschweig: Vieweg 1932.

Edwards 1980. Harold M. Edwards: The Genesis of Ideal Theory. — Archive for History of Exact Sciences 23 (1980), S. 321–378.

Edwards et al. 1982. Harold Edwards/Olaf Neumann/Walter Purkert: Dedekinds „Bunte Bemerkungen“ zu Kroneckers „Grundzüge“. — Archive for History of Exact Sciences 27 (1982), S. 49–85.

Edwards 1984. Harold M. Edwards: Galois Theory. — New York u. a.: Springer 1984.

Edwards 1990. Harold M. Edwards: Divisor Theory. — Boston u. a.: Birkhäuser 1990.

Eichler 1963. Martin Eichler: Einführung in die Theorie der algebraischen Zahlen und Funktionen. — Basel/Stuttgart: Birkhäuser 1963.

Flanders 1960. Harley Flanders: The meaning of the form calculus in classical ideal theory. — Transactions of the American Mathematical Society 95 (1960), S. 92–100.

Geroldinger et al. 1995. Alfred Geroldinger/Jiři Močkoř: Quasi-divisor theories and generalizations of Krull domains. — Journal of Pure and Applied Algebra 102 (1995), S. 289–311.

Gilmer 1970. Robert Gilmer: An embedding theorem for HCF-rings. — Proceedings of the Cambridge Philosophical Society 68 (1970), S. 583–587.

Gilmer 1992. Robert Gilmer: Multiplicative Ideal Theory. — Kingston (Ontario): Queen's Papers 1992.

Griffin 1967. Malcolm Griffin: Some results on v-multiplication rings. — Canadian Journal of Mathematics 19 (1967), S. 710–722.

Houston et al. 1984. Evan G. Houston/Saroj B. Malik/Joe L. Mott: Characterizations of $*$-multiplication domains. — Canadian Mathematical Bulletin 27 (1984), S. 48–52.

Houston 1986. Evan G. Houston: On divisorial prime ideals in Prüfer v-multiplication domains. — Journal of Pure and Applied Mathematics 42 (1986), S. 55–62.

Huckaba et al. 1981. James A. Huckaba/Ira J. Papick: A localization of $R[x]$. — Canadian Journal of Mathematics 33 (1981), S. 103–115.

Huckaba 1988. James A. Huckaba: Commutative rings with zero divisors. — New York/Basel: Dekker 1988.

Hurwitz 1895. A. Hurwitz: Ueber einen Fundamentalsatz der arithmetischen Theorie der algebraischen Größen. — Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse (1895), 230–240.

Jaffard 1960. Paul Jaffard: Systèmes Idéaux. — Paris: Dunod 1960.

Kang 1989. B. G. Kang: Prüfer v-Multiplication Domains and the Ring $R[X]_{N_v}$. — Journal of Algebra 123 (1989), S. 151–170.

Koch 1966. Helmut Koch: Zur Begründung der Arithmetik in algebraischen Zahl und Funktionenkörpern. — Wissenschaftliche Zeitschrift der Humboldt-Universität zu Berlin. Mathematisch-naturwissenschaftliche Reihe 15 (1966), S. 187–189.

Koch 1992. H. Koch: Number Theory II. Algebraic Number Theory. — Berlin u. a.: Springer 1992.

König 1903. Julius König: Einleitung in die allgemeine Theorie der algebraischen Grószen. — Leipzig: Teubner 1903.

Kronecker 1882. Leopold Kronecker: Grundzüge einer arithmetischen Theorie der algebraischen Größen. — Crelle, Journal für die reine und angewandte Mathematik 92 (1882), S. 1–122. Zitiert nach *Kronecker 1897*, S. 237–387.

Kronecker 1897. Leopold Kronecker: Werke, Bd. 2. — Leipzig: Teubner 1897.

Krull 1932. Wolfgang Krull: Allgemeine Bewertungstheorie. — Journal für die reine und angewandte Mathematik 167 (1932), S. 160–196.

Krull 1935. Wolfgang Krull: Idealtheorie. — Berlin: Springer 1935.

Krull 1936a. Wolfgang Krull: Beiträge zur Arithmetik kommutativer Integritätsbereiche. I. Multiplikationsringe, ausgezeichnete Idealsysteme, Kroneckersche Funktionalringe. — Mathematische Zeitschrift 41 (1936), S. 545–577.

Krull 1936b. Wolfgang Krull: Beiträge zur Arithmetik kommutativer Integritätsbereiche. II. v-Ideale und vollständig ganz abgeschlossene Integritätsbereiche. — Mathematische Zeitschrift 41 (1936), S. 665–679.

Krull 1942. Wolfgang Krull: Beiträge zur Arithmetik kommutativer Integritätsbereiche. VIII. Multiplikativ abgeschlossene Systeme von Idealen. — Mathematische Zeitschrift 48 (1942/43), S. 533–552.

Lorenzen 1939. P. Lorenzen: Abstrakte Begründung der multiplikativen Idealtheorie. — Mathematische Zeitschrift 45 (1939), S. 533–553.

Malik et al. 1988. Saroj Malik/Joe L. Mott/Muhammad Zafrullah: On t-invertibility. — Communications in Algebra 16 (1988), S. 149–170.

Matsuda 1980. Ryûki Matsuda: Notes on Prüfer v-Multiplication Domains. — Bulletin of the Faculty of Science. Ibaraki University. Series A. Mathematics 12 (1980), S. 9–15.

Matsuda 1983. Ryûki Matsuda: On a Question Posed by Huckaba-Papick. — Proceedings of the Japan Academy. Series A 59 (1983), S. 21–23.

Mott et al. 1981. Joe L. Mott/Muhammad Zafrullah: On Prüfer v-multiplication domains. — Manuscripta Mathematica 26 (1981), S. 1–26.

Močkoř 1983. Jiří Močkoř: Groups of Divisibility. — Dodrecht u. a.: Reidel 1983.

Močkoř et al. 1993a. Jiři Močkoř/Angeliki Kontolatou: Groups with Quasi-divisors Theory. — Commentarii Mathematici Universitatis Sancti Pauli 42 (1993), 23–36.

Močkoř et al. 1993b. Jiři Močkoř/Angeliki Kontolatou: Quasi-divisors Theory of Partly Ordered Groups. — Grazer Mathematische Berichte 318 (1993), S. 81–98.

Papick 1982. Ira J. Papick: A Note on Prüfer v-Multiplication Domains. — Bolletino della Unione Matematica Italiana (6) 1-A (1982), S. 133–136.

Prüfer 1932. Heinz Prüfer: Untersuchungen über Teilbarkeitseigenschaften in Körpern. — Journal für die reine und angewandte Mathematik 168 (1932), S. 1–36.

Querre 1980. Julien Querre: Idéaux divisoriels d'un anneau de polynômes. — Journal of Algebra 64 (1980), S. 270–284.

Sheldon 1974. Philip B. Sheldon: Prime ideals in GCD-domains. — Canandian Journal of Mathematics 26 (1974), S. 98–107.

Skula 1970. Ladislav Skula: Divisorentheorie einer Halbgruppe. — Mathematische Zeitschrift 114 (1970), S. 113–120.

Swan 1984. R. G. Swan: n-generator Ideals in Prüfer domains. — Pacific Journal of Mathematics 111 (1984), S. 433–446.

Tang 1972. Hwa Tsang Tang: Gauss' Lemma. — Proceedings of the American Mathematical Society 35 (1972), S. 372–376.

van der Waerden 1967. B. L. van der Waerden: Algebra, Bd. 2. — Berlin/Heidelberg/New York: Springer 1967.

Weyl 1966. Hermann Weyl: Algebraische Zahlentheorie. — Mannheim: Bibl. Institut 1966.

Zafrullah 1978. Muhammad Zafrullah: On finite conductor domains. — Manuscripta Mathematica 24 (1978), S. 191–204.

Zafrullah 1984. Muhammad Zafrullah: Some polynomial characterizations of Prüfer v-multiplication domains. — Journal of Pure and Applied Algebra 32 (1984), S. 231–237.

Zafrullah 1985. Muhammad Zafrullah: A general theory of almost factoriality. — Manuscripta Mathematica 51 (1985), S. 29–62.

Zafrullah 1987. Muhammad Zafrullah: The v-operation and intersections of quotient rings of integral domains. — Communications in Algebra 13 (1987), 1699–1712.

Zariski et al. 1958. Oscar Zariski/Pierre Samuel: Commutative Algebra, Vol. 1. — New York/Heidelberg/Berlin: Springer 1958.

Lebenslauf

Ich wurde am 4. Oktober 1967 in Stade geboren. Nach der Grundschule in Buxtehude besuchte ich für zwei Jahre das Gymnasium Neu Wulmstorf, danach für vier Jahre das Gymnasium Buxtehude-Süd und anschließend das Halepaghen-Gymnasium in Buxtehude, wo ich 1986 die allgemeine Hochschulreife erwarb. Von 1986 bis 1988 diente ich als Reserveoffiziersanwärter bei der Bundeswehr. Zum Wintersemester 1988/89 immatrikulierte ich mich an der Georg-August-Universtät Göttingen im Diplomstudiengang Mathematik mit dem Nebenfach Wirtschaftswissenschaften. Nach zwei Semestern wechselte ich in den Studiengang Lehramt an Gymnasien mit den Fächern Mathematik und Geschichte. Im Wintersemester 1994/95 legte ich das 1. Staatsexamen ab. Seit dem Sommersemster 1995 bin ich als DFG-Mitarbeiter am Mathematischen Institut der Georg-August-Universität Göttingen beschäftigt.

Göttingen, den 9. Dezember 1996 *Friedemann Lucius*